

The Cyber Threat Handbook 2020

The Organised Cybercrime



Editorial



Pierre JEANNE

VP Cybersecurity Technologies
and Solutions CTS

Organised cybercrime has now reached unprecedented levels on a global scale. This demanding and incredibly complex phenomenon gives rise to as many questions as it does threats.

The damage caused to the global economy by organised cybercrime has risen to unprecedented levels since 2018, valued at a total of hundreds of billions of dollars.

According to many observers, including France's national agency for information system security (ANSSI), cybercrime will be the biggest threat we will face in the coming years. But how do we understand a phenomenon that is so diffuse, intertwined and ever-changing? How can we protect ourselves against a phenomenon that we don't completely understand, and whose outlines are blurred, at a time when the current threat level from cybercrime poses critical strategic risks for companies and organisations?

Thales's Cyber Threat Intelligence (CTI) team aims to explore this decisive question, in order to provide our partners and the general public with key insights into how organised cybercrime works.

Ransom demands now run to millions or tens of millions of euros, instead of just thousands previously, and can threaten the very survival of strategic organisations.

These ransom demands have brought sweeping change to the cybercrime threat landscape, with attackers displaying characteristics similar to major State-sponsored espionage groups while retaining their core purpose of securing financial gain.

This new report is a reflection on the nature of cybercrime, its modes of operation, the world views which inspire it, and the roles of cybersecurity actors and businesses.

The report is intended as a guide to the concepts that should be borne in mind when analysing cybercrime, and as a call for a shared reflection on the best way to create new methods of analysis. It does not take a moral stance, or engage in criticism, but seeks to identify the most effective drivers that will help people understand cybercrime, so that together we can take proactive steps to ensure everybody's security. The report offers a new and different perspective, and seeks to propose a methodology that will help our partners and the general public to understand this extraordinarily complex phenomenon and support the development of effective response strategies.

Although this report may appear demanding on the reader or unusual in its assertions, its insights could help us all to understand certain phenomena in a completely new way.

“The greatest ordeal is to fear what can be prevented.”¹

¹ Thales of Miletus, *Les sentences et adages* (Sentences and adages) (sixth century BCE).

Foreword

This ambitious report sets out several objectives that are the responsibility of all citizens, specialists, researchers and decision-makers. The reader should keep these objectives in mind.



We cannot consider our technical analyses, our reflections, our daily readings or our cyber defence policies to be definitive.

Cybercrime is a living organisation. It is therefore constantly changing, constantly redefining itself. As citizens, as specialists or as managers of small or large organisations, we have to be always vigilant in order to adapt our strategies.



As we are all victims, and even potential targets, we must change our perspective to a dynamic rather than a passive posture.

Organised cybercrime is strategic because actors embody it. It is not programmatic or deterministic. Each individual, organisation or institution is therefore a target or potential collateral victim of these evolving strategies of compromise.



Our analytical frameworks must be dynamic in order to adapt to the interaction phenomenon.

It is not an organisation of cybercriminal actors. It is an organisation of cybercriminal interactions. We need to categorise in order to understand. However, if what we seek to understand is fluid, our categories of understanding cannot be rigid. We need to focus on the nature of the interactions at the source of the cybercriminal organisation to prevent its consequences.



We cannot ignore our role as organisers of cybercrime when dealing with it.

By interacting with cybercrime - by analysing it, informing ourselves about it, protecting ourselves against it or commenting on it - we organise it. In interacting with cybercrime, we cannot exclude the implications of our actions in the way we conduct ourselves. We have to be conscious of the need for responsibility in our daily personal and professional lives.



By understanding these principles, we can be proactive towards the phenomenon in our daily lives as citizens, researchers, specialists, or decision-makers.

Cybercriminal interactions and the cybercriminal organisation are co-constituent. We understand in this work that these interactions take the form of relationships of competition, of reference, of will to distinguish oneself, of dependence on others and of will to be independent by perpetuating the meaning given to acts. By understanding our responsibility in the organisation of cybercrime, we accept to be part of a game. It is only by accepting to be part of it that we can understand these principles of interaction.

Table of contents

INTRODUCTION	6
• Cybercrime gets organised	6
• France: organised cybercrime takes centre stage	7
• Huge costs make for a strategic challenge at global level	8
• Vast revenues on a global scale	8
• Finding a strategy to meet the challenges of organised cybercrime	8
- A guide to aid understanding	8
- The organising principles behind cybercrime	9
• Why this report was written	13
TOWARDS A NEW WAY OF UNDERSTANDING ORGANISED CYBERCRIME	14
• Engaging with the complexity of cybercrime	14
- Hard to define by definition: construct versus perception	14
- Understanding the organised nature of cybercrime: key to an effective understanding of the phenomenon	17
- A living, organised phenomenon that cannot be analysed effectively via a snapshot vision	18
- A concept that may appear virtual, but which harbours real challenges and consequences	19
• A different reading of cyber threats	21
- Cybercrime as a web of intertwined interactions	21
- Cybercrime defined as an interlinking of interactions	24
- Dynamic analysis: understanding an object by navigating through it	26
- We are part of the makeup of cybercrime	28
• Organised cybercrime: a criminal social organisation with determinants of a technical nature	30
- Understanding the interlinked relationships between 'macro' and 'micro'/'contextual' and 'individual' phenomena	30
- Cyberdefence as a discipline first, a provider of operational tools second	32
ORGANISED CYBERCRIME	34
• The determining factors of strategic cybercrime interaction	35
- Differentiation via competition and referencing	35
- Specialisation based on strategic and technical distinction: the source of the division of labour in cybercrime "society"	38
• Interaction and the cybercrime organisation	42
- Independence within interdependence (organic solidarity)	42
- Cybercrime culture: shaping action	45
APPLICATION DE CES CONCEPTS AUX PHÉNOMÈNES DE BIG GAME HUNTING ET DE CHANTAGE À LA DIVULGATION	50
• Engaging with complexity: a resurgence of ransomware attacks, or a change in behaviour?	50
• «Increase in ransomware attacks» refers to the confirmation of the BGH paradigm (dynamic vision).	51
- BGH: a new distinctive feature for major cybercriminals (specialisation)	51
THE WIDESPREAD ADOPTION OF BLACKMAIL DISCLOSURE IS THE RESULT OF A COMPLEX PROCESS	52
• The origins of a not-so-new phenomenon (differentiation/specialisation and a sustainable sense of purpose)	56
• Emergence as a result of a diverse set of factors (differentiation/specialisation and a sustainable sense of purpose)	57
- From tactical change and peer adoption to confirmation of effectiveness	57
- Inspiration based on pre-existing practices from outside the cybercrime arena	57
- Identifying internal developments in the cybercrime arena	60
- A practice resulting from a strategic reflection centred on an in-depth perception of cyberdefence responses	61
CONCLUSION	66
• A guide and inputs to aid understanding	66
• New keys to understanding	68
• Application to a use case: disclosure blackmail	69
• Recommendations and good practices	72



Introduction

Thales's Cyber Threat Intelligence (CTI) team has been monitoring cybercrime for several years.

Since mid-2018, a significant new trend has been observed, involving a new form of attack focused in particular on ransomware in France and in other countries.

The proliferation in ransomware attacks has taken place against the backdrop of the broader phenomenon of Malware-as-a-Service (MaaS), as well as more extensive interactions between major cybercriminals.

High-level MaaS capabilities are emerging to support the practice of Big Game Hunting (BGH), which is explained in this report and presents a major threat to organisations.

A number of Ransomware-as-a-Service operations also proved to be particularly effective in 2019. One of the best known, GandCrab (developed by [ATK168 - Pinchy Spider](#)), announced that it was shutting down operations the same year, having achieved total earnings of \$150 million in twelve months², to be replaced by other services such as Sodinokibi (likely developed by the same group).

CYBERCRIME GETS ORGANISED

In 2019, [ATK88 \(FIN6\)](#) deployed its Ryuk ransomware to target the bio-analysis firm Eurofins. The company reported a loss of 62 million euros linked to the attack in its quarterly results. The same group, which also targeted three hospitals in Alabama, the city of New Orleans, and the firms Altran (which lost 20 million euros) and Norsk Hydro (75 million euros) with its LockerGoga ransomware, is closely linked to another major cybercrime group, [ATK103 \(TA505\)](#), which this year used its CIOp ransomware to attack Rouen University Hospital.

We also know that the first group, [\(ATK88-FIN6\)](#), uses the FlawedAmmy malware developed by the second group, [\(ATK103-TA505\)](#). These existing links were subsequently strengthened by the emergence of another group, [ATK104 \(Mummy Spider\)](#) and its loader malware, Emotet. So what is behind this closer relationship, and how does it increase the threat?

Essentially, as a loader, Emotet downloads other malware to the machines that it has infected, and simply sits in place to manage the download process. However, the number of machines infected by Emotet across all sectors of the economy is huge.

² <https://news.sophos.com/fr-fr/2019/06/05/ransomware-gandcrab-tire-sa-reverence/>



Until recently, Emotet downloaded several different items of malware, in particular TrickBot, itself sometimes used by the Ryuk ransomware from [ATK88 \(FIN6\)](#).

Although we don't know the precise nature of the links between the three cybercrime groups [ATK88 \(FIN6\)](#), [ATK103 \(TA505\)](#) and [ATK104 \(Mummy Spider\)](#) – in other words whether they are of a commercial nature or based on mutual support – this convergence of interests certainly has the potential to create an extremely powerful network. Emotet, strengthened by this link with [ATK103 \(TA505\)](#) and [ATK88 \(FIN6\)](#), is capable of dropping ransomware with devastating consequences.

In May 2019, Baltimore (Maryland) was hit by the RobbinHood ransomware, in an attack that cost the city a total of \$18 million³. A total of 22 US cities were targeted by massive ransomware campaigns in 2019, with the city of New Orleans declaring a state of emergency in mid-December after being infected by the Ryuk malware from [ATK88 \(FIN6\)](#)⁴.

In October 2019, the M6 Group, France's largest privately-owned multimedia company, was hit by the BitPaymer ransomware created by [ATK180 \(Indrik Spider\)](#). BitPaymer demands ransoms of up to 216 bitcoins⁵ ((equivalent to approximately 2 million euros at October 2019 values⁶). A number of attacks on city authority networks were also observed, including certain networks that are of critical importance for local populations but are very poorly protected.

These few examples are typical of the changes currently taking place at the highest levels of cybercrime. Such developments are difficult to track, but their consequences are significant.

In early 2020, Guillaume Poupard, Director-General of France's national agency for information system security (ANSSI), said in an interview with the French newspaper Les Échos that "The biggest threat in future [will be] organised cybercrime⁷ ».

With several months of the year 2020 still remaining, ANSSI has already handled 104 ransomware attacks in France, an increase of 34% compared with last year, when 69 attacks took place.

The consequences of such attacks, in terms of business continuity and even the very survival of the targeted organisation, are becoming increasingly devastating.

FRANCE: ORGANISED CYBERCRIME TAKES CENTRE STAGE

³ <https://www.leparisien.fr/economie/la-cyberattaque-de-baltimore-a-coute-plus-de-18-millions-de-dollars-a-la-ville-20-07-2019-8120535.php>

⁴ <https://www.usine-digitale.fr/article/la-nouvelle-orleans-en-etat-d-urgence-face-a-une-cyberattaque-d-envergure.N913859>

⁵ CROWDSTRIKE. CSA-19255 INDRIK SPIDER Demands Highest BitPaymer Ransom to Date Changes to Ransomware Observed. 22 Feb. 2019.

⁶ <https://fr.investing.com/crypto/bitcoin/historical-data>

⁷ <https://www.lesechos-fr.cdn.ampproject.org/c/s/www.lesechos.fr/amp/1164596>



HUGE COSTS MAKE FOR A STRATEGIC CHALLENGE AT GLOBAL LEVEL

This phenomenon has reached even more worrisome proportions at global level.

The United Nations and Accenture estimate that organised cybercrime will cost the global economy around \$5.2 trillion⁸ between 2020 and 2025. Cybersecurity Ventures places the estimated cost at \$6 trillion per year⁹.

This is equivalent to half of China's GDP being lost every year as a result of what we must now understand as organised cybercrime. The phenomenon has clearly assumed strategic proportions.

VAST REVENUES ON A GLOBAL SCALE

The phenomenon is also gaining in significance in terms of revenues. The Cybersecurity firm Bromium, and Dr Mike McGuire, a researcher in criminology at the University of Surrey (UK), estimate that revenues from cybercrime totalled \$1.5 trillion in 2018¹⁰.

This means that cybercrime generates 1.5 times more income (as an annual average) than counterfeiting, and 2.8 times more than the illegal drugs trade (3.5 times more according to the highest estimate)¹¹.

FINDING A STRATEGY TO MEET THE CHALLENGES OF ORGANISED CYBERCRIME

This is what this report is all about. We have to ask ourselves how cybercrime has reached such levels, and why it is so difficult for us to understand.

Thales's CTI team has conducted an in-depth analysis of the phenomenon, and has developed some key insights to aid greater understanding of the nature of the organisation behind the threat.

> A GUIDE TO AID UNDERSTANDING

Cybercrime appears to be a living organism.

UNDERSTANDING THE DIFFERENCE BETWEEN PERCEIVED CYBERCRIME AND OUR CONSTRUCT OF CYBERCRIME

As part of our work, we identified a number of principles. Firstly, it is important to distinguish between **perceived cybercrime** and our **construct of cybercrime**. This split between construct and perception is linked to the way we consider the phenomenon itself.

⁸ Estimates provided by Xavier Raufer, holder of a doctorate in geopolitics from Sorbonne University, Paris. A criminologist since 1975, Xavier Raufer has built up extensive expertise in social and political violence, terrorism and organised crime. He heads the department for research into contemporary criminal threats at Paris 2 Panthéon-Assas University. He is also an associate professor at a number of universities around the world, including Fudan University in Shanghai, and George Mason University in the United States, and is a regular contributor to the media (including Atlantico, Boulevard Voltaire, etc.). Dr Raufer is currently editing a collection of essays on criminology for the scientific publisher CNRS-Editions, and has written several books on criminology and terrorism, the most recent of which was entitled *Cybercriminologie* (Cybercriminology) (Editions CNRS, 2015): <https://eesd.cnam.fr/membres/xavier-raufer-1114293.kjsp?RH=1593770472451>



When analysing the phenomenon of organised cybercrime, we perceive it to be extremely complex. We make an effort to simplify it, in order to explain it to our personnel and partners. Yet we increasingly tend to reify this simplified form of organised cybercrime – to give it concrete form – so that we increasingly believe that the construct of cybercrime is our perception of cybercrime.

This means that we are no longer analysing what we actually perceive, but what we have constructed intellectually on the basis of our simplification. As a result, we are not fully able to comprehend certain phenomena, such as the emergence of data disclosure blackmail, targeted at organisations by major ransomware operators.

In this report, therefore, we will endeavour to re-establish the fundamentals of these two realities: our construct, and our perception.

We perceive that cybercrime is an organisation, an organism, a space for an infinite range of interactions between a multitude of independent yet interdependent players.

A DYNAMIC VISION: MORE EFFECTIVE THAN A SNAPSHOT ANALYSIS

Analysing this phenomenon requires a **dynamic vision**.

This means navigating right to the heart of the subject, while accounting for uncertainties related to the context, and examining our own role in the organisation of organised cybercrime.

This dynamic approach is the only way to achieve the required level of reflexivity and self-criticism, and overcome the limitations associated with our usual **snapshot analysis**.

With a snapshot analysis, we categorise, sub-categorise, and even over-categorise, so that we end up considering the different dimensions independently of one another, and constructing only a unidirectional vision.

A dynamic analysis is strategically focused and lucid; a snapshot tends to be programmatic and deterministic.

› THE ORGANISING PRINCIPLES BEHIND CYBERCRIME

The sole aim of this methodology based on reflexive self-criticism is to identify the major principles behind organised cybercrime, using a set of analytical tools that boost our understanding and help us to eliminate bias.

⁹ <https://1c7fab3im83f5gqiw2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>

¹⁰ <https://securityintelligence.com/news/cybercrime-profits-soar-to-1-5-trillion/>

¹¹ By way of comparison, the illegal drugs trade generated annual revenues of between \$426 and \$652 billion at global level between 2014 and 2017, while counterfeiting generated between \$923 billion and \$1.13 trillion over the same period: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>



Organised cybercrime is a space where interactions take place. Yet these interactions are themselves spaces. We have to move away from an approach based on systematic and exclusive micro-analysis of units, attackers, tools, arsenals, etc., and force ourselves to focus on the interactions between units.

THE ROLE OF DIFFERENTIATION AND SPECIALISATION IN THE EXPANSION OF CYBERCRIME

The first principle identified here is the living nature of organised cybercrime, which is going through a process of [organisational expansion](#).

thanks to the continuous proliferation of cybercrime actors and interactions between them. This process is driven by two trends that can be observed among today's organised cybercrime actors: [differentiation](#) and [specialisation](#).

The concept of differentiation

Attackers are constantly looking, albeit unconsciously, to differentiate themselves. The unconscious nature of this search for differentiation is linked to two types of instincts that can be found in other social spaces: [the reference instinct](#), and [the competitive instinct](#). These instincts are highly visible in the Big Game Hunting (BGH) arena, for example.

The reference instinct pushes attackers to monitor themselves continuously to check that they are not being left behind, and to ensure that they continuously improve their tactics, techniques and procedures (TTPs). The competitive instinct is the corollary of the reference instinct: although they are not in direct opposition, the fact that attackers are operating in the same space, and employing similar TTPs and arsenals, only serves to foster competition.

These two instincts drive a process of differentiation, a search for improved performance, innovation, and sometimes even recognition.

The concept of specialisation

The compulsive search for differentiation is intrinsically linked to the drive for [specialisation](#). To exist as credible actors within the cybercrime universe, attackers have to specialise by displaying [strategic distinction](#) or [technical distinction](#).

Actors who employ disclosure blackmail are displaying strategic distinction.

Actors such as [ATK104 \(Mummy Spider\)](#), who developed the Emotet loader, are characteristic of technical distinction.

As we shall see, these two types of distinction are, once again, two sides of the same coin, in that they are both aspects of specialisation.



CONCENTRATION WITHIN CYBERCRIME, LINKED TO “INDEPENDENCE WITHIN INTERDEPENDENCE” AND A SUSTAINABLE SENSE OF PURPOSE

Organised cybercrime, despite its natural expansion, retains a form of constancy. There is something that counterbalances this expansion, and ensures harmony within this complex phenomenon.

Independence within interdependence

Differentiation and **specialisation** lead to the expansion of cybercrime, by increasing the number of actors and interactions. However, this apparently disorganising pressure is counterbalanced by a **process of concentration** within the organisation.

As we have explained, a trend towards differentiation and specialisation can be observed among cybercrime actors; this causes the organisation to expand. Yet it is one of the greatest paradoxes of organised cybercrime that these natural inclinations on the part of actors actually ensure the harmony of the overall organisation. Attackers become **independent in their interdependence**.

As they differentiate and specialise, actors have a growing need for interactions with their peers. They can only be independent in their actions by being mutually dependent on one another. This is what we refer to as **independence within interdependence**.

For example: the Emotet model requires buyers within the Big Game Hunting arena to make it work, while those same buyers need the services of Emotet to make their model work.

Major organised cybercrime actors draw strength from their dependence on other major actors; this enables them to become independent in the pursuit of their own strategies.

A sustainable sense of purpose

Finally, one of the concepts and tools that we propose here is a co-constituent of this trend towards interdependence and concentration within organised cybercrime. We refer to this as **a sustainable sense of purpose**.

A culture exists at the highest levels of cybercrime which functions as an overall organising principle.

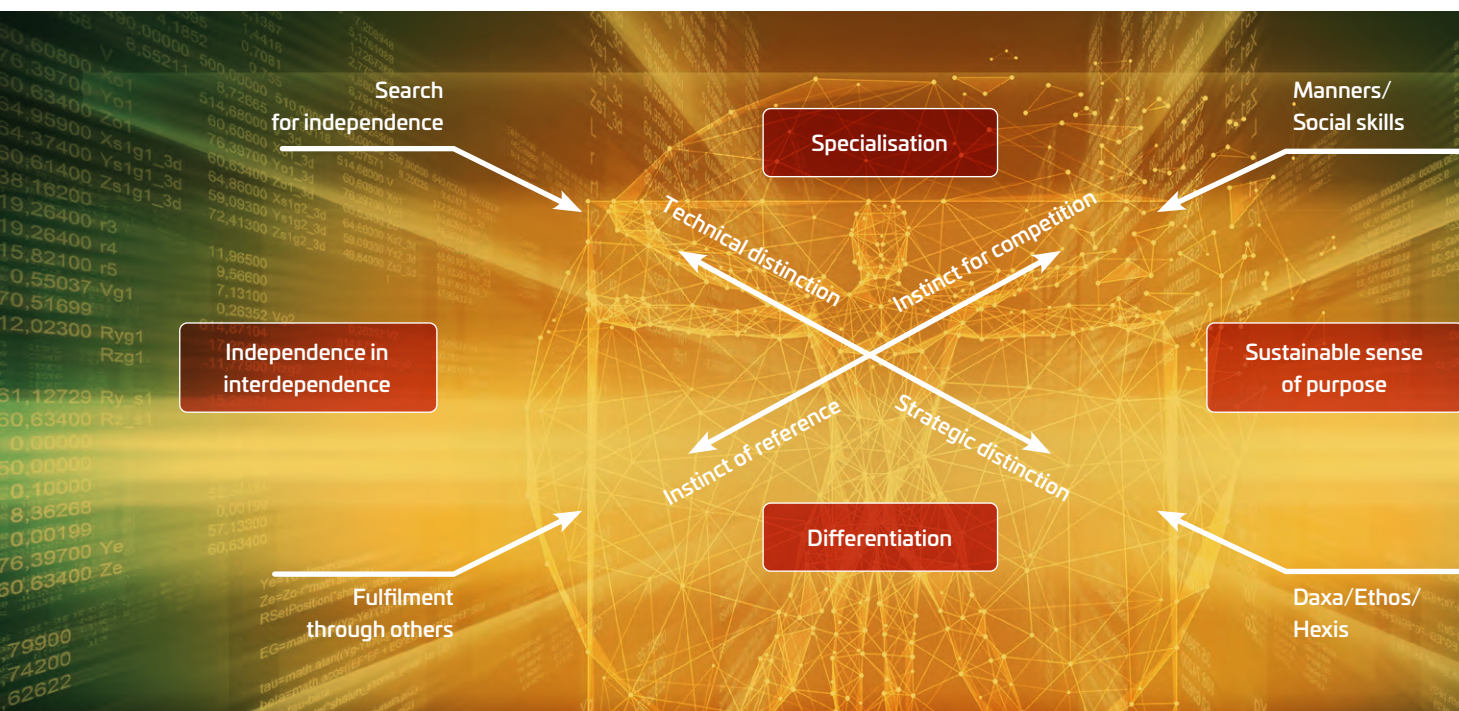
This culture can be readily identified when observing certain practices which, although they are not always rational, appear to be framed by a **code of cybercriminal behaviour**. This code consists of a set of principles, representations and norms which underpin the actions of cybercriminals and guide their purpose.



