Secureworks®

2021 State of the Threat

A YEAR IN REVIEW

Table of Contents

01

A Letter From Our Chief Threat Intelligence Officer

After the global uncertainties of 2020, I think we all hoped that 2021 would shape into a degree of normality. But when it comes to cybersecurity, that has not been the case. We started the year looking at the aftermath of SolarWinds, and we haven't looked back. From HAFNIUM to Colonial Pipeline to Kaseya, the headlines have kept coming all year long.

What has risen to the top is that threat actors continue to innovate and evolve tried-and-true techniques in order to broaden the threat landscape. The Secureworks® Counter Threat Unit™ analyzes trillions of security events every year that often lead to the discovery of early stage ransomware, business email compromise, and nation-state sponsored espionage attacks, and more. As a result, we are able to paint one of the most comprehensive views of the threat anywhere in the security industry.

In this year's Secureworks Threat Intelligence Report, the team will provide insights and findings generated by coupling the expertise of our research group with direct observations from a vast pool of customer telemetry and incident response engagements. It is my hope, as leader of this talented team of threat researchers, that you will be able to use this summary of what we have seen day in and day out to make your own organization safer from the threats that really matter.

And, as always, our entire Secureworks team is here for you. This annual Threat Intelligence Report is only one way we use our deep understanding of the threat, backed by 20+ years of experience, to strengthen security in the communities we serve. From our researchers to incident response to our adversary group to our operations teams to our product engineers who have built our Taegis™ XDR platform software from the ground up—we are one team dedicated to protecting your progress, enabled by technology.

We are honored to be part of your security journey and hope you get new insights out of the research we present here.

Barry R. Hensley

Barry Hensley
Chief Threat Intelligence Officer
Secureworks

02

Executive Summary and Key Findings

The past year has seen headlines dominated by stories of cyberattacks: Russian supply chain attacks, Chinese espionage groups compromising tens of thousands of Microsoft Exchange servers, and widespread and brazen ransomware attacks by Russia-based cybercriminals.

Condemnations from the U.S. and their allies followed each of these attacks, aimed at shining a light on the perpetrators and holding hostile governments accountable for the malicious cyber activity they have conducted and enabled. The threat level to businesses globally remains high, especially as many organizations are rapidly pursuing IT transformation to support operations in a pandemic environment.

Amidst all this activity, Secureworks Counter Threat Unit (CTU™) researchers continue to track these threats and use their knowledge to develop insights and protections for Secureworks' customers. Their high-level findings for the period June 2020 to June 2021 are, in order of risk presented to Secureworks' customers:

Secureworks®

01

Ransomware remains the number one threat for most organizations. It rose eight percent as a proportion of IR engagements worked in Q1 and 2, 2021 compared to the previous year. There are very few other threats that can cause total loss of business operations for an extended period of time. Ransomware attacks are opportunistic - any organization that is perceived to have money can be a target - and most attacks occur due to gaps in security controls.

02

2021 has seen significantly increased use of zero-day exploits by threat actors, compared to 2020. But threat actors also continue to leverage known but **unpatched vulnerabilities in mass scan-and-exploit attacks.**

03

Just like ransomware, other types of cybercrime continue to flourish. Business Email Compromise (BEC) remains a significant threat. A flourishing landscape of **loaders and downloaders** continues to service the demand for malware-based network access for all types of adversary. **Law enforcement intervention** against these threats, e.g. the Emotet takedown, has led to **tactical successes** but is **yet to cause significant strategic impact.**

04

Both BEC attacks targeting single-factor Microsoft 365 email accounts, and Russian espionage operations leveraging compromised Azure applications and stolen SAML token-signing certificates, e.g. the SolarWinds supply chain compromise, continue to show that **identity is king.** The role of security controls around authentication will remain crucial as more organizations move to cloud services or hybrid operating models.

05

Despite the level of attention it attracts, state-sponsored activity remains targeted and narrowly focused, according to the priorities of the country it originates from. CTU researchers continue to see significant levels of activity from groups affiliated with **China, Iran, Russia and North Korea.**

06

Cybercriminal and state-sponsored threat actors continue to leverage widely available offensive security tools (OSTs) in network intrusions. These tools are easy to use, carry no development cost, and are hard to attribute, making them an attractive proposition. **Cobalt Strike**, by far the most popular OST tool used by threat actors, **featured in 19 percent of network intrusions.**

03

About the Report

This report lays out CTU researchers' view of the significant developments in the threat landscape over the past year. Unsurprisingly, post-intrusion ransomware features extensively, as it remains the most significant threat facing Secureworks' customers.

The report also explores developments in ransomware precursors. The deployment of ransomware is the final stage of an attack: the best time to detect ransomware attackers is in the hours and days prior to that moment. That makes understanding the tools and techniques threat actors use crucial. Scanning and exploiting vulnerable public-facing infrastructure, malware delivered via spam emails, and off-the-shelf penetration testing tools such as Cobalt Strike all feature heavily.

For a subset of organizations, nation state advanced persistent threat (APT) actors also form a significant threat. China, Iran, Russia, and North Korea have all impacted Secureworks' customers in different ways over the past year. The report looks at the activities of each of those countries in turn. It also draws out the lessons from two high profile but very different APT attacks: the SolarWinds supply chain compromise and the exploitation of Microsoft Exchange Server vulnerabilities.

Throughout, the report will also focus on how attacks can be prevented. Customers can use this information to guide risk management decision-making, inform best practice, and prioritize resource allocation.

The Secureworks View of the Threat

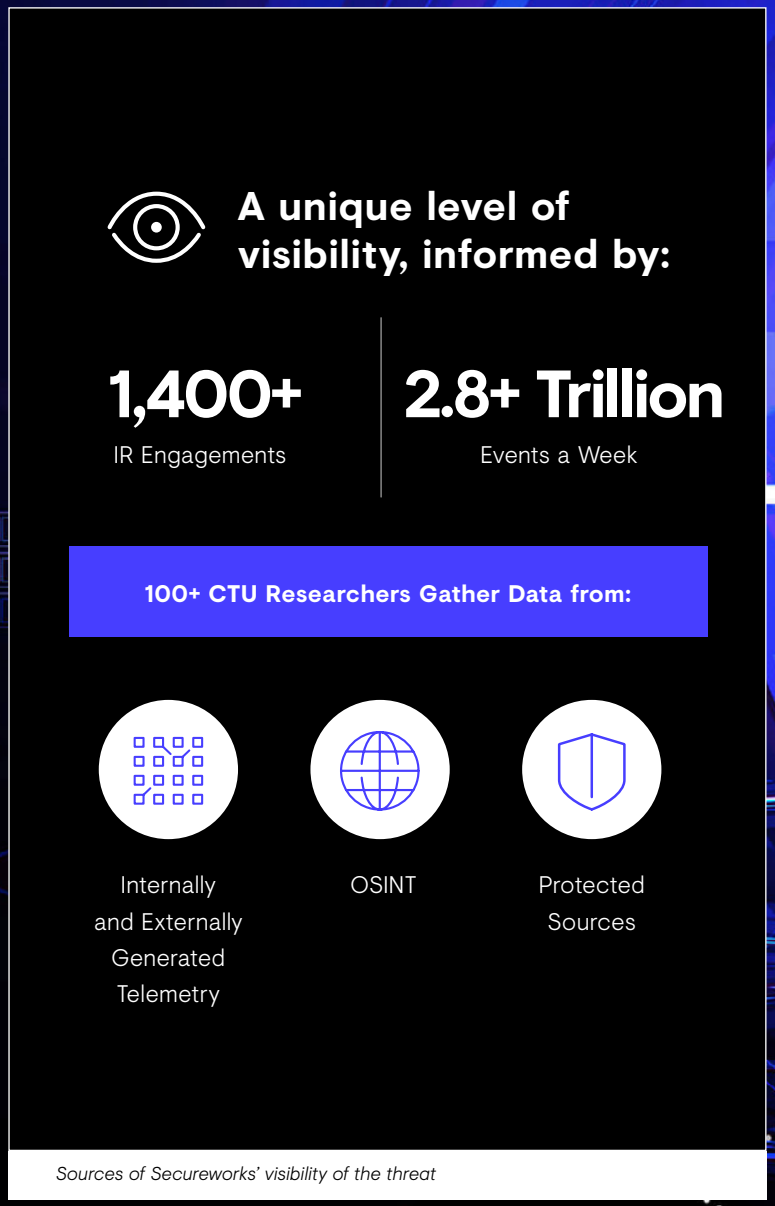
Secureworks' unique view of the threat landscape comes from a combination of the incident response engagements it carries out, the telemetry it monitors from the Taegis XDR platform, and the technical and tactical research carried out by the Counter Threat Unit into threat actor activity. Together, that all adds up to a unique level of visibility into threat actor intent, capability, and activity.

In the 12 months from July 2020, the Secureworks Incident Response team and Secureworks Counter Threat Unit conducted over 1,300+ incident response engagements, across a wide spectrum of industry sectors.

- Secureworks processes approximately two trillion events every single week, gathered from security infrastructure in thousands of customer environments around the world.

- CTU researchers gather and analyze data from internally generated and externally collected telemetry, from multiple sources of open-source information, including dark web forums, proprietary botnet emulation systems, and intelligence provided by partners.

The result is a vivid, yet fine-grained picture of threat actor activity that portrays both the thrust of their high-level tactics and the technical details of their tooling. This knowledge fuels the elite threat detection and integrated response actions that Taegis XDR delivers. It finds form in the expert threat intelligence products published every week by the CTU and is condensed in this analysis of the state of the threat landscape over the past year.



Sources of Secureworks' visibility of the threat

04

Ransomware Remains the Number One Threat for Most Organizations

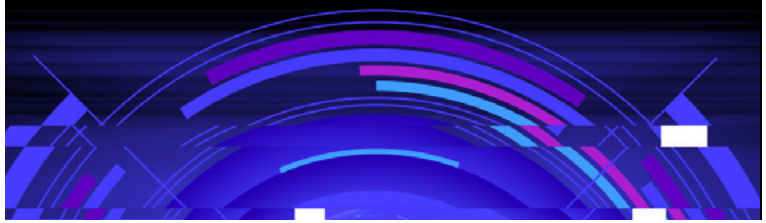
The post-intrusion ransomware landscape is thriving. Volume of incidents, number of ransomware operators, and average ransom demands all continue to increase. The ransomware-as-a-service[1] affiliate model allows operators to scale their operations and significantly lowers the barrier to entry. A successful ransomware attack can instantaneously cripple even the largest of organizations. All of this makes ransomware the single greatest threat facing Secureworks' customers today. As a result, ransomware engagements account for more than half of the financial crime incidents worked by Secureworks incident responders.

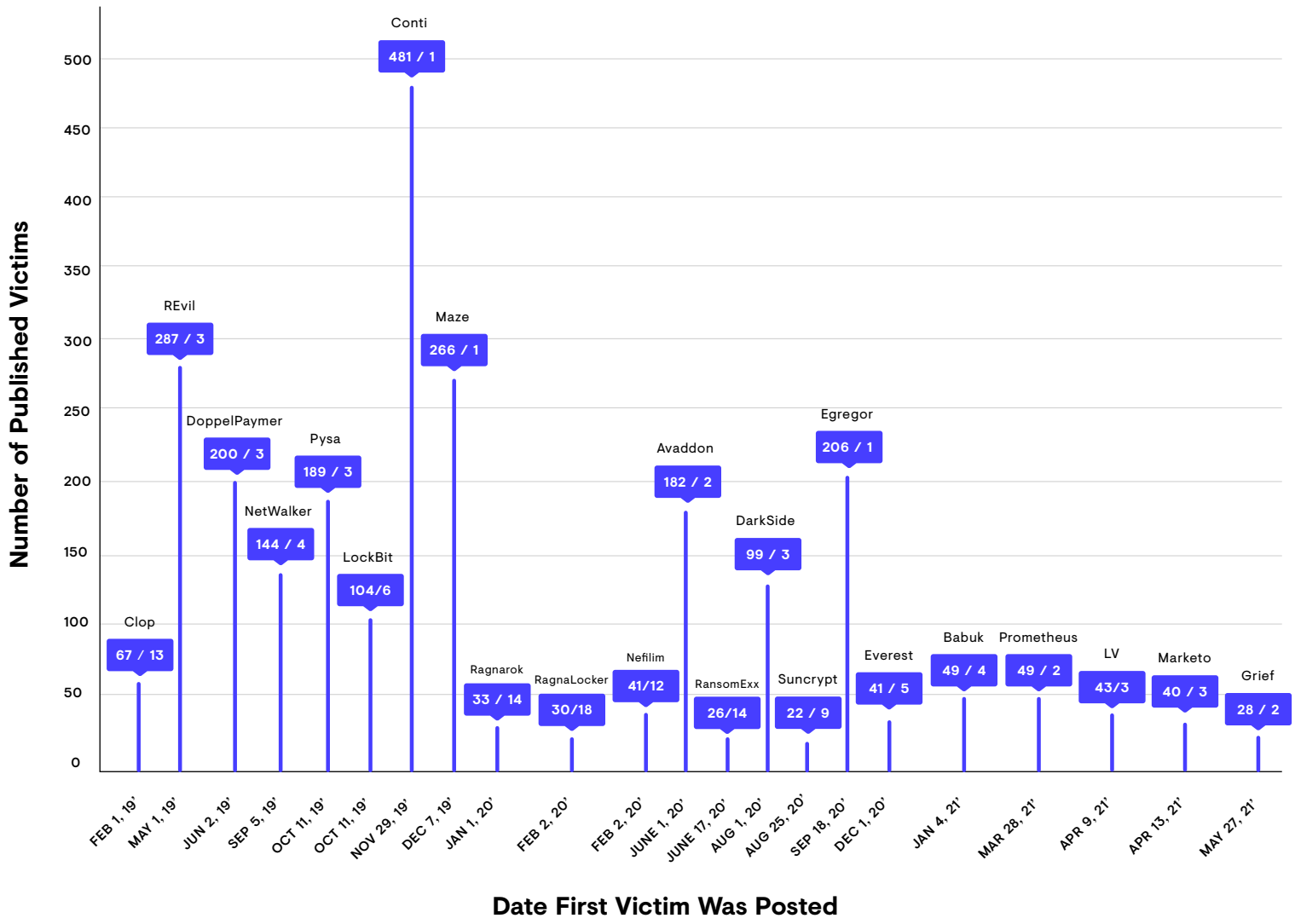
Organizations that apply good security basics can demonstrably reduce their chances of falling victim to ransomware attacks, yet a substantial number continue to struggle with this. At the macro level, a coordinated response to the ransomware actors from international law enforcement and government policy looks promising but is yet to have a major effect.

How Secureworks Carries Out Attribution

Threat group names used by Secureworks refer to observed activity clusters or intrusion sets. If CTU researchers attribute an attack to a group, it is because the indicators and the tactics, techniques, and procedures observed during the attack match or align with those seen in previous activity attributed to the group. Groups are also clusters of individuals, but individual threat actors may work for more than one group, or may change groups.

The names are based on metals. In this report you will meet GOLD cybercriminal groups, as well as state-sponsored groups that are IRON (Russia), BRONZE (China), COBALT (Iran), or NICKEL (North Korea). The Secureworks **Threat Group profiles** are available on the Secureworks website with further information about most of the groups featured in this report.





Ransomware leak site statistics as of mid-August 2021. The number that follows the slash represents the "Number of days between new victims". (Source: Secureworks)

GOLD ULRICK – Back Refreshed and With Different Tradecraft

GOLD ULRICK is the distributor of the Conti and Ryuk ransomware families. GOLD ULRICK is likely comprised of some or all of the same operators as **GOLD BLACKBURN**, the group responsible for the distribution of malware such as TrickBot, BazarLoader, and Buer Loader. Ryuk was one of the most prevalent ransomware strains encountered by Secureworks incident responders from late 2018 through 2019. It seemed to have disappeared between February and September 2020 but attacks then resumed activity, alongside 'name-and-shame' attacks using the Conti ransomware.

CTU researchers assess that since approximately late 2019, GOLD ULRICK began expanding its activities by working with various other operators who were recruited through existing trusted relationships rather than via adverts on underground forums. In August 2021, a persona claiming to be a disgruntled Conti affiliate released a swathe of information including tools and standard operating procedures provided to Conti affiliates by GOLD ULRICK.

Prior to February 2020, Ryuk attacks typically followed a consistent playbook: leveraging an existing TrickBot infection for initial access, deploying PowerShell Empire or Cobalt Strike across the environment, and then staging Ryuk on domain controllers and deploying it widely across the enterprise using either PSExec and batch scripts or Group Policy Objects. The script below is a PowerShell script used to create a Group Policy Object that weakens domain-joined systems' security settings prior to deployment of Ryuk.

