tenable
RESEARCH

THE RANSOMWARE ECOSYSTEM

How commodification of tactics and techniques birthed an industrial revolution of global cybercrime

Contents

Introduction

At the RSA Conference in 2020, Joel DeCapua, a supervisory special agent with the Federal Bureau of Investigation (FBI), **revealed that ransomware groups had collectively earned over $144 million** from 2013 through 2019, which was considered a staggering number at the time. However, in 2020 alone, ransomware groups **reportedly earned $692 million from their collective attacks**, nearly five times more than in the previous six years combined. These numbers are likely undercounts of the true figures because of a lack of insight into the cryptocurrency wallets used by all of the ransomware groups along with delays in receiving such data. However, these numbers underscore one undeniable fact: ransomware has cemented itself as one the greatest threats to global organizations today — and it has become a lucrative criminal ecosystem in the process.

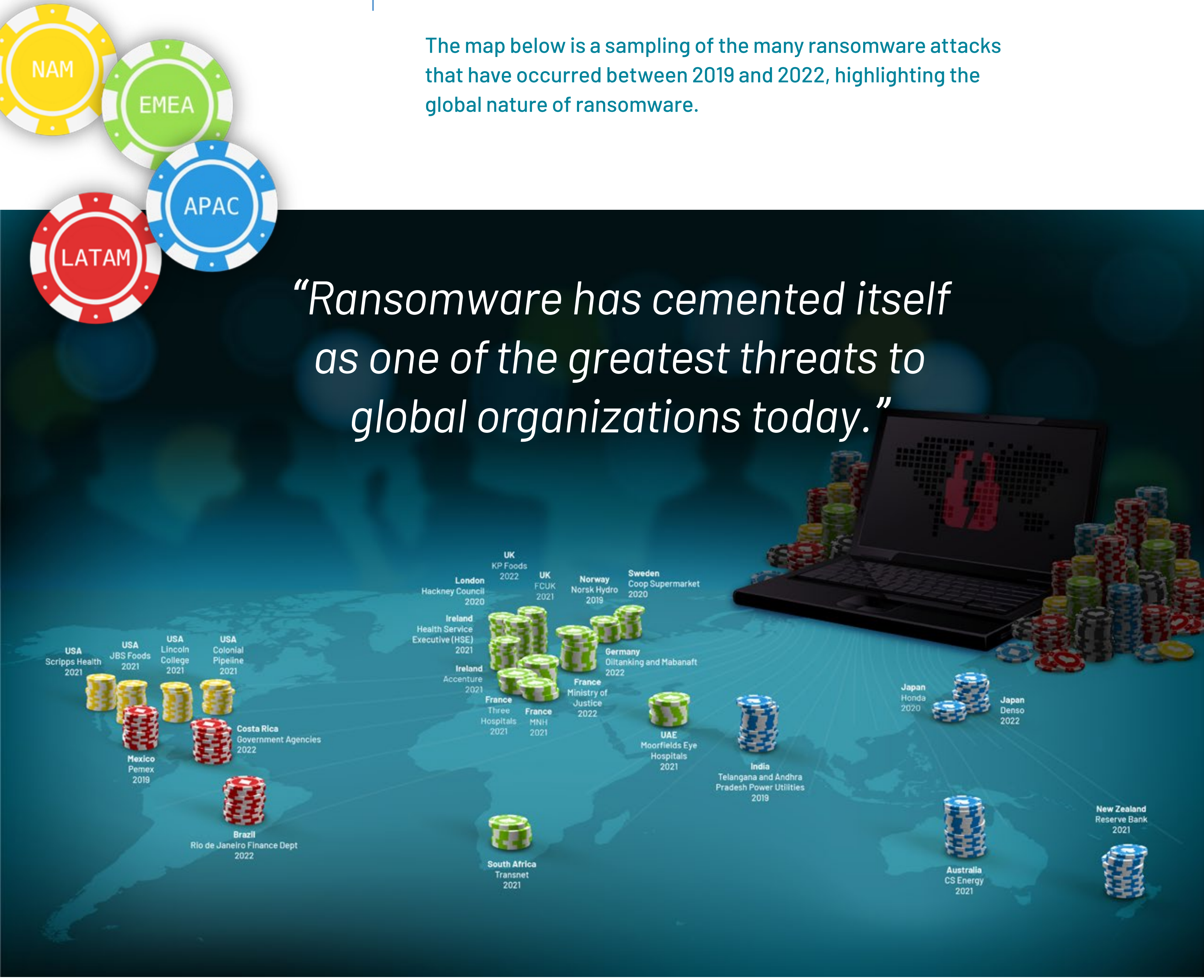
Advanced persistent threat (APT) groups consist of individuals that target organizations and governments around the world in service of nation states. These groups include those that serve as part of the nation states directly or receive tacit backing from nation states (state sponsored) but operate independently.

Advanced persistent threat (APT) groups have long been considered by many to be the most dangerous threat to organizations. These groups focus more on cyberespionage and are less financially driven, which limits their scope to a targeted set of organizations and governments. Meanwhile, threat actors in the cybercrime world are primarily motivated by financial gain because, as rapper DJ Quik says, “If it don’t make dollars, it don’t make sense.”

In reality, no organization is truly safe from ransomware, as large to small organizations are fair game.

