CYBERCRIME TRENDS AND HIGHLIGHTS
Q3 - OCTOBER 2021

Arete

For Every Action, There Is an Equal and Opposite Reaction

For Every Action, There