However, since September 2020 this expansion has resulted in divergent tactics, techniques and procedures during observed intrusions involving Ryuk and Conti deployments. In one example in early 2021, Secureworks incident responders helped an organization where the threat actor had accessed the environment using stolen VPN credentials and deployed Conti manually to a small number of systems using Remote Desktop Protocol (RDP). Not only is this a significant departure from previously observed tactics, techniques and procedures (TTPs), but the more localized deployment also caused far less impact to the affected organization, very unlike previous GOLD ULRICK intrusions where enterprises have experienced weeks or months of downtime.

```
#import powershell modules
Import-Module activedirectory
Import-Module grouppolicy
#Edit migtable
$domain = $env:USERDNSDOMAIN
$target = Get-ADDomain
$t = $target.DistinguishedName
$doinfo = Get-ADDomainController
$a = Get-Content -path "C:\temp\All in one\GPO.migtable"
$mt1 = foreach ($s1 in $a){$s1.replace("Domain_for_import","$env:userdnsdomain")}
$new_migtable = foreach ($s2 in $mt1){$s2.replace("DomainController","$env:COMPUTERNAME")}
$new_migtable | Set-Content "c:\temp\All in one\1.migtable"
    #Create new GPO and import backups settings
#1 ADD Reg keys
Import-GPO -BackupGpoName "All in One Policy (v.02)" -Path "c:\temp\All in one\" -CreateIfNeeded -Domain $env:USERDNSDOMAIN
-TargetName "Default Policy" -MigrationTable "c:\temp\All in one\1.migtable"
#5 Enable GPO links
new-GPLink -Name "Default Policy" -Domain $env:USERDNSDOMAIN -Enforced Yes -LinkEnabled Yes -Target $t -Order 1
```

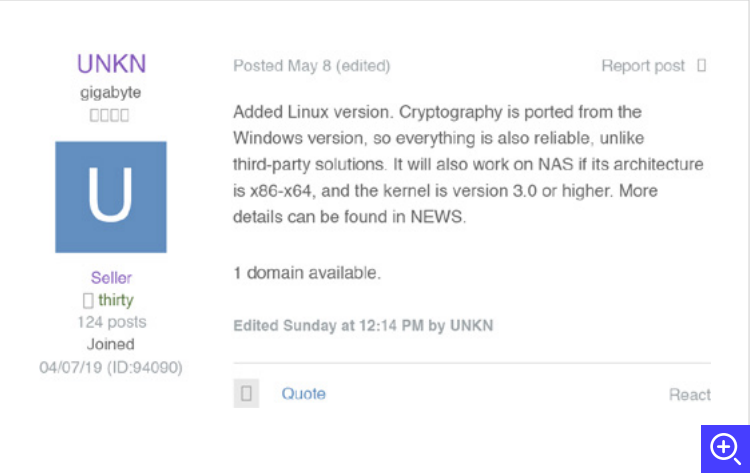
PowerShell script (_this_domain.ps1) used in Ryuk attacks to create Group Policy Object. (Source: Secureworks)

Innovation and Evolution

The last 18 months have seen constant evolution in the ransomware landscape, as criminal groups continue to explore ways to maximize profitability.

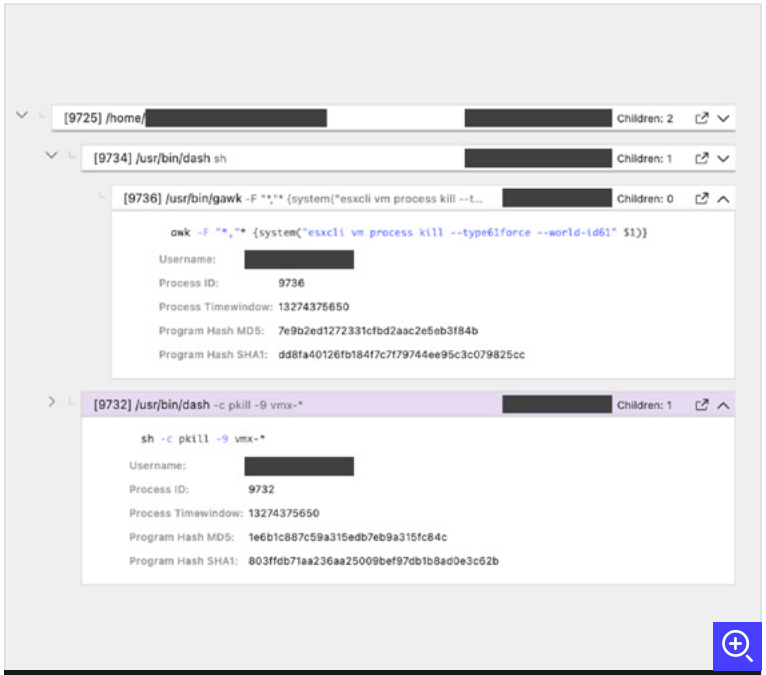
GOLD VILLAGE (Maze) pioneered the name-and-shame approach in December 2019. It was quickly followed by GOLD HERON (DoppelPaymer), GOLD SOUTHFIELD (REvil) and GOLD MANSARD (Nemty). Between March 2020 and June 2021, the number of active name-and-shame groups tracked by CTU researchers rose from four to 27. During that time, some groups launched and terminated operations, and others rebranded.

A small number of ransomware operators started adding Linux versions of ransomware to their repertoire, including 777, Babuk, HelloKitty, REvil, and DarkSide.



May 2021 forum post advertising REvil Linux variant. (Source: Secureworks)

Linux ransomware often targets VMware ESXi servers, a hypervisor for deploying and hosting virtual machines. This shows the threat actors are devoting resources to improve their effectiveness against enterprise targets.

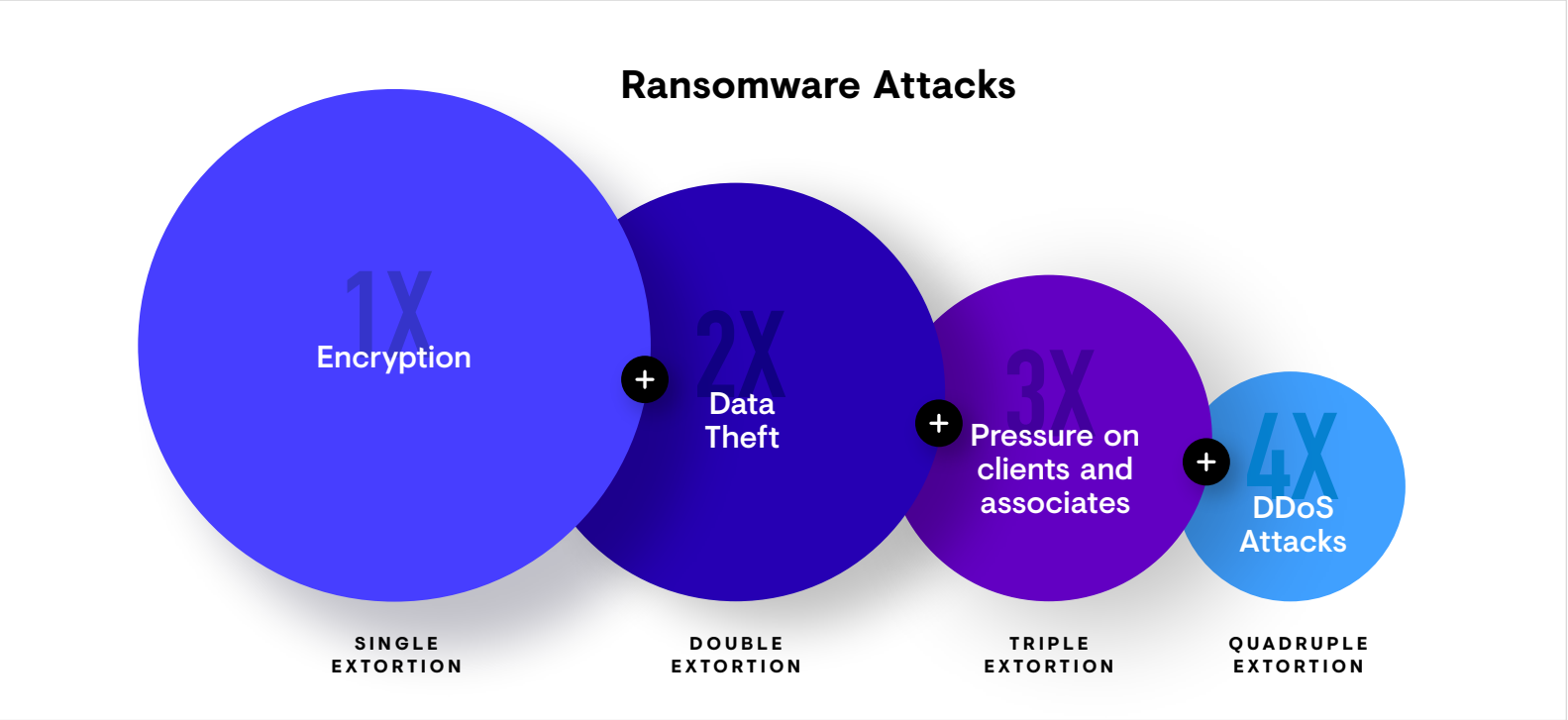


REvil Linux variant ('REvix') attempting to shut down VMs prior to encryption of the hypervisor. (Source: Secureworks)

Name-and-Shame Remains the Name of the Game

Name-and-shame attacks allow for 'double extortion'. Victims are under pressure to pay to recover their data (availability), but also to prevent it being published online (confidentiality). For some, the threat of sensitive business or client information being made public may be worse than the consequences of their systems being encrypted. The extra threat also comes with a deadline to pay, increasing the pressure to hand over the ransom to avoid further pain in an already painful situation.

Name-and-shame has become the predominant operating method for most ransomware groups, with victims being added to public leak sites at a worrying rate. The most active name-and-shame ransomware group over the past year was GOLD PHANTOM's Egregor, adding an average of 60 victims a month to its leak site between its launch in September 2020 and its apparent demise at the end of 2020. GOLD ULRICK added an average of 23 new Conti victims a month across the entire period. Grief, the successor to DoppelPaymer launched by GOLD HERON at the end of May 2021, added 23 during June alone.



Ransomware operators are adding extra tactics to exert extra pressure. (Source: Secureworks)

Name-and-shame dark web leak sites provide useful insight into the activities of these ransomware groups but may be misleading in terms of scale. They only list organizations that have not immediately paid ransom demands, and they may not list all victims. When Avaddon ceased operation in June 2021, its public leak site had listed a total of 182 victims since the beginning of June 2020. However, when the group shut down its operation, it released a total of 2,934 individual decryption keys[2], each corresponding to a specific victim. That's nearly 16 times as many and shows that often only a minority of victims will appear on their public sites.

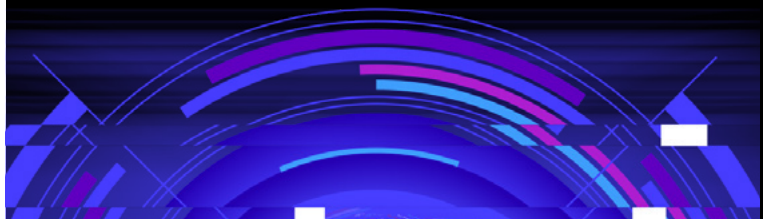
There are also still successful ransomware operations that do not use name-and-shame tactics, such as **GOLD DUPONT**. CTU researchers have observed GOLD DUPONT successfully operate Defray and 777 ransomware in several fast and extremely aggressive post-intrusion attacks using Vatet loader, a file transfer tool called ArtifactExx, Cobalt Strike, PyXie RAT, and a variety of native Windows utilities. However, there are now significantly more successful ransomware operations that incorporate name-and-shame tactics than do not.

Hack and Leak — A Move Away from Encryption?

Some operators have experimented with data theft and extortion only:

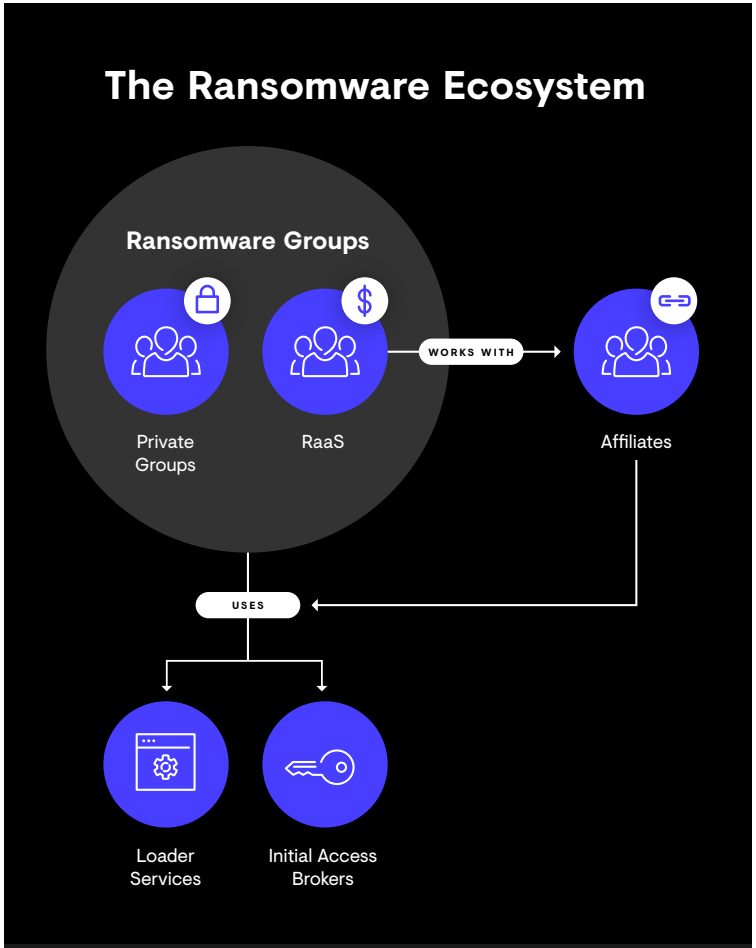
- In the December 2020 attack on the Accellion File Transfer Appliance (FTA) software by **GOLD TAHOE,** operator of Clop ransomware, all the attacker did was exfiltrate data from the Accellion appliance and post it to the Clop leak site.
- Babuk separately claimed to have abandoned ransomware in favor of theft and extortion only in late April 2021, although with limited success.
- In one incident worked by Secureworks incident responders, the threat actor was disturbed during their lateral expansion and consolidation activity. In response to being disrupted, the group immediately shifted into demanding an extortion payment to prevent the data they had already stolen being leaked online.

It is unclear whether theft and extortion without data encryption is a viable business model, even when it is done well. Manufacturing organizations, for example, are far more likely to feel the pain of production downtime caused by critical systems being unavailable. Victims based in countries with relaxed regulatory regimes may not feel sufficiently pressured to prevent data leaking into the public domain to pay the extortion fees demanded.



Opportunistic Compromise, Targeted Deployment

The ransomware landscape is complex, with multiple different actors collaborating at different stages of the attack lifecycle.



The ransomware ecosystem. (Source: Secureworks)

Initial access brokers (IABs) play a critical role in facilitating opportunistic compromises that lead to ransomware deployment. IABs often use publicly available scanning tools to identify vulnerabilities and indiscriminately exploit those flaws.

Once initial access is available, operators may choose to infect systems based on the perceived maturity of a potential victim's security controls, and the victim's annual revenue. Some ransomware groups may prioritize certain victims due to perceived success. For example, previous attacks on manufacturing organizations showed that forcing critical manufacturing processes offline provides a strong incentive for the victim to pay the ransom.

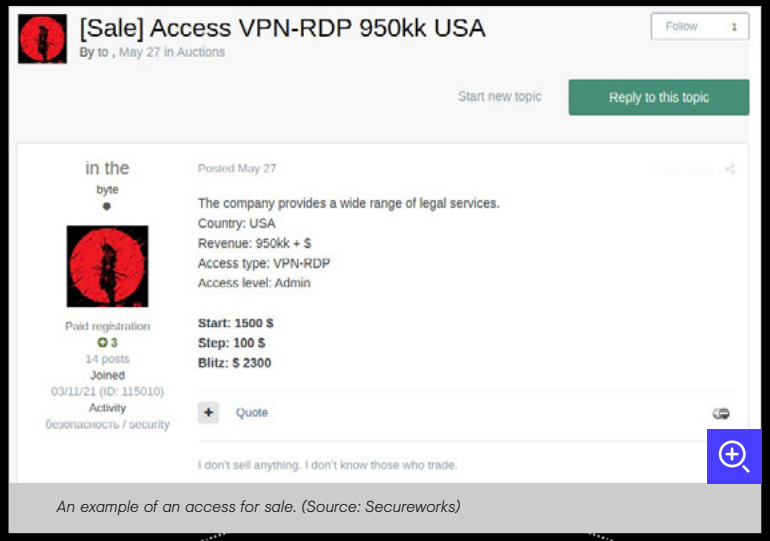
Once inside the network the attacker will attempt to target or discover the files and processes that would give them most leverage when disrupted, exfiltrated or encrypted. For example, the Clop operator has been reported to prioritize access to the workstations of senior executives during exfiltration of data from victim organizations. The reason for this tactic is reported to be to obtain the most valuable information.