In Tenable's 2021 Threat Landscape Retrospective report, the Security Response Team determined that at least 38% of all data breaches in 2021 were the result of ransomware attacks, compared to 35% in 2020. In the healthcare sector, ransomware represented 36.2% of breaches, while it represented 24.7% of breaches in education. This doesn't mean ransomware is any less prevalent in other sectors. However, because of the stringent reporting requirements for healthcare organizations in the United States, it is no surprise that the bulk of ransomware attacks are reported in that sector. A recent survey by Sophos found that 66% of businesses reported experiencing a ransomware attack in 2021. In reality, no organization is truly safe from ransomware, as large to small organizations are fair game.

The map below is a sampling of the many ransomware attacks that have occurred between 2019 and 2022, highlighting the global nature of ransomware.


NAM
EMEA
APAC
LATAM
USA Scripps Health 2021
USA JBS Foods 2021
USA Lincoln College 2021
USA Colonial Pipeline 2021
Mexico Pemex 2019
Costa Rica Government Agencies 2022
Brazil Rio de Janeiro Finance Dept 2022
UK KP Foods 2022
London Hackney Council 2020
UK FCUK 2021
Norway Norsk Hydro 2019
Sweden Coop Supermarket 2020
Ireland Health Service Executive (HSE) 2021
Ireland Accenture 2021
Germany Oiltanking and Mabanaft 2022
France Ministry of Justice 2022
France Three Hospitals 2021
France MNH 2021
UAE Moorfields Eye Hospitals 2021
India Telangana and Andhra Pradesh Power Utilities 2019
Japan Honda 2020
Japan Denso 2022
South Africa Transnet 2021
Australia CS Energy 2021
New Zealand Reserve Bank 2021

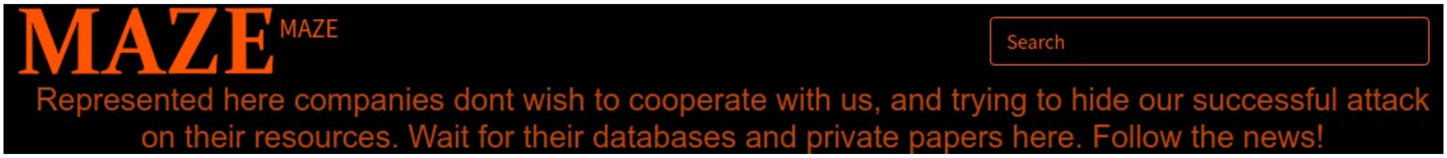
"Ransomware has cemented itself as one of the greatest threats to global organizations today."

One of the primary reasons ransomware has prospered is due to the advent of ransomware-as-a-service (RaaS). RaaS catapulted ransomware from a fledgling threat into a force to be reckoned with. RaaS is a service model, just like Software-as-a-Service, where instead of providing access to legitimate software applications, ransomware groups provide the malicious software (ransomware) and infrastructure necessary to facilitate ransomware attacks while relying on third parties, known as affiliates, to do the actual dirty work of gaining initial access into an organization before deploying the ransomware.

Ransomware has become its own self-sustaining industry. Previously, attacks were perpetrated by the same ransomware groups that developed and propagated the malware, but the advent of RaaS has attracted multiple players. Each has a vital role, making up what we refer to as the ransomware ecosystem. Outside of the ransomware groups, the other key players include affiliates and initial access brokers (IABs).

RaaS was just the beginning. Ransomware's current dominance is directly linked to the emergence of a technique known as double extortion.

In 2019, the Maze ransomware group pioneered the double extortion technique as part of its attacks against companies. It involves exfiltrating data from victim organizations and publishing teasers about these breaches on the dark web on public shaming sites, commonly known as leak websites.



Represented here companies dont wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news!

Image Source: Krebs on Security

Since double extortion was introduced, the majority of ransomware groups operating today have incorporated it into their attacks, hosting their own leak websites on the dark web. In the sports world, teams that have pioneered winning techniques, like the NFL's West Coast Offense or Tampa 2 Defense, are often copied by other teams hoping to find similar success. In the same way, ransomware groups have copied Maze's technique, and the massive success seen in ransomware is undeniably owed to double extortion.

While there have been some efforts to curtail ransomware attacks over the years, such as law enforcement actions to arrest ransomware operators and government sanctions against cryptocurrency exchanges, ransomware activity is unabated. We continue to see ransomware groups successfully attacking organizations across a variety of industries, with some ransomware groups even returning from the dead.

Our goal with this report is to help demystify the ransomware ecosystem by exploring the key players involved, as well as the techniques and tactics utilized by ransomware operators and their affiliates to infiltrate organizations and distribute ransomware payloads. We also provide a list of the most common vulnerabilities likely to be exploited as part of a ransomware attack, to help security practitioners prioritize remediation.

THE WHO: BREAKING DOWN THE RANSOMWARE ECOSYSTEM

The ransomware ecosystem is made up of three distinct groups of criminals

Initial Access Brokers

IABs are a specialized group of cybercriminals responsible for gaining access to organizations through a variety of means. This category includes individuals and groups dedicated to this craft. Instead of directly using this access, IABs maintain persistence within the networks of victim organizations and sell it to other individuals or groups within the cybercrime ecosystem. Their fees are very affordable, as they vary between the types of organizations they've compromised and the type of access. For instance, researchers at Digital Shadows analyzed over 500 listings by IABs in 2020 and found the price varied widely, ranging on average from $303 for control panel access to as much as $9,874 for Remote Desktop Protocol (RDP) access.

For ransomware affiliates, IABs provide an invaluable service, the cost of which can easily be recouped with ransom payments from victims. Affiliates leverage IABs to help expedite their efforts to infect organizations.

