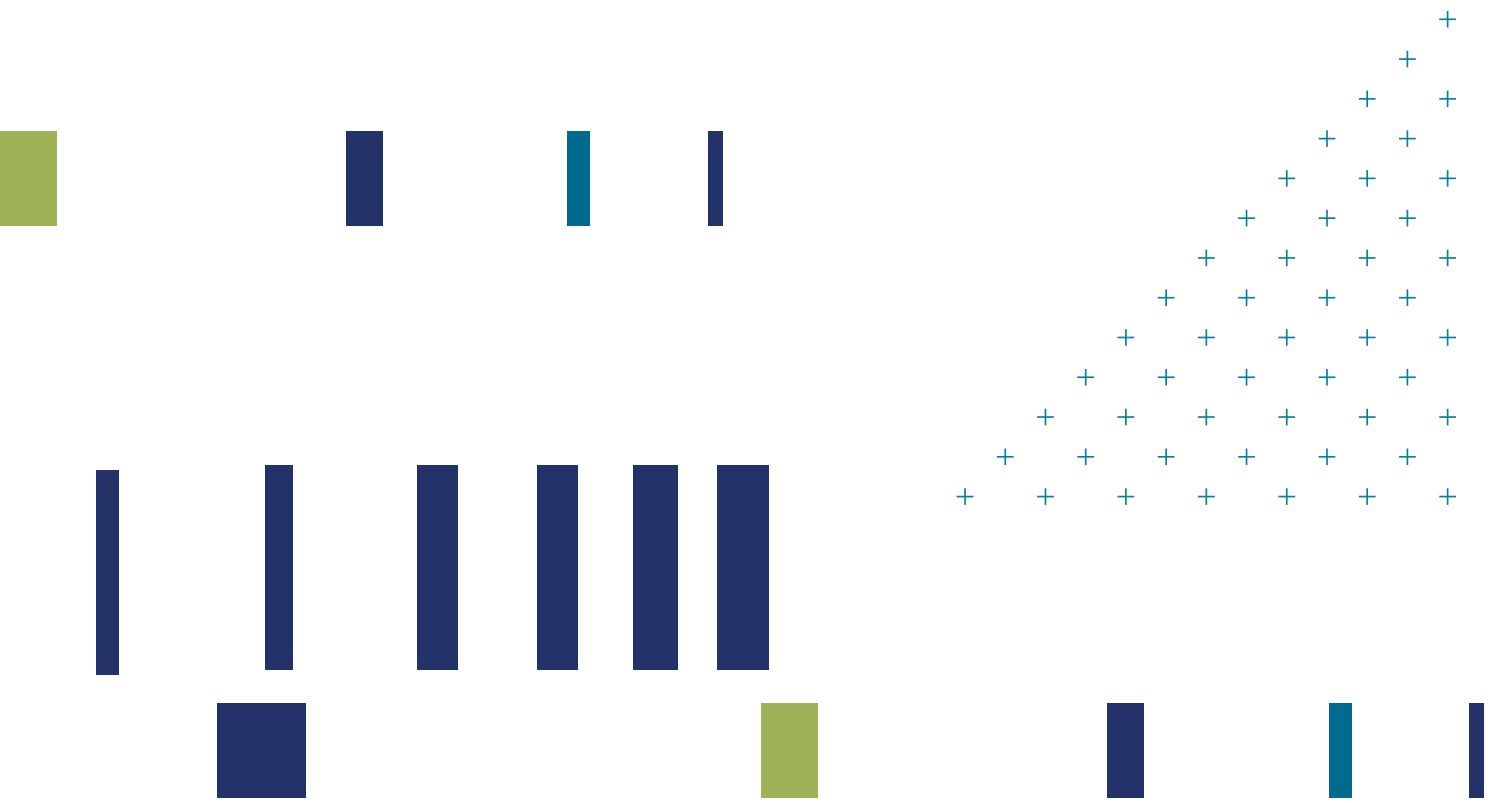
CONNECTWISE

CONNECTWISE EBOOK SERIES

2022 MSP Threat Report

CONTENTS



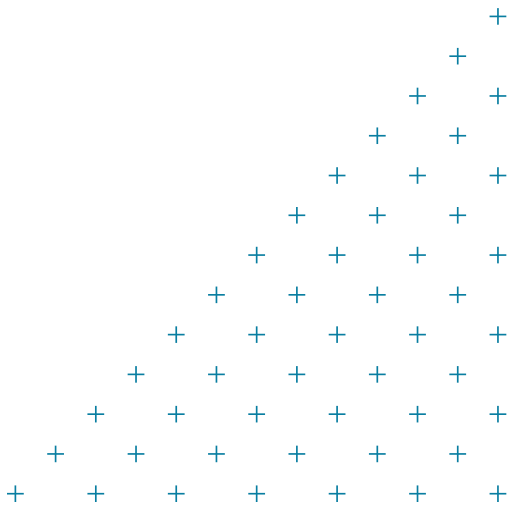
Introduction

In 2019 we discovered a shift of hacking activity focused on managed service providers (MSPs). It became clear that MSPs needed more business-specific information to protect their business and customers proactively, so ConnectWise created the annual MSP Threat Report.

For the past three years, we've compiled, analyzed, and discussed data with internal and external cybersecurity experts to report on the state of cybersecurity for MSPs. This includes making predictions and recommendations about evolving cyberthreats. So far, our predictions have proved true.

As predicted for 2021, ransomware attacks continued to become even more MSP-focused. It's no surprise because MSPs are a far more lucrative target than individual businesses due to the potential to ransom several companies at once. This report covers that and other significant cyberthreat events in 2021, emerging and continuing trends, and what the data tells us about the future of cybersecurity.

This report was created by the ConnectWise Cyber Research Unit (CRU)—a dedicated team of ConnectWise threat hunters that identifies new vulnerabilities, researches them, and shares what they find for all to see in the community. The CRU monitors ransom leak sites and malicious botnets for new threats, uses OSINT resources, and utilizes data from the ConnectWise SIEM powered by Perch to help create content and complete research.



Key Cybersecurity Events and Trends of 2021

Twenty-twenty-one was a tumultuous year that drastically altered the threat landscape in general and specifically for MSPs. A main theme of 2021 was the significant increase in the success of worldwide law enforcement activity, taking down various cybercrime groups and recovering money. As a result, some groups got spooked and dropped out. However, ransom activity continues to increase because there's just so much money in it and attacks on mid-tier entities draw less attention from government agencies. Small cybercrime groups still come and go, but the bigger groups are better organized and even more vicious, employing triple threat techniques: ransom, data leaks, and DDoS. In some cases, attackers even contact victims' clients and partners.