What we have here is a kind of **doxa** – a body of shared opinion, manifested as a principle of commitment on the part of attackers. They believe that if they commit fully to this shared code of cybercriminal behaviour when carrying out an attack, the attack will have a greater chance of succeeding. This belief forms part of a deeply embedded culture or **ethos**.

The attackers' perception is based on the evidence of their own experience. Unless they are driven to do so by external influences, they will behave as they have always behaved.

We illustrate these cultural structures using the example of the professional attitude adopted by major cybercriminals towards their victims.



Contextual corpus
developed to explain the
living nature of organised
cybercrime.

Finally, these two principles (the principles of commitment and perception) form the basis of a hexis, a “way of being” when carrying out actions, a “natural” behaviour on the part of attackers, accompanied by a set of practices which have become established as habitual.



This report is a reflection on the nature of cybercrime, its modes of operation, and the place occupied within it by cybersecurity actors and businesses.

It does not take a moral stance, or engage in criticism, but seeks to identify the most effective drivers that will help people understand cybercrime, so that together we can take proactive steps to ensure everybody's security.

The aim is to offer a new and different perspective, and to propose a methodology that will help our partners and the general public to understand this extraordinarily complex phenomenon and support the development of effective response strategies.

Although this report may appear demanding on the reader or unusual in its assertions, its insights could help us all to understand certain phenomena in a completely new way:

- Big game hunting has been ravaging organisations since 2018 (victims include Rouen University Hospital, and firms such as Altran, Eurofins, etc.), with unusually sophisticated attacks and ransom demands running to millions of euros. The sheer scale of this phenomenon is symptomatic of the profound changes that have taken place in the world of cybercrime.
- A new trend is emerging in 2020 involving blackmail based on threats to disclose organisations' online data (disclosure blackmail). The method explained in this report is designed to help readers understand the origins of a development which, this year, has rocked cybersecurity policies to the very core and plunged organisations into uncertainty.

The Thales CTI team's humble attempt to provide clarity and serenity in the face of such changes is inspired by the following aphorism:

« The greatest ordeal is to fear what can be prevented.¹² »

¹² *Thales of Miletus, Les sentences et adages (Sentences and adages) (sixth century BCE).*

Towards a new way of understanding organised cybercrime

ENGAGING WITH THE COMPLEXITY OF CYBERCRIME

> HARD TO DEFINE BY DEFINITION: CONSTRUCT VERSUS PERCEPTION

What is cybercrime? As a security company, we often leave those who ask this question feeling short-changed, because we struggle to give an entirely suitable answer that addresses both the individual and contextual aspects of the issue.

Instinctively, we focus on analysing the nature of the attackers, defining them on the basis of their motivation and their resources – in other words, the technical arsenal they are capable of deploying.

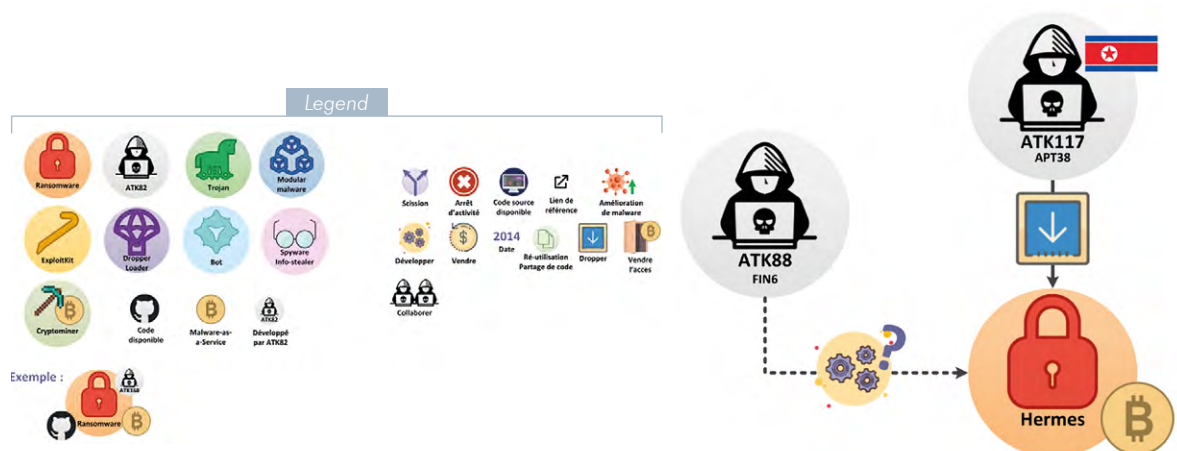
Cybercrime is committed by groups of attackers with a shared motivation: to seek financial gain using cyber-specific tools such as ransomware, cryptominers, etc. It is this motivation, and these techniques, which define such attackers as cybercriminals.

So, do we think that's a definitive answer to the question? Nothing could be further from the truth.

This answer appears to contain a number of paradoxical elements:

- > What about groups of attackers, such as some Lazarus sub-groups, which are categorised as State-sponsored (i.e. Advanced Persistent Threats (APTs)), and therefore not as criminal groups, and which conduct financially motivated attack campaigns?
- > What about groups in the cybercriminal category, often associated with the concept of Big Game Hunting, such as Maze, which have strategies and technical infrastructure similar to those of some State-sponsored espionage groups?

Some State-sponsored groups adopt cybercrime TTPs, and even use cybercrime attack infrastructure





These paradoxes lead us back to the original question.

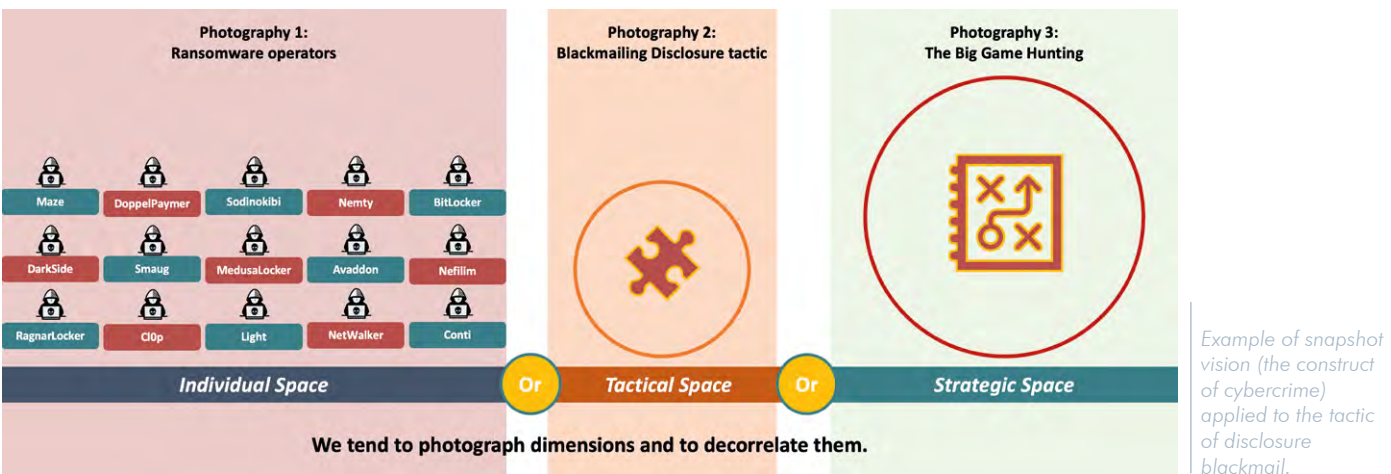
“Cybercrime” is a word, an abstraction, defined by those who are faced with this distinctive reality, those who consider themselves part of it (cybercriminals) and those who seek to analyse it (targets and security companies). These actors are part of the reality that they are seeking to describe.

As security companies, we distinguish between cybercrime actors and other cyber actors, between targeted organisations and non-targeted organisations, based on purely intellectual and intentionally selected factors. We do this with reference to the supposed nature of what we are observing, i.e. the attackers. However, they are also observing us, and interacting with us by adapting their attacks. It is this triple dynamic – our construct, their construct, and a combination of the respective constructs – which creates cybercrime as a distinct idea, an abstraction.

This means that there are actually two forms of cybercrime: perceived cybercrime, and the abstract construct of cybercrime. We need to look at how these two forms can potentially distort our analysis.

This is what makes the work of analysts so difficult. We have to deconstruct the assumptions of those we are observing (the attackers), our own assumptions in relation to what we are observing (ourselves), and the assumptions of other analysts (our colleagues), while also continuously deconstructing the analysis framework of our community of reference (the cyber threat intelligence/cyberdefence community).

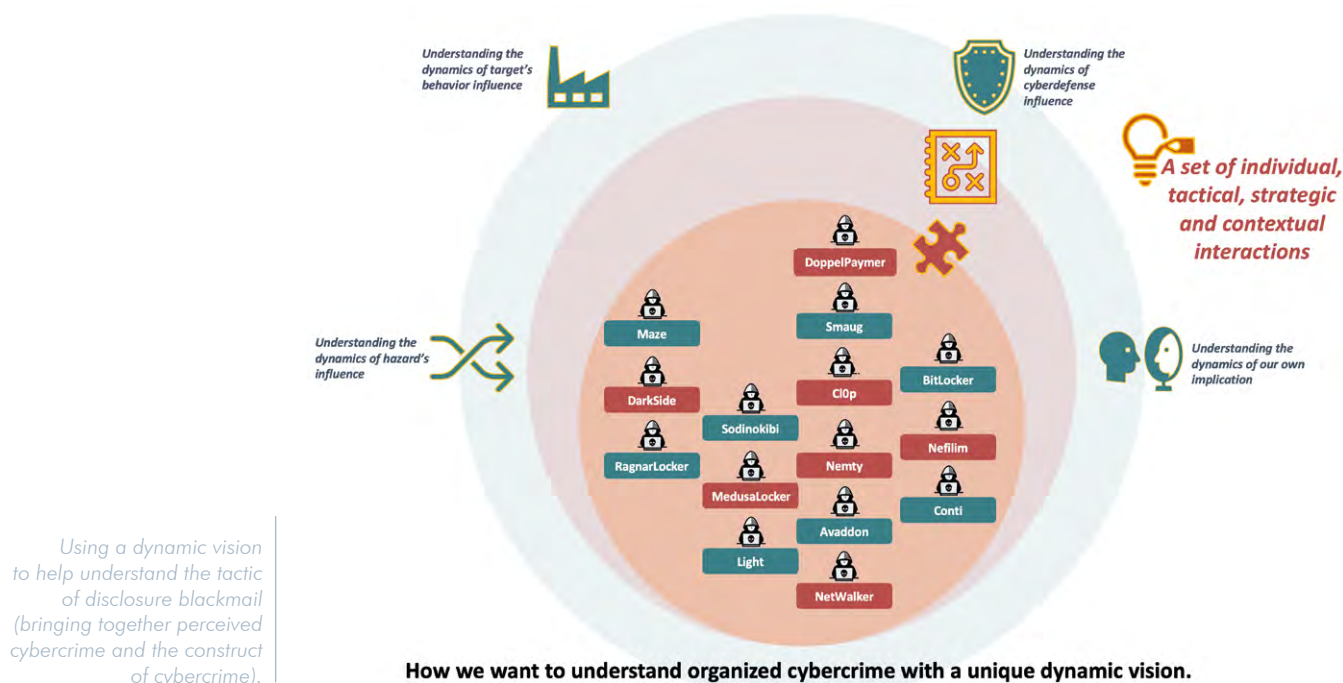
This is what we aim to establish in this report on cybercrime.





It seems to us that the objects used to define cybercrime distort the reality of cyberdefence that we are aiming to capture. The analytical approach that we have observed being used to create the construct of cybercrime is often a deterministic, snapshot approach. Cybercrime is made up of criminal actors seeking financial gain. They employ a rational *modus operandi* (in the form of their TTPs) to achieve this. They use ransomware, encrypt data, etc. None of this is incorrect, but it quickly leads to a feeling of unease, manifested in a sense of incompleteness.

In this report, we propose to apply a dynamic element to this snapshot vision. What do we mean by a dynamic vision? The snapshot-type description referred to in the previous paragraph focuses on fixing stable, exclusive spaces as part of a co-construction approach. We describe and categorise an organisation, the construct of cybercrime, on a snapshot basis; we do not analyse it. We rarely ask ourselves where this construct comes from, and what its principles are. A dynamic vision seeks to include ourselves, as observers, in cybercrime, to include the construct of cybercrime within perceived cybercrime, and to bring these two forms together. This vision necessarily involves self-criticism of our own approaches to analysis. This is the basis of our method *C'est un appel à la méthode*.





➤ UNDERSTANDING THE ORGANISED NATURE OF CYBERCRIME: KEY TO AN EFFECTIVE UNDERSTANDING OF THE PHENOMENON

To start with a logical assumption: using the term “cybercrime” to define the subject of our discussions means that a phenomenon, with a distinctive organisation, does indeed exist, which merits our use of the term. We apply a distinctive descriptor only when what we observe has a distinctive character.

To go back to our starting point: we describe cybercrime, we see it, as a structure, an organisation.

In early 2020, Guillaume Poupard, Director-General of France’s national agency for information system security (ANSSI), said in an interview with the French newspaper Les Échos:

« The biggest threat in future [will be] organised cybercrime ¹³ ».

This statement from the person responsible for information system security in France is neither a prophecy, nor conjecture. The way that the cybercrime phenomenon has been growing and taking shape in recent years provides definitive evidence of this reality: cybercrime exists as an organisation.

To understand this phenomenon of the “organised” nature of cybercrime, we propose to deconstruct the evolution of the dynamic referred to by Guillaume Poupard. We propose to analyse the organisation of perceived cybercrime. Cybercrime should no longer be considered as an observable phenomenon, but as having an organised, comprehensible logic.

This emerging organisational process is key to understanding global cybercrime and its impact on companies.

We are now faced the problem of answering the following question: how is perceived cybercrime organised? This is where the analysis becomes more difficult.

Explaining cybercrime is just as difficult as defining it. Yet the logic is the same.

We organise cybercrime through our cyberdefence policies, which are based on what we – both cybercriminals and ourselves – consider to be cybercrime (this is the construct of cybercrime).

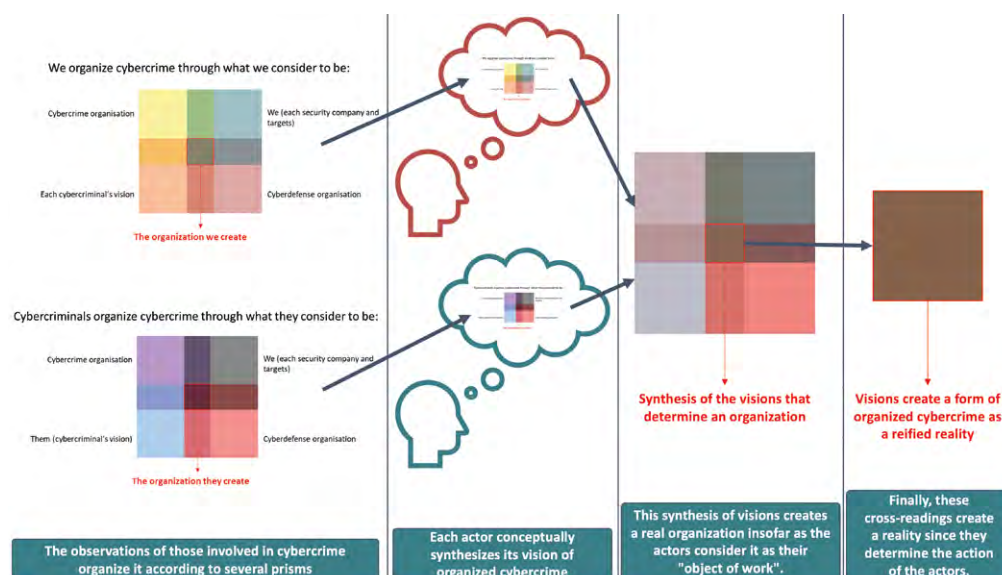
¹³ <https://www.lesechos-fr.cdn.ampproject.org/c/s/www.lesechos.fr/amp/1164596>



Cybercriminals organise cybercrime through the conception that they have of it, the conception that they have of us and our cyberdefence, and the conception that they have of themselves. Cybercrime organises itself, and is organised by cybercriminals and ourselves. Uncertainties related to the external context also play a role.

At this stage, identifying the keys to understanding cybercrime is a complex matter; analysis appears increasingly difficult. This is because the construct of cybercrime is permanently in our minds. Yet there is one invariable factor: interaction, which acts as the living element of the organisation.

We mentally organise cybercrime in the form of a construct of cybercrime, and refer to this mental abstraction as the basis for taking action.



> ALIVING, ORGANISED PHENOMENON THAT CANNOT BE ANALYSED EFFECTIVELY VIA A SNAPSHOT VISION

Organised cybercrime takes the form of a living self-eco-organisation¹⁴ :

- > It is referred to as an «organisation» because it continuously sustains itself as a phenomenon that is distinctive in terms of how it appears from the outside, and how it operates internally.
- > The reference to "self" expresses the fact that all the actions, aspirations and imaginings of cybercrime and cyberdefence actors, although they may appear disorganised, are the source of the phenomenon's organised nature, while also being the essence of the phenomenon itself.

¹⁴ Introduction à la pensée complexe (Introduction to complex thought), Edgar Morin, Éditions du Seuil, 2005.



- The «eco» element indicates that cybercrime does not exist in isolation, despite our abstractions. It interacts repeatedly with different environments (political, social, psychological, technical, etc.).

To the observer, it appears unitary and organised, retaining a form of continuity in its distinctiveness, and therefore its “identity”, although in reality it is disorganised, and is subject to a multitude of changes.

It therefore appears complex, because it is driven by a vast number of internal interactions, as well as various types of external interactions, which are themselves co-constituent elements. It is complex not only because it is not solely technical in nature, but also because it is not purely rational in terms of a cost/benefit model with a solely financial viewpoint (there is also the issue of fundamental reputational capital, for example). Finally, it is also subject to uncertainty, chance and the patterns of thinking of its actors. This last element among the myriad aspects of the complexity of organised cybercrime is key to its organisational autonomy.

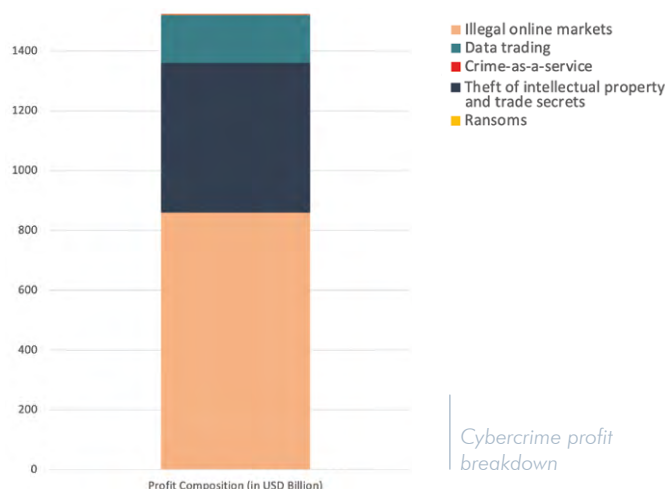
This explanation might almost give the impression that cybercrime does not exist, at least not as we understand it within the scope of our construct of cybercrime. However, even though, for the time being, we are unable to pin down a definition of what it is, we know, thanks to the way in which it is manifested (in other words, the consequences of cybercrime), that it is part of a perceptible reality which is capable of being analysed.

➤ A concept that may appear virtual, but which harbours real challenges and consequences

The Cybersecurity firm Bromium, and Dr Mike McGuire, a researcher in criminology at the University of Surrey (UK), estimate that revenues from cybercrime totalled \$1.5 trillion in 2018¹⁵.

This figure becomes even more striking if we compare it with revenues from other illegal activities.

The report on «Transnational Crime and the Developing World» published by the American think tank Global Financial Integrity¹⁶, reveals that the illegal drugs trade generated annual revenues of between \$426 billion and \$652 billion at global level between 2014 and 2017, while counterfeiting generated between \$923 billion and \$1.13 trillion over the same period¹⁷.