For IABs, the emergence of RaaS has propelled their services to new heights. A recent report from Group-IB showed the market for IABs skyrocketed from $1.6 million over a one-year period between 2018 and 2019 to $7.1 million over a one year period between 2020 and 2021. These figures are significantly lower when compared to the millions being earned by affiliates and ransomware groups, but this is by design: by selling access without actually deploying the ransomware, IABs take on less risk.

While IABs are typically independent players, researchers at Google identified an IAB called EXOTIC LILY that worked closely with the Conti ransomware group. This type of relationship eliminates the need for a middle-person, such as an affiliate, allowing an IAB to capture the greater profit sharing afforded to most affiliates. For IABs, there is an additional risk involved with the strategy of partnering with ransomware groups directly, as it could put them directly in the crosshairs of government or law enforcement agencies, but with higher stakes come greater returns.

Affiliates

If ransomware is a vehicle, then affiliates are the drivers responsible for propelling ransomware attacks forward. This type of partnership is one of the key elements that has helped ransomware flourish over the last four years. The success of most ransomware groups is largely a byproduct of the affiliate programs they've put in place. These affiliate programs are no different from those of legitimate businesses. Just as affiliates bring companies leads, ransomware affiliates find and infect victims with ransomware and bring them to ransomware groups to "close the deal" – negotiate, so to speak.

Affiliates compromise organizations by purchasing access through IABs as well as using common attack vectors such as spearphishing (with malware), brute forcing RDP systems, exploiting unpatched or zero-day vulnerabilities and purchasing stolen credentials from the dark web.

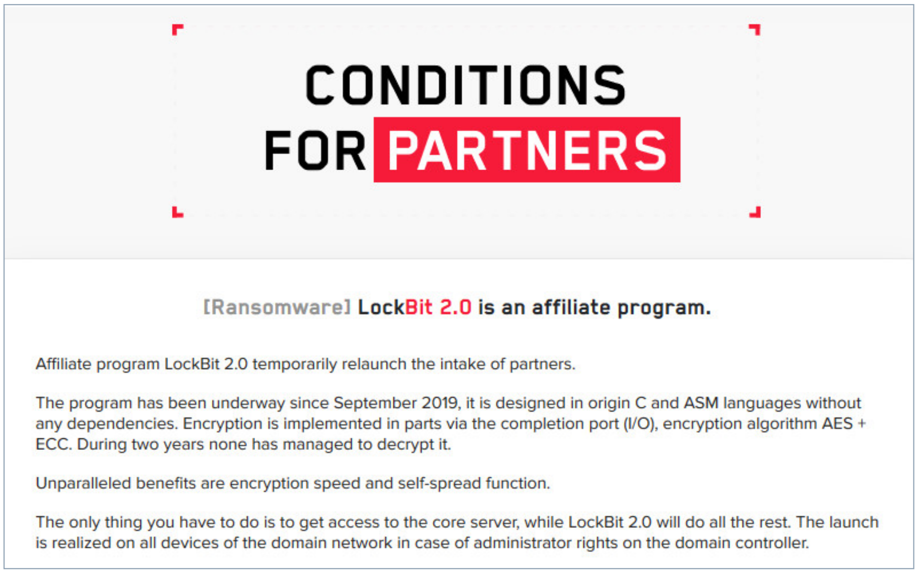
When a cybercriminal becomes an affiliate for certain ransomware groups, they are often given a playbook of instructions on how they will play their part. These playbooks also include a variety of recommendations on how to breach organizations.

RaaS offers an added benefit for affiliates, enabling them to operate independently of any one ransomware group, opening up the opportunity for them to work with multiple groups concurrently. The autonomy provides stability for affiliates: if one ransomware group disappears into the sunset or is dismantled through law enforcement action, there are others to take its place.

Ransomware Groups

Ransomware groups consist of various members responsible for developing and testing the ransomware itself, creating and hosting leak websites on the dark web and managing the negotiation process with each victim, as well as other tasks including reverse engineering, administrative work and even human resources or recruitment. Ransomware groups get the most notoriety and attention for attacks because RaaS is the "product" being marketed and sold in this equation.

Image Source: BleepingComputer



CONDITIONS
FOR PARTNERS

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Ransomware groups operate like businesses

Modern ransomware groups operate like traditional businesses. Because they partner with others in the ransomware ecosystem, they also market themselves like businesses, vying for the attention of affiliates with bold claims like fastest encryption speeds and self-spreading functionality.

Affiliates are the key to a ransomware group's success

For a ransomware group to succeed, they need to recruit affiliates to conduct attacks and provide a steady stream of "customers" (victims). So it's no surprise that ransomware groups are also very generous when courting affiliates. The affiliates they partner with earn the bulk of the ransom demand, taking a cut that ranges between 70%-80% of the total ransom. Some groups have become more aggressive with their affiliate offers, such as the ALPHV (a.k.a BlackCat) ransomware group offering a 90% cut to affiliates. When you consider how many ransomware groups are operating today, it makes sense that groups need to be aggressive in order to recruit affiliates.

What about all of the ransomware groups in the ecosystem?

In 2021, the FBI said it was tracking over 100 active ransomware groups. Ransomware groups like REvil, DarkSide and BlackMatter became more well known recently after notable supply chain attacks against Managed Service Providers (MSPs) and high value targets in critical infrastructure and food processing. More recently, groups like Conti, LockBit.2.0, Hive and ALPHV/BlackCat have risen through the ranks to fill the void left behind as ransomware groups disappeared or were taken down through law enforcement action. This is part of the lifecycle of ransomware groups. New and emerging groups will capture the lion's share of attention from affiliates seeking new partnerships, and, ultimately, from government and law enforcement agencies. Knowing about these groups provides us with some insight into their activities, such as the industries or geographical regions they target. However, the ransomware ecosystem thrives in the numbers game, where the emphasis is more about quantity over quality.