In other words, post-intrusion operators are generally selective about the victims they hit once initial access has been gained and a degree of triage carried out, but the initial compromise is opportunistic. Ultimately, ransomware attacks occur where access can be most easily obtained and maintained.

Buying and Selling Access

Offers of access brokering on underground forums is widespread and IABs are used by both ransomware-as-a-service (RaaS) and private ransomware groups. CTU researchers frequently observe advertisements for access to organizations in a wide range of verticals, with healthcare, hospitality, retail, and education being the most common.

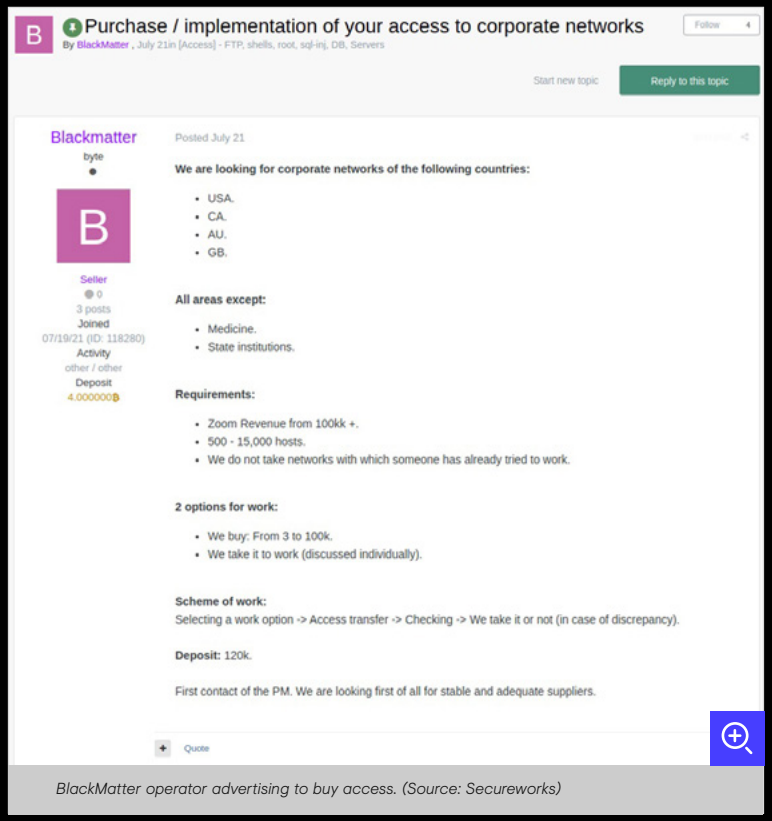
In May 2021, a single forum persona tracked by CTU researchers advertised VPN/RDP access to multiple companies in France and the U.S., including a medical research company, a hotel complex, a restaurant chain, and a tobacco and beverage company. The asking price was $800 USD in total. Two different threat actors were selling access to one U.S. university each. One asking price was $250, the other, for domain admin logins, was $6,000.



An example of an access for sale. (Source: Secureworks)

Listings do not name the victim but do provide basic details such as sector, geography, and revenue. A threat actor buying that access will only find out who the victim is once they have paid into an escrow account run by the forum.

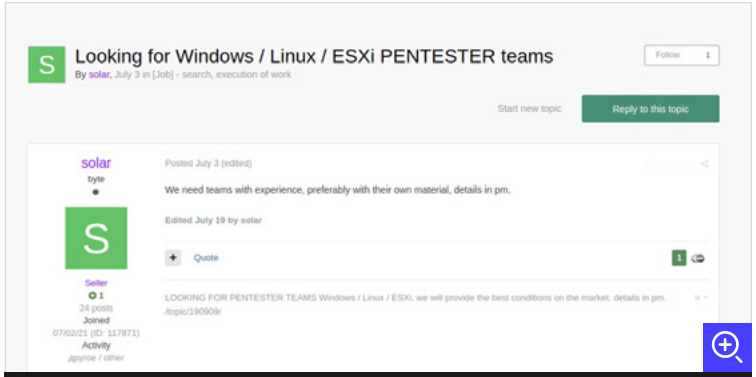
CTU researchers have also observed ransomware operators advertising to buy access, rather than IABs advertising to sell it. One example of this is the BlackMatter ransomware, likely operated by the GOLD WATERFALL threat group who previously operated the DarkSide RaaS.



BlackMatter operator advertising to buy access. (Source: Secureworks)

Affiliates Drive Scale

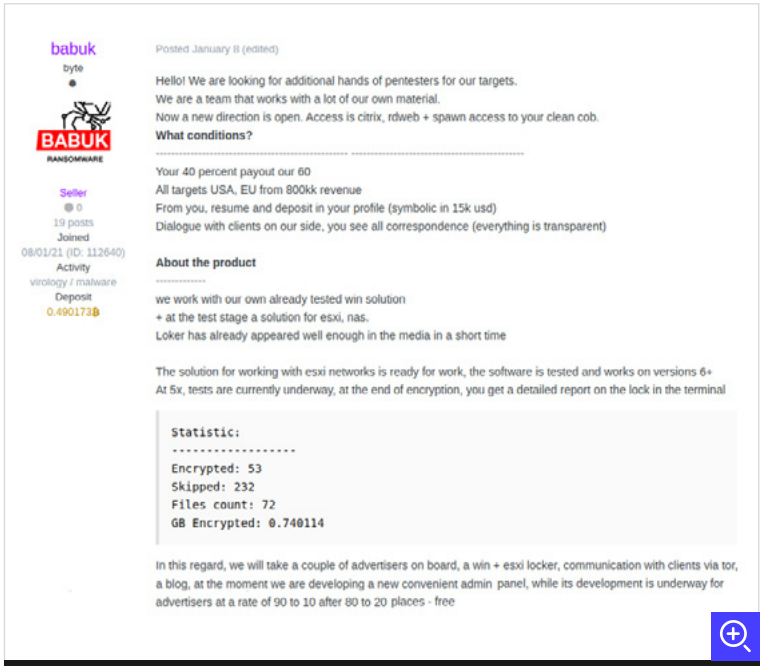
The RaaS model has been fundamental in driving scale in the ransomware ecosystem. The use of affiliates greatly increases the number of organizations that can be targeted concurrently. Conversely, the scale of ransomware activities may be constrained or gated by the number of human operators available. Affiliate schemes are therefore key enablers to 'growth', but attack sophistication can vary when affiliates have different skill levels.



Groups looking for affiliates on underground forums often advertise for 'pentesters'. (Source: Secureworks)

It is likely that affiliates and RaaS operators form enduring relationships when mutually beneficial. However, each RaaS operation has a limited number of affiliate 'seats' available, so affiliates may move to another RaaS operation once a campaign is complete. For example, Babuk operators claimed at the beginning of 2021 they could support two affiliates concurrently, while GOLD SOUTHFIELD claimed that the REvil RaaS could support ten prior to it being shut down. Because operators usually manage the process of negotiation with victims, limiting the number of affiliates allows them to manage the number of victims they are negotiating with.

Affiliates can also cause groups problems. It is thought that affiliates were behind both the REvil Kaseya attack and the DarkSide Colonial Pipeline attack. To control risks of this nature, some operators may forbid affiliates from proceeding with attacks on organizations in certain sectors e.g., healthcare, education, non-profit organizations, critical infrastructure. Limiting the number of affiliates also helps with oversight.



Babuk advertising for two affiliates. (Source: Secureworks)

Law Enforcement and Government Action Against Ransomware

The cumulative impact of ransomware attacks is now being viewed by governments as a national security threat, driven in part by public services being impacted by attacks against healthcare providers, fuel distribution organizers, and more.

In early June 2021, the FBI director, Christopher Wray, said[3] that cybercrime threat presented "a lot of parallels" to the threat of terrorism before 9/11. In response to a question about whether the U.S. was considering military action against ransomware operators, the commerce secretary, Gina Raimondo, said[4] that "all the options" were being considered. So far, a range of different response options are being used.

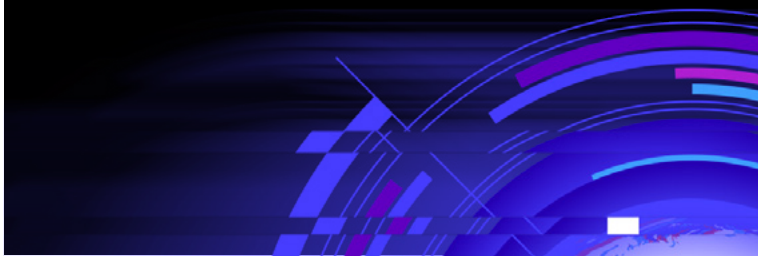
This increasingly assertive law enforcement response is unlikely to change direction in the short term. The ransomware problem remains a difficult one to address. Many of the operators are located either in Russia or in Commonwealth of Independent States (CIS) countries. If they avoid targeting Russian or CIS entities as victims, they are largely left alone by law enforcement. Some actors have been linked with elements of the Russian government and intelligence services, including Maksim Yakubets who was indicted by the U.S. in 2019 for cybercrime offenses. Yakubets previously worked for the Russian Federal Security Service (FSB) and is thought to have FSB familial ties.

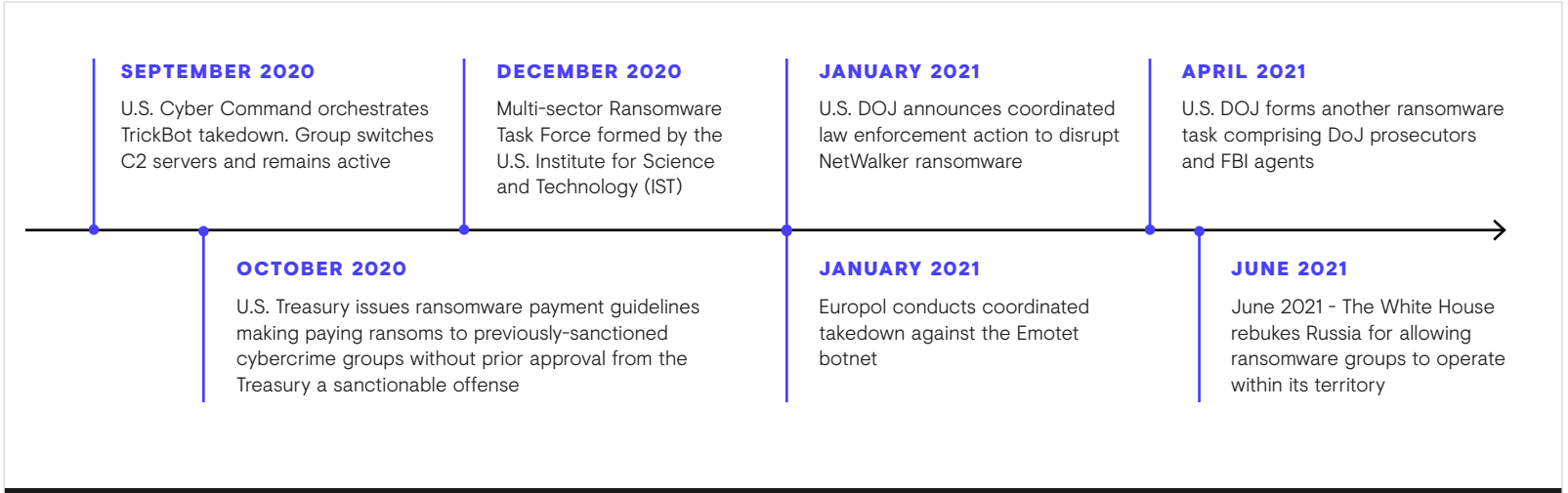
The Impact of Malware Loader Takedowns

Both TrickBot and Emotet were the targets of takedown activity. There were two operations against TrickBot , one in **September 2020**[5] by U.S. Cyber Command, and then separate actions by **Microsoft**[6] in October and November. There was one against the Emotet botnet in late January 2021 by international law enforcement[7].

By the beginning of 2021, TrickBot's operator GOLD BLACKBURN had rebuilt its botnet. TrickBot is now back at full strength. GOLD BLACKBURN has also increased its use of other malware including Team9 (also known as BazarLoader) and BuerLoader. The Emotet botnet, operated by the GOLD CRESTWOOD threat group since 2014, has not reconstituted, although CTU researchers assess that the GOLD CRESTWOOD threat group will re-tool or begin to collaborate more directly with other cybercriminal groups such as the GOLD LAGOON threat group that operates the QakBot botnet.

By 2020, the Emotet malware distribution or 'loads' service was only servicing TrickBot, Qakbot and, according to open source **reporting**,[8] IcedID. All of these botnets have their own distribution capabilities, so they simply switched to their own distribution methods. Overall, there has been little significant change in the amount of malware being distributed to potential victims.





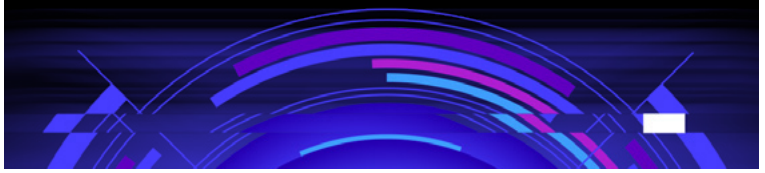
Law enforcement and government action against ransomware threat actors

The Biden administration has raised concerns about ransomware with Russia's President Putin and has claimed that its message has been heard. It is positive that ransomware is now on the agenda for such high-profile dialogue, although the prospects for substantive action being taken. Russia has a long-standing history of non-extradition to the U.S. and other countries, and it is unclear what the U.S. and other countries could or would want to offer in return for Russian cooperation against organized criminals located in Russia.

It seems likely that the game of ransomware whack-a-mole will continue for some time to come. Indeed, the overall level of activity in the ransomware space as a whole has not changed greatly, despite these interventions. By being careful to avoid organizations that significantly impact critical infrastructure or public services, most RaaS and private operations can operate below the threshold at which public opinion will force a more aggressive law enforcement response.

New Name, Same Game

Ransomware groups appear to have realized that there is such a thing as being 'too successful', and that too much public and law enforcement scrutiny can be a bad thing. In May 2021, the response to the Colonial Pipeline incident led to GOLD WATERFALL shuttering its DarkSide operation, only to re-emerge several months later with the BlackMatter ransomware. In July, the prolific REvil ransomware-as-a-service operation shut down following an attack that hit hundreds of organizations through a vulnerability in Kaseya remote monitoring and management software. REvil recommenced operations in September 2021.



Organizations Can Protect Themselves

Despite takedowns and other law enforcement activity, the opportunistic nature of attacks, combined with the drive to scale, mean that all organizations need to be at the top of their security game.

Organizations that patch promptly and regularly, protect external facing applications with multi-factor authentication, implement the principle of least privilege, segment networks, and implement endpoint and network traffic monitoring and detection can protect themselves against ransomware. It is no coincidence that the financial sector, subject to all-encompassing regulatory requirements concerning security, is less prone to ransomware than other, less strictly regulated sectors. Organizations can and do protect themselves against ransomware every day.

Security basics add up to ransomware protection.

Examples include:

An administrative user was prompted to approve a VPN access request that they did not initiate. A threat actor was likely using a stolen or guessed username and password in an attempt to access the user's VPN account. Because the organization used multi-factor authentication (MFA) the user had an opportunity to reject the request. The subsequent investigation showed that this one control was critical in preventing the threat actor being able to gain privileged access to the environment.

CTU researchers discovered a Cobalt Strike command and control IP address identified from one DarkSide ransomware engagement in another organization's firewall logs. The customer was notified, initiated their incident response procedures, and uncovered evidence of credential theft, privilege escalation, installation of Cobalt Strike across multiple systems, and access to business-critical servers. The organization was able to contain the intrusion before the threat actor was able to deploy ransomware. Although indicator-based controls are insufficient on their own, they can sometimes help and should certainly not be dismissed.

05

Scan-and-Exploit— Patch or Be Punished

Patching is always easier said than done. Keeping track of the systems and software packages that exist, keeping track of the patches, prioritizing them, finding resources to apply the patches, finding appropriate maintenance windows to avoid user impact, and even just accepting the risk of changing a working critical system are all hard in today's enterprises. But the fact is that threat actors know this, and unpatched vulnerabilities are easy prey for them.