In the rest of this section, we'll review the timeline of key cybersecurity events in 2021. Then we'll break down what this all means for you as an MSP and offer recommendations on how to structure your business and behavior to tackle the upcoming challenges of 2022.

Q1: Governments Cooperate to Stop Hackers

Observations

1. Government agencies worldwide increase their efforts to take down major cybercrime groups, showing that everyone must do their part to protect the industry, from individuals to global law enforcement.
2. The average ransom increases, with some companies receiving demands for up to $50 million.

January

- Emotet is responsible for 75% of cybersecurity incidents reported by ConnectWise partners
- On January 27, 2021, a team of law enforcement agencies from around the world announced that they seized and took down the Emotet infrastructure and arrested an undisclosed number of operators as part of Operation LadyBird[1]
- On January 27, 2021, the US Justice Department announced the disruption of the Netwalker ransomware operation
- On January 30, 2021, the threat actors behind FonixCrypter Ransomware gave in to their conscience and voluntarily halted operations[1]

February

- On February 4, 2021, Ukraine's Cyber Police announced that, with the aid of law enforcement agencies in the US and Australia, they had shut down the world's largest phishing services and arrested the individual responsible for the uPanel phishing kit[1]
- The actors behind the Ziggy ransomware announced on February 7, 2021, via Telegram that they were shutting down, and they released all their decryption keys[1]
- ConnectWise incident response team notified the CRU, previously part of Perch, of an increase in Lockbit ransomware attacks using a three-year-old vulnerability (CVE-2018–13379) in Fortinet SSL VPN appliances for initial access[2]
- SonicWall releases patch for SMA 100 Series Version 10.x to address a critical 0-day vulnerability actively being exploited[3]

March

- CompuCom, a large MSP that provides remote support and other services for several well-known names such as Home Depot, Target, Citibank, and Wells Fargo, is compromised by DarkSide, costing them $10 million in cleanup costs, and sales down 17% in Q1 2021[4]
- Critical 0-day vulnerabilities in on-premises Microsoft Exchange servers collectively known as Proxylogon (CVE-2021–26855, CVE-2021–26857, CVE-2021–26858, and CVE-2021–27065), were publicly disclosed, leading to massive scanning and compromised servers. Threat actors initially deployed web shells and stole data in users' mailboxes, then followed up with coin miners and eventually ransomware.[5]
- REvil targets computer manufacturing company Acer with a ransom of $50 million[6]

Q2:
US Government Takes a Stand

Observations

1. The US government steps up its role in cybersecurity, including announcing sanctions, declaring cyberattacks an act of terrorism, and forming a new ransomware task force.
2. Large enterprises—Colonial Pipeline and JBS Foods—are forced to shut down partially or fully after suffering ransomware attacks, resulting in substantial monetary losses and other issues.

April

- CL0P began sending emails directly to customers and partners of their victims using email addresses extracted from stolen data and warning them that their data would be leaked if the targeted company did not pay the ransom[7]
- Microsoft patches four more RCE vulnerabilities in Microsoft Exchange[8]
- The US formally blames Russia for the SolarWinds Orion attack and interference with the 2020 presidential election and reacts by issuing a wide range of sanctions[9]
- Pulse Secure released a new CVE (CVE-2021–22893) for an unauthenticated remote code execution 0-day vulnerability for Pulse Connect Security actively being exploited by 12 malware families[10]
- Codecov's Bash Uploader script was compromised, allowing the threat actor to steal credentials for major tech companies such as IBM and HP[10]

- Sealed court orders were made public that disclose information that the FBI received a warrant to remotely access and delete web shells on Exchange servers compromised with ProxyLogon[11]

May

- US Justice Department forms a new Ransomware and Digital Extortion Task Force[12]
- Ransomware attack by DarkSide on Colonial Pipeline results in subsequent shutdown of a major oil pipeline in the US and gas shortage across the East coast. Colonial Pipeline pays ransom of $4.4 million.[13]
- In response to the Colonial Pipeline attack, US President Joe Biden issues an executive order dictating new guidelines and regulations for government contractors as well as companies that provide IT and OT services[13]
- DarkSide shuts down operations after receiving excess attention by US law enforcement after the Colonial Pipeline attack[13]
- Two popular cybercrime forums (XSS and Exploit) ban ransomware ads in response to the Colonial Pipeline attack[13]
- VMware released patches to remediate two vulnerabilities (CVE-2021–21985, CVE-2021–21986) that affect VMware vCenter Server and VMware Cloud Foundation. CVE-2021–21985 specifically has a CVSS score of 9.8 and is considered a critical vulnerability[14]
- JBS Foods, the world's largest provider of beef, chicken, and pork, closed facilities in several states and canceled shifts in others due to a ransomware attack by REvil[15]

June

- FBI now considers ransomware attacks as terrorism[16]
- 63.7 (over $2.6 million) of the 75 Bitcoin (over $3.1 million) paid to DarkSide affiliate in the Colonial Pipeline attack was recovered by the FBI[17]
- Windows releases first patch for a critical Windows Print Spooler RCE, dubbed PrintNightmare. The patch is insufficient to address the vulnerability[18]

Q3:
Large Enterprises Join Forces to Combat Ransomware

Observations

1. Large enterprises partner with the US federal government to create the Joint Cyber Defense Collaborative to combat ransomware.
2. REvil disappears then reappears with new victims posted; the group shares that its spokesperson "disappeared without a trace."

July

- Right before the July 4 holiday in the US, REvil launches a major Buffalo Jump attack targeting over 40 MSPs and over 1500 of their customers using a vulnerability in Kaseya VSA[19]
- Chinese government is blamed for the original attacks targeting Exchange servers using ProxyLogin by the threat actor group Hafnium[20]
- Several more printer-related vulnerabilities disclosed, Microsoft tries another patch to address PrintNightmare vulnerability[21]
- HiveNigthmare (a.k.a. SeriousSAM) vulnerability disclosed, which allows an unprivileged user to access the Windows SAM database and steal password hashes[22]
- REvil mysteriously disappears from the Dark Web[23]
- New Ransomware group, BlackMatter, begins advertising for new affiliate program. BlackMatter is believed to be the successor of DarkSide, which shut down operations after the Colonial Pipeline attack[24]

August

- Additional Exchange vulnerabilities disclosed at BlackHat and Defcon[25]
- US President Joe Biden signs a National Security Memorandum (NSM) on "Improving Cybersecurity for Critical Infrastructure Control Systems"[26]
- Information (including a PoC) is released regarding an attack method, dubbed PetitPotam, that could allow a remote attacker to perform a full domain takeover[27]
- CISA partners with Amazon, Microsoft, and Google to form the Joint Cyber Defense Collaborative to combat ransomware[28]
- Global IT consultancy firm, Accenture, hit with LockBit ransomware with a $50 million ransom[29]
- Critical RCE vulnerability disclosed for Confluence[30]