Ultimately, the groups themselves are ephemeral. We have seen multiple ransomware groups disappear over the years, either of their own accord or as a result of government and law enforcement action. We also hear numerous reports that newer groups include members of past ransomware groups. For instance, REvil was the successor to the infamous GandCrab ransomware outfit, while Conti is considered the successor to Ryuk. The famous phrase of the Ironborn in the Game of Thrones saga is applicable to today's ransomware groups: "What is dead may never die, but rises again, harder and stronger."

Because of the impermanence of these ransomware groups, diving deep into some of these groups here would be a moot point, as the references may easily be outdated a year from now. However, the one thing that's not impermanent is the vital role IABs and affiliates play in ransomware attacks. For instance, when the BlackMatter ransomware group shut down, its affiliates pivoted their victims to LockBit 2.0. Ultimately, we believe that more attention should be given to affiliates and IABs in the ecosystem at large.

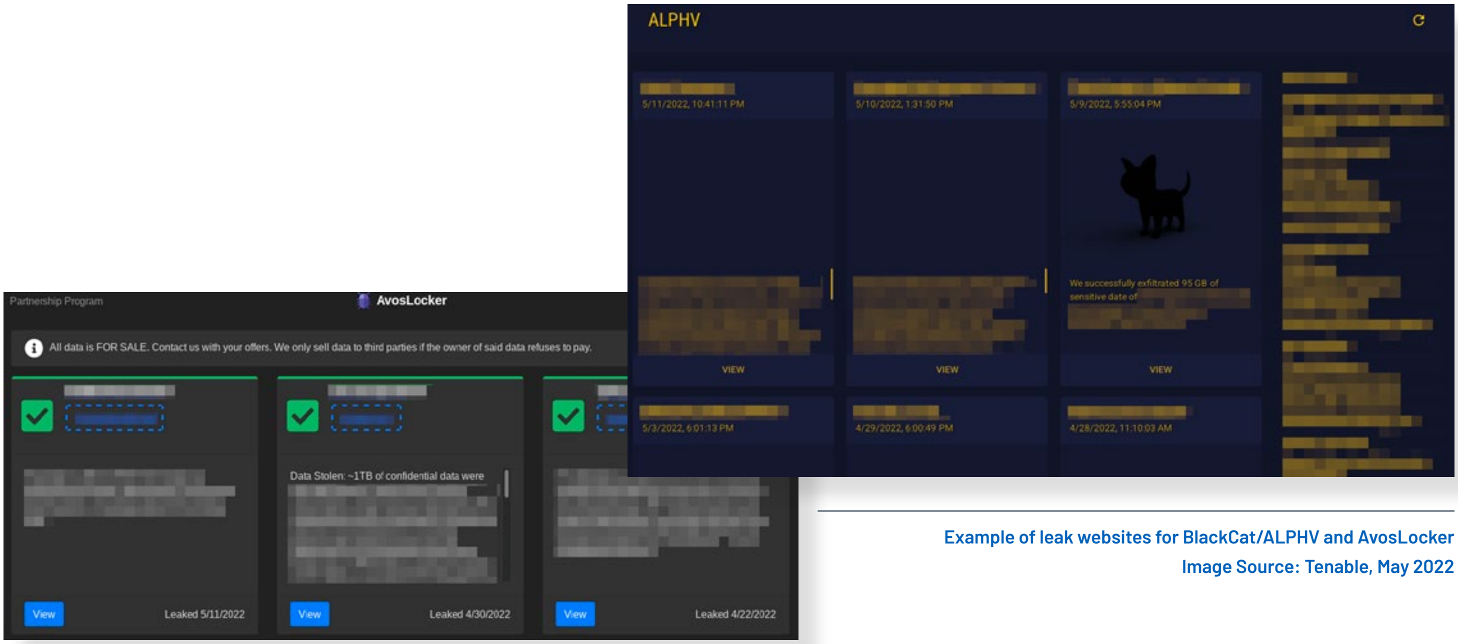
THE WHAT: RANSOMWARE GROUPS THRIVE THROUGH EXTORTION TACTICS

Now that we know who the players are in the ransomware ecosystem, the natural question is: What has enabled ransomware to surge and become the greatest threat to organizations today? It's the extortion factor.

Traditionally, ransomware attacks focused on encrypting files within a network to serve as the incentive for organizations to pay up. This method of extortion was very successful. However, as organizations began to rely on restoring ransomed files from backups, ransomware groups needed another mechanism to extort their victims. This is where double extortion emerged, becoming the catalyst for the extreme profits being earned by ransomware groups.

It's not just about stealing files; it's about threatening to publish them

As outlined earlier in this report, the double extortion tactic has proven itself to be a jackpot for ransomware groups. Yet, it's not just about exfiltrating files from a victim's network. Possessing these files is just the beginning. What makes double extortion so sinister is that the ransomware groups use these stolen files as a lure, teasing organizations by publishing samples on their personal leak websites hosted on the dark web and threatening to publish the remainder unless the ransom is paid.



ALPHV

5/11/2022, 10:41:11 PM

VIEW

5/10/2022, 1:31:50 PM

VIEW

5/9/2022, 5:55:04 PM

We successfully exfiltrated 95 GB of sensitive date of

VIEW

5/3/2022, 6:01:13 PM

4/29/2022, 6:00:49 PM

4/28/2022, 11:10:03 AM

Partnership Program

AvosLocker

All data is FOR SALE. Contact us with your offers. We only sell data to third parties if the owner of said data refuses to pay.