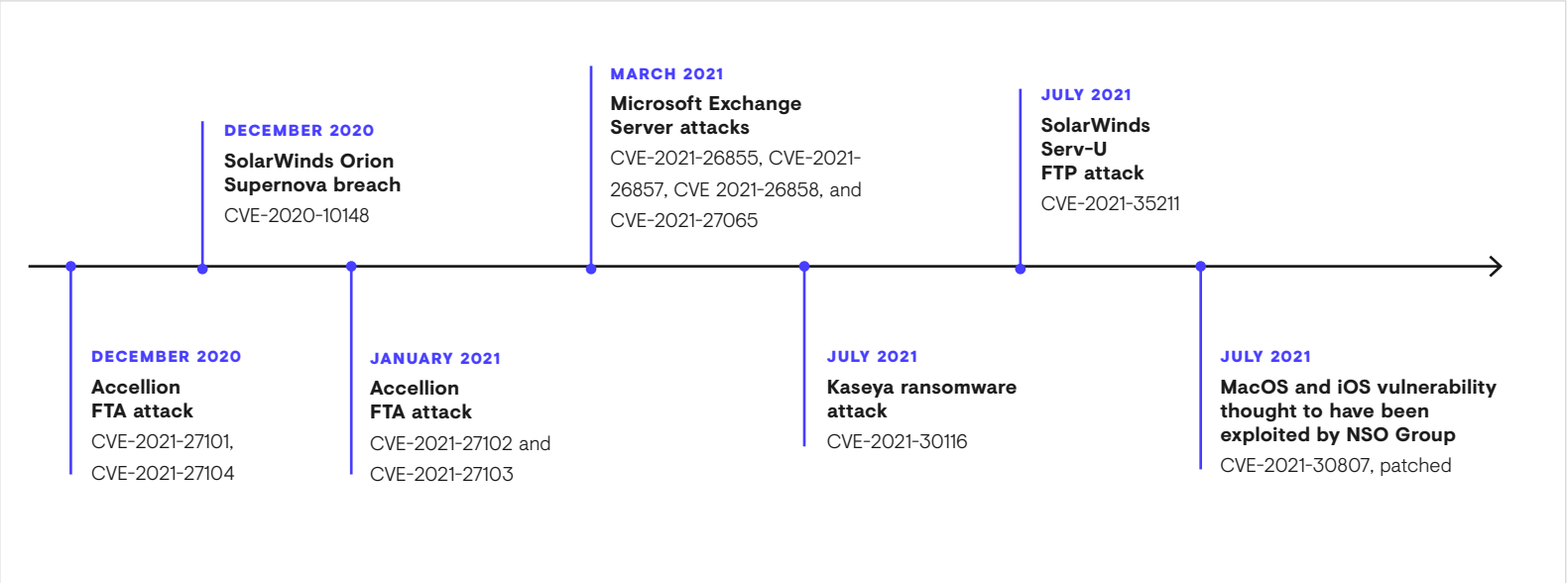
Multiple groups, both cybercriminals and state-sponsored, will scan the internet for unpatched vulnerabilities to exploit – the so-called scan-and-exploit approach. Most of the time threat actors exploit vulnerabilities where patches have been available for some time. For example, according to data[9] released from the U.S. National Security Agency (NSA), FBI, and CISA, the top three CVEs routinely exploited in 2020 were well-known: Citrix vulnerability CVE-2019-19781, Pulse Connect Secure's CVE 2019-11510, and CVE 2018-13379 in Fortinet FortiOS.

However, 2021 has also seen a proliferation of zero-day vulnerabilities being used. Zero-day vulnerabilities in the wild used to be very rare, but Google Project Zero data[10] showed that the number of zero-days exploited in 2021 had passed 2020's annual total of 25 by mid-2021. By early August 2021 it stood at 37. Zero-day vulnerabilities typically take lots of time, resources and expertise to identify, and they're generally used sparingly to avoid detection. It's unclear what has fueled the growth in identified zero-day exploits; it could be that we are all just getting better at detecting their usage, or it could be that threat groups – particularly state-sponsored and ransomware groups – have more resources at their disposal to buy or find them.

In most cases zero-days are exploited and discovered and exploited in highly targeted attacks, meaning that fewer organizations are impacted. However, once exploit code becomes publicly available, it will rapidly be rolled into commonly available offensive security tools, and many opportunistic threat actors will start leveraging it.

The most effective way of preventing scan-and-exploit is through good vulnerability management, backed up by layered security controls. Timely threat intelligence can help you prioritize which vulnerabilities are more important – e.g., if they're being actively exploited in the wild or are more easily weaponized.

The message is clear: patching is not straightforward, but without it organizations leave themselves exposed, particularly where they are running critical servers on-premises rather than on managed cloud infrastructure. Where systems cannot be patched, organizations need to consider compensating controls to prevent, detect and contain exploitation of those systems by threat actors looking to drop ransomware, steal credentials or exfiltrate sensitive data.



Prominent attacks leveraging zero-day exploits

2019 Vulnerability Remains Popular Access Vector

Throughout 2020, Secureworks analysts observed financially motivated and state-sponsored threat groups such as **COBALT FOXGLOVE**, **IRON LIBERTY**, and **BRONZE UNION** exploiting Citrix NetScaler vulnerability CVE-2019-19781 as the IAV in network breaches. This vulnerability allows an unauthenticated user to execute arbitrary code. In the incidents studied by Secureworks analysts, the threat actors delivered a range of malware, including web shells and cryptocurrency miners. The publication of proof-of-concept exploits and the ubiquity of Citrix NetScaler at the network perimeter of organizations worldwide made this vulnerability an attractive vector for threat actors with a range of motivations and varying levels of technical sophistication.

On-Premises Exchange Server— a Lesson in Patching and Exploitation

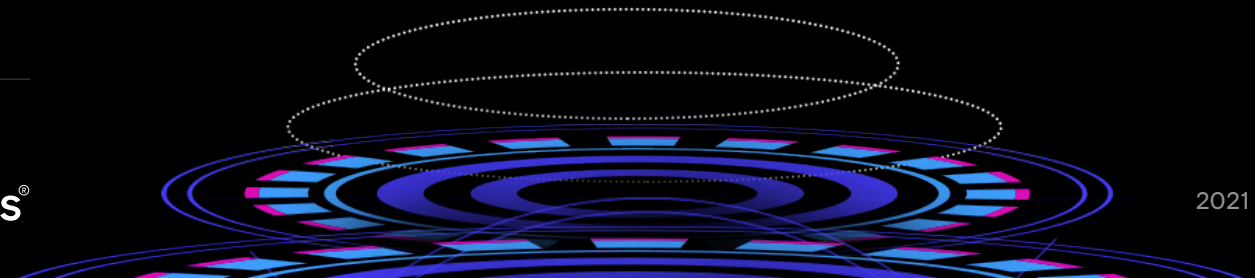
In March 2021, Microsoft disclosed four vulnerabilities in on-premises Microsoft Exchange Server that were under active exploitation by Chinese state-sponsored threat actors: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. These were patched by Microsoft at the beginning of March. CVE-2021-26855 became known as ProxyLogon. A further four critical remote code execution vulnerabilities were patched by Microsoft on April 13, followed by an additional four patched in May.

Despite considerable publicity at the time about the attacks and vulnerabilities, **industry estimates**[11] suggested that at least 125,000 on-premises Exchange Servers globally remained unpatched by March 9, out of about 250,000 globally. However, by late March 2021, **media reports**[12] indicated that 92 percent of vulnerable Exchange servers had applied the March patches. CTU researchers advised throughout that all organizations using affected versions of on-premises Microsoft Exchange Server, even if they had patched, should assume that they could have been compromised and should investigate for signs of an intrusion. This assessment was reinforced by action taken by the FBI, **announced**[13] in April by the Department of Justice, to access web shells remaining on U.S.-based Exchange servers and delete them.

Soon after the Exchange Server vulnerabilities became public in March, CISA **stated**[14] that it was "aware of widespread domestic and international exploitation of these vulnerabilities." In other words, cybercriminals wanted a slice of the ProxyLogon pie. Despite the pressure to patch, exploitation of unpatched servers continued for several months.

Ransomware variants known to have been deployed to exposed Exchange servers included the previously unknown DEARCRY or Ransom:Win32/DoejoCrypt.A, and Black Kingdom. Babuk also claimed to have leveraged an Exchange server vulnerability. In April, attackers behind the Prometei **Botnet**.[15] leveraged Exchange server vulnerabilities to deploy Monero cryptominers and other malware, and to harvest credentials.

The trend of opportunistic threat actors weaponizing vulnerabilities first identified in targeted attacks is not new. Cybercriminals are opportunists and will look to use publicly available exploit code against organizations that are yet to patch.



06

Beyond Ransomware, the Broader Cybercrime Landscape Continues to Flourish

The cybercrime landscape has always been diverse. While many groups have coalesced around lucrative ransomware operations, there remain other threats. Business email compromise and cryptojacking remain significant problems, as does significant levels of credential harvesting, providing fuel to the cybercriminal ecosystem.

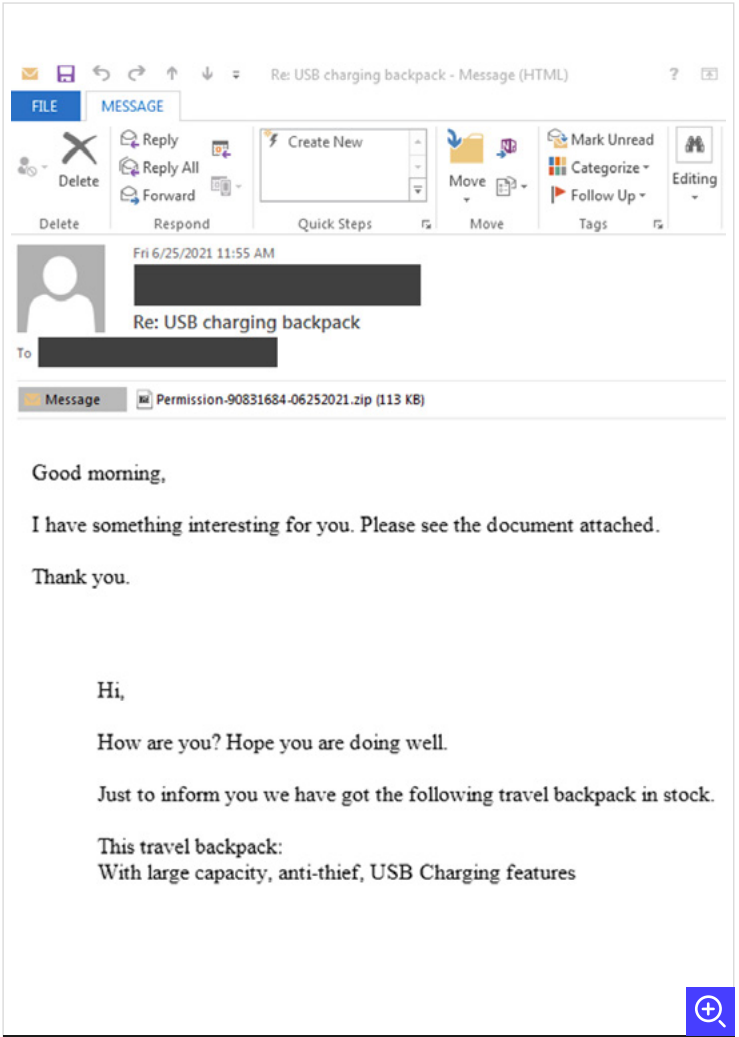
The past year has also been notable for the law enforcement fightback. Numerous attempts – some more successful than others – have been made to disrupt or destroy some of the key channels cybercriminals use to compromise their victims and make money.

Loaders and the Impact of Law Enforcement Takedowns

Whether the ultimate payload is ransomware or cryptominers, loader malware and botnets have always played a significant part in delivery. Emotet had long been one of the most prevalent and successful malware families affecting enterprise organizations, and it often provided the initial access point for ransomware groups. But in January 2021 the Emotet botnet disappeared, successfully disrupted by a collaborative effort between law enforcement agencies from the Netherlands, Germany, United States, United Kingdom, France, Lithuania, Canada and Ukraine in one of the most wide-reaching law enforcement actions against malware ever seen. Emotet disappeared and has not returned.

The successful disruption of Emotet left a vacuum. The loader ecosystem quickly moved to fill it. Botnets active in the past year have included IcedID, Chanitor, Cutwail, Dridex, QakBot, Flubot, and Teabot.

- **IcedID** in particular has increased its activity levels. Despite a month-long hiatus in June 2021, it has been widely distributed through multiple services, and many threat groups have leveraged the botnet to distribute Cobalt Strike.
- **Chanitor** has increased its distribution tempo to three to four campaigns per week, distributing Ficker Stealer and Cobalt Strike. This is likely now the largest botnet regularly distributing credential theft malware.
- **GOLD HERON** has used several spam services, including Cutwail, to distribute Dridex 2.0, Cobalt Strike, and ultimately DoppelPaymer and Grief ransomware.



Snippet of hijacked email thread delivering QakBot. (Source: Secureworks)

- **GOLD BLACKBURN**, at one point the largest customer of Emotet, has had no difficulty finding alternative distribution channels for TrickBot and BazarLoader. These malware families remain top sources of Conti and Ryuk ransomware infections. TrickBot has also re-implemented web injection capability signaling a possible return to high-value financial transaction fraud.
- **GOLD LAGOON**, like GOLD BLACKBURN, was also a customer of Emotet. It has continued operations since the takedown with Qakbot malware. It has used its own infrastructure to distribute Qakbot using familiar hijacking of reply-to chains in email spam campaigns.

In some cases where the victim is running Active Directory, Qakbot has been used to drop Cobalt Strike, which has then led to ransomware. Qakbot C2 infrastructure appeared to go down in early July 2021. Initially it appeared as if the disappearance might be permanent, but GOLD LAGOON restarted Qakbot activity in September 2021.

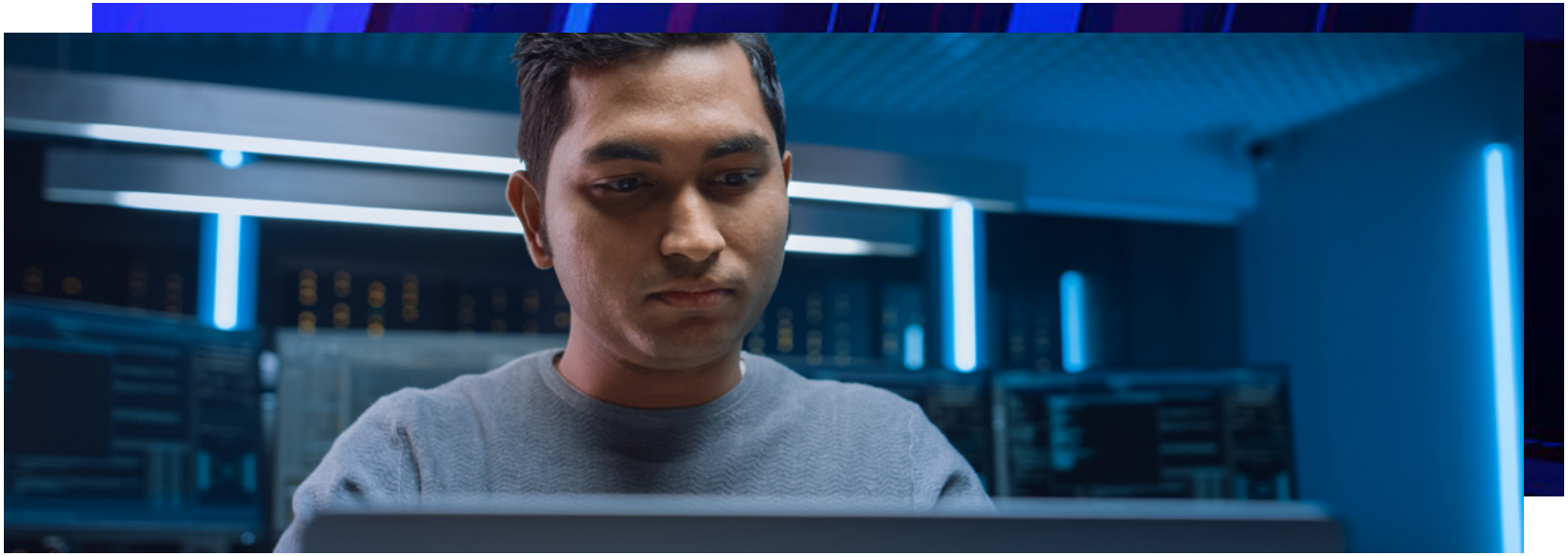
Increased law enforcement activity and collaboration with industry is undoubtedly a good thing. However, it remains challenging to deliver long-lasting change when the main players remain out of reach from more traditional law enforcement action. Inevitably, law enforcement action leads to evolution in the remaining botnet landscape and sometimes removing well-known well-understood capabilities makes it

Reconnaissance commands running on host infected with QakBot. (Source: Secureworks)

harder to detect threat actors as they move to new capabilities. Much like the security community, criminals will study the technical details of takedown operations and use that knowledge to make their own botnets more resilient.