September

- Microsoft released a security advisory for a new RCE vulnerability (CVE-2021–40444) in MSHTML vulnerability[31]
- CISA releases information on Conti, frequently uses legitimate RMM software for Buffalo Jump-type attacks[32]
- VMware VCenter being actively targeted using CVE-2021-22005[33]
- US farmer cooperative, NEW Cooperative, attacked by BlackMatter ransomware with $5.9 million ransom[34]
- REvil returns, their sites come back online with new victims listed. New REvil spokesperson says original spokesperson, UNKWN, disappeared without a trace[35]

Q4: Microsoft Acknowledges Cyberattack Shift to TSPs

Observations

1. Late-year predictions say over 700 million ransom attacks will happen by the end of 2021.
2. At least two large players acknowledge the shift of bad actors targeting MSPs and other IT solution providers (ITPS) specifically.

October

- Microsoft releases a report on DEV-0343, an Iranian hacker group that conducted password spraying attacks against more than 250 Office 365[36]
- Microsoft's Digital Defense Report highlights the shift in nation-state threat actors to target IT solution providers (TSPs)[37]
- According to a report released by Microsoft, Nobelium, the alleged Russian state actor that apparently launched the SolarWinds Orion cyberattacks, has targeted at least 140 resellers and technology service providers since May 2021[38]

November

- A report released by UnCommonX, an MSSP that leans heavily on its own SaaS-based solutions, suggests nearly two in three midsize organizations have suffered a ransomware attack in the past 18 months, and 20 percent of them spent at least $250,000 to recover from it[39]
- SonicWall said in a report released in November that they

have logged nearly 500 million attempted ransomware attacks through September 2021 and predict over 700 million by the end of the year[40]

- REvil affiliate indicted for multiple ransomware attacks, including the July 2021 Kaseya attack[41]
- After a 10 month hiatus, a new version of Emotet emerges and begins spamming[42]
- The Secure Equipment Act of 2021 is signed into law which directs the FCC to prohibit sales of devices from Chinese state-backed suppliers such as Huawei, ZTE, Hytera, Hikvision and Dahua in the U.S.[43]
- Palo Alto releases a report of an attack campaign targeting ManageEngine ADSelfService Plus[44]

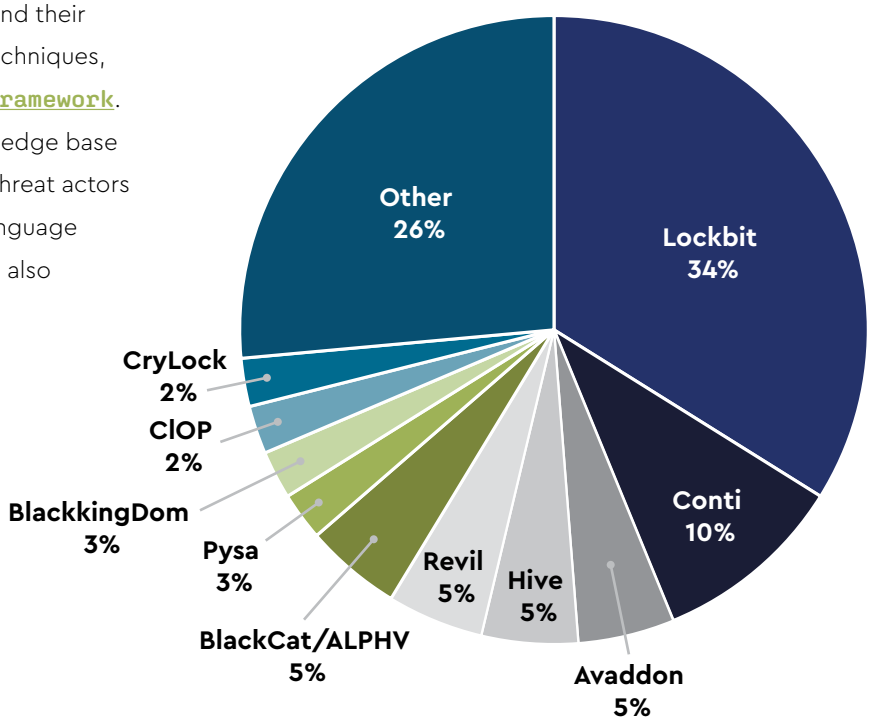
December

- A critical RCE vulnerability in Apache's Log4j library is discovered[45]. This vulnerability affects hundreds of thousands of applications and continues to be a major security issue. Several additional vulnerabilities in Log4j have been discovered since, though none as severe as the original[46,47]
- Kronos, an HR cloud-hosted software company, is targeted by a ransomware attack, disrupting payroll for customers for over a month[48]
- Darktrace releases a report suggesting attackers are targeting MSSPs and their backup servers[49]
- ConnectWise incident response team notified the CRU of an increase in ALPHV ransomware attacks targeting our partners.
- Inetum Group, a Global IT consulting firm with 27,000 employees across over countries, was targeted by a ransomware attack, believed to be ALPHV (aka BlackCat)[50]

2021 Top Threat Actor Profiles

Several ransomware groups now see MSPs are prime targets. The CRU has gathered information on the top 5 ransomware groups below that we observed targeting MSPs and their clients. We have mapped each groups' tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK® framework. MITRE's ATT&CK framework is a data driven knowledge base of the tactics and techniques currently in use by threat actors today. It is a handy tool that provides common language to describe how threat actors operate. MITRE has also defined common mitigation techniques that defenders scan use and mapped these mitigations to each ATT&CK technique and sub-technique. Below is a brief summary of each group along with a graphical overview of each groups' TTPs mapped to ATT&CK. We have expanded on this in the Appendix with a full listing of each groups TTPs with definitions and mappings to mitigation techniques.