¹⁵ <https://securityintelligence.com/news/cybercrime-profits-soar-to-1-5-trillion/>

¹⁶ <https://www.talkingdrugs.org/report-global-illegal-drug-trade-valued-at-around-half-a-trillion-dollars>

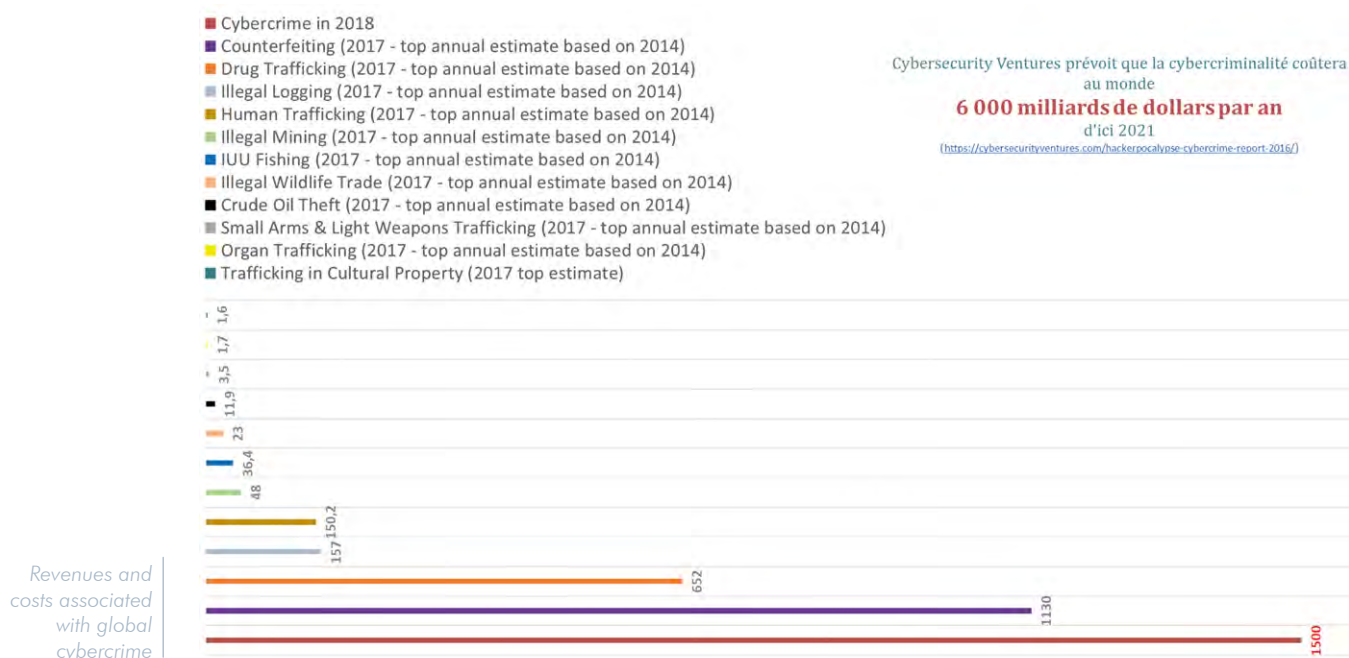
¹⁷ <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>



This means that, on a global scale, cybercrime generates 1.5 times more income (as an annual average) than counterfeiting, and 2.8 times more than the illegal drugs trade (3.5 times more according to the highest estimate).

Looking at a breakdown of the \$1.5 trillion in profits generated by cybercrime, we can see that the vast majority of these revenues originate from illegal online markets (57.3%) and theft of intellectual property and trade secrets (33.3%). Revenues from ransoms – which receive extensive media coverage – represent only 0.07% of estimated profits.

Despite the sheer size of the amounts involved, the real problem that we have identified with regard to cybercrime is not so much the profits themselves, but the damage done to the global economy. In 2018, McAfee and the Centre for International Strategic Studies estimated that cybercrime had caused losses worth a total of \$600 billion at global level¹⁸. The highest estimates, such as those from the United Nations and Accenture for the period 2020-2025, and from Cybersecurity Ventures for 2021, predict that organised cybercrime will cost the global economy around \$5.2 trillion¹⁹ and \$6 trillion²⁰ respectively.



¹⁸ <https://www.mcafee.com/enterprise/fr-ca/assets/executive-summaries/es-economic-impact-cybercrime.pdf> & https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf

¹⁹ Estimates reported by Xavier Raufer (holder of a doctorate in geopolitics from Sorbonne University, Paris): <https://eesd.cnam.fr/membres/xavier-raufer-1114293.kjsp?RH=1593770472451>

²⁰ <https://1c7fab3im83f5gqiw2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>



> CYBERCRIME AS A WEB OF INTERTWINED INTERACTIONS

Cybercrime, therefore, is an organisation which grows out of the disorganisation created by actors (attackers, targets and observers), as well as out of context-related uncertainties. The disorganisation is itself created by cybercrime as an organisation.

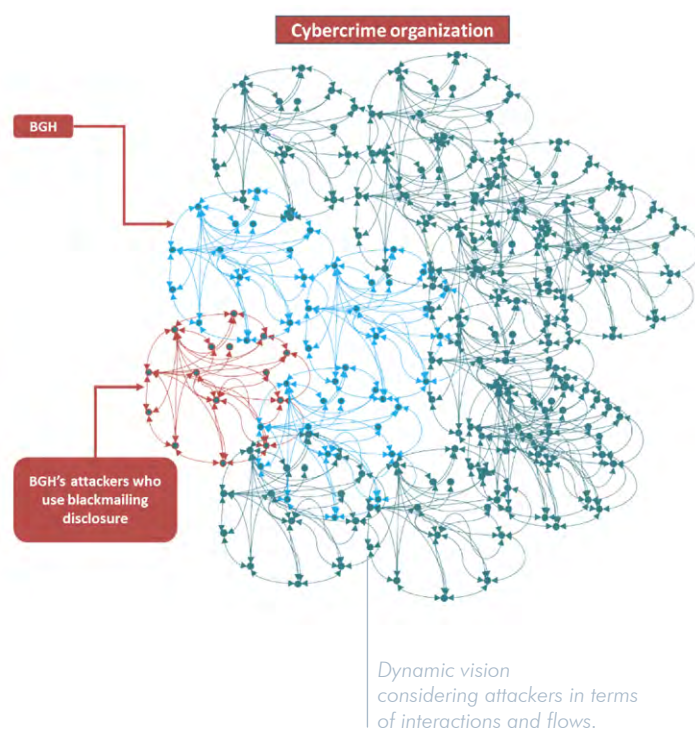
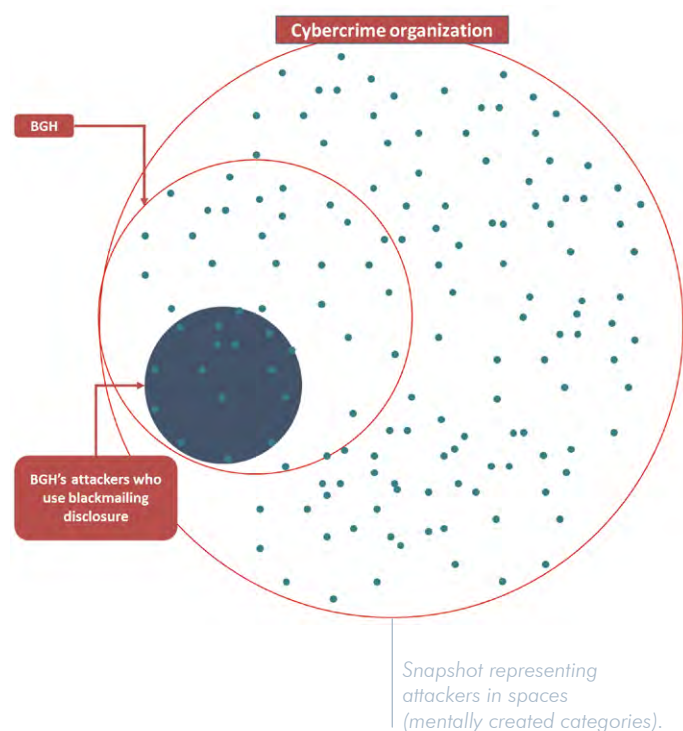
It is a space in which an infinite number of interactions take place. It can be viewed in two different ways:

- > As a cybercrime space, an organised sphere, by means of a snapshot vision.
- > As an infinite number of interactions, with perpetual, disorganised links, by means of a dynamic vision.

With a vision that encompasses both of these readings, the sphere becomes a set of infinite links, which is itself a sphere.

We must consider the cybercrime space as “cybercrime interactions”, and “cybercrime interactions” as the cybercrime space. The object is a process, and the process is an object.

A DIFFERENT READING OF CYBER THREATS



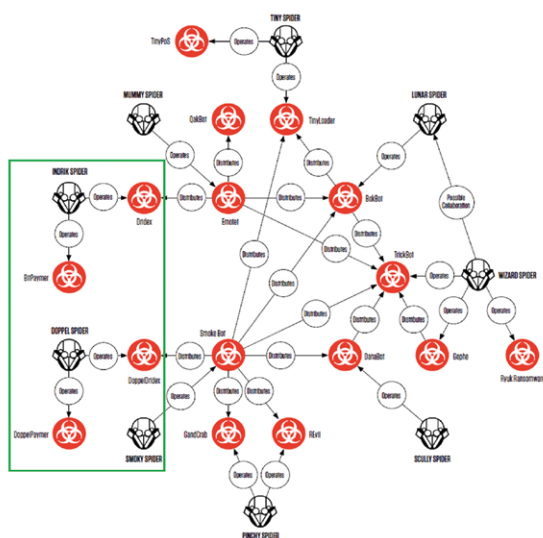


It is difficult to grasp the idea that the fixed is infinitely dynamic, and the infinitely dynamic is fixed. As we have explained, analyses by CTI frequently tend only to view cybercrime as a fixed space, a set of categorisations.

Some analyses have addressed this dynamic aspect by studying the nature of the links that arise between attackers and malware when attackers are building their TTPs. Nevertheless, they have failed to grasp the notions of recursion and dimensional plurality. They do not show the dynamic relationship between the different dynamics (the “dynamic of dynamics”).

By way of example, the 2020 annual report of the US firm CrowdStrike²¹, takes the valuable step of identifying relationship processes. However, the issue of recursion is not addressed, and only attacker-malware and malware-malware relationships are considered.

Mapping
conducted by
the US firm
CrowdStrike.



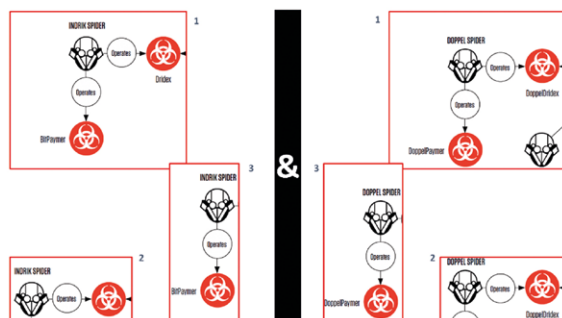
Looking, for example, at the groups ATK180 (Indrik Spider) and ATK206 (Doppel Spider) (see box), a striking similarity emerges between the two groups. This similarity becomes all the more striking if we look at the names of their malware (and the way they operate, which is not shown here, but is almost identical).

However, the links are one-way only, in the attacker-to-malware direction. They focus on the modalities of operations, but not on their origins.

As a result, two sets of relationships emerge, which are completely separate, but which display significant similarities.

In this specific example, a number of sources indicate that ATK206 (Doppel Spider) is a secessionist fringe group of ATK180 (Indrik Spider). It is also known that the similar nature of the arsenals deployed is associated with emulation and reappropriation on the part of ATK206 (Doppel Spider).

Vision
showing two
different
interaction
spaces.



Adding an extra dimension – probable or confirmed relationships between the two attackers – and adding a recursive vision (based on a model whereby “the cause is itself a consequence, which is itself a cause”, etc.), we can see, via a simple example, the first signs of the complexity of cybercrime as a living object.

Looking at potential relationships between these two groups enables us to identify a new aspect of interaction relating

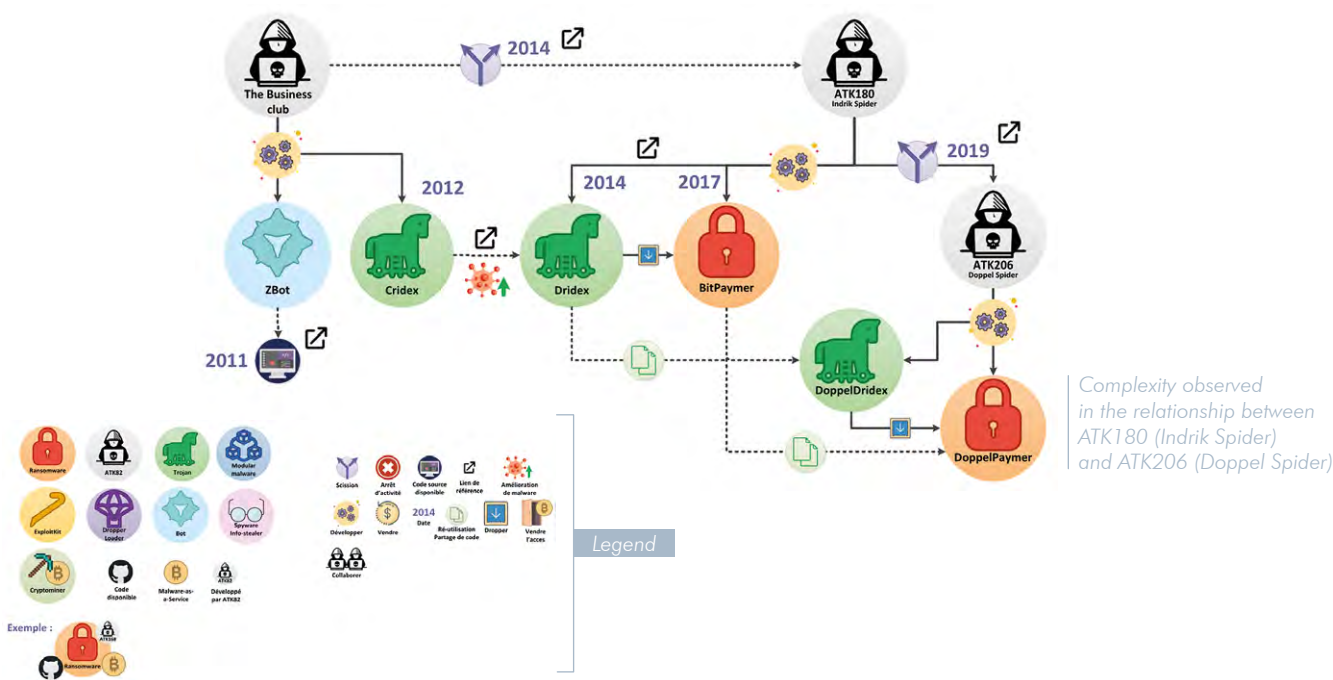
²¹ CrowdStrike Global Threat Report 2020.



to referencing and competition. Malware itself is subject to interaction processes in the form of referencing and re-use. This gives a considerable boost to our understanding. Having started with two times three relationship spaces, we now have 11 (see infographic, “Dynamic analysis of relationship between ATK180 (Indrik Spider) and ATK206 (Doppel Spider)”).

If we include the structural role played by the actors’ different visions of the phenomenon itself, we can add five higher dimensions:

1. CrowdStrike’s vision of the phenomenon.
2. The attackers’ (assumed) vision of the phenomenon.
3. To move away from the idea that actors are not observing each other, the notion that the attackers are obtaining information on CrowdStrike’s vision (on the basis of the company’s report) must also be considered.
4. These preliminary visions (14 in total) themselves make up a fifteenth vision – the vision that we, as security companies, have of the phenomenon (in other words, the observer is being included in the observation).
5. The sixteenth and final preliminary vision is methodological in nature, and involves a critical consideration of our own vision of the phenomenon (the observer observing how they observe).





This gives us a total of 16 preliminary visions, which exist in an intellectual and perceptible sense, and which we must keep in mind in order to understand the incredible complexities behind this apparently simply relationship between these two groups of attackers.

Unfortunately, we haven't yet gone far enough, because all of these visions are themselves constituent parts of the whole set of visions, taken individually. In addition, we have not taken account of the importance of context: what were the reasons behind the split between these two groups?

This is where we start to feel a little dizzy, because we are coming up against our inability to understand everything. Behind this simple split between two groups, an infinite number of interaction spaces and space interactions are dialoguing with each other, and the interactions themselves are intertwined. So we are sensing our limits; yet we have understood the essential.

> **Cybercrime defined as an interlinking of interactions**

We now understand the essential. Our idea of a cybercrime "organisation" is an abstraction defining a disorganised array of interactions of different types. We are bringing together perceived cybercrime and the construct of cybercrime through a dynamic vision.

We also understand our role. By considering this set of interactions as a "cybercrime space", we are reifying this space. We, as observers, have a fully-fledged structural role: to create the construct of cybercrime from the perception of cybercrime.

Let us now come back to our idea of a snapshot and dynamic vision. As explained previously, constructing a snapshot vision is not difficult. We do so instinctively, because it provides reassurance.

This type of vision creates a frozen image of a de facto state, allowing us the time to analyse it, and reinforcing our view that we are capable of doing so. In short, it gives us the feeling that we have fully mastered this vision, this frozen-in-time organisation.

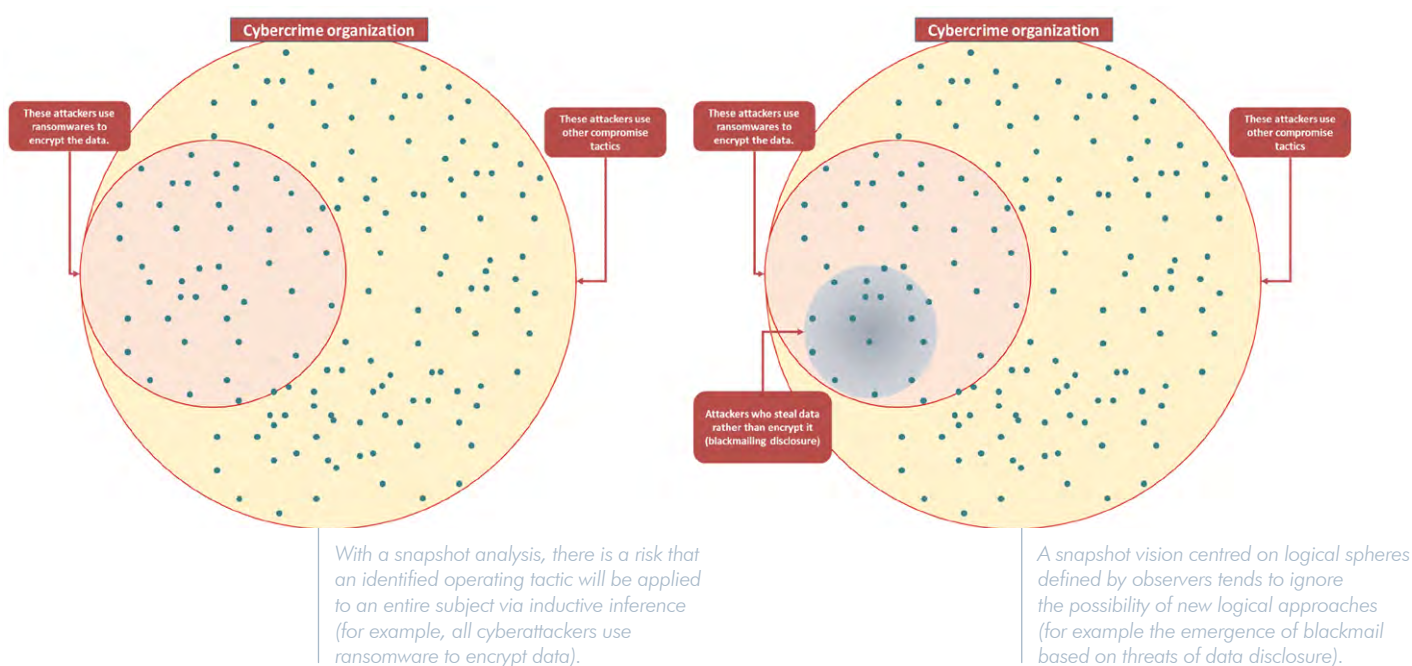
However, any observer or analyst has, at the same time, the permanent, uncomfortable feeling that what they are observing is slipping through their fingers. This feeling of powerlessness, of disconnect, is the very manifestation of the limits of the snapshot vision. The reason for this is that the vision only provides reassurance within a particular time and space.



To paraphrase David Hume²² this principle is the same as believing that the sun will necessarily rise tomorrow. It does indeed seem ludicrous to believe that the sun will not rise tomorrow. The sun rises every morning. Yet this logic is based merely on a snapshot of a past logic.

There is nothing which proves, definitively and logically, that because the sun rose this morning, it will necessarily do so tomorrow: "In the conception of common sense, we simply take it for granted (without posing ourselves any problems) that our belief in the regularities is justified by the repetition of the observations which are the causes of the genesis of this belief²³ ».

The snapshot vision, therefore traps us in a belief. With regard to cybercrime, this belief may be manifested, for example, in the idea that ransomware attacks are intended to encrypt the target's data, since the majority of ransomware attacks in the past were intended to encrypt the target's data.



²² Enquête sur l'entendement humain (An Enquiry Concerning Human Understanding), David Hume, Flammarion, 2006, p.85.

²³ La connaissance objective (Objective Knowledge), Karl Popper, Flammarion, 1998, p.42.



In 2020, the cyberdefence community was surprised by a change in tactic (the emergence of disclosure blackmail, instead of simple data encryption). This morning, the cybercriminals did not encrypt data. This morning, the sun did not rise.

> **Dynamic analysis: understanding an object by navigating through it**

In this situation, we are coming up against the limits of our usual *modus operandi* for understanding cybercrime, and cyber threats in a broader sense. This analytical approach has to be made more agile, so that it does not become meaningless, or even damaging, for our partners. We have to combine it with a dynamic and reflexive vision.

What do we mean by a dynamic vision?

As we have said, cybercrime appears to be a set of observable sub-organisations (groups of attackers, the cyberdefence community, etc.) and abstract sub-organisations (Big Game Hunters, Fire-and-Forget specialists, etc.).

These two types, whether they are real (in the form of perceptible organisations) or invented by us to improve our understanding as part of a snapshot approach, reflect specific modes of recursive action, in other words interaction.

Action is at the heart of our analyses, although we are not necessarily aware of this. We don't hesitate to talk about "groups of attackers" as if they were the active embodiment of their TTPs, for example. Our construct of the cyberdefence community is based on actions implemented for the purpose of interactive defence. Big Game Hunters are defined via their targeted actions, and Fire-and-Forget specialists via their indiscriminate actions.

Yet we are often content simply to describe actions on a one-way basis, from attacker to target, and within a unidimensional framework, in which the attacker operates the ransomware for the purpose of encrypting the target's data.

We include action in our snapshot model most often by ignoring the fact that the determinants of the attackers' actions, and of our own actions, are in dialogue with uncertainties, transformations, base motivations at an internal level, reference frameworks, etc. We frequently also ignore the fact that pure rationality does not act in a deterministic manner on actions, because it does not exist in this form,

To envisage action in a dynamic model, it is necessary to consider that it is itself the product, and the creator, of other actions: a set of interactions.