For example, within a day of the Emotet takedown CTU researchers observed configuration changes in the Qakbot botnet operated by GOLD LAGOON. The fact that Emotet infrastructure was hosted in Western Europe made it easier for law enforcement to carry out a successful takedown. As a result, several botnet operators immediately moved their infrastructure into jurisdictions such as Russia to take them out of the reach of U.S. or European law enforcement.

Botnet operators are also writing variants of their loaders in different languages to help evade detection. Buer, originally written in C, now has a variant written in Rust. Others are developing new loaders in uncommon languages, for example NimzaLoader written in Nim. Other reasons for using new languages include: enhancing capabilities, frustrating malware analysis, and reviving old malware through new delivery mechanisms. Network defenders should mitigate the threat posed by malware written in uncommon languages by using tools with behavioral detections as well as static signatures.



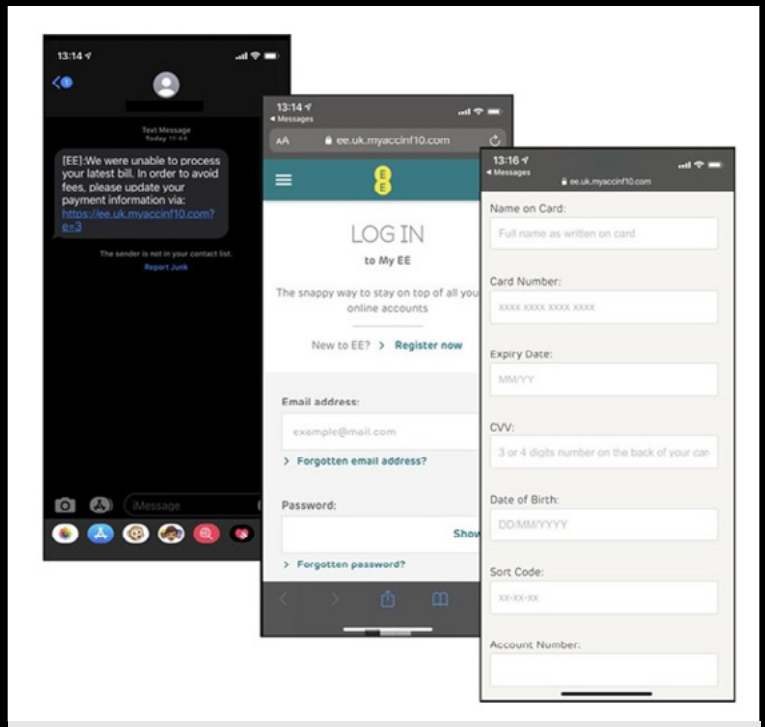
Mobile Botnets Take Shape

One further change comes from the growth of mobile botnets, particularly FluBot and TeaBot. These are primarily delivered via package delivery scam text messages (also known as SMS phishing or smishing), affecting users in Europe. With the growth in online shopping prompted by the COVID-19 pandemic, missed delivery texts are designed to elicit action from unsuspecting consumers. Spam campaigns have been constant (including over weekends) and the threat actors regularly updated both the malware and their infrastructure in order to reach different geographies.

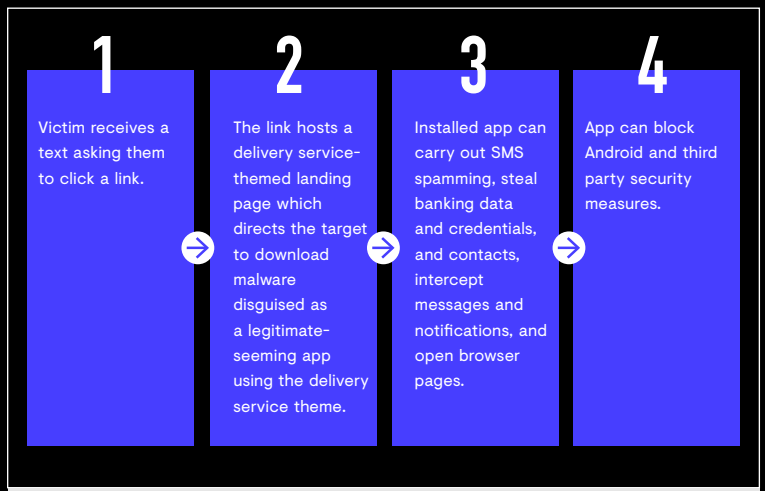
Victims receive a text requesting them to click a link. The link hosts a delivery service-themed landing page which directs the target to download malware disguised as a legitimate-seeming app using the delivery service theme. Once installed, the app can carry out SMS spamming, steal banking data, contacts and credentials, intercept messages and notifications, and open browser pages. It can also block Android security measures and prevent third-party security apps from being installed.

The Flubot botnet has also been observed distributing TeaBot malware.

Mobile malware continues to be dominated by Android malware, given its open nature compared to iOS's closed sandbox approach. With the exception of occasional highly-targeted zero-day exploits, malware continues to be a rarity on Apple's mobile devices.



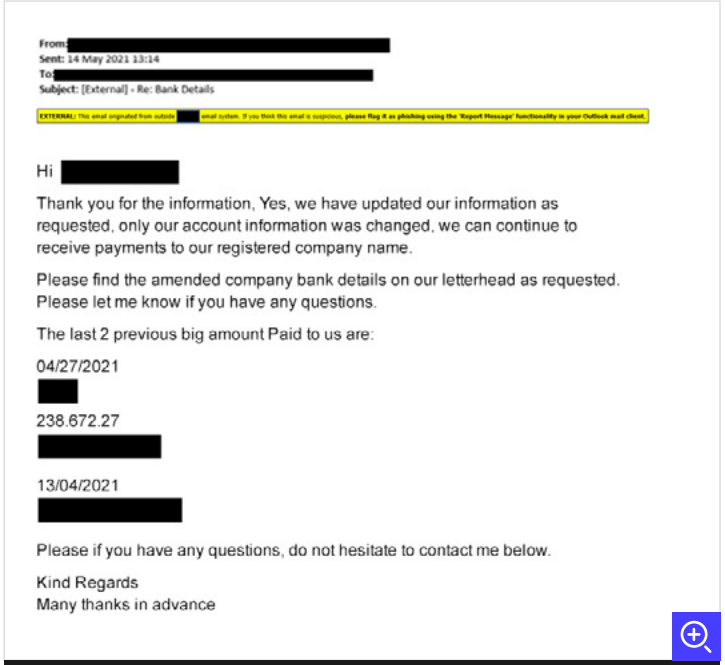
An example of a SMS lure. (Source: Secureworks)



Mobile botnet delivery

Business Email Compromise

While email account compromise doesn't grab the headlines in the same way that ransomware does, email account compromise remains highly prevalent and a lucrative source of revenue for cybercriminals. Malicious actors continue to compromise email accounts, monitor communications, and, when the time is right, inject themselves into a legitimate business transaction with a fake invoice. This entices unsuspecting billing departments to send large amounts of money to the wrong person.



From: [redacted]
Sent: 14 May 2021 13:14
To: [redacted]
Subject: [External] - Re: Bank Details

EXTERNAL: This email originated from outside [redacted] email system. If you think this email is suspicious, please flag it as phishing using the 'Report Message' functionality in your Outlook mail client.

Hi [redacted]

Thank you for the information, Yes, we have updated our information as requested, only our account information was changed, we can continue to receive payments to our registered company name.

Please find the amended company bank details on our letterhead as requested. Please let me know if you have any questions.

The last 2 previous big amount Paid to us are:

04/27/2021
[redacted]
238.672.27
[redacted]
13/04/2021
[redacted]

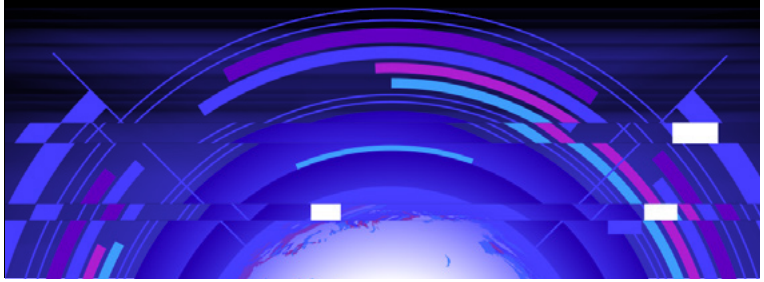
Please if you have any questions, do not hesitate to contact me below.

Kind Regards
Many thanks in advance

An example of a BEC phishing email. (Source: Secureworks)

In one BEC engagement in 2020, Secureworks assisted an organization where the victim clicked a link in a phishing email and entered their credentials on a fake Microsoft 365 login page. The attacker used the stolen credentials to access the victim's single-factor authentication email account and multiple email threads relating to payments and invoices. The threat actor then created forwarding rules to send all emails from that account to an attacker-controlled Gmail account. A day after the initial compromise, the threat actor registered a lookalike domain to spoof the victim's company and started attempting to change the destination of regular payments. Before the week was over, the attacker leveraged the existing email threads to send emails from the spoofed domain to other employees within the company and convince the victim to initiate wire transfers to attacker-controlled accounts.

In another incident, a threat actor convinced an individual to approve a large remittance to a fraudulent bank account. The initial compromise was again via a phishing email. The victim provided their email credentials, which gave the attacker access. Using that access, the threat actor created a forwarding rule to monitor incoming messages so they could identify messages pertaining to financial transactions. The investigation revealed logins to the victim's email account from IP addresses located in Dubai at the same time the legitimate user was logged in from a U.S.-based IP address.



FBI figures[16] covering both personal and business email compromise show a rise to $1.85 billion (USD) reported losses in 2020, up from $1.75 billion in 2019. That only includes losses in the U.S. The average wire transfer sum[17] requested in a BEC attack in early 2021 was $85,000 (USD). However, BEC threat actors are opportunists and will tailor their demands to the size of their victim, with the aim of making as big a gain as possible. In the example shown below the intended amount exceeded a million dollars (USD).

A BEC attack only requires access to email inboxes. With cloud-based email services, that can mean just a username and password, with no requirement to deploy malware or any other tools. Multi-factor authentication on email accounts is therefore an essential protection, as is something as simple as monitoring for changes on mail forwarding rules. There are often two victims in a BEC incident – the victim of the malware compromise, and the victim who loses money. A breach of the money-losing victim's network is not necessary, if you can compromise the mailbox of a business contact they interact with. That reinforces the importance of verifying business partners and having robust processes in place to validate new account details out-of-band.

Cryptojacking

With Bitcoin and other cryptocurrency prices reaching historic highs for much of 2021, illicit cryptomining attacks also remained attractive to criminal threat actors.

Although cryptomining malware may seem like more of a nuisance activity than a serious threat, and its share of attacks seen by incident responders is dropping, it should be taken seriously. Cryptomining attacks represent a threat actor being able to remotely execute code within your environment. That could just as easily result in ransomware or some other kind of threat if they decide that's a more lucrative option. Cryptomining can also have a significant financial impact when directed against cloud services, as threat actors can rapidly spin up new images to mine cryptocurrency, generating a huge bill for the affected organization.

COMMAND LINE

```
C:\Users\[redacted]\rhc.exe cmd /C "it_update -o
xmr-asia1.nanopool.org:14433 -u
[redacted]
[redacted] --tls --coin monero --max-cpu-usage 20 -B --donate-
level 1 -l log_it.txt --rig-id[redacted]"
```

Monero cryptocurrency miner launched using hidec program to hide console window. (Source: Secureworks)

07

Identity is King

The shift over the last decade towards globally accessible cloud-based resources was boosted by the COVID-19 pandemic. Workforces are often now fully remote, and the concept of a hard perimeter between an enterprise's resources and the big wide internet is gone. Many organizations now rely on identity federation for single sign-on across on-premises and cloud resources. Access to all an enterprise's systems and data is managed by a single authentication point. As a result, compromising the right identity – or worse, the systems verifying the identities – potentially gives a threat actor unfettered access to critical business data. Identity truly is the new perimeter.

The SolarWinds breach cast light on this increasingly important issue – how authentication mechanisms can be stealthily subverted to reach sensitive resources hosted on cloud services. In doing so, it revealed the fragility of cloud single sign on.

Having gained initial access via trojanized SolarWinds code, the **IRON RITUAL** group were able to completely bypass authentication controls in several of their victims by stealing SAML token-signing certificates or other secret key material. Their administrative access also allowed them to add new credentials, modify permissions to cloud applications, and evade multi-factor authentication by enrolling additional devices they had access to. It formed a striking, real-world example of a cross-domain compromise.

In one incident Secureworks responded to in December 2020, IRON RITUAL had added credentials to an Azure application. They then used those credentials for persistent access to the cloud environment, effectively creating a backdoored Azure application that gave access to email, chat messages, OneNote notebooks, SharePoint files, and security telemetry for alerts for suspicious account logins, likely to monitor for evidence that the unauthorized access was detected.

In this case, the targeted application was a backup application that already had an extensive set of permissions, but threat actors can also add new permissions to compromised cloud applications to gain increased access to resources.

Detection of this kind of activity once the threat actors hold the keys is extremely difficult. Organizations must focus on prevention or detecting intrusions earlier in the kill-chain before they compromise these critical assets. **The management of identity, secret keys and cross-domain trust is becoming an increasingly fundamental requirement for securing systems and data.**

Identity Abuse is Not New, But it is Evolving

Threat actors subverting authentication mechanisms is nothing new. In 2017 CTU researchers reported on **IRON TWILIGHT** abusing OAuth to retain access to targeted email accounts. Most on-premises network intrusions, whether they be ransomware or cyber espionage, have long involved credential theft that is then used for privilege escalation, lateral movement and data access.

It is likely that more adversaries will begin to adopt these techniques. As organizations increasingly move data and resources into cloud services, compromising the right user identities can potentially grant unfettered access to sensitive data and systems.

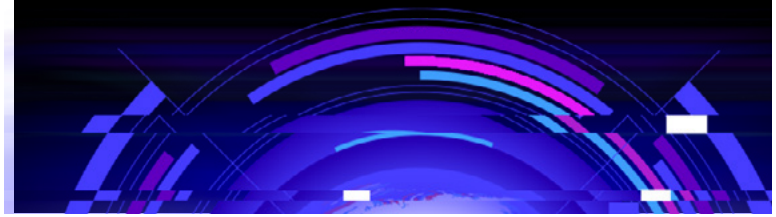
What Do I Need To Do?

It's increasingly important in the face of these identity-based threats that organizations understand the level of risk they face with centralized authentication systems and adapt their mitigation strategies accordingly. However, attacks that abuse application permissions or compromise authentication mechanisms are extremely difficult to detect, so the focus should be on protecting critical assets to prevent their compromise and detecting attackers earlier in the kill-chain before they can reach those critical assets.

Targeting MFA

One of the most important things that organizations can do to protect themselves against attacks is to implement multi-factor authentication. Inevitably, as a result, threat actors are trying to find ways to subvert MFA.

- Iranian threat group **COBALT ILLUSION** has used social engineering techniques to convince targets to divulge SMS codes and other multi-factor tokens to bypass MFA.
- A March 2021 Secureworks incident response engagement revealed how a threat actor used a loophole in the MFA implementation to bypass it. After accessing a Microsoft 365 email account with stolen or guessed credentials, the threat actor attempted to access an MFA-protected Citrix system. The MFA system had an option to send the MFA token to the user's email address, which was not protected by MFA, meaning it could be accessed with just a static password. This defeated the purpose of MFA, which should require access to a physical device such as a phone or token.
- 'Illicit consent attacks' have been explored, where a threat actor can create a malicious application that imitates a legitimate OAuth application. This can grant the threat actor a token which gives them long-term access to the user's applications if they authorize it, bypassing MFA.