Top 10 Ransomware Targeting MSPs – 2021



LockBit/LuckyDay/LockBit 2.0/ ABCD

- Ransomware-as-a-service provider that first appeared in September 2019, originally dubbed "ABCD"
- Known for their fast encryption, they claim to have the fastest encryption of any ransomware
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for 33% of all ransomware incidents we observed targeting MSPs and their customers in 2021

Conti

- Ransomware-as-a-service provider that first appeared in December 2019
- Typically distributed via TrickBot
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for 10% of all ransomware incidents we observed targeting MSPs and their customers in 2021

Avaddon

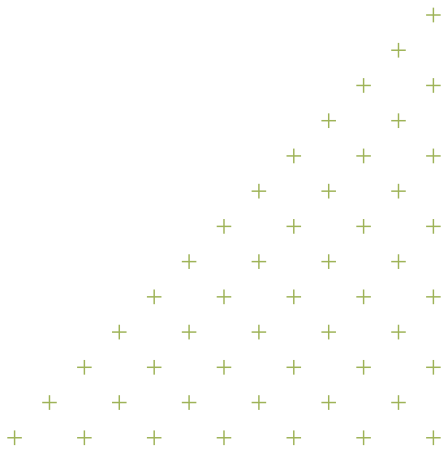
- Ransomware that first appeared in June 2020
- Does not harm systems with operating system language or keyboard layouts set to the specific languages typically used in the Commonwealth of Independent States (formerly the Soviet Union)
- Uses a triple extortion method of encrypting files, threatening to leak stolen data, and using DDoS attacks to coerce victims into paying
- Responsible for 5% of all ransomware incidents we observed targeting MSPs and their customers in 2021
- Avaddon shut down operations and released its decryption keys on June 11, 2021

Hive

- Ransomware-as-a-service that first appeared in June 2021
- Targets Windows, Linux, and ESXi
- Written in Golang
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for 5% of all ransomware incidents we observed targeting MSPs and their customers in 2021

REvil/Sodin/Sodinokibi

- Ransomware-as-a-service that first appeared in April 2019
- Highly configurable, successor to GandCrab
- Uses the double extortion method of encrypting files and threatening to leak stolen data
- Responsible for large scale ransomware attacks targeting over 40 MSPs and at least 1500 of their customers using Kaseya VSA in July 2021
- REvil servers went offline in October 2021, then in January 2022, the Russian Federal Security Service said they had dismantled REvil and charged several of its members after being provided information by the US



Top 5 Threat Actor Heat Map

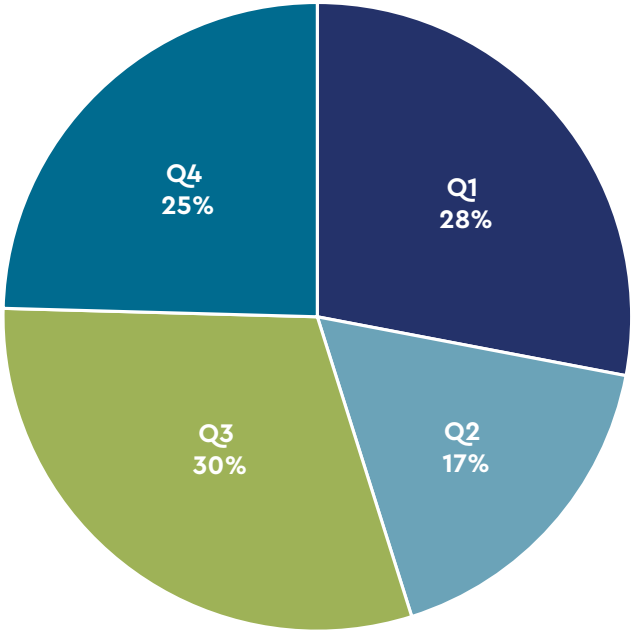
A few common techniques emerge when comparing TTPs used by the top five threat actors. The MITRE ATT&CK® framework includes a list of more than 370 techniques across 14 tactics. Ensuring controls and detection across all these techniques can be a daunting task. However, if you focus on the most-used tactics, MSPs can ask this question to prioritize their efforts: "What techniques do we realistically need to be prepared to defend against?"

We can see in the heat map above that phishing (T1566) and valid accounts (T1078) are the most-used techniques for initial access (TA0001), with phishing (T1566) being used by all five threat actors. While 0-days and exploiting public-facing application (T1190) are still major concerns, MSPs can significantly reduce their attack surface by implementing common mitigations such as email filters, user training, password hygiene, and MFA. We can also see that execution (TA0002) is often performed using tools and applications built into the operating system with PowerShell (T1059.001) and Windows Command shell (T1059.003) scripting being the most common techniques.

A SIEM can be a powerful tool for detecting these techniques, especially if you enable PowerShell script block logging. Execution control, script blocking, and code signing are all good mitigations for dealing with these techniques.

Notable Findings

Total Security Incidents By Quarter – 2021



Throughout 2021, the ConnectWise Cyber Research Unit, also known as the CRU, collected data regarding 500 cybersecurity incidents from our MSP partners and their clients. Of those 500 incidents, 40% were related to ransomware, 25% were directly related to Exchange vulnerabilities, and 10% were coin miners with some overlap. We saw the most incidents occur in Q1 and Q3.

A majority of the incidents in Q1 were directly related to the original release of the ProxyLogon vulnerability in Microsoft Exchange or Emotet infections, which quickly dropped off after the takedown of Emotet in January.

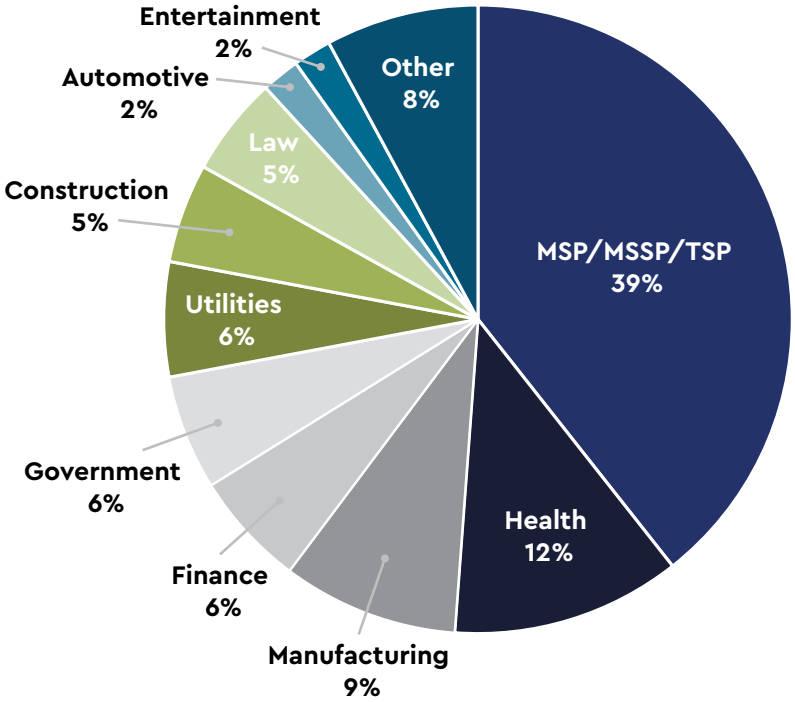
A trend we saw with ProxyLogon that continued when other significant vulnerabilities occurred, such as PrintNightmare or Log4Shell, was threat actors mass scanning for a recent vulnerability and then deploying coin miners. As time went on, the attacks became more sophisticated, and eventually, new ransomware variants appeared, specifically targeting vulnerable Exchange servers, such as DearCry and Black KingDom.