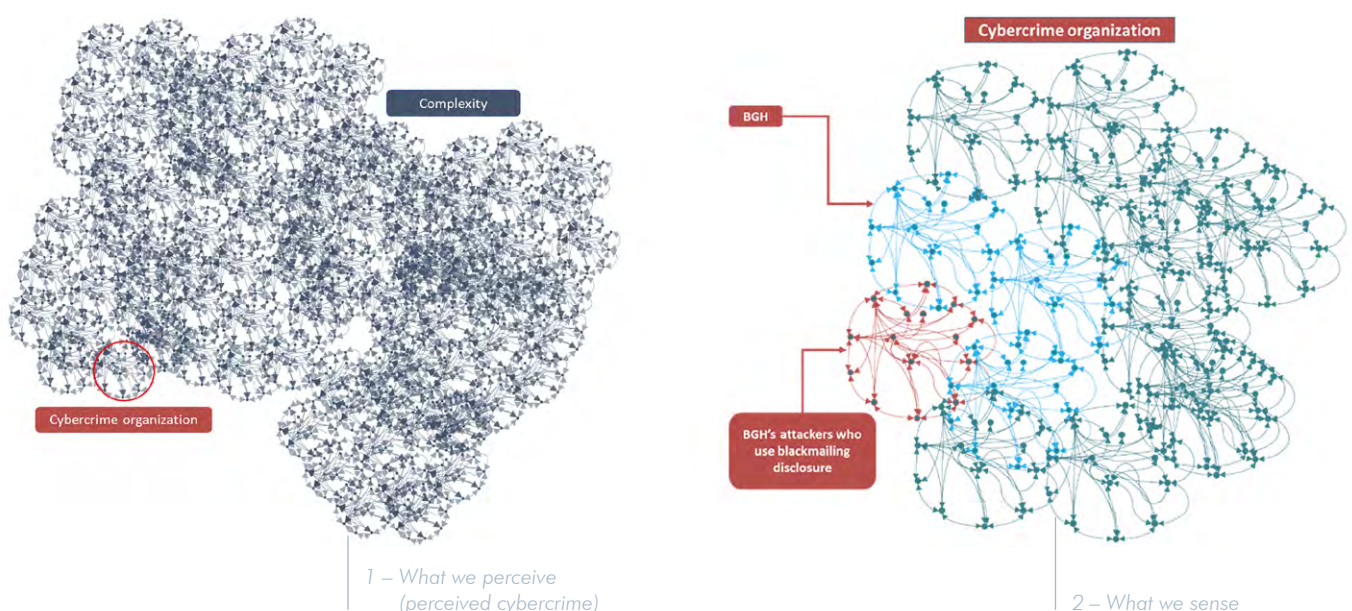
The modalities of action of cybercrime actors are not programmatic. They do not follow a stable logic within a stable environment, and do not originate from purely rational actors. The modalities of action of cybercrime actors are strategic.



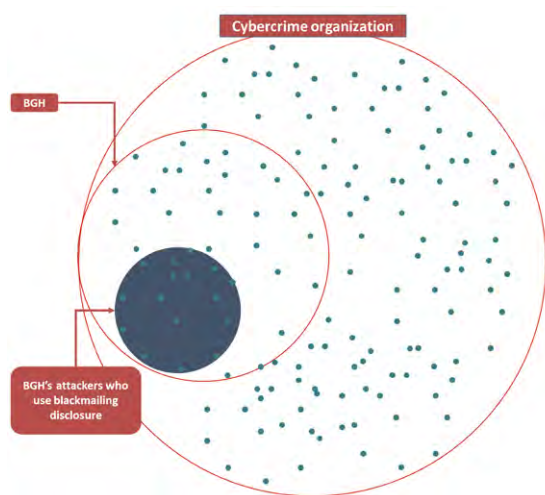
« The advantage of a programme clearly lies in its extremely economical nature: there is no need to reflect, everything happens automatically. A strategy, on the other hand, is determined by taking account of a situation characterised by uncertainty, as well as adverse issues, or even opponents, and has to be modified on the basis of information provided along the way. It may exhibit considerable flexibility. However, in order for a strategy to be implemented by an organisation, the organisation must not be designed to obey a programmatic approach, but must be capable of processing the elements which contribute to the formulation and development of the strategy.²⁴ »

Interaction – meaning a disorganised set of strategic actions of various kinds – is thus itself of a strategic nature. The strategies of the different actors (including ourselves), shaped by this set of interactions, form the basis of what we call “organised cybercrime”.

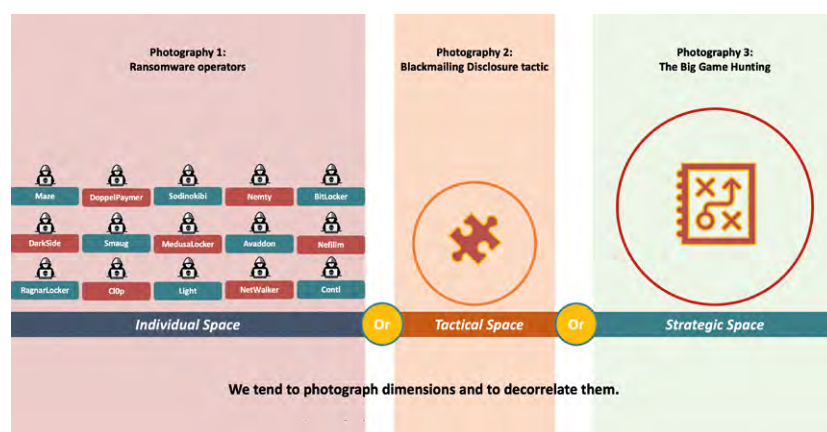
The best way to analyse such a process is not to try and master it via a snapshot, but to accept the need to navigate within it, and find a way through its singularities, in a dynamic manner.



²⁴ Introduction à la pensée complexe (Introduction to complex thought), Edgar Morin, Éditions du Seuil, 2005, p. 120.



3 – How we analyse it (our construct of cybercrime)



4 – How we explain it

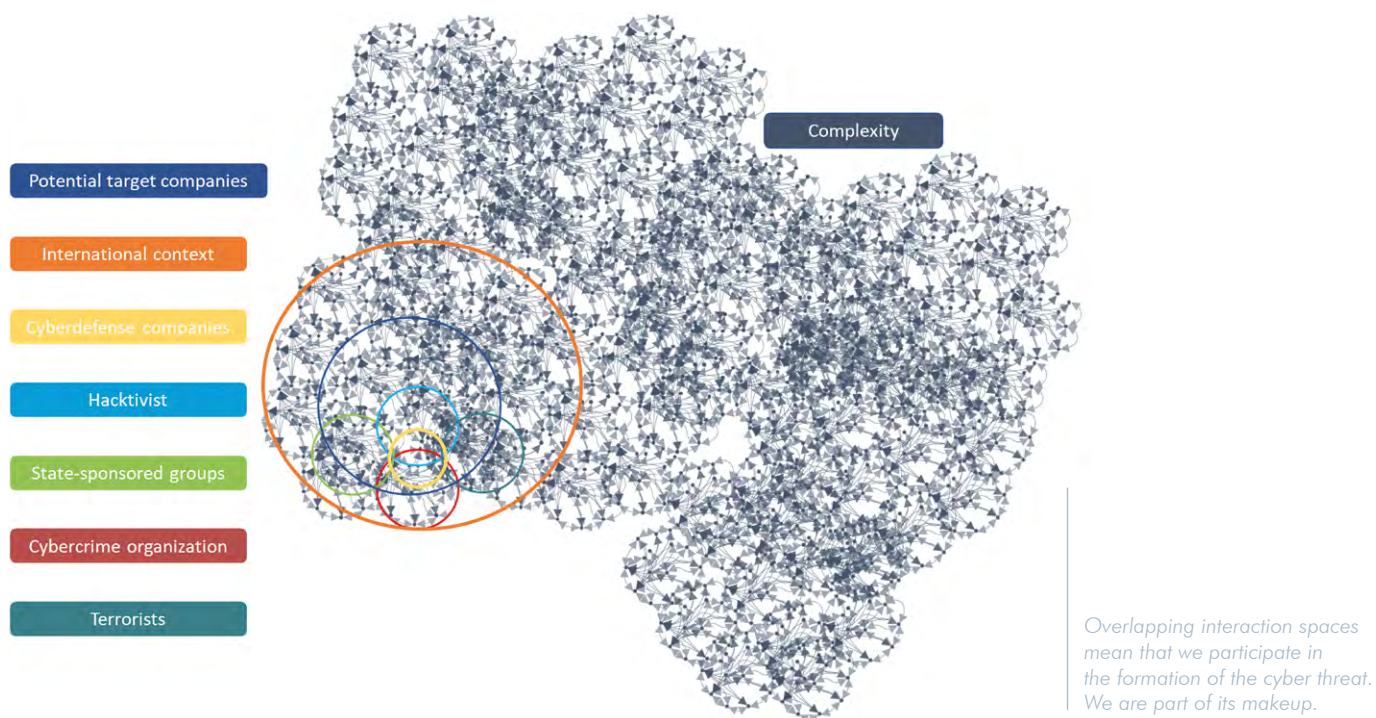
> We are part of the makeup of cybercrime

Now that we have understood that it is the interactions among actors, as a set of strategies, which are the source of cybercrime as a perceptible phenomenon, we cannot exclude ourselves from it.

The paradox can be described as follows: we are co-constituents of cybercrime. We become part of it as soon as we have strategic thoughts about it. We are part of its makeup. The analysis of cybercrime as a subject is necessarily a reflexive self-analysis.

Our cyberdefence policies, our arrangements for investigation and analysis (CTI), and the way we engage via the media, are necessarily part of the logic of interactions which produces the threat.

By interacting with it, while aiming to defend ourselves against it, or obtain information about it, we breathe life into it, and provide the impulse it needs to innovate and develop strategies.



This statement may appear obvious when it is read on the page. However, it has not been extensively integrated into our cyberdefence policies, because the analytical tools that we use are rarely applied to these policies, or to ourselves. We are lacking in reflexive self-analysis.

To use a metaphor based in the everyday: it's as if we are playing a game of chess, and watching the way our opponent is playing, without realising that they are able to do the same to us; we forget that we are part of the game too

What we are doing is ignoring the strategic nature of our opponents' thought processes, and viewing them simply as programmatic.

Cyberattackers are observing us. They are analysing and deconstructing our cyberdefence policies, what we say, and how we understand things, while trying to anticipate our moves, our best practices, and our advice. They are adapting and innovating.

²⁴ *Introduction à la pensée complexe (Introduction to complex thought)*, Edgar Morin, Éditions du Seuil, 2005, p. 120.



Our participation in the formation of the cyber threat boils down to this simple situation, even though we would rarely put it this way ourselves: we are a determinant of cybercrime.

« Having a strategy implies having a goal. There cannot be a strategy where the action has no final goal. Conversely, an action that is not finalised cannot be strategic.²⁵ »

The conception of an action is only strategic if it stands in opposition to an Other, with both will and intelligence. If this is not the case, it is merely technical in nature.²⁶ »

ORGANISED CYBERCRIME: A CRIMINAL SOCIAL ORGANISATION WITH DETERMINANTS OF A TECHNICAL NATURE

> Understanding the interlinked relationships between ‘macro’ and ‘micro’/‘contextual’ and ‘individual’ phenomena

We have set out a simple principle: cybercrime is both an abstraction created by the perspective of the actors involved, and a reality reified by their actions. It is both a cybercriminal social organisation and a disorganised set of interactions, whether desired or not, conscious or not.

It has a complex form, and is necessarily understood by its actors in a strategic way.

« Whatever is well conceived is clearly said, And the words to say it flow with ease.²⁷ »

Even though we know this, and sense it, we are still in the habit of analysing organised cybercrime via a snapshot vision. This means that we habitually apply programmatic rather than strategic thought to cyberattackers.

We analyse their TTPs via a matrix (Mitre Att&ck) which is the very epitome of a programmatic approach, and we describe the way in which attacks unfold, and their determinants, via compromise chains (Kill Chain).

These tools are useful for providing explanations to our partners, but they are in no way sufficient for our understanding. But how did we end up with this conditioned response, this tropism?

²⁵ *Politique Étrangère, Institut français des relations internationales, « La stratégie en théories », Vincent Desportes, 2014/2 Été, p.167.*

²⁶ *Politique Étrangère, Institut français des relations internationales, « La stratégie en théories », Vincent Desportes, 2014/2 Été, p.168.*

²⁷ *L'art poétique, (Chant 1), Nicolas Boileau, parution 1674.*



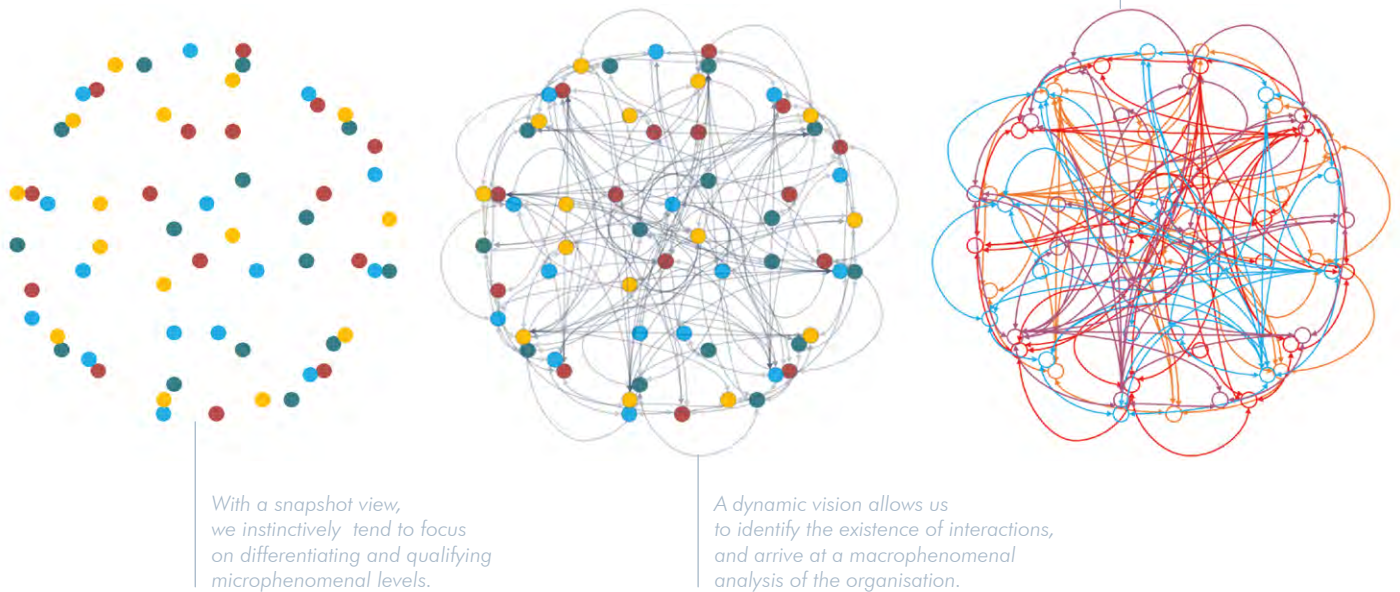
We have a natural tendency, when trying to comprehend the cyber threat, and organised cybercrime in particular, systematically to use analyses we have conducted at a microphenomenal level as a starting point. This often leads to a tendency (explained above) towards inductive inference²⁸. We generalise on the basis of specific cases, or microphenomena, such as the modes of action used by attackers, from organising principles to a higher-level structure, such as “organised cybercrime” itself.

We also have a tendency to ignore contextual factors, which prevents us from addressing the strategies employed by cybercrime actors. Yet, as Vincent Desportes and Edgar Morin explain, understanding the actions of actors, in their strategic form, necessarily involves taking account of otherness as a context capable of generating uncertainty.

Action in the microphenomenal space (the attackers’ space) is strategic because it is partly determined by a macrophenomenal space, an organisation of disorganised interactions. We cannot claim clearly to understand cybercrime if we separate the context from the actor, and the actor from the context.

This need is becoming increasingly acute, particularly in light of the emergence of new practices such as disclosure blackmail. We have to understand the dialogue between the context and the individual action, and cross-check the micro-analysis of the actors against the macro-analysis of the contexts.

We have to qualify and differentiate the interactions in order to arrive at a synthesis of the micro and macro levels, and understand the complexity of the whole.



²⁸ *La connaissance objective*, Karl Popper, Flammarion, 1998, p.42.



> Cyberdefence as a discipline first, a provider of operational tools second

At the start of this report, we talked about our natural, and necessary, tendency to create abstractions. This is the intellectual exercise which allows us to create levers for intuiting and understanding the distinctive properties of the observed object, which we often call concepts.

Cyberdefence and cyber threat intelligence provide operational tools for organisations. However, they are first and foremost disciplines, spaces in which specialists undertake research to further the development of a specific area of expertise. The search for knowledge in cyberdefence and CTI is not an end in itself. It is not a pedantic, pseudo-philosophical pursuit. The research and reflection work undertaken within these disciplines is necessary to keep organisations safe and secure.

Yet we tend to inhibit our reflections, focusing only on simple analyses. The abstractions and concepts that we employ provide an interesting example. We tend to create them solely via the categorisation of objects.

We categorise cybercriminals, State-sponsored groups, etc. via essentialisation, and sub-categorise cryptominers, ransomware operators, and espionage/sabotage groups in the same way. We categorise Big Game Hunting, Fire-and-Forget, etc. on the basis of behaviours.

In addition, our abstractions are often focused on, and for the purpose of, an empirical approach, starting with the observed object and moving towards the abstraction of its essence, formulated as a concept (for example Big Game Hunting), but rarely on the reflections that we have in respect of these objects.

This is another dimension that we aim to provide with the dynamic vision: navigating among the elements of the cybercrime object on the basis of interactions, but also navigating between and within our own concepts, in order to assess their pertinence.

We construct concepts of reason by categorising the objects of our analysis, but we still lack concepts of understanding, as units of reflection, in respect of these observed phenomena.

The implication of this trend can be directly observed in the example of disclosure blackmail, which emerged in late 2019.

We were capable of detecting this change, and distinguishing it from the conventional tactic involving encryption only, and we were therefore able to create a new abstraction, and a new category of tactic. We created a concept of reason: disclosure blackmail.



So what about the attempt to create a concept of understanding in respect of this change in tactic?

We have not thought extensively about the origins of this change, which radically altered our understanding of the specialist cyber threat. As we will show, this new tactic originated from a number of elements (including inspiration drawn from other cyber threat areas; emulation and innovation within the cybercrime sphere; the bypassing of our cyberdefence policy strategies; and a successful arm wrestle with targets via a focus on new fears).

« Whatever we may have to decide as to the possibility of the concepts derived from pure reason, it is at least true that they are not to be obtained by mere reflection, but only by inference. Concepts of understanding are also thought a priori antecedently to experience and for the sake of experience, but they contain nothing more than the unity of reflection upon appearances, in so far as these appearances must necessarily belong to a possible empirical consciousness. Through them alone is knowledge and the determination of an object possible. They first provide the material required for making inferences, and they are not preceded by any a priori concepts of objects from which they could be inferred. On the other hand, their objective reality is founded solely on the fact that, since they constitute the intellectual form of all experience, it must always be possible to show their application in experience. ²⁹ »

« Concepts of reason enable us to conceive, concepts of understanding to understand (perceptions). ³⁰ »

The dynamic vision which we recommend unfortunately cannot do without these concepts, particularly if it is aimed at finding the keys to understanding the dialogue between micro- and macro-analysis, between organisation and interaction, and between the operational use of our intelligence and reflections on its own foundations.

Because we do not have this corpus of concepts at our disposal, except for those relating to interaction and organisation, we have to turn to other disciplines which have already carried out this preliminary reflexive work.

²⁹ *Critique de la raison pure (Critique of pure reason)*, Emmanuel Kant, Flammarion, 2006, p.340.

³⁰ *Ibid.*, p.340-341.



Organised cybercrime

Comme nous l'expliquions, notre dotation en concepts de l'entendement demeure trop résiduelle pour prétendre comprendre un phénomène comme celui de la cybercriminalité organisée.

Nous avons besoin de sortir de notre discipline, de chercher ailleurs, de trouver des clés de lecture pertinentes, sans pour autant tomber dans la recherche d'une application pure et parfaite de concepts qui sont nés par l'analyse d'autres phénomènes.

Sans tombé dans l'application systématique pour coller à une théorie particulière, il semble que le concept de 'champ', développé par le sociologue Pierre Bourdieu, puisse apporter quelques éclaircissements essentiels à ce que nous prétendons comprendre sur l'organisation de la cybercriminalité perçue.

Mais qu'est-ce qu'un champ ?

« The locus of a specific legality, manifested by a constitutive "as" (the economy as the economy, the law as the law, art as art, etc.)³¹ ».

The internal logic of a field is thus produced by the actors themselves, via the mobilisation of their capital and via the internal competition in which they engage, for the purpose of acquiring a greater "quantity" of capital, enabling them to achieve dominance. An agent, in our case a cybercriminal, who does not play the game is immediately and unconsciously ejected from the field, because of their detrimental effect. Within the field, agents battle constantly to gain more capital and ensure even greater dominance, but also, quite simply, to remain in the field. The ultimate objective is, of course, to achieve a level of capital such that, over and above achieving a position of domination, it becomes possible to change the nature and the rules of the field.

For our purposes, the field is organised cybercrime, produced by cybercriminals themselves mobilising their financial, technical and reputational capital within a competitive framework for the purpose of continuously obtaining larger amounts of these different types of capital.

The aim of this continuous internal battle is to remain within the cybercrime field, in other words to be considered as a fully-fledged actor. The ultimate objective is 'dominance'. It is difficult to see where this idea of dominance fits in for our purposes, but we will see that it exists in a specific form. Finally, we understand that there are certain 'rules' in the form of codes adopted by cybercriminals which play a structural role, both for the actors themselves and for the field of organised cybercrime itself.

³¹ Bourdieu, Pierre, "Champ du pouvoir et division du travail de domination" ("The field of power and the division of the labour of dominance"), *Actes de la recherche en sciences sociales (journal)*, No. 190 (December 1, 2011): 126-139.



So how does this benefit us?

As we explained in the first part of the report, we have a particular tendency to carry out micro-analyses in snapshot form. We produce reports on attackers like Maze, Nefilim, Sodinokibi, Ryuk, etc., but we rarely attempt to understand the determining factors, apart from the financial goals, which define their courses of action.

We often focus on describing the courses of action, and the reasons for them, but we rarely look at the influences that lie behind these courses of action and these reasons.

The concept of the field, and the entire corpus associated with it, enables us to define the determinants of the actions, and the associated influences. We are able to identify levers of understanding which allow us to draw up useful action models for cyberdefence.

How does the concept help us understand organised cybercrime?