View Leaked 5/11/2022

Data Stolen: ~1TB of confidential data were

View Leaked 4/30/2022

View Leaked 4/22/2022

Example of leak websites for BlackCat/ALPHV and AvosLocker
Image Source: Tenable, May 2022

The threat of exposing a company's private files has ripple effects, as information on an organization's customers could also be at stake, providing additional pressure to pay the ransom. Even if an organization is able to recover operationally from the ransomware attack, it may still decide to pay the ransom, as JBS did in June 2021 when it paid $11 million to the REvil ransomware group:

> *"At the time of payment, the vast majority of the company's facilities were operational. In consultation with internal IT professionals and third-party cybersecurity experts, the company made the decision to mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated."*
>
> — JBS Media Statement

Under pressure: Expanding the types of extortion tactics gives added leverage

Double extortion is the linchpin for ransomware's current success. However, it's now become a tactic that is nearly three years old. As ransomware groups found their footing, they also added new extortion techniques to their repertoire as a way to place additional pressure on victim organizations. Some have called these tactics "triple extortion" or "quadruple extortion," though, whatever you choose to call it, these tactics remain part of the same extortion tree.

Extortion Tactic	Why it works
Using Distributed Denial of Service (DDoS) attacks	By taking down a company's website using DDoS, the victims are impacted in two ways: first, they're unable to provide online customers with access to their goods and services; and, second, they're also unable to provide customers with regular updates about the status of the incident, leading to additional stress on customer support and concerns on the part of customers.
Contacting customers of ransomware victim	By contacting the customers of a victim organization, the ransomware groups threaten to leak files associated with these customers, which ensures that the customers will contact the victim organization to place added pressure on them to pay the ransom.
Contacting employees of victims	Similar to contacting customers, by contacting employees of a victim organization, the ransomware groups use fear tactics to convince employees to place pressure on management to pay the ransom demand.
Warning victims not to involve professional negotiators and/or law enforcement	By intimidating the victim from contacting a professional negotiator or involving law enforcement in the negotiations, they're able to place additional pressure on victim organizations to negotiate directly with the groups, ensuring the desired outcome of a ransom payment.
Threatening to auction stolen data if ransom demand is not paid	By threatening to auction off the stolen data to a third party, the ransomware groups hope to place additional pressure on victim organizations to pay the ransom demand or risk having their stolen data given to another cybercriminal gang.
Threatening to use disk-wiping functionality on all affected systems	By threatening to use a disk wiper, which would render encrypted systems totally unusable and unrecoverable, ransomware groups aim to force the victims to pay the ransom demand.

While the above extortion tactics aren't as widely adopted as the tried and true method of threatening to publish stolen files on leak websites, they do place added pressure on victim organizations to pay.

THE HOW: COMMON VECTORS FOR RANSOMWARE ATTACKS

After detailing who the players are within the ransomware ecosystem and what has enabled ransomware attacks to surge, the final question left to answer is: How do IABs, affiliates and ransomware groups get into victim networks in order to distribute ransomware? There are a variety of tactics, techniques and procedures used – both common and unorthodox.

Ransomware groups provide affiliates with a playbook

We know about the existence of ransomware playbooks because in 2021 a disgruntled affiliate for Conti, a prolific ransomware group that emerged in 2020 and has made over $180 million in profits, leaked the group's affiliate playbook. In 2022, a member of Conti published a cache of private conversations between the group's members, which came to be called ContiLeaks. These leaks revealed a lot about the business element of current RaaS groups like Conti and help us better understand the inner workings that underpin the ransomware ecosystem.

However, affiliates aren't beholden to the playbooks provided, as they're free to operate using their own methods, including purchasing access via IABs or procuring exploits from public source code repositories.

Finding the path of least resistance

For ransomware affiliates, the way into an organization is largely driven by the approach of the path of least resistance. There are several common attack vectors used to breach an organization's defenses.

Spearphishing

The most common method for targeting organizations is through spearphishing, whereby attackers send crafted emails to victims that include malicious attachments or links to external websites hosting malware. The malware used in these attacks is not the ransomware itself, but rather a first-stage downloader, a trojan designed to download secondary and tertiary malware components. These additional malware components will ultimately lead to a ransomware payload. Some of the more popular downloaders that have contributed to ransomware attacks over the years include the vaunted Emotet, Trickbot and Qakbot trojans, as well as BazarLoader.

Remote Desktop Protocol

RDP is another popular avenue ransomware affiliates will use to target organizations. Because RDP is publicly accessible, attackers can use scripts to attempt to brute force their way into these systems, targeting weak passwords by using a combination of known default passwords and dictionary attacks. To underscore how valuable of an attack vector RDP is, some within the industry jokingly refer to it as the Ransomware Deployment Protocol.

Exploitation of vulnerabilities

Software vulnerabilities play a key role in facilitating ransomware attacks through several avenues. These include vulnerabilities used as part of malicious documents, vulnerabilities found in perimeter devices like Secure Socket Layer Virtual Private Networks (VPNs), as well as a plethora of flaws designed to elevate privileges once inside an organization's network.

For instance, ProxyLogon and ProxyShell, a collection of flaws in Microsoft Exchange Server that we crowned as the most targeted vulnerabilities as part of our 2021 Threat Landscape Retrospective report, have been leveraged by several ransomware groups throughout the last year.