In Q3 we saw a significant increase in MSP partners with stolen credentials appearing on the Dark Web.

Ransomware Operators Are Focusing on MSPs

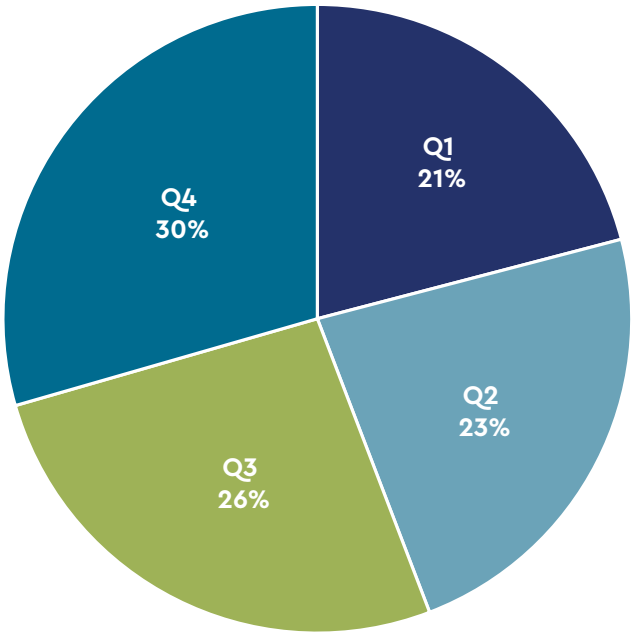
According to a report by Sonicwall in October 2021, ransomware surged by 148% in 2021 compared to 2020.

Top 10 Industries Targeted by Ransomware – 2021



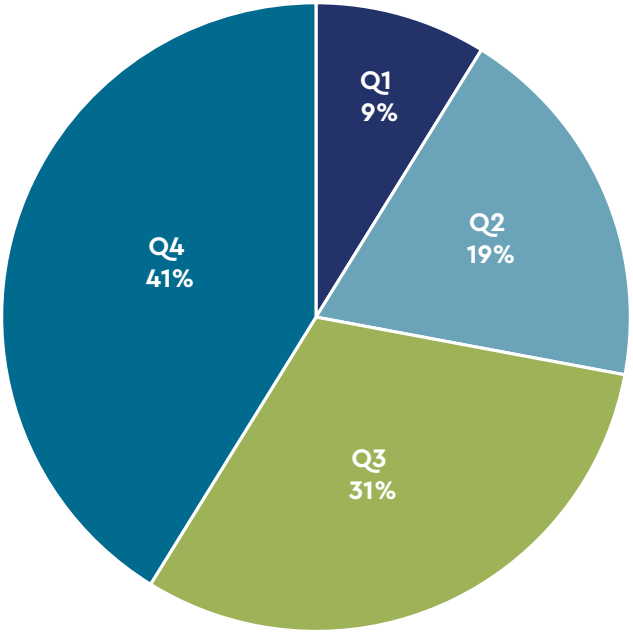
We saw a 10–15% increase in ransomware incidents by quarter, with 56% of all incidents occurring in the second half of 2021, according to the data the CRU collected from around 200 ransomware incidents in 2021 targeting MSPs and their clients.

Ransomware Incidents By Quarter – 2021



When we filter the data to only include MSPs, we can see a significant increase in ransomware incidents targeting MSPs in the second half of 2021, with 72% of all ransomware incidents directly targeting MSPs occurring in the second half of 2021. For the purposes of this report, we recorded the mass ransomware attacks that occurred during the July 2 Kaseya incident as a single incident. The data suggests that MSPs are in the spotlight more than ever. The massive ransomware attack in July that targeted at least 40 MSPs and over 1500 of those MSPs' clients right on the heels of the Colonial Pipeline attack put the spotlight on MSPs for threat actors, researchers, and government officials alike.

Ransomware Incidents Targeting MSPs By Quarter – 2021



Significant Events of 2021

Emotet takedown, then return

Emotet is one of the longest-lasting cybercrime services in existence. Their first banking Trojan was identified in 2014 and was one of the most heavily distributed malware families of 2020. It is typically distributed via malicious Word documents sent by email with language such as "Your invoice," "Payment Details," or possible shipping updates. Once infected, it attempts to connect to a Command and Control (C2) server for additional instructions. The Emotet botnet operated as a service that was rented out to other threat actors and used for deploying additional malware, frequently ending in ransomware.

On January 27, 2021, a team of law enforcement agencies from around the world announced that they seized and took down the Emotet infrastructure and arrested an undisclosed number of operators as part of Operation LadyBird. Hundreds of servers used by Emotet for its C2 were seized, with many active Emotet infections worldwide now connecting to sinkhole server domains. A sinkhole server domain is a domain name where the DNS servers have been configured to respond with false information. In this case, DNS requests for Emotet's C2 servers return IP addresses that belong to law enforcement, essentially crippling the malware and preventing any further infections. Law enforcement gained control of the Emotet botnet and pushed out a new module that made it uninstall itself on any infected machines on April 25, 2021.

There was no further sign of Emotet until November 15, 2021. That's when researchers worldwide began seeing a new version of Emotet being distributed. The initial sighting showed an Emotet DLL being downloaded by Trickbot. Now multiple reports have come in about new malicious emails with malicious Emotet attachments spoofing replies from stolen email chains, presumably originating from already infected hosts. The attachments observed so far have been Word *.DOCM, Excel *.XLSM, or Zip files. The newer version of Emotet is mostly the same as the older version; however, the new version now encrypts C2 traffic via HTTPS instead of relying on unencrypted HTTP.

Since November, it has been back to business as usual for Emotet with several malspam campaigns being launched in the past month that server Emotet. We were hopeful at the beginning of the year that Emotet was dead, but it seems like it will still be around for a while.

Colonial Pipeline ransomware attack and the resulting ransomware rollercoaster

On May 7, 2021, Colonial Pipeline, the largest oil pipeline in the US, was targeted by a ransomware attack from an affiliate of the ransomware as a service (RaaS) group known as DarkSide. The entire pipeline that carries gasoline, diesel, and jet fuel from Texas to the East Coast was shut down as a precaution, which resulted in fuel shortages and panic buying in the region. The pipeline was down for nearly six days, with operations spinning back up late in the day on May 12 and returning to full operation on May 15.

While this is perhaps one of the most public ransomware attacks, and Colonial Pipeline paid a $4.4 million ransom, it is not by any means the largest payout in recent history. Some reports from 2020 suggest payouts as large as $10 million and ransom demands as high as $30 million.