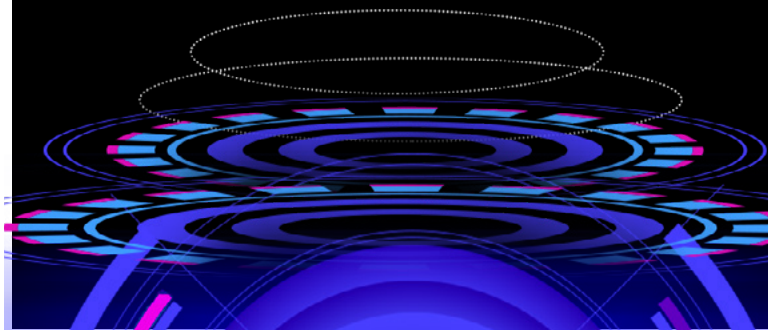
Identity federation and single sign-on are effectively based on a PKI-based trust model, so protecting the integrity of that trust is critical for all organizations. Private keys are used to sign assertions that say, 'I trust this user, and you trust me, so you can trust this user'. If those private keys are stolen, a threat actor can masquerade as any user and the trust relationship breaks down. Key management is a crucial aspect to securing that trust – making sure it's understood what your critical keys are, where they are stored, who has access to them, when they're changed. Systems storing critical keys should be hardened and segregated. Hardware Security Modules (HSMs) or software-based key management solutions can be leveraged. Private keys should be rotated if there is any suspicion they may have been compromised.

Detection of this type of threat requires threat analysts to be proficient in hunting through hybrid cloud identity systems. Detection relies on identifying unusual or anomalous behavior, which makes accurate signature-based detections very difficult. Expertise is required to understand what normal authentication events look like for that particular organization, and to find the small number of events that could be considered anomalous.

Preventing and Identifying Azure Compromises

To reduce risks resulting from the **compromise of Azure applications**, organizations creating applications should apply least privilege to ensure that the applications do not request excessive permissions. The permission requests should also use appropriate wording to ensure that users and administrators clearly understand what they are consenting to. Organizations that use Azure applications should remove unnecessary third-party applications from their environment and disable user consent where possible.

Application owners should monitor for "Update application - Certificates and secrets management" events in the Azure Audit Log or the legacy Unified Audit Log to identify suspicious activity. Organizations investigating potential application compromise should review Sign in logs for evidence of an application signing in from one or more previously unseen IP addresses. When investigating activities such as suspicious email access through the Mail.Read permission, organizations should review MailItemsAccessed events to identify the application ID used to access the user mailbox. This ID could reveal anomalous access to data that may indicate a compromised application.



08

State-Sponsored Threats: Targeted and Focused

In the aftermath of SolarWinds and HAFNIUM, state-sponsored threat activity replaced ransomware as the cyber threat that grabbed the most media attention. Perhaps that's why research findings[18] released by the Economist Intelligence Unit (EIU) and the Cybersecurity Tech Accord in February 2021 showed that a majority of businesses see state-sponsored cyberattacks as a major threat.

Hostile state-sponsored threat groups have relatively static, long-term intelligence requirements that are reflected in their targeting. Most hostile state actor activity is focused on accessing specific types of data or organizations, meaning that it is far less of a threat to most organizations than opportunistic cybercrime. The SolarWinds supply chain compromise that stole the headlines in December 2020 was a good example of this. In all cases where CTU researchers identified that customers had downloaded the trojanized SolarWinds update, IRON RITUAL deliberately removed its own access to those networks because its focus was purely on a very small and specific set of organizations, nearly all of them national security-related.

Not all cyber espionage attacks are the same. Different countries have different priorities that drive their espionage activities, and groups affiliated to different elements of the state apparatus within individual countries may have different priorities too.

Ad-hoc tasking may also lead to changes in activity types – for example espionage campaigns into COVID-19 research activities carried out by Russian, Iranian, Chinese and North Korean groups. In fact, throughout the year, all four of these major sponsors of APT activity were active.

Secureworks®

China

Sharing and Evolving Tactics

Main motivations:

- ⚠ Espionage
- ⚠ Intellectual Property
- ⚠ Theft

China

Chinese threat groups remain extremely active, with a continued focus on intellectual property theft, access operations against core telecommunications and internet infrastructure operators, and traditional espionage against political and military targets.

Chinese threat groups are demonstrating increased operational security and increased levels of coordination, including sharing of tools and exploits as well as extensive use of commodity tooling to make attribution more challenging. Likely as a result of organizational restructuring within the People's Liberation Army (PLA), some PLA-linked threat groups also appear to be practicing clearer deconfliction of operations, with an increased focus on specific geographies rather than on particular types of target organization.

In general, Chinese groups appear to have improved their operational security over the period, making detection of activity harder. They have used 'living off the land' (using tools already available in the target environment) more, and they have followed other countries in preferring openly available tools such as Cobalt Strike to bespoke tools. However, there have also been elements of business as usual. PlugX remains a popular tool with multiple groups, while BRONZE UNION continues its use of HyperBro.

Other observed Chinese threat group activity during the period has included:

- Ongoing targeting of near-neighbor countries that are part of the Belt and Road initiative, China's global infrastructure development investment strategy program.
- The use by **BRONZE PRESIDENT** of USB sticks to disseminate PlugX malware in October and November 2020. The November incident involved an updated version of PlugX that deleted older PlugX malware. This is not a new technique for the group – in early 2020 it had used USB drives in campaigns in Southeast Asia, particularly Myanmar. Secureworks has also seen it in use against international NGOs and food industry organizations, as well as in Thailand and Japan.
- The use by groups like BRONZE SPIRAL of small office and home office (SOHO) routers in the target country as the last hop of an attack. This makes attribution more difficult and also makes attack traffic look like it is terminating in the same country as the target, which might allow it to blend in as legitimate network traffic.

Optimizing Organizational Structures: Sharing Tools and Access?

On March 1, CTU researchers observed mass exploitation of on-premises Exchange Servers shortly before **Microsoft**[19] released out-of-band patches for those same zero-day vulnerabilities. **Related reporting**[20] indicated that the campaign had been ongoing in a less noisy fashion since at least January 2021.

The sudden increase in activity just before the vulnerabilities became public potentially indicated that the threat actors knew their access was about to be curtailed. Subsequent **reporting**[21] indicated that perhaps as many as ten distinct Chinese groups were leveraging the vulnerabilities to deploy web shells for ongoing access to targeted environments (see below).


```
{
    "Process": {
        "image_path": "C:\\Windows\\System32\\cmd.exe",
        "commandline": "\"cmd\" /c cd /d
\"C:\\\\inetpub\\\\wwwroot\\\\aspnet_client\\\\system_web\"&net group \"Exchange
Organization administrators\" administrator /del /domain&echo [S]&cd&echo [E]",
        "username": "NT AUTHORITY\\SYSTEM",
        "create_time": "2021-03-01T03:53:35.569496Z",
        "program_md5": "9a4D3grWD1sXuC8s1oQC/g==",
        "parent_image_path": "C:\\Windows\\System32\\inetsrv\\w3wp.exe",
        "was_blocked": false,
        "user_is_admin": true,
        "process_is_admin": true,
        "endpoint_platform": "PLATFORM_WINDOWS"
    },
    "ParentCreateTime": "2021-02-19T20:36:12.953916Z",
    "HostProgram": null,
    "TargetProgram": null,
    "Id": {
        "Process_Id": {
            "pid": 19336,
```


Threat actor leveraging Exchange zero-days to deploy China Chopper web shell. (Source: Secureworks)

In one case, CTU researchers observed the BRONZE UNION threat group using the Exchange vulnerabilities to re-gain access to an environment that they had recently been evicted from.

While the degree of sharing that took place during these intrusions was notable, it appears increasingly common. In fact, knowledge and tool sharing across Chinese APTs is not considered unusual, with groups using malware provided by the same 'Digital Quartermaster'. A Digital Quartermaster is thought to be an organization that develops, maintains and supplies malware to operational threat groups that are responsible for the intrusion activity.

There is also evidence of multiple groups sharing exploits prior to them being publicly available. This manifestation of closer tradecraft sharing is likely to be one result of the restructuring of the People's Liberation Army (PLA) that has been under way since late 2015. It is highly likely that similar levels of sharing are going on with groups connected to the Ministry of State Security (MSS), which also has a remit to conduct overseas cyber operations.

One example is ShadowPad, a modular remote access trojan (RAT) that can extract information about the host, execute commands, interact with the file system and registry, and deploy new modules to extend functionality. CTU researchers assess that ShadowPad is currently used by at least eight different Chinese threat groups against targets globally including the U.S. and UK. CTU researchers discovered that many of the threat groups observed using ShadowPad since the beginning of 2019 such as **BRONZE BUTLER** and **BRONZE HUNTLEY** have been linked to the Chinese PLA. Before 2019 only **BRONZE ATLAS**, a group operating on behalf of the MSS, leveraged the ShadowPad malware. Most recently, CTU discovered a sample linked to **BRONZE UNIVERSITY.**

Supernova

In a **November 2020**[22] incident response engagement, CTU analysts observed a likely China-based threat group leveraging SolarWinds software to deploy the SUPERNOVA web shell. Earlier in 2020, Secureworks incident responders identified similar intrusion activity on the same network. Analysis suggested that the threat actor initially gained access as early as 2018 by exploiting a vulnerable public-facing ManageEngine ServiceDesk server. attacker used their access to periodically harvest and exfiltrate domain credentials. In August 2020, the threat actor returned to the network via the ManageEngine ServiceDesk server, harvested credentials from two servers, likely exfiltrated these credentials through the ManageEngine server, and then used them to access files from Microsoft 365-hosted SharePoint and OneDrive services.

SUPERNOVA was publicly disclosed by **FireEye**[23] in December when it revealed details of its internal investigation of the compromise by the threat group that CTU researchers track as IRON RITUAL. But it was only later in December that it **became clear**[24] that SUPERNOVA was in fact the work of a different and unrelated group. Then, on December 24, 2020, SolarWinds confirmed that threat actors had exploited CVE-2020-10148, a SolarWinds Orion API authentication bypass vulnerability in its Orion Platform, to deploy SUPERNOVA.

CTU researchers track the operators of the SUPERNOVA web shell as **BRONZE SPIRAL**. The CTU team was initially unable to attribute the August activity to any known threat groups. However, similarities to the BRONZE SPIRAL intrusion in late 2020 suggest that the same threat group was responsible for both intrusions. These include use of identical commands, servers, working directories, and compromised administrator accounts.

The threat group also makes extensive use of native system tools and 'living off the land' techniques (see below) to enable long-term access to target networks and theft of intellectual property.

```
3       "image_path": "C:\\Windows\\SysWOW64\\cmd.exe",
4       "commandline": "cmd /c \"powershell /c \"$mypwd=ConvertTo-SecureString -String \\\"1234\\\" -Force
-AsPlainText;Get-ChildItem -Path cert:\\localMachine\\my| where {$_.Subject -like \\\"CN=SolarWinds-Orion\\\"}
| Export-PfxCertificate -FilePath C:\\inetpub\\SolarWinds\\license.txt -Password $mypwd\"&echo
AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&fsutil fsinfo drives>>C:\\inetpub\\SolarWinds\\license.txt&
tasklist /v>>C:\\inetpub\\SolarWinds\\license.txt&systeminfo>>C:\\inetpub\\SolarWinds\\license.txt&net
start>>C:\\inetpub\\SolarWinds\\license.txt&ipconfig /all>>C:\\inetpub\\SolarWinds\\license.txt&arp
-a>>C:\\inetpub\\SolarWinds\\license.txt&dir c:\\>>C:\\inetpub\\SolarWinds\\license.txt&dir
c:\\progra~1\\>>C:\\inetpub\\SolarWinds\\license.txt&dir c:\\progra~2\\>>C:\\inetpub\\SolarWinds\\license.txt&
echo AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&dir \"C:\\Documents and Settings\\All Users\\Start
Menu\\Programs\\Startup\">>C:\\inetpub\\SolarWinds\\license.txt&netstat -ano>>C:\\inetpub\\SolarWinds\\license.
txt&whoami /all>>C:\\inetpub\\SolarWinds\\license.txt&net localgroup
administrators>>C:\\inetpub\\SolarWinds\\license.txt&dir c:\\users\\>>C:\\inetpub\\SolarWinds\\license.txt&reg
query HKEY_LOCAL_MACHINE\\SOFTWARE>>C:\\inetpub\\SolarWinds\\license.txt&netsh firewall show
config>>C:\\inetpub\\SolarWinds\\license.txt&net use>>C:\\inetpub\\SolarWinds\\license.txt&dir
C:\\inetpub\\SolarWinds\\bin\\*logoimag*>>C:\\inetpub\\SolarWinds\\license.txt&echo
AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&type C:\\inetpub\\SolarWinds\\bin\\App_Web_logoimagehandler.
ashx.*>>C:\\inetpub\\SolarWinds\\license.txt&echo AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&type
C:\\inetpub\\SolarWinds\\bin\\logoimagehandler.ashx.*>>C:\\inetpub\\SolarWinds\\license.txt&echo
AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&\"",
```

BRONZE SPIRAL reconnaissance script using native system utilities. (Source: Secureworks)

Secureworks®

Iran

A Narrow Geographical Focus (For Now)

Main motivations:

- Espionage
- Monitoring dissidents
- Sabotage

Iran

Over the past year, Iranian threat groups have maintained a steady level of activity. Mainly this involved espionage and surveillance operations against individuals perceived as valuable information sources or potential threats to the Iranian regime, such as journalists, academics, human rights defenders, and employees of government, intergovernmental organizations (IGO), and non-governmental organizations (NGO). Iran's main focus has been the Middle East – Saudi Arabia, the United Arab Emirates (UAE), and Israel in particular – rather than Western organizations, reflecting its perception of the chief source of risk to its interests. With the election of the new hard-line president Ebrahim Raisi, its regional geographical focus may soon change.

Iran also carried out cryptographic wiper attacks masquerading as ransomware attacks. These primarily focused on Israeli targets but similar wiper attacks are also starting to be seen against the UAE, likely as a result of the recently formed political links between the UAE and Israel.

In the past year, CTU researchers analyzed incidents including:

- **COBALT FOXGLOVE** using a compromised Citrix server for entry, deploying the Ngrok tunneling tool to add an additional access mechanism to the environment.
- **COBALT ULSTER** carrying out spear phishing campaigns targeting Iraqi and Turkish organizations using humanitarian and COVID-19-related themes during May and June 2020.
- **COBALT EDGEWATER** using employment-themed lures to target entities in Lebanon using MailDropper malware, which uses mailboxes to relay C2 messages. A 2020 MailDropper campaign used a mailbox at the Lebanese Directorate of General Security. Campaigns in 2021 used mailboxes associated with the Lebanese Army and a leading Lebanese mobile telecom network operator. Threat actors could leverage these mailbox compromises to conduct broader intrusions into these networks.

Lure documents associated with COBALT ULSTER. Source: Secureworks

CTU researchers also investigated a May 2021 phishing campaign carried out by **COBALT ILLUSION** that used the legitimate Dropbox online file-hosting platform to evade email security controls. The campaign involved phishing activity targeting a European nation's Ministry of Foreign Affairs, an intergovernmental organization (IGO), and government employees in Israel. It is likely that other organizations were also targeted. At least one targeted individual had prior links to Iran.