In terms of the analysis, remember that “groups of attackers” are not fictional entities which are disembodied and/or which do not have the capacity to think for themselves. Such groups are made up of real people who act, react and interact according to cognitive principles similar to those that apply to everybody. This means that their identity, created by the culture and codes of the field in which they operate, influences and is influenced by the field itself.

Knowing the codes of the common culture of the ecosystem and the individual behavioural tendencies of the groups thus allows a better understanding of the threat, and allows us more effectively to envisage protection solutions.

The field – meaning this space, made up of its actors, which performs a structural role in respect of their behaviour – comes into being once certain conditions are met. It appears that these conditions are manifested in a troubling manner in organised cybercrime.

➤ Differentiation via competition and referencing

The social world is thus differentiated into a multitude of fields, each functioning in its own way. These spaces, in their logic, are referred to as “game” spaces, because agents operating within them (members of the field in question) attempt to assert their power (their capacity to mobilise their forces and resources in order to impose their will) in a state of *illusio*³², in other words in the belief that what is at stake in this social relationship makes it worth engaging in the game, i.e. in the social relationship itself.

THE DETERMINING FACTORS OF STRATEGIC CYBERCRIME INTERACTION

³² Bourdieu, Pierre: *Raisons pratiques (Practical reasons)*, Paris: Seuil, 1994, p.151



« The division into relatively autonomous fields is the culmination of a process of differentiation [...] it can be described as a process of instituting different game spaces in which specific forms of capital are generated and realised, as both assets and characteristic stakes of each form of game³³».

The process of differentiation in the cybercrime field is manifested via two interlinked processes: competition and reference.

THE COMPETITIVE INSTINCT

Cybercrime actors are continuously seeking financial, technical and reputation capital from a strategic perspective, i.e. for the purpose of achieving a single objective: financial gain. The proliferation of such actors naturally creates a phenomenon of competition.

Major cybercriminals, for example those involved in Big Game Hunting, have developed a particular type of joint approach, involving sophisticated, specifically targeted ransomware attacks, similar to those seen from State-sponsored groups, and focused on major organisations.

Players like these are competing against each other, as well as against other cybercriminals employing different TTPs, such as Fire-and-Forget (an approach more or less diametrically opposed to Big Game Hunting).

This competition drives continuous innovation in terms of methods and strategies. However, the quest to garner increased financial, technical and reputational capital continues unabated.

THE REFERENCE INSTINCT

Competition is accompanied by a reference process. Some groups, with large amounts of capital, have an advanced capacity for innovation, and exhibit a form of dominance, notably because they are capable of changing the common rules. These actors serve as references.

The Maze group, for example, brought about a step change in the rules in late 2019 when it started using disclosure blackmail, unleashing a slew of imitations among competitors. The latter began systematically incorporating the tactic into their TTPs, while referencing Maze, which only served to accentuate the phenomenon of differentiation.

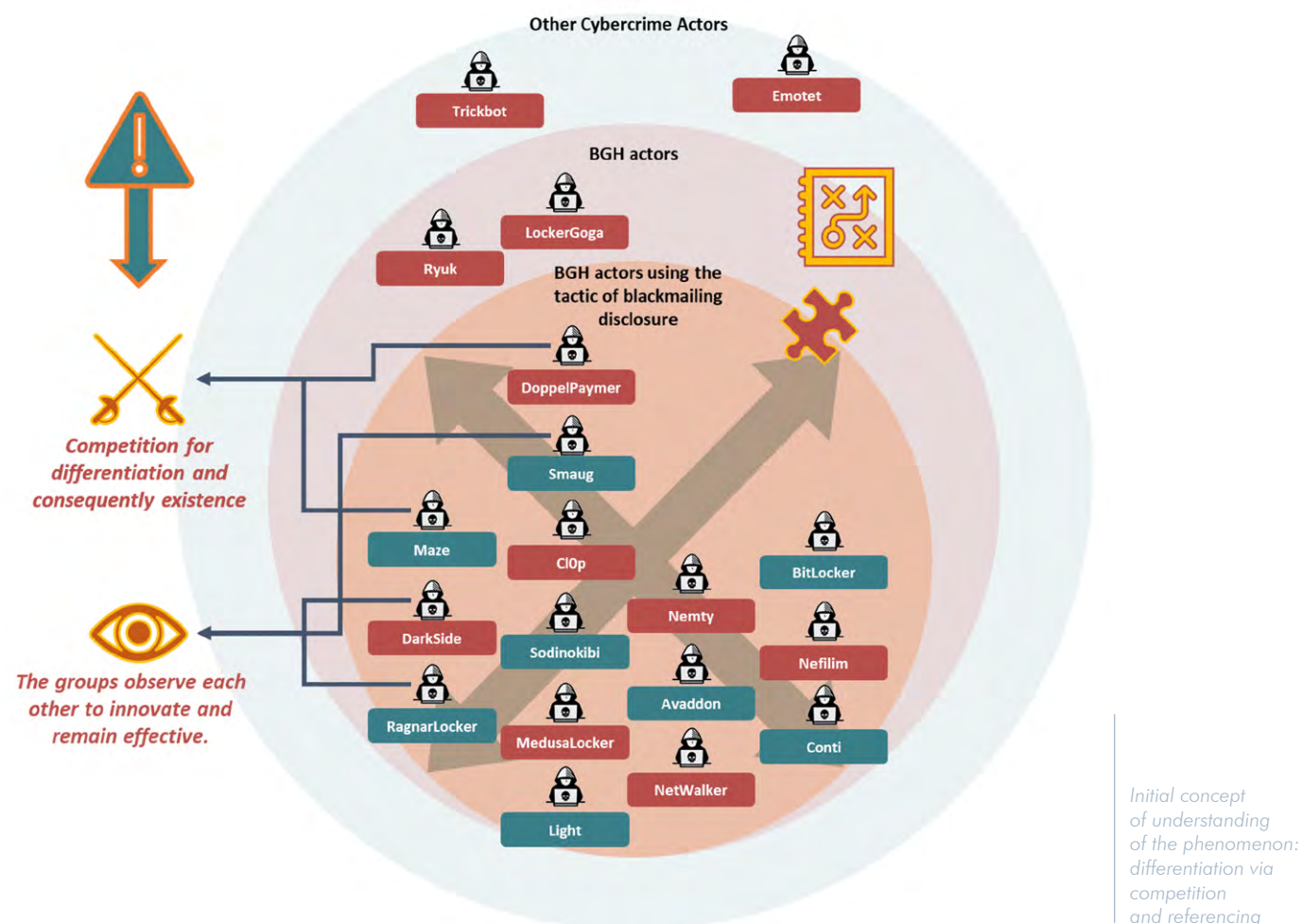
³³ Bourdieu, Pierre, "Champ du pouvoir et division du travail de domination" ("The field of power and the division of the labour of dominance"), *Actes de la recherche en sciences sociales (journal)*, No. 190 (December 1, 2011): 126-139.



A COMBINATION OF INSTINCTS DRIVING THE DIFFERENTIATION PROCESS

This process of differentiation, which we know to be involuntary, is thus driven by competition among peers, and with other models, and reinforced by a process of referencing the 'dominant' groups in the field.

This differentiation brings with it another decisive phenomenon: specialisation. The process of specialisation is becoming increasingly widespread in organised cybercrime.





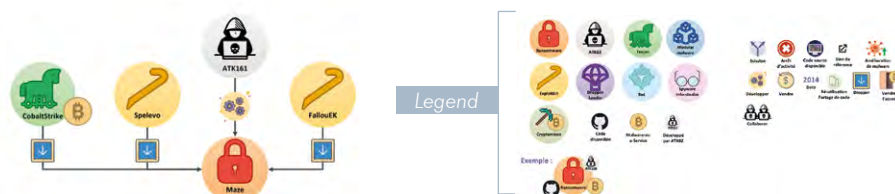
> Specialisation based on strategic and technical distinction: the source of the division of labour in cybercrime “society”





















The specialisation observed in the cybercrime arena is interesting because, in the same way as differentiation based on competition and referencing, it is driven by technical and strategic aspects.

THE INSTINCT FOR STRATEGIC DISTINCTION

Specialisation must not be seen as a step that follows differentiation, but as a process that is incorporated into it.

Strategically, groups specialise in particular approaches. (This explains why we have a tendency to classify them.) Examples include Big Game Hunting, and Fire and Forget. These classifications designate specialised strategic approaches. Maze is typical of the groups that have chosen to distinguish themselves strategically via an innovative technique.



	0 Preparation	1 Intrusion	2 Reconnaissance and lateral movement						3 Exploitation	
STRATEGIC	 Maze scans the internet looking for insecure corporate access	 The Maze group uses vulnerabilities or default username/password combos to get to the system	  The group takes a look at the systems  It's propagating to the domain controller  It collects information on the network (collection of files for ransom demands as well).						 The group often manually deploys its ransomware on the targeted systems	
OPERATIONAL	 Pre-Attack	 Initial Access ↓ T1078	 Credential Access ↓ T1110	 Execution ↓ T1486 T1490 T1203	 Defense Evasion ↓ T1027 T1497 T1202	 C&C ↓ T1043 T1071	 Discovery ↓ T1497 T1057	 Lateral Movement ↓ T1076 T1077	 Collection ↓ Thales 006	 Impact ↓ T1486 T1490 Thales 007
TECHNICAL		 The Maze group uses vulnerabilities or default username/password combos to get to the system	 Cobalt Strike Cobalt Strike is a commercial, full-featured, penetration testing tool which bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system. In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz. Mimikatz Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks. Metasploit Its purpose is to provide information on computer system vulnerabilities, to assist in the penetration and development of signatures for intrusion detection systems (IDS, Intrusion Detection System). Human Operator						 Maze Maze is a ransomware that appeared in 2019. It is spread through spearphishing, as well as exploit kits such as the FalloutEK, and Splovo. This ransomware is associated with a single threat actor, and it doesn't seem like it is shared nor part of a malware as a service operation. <u>This ransomware was one of the first to threaten to publish stolen information on its website, mazenews1.itop</u> Once the ransomware finished encrypting all files, it drops a file named "DECRYPT-FILES.txt" in every	

Schematic description of Maze technique culminating in the tactical innovation of disclosure blackmail



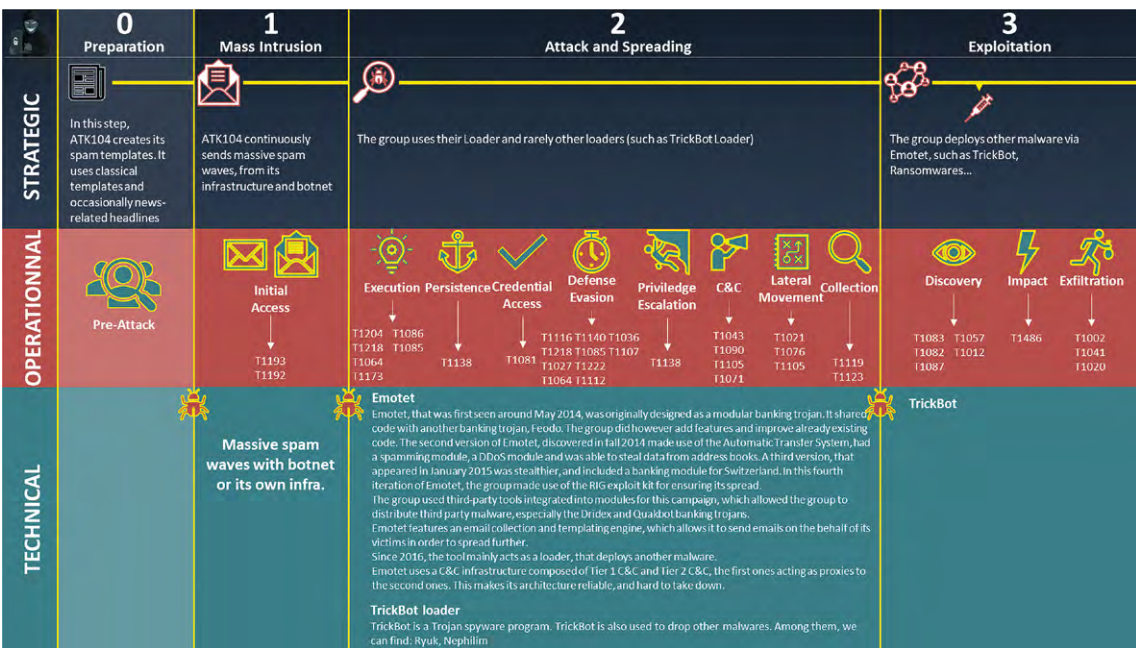
This strategic specialisation is also driven by technical specialisation, whereby groups comprising a few dozen individuals focus on maintaining and enhancing a single malware or tool, with a view to combining it with other equally specialised tools developed by other groups.

THE INSTINCT FOR TECHNICAL DISTINCTION

There is thus a concentration of efforts to create ransomware, infostealer, downloader, botnet or RAT programmes specific to certain groups. The Emotet³⁴ loader, for example, has so far been the sole known area of focus for the group which created it. The group sells the loader's services to the majority of major cybercriminals currently in active operation.

By selling the loader on a bespoke basis to Big Game Hunting actors, for example, the group accentuates the latter's strategic specialisation.

At the same time, its own technical specialisation, centred on Emotet, also forms the basis for its strategic specialisation within a conventional market model known in the cyberdefence community as Malware-as-a-Service (MaaS).

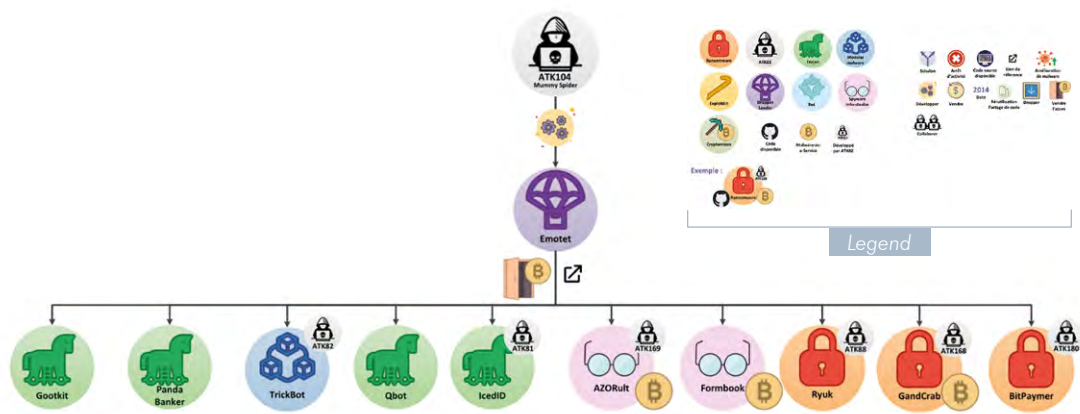


Schematic description of attack technique of group ATK104 (Mummy Spider) based on the Emotet malware

³⁴ <https://attack.mitre.org/software/S0367/>



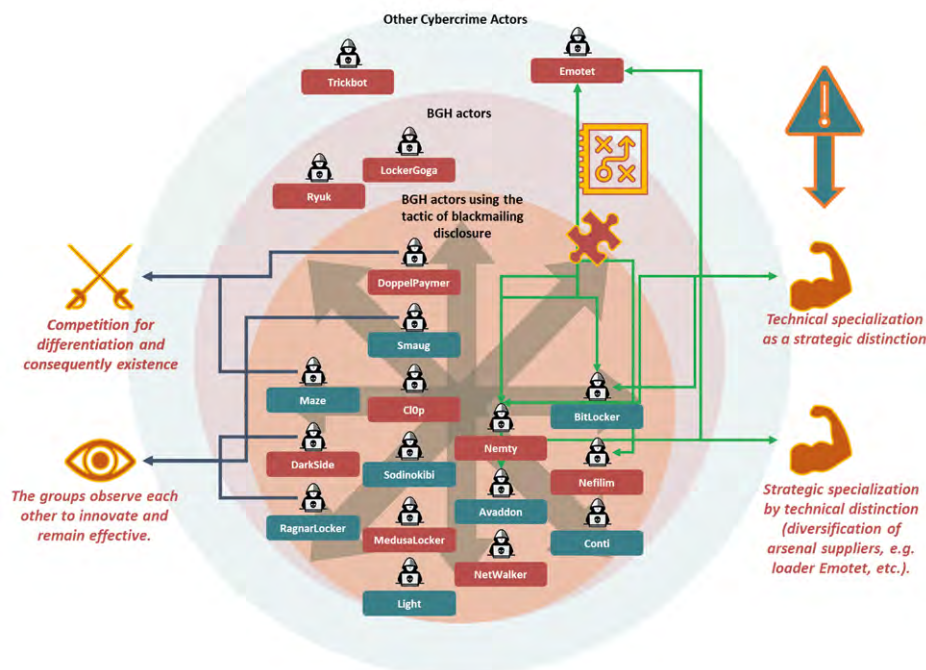
The technical specialisation of Emotet is the source of its differentiation (strategic distinction)



A COMBINATION OF INSTINCTS DRIVING THE SPECIALISATION PROCESS

These two types of specialisation, as we have already understood, drive each other forward. At the same time, they produce, and are produced by, the impulse for differentiation among groups of attackers.

They are in competition, and yet they emulate each other; they are autonomous, and yet they depend on each other for their specialisation and performance.



Second concept of understanding: strategic and technical specialisation

Here, we identify a first principle for understanding organised cybercrime which corroborates what we explained in the first part of the report: the tendency to interaction is natural; it is incorporated into normal practice (as a norm), and forms the basis of the organisation process.

This entity is a space in which these tendencies are expressed, and which itself has a living form. This space is not biological, but social. We are rapidly discerning the existence of a cybercrime social space. This space is driven by the same principles of differentiation and specialisation which themselves provide the driving impulse for the cybercrime social space. This particular form of complexity can be referred to as the social division of cybercrime labour.





INTERACTION AND THE CYBERCRIME ORGANISATION

> Independence within interdependence (organic solidarity)

Now that we have defined cybercrime's nature as an 'organisation' (a blend of differentiation and specialisation processes, which are themselves produced by the blending of competitive and referencing tendencies and strategic and technical distinctions), we shall come back to the question of interaction.

As we have understood, these tendencies on the part of attackers, which form the basis of the operation of organised cybercrime, necessarily produce recursive interactions, patterns of logic driven by competition and inspiration (or even emulation), as well as innovation, for the purpose of achieving strategic and technical distinction.

It is not the vast number of groups of attackers which gives substance to organised cybercrime, but the tendency of these groups to interact. Interactions create permanent motion within organised cybercrime, drawing it together, and breathing life into it.

Yet this set of interactions, which gives an organised form to cybercrime, and which allows groups of attackers to increase their financial and technical capital, does not ensure the dominance of a particular group.

THE ROLE OF ORGANISATION CREATOR AND CYBER THREAT OBSERVER

It is at precisely this point that we come in, as observers, critics and analysts. We provide the final building block for the field of organised cybercrime. As we stated in the first part of the report, we must reflect on our own role.

Our action, which paradoxically runs counter to our aims, involves providing reputational capital to certain groups of attackers. Cybercriminals observe us, and are able to evaluate themselves thanks to what we do. What we are drawing attention to here is the way in which security companies and the media handle information on certain groups. Too often, we step across the fine line between an affirmative statement and a performative statement. It is this second approach to presenting information which provides certain attackers with reputational capital.

To adopt the metaphor coined by Barbara Cassin³⁵ to explain the difference between these two types of statement, an affirmative statement would be to say "he is running", while a performative statement would be to say "I apologise". When I see a person running, and I say "he is running", I am simply affirming the existence of a phenomenon. On the other hand, when I say "I apologise", I am not observing, I am performing. It is because I make this statement, because I say it, that it becomes true and real. If I do not apologise, via my verbal or body language, the phenomenon of the apology does not exist.

³⁵ Quand dire c'est vraiment faire, Homère, Gorgias et le peuple arc-en-ciel, Fayard, 2018, p.25-26.



Security companies, when dealing with an attack by a particular group, make affirmative statements. They explain and analyse the attack, the emergence of new TTPS, etc. They affirm the existence of a phenomenon. Yet politicians, the media and other information sources increasingly tend to take an interest in such issues when they cause a sensation.

They create a performative discourse, particularly by applying superlatives to the analyses produced by security firms, so that groups with admittedly powerful technical capabilities, for example, are described as “the biggest threat”, “the most dangerous”, etc.

These modes of discourse are performative in that they tend to create a certain reality in the form of reputational capital for the groups of attackers involved, which reinforces the referencing tendency.

It should also be noted that security agencies and companies, by using their concepts of categorisation in the analyses that they publish (the example of Big Game Hunting is applicable again here), participate in this reification via performative discourse.

The attackers do not say, and do not say to themselves, that they are involved in Big Game Hunting. We do so, by highlighting certain groups, which contributes to their reputation.

The tendencies towards differentiation and specialisation thus result in the accrual of financial and technical capital, while the performative discourse in which we engage with respect to organised cybercrime has the effect of increasing reputational capital.

This capital is not entirely produced by us; some major groups are already recognised for their qualities by their peers. Nevertheless, through our involvement as observers, we boost reputational capital, and reinforce the dominance of certain groups of attackers.

Actors who achieve this level of financial, technical and reputational capital are the dominant class within the field, according to Bourdieu’s concept.

« The dominant class, despite its divisions and antagonisms, tends to constitute corps – groups of agents who are socially united by the imposition of an identical name, such as clubs [...] which means symbolically redoubling and reinforcing objective ties linked to their solidarity of interests and affinity of habits, i.e. their vicinity in social space ³⁶ ».

³⁶ Bourdieu, Pierre, “*Champ du pouvoir et division du travail de domination*” (“*The field of power and the division of the labour of dominance*”), *Actes de la recherche en sciences sociales (journal)*, No. 190 (December 1, 2011): 126-139.



In our case, groups of attackers do not impose an identical name upon themselves; we do it via performative discourse.

It is here that we encounter the limits of applicability of the concept of the field to organised cybercrime. It is not possible for us to determine whether this “dominant class” of attackers itself tends to constitute clubs which together exercise dominance over other groups of attackers.

INTERACTIONS THAT UNDERLIE THE ORGANISATION DRIVEN BY THE INTERDEPENDENCE OF ACTORS

Nevertheless, through the identification of their common traits, cyberattackers form interaction links that can be referred to as “solidarity”³⁷, to use the terminology of Émile Durkheim. The latter’s idea is that there is a distinction between mechanical solidarity – based on a greater or lesser degree of coercion to guarantee the creation of links (for example between States and the groups that they sponsor) – and organic solidarity, in which links are created via the interdependence of agents, in the same way that the organs in the human body are interdependents³⁸.