This year, we've seen major vulnerabilities (such as those mentioned above) being used to target tens of thousands of organizations around the world within a short time. And then there's the SolarWinds supply chain attack. We continued to see new information revealed throughout the year, such as an update in May from the SolarWinds CEO that the attack dates back to at least January 2019. The US suggested in January that Russian state actors were behind the attack. In response, President Biden imposed new sanctions against Russia in April. Meanwhile, Russia's foreign intelligence service made unsubstantiated claims that the US and UK were actually behind the hack.

The hit to critical infrastructure has spurred several official responses from the US government. In response to all the above, President Biden released an executive order on May 12 dictating new guidelines and regulations for government contractors as well as companies that provide IT and OT services. **If you're interested in learning more about how the executive order will impact MSPs, check out this webinar**.

Also, there were five bi-partisan cybersecurity bills submitted in the House this week alone. The bills include:

- HR 2980, The "Cybersecurity Vulnerability Remediation Act"
  Authorizes CISA to assist critical infrastructure owners and operators with mitigation strategies against the most critical known vulnerabilities.
- HR 3138, The "State and Local Cybersecurity Improvement Act"
  Seeks to authorize a new $500 million grant program to provide state, local, tribal, and territorial governments with dedicated funding to secure their networks from ransomware and other cyberattacks.
- HR 3223, The "CISA Cyber Exercise Act"
  Establishes a National Cyber Exercise program within CISA to promote more regular testing and systemic assessments of preparedness and resilience to cyberattacks against critical infrastructure.
- HR 3243, The "Pipeline Security Act"
  Enhances the ability of the TSA—the principal federal entity responsible for pipeline security—to guard pipeline systems against cyberattacks, terrorist attacks, and other threats. This measure codifies the TSA's Pipeline Security Section and clarifies the statutory mandate to protect pipeline infrastructure.
- HR 3264, The "Domains Critical to Homeland Security Act"
  Authorizes DHS to conduct research and development into supply chain risks for critical domains of the United States economy and transmit the results to Congress.

As of Q1 2022, these bills are still all in review and have not been enacted.

In October, the US convened 30 nations from around the world to discuss strategies for combating ransomware, intentionally omitting Russia, which is seen as one of the biggest sources of the cyberthreat problem.

On June 7, the Department of Justice reported that the FBI was able to recover $2.3 million of the cryptocurrency ransom paid by Colonial Pipeline. Bitcoin transactions are all recorded in a public blockchain that anyone can access. These transactions are recorded based on a unique Bitcoin wallet address that is not directly tied to an individual identity within the Bitcoin protocol itself. One method of cashing out Bitcoin is to get a Bitcoin wallet from one of many public crypt exchanges. Exchanges in the US do require individuals to prove their identity before being able to cash out, and in most cases, the exchange itself is actually in control of the wallet. The FBI was able to track the movement of the Bitcoin used in the Colonial Pipeline ransom payment to a public exchange within the US and then was able to seize the Bitcoin with a court order.

The Colonial Pipeline attack, and the US government's response, also prompted responses within the RaaS ecosystem itself. Two major cybercrime forums (XSS and Exploit) have been used by RaaS groups to recruit affiliates banned ransomware ads. The admins of the Exploit forum say the recent attention of indiscriminate targeting of ransomware attacks is the source for their decision to ban ransomware ads and the removal of all topics related to ransomware operations and all affiliate programs. The full statement is as follows:

> Good day,
>
> We are glad to see pentesters, malware specialists, coders, but we are not happy with lockers – they attract a lot of attention. This type of activity is not good to us in view of the fact that networks are locked indiscriminately we do not consider it appropriate for RaaS partner programs to be present on our forum.
>
> It was decided to remove all affiliate programs and prohibit them as a type of activity on our forum.
>
> All topics related to lockers will be deleted.

After the attack, DarkSide released a statement stating that they will now vet targets and forbid their affiliates from targeting certain companies. The press release issued by DarkSide states:

> We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives.
>
> Our goal is to make money, and not creating problems for society.
>
> From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future." – DarkSide gang.

However, soon after this press release, DarkSide reported that several servers in their control were shut down "at the request of law enforcement agencies," and a significant portion of their cryptocurrency was transferred to an unknown wallet. Then, DarkSide shut down all operations and sent the following message to their affiliates (provided by Intel471):

> Starting from version one, we promised to speak about problems honestly and openly. A couple of hours ago, we lost access to the public part of our infrastructure, in particular to the
>
> - Blog
> - payment server
> - CDN servers
>
> At the moment, these servers cannot be accessed via SSH, and the hosting panels have been blocked.
>
> The hosting support service doesn't provide any information except "at the request of law enforcement authorities." In addition, a couple of hours after the seizure, funds from the payment server (belonging to us and our clients) were withdrawn to an unknown account.
>
> The following actions will be taken to solve the current issue: You will be given decryption tools for all the companies that haven't paid yet.
>
> After that, you will be free to communicate with them wherever you want in any way you want. Contact the support service. We will withdraw the deposit to resolve the issues with all the affected users.
>
> The approximate date of compensation is May 23 (due to the fact that the deposit is to be put on hold for 10 days on XSS).
>
> In view of the above and due to the pressure from the US, the affiliate program is closed. Stay safe and good luck.
>
> The landing page, servers, and other resources will be taken down within 48 hours.

On the same day, another RaaS group, Babuk, made a similar announcement claiming they were handing over their ransomware source code to another group, and they would focus only on data leaks. Since then, REvil and Avaddon released coordinated statements regarding amendments to the rules of their organizations, barring affiliates from targeting government, healthcare, educational, and charity organizations, and that any other targets must be pre-approved.

In July, a new ransomware group called BlackMatter began operations and is believed by many to be a rebrand of DarkSide, the RaaS group associated with the Colonial Pipeline attack.

Kaseya ransomware event

On July 2, 2021, Kaseya was compromised and used to spread Sodinokibi (aka REvil), the successor of GandCrab, ransomware through their on-prem VSA appliance. According to Kaseya, around 40 MSPs had their VSA appliances compromised, which REvil then used as a platform for a Buffalo Jump to target their clients, reaching as many as 800-1500 small- and medium-sized businesses. This included Swedish grocery retailer Coop, forcing them to close 800 stores that Saturday. REvil is the same RaaS Russian cybercrime gang linked to the JBS meat processor attack in May and was particularly busy over the summer months, targeting energy companies and even a US nuclear weapons contractor.

In the aftermath of the attack, REvil suddenly shut down all operations and disappeared without a trace leaving many victims unable to pay ransoms if they chose and no way of decrypting their data. On July 22, Kaseya was able to obtain a master decryptor key from a "trusted third party" and distributed it to their customers.