As part of the leak of Conti's affiliate playbook, we know that affiliates were instructed to use vulnerabilities like PrintNightmare and ZeroLogon to elevate privileges. We highlighted over 30 vulnerabilities leveraged by Conti and its affiliates and it is clear that ransomware groups and affiliates are waiting on the sidelines in anticipation of the next big vulnerability to incorporate into their playbooks.

While ransomware groups covet zero-day vulnerabilities, the majority of ransomware attacks rely on leveraging unpatched, legacy vulnerabilities across a wide spectrum of software solutions.

We've put together a list of vulnerabilities associated with ransomware attacks in the Appendix section of this report that includes vulnerabilities highlighted over several years as well as cross-referenced from a list of flaws created by security researchers Allan Liska and another under the pseudonym "pancake3lullz" to help identify common vulnerabilities used for initial access.

We've put together a list of vulnerabilities associated with ransomware attacks in the Appendix section of this report that includes vulnerabilities highlighted over several years as well as cross-referenced from a list of flaws created by security researchers Allan Liska and another under the pseudonym "pancake3lullz" to help identify common vulnerabilities used for initial access.

Purchasing access from IABs

As discussed earlier, IABs provide ransomware affiliates a cost effective and time saving way to gain entry into an organization that has already been compromised. IABs have already done the reconnaissance and additional legwork by utilizing some of the vectors identified above, from sending spearphishing emails to exploiting vulnerabilities and brute forcing weak RDP systems. These efforts make the IABs role in the ransomware ecosystem invaluable.

Third-party compromises

Third parties provide an additional attack vector for ransomware attacks. In the case of the Cl0p ransomware group, they leveraged multiple vulnerabilities in the Accellion File Transfer Appliance, an application that gives organizations a way to transfer files, to steal data from at least 50 organizations. In July 2021, a REvil ransomware affiliate exploited multiple zero-day vulnerabilities in Kaseya's Virtual System Administrator (VSA) to ransom companies that partner with MSPs for remote administration of their systems.

Targeting remote monitoring and management software like Kaseya VSA is not common, but it is certainly not new. In the past, other ransomware groups like GandCrab and Zeppelin targeted flaws in these products and the MSPs that use them.

Recruiting insiders within companies and governments

Though not as prominently discussed, ransomware groups have made explicit offers to members of organizations and government agencies to help facilitate ransomware attacks. In these instances, the insiders themselves are another type of affiliate. For instance, the LockBit 2.0 ransomware group offered "millions of dollars" to insiders that would provide credentials for corporate email accounts, RDPs and VPNs or were willing to self-infect their corporate devices with malware. More recently, in May, the Conti ransomware group claimed to have insiders within the Costa Rican government assisting in their attacks against the country.

Active directory plays pivotal role in ransomware attacks

Initial access is how ransomware groups and affiliates gain access to an organization's network. Once inside, they often set their sights on Active Directory, as gaining domain privileges provides attackers the necessary capabilities to distribute their ransomware payloads across the entire network. This includes the use of critical vulnerabilities like Zerologon and PetitPotam. For instance, researchers at the DFIR Report delved into two cases where threat actors were able to launch the Ryuk ransomware across an entire domain within five hours and two hours, respectively, from the initial phishing email, leveraging Zerologon along the way.

Besides vulnerabilities, ransomware attackers will also utilize popular tools in their pursuit of domain privileges, including AdFind, Bloodhound, Kerberoasting and NTDS dumping.

Ransomware Attacks Will Persist: Here's How to Defend Against Them

When you take into consideration how profitable the ransomware ecosystem is, there will always be an incentive for the players to persist and amplify their activities. While there is no panacea for ransomware attacks, we know many of the most common ways ransomware groups and affiliates target organizations. Here are some of the steps organizations can take to mount the best defense against ransomware attacks.

Guidance	Why this helps
Use multifactor authentication for all accounts within your organization	Ransomware groups purchase access to organizations through IABs that provide credentials or exploit vulnerabilities that reveal login credentials. By adding multifactor authentication as a requirement, it adds another extra layer for ransomware attackers to have to overcome. This can be further strengthened through adaptive multifactor authentication, whereby several signals, including user location, are used to identify suspicious login attempts.
Require the use of strong passwords for accounts	Reliance upon weak or default passwords makes it easier for ransomware groups to gain access to accounts. Make it more difficult for attackers to brute force their way in by ensuring password requirements include lengthy and non-dictionary words as well as flagging passwords that have already been exposed as part of a data breach.
Continuously audit permissions for user accounts within your organization	Once inside an organization, ransomware groups and affiliates will try to create new accounts with elevated permissions or abuse existing accounts with elevated permissions, even accounts linked to employees no longer with your organization. This is why it's important to audit existing and newly created user accounts to ensure no misconfigurations are present and the principle of least privilege is adopted in your organization.
Identify and patch vulnerable assets in your network in a timely fashion	We know ransomware groups are adept at leveraging unpatched, legacy vulnerabilities, so it is important for organizations to identify vulnerable assets within their networks and apply available patches. The sooner the better as the window of exploitation for attackers is wide.
Review and harden Remote Desktop Protocol (RDP)	Leaving RDP open to the internet is the perfect scenario for ransomware groups. If you don't require it, disable it. If you do need it, then make sure the strong password requirement is in place for RDP.
Strengthen Active Directory security by addressing misconfigurations and detecting common AD attack paths	Once inside an organization, ransomware groups and affiliates will often look to take advantage of the misconfigurations within an organization's Active Directory security posture. They will also leverage common attack paths to test the waters, so it is vital that your Active Directory environment is being monitored and known attack paths are addressed.