For Bourdieu, organic solidarity within the concept of the field:

« [Is that which]...unites the fractions of the dominant class insofar as it contributes to dominance, and which is ratified and reinforced by exchanges that allow for the establishment of two-way relationships of obligation and dependence [...] [and] does not preclude the permanent struggle for the imposition of the dominant principle of dominance, and at the same time, for the conversation or transformation of the structure of power within the field of power. ³⁹ »

Within organised cybercrime, it appears to be the incorporation by attackers of the logic of competition/referencing/strategic distinction/technical distinction, together with our discourse, that creates the push towards such interdependence.

It is important to understand, however, that, in this logical framework, “dominance” is not sought for the purpose of maintaining a form of inequality. Within the scope of an interaction (or in other words within the scope of such interdependence), the “dominant” parties are dependent on the “dominated” parties, and vice versa.

There is no overwhelming, unidirectional pressure, and there appears to be no desire to create such a pressure within cybercrime, for the reasons mentioned above.

On the other hand, “dominance” is sought after within organised cybercrime because it allows financial, technical and reputational capital to be preserved and strengthened. It is this capital which itself ensures the success of attackers’ target compromise strategies.

³⁷ Émile Durkheim, “De la division du travail social” (“The division of labour in society”), in particular Book I: *La Fonction de la division du travail* (The function of the division of labour), Chapter III: *La solidarité due à la division du travail ou organique* (Organic solidarity due to the division of labour), 1893, p. 106-124: http://classiques.uqac.ca/classiques/Durkheim_emile/division_du_travail/division_travail_1.pdf

³⁸ Ibid. The issue of solidarity in Durkheim is studied in Chapter IV, “Les nouvelles règles du champ : l’indépendance dans l’interdépendance” (“The new rules of the field: independence within interdependence”)

³⁹ Ibid.



Organised cybercrime is thus driven by differentiation and specialisation, by MaaS and the growth in exchanges which, taken together, constitute a division of labour within the “society” that is cybercrime.

A new, fundamental paradox now appears: the groups of attackers are interdependent with respect to each other, and with respect to us; it is this that allows them, and allows us, to be independent in the pursuit of our respective strategies. It is this independence within interdependence which creates organic solidarity, and which makes organised cybercrime⁴⁰.

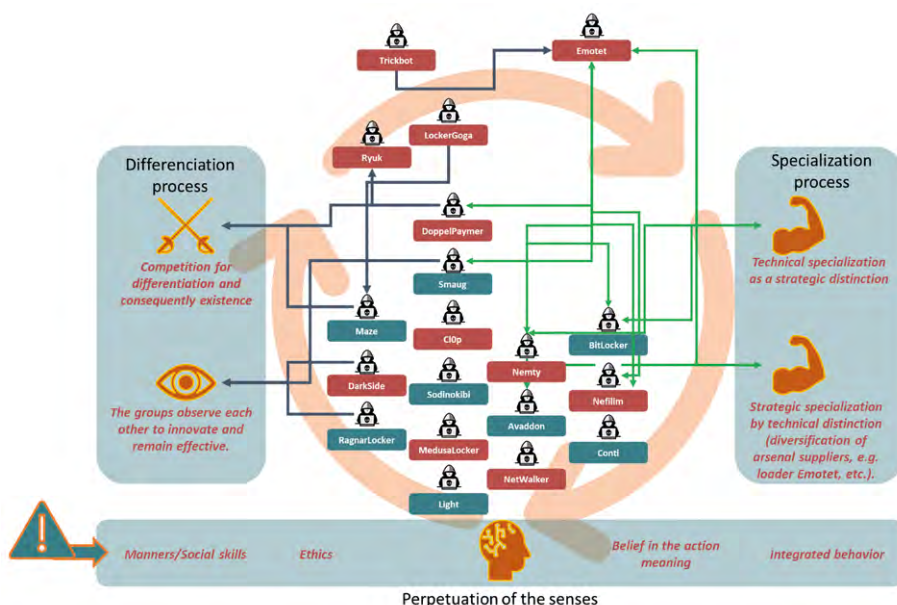
> Cybercrime culture: shaping action

Finally, we see that interaction between attackers, which contributes to the construction of organised cybercrime, must be understood via another concept: the idea of a sustainable sense of purpose.

Groups of cybercriminals, by continuously interacting among themselves, obviously tend, whether rationally or not, to construct an internal organisation, a form of cybercrime culture.

A CYBERCRIME CULTURE IN THE FORM OF A SUSTAINABLE SENSE OF PURPOSE

How can we determine the existence of a “cybercrime culture” when our subject – cybercriminals as social individuals – is difficult to observe?



The structural role of “culture” in creating a sustainable sense of purpose for cybercriminal action.

⁴⁰ Ibid.



In the absence of direct observation of the subject, we can use as our starting point certain practices and behaviours which, as we will see, are not purely rational in terms of completing a strategy.

First, let us recall what we said in the first part of the report, about how actors – cybercriminals, targets and observers – view themselves and their involvement in the organisation, and what we demonstrated via the dynamic reading of the relationship between ATK180 (Indrik Spider) and ATK206 (Doppel Spider).

The actors necessarily form their own representation of the reality that surrounds them, and this integrated representation has a significant influence on their behaviour.

We can consider, on the one hand, that organised cybercrime is constructed by the interactions between actors. But we must, above all, consider on the other hand that the whole of organised cybercrime is present in each actor, in the sense of a particular reading of the ecology that surrounds them.

This reading is constructed on the basis of two important schemes, which are also co-constituents.

The first, which can be considered similar to a form of habitus according to Pierre Bourdieu's terminology, is a continuum of principles in the mind of each cybercriminal, which must be respected.

« A system of sustainable and transposable provisions, structured structures intended to function as structural structures, i.e. as a generating and organising principle of principles and representations.⁴¹ »

It is a kind of code of cybercriminal behaviour, a set of structured principles, representations and integrated norms.

This code of behaviour itself provides a structure for organised cybercrime, in that it sets out a framework understood by all. Cybercriminals cannot deviate from it without risking being subject to a form of 'social' pressure to mend their ways.

During ransomware attacks, for example, cybercriminals are required by the code to conduct themselves, and express themselves, in a professional manner.

⁴¹ Pierre Bourdieu, *Le sens pratique* (The logic of practice), Minuit, 1980, p. 88



They have to present themselves as serious players, with no hidden agenda, and no intentions apart from those stated at the time of compromise (in other words, requesting money in exchange for encrypted and/or stolen data).

This concern with how attackers present themselves to targets reflects a kind of “cybercriminal ethics”, although such ethics are not necessarily applied in a rational manner during the attacks themselves. Targets pay primarily because of the pressure exerted on them, not because their attackers have created a sense of their reliability by acting as serious professionals.

Nevertheless, many cybercriminals have adopted the principle of demonstrating to targets and observers that they are serious players, not amateurs, and that they operate according to state-of-the-art principles.

This code of behaviour for organised cybercrime thus provides a structured set of principles which act as the underlying structure for cybercriminals’ behaviour.

It should be noted, however, that these principles are not fixed, but can evolve over time. To take the example of disclosure blackmail: the professionalism still remains, but it is now accompanied by a much greater degree of pressure.

The conventional ethical arrangement in the past was: you pay, I decrypt; you don’t pay, I don’t decrypt.

The consequences were easily foreseeable for both parties. No advantage was taken of the element of uncertainty, even though, from the point of view of the target, taking the attacker at their word constituted a gamble.

The ethical approach then evolved slightly, with simple uncertainty – concentrated on the attacker’s honesty and professionalism – being replaced by complex uncertainty.

Uncertainty regarding the attacker’s honesty is now supplemented by the uncertainty of the unforeseeable (in terms of the nature of the data which may be disclosed, and the consequences of that disclosure in legal, business, competitive, financial, reputational and insurance terms, for example). The ethics remain, but the duel behind closed doors has become a duel in an arena.

These principles, adopted by cybercriminals and providing the underlying structure for their actions and the way they carry out those actions, are thus similar to a form of habitus, a set of structured organising principles.



A SUSTAINABLE SENSE OF PURPOSE: THE ORGANISING IMPULSE WITHIN CYBERCRIME

If we return to the example of the desire to appear professional in relationships with targets, we can see another element which, in this case, can be considered similar to what Pierre Bourdieu called *illusio*⁴². We used this term at the start of the section on “The determining factors of strategic cybercrime interaction”, with a simple definition which needs to be filled out. We defined *illusio* as the belief that what is at stake in this social relationship – financial gain – makes it worth engaging in the game, in other words in the social relationship itself.

The definition of *illusio* needs to be filled out because it presents a paradoxical image of rational belief. Returning to our example of the desire to appear reliable/professional in the eyes of the target: as we have said, there is a degree of irrationality in this practice, because the target rarely believes that the attacker is reliable, particularly since the advice of cybercrime professionals is never to pay. What is more, it is the blackmail, rather than the reliability, which makes the target give in to the attacker’s wishes⁴³.

Despite this, cybercriminals continue to behave in a way which could be considered as being akin to professionalism in a ‘corporate’ sense. In reality, this is a manifestation of the existence of different forms of *illusio*, as we have said. First, we have the restricted definition already given: the belief that what is at stake in this social relationship makes it worthwhile/worth engaging in the game.

This is a form of *doxa*, a commitment principle: the attacker believes that if they commit fully to this behaviour when carrying out an attack, this will ensure a stronger relationship of trust with potential targets, and ensure the success of their future attacks, for example. In other words, it is worthwhile. Yet there is indeed a form of belief in this attitude, as we have said, because targets do not habitually trust attackers, and nor do they pay.

If we include thoughts of the target in our reading, there is also a principle of perception, an *ethos*, which is definitively irrational. This is the principle of what is evident in the eyes of the attacker: as an attacker, I am unable even to envisage behaving badly with the target. Professionalism is essential; that goes without saying.

Yet – and this is where we perceive the irrationality – the target does not envisage this as “going without saying”. They are rarely willing to pay, because they do not have this perception of the professional attitude as a sign of trust and honesty on the part of the attacker.

Finally, this pseudo-rational *doxa*, in the sense that this attitude would increase the chances of success in the future, and this *ethos*, in the sense that an attacker

⁴² Bourdieu, Pierre: *Raisons pratiques (Practical reason)*, Paris: Seuil, 1994, p. 151

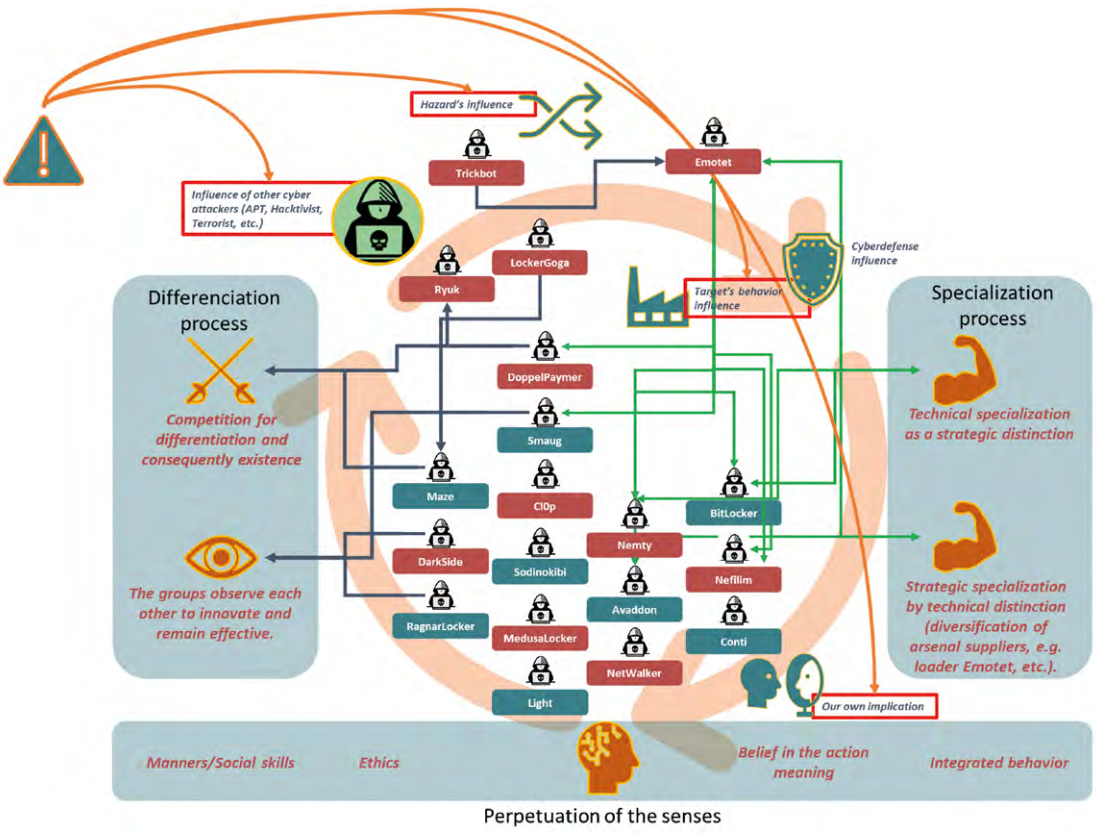
⁴³ We used the valuable work of Paul Costey for this development on the question of the existence of cybercrime *illusio(s)*. Paul Costey, “L’*illusio* chez Pierre Bourdieu. Les (més) usages d’une notion et son application au cas des universitaires”, (“*Illusio* in Pierre Bourdieu. The (mis)uses of a concept and its application to the case of university academics”), *Tracées*, 8/2005, p. 13-27. Available here: <https://journals.openedition.org/traces/2133#fn13>



is unable to envisage behaving in a different way, even if that appears irrational to the target, takes the form of a set of behavioural skills, a “way of being”.

This way of behaving when carrying out actions, this hexis, is akin to the notion of habitus. Within the scope of the relationship with the target, this behaviour becomes a structured and structural principle. It is observed, for example, in the similarity of the ransom demands sent to targets, which often follow an identical pattern.

It is these shared organising practices, principles and representations which define a cybercrime culture, even though cybercriminals would not identify or describe it as such. The practices, principles and representations form the basis of the sustainable sense of purpose which feeds into the logic of interaction. However, this sustainable sense of purpose applies to the purpose of actions, but not necessarily to the modalities for carrying them out, as we have seen with the emergence of disclosure blackmail.



Cybercrime is organised on the basis of differentiation and specialisation processes, and on the basis of a sustainable sense of purpose for actions, applicable to all actors.

Applying these concepts to the phenomena of Big Game Hunting and disclosure blackmail

The disclosure blackmail implemented by some cybercriminals in the form of integrated tactics is a phenomenon which first appeared in late 2019, notably with the attack by Maze against the American group Southwire.

In this section, we propose to take a look back at this development, and discuss the phenomenon known as Big Game Hunting from a broader perspective. We will also endeavour to arrive at an understanding of this phenomenon using the method explained in the first two parts of the report.

ENGAGING WITH COMPLEXITY: A RESURGENCE OF RANSOMWARE ATTACKS, OR A CHANGE IN BEHAVIOUR?

2019 was marked by an increase in cybercrime attacks using ransomware. This observation, shared by some security professionals, has been reported in the general and specialist media over the past year-and-a-half.

However, talking only about ransomware attacks runs the risk of introducing analysis biases. In fact, this “observation” is itself the result of a set of biases.



The risk of generalising
(Cybercrime defined as an
interlinking of interactions)

But where do these analysis biases come from? There is nothing that allows us to affirm or deny that this analysis represents a solidly verified and justified truth. It appears extremely difficult to arrive at a definitive measurement of the extent of a phenomenon such as ransomware attacks and/or organised cybercrime on a global scale.

A simple vision
of the transition to the tactic
of disclosure blackmail by BGH
actors (snapshot in unidirectional,
unidirectional mode).



France’s national agency for information system security (ANSSI), which has handled 104 ransom attacks since the beginning of 2020, points out that there has indeed been an increase. However, the agency also made the following comment: “These figures do not provide an exhaustive vision of the current situation in France regarding ransomware. This state of affairs is based only on the facts brought to the attention of the agency (by its beneficiaries and partners), and processed by it.”⁴⁴

Moreover, ANSSI has not observed an indiscriminate resurgence in the number of cyberattacks employing ransomware, but a resurgence in the specific tactic of Big Game Hunting (BGH).

« “Since 2018, however, ANSSI has observed a resurgence in ransomware attacks targeting organisations with significant financial resources or particularly critical activities. The importance of the targets brings ransomware into the category of attacks known as Big Game Hunting.

⁴⁴ <https://www.ssi.gouv.fr/actualite/rancongiels-face-a-lamplur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publient-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/>



The agency has additionally observed that some criminal groups are now combining the threat of disclosure of sensitive data with the use of ransomware, thereby increasing the pressure on victims to pay the ransom.⁴⁵»

2019 was marked by a series of even more elaborate targeted ransomware attacks on organisations (companies and institutions). These attacks are characterised by a greater than normal degree of sophistication and preparation. In addition, the targets are often large organisations, and the ransoms demanded are in the millions of Euros. This type of increasingly widespread attack is commonly known as Big Game Hunting (BGH)⁴⁶.

➤ **BGH: a new distinctive feature for major cybercriminals (specialisation)**

In terms of targeted attacks, this represents the consolidation of a phenomenon that has been known as 'Big Game Hunting' since mid-2018. This phenomenon, which has become part of core cybercrime practice according to ANSSI and its partners⁴⁷, is driven by attacker groups with significant financial and technical resources, who choose to carry out technically, tactically and strategically elaborate campaigns against extremely specific targets of very high value.

2019: A BIG YEAR FOR BGH

The slew of BGH attacks in 2019 started in January of that year, when the company Altran was compromised by the Locker Goga malware, which also went on to hit the Norwegian company Norsk Hydro two months later (in March). In May, the city of Baltimore in the United States was hit by the RobbinHood ransomware.

A month later, Eurofins became a victim. The bio-analysis group reported a loss of 62 million euros linked to the attack in its quarterly results.

BGH actors also struck in France, with Rouen University Hospital being compromised by the CIOp malware operated by ATK103 (TA505), a large group of Russian-speaking cybercriminals.

The M6 Group, France's largest privately-owned multimedia group, fell victim to the BitPaymer ransomware created by ATK180 (Indrik Spider).

A number of attacks on city authority networks were also observed, including certain networks that are of critical importance for local populations but are very poorly protected.

«INCREASE
IN RANSOMWARE
ATTACKS» REFERS TO
THE CONFIRMATION
OF THE BGH PARADIGM
(DYNAMIC VISION).

M6, one of France's biggest TV channels, hit by ransomware

Unlike The Weather Channel earlier this year, M6 remained on the air.

<https://securityaffairs.co/wordpress/92575/hacking/m6-group-ransomware-attack.html>

⁴⁵ Ibid.

⁴⁶ The appropriateness of the term Big Game Hunting to describe the concept in question appears increasingly questionable. In this section, we take a new look at the usual definitions applied to the term. Given that the attack methodologies described using the term appear to be undergoing a process of radical change, it seems necessary to raise questions about its pertinence. We indirectly provide some pointers on the limits of the concept here, but it is not our intention to call it into question in a definitive sense.

⁴⁷ <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf>



Although Big Game Hunting mainly affects organisations able to pay a high ransom, it must be understood that these organisations are not chosen simply on that basis.

Attackers scan the networks of an array of large companies and government bodies in search of a vulnerability that they can easily exploit. For example, vulnerabilities in the RDP protocol were widely used in late 2019/early 2020. Once a vulnerable network has been identified, the attacker determines the level of potential benefit offered by the future victim.

The huge advantage of these attacks was how simple they were to implement. First, the attacker did not need a highly developed command and control (C&C) infrastructure.

When the ransomware was activated, it simply created a file that usually included an email address to contact the attacker. It was via email that the ransom was negotiated, the crypto-wallet address was provided, and the decryptor was sent. The e-mail address was created anonymously by the attacker using the free ProtonMail service.



Specialisation via distinction

See: Specialisation based on strategic and technical distinction: the source of the division of labour in cybercrime «society»

Secondly, a number of ransomware-as-a-service operations also stood out due to their effectiveness in 2019. One of the best known, GandCrab (developed by ATK168 - Pinchy Spider), announced that it was shutting down operations the same year, to be replaced by other services such as Sodinokibi (possibly developed by the same group). These services were used by groups that did not have the time or skills to develop malware at this level.

These two characteristics of BGH attacks have been key factors behind the immense popularity of the technique. All that was required to have a severe impact on large companies was for a group of attackers to create a mailbox, buy good-quality ransomware, and distribute it.



Observers and targets as co-constituents of organised cybercrime

See: We are part of the makeup of cybercrime

The exponential growth in the popularity of this technique has nevertheless created enough of a stir for these large companies to take adequate measures to protect themselves against it. As a result, critical data backup, RDP monitoring and the use of specialised trading services have quickly become commonplace

These adaptation measures implemented by companies have pushed attackers to innovate.

A BIG GAME HUNTING MODEL CAPABLE OF RAPID ADAPTATION (STRATEGIC VERSUS PROGRAMMATIC THOUGHT)

In December 2019, BGH actors turned to disclosure blackmail. The American company Southwire, specialising in wire and cable production, was hit by the Maze ransomware. This attack is particularly interesting since it appears to define the contextual premises for the use of the new tactic of disclosing blackmail to ensure ransom payments.

After learning of the theft of sensitive information, Southwire did not deny paying the \$6 million ransom demanded, and took legal action against the attackers for violation of GDPR⁴⁸. The attackers then decided to publish part of the stolen data on a Russian hacking forum to induce the company to pay the ransom, together with the following message:

« But now our website is back but not only that. Because of southwire actions, we will now start sharing their private information with you, this only 10% of their information and we will publish the next 10% of the information each week until they agree to negotiate. Use this information in any nefarious ways that you want ⁴⁹».

It is interesting to note that the use of this tactic appears not to be simply a matter of circumstance.

In the words of the Maze operators themselves, it was a possibility that had been thought out and prepared for:

« Before lawsuit it was just few files as a proof. Now it is 10% of 120GB, but not in retaliation. It was planned if they don't negotiate. [...] ⁵⁰ ».