It was generally believed that REvil would return eventually under a new name; however, in September, their dark web server suddenly returned to life after two months of silence. On September 9, a new user on a common Russian cybercrime forum named REvil began posting, including an explanation of events leading to their shutdown and the disappearance of their spokesperson, UNKWN. Below is a translation of that post:

> As Unknown (aka 8800) disappeared, we (the coders) backed up and turned off all the servers. Thought that he was arrested. We tried to search, but to no avail. We waited – he did not show up and we restored everything from backups.
>
> After UNKWN disappeared, the hoster informed us that the Clearnet servers were compromised and they deleted them at once. We shut down the main server with the keys right afterward.
>
> Kaseya decryptor, which was allegedly leaked by the law enforcement, in fact, was leaked by one of our operators during the generation of the decryptor."
> - REvil

After a month of operations, REvil's sites went down again in October. A user named "o_neday," believed to be affiliated with the RaaS gang, posted on the XSS cybercrime forum stating that someone had hijacked their domain.

> "But since we have today at 17.10 from 12:00 Moscow time, someone brought up the hidden-services of a landing and a blog with the same keys as ours, my fears were confirmed. The third-party has backups with onion service keys..."

Then in November, the US Department of Justice announced charges filed against a 22-year old Ukrainian national believed to be an affiliate of the REvil RaaS program involved in the July attack targeting Kaseya and their customers. He was extradited to the US in March 2022 to stand trial for the attack. However, some experts believe that individual convictions won't slow down ransomware attacks because cybercriminal gangs and how they "do business" is in consistent flux.

On January 14, 2022, Russia's security agency arrested 14 alleged members of REvil based on intelligence shared with them by the US. According to US officials, one of those arrested was also involved in the Colonial Pipeline attack.

There have been no reports of any new REvil activity since their public-facing sites went down in October 2021. Combined with the recent arrests, this may be the last we hear of REvil, but we thought the same about Emotet. Only time will tell.

2022 Predictions from the CRU

This prediction was written before the Russian takedown of REvil, one of the most notorious ransomware threat actors of all time, and we know the rest of the story has yet to unfold. Many cybersecurity experts never thought we'd see the day when Russian and US authorities might work together to bring down a ransomware group. But we do predict more will come.

As ransomware continues to escalate in severity, cost, and volume, the pressure will continue to mount. We noted that ransomware attacks in Q3 2021 surpassed those of Q1 and Q2 combined. We expect that trend to continue. Additionally, as noted above and below, Congress is facing pressure to do more to remove the safe havens of cybercriminals. National Cyber Director Chris Inglis told congress last year, Congress should "remove the sanctuary [to ransomware criminals] and bring to bear consequences on those who hold us at risk."

Unfortunately, that won't happen immediately. We predict that more critical infrastructure will be targeted in 2022 before the political climate reaches a fever pitch. But when that happens, expect a flurry of cybercriminal extradition, takedowns, and arrests among law enforcement worldwide. We also predict that 2022 will see the genesis of international cyber law, which may even include treaties with adversarial nation-states.

1 The anatomy of an MSP will be different in 2022

Throughout the changes of the past few years, a new MSP species is emerging. This new MSP has several new traits born through an evolution of events. As private equity has entered the channel, deep financial pockets have given way to a new super-MSP. Mergers and acquisitions have brought MSPs together, spanning the continent and merging into complex, highly capable, fast-growth organizations. While the industry will continue to see small and nimble MSPs, market dynamics have changed forever. These super-large MSPs must have attention to detail and a focus on efficiency and automation to grow. They'll need to attract talent across the world and be wise as they determine what and how much to outsource. Cybersecurity will always be the future for these MSPs, but it will become more critical than ever before.

2 Federal regulators and legislators will create and define clarity on ransomware payments for the first time

The NIST Cybersecurity Framework remains one of the most effective and useful standards our nation has created. MSPs across the nation have used it to mature their own organizations and that of their clients. But it has become apparent that a voluntary standard is not sufficient in the eyes of our regulators and legislators. To quote Director of the Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, "It is apparent that voluntary standards are probably not getting the job done." While mandatory standards for all organizations might take many years to enforce, we're beginning to see the wheels of government move in such a way that might become impossible to stop.

We've already seen the Treasury department issue clarification and a warning to any individual or business making a ransom payment. We know the Federal Reserve and other financial regulators have issued clarity around cryptocurrency and its use in ransomware payments. And while crypto is certainly not the enemy, it's drawn the ire of regulators as the primary means of payment.

But we predict more will happen throughout 2022. Easterly and others in the federal government have testified to Congress multiple times around cybercrime, ransomware threat actors, and the changes organizations need to enact to drive better cybersecurity. We've also seen new legislation in committee describing MSPs and their role in the supply chain. These things will culminate in more cybersecurity legislation in the coming years.

3 The SMB market is going to spend more in 2022

While the world economy is still reeling from the job market shortages, MSPs often feel the pain more than any other industry. While the talent shortage is near all-time highs, MSPs now compete against large multi-national corporations for the same talent. The message is clear: As an MSP, you're going to have to do more with less, and you'll have to pay more to get the talent you need. Unfortunately, these are the cards we've been dealt; there's no end in sight.

When you add cyber insurance changes mandating enhancements and compliance requirements like CMMC coming into full effect, MSPs need to expect to spend more than ever before. As a result, MSPs will need to learn, once again, how to navigate these waters with their own clients. SMB spending, by nearly every study produced, is going to rise significantly throughout the year. While some of it may be forced by outside factors such as insurance and compliance, MSPs will still need to build expertise to guide and teach their clients that what has worked in the past won't suffice for the future. Investments in cyber detection, response, and automation will be more important than ever to an MSP looking to protect its margins and grow throughout 2022.

4 Threat actors will change tactics to stay under the radar in response to law enforcement success

In 2021, law enforcement had more success than ever tracking threat actors, making arrests, and recovering funds. Multiple threat actor groups changed their behavior in response to stay under the radar. At the beginning of 2021, double and triple extortion become the new normal, many threat actors were focused on "Big Game Hunting," and we saw several attacks targeting critical infrastructure. We predict these tactics to change in 2022.

First, double an triple extortion will grow. Double extortion includes stealing proprietary data from victims before deploying ransomware and then threatening to leak or sell that data unless an additional payment is made. Triple extortion includes threats of DDoS attacks or threat actors directly contacting clients or partners of victims. A new tactic, that we predict will grow in 2022, is threat actors stealing and extorting data without deploying ransomware.

Second, we have already seen in 2021 that multiple ransomware operators have banned attacks on critical infrastructure. We predict in 2022 that financially motivated threat actors will further avoid targeting critical infrastructure.