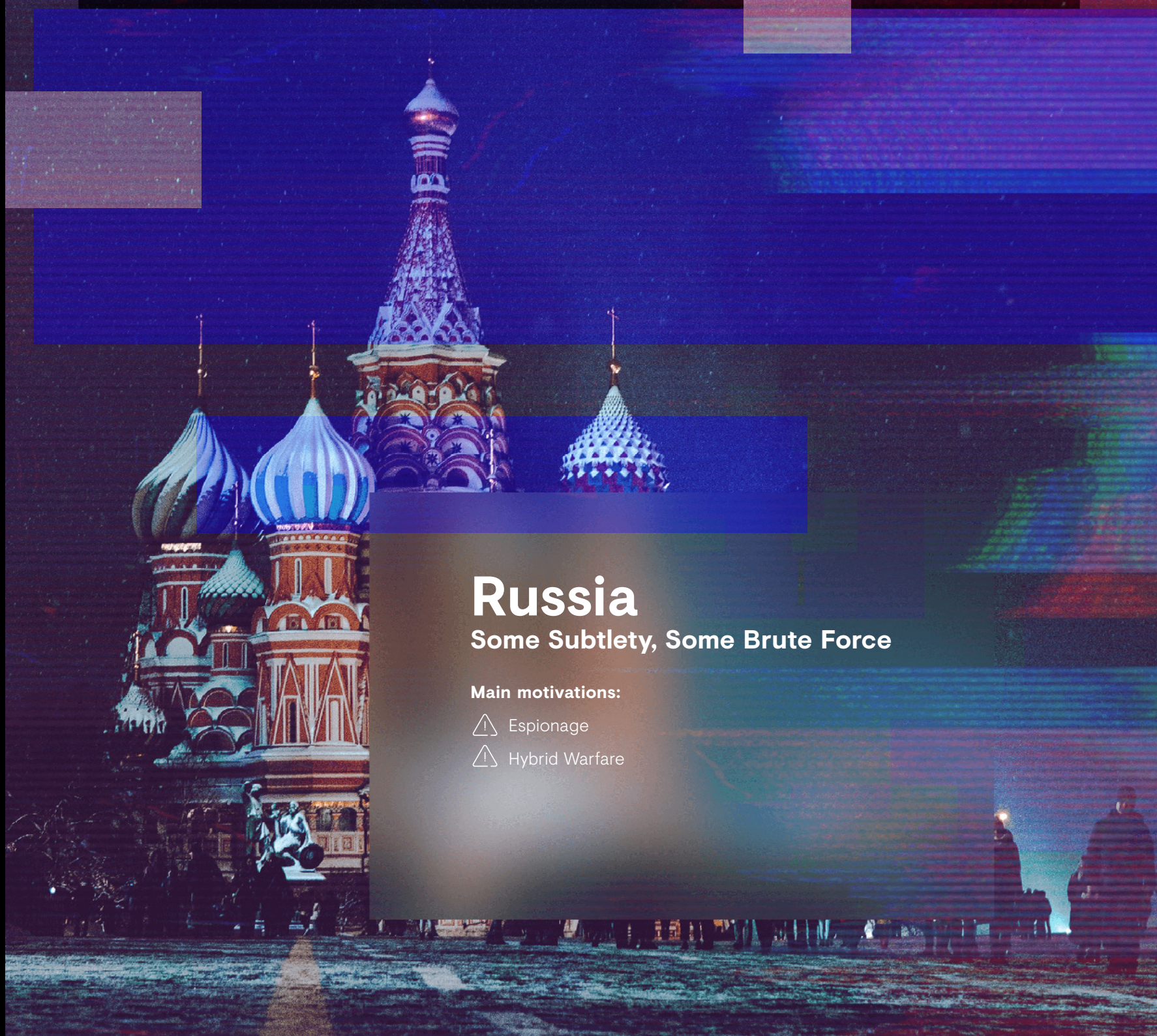
COBALT ILLUSION usually follows a well-worn playbook in its phishing operations, appearing to pay limited attention to operational security and taking few measures to prevent their infrastructure from being identified and tracked. CTU researchers advise that customers who think they might be a target of Iranian groups review available log data for interactions with COBALT ILLUSION phishing infrastructure. Deploying multi-factor authentication MFA adds additional protection, although COBALT ILLUSION has previously attempted to convince targets to divulge SMS codes and other multi-factor tokens to bypass this security control.

Several groups have continued Iran's association with wipers and ransomware:

- The 'PowGoop' downloader linked to Thanos ransomware attacks against state-run organizations in the Middle East showed coding overlaps with tools seen by Secureworks during previous incident response engagements involving COBALT ULSTER. This raised the possibility that COBALT ULSTER could have facilitated the ransomware attacks by providing network access to another threat actor. Victims included a state-owned oil and gas producer based in Sharjah, United Arab Emirates, and a governmental agency in Egypt. If Iranian state-sponsored actors were involved in these incidents, it would suggest the attacks were designed more for sabotage than financial gain.
- Analysis of the N3tw0rm ransomware and ransom note observed in attacks against Israel in April 2021 indicates links to the Pay2Key ransomware, which was used in 2020 operations that also focused on Israel. CTU researchers link Pay2Key to COBALT FOXGLOVE. N3tw0rm attacks use name-and-shame tactics including bulk data theft and publication of victim names. The impacted organizations operate in Israel in the logistics, retail, and engineering verticals. CTU analysis suggests that the targeting is likely opportunistic but focused on entities that are geographically located in Israel.

Although these activities look superficially like ransomware, they are probably not what they seem. CTU researchers believe that N3tw0rm and Pay2Key are used in Iranian state-sponsored operations but are designed to look like cybercrime attacks to misdirect attribution. Any resulting financial gain may be a secondary benefit. Low value ransom demands may be designed to encourage victims to pay quickly, but the threat actors probably do not plan to provide a decryptor. In this model, the threat actors use the ransomware as a cryptographic wiper and achieve the dual purpose of data destruction and financial gain. A similar approach seems to be in use by the Agrius or Black Shadow group that attacked businesses in the insurance and finance sectors in Israel in late 2020 and in 2021. It has also been seen using a type of wiper malware previously seen in use by threat actors connected with **COBALT GYPSY**.

Secureworks®



Russia

Some Subtlety, Some Brute Force

Main motivations:

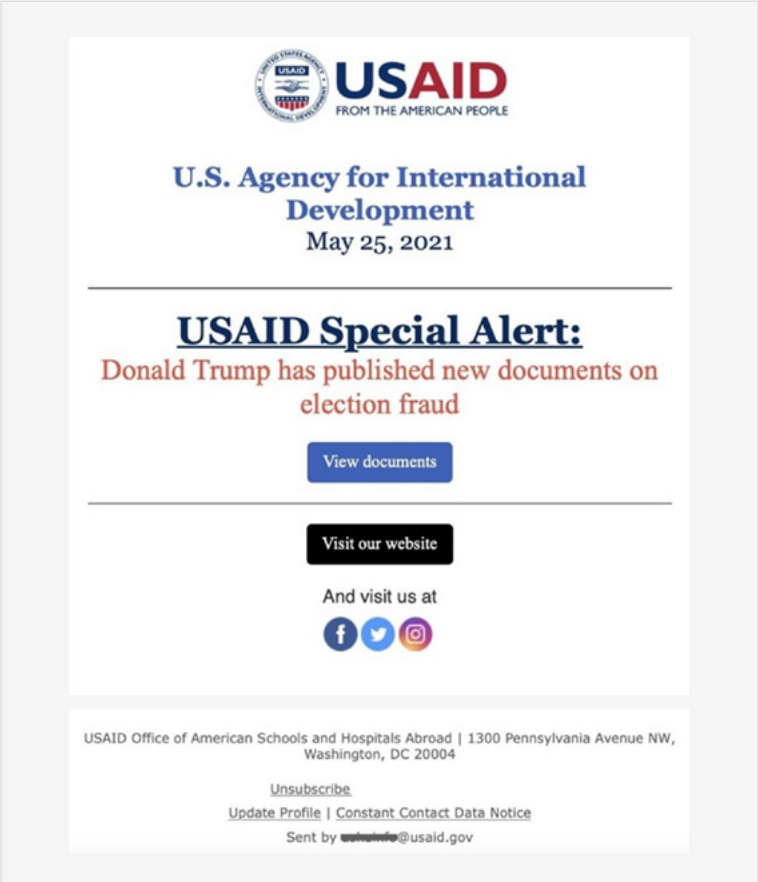
- ⚠ Espionage
- ⚠ Hybrid Warfare

Russia

Russian cyber espionage activity has been under the spotlight during the period, with **IRON HEMLOCK's** network intrusions targeting COVID-19 vaccine development, U.S. indictments against six GRU officers associated with the **IRON VIKING** threat group, and extensive media reporting of IRON RITUAL's SolarWinds supply chain attack.

Despite the number of headlines, Russian threat group activity continues to be narrowly focused against traditional espionage targets such as government, non- and inter-governmental organizations (NGOs and IGOs), policy and think tanks, and related supply chain organizations. Nowhere was this better illustrated than with the SolarWinds campaign, where CTU researchers observed IRON RITUAL deliberately and permanently disabling their own access to all Secureworks customers who had downloaded the trojanized SolarWinds code, presumably on the basis that they were not deemed to be relevant to their goals and they wanted to minimize the chances of detection.

IRON RITUAL itself also carried other, somewhat less sophisticated attacks. One example was a U.S. Agency for International Development (USAID)-themed phishing campaign[26] targeting governmental, non-governmental organizations (NGOs), and intergovernmental organizations (IGOs) based in the United States, Ukraine, and the European Union. A second campaign targeted IT companies, government bodies, NGOs, think tanks, and financial services in the U.S., UK, Germany, Canada, and 32 other countries using password-spraying and brute force attacks.



USAID-themed phishing email. (Source: Secureworks)

Despite similar targets, the TTPs used in these campaigns were considerably less sophisticated than those used in the SolarWinds campaign and far more easily detected. The USAID phishing activity was high volume, noisy, and required a user to perform a series of actions before malware could be installed to provide ongoing access to the machine. The second campaign involved spraying large numbers of username and password combinations in an attempt to guess login credentials, and was assessed by Microsoft to have been largely unsuccessful.

A lack of subtlety also marked other elements of other Russian state-sponsored activity observed over the period. This included **IRON LIBERTY**[27] targeting[28] U.S. government and aviation networks in September 2020. Tactics used included brute-force password attacks, SQL injection, domain spoofing of legitimate aviation and government organizations, spear phishing, strategic web compromises, and harvesting NTLM credentials. Vulnerabilities that were reportedly leveraged affected Citrix Netscaler (CVE-2019-19781), Microsoft Exchange (CVE-2020-0688), Exim (CVE-2019-10149), Fortinet VPN (CVE-2018-13379), and Windows NetLogon (CVE-2020-1472).

However, not all Russian threat groups have continued to rely on historic tried-and-tested techniques. In July 2021, U.S. and UK security agencies released a joint advisory[29] about IRON TWILIGHT's use of a Kubernetes cluster to conduct distributed brute-force attacks against Microsoft 365, on-premises email servers, and other service providers. The use of an attacker-owned Kubernetes cluster is notable, as it offers automation, scalability, and the ability to redeploy infrastructure rapidly and easily across various commercial providers to evade IP-based blocking.

Secureworks®

SolarWinds - Sunburst to SAML

On December 13, 2021, news broke of a sophisticated supply chain compromise that used trojanized SolarWinds Orion platform software updates to carry out cyber espionage activities. Targets were primarily organizations in the U.S. government, political and research verticals, and their supply chain organizations including cybersecurity vendors and technology providers. The attack was carried out by IRON RITUAL (also known as NOBELIUM), a state-sponsored Russian threat group operating on behalf of the SVR, Russia's foreign intelligence service.

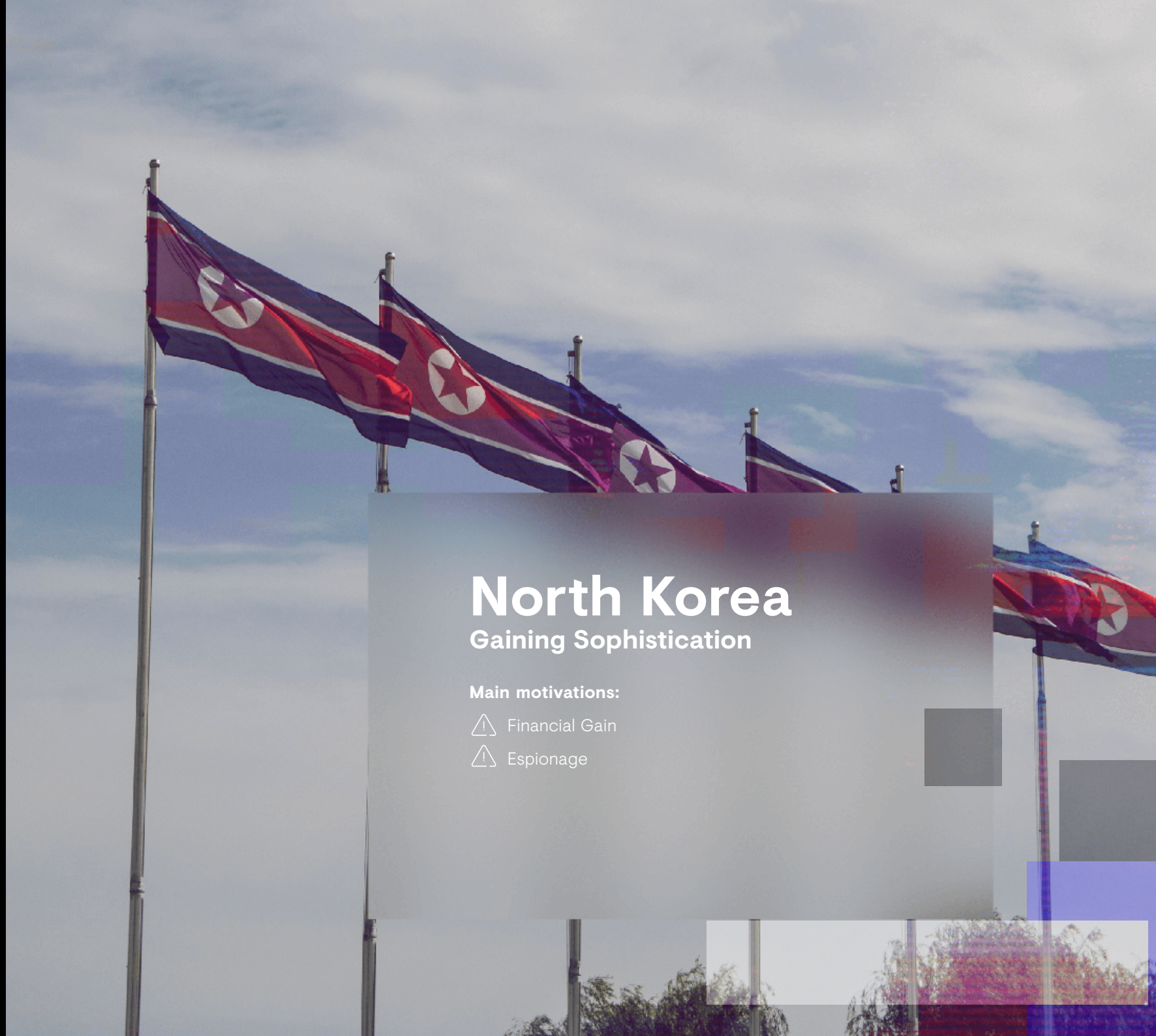
The customized nature of tools and techniques used in IRON RITUAL operations has meant that CTU researchers have been unable to definitively link the threat group with another SVR-linked group, IRON HEMLOCK (also known as The Dukes or APT29), the group responsible for the compromise of the U.S. Democratic National Committee's network in 2016.

IRON RITUAL used malware including the SolarWinds Orion-based SUNBURST backdoor as well as in-memory Cobalt Strike, delivered using the TEARDROP and RAINDROP loaders. While trojanized SolarWinds code was one method of access, the threat actor also used other methods to achieve and maintain persistent access to target environments. They demonstrated a capability to pivot from traditional on-premises network compromise to cloud-based resources.

While as many as 18,000 organizations received the trojanized SolarWinds software, only a fraction of those saw any follow-on activity that would indicate that they were objects of interest to the threat actor. In the vast majority of cases the threat actors instructed the SUNBURST backdoor to permanently stop communicating, thereby removing their own access to compromised systems. The White House **estimated**[25] that nine federal agencies and 100 private organizations experienced follow-on activity, all of whom were in the government or political spheres and their supply chains.

The ratio of organizations compromised by SUNBURST to those that experienced follow-on activity emphasizes the importance of understanding threat actor intent. It became clear fairly quickly during the SolarWinds revelations that only a small number of organizations affected by the SolarWinds issues were genuine targets of the threat actor.

Secureworks®



North Korea

Gaining Sophistication

Main motivations:

- Financial Gain
- Espionage

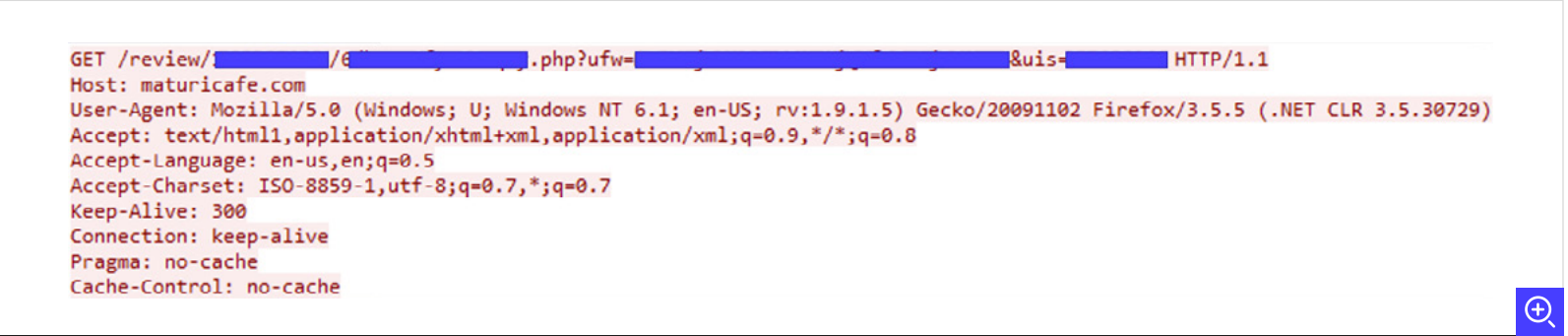
North Korea

North Korea's cyber operations continued to gain in sophistication over the period, although they still lag behind Russia and China. North Korean groups continued to prioritize specific organizations and individuals involved in defense, government and security research in South Korea and the U.S.. Other targets included those in neighboring East Asian countries, especially Japan. The targeting of entities in Russia, Israel and India was also observed.