Although such high-quality BGH-type attacks remain on the fringe of the ransom demand phenomenon, they are part of a growing trend. Nevertheless, media coverage of such attacks has reinforced a feeling that ransomware attacks in general are 'proliferating'. This feeling often overshadows the fact that what we are actually seeing is an 'increase in a particular mode' of ransomware attack, i.e. BGH.

The reaction of the target as a source of uncertainty

See: Understanding the interlinked relationships between 'macro' and 'micro'/contextual' and 'individual' phenomena



Strategic rather than programmatic thought

See: We are part of the makeup of cybercrime



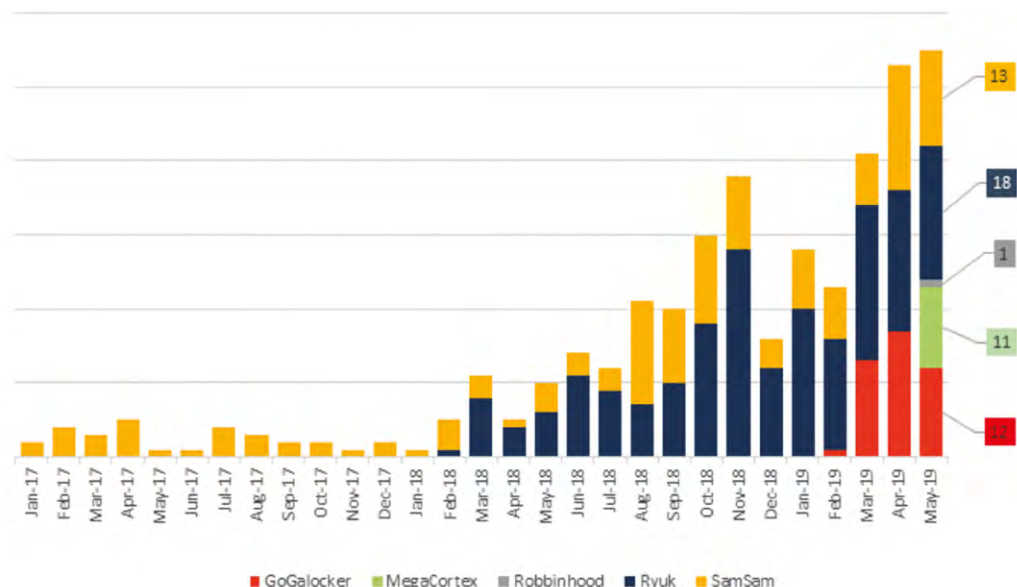
⁴⁸ <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf>

⁴⁹ <https://www.bleepingcomputer.com/news/security/maze-ransomware-publishes-14gb-of-stolen-southwire-files/>

⁵⁰ Ibid.



Proliferation of attacks involving certain ransomware programmes used for BGH (ANSSI, citing data from Symantec).



This constitutes a cognitive bias, motivated by a search for simplification, as we have explained. This bias is important for three reasons:



A snapshot vision can get in the way of a dynamic vision.

See: Cybercrime defined as an interlinking of interactions



Differentiation / Specialisation

See: The determining factors of strategic cybercrime interaction

- On the one hand, it suggests, by presenting these examples of BGH, that this specific tactic is behind a possible general proliferation of ransomware attacks. However, the transposition of a specific situation to provide an explanation for a general logical principle is highly typical of a simplistic approach. There is therefore a logical bias.
- On the other hand, as ANSSI reminds us, these targeted attacks use methods and techniques previously deployed by State-sponsored groups specialised in strategic and/or industrial espionage. The financial resources and the level of technical preparation required (zero-day search, manual propagation, significant preparation time, etc.)⁵¹ are still accessible to a residual number of cybercriminal groups. There is therefore an empirical bias.
- Finally, these two biases, logical and empirical, tend to inhibit the production of a pertinent analysis that is essential for the implementation of proactive cyberdefence.

⁵¹ <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf>





The widespread adoption of blackmail disclosure is the result of a complex process

THE ORIGINS OF A NOT-SO-NEW PHENOMENON (DIFFERENTIATION/SPECIALISATION AND A SUSTAINABLE SENSE OF PURPOSE)



Differentiation arising out of competitive and reference instincts.

See: *Differentiation via competition and referencing*

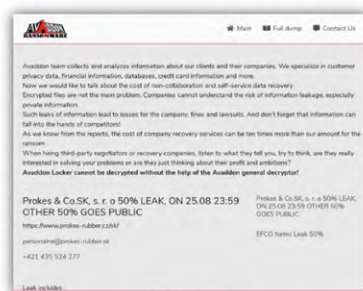
As discussed earlier, in terms of understanding this type of threat, blackmail disclosure is an interesting and fundamental change in BGH strategy.

The practice was initiated by Maze against Southwire as a 'considered possibility' even before launching the attack, according to the attacker's own confession.

However, during its second major attack, which made use of blackmail disclosure, the practice was not a 'possibility' within the Maze group's modus operandi, but an integrated and decisive part of its strategy

On the morning of January 30, 2020, Bouygues Construction was attacked by Maze. The cyberattack caused the company's servers to be shut down, but site activity does not seem to have been affected. The group demanded a ransom of 10 million euros in return for not disclosing the 200 GB of data that appeared to have been stolen. This attack made disclosure blackmail a recurrent component of Maze's modus operandi.

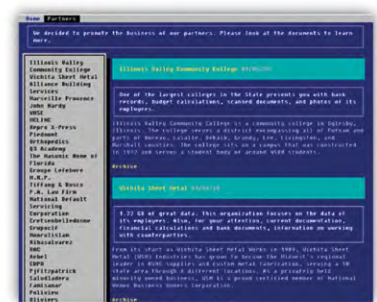
This new method was quickly replicated in the use of other ransomware employed in BGH models (although not exclusively), such as DoppelPaymer, Sodinokibi, Nemty, BitLocker, DarkSide, Smaug, MedusaLocker, Avaddon, Nefilim, RagnarLocker, ClOp, Light, NetWalker and now Conti.



Avaddon leak website



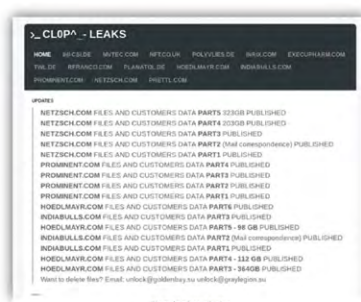
DarkSide leak and communication website



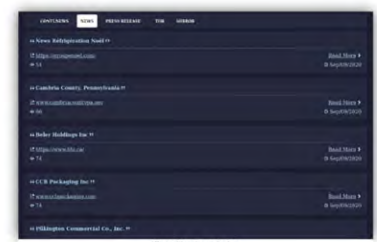
Pysa leak website



RagnarLocker leak website



ClOp leak website



Conti leak website

Dataleak websites of major players in organised cybercrime



› From tactical change and peer adoption to confirmation of effectiveness

By changing this tactical building block of its *modus operandi*, the Maze group initiated a broader and more complex change in the BGH format.

relationship based on inspiration with a reference model seems to have started in more or less rational form. This relationship modified the reference framework of BGH actors as well as the norms of Big Game Hunting.

In rational terms, this new tactic of disclosure blackmail appears entirely appropriate, since the «logical» probability of recovering the ransom demanded is higher (as we explain in the section “A practice resulting from a strategic reflection centred on an in-depth perception of cyberdefence responses”).

But there is also an element of irrationality, even if it seems minimal here. As far as we know, there was no evidence that the groups which mimicked Maze by adding this tactical element of disclosure blackmail to their TTPs had empirical, rather than logical, proof that this tactic could «work better» if a good cyberdefence policy was implemented.

› Inspiration based on pre-existing practices from outside the cybercrime arena

From our point of view, disclosure blackmail, and its dissemination as an acceptable and accepted tactic of BGH actors, stems from three important exogenous factors.

- › Firstly, BGH actors observe other forms of cyber threats, and may unconsciously perceive them as models. In this case, disclosure blackmail has already been observed in the *modus operandi* of some APTs, but also in very distantly related practices such as the phenomenon of sextortion.
- › Secondly, attackers monitor security companies and observe best practices (often published), allowing them to understand the strategy adopted by their targets.
- › Thirdly, BGH targets – by definition large groups capable of withstanding a large ransom – often have a good cyberdefence policy in technical and crisis management terms.

EMERGENCE AS A RESULT
OF A DIVERSE SET
OF FACTORS
(DIFFERENTIATION/SPECIALISATION
AND A SUSTAINABLE SENSE OF
PURPOSE)

Differentiation/specialisation and
a sustainable sense of purpose

See: *The determining factors of strategic
cybercrime interaction & Interaction and
the cybercrime organisation*





INSPIRATION FROM RELEVANT PRACTICES IN OTHER AREAS OF THE CYBER THREAT LANDSCAPE

One of the earliest well-known examples of the use of disclosure of a major target's data to force compliance with attackers' demands occurred in 2014, when Sony Pictures was attacked by a North Korean hacker group.

Sony Pictures had just announced the release of the film «The Interview» which depicted the assassination of the North Korean leader Kim Jong-Un. The hackers, who had paralyzed the production company, demanded that the film be withdrawn. Sony Pictures refused. Following this refusal, the hackers posted the stolen data online

It is interesting to note that the attackers chose to disclose this data on a massive basis, without prior sorting. However, this attack demonstrated to everybody, via the media, that the indirect consequences of a cyberattack can be worse than the attack itself. For example, in addition to revealing news about future projects, the emails obtained by the hackers revealed damaging conversations among Sony executives, in particular racist exchanges between Sony Pictures co-chairperson Amy Pascal and producer Scott Rudin. Sony had such difficulty dealing with this indirect consequence of the attack that it threatened to sue The New York Times, Bloomberg and Businessweek.

The indirect impact of this cyberattack on Sony Pictures' reputation was more damaging than the direct financial impact (which went on to exceed \$100 million).

This type of media event necessarily creates, to a greater or lesser degree, drivers of inspiration, all the more so in this case because the film «The Interview» has never had a theatre release. The strategy worked.

In addition to the unconscious influence of this practice originating from other areas of the cyber threat landscape, and its conscious strategic use, attackers monitor security companies and national information systems security agencies.

CLOSE SCRUTINY OF OUR PREVENTION, MITIGATION AND COUNTERMEASURES STRATEGIES FOR RANSOMWARE ATTACKS

BGH-type attack groups are becoming increasingly similar in their modus operandi and preparation to some State-sponsored espionage groups.

They have therefore become accustomed to carrying out targeted, adaptive attacks. This agile approach is obviously adjusted to take account of prevention, mitigation and countermeasures solutions recommended to customers.

Accordingly, the main recommendations that cyberdefence specialists generally make to mitigate the risk of attacks are as follows ⁵² :

⁵² On the basis of ANSSI's recommendations: «Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident?» ("Ransomware attacks concern everybody. What is the best way to anticipate them, and respond to an incident?"), url: <https://www.ssi.gouv.fr/actualite/rancongiels-face-a-lampleur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publie-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/>



- › Back up data,
- › Keep software and systems up to date,
- › Use anti-virus software, and keep it up to date,
- › Partition information systems,
- › Limit user rights and application permissions,
- › Control Internet access,
- › Monitor the press,
- › Raise awareness among employees,
- › Assess the possibility of purchasing cyber-insurance,
- › Implement a cyberattack response plan,
- › Reflect on a cyber-crisis communications strategy.

The following response actions are advised if an attack actually occurs:

- › Adopt the right reflexes,
- › Ensure a managed response to the crisis,
- › Seek technical support,
- › Communicate at the right level,
- › Do not pay ransoms,
- › File a complaint,
- › Restore systems from healthy sources.

Data backup is the only effective countermeasure against a conventional encryption tactic in the event of an attack, because the encrypted data then no longer has any value for the purpose of exerting pressure on the target.

However, this “definitive” countermeasure proves totally ineffective against the tactic of disclosure blackmail.

The remainder of the recommendations depend on the target maintaining their cyberdefences in the best of health at all times; few companies, even the best protected, are beyond reproach in that area. As a result, attackers focus on their targets’ vulnerabilities. They can use exploits, linked to a specific type of machine or software version, to scan the target’s network in search of a vulnerable machine or software to enable them to carry out their attack.



BGH actors are also beginning to specialise in the search for zero-day vulnerabilities that can help circumvent targets' patching policies and, in particular, offer an alternative to traditional spearphishing for the purpose of gaining initial access.

TARGETS ARE ALSO SCRUTINISED

Data backup, which acted as a kind of physical buffer against data encryption, has become obsolete in the face of disclosure blackmail. Attackers are no longer faced with a «definitive» countermeasure.

Using observation, zero-day search or regular phishing, they can gamble on an error on the part of their target to enable them to compromise it. Companies thus find themselves in an advanced threat continuum.

The growing maturity of large companies has led to the practice of data backup becoming more widespread, making advanced ransomware attacks with simple encryption less effective, or even inappropriate, for large ransom demands.

Blackmail disclosure, as explained above, moves us away from this logic of the binary arm-wrestle between “paying” and “not paying”, a process which was becoming increasingly disadvantageous for attackers. This new tactic allows attackers to gain the upper hand, with several different possibilities for exerting pressure.

> Identifying internal developments in the cybercrime arena

The new method of threatening to disclose data (disclosure blackmail) has been one of the latest trends to create bridges between two techniques that are well-established and are associated with different groups. These techniques are:

- > Ransomware
- > Data stealers

A NEW TACTIC ARISING FROM SYMBIOSIS BETWEEN TWO PRE-EXISTING METHODS: RANSOMWARE AND DATA STEALERS

How did ransomware and data stealers meet up? The two methods are seemingly very different, and have different targets.

The link between them dates back a relatively long way, however, and was primarily established by another player in the field: banking trojan operators.

Banking trojan operators sell access to compromised machines to other groups. Originally, they used to sell access to either of the groups in question, but not both.

However, stealers typically need access to the target's computer once, in order to steal as much as possible. It therefore makes sense to drop a stealer, allow it to collect everything of value, and then drop ransomware.



Banking trojans that were already dropping malware therefore began dropping both stealers and ransomware, in order to maximise value

Stealers which operate via purchased access, however, decided to take the matter into their own hands, and integrated ransomware deployment directly into their malware.

One of the more popular stealers, AZORult, has had this feature since July 2018.

A COMBINED APPROACH THAT HAS BECOME WIDESPREAD IN BGH

Ransomware authors went through the same process, of course, and groups that typically stuck to the “Fire-and-Forget” methodology began thinking about dropping a stealer before activating the ransomware.

The Ryuk group, for example, briefly released a malware programme called RyukStealer, based on most of Ryuk’s codebase.

These new activities did not pass unnoticed, and groups that conduct targeted attacks (i.e. Big Game Hunters) thought about doing the same.

These groups began stealing data, and may have gained the impression, partially due to the work of State-sponsored groups which steal confidential data, that they were sitting on a gold mine.

They therefore equipped themselves with data theft capabilities. Instead of trying to sell the information, however, they went down another route, and began using it to extort ransoms more effectively.

This might be due to the fact that selling sensitive data is complex, owing to the need to have access to the right networks and find interested parties.

Publicly announcing that you have stolen the data before encrypting the system therefore serves two purposes:

- It may induce targets to pay
- It shows that you have access to the information, potentially allowing you to make contact with buyers.

➤ A practice resulting from a strategic reflection centred on an in-depth perception of cyberdefence responses

We now understand that the establishment of disclosure blackmail as a standard tactic by BGH actors is the product of a complex set of factors internal and external to organised cybercrime.

We have also explained that this set of interactions in the form of patterns of inspiration was more or less rational within cybercrime



Rationally, a group like Maze, and the groups that have been inspired by it, know that the effectiveness of conventional encryption and ransom tactics is determined by three limitations:

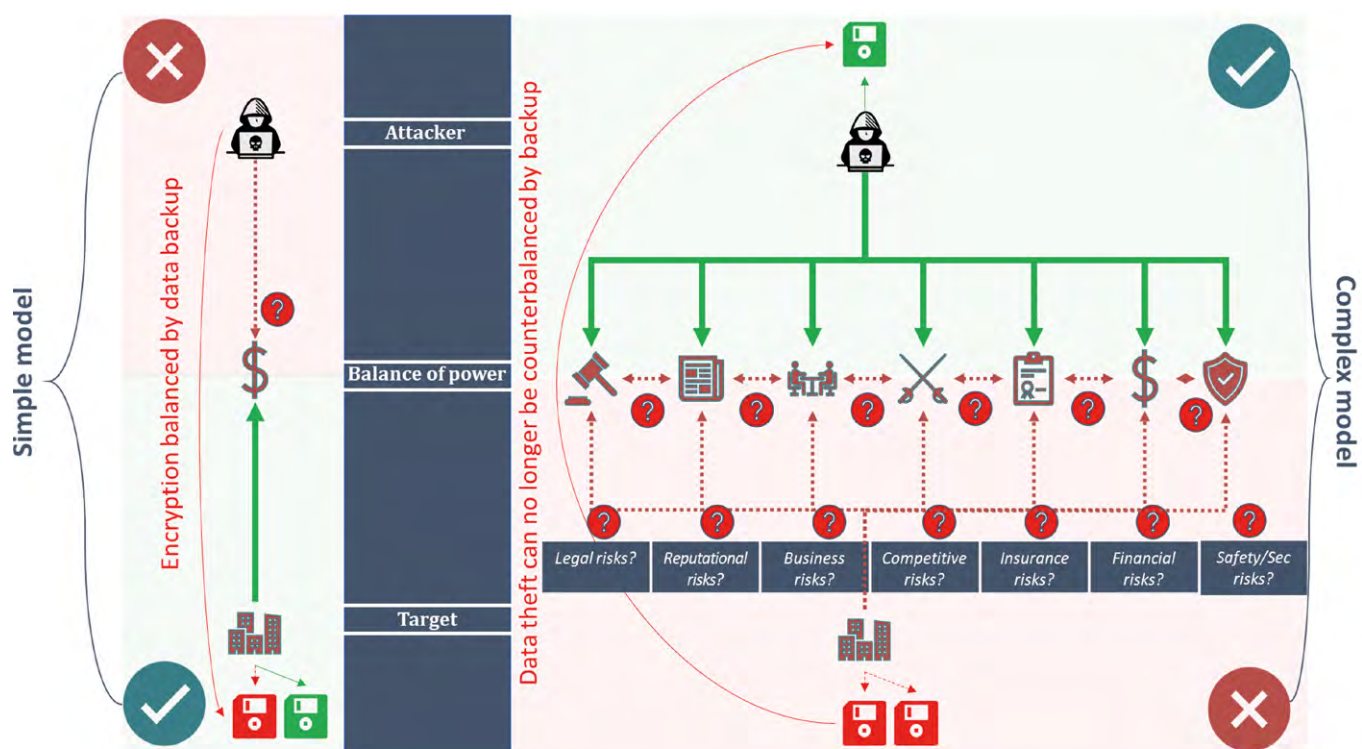
- The levers applied in the old model do not allow irresistible pressure to be exerted on the target. The model involves a simple choice, with calculable and conceivable consequences. It does not involve uncertainty in the mind of the target. Encrypting the data, and then threatening not to decrypt it if payment is not made, leaves the target with the simple choice of whether to pay, or not to pay.
- This choice has been facilitated by companies and information systems security agencies who regularly advise targets not to pay, and to perform regular data backups and network traces to minimise the one-off impact of data loss.
- Lastly, this tactic is old, and has therefore been carefully considered and effectively integrated by large companies targeted by BGH actors.

There is therefore scope for attackers to adapt their strategic thinking to the limits determined by the targets.

Disclosure blackmail establishes a principle of uncertainty in the mind of the target, who does not know how their data will be used, and cannot envisage the magnitude of the impact.

This state of uncertainty is not altered by making regular backups or taking steps to trace the attacker. Finally, the fact that the tactic is new means that there is no definitive, perfect solution, which gives attackers a head start.

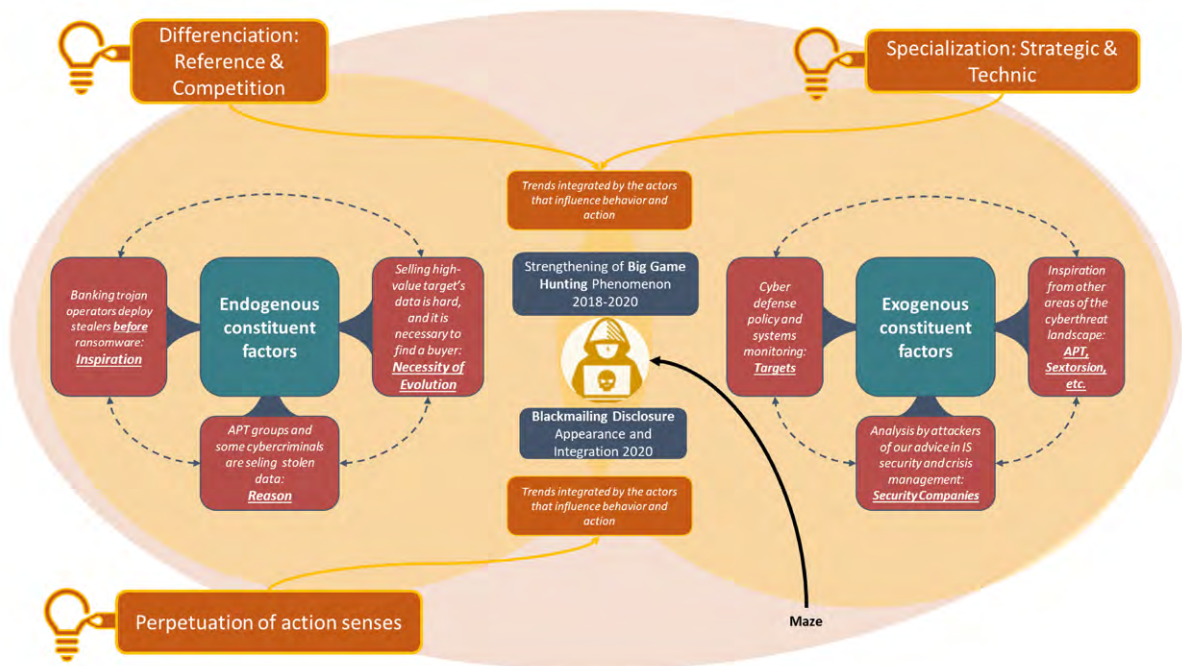
Another psychological effect which is key to attackers' ability to complicate the crisis management process is the difficulty of estimating which data will be potentially damaging on different levels (reputational, legal, competitive, business, etc.). This increases the pressure on the target.