Establish and regularly perform scheduled updates for encrypted, offline backups	Ransomware succeeds through double extortion attacks that include the encryption of files within an organization's network. This process can lead to unplanned downtime and may factor into an organization's decision in paying the ransom demand. Ransomware groups aren't afraid to target backups, so it is important to establish a regular practice of storing encrypted backups offline.
Use appropriate software (antivirus, anti-malware) to identify malware on your network	Because spearphishing with malicious attachments or links to malware often lead to ransomware infections, it is important to use solutions like antivirus or anti-malware to help detect against threats like downloader trojans.
Implement security awareness training to educate your employees about common attack vectors	Social engineering attacks, including spearphishing through email or on social networks is another way cybercriminals get malware onto systems within your network. By providing user awareness training, your employees and staff can receive guidance on how to identify common attack vectors used by cybercriminals which will play an important role in protecting your networks.
Plan for an attack by conducting tabletop exercises	It's often not a question of if but when an attack will occur. This is why it's imperative that your organization runs through an example scenario using tabletop exercises, which can be used to help prepare for a real-world attack. CISA provides its own CISA Tabletop Exercise Packages (CTEP) that can help guide this process.

The ransomware ecosystem remains vast and constantly in flux as ransomware groups come and go and affiliates move toward supporting other groups. In spite of the turnover, affiliates and IABs remain prominent fixtures in this space. Ultimately, the ransomware ecosystem's success and survival are made possible through the cooperation of all of these disparate parts.

Organizations are not entirely helpless. Law enforcement and government actions have provided a level of deterrence. For instance, the response by the United States to the Colonial Pipeline and JBS attacks put added pressure on several ransomware groups to turn their efforts away from such industries. While that may not deter all ransomware groups, it certainly has led to several groups advising potential affiliates that certain industries are off-limits.

With RaaS and double extortion, Pandora's box has been opened, and attackers show no sign of slowing down. So long as the ransomware ecosystem continues to thrive, so, too, will the attacks against organizations and governments. It's imperative that organizations and government entities prepare themselves in advance so they are in the best position possible to defend against and respond to ransomware attacks.

Appendix of Vulnerabilities Exploited by Ransomware Affiliates and Groups

CVE	Description	CVSS Score
CVE-2017-0199	Microsoft Office/WordPad Remote Code Execution Vulnerability	7.8
CVE-2017-11882	Microsoft Office Remote Code Execution Vulnerability	7.8
CVE-2018-13374	Fortinet FortiOS Improper Access Control Vulnerability	8.8
CVE-2018-13379	Fortinet FortiOS Path Traversal/Arbitrary File Read Vulnerability	9.8
CVE-2018-8120	Microsoft Win32k Elevation of Privilege Vulnerability	7
CVE-2018-8174	Microsoft Windows Visual Basic Script Engine	7.5
CVE-2018-8440	Microsoft Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	7.8
CVE-2018-8453	Microsoft Win32k Elevation of Privilege Vulnerability	7
CVE-2019-0604	Microsoft SharePoint Improper Input Validation Vulnerability	9.8
CVE-2019-0708	Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability ("BlueKeep")	9.8
CVE-2019-1108	Microsoft Windows Remote Desktop Protocol Client Information Disclosure Vulnerability	6.5
CVE-2019-11510	Pulse Secure Arbitrary File Read Vulnerability	10
CVE-2019-11539	Pulse Secure Command Injection Vulnerability	7.2
CVE-2019-11634	Citrix Workspace App and Receiver Incorrect Access Control Vulnerability	9.8
CVE-2019-1224	Microsoft Windows Remote Desktop Protocol Server Information Disclosure Vulnerability	7.5
CVE-2019-1579	Palo Alto Networks PAN-OS Remote Code Execution Vulnerability	8.1
CVE-2019-18935	Telerik UI .NET Deserialization Vulnerability	9.8
CVE-2019-19781	Citrix Application Delivery Controller (ADC) and Gateway Directory Traversal Vulnerability	9.8
CVE-2019-2725	Oracle WebLogic Server Deserialization Vulnerability	9.8
CVE-2019-3396	Atlassian Confluence Widget Connector Server-SIde Template Injection Vulnerability	9.8
CVE-2019-5591	Fortinet FortiOS Information Disclosure Vulnerability	6.5
CVE-2019-7481	SonicWall SMA100 Pre-Authentication SQL Injection Vulnerability	7.5
CVE-2020-0609	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability	9.8
CVE-2020-0610	Microsoft Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution	9.8
CVE-2020-0688	Microsoft Exchange Validation Key Remote Code Execution Vulnerability	8.8
CVE-2020-0787	Microsoft Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability	7.8
CVE-2020-0796	Windows SMBv3 Client/Server Remote Code Execution Vulnerability ("SMBGhost")	10