Unlike other nation state cyber operations, North Korea places a strong emphasis on revenue generation. This was in evidence before the coronavirus pandemic when the country needed to address the economic damage caused by UN sanctions in response to North Korea's nuclear weapons program. It is even more of a focus now as it deals with the crippling impact of its border closure with China – by far its largest trading partner – to limit the spread of the disease. North Korean state groups have used ransomware, cryptocurrency thefts and manipulation of the global financial system, such as SWIFT, in pursuit of topping up ailing state bank accounts. This motivation to make money places North Korean targeting more in line with some cybercrime groups than other hostile nation states. Companies that are not traditional nation-state APT targets could find themselves in the sights of these groups.

Organizations involved in defense research, particularly those in South Korea, continue to be a top target for espionage-focused North Korean threat groups. Individual defense contractors have also been targeted with lure documents that deploy malware. A campaign by the **NICKEL ACADEMY** group used social engineering techniques to target security researchers[30], possibly in the hope of obtaining zero-day vulnerabilities that could be used in their attacks.

In late 2020, North Korean groups also targeted[31] organizations involved in COVID-19 vaccination research. Based on tactics observed by CTU researchers, the NICKEL HYATT, NICKEL ACADEMY, and NICKEL KIMBALL threat groups have all been involved in such activity. The public position of the North Korean regime is that there have been no

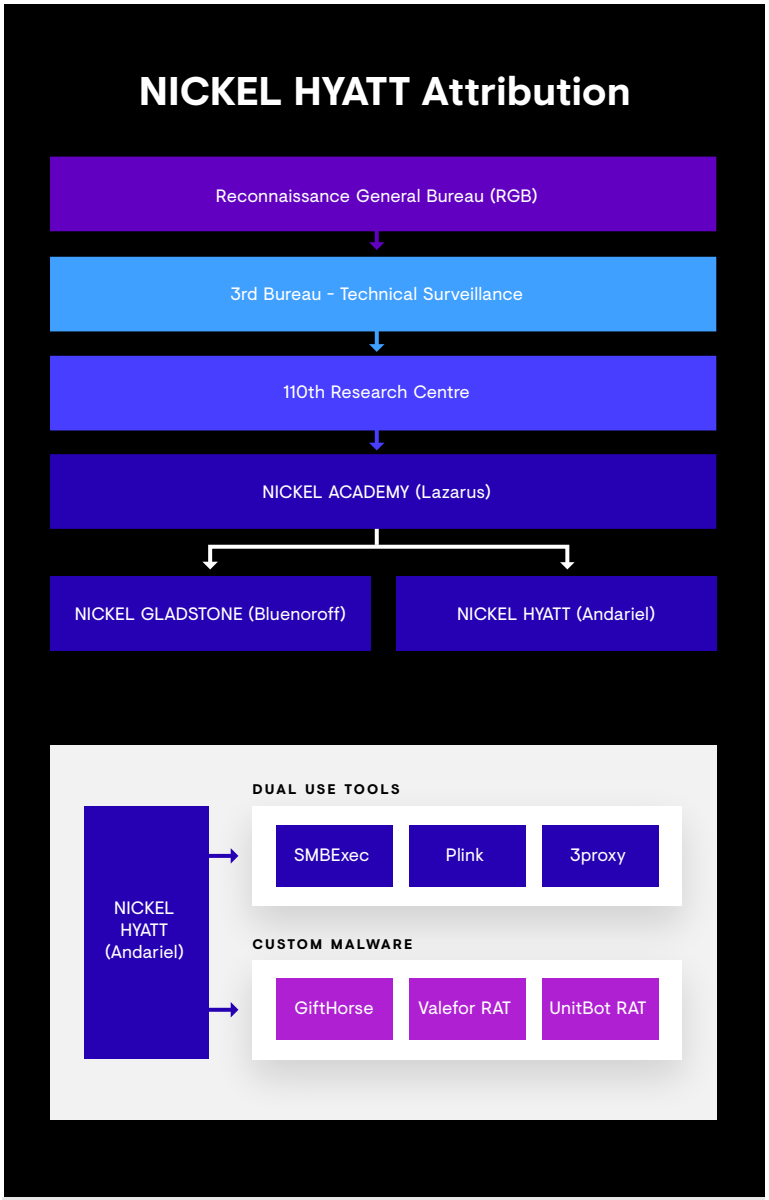


A network traffic excerpt from a NICKEL HYATT engagement. (Source: Secureworks)

COVID-19 cases in North Korea, and it has turned down offers of vaccines from Russia. However, while some crossover in operational objectives between threat groups is expected, efforts by these three normally separate groups could indicate that the North Korean government set this specific espionage objective as an overarching priority.

In one example, Secureworks incident responders found evidence that NICKEL HYATT compromised a life sciences company in East Asia in Q3 2020. This life sciences company had been known to be working on COVID-19 vaccine development and manufacturing. The threat actors obtained initial access by compromising a managed service provider and then leveraged a jump host intended for remote administration of the network. The intrusion was detected at an early phase, and initial data exfiltration was limited to network enumeration-related log data. Tools used during the intrusion included some seen in previous NICKEL HYATT engagements as well as others new to our observations of their activity.

Cryptocurrency heists were another way for North Korean groups to steal money. U.S. authorities reported in February 2021 that North Korean threat groups had targeted organizations for cryptocurrency theft in over 30 countries in 2020 alone. North Korea has used AppleJeus malware disguised as cryptocurrency trading platforms since at least 2018 and have also been seen employing TFlower ransomware for economic gain.



NICKEL HYATT Attribution. (Source: https://home.treasury.gov/news/press-releases/sm774)

09

The Pervasiveness of Cobalt Strike

Between January and July 2021, Cobalt Strike featured in 19 percent of network intrusions investigated by Secureworks incident responders, including ransomware groups and other financially-motivated criminals as well as state-sponsored actors from Russia, China, Iran and more. Why has this tool become so pervasive?

Cobalt Strike is a ubiquitous penetration testing toolkit available under a commercial licensing model. Developed for teams conducting authorized security assessments, it can be used for command and control, lateral movement, persistence, privilege escalation, and defensive evasion. Since its initial release in 2012, Cobalt Strike remains under active development and is currently on version 4.4. Unfortunately, what works well for red teams works equally well for threat actors.

There are a number of reasons why 'Offensive Security Tools' (OSTs), and particularly Cobalt Strike, have become so popular with threat actors:

Minimal development cost. There is a healthy community of security professionals spending considerable time developing commercial products like Cobalt Strike and open source OSTs. If a threat actor can obtain a cracked version of Cobalt Strike – and a large number can – then they benefit from all the development time, cost and expertise that has gone into it.

Easy to use. Years of customer feedback and software development mean that Cobalt Strike is optimized for ease of use, including verbose user documentation, blogs, and videos.

Fully featured. Because it has been developed as a one-stop-shop for post-exploitation activity, Cobalt Strike incorporates functionality that otherwise could only be leveraged by deploying multiple tools. Other public C2 frameworks attempt to emulate this range of functionality, but very few manage to do so or are so well established.

Hard to attribute. A threat group using custom malware and bespoke tactics is much easier to identify from technical artifacts than one that is using openly available tools with standard configurations.

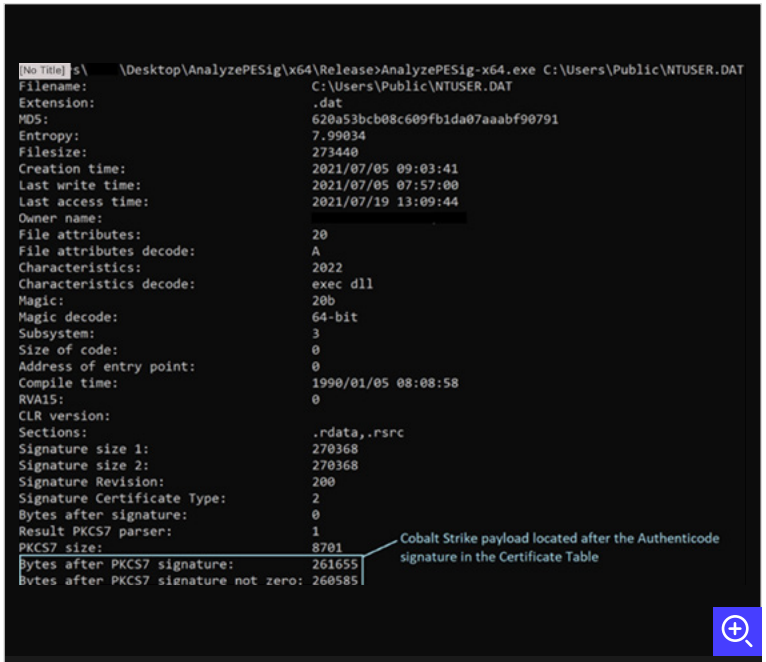
In many cases, threat actors deploy Cobalt Strike using out-of-the-box configuration options. However, CTU researchers have observed some threat actors employing notable methods of loading or using Cobalt Strike:

- The Vietnamese threat group **TIN WOODLAWN** authored a custom stager that CTU researchers dubbed[32] 'CommaChameleon' because it uses '-comma' as the PowerShell command-line switch. The stager waits for an encrypted payload to be written to a named pipe that it creates, and then injects the payload into a legitimate Windows executable.

- The BRONZE ATLAS threat group used a custom loader that exploited a 2013 vulnerability[33] with an opt-in fix to reflectively load a Cobalt Strike raw stageless payload artifact[34]. The data that the payload was extracted from was embedded after the Authenticode signature within the Certificate Table of a signed Windows DLL file. BRONZE ATLAS has also used legitimate 'function-as-a-service' platforms such as Cloudflare Workers to redirect Cobalt Strike traffic to their C2 servers. Criminal groups have been reported[35] to use the same tactic.

- The leak, allegedly by a disgruntled affiliate, of playbooks and tools provided to affiliates of GOLD ULRICK revealed a number of custom 'Aggressor Scripts[36], largely comprised of OSTs. These scripts are intended to make it easier for affiliates to conduct network intrusions using GOLD ULRICK's Conti ransomware.

Threat actors will always look to make use of tools that are widely available, especially where they offer the kind of benefits that Cobalt Strike provides. Mitigating the threat posed by Cobalt Strike and other OSTs requires comprehensive instrumentation across the environment, particularly on servers and user endpoints, so that activity can be detected early.



Cobalt Strike payload embedded in Windows DLL file with a valid digital signature. (Source: Secureworks)

10

Conclusion — The Continuing Importance of Fundamentals

New brands, new tools, new leak sites: In some ways the ransomware landscape has changed over the past year. In other ways it hasn't. Ransomware-as-a-service remains an important model, driving scale in terms of numbers of attacks. Attacks remain primarily opportunistic, thanks to initial access broker use of scan-and-exploit. Increasingly assertive law enforcement activity against ransomware groups has won some battles but the war continues to rage.

2021 also saw a significant increase in the use of zero-day exploits, with the total by the middle of the year greatly exceeding the total for all of 2020. Threat actors of all types also continued to exploit vulnerabilities long after patches were available, exploits were publicly disclosed, and compromises were widely reported.

State-sponsored threat activity remains narrowly targeted but often drives the focus of security practitioners and the media alike. The way in which the SolarWinds breach cast light on how threat actors can subvert authentication mechanisms to reach sensitive resources hosted on cloud services is a case in point.

Fortunately, good fundamental security practice, such as regular patching, the use of strong authentication, including MFA, and implementing the principle of least privilege are non-negotiables.

These essential controls should be coupled with thorough monitoring and detection of endpoints and network assets. There are certainly many additional opportunities to increase security by collecting and reviewing other essential telemetry such as identity, application and cloud logs, and data from email appliances, etc., which are often overlooked.

No security program is complete without regular adversary testing to bring to light any immediate gaps in your security controls while allowing you to test your incident response preparedness.

All these initiatives, along with a risk-based approach, provide valuable protection against financially motivated and state-sponsored threat actors alike.

1 **Ransomware Evolution**
https://www.secureworks.com/research/ransomware-evolution

2 **Avaddon Ransomware Shuts Down and Releases Decryption Keys**
https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

3 **F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat**
https://www.nytimes.com/2021/06/04/us/politics/ransomware-cyberattacks-sept-11-fbi.html

4 **Ransomware Attacks 'Are Here to Stay,' Commerce Secretary Says**
https://www.politico.com/news/2021/06/06/ransomware-attacks-commerce-secretary-492005

5 **A Trickbot Assault Shows US Military Hackers' Growing Reach**
https://www.wired.com/story/cyber-command-hackers-trickbot-botnet-precedent/

6 **New Action To Combat Ransomware Ahead Of U.S. Elections**
https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

7 **World's Most Dangerous Malware Emotet Disrupted through Global Action**
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

8 **IcedID Stealer Man-in-the-browser Banking Trojan**
https://blog.cyberint.com/icedid-stealer-man-in-the-browser-banking-trojan

9 **Top Routinely Exploited Vulnerabilities**
https://us-cert.cisa.gov/ncas/current-activity/2021/07/28/top-routinely-exploited-vulnerabilities

10 **What's Behind The Explosion in Zero-Day Exploits?**
https://www.itpro.co.uk/security/zero-day-exploit/360447/why-zero-day-exploits-are-surging-on-an-unprecedented-scale

11 **Remediation Steps for the Microsoft Exchange Server Vulnerabilities**
https://unit42.paloaltonetworks.com/remediation-steps-for-the-microsoft-exchange-server-vulnerabilities/

12 **Microsoft: 92% Of Vulnerable Exchange Servers Are Now Patched, Mitigated**
https://www.zdnet.com/article/microsoft-92-of-vulnerable-exchange-servers-are-now-patched-mitigated/

13 **Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities**
https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft

14 **Microsoft IOC Detection Tool for Exchange Server Vulnerabilities**
https://us-cert.cisa.gov/ncas/current-activity/2021/03/06/microsoft-ioc-detection-tool-exchange-server-vulnerabilities

15 **Prometei Botnet Exploiting Microsoft Exchange Vulnerabilities**
https://www.cybereason.com/blog/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities

16 **Internet Crime Report 2020**
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

17 **Phishing Activity Trends Report**
https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

18 **Securing a Shifting Landscape: Corporate Perceptions of Nation-State Cyber-Threats**
https://eiuperspectives.economist.com/technology-innovation/securing-shifting-landscape-corporate-perceptions-nation-state-cyber-threats

19 **HAFNIUM Targeting Exchange Servers With 0-day Exploits**
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

20 **Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities**
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

21 **Exchange Servers Under Siege From at Least 10 Apt Groups**
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

22 **SUPERNOVA Web Shell Deployment Linked to SPIRAL Threat Group**
https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group

23 **Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor**
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

24 **Analyzing Solorigate, the Compromised Dll File That Started a Sophisticated Cyberattack, and how Microsoft Defender Helps Protect Customers**
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

25 **Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021**
https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/

26 **New Nobelium Activity**
https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

27 **Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets**
https://us-cert.cisa.gov/sites/default/files/Joint_CISA_FBI_CSA-AA20-296A__Russian_State_Sponsored_APT_Actor_Compromise_US_Government_Targets.pdf

28 **Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets**
https://us-cert.cisa.gov/sites/default/files/Joint_CISA_FBI_CSA-AA20-296A__Russian_State_Sponsored_APT_Actor_Compromise_US_Government_Targets.pdf

29 **Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments**
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

30 **Update on Campaign Targeting Security Researchers**
https://blog.google/threat-analysis-group/update-campaign-targeting-security-researchers/

31 **Exclusive: Suspected North Korean Hackers Targeted COVID Vaccine Maker AstraZeneca**
https://www.reuters.com/article/idUKKBN2871A2

32 **Detecting Cobalt Strike: Government-Sponsored Threat Groups**
https://www.secureworks.com/blog/detecting-cobalt-strike-government-sponsored-threat-groups

33 **Microsoft Security Bulletin MS13-098 - Critical**
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-098

34 **What is a Stageless Payload Artifact?**
https://blog.cobaltstrike.com/2016/06/15/what-is-a-stageless-payload-artifact/

35 **Big Game Hunting: Now in Russia**
https://blog.group-ib.com/oldgremlin

36 **Aggressor Script**
https://www.cobaltstrike.com/aggressor-script/index.html

About Secureworks

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

For more information,call **1-877-838-7947** to speak to a Secureworks security specialist or visit **secureworks.com**

Secureworks®