Lastly, we predict many ransomware operators will shift from "Big Game Hunting" to focusing on mid-tier organizations that are capable of decent-sized payout but will not get as much public attention when compromised.

About the MSP Threat Report 2022

This report was created by the ConnectWise Cyber Research Unit (CRU)—a dedicated team of ConnectWise threat hunters that identifies new vulnerabilities, researches them, and shares what they find for all to see in the community. The CRU monitors ransom leak sites and malicious botnets for new threats, uses OSINT resources, and utilizes data from the ConnectWise SIEM powered by Perch to help create content and complete research. **To see all of the CRU's threat reports,** click here.

ConnectWise CRU Feeds

If you liked this report, please sign up for the ConnectWise Cyber Research Unit feeds. This repository contains lists of threat intelligence indicators discovered by the CRU using the ConnectWise SIEM or found during threat hunting. This data is threat intelligence the CRU has been collecting for years and using internally at ConnectWise for threat hunting and threat analysis assistance. We use this intelligence daily, searching for these indicators in our partner's network data to find new threats and filter out false positives. This feed is updated daily. You can also see the latest details with MITRE ATT&CK Mappings with Mitigations.

Sign up for the CRU feeds now >> https://github.com/ConnectWise-Software/ConnectWise-CRU

ConnectWise Cybersecurity Management

The ConnectWise Cybersecurity Management solution includes software and support services that enable TSPs to protect their client's critical assets. With tools for 24/7 threat detection monitoring, incident response, and security risk assessment, ConnectWise removes the complexity of building an MSP-powered cybersecurity stack while lowering the costs of support staff.

Learn more >> www.connectwise.com/platform/security-management

ConnectWise

ConnectWise is the world's leading software company dedicated to the success of IT solution providers (TSPs) through unmatched software, services, community, and marketplace of integrations. ConnectWise offers an innovative, integrated, and security-centric platform—Asio™—which provides unmatched flexibility that fuels profitable, long-term growth for partners. ConnectWise enables TSPs to drive business efficiency with automation, IT documentation, and data management capabilities. And increase revenue using remote monitoring, cybersecurity, and backup and disaster recovery technologies.

Learn more >> connectwise.com

References

Endnotes

1 https://www.connectwise.com/resources/good-news-everyone-ok-maybe-not-everyone

2 https://perchsecurity.com/perch-news/perch-bulletin-fortios-cve-2018-13379/

3 https://www.cisa.gov/uscert/ncas/current-activity/2021/02/02/zero-day-vulnerability-sonicwall-sma-100-series-version-10x

4 https://www.msspalert.com/cybersecurity-breaches-and-attacks/malware/compucom-cleanup-costs-msp-for-sale/

5 https://www.connectwise.com/resources/its-been-a-busy-week

6 https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/

7 https://www.connectwise.com/resources/ransomware-operators-try-out-new-scare-tactics

8 https://perchsecurity.com/perch-news/another-round-of-microsoft-exchange-vulnerabilities/

9 https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

10 https://www.connectwise.com/resources/another-day-another-0-day

11 https://www.connectwise.com/resources/whos-going-to-replace-emotet

12 https://www.msspalert.com/cybersecurity-markets/americas/u-s-federal-agencies-unite-to-mitigate-ransomware-menace/

13 https://www.connectwise.com/resources/colonial-pipeline-hack-and-the-changing-landscape-of-ransomware

14 https://www.connectwise.com/resources/new-ransomware-technique-why-encrypt-when-you-can-wipe

15 https://www.connectwise.com/resources/steaks-are-high-as-ransomware-starts-affecting-the-average-american

16 https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/fbi-investigating-100-ransomware-variants/

17 https://www.connectwise.com/resources/vmware-exploit-being-used-in-the-wild

18 https://www.connectwise.com/resources/a-nightmare-on-spooler-street

19 https://perchsecurity.com/perch-news/rmm-buffalo-jumping-independence-day-remix/

20 https://www.msspalert.com/cybersecurity-news/microsoft-exchange-hafnium-attack-timeline/

21 https://www.connectwise.com/resources/the-print-nightmare-just-doesnt-stop

22 https://www.connectwise.com/resources/the-print-nightmare-just-doesnt-stop

23 https://www.bleepingcomputer.com/news/security/revil-ransomware-gangs-web-sites-mysteriously-shut-down/

24 https://www.connectwise.com/resources/a-new-ransomware-gang-on-the-block

25 https://perchsecurity.com/perch-news/multiple-mail-maladies-vulnerabilities-in-starttls-and-exchange/

26 https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

27 https://www.msspalert.com/cybersecurity-breaches-and-attacks/microsoft-petitpotam-ntlm-attack-mitigation/

28 https://www.msspalert.com/cybersecurity-markets/americas/cisa-amazon-microsoft-and-google-unite-to-fight-ransomware-attacks/

29 https://www.bleepingcomputer.com/news/security/accenture-confirms-data-breach-after-august-ransomware-attack

30 https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

31 https://www.connectwise.com/resources/new-windows-office-0-day-rce-vulnerability

32 https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

33 https://www.connectwise.com/resources/19-new-vmware-vulnerabilities-one-critical

34 https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-59m-blackmatter-ransomware-attack/

35 https://www.bleepingcomputer.com/news/security/revil-ransomware-is-back-in-full-attack-mode-and-leaking-data/

36 https://www.microsoft.com/security/blog/2021/10/11/iran-linked-dev-0343-targeting-defense-gis-and-maritime-sectors/

37 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

38 https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/

39 https://info.uncommonx.com/hubfs/UncommonXStateofCybersecurityMidsizeOrganizations.pdf

40 https://www.msspalert.com/cybersecurity-research/500-million-attempted-ransomware-attacks-so-far-in-2021/

41 https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

42 https://www.connectwise.com/resources/emotet-is-back

43 https://www.msspalert.com/cybersecurity-markets/verticals/u-s-telecom-networks-what-secure-equipment-act-means-for-mssps/

44 https://unit42.paloaltonetworks.com/manageengine-godzilla-nglite-kdcsponge/

45 https://www.connectwise.com/resources/major-vulnerability-in-the-most-common-java-logging-module

46 https://www.connectwise.com/resources/updates-for-log4j-and-december-patch-tuesday

47 https://www.connectwise.com/resources/a-new-new-new-new-log4j-vulnerability

48 https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits

49 https://www.msspalert.com/cybersecurity-research/mssps-among-hardest-hit-by-cyberattacks-targeting-backup-vulnerabilities/

50 https://www.bleepingcomputer.com/news/security/global-it-services-provider-inetum-hit-by-ransomware-attack/