CVE-2020-12271	Sophos XG Firewall SQL Injection Vulnerability	9.8
CVE-2020-12812	Fortinet FortiOS Improper Authentication Vulnerability	9.8
CVE-2020-1472	Microsoft Netlogon Elevation of Privilege Vulnerability ("Zerologon")	10
CVE-2020-16896	Microsoft Windows Remote Desktop Protocol Information Disclosure Vulnerability	7.5
CVE-2020-2021	Palo Alto Networks PAN-OS Authentication Bypass in SAML Authentication Vulnerability	10
CVE-2020-36198	QNAP Malware Remover Command Injection Vulnerability	6.7
CVE-2020-5135	SonicWall SonicOS Denial of Service Vulnerability	9.4
CVE-2020-5902	F5 BIG-IP Traffic Management User Interface (TMUI) Remote Code Execution Vulnerability	10
CVE-2020-8195	Citrix ADC and Gateway Improper Input Validation Vulnerability	6.5
CVE-2020-8196	Citrix ADC and Gateway Improper Access Control Vulnerability	4.3
CVE-2020-8243	Pulse Connect Secure Code Injection Vulnerability	7.2
CVE-2020-8260	Pulse Connect Secure Unrestricted File Upload Vulnerability	7.2
CVE-2021-1675	Microsoft Windows Print Spooler Remote Code Execution Vulnerability ("PrintNightmare")	8.8
CVE-2021-20016	SonicWall SMA100 SQL Injection Vulnerability	9.8
CVE-2021-20028	SonicWall Secure Remote Access (SRA) SQL Injection Vulnerability	9.8
CVE-2021-20655	FileZen OS Command Injection Vulnerability	7.2
CVE-2021-21972	VMware vSphere Client Remote Code Execution Vulnerability	9.8
CVE-2021-21985	VMware vSphere Client Remote Code Execution Vulnerability	9.8
CVE-2021-22005	VMware vCenter Server Remote Code Execution Vulnerability	9.8
CVE-2021-22893	Pulse Connect Secure Improper Authentication Vulnerability	10
CVE-2021-22941	Citrix ShareFile Improper Access Control Vulnerability	9.8
CVE-2021-22986	F5 BIG-IP iControl REST Remote Command Execution Vulnerability	9.8
CVE-2021-26084	Atlassian Confluence Server Webwork OGNL Injection Vulnerability	9.8
CVE-2021-26085	Atlassian Confluence Server Arbitrary File Read Vulnerability	5.3
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability ("ProxyLogon")	9.8
CVE-2021-27101	Accellion File Transfer Application (FTA) SQL Injection Vulnerability	9.8
CVE-2021-27102	Accellion File Transfer Application (FTA) OS Command Injection Vulnerability	7.8
CVE-2021-27103	Accellion File Transfer Application (FTA) Server-Side Request Forgery (SSRF) Vullnerability	9.8
CVE-2021-27104	Accellion File Transfer Application (FTA) OS Command Injection Vullnerability	9.8
CVE-2021-28799	QNAP NAS Improper Authorization Vulnerability	9.8
CVE-2021-30116	Kaseya Virtual System Administrator (VSA) Credentials Leak and Business Logic Vulnerability	9.8

CVE-2021-30119	Kaseya VSA Cross-Site Scripting (XSS) Vulnerability	5.4
CVE-2021-30120	Kaseya VSA Two-Factor Authentication Bypass Vulnerability	7.5
CVE-2021-31166	Microsoft Windows HTTP Protocol Stack Remote Code Execution Vulnerability	9.8
CVE-2021-31206	Microsoft Exchange Server Remote Code Execution Vulnerability ("ProxyShell")	8
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability ("ProxyShell")	7.2
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability ("ProxyShell")	9.8
CVE-2021-34523	Microsoft Exchange Server Elevation of Privilege Vulnerability ("ProxyShell")	9.8
CVE-2021-34527	Microsoft Windows Print Spooler Remote Code Execution Vulnerability ("PrintNightmare")	8.8
CVE-2021-34730	Cisco Small Business RV Routers Improper Input Validation Vulnerability	9.8
CVE-2021-36942	Microsoft Windows LSA Spoofing Vulnerability ("PetitPotam")	5.3
CVE-2021-38646	Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability	7.8
CVE-2021-38647	Microsoft Azure Open Management Infrastructure Remote Code Execution Vulnerability	9.8
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	8.8
CVE-2021-40449	Microsoft Win32k Use-After-Free Vulnerability	7.8
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	9.8
CVE-2021-41773	Apache HTTP Server Path Traversal Vulnerability	7.5
CVE-2021-42013	Apache HTTP Server Path Traversal Vulnerability	9.8
CVE-2021-42258	BQE BillQuick Web Suite SQL Injection Vulnerability	9.8
CVE-2022-26134	Atlassian Confluence and Data Center OGNL Injection Vulnerability	10
NO-CVE-ID	EntroLink PPX-Anylink Remote Code Execution Vulnerability	N/A

How Tenable Can Help

Tenable has released scan templates for Tenable.io, Tenable.sc and Nessus Professional which are pre-configured to allow quick scanning for the vulnerabilities discussed in this report. In addition, Tenable.io customers have a new dashboard and widgets in the widgets library and Tenable.sc users also have a new dashboard covering the Ransomware Ecosystem.

About the Tenable Security Response Team

Tenable Research seeks to step out in front of the curve of the vulnerability management cycle. Our Security Response Team tracks threat and vulnerability intelligence feeds to make sure our plugin teams can deliver coverage to our products as quickly as possible. The SRT also works to dig into technical details and author white papers, blogs and additional communications to ensure customers are fully informed of the risks. The SRT provides breakdowns for the latest vulnerabilities on the Tenable blog.

Tenable Research has released over 171,000 plugins and leads the industry on CVE coverage. The team is focused on diverse work that makes up the foundations of vulnerability management: writing plugins for vulnerability and asset detection; developing audit and compliance checks; improving VM automation.

About the Author

Satnam Narang is a Senior Staff Research Engineer with the Security Response Team.

Contributors

Claire Tills, Senior Research Engineer, Security Response
Scott Caveza, Senior Manager, Security Response

Tenable, Inc.
6100 Merriweather Drive 12th Floor
Columbia, MD 21044
North America
+1 (410) 872-0555

www.tenable.com

About Tenable

Tenable® is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at tenable.com.

tenable®