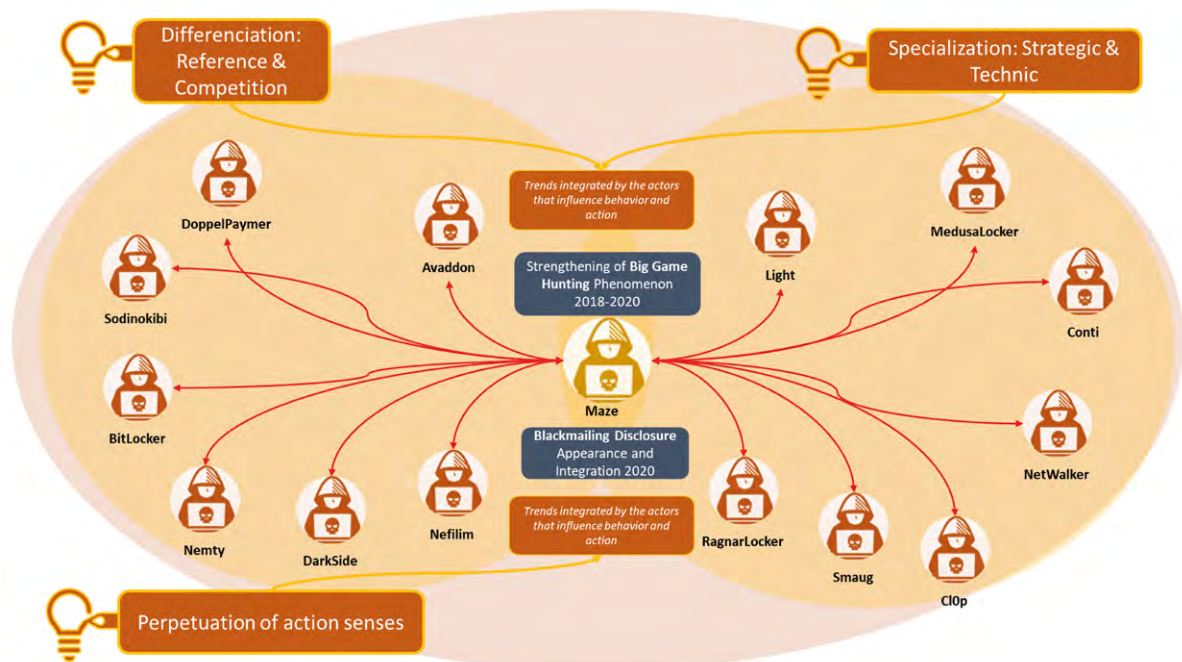
Moving from a simple ransomware attack model to a complex model with the potential for greater harm to the target



The macrophenomenon of interaction (the cybercrime organisation) influences the microphenomenal levels (strategic thinking on the part of actors)



The microphenomenon (strategic thinking on the part of actors) incorporates interaction via a sustainable sense of purpose, and influences the macrophenomenal level (the cybercrime organisation).





Conclusion

What are the key points to take away from this report on organised cybercrime, which exhibits such specific features in the area of Cyber Threat Intelligence?

A GUIDE AND INPUTS TO AID UNDERSTANDING

Cybercrime is not an organisation of cybercrime actors. It is an organisation of interactions between actors whose intention is to take action in respect of what they consider to be cybercrime.

This simple idea, which required such lengthy development, must always be borne in mind when we are dealing with cybercrime.

Cybercrime, as a macrophenomenon, can be likened to a set of structural and structured interactions between actors who have an interest in exerting influence within a context of transgression of a system of legal norms.

It is an organisation of cybercrime interactions, and not a space of cybercrime actors.

The actors are groups of real people. They carry out “actions” of a strategic nature, in a relationship of opposition, to pursue an interest within the context of transgression of a social system with legal norms (a crime or misdemeanour).

« The conception of an action is only strategic if it stands in opposition to an Other, with both will and intelligence. If this is not the case, it is merely technical in nature. ⁵³ ».

It is the interactions between cyberattackers (not only “cybercriminals”), their targets, observers, cyberdefence advisors, and all the other actors involved in this context of transgression, in the pursuit of their interests, which organise cybercrime. They are also modelled by that same organisation. The organisation is structured by the interactions, and also structures them.

There is, therefore, a diversity of interests. The desire to secure financial gain; the desire to protect oneself; the desire to advise; the desire to comment and explain. All these interests organise cybercrime as a macrophenomenon of interactions.

It is this innovative approach that we wished to develop.

⁵³ *Politique Étrangère* (journal), Institut français des relations internationales, “La stratégie en theories” (“Strategy in theories”), Vincent Desportes, 2014/2 Summer, p. 168.



Adopting an approach based on interaction enables the invariable nature of the actors to be dismantled. No actor is a criminal in essence; no actor is therefore deterministically restricted to programmatic behaviour.

There are no definitive “cybercrime” actors, or at least, interactions between “cybercrime” actors are not the only component of organised cybercrime.

The possibility thus arises of envisaging the importance of the strategic context of transgression of an accepted system with legal norms in which actors of very different types operate.

The analysis of organised cybercrime thus focuses on all of the interactions between actors with an interest in influencing this context. Cybercriminals, APTs, hacktivists, cyberterrorists, targets, commentators, observers, and all actors with a possible interest in this context, organise cybercrime in the sense that they interact with each other within it.

If action, being the pursuit of interests, is influenced by a context of interactions in perpetual evolution, it is not determined on the basis of essence. Action in the form of interaction is thus strategic by its very nature.

If the interactions that form the basis of the organisation of cybercrime originate from actors acting strategically as a function of their context, they cannot be solely technical in nature.

This means that the “links” presented as technical relationships (for example, sharing of arsenals) are the manifestation of deeper, fundamental interactions between actors.

It is these fundamental interactions which enable us to understand how cybercrime is organised.

Our categories of empirical observations, and our concepts of reason (groups of attackers, cybercriminals, etc.), are no longer sufficient to enable us to comprehend these fundamental interactions.

We have to create concepts of understanding, which reflect a profound dialogue between our own understanding and what we perceive. These concepts – which can sometimes be likened to intuition – are only pertinent insofar as they are empirically verifiable. Yet for all that, let us not fear our intuition.

« Concepts of reason enable us to conceive, concepts of understanding to understand (perceptions).⁵⁴ »

⁵⁴ *Critique de la raison pure (Critique of pure reason)*, Emmanuel Kant, Flammarion, 2006, p.340-341.

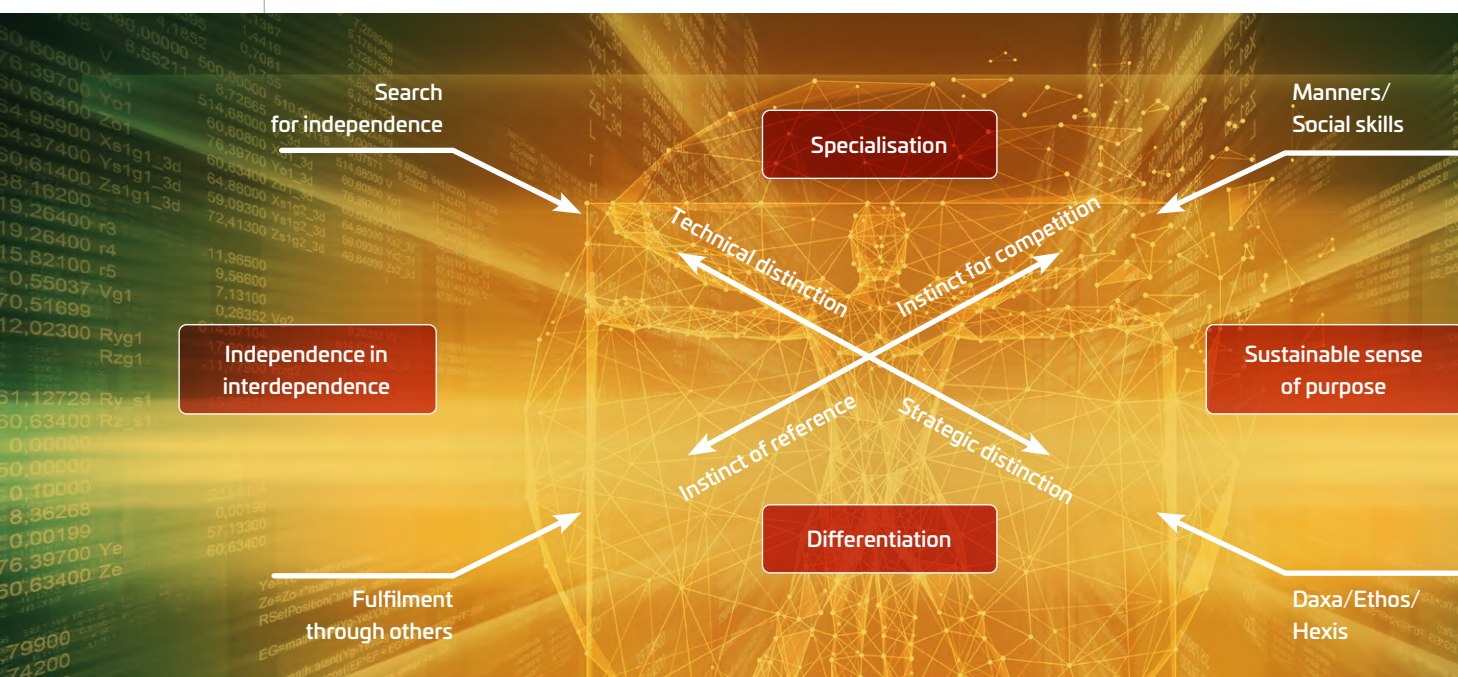


NEW KEYS TO UNDERSTANDING

The concepts that enable us to understand what generates interaction and breathes life into cybercrime as an organisation.

Starting from this simple observation, some new concepts are set out in this report:

- If there is no fixed space, but only the effects of vast numbers of interactions, applying only a snapshot vision is inadequate.
- Without a dynamic vision, capable of navigating through the recursive nature of the interactions in the multiplicity of dimensions of the threat and the analysis frameworks applied to it (cybercrime does not refer only to cybercriminals, for example), we instinctively dismember the reality that we wish to understand. We put ourselves in even greater danger.
- This cross-referencing of visions allows us to bring together the construct of cybercrime, the intellectual construct of the observed object, and perceived cybercrime in the form of a multi-dimensional and recursive interaction space.
- These interactions are produced by a complex set of processes, designated by means of the following concepts:
 - Expansion of the organisation as an observed reality, linked to a process of:
 - Differentiation via competitive instinct and reference instinct,
 - Specialisation via the instinct for strategic distinction and the instinct for technical distinction,
 - Concentration of the organisation as an observed reality, linked to a process of:
 - Relationships of independence within interdependence,
 - A need for a sustainable sense of the purpose behind actions.





At the start of this report, we explained that one of the most sophisticated and predatory forms of cybercrime today is a phenomenon generally referred to by the Cyber Threat Intelligence community as Big Game Hunting (BGH).

BGH attackers – typically groups of cybercriminals with extensive financial resources, significant technical capabilities, and a high level of tactical development and strategic thought – target elaborate, extensively prepared ransomware attacks at very large organisations.

Ransom demands now run to millions or tens of millions of euros, instead of just thousands previously, and can threaten the very survival of strategic organisations.

BGH actors have, in particular, been responsible for the widespread use of disclosure blackmail, an innovative attack tactic, which has been catching organisations off guard since late 2019.

This phenomenon has brought sweeping change to the cybercrime threat landscape, with attackers displaying characteristics similar to major State-sponsored espionage groups (Advanced Persistent Threats) while retaining their core purpose of securing financial gain. A new dimension is emerging, with major cybercriminals and State-sponsored groups observing and emulating each other, resulting in further blurring of the conceptual boundary between cybercrime and espionage.

Inspired by these developments, organised cybercrime has created hybrids known as criminal APTs.

The final part of this report focuses on analysing this phenomenon and its evolution through the prism of developed concepts.

Online data disclosure blackmail is thus no longer considered solely from the point of view of the emergence of a new tactic developed by BGH actors, but also as the culmination of a long process of interactions which models both macro and micro aspects.

Macrophenomenal phenomena influence the emergence of the tactic at the microphenomenal level (at the level of the Maze operator):

➤ Endogenous constituent factors

- APT groups and some cybercriminals were already selling stolen data: reason (differentiation via reference instinct and competitive instinct)
- It is difficult to sell data from a high-value target, and it is necessary to find a buyer: need for evolution (specialisation via strategic distinction)
- Banking trojan operators deploy stealers before ransomware: inspiration (differentiation via reference instinct and competitive instinct)

APPLICATION TO A USE CASE: DISCLOSURE BLACKMAIL



➤ Exogenous constituent factors

- Inspiration from other areas of the cyber threat landscape: APT, sextortion, etc. (differentiation via reference instinct and competitive instinct, and specialisation by moving closer to the APT model, with a tendency towards hybridisation).
- Analysis by attackers of our advice on IS security and crisis management (in particular the advice not to pay): security companies (differentiation via reference instinct and competitive instinct)
- Cyberdefence policy and systems monitoring: objectives (differentiation via reference instinct and competitive instinct)

Macrophenomenal interaction thus lies at the heart of the emergence of the practice at the level of Maze (micro level). These interaction concepts and processes, combined with the concept of a sustainable sense of the purpose behind actions, enable the transposition of this approach to the BGH structure to be understood.

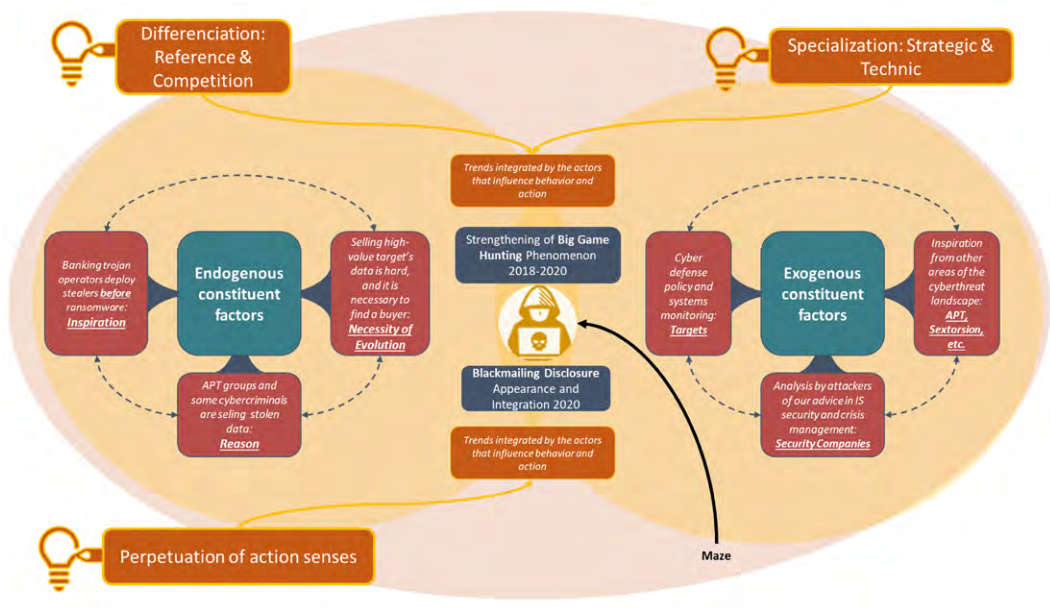
The same principle can be observed from the micro level (Maze operator) to the macro level, with increasing hybridisation of Big Game Hunting actors:

- While the manifestation of the definitive emergence of blackmail as an integrated practice was revealed at the level of the operator of the Maze ransomware against Southwire (macro to micro), the same principles led to the standardisation of the tactic among BGH actors as well as more broadly (micro to macro):

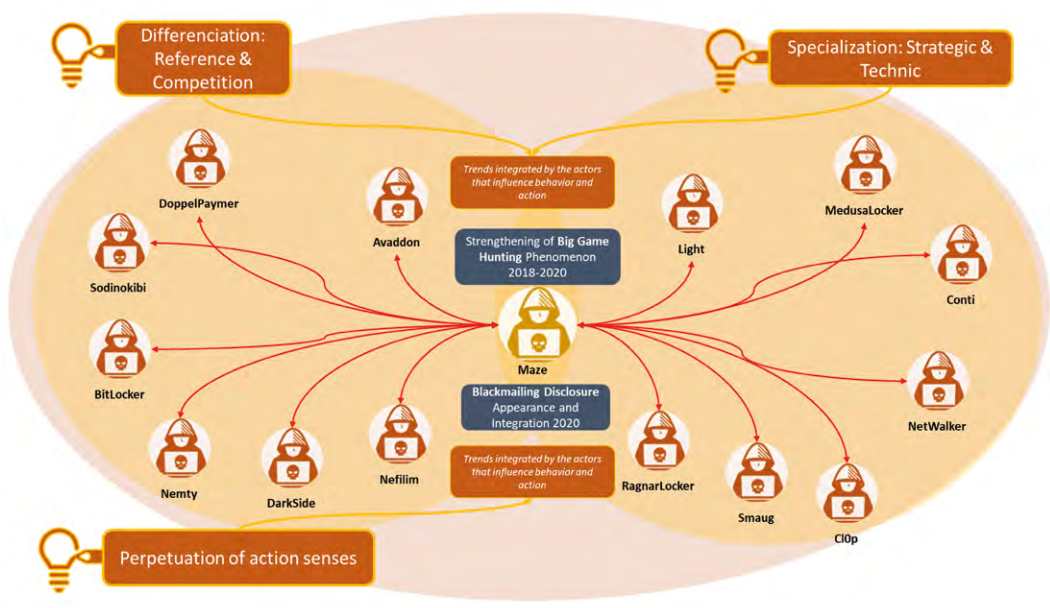
- | | | |
|-----------------|-----------------|--------------|
| ➤ DoppelPaymer, | ➤ Smaug, | ➤ ClOp, |
| ➤ Sodinokibi, | ➤ MedusaLocker, | ➤ Light, |
| ➤ Nemty, | ➤ Avaddon, | ➤ NetWalker, |
| ➤ BitLocker, | ➤ Nefilim, | ➤ Conti. |
| ➤ DarkSide, | ➤ RagnarLocker, | |

These new concepts enable us to understand the importance of interaction, which transcends the micro and macro levels and organises cybercrime in its entirety.

Interaction is the very foundation of organised cybercrime.



The macrophenomenon of interaction (the cybercrime organisation) influences the microphenomenal levels (strategic thinking on the part of actors)



The microphenomenon (strategic thinking on the part of actors) incorporates interaction via a sustainable sense of purpose, and influences the macrophenomenal level (the cybercrime organisation)



RECOMMENDATIONS AND GOOD PRACTICES

> Follow the operational recommendations issued by ANSSI⁵⁵

- > To reduce the scope of attacks, and the damage resulting from them:
 - > Back up data,
 - > Keep software and systems up to date,
 - > Use anti-virus software, and keep it up to date,
 - > Partition information systems,
 - > Limit user rights and application permissions,
 - > Control Internet access,
 - > Monitor the press,
 - > Raise awareness among employees,
 - > Assess the possibility of purchasing cyber-insurance,
 - > Implement a cyberattack response plan,
 - > Reflect on a cyber-crisis communications strategy.
- > Following an attack:
 - > Adopt the right reflexes
 - Keep a log,
 - Quickly disconnect data backup media if they are isolated and not infected,
 - After identification of an attack, search for threat characteristics in IS logs (IoC, etc.),
 - Do not disconnect the electrical power supply of machines, but put them into sleep mode,
 - Do not switch on machines that are already switched off,
 - Prohibit the use of peripherals,
 - Retain encrypted data in case a decryption solution is subsequently discovered and published
 - > Ensured a managed response to the crisis,
 - > Seek technical support,
 - > Communicate at the right level,
 - > Do not pay ransoms,
 - > File a complaint,
 - > Restore systems from healthy sources.

⁵⁵ On the basis of ANSSI's recommendations: «Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ?» ("Ransomware attacks concern everybody. What is the best way to anticipate them, and respond to an incident?"), url: <https://www.ssi.gouv.fr/actualite/rancongiels-face-a-lamplur-de-la-menace-lanssi-et-le-ministere-de-la-justice-publient-un-guide-pour-sensibiliser-les-entreprises-et-les-collectivites/>



› Keys to understanding a dynamic approach to cyberdefence

- › Focus on analysis of interaction nodes between threat elements. Start with reference groups. Determine recurrent schemes and cyclical behaviours.
 - › For example: if there is extensive activity by a group like Emotet, which operates cyclically in waves of compromise targeted at new machines, do not simply enable detection and protect against Emotet, but also protect against Trickbot and the Ryuk ransomware (three actors who interact extensively), and if possible against Nephilim.
- › Identify common interaction schemes by focusing on attackers' cultural practices so as not to conceal certain elements of a threat.
 - › For example: if an attacker changes behaviour, or if a new attacker appears, and they are considered a threat. To consider their behaviour, it is necessary to determine whether they exhibit TTPs, an attitude to targets, formalised approaches (such as ransom notes) or ethics (such as not targeting a particular sector) that are similar to other reference attackers. The more extensive the interactions (in terms of reference or competition), the easier it will be to analyse the attacker.
- › Track new trends in organised cybercrime (an increase in interactions implies a high level of replication of new tactics).
 - › For example: disclosure blackmail
- › Threat analyses should no longer be based solely on the assumed nature of the attackers, but on the latter's practices and interactions.
 - › For example: sectors which are highly dependent on OT/ICS/SCADA systems, which typically focus on advanced threats such as State-sponsored espionage groups, must expect a resurgence of specialised ransomware-type attacks following the EKANS attack against the firms Honda and Enel in June 2020.
- › Engage in threat analysis as part of defence/security measures by envisaging responses that can be elicited from attackers.
 - › For example: if security policy and the training provided to employees of a company are at the correct level, envisage attackers' bypass strategies (for example supply chain-type attacks).
- › Adopt a comprehensive approach to crisis management, rather than simply focusing on financial aspects.
 - › For example: in the event of data disclosure blackmail, make plans to manage the reputational, legal, business, competitive, insurance, financial and safety/security aspects of the crisis.





4, avenue des louvresses
92230 Gennevilliers
France
Tél: +33(0)1 41 30 30 00

> thalesgroup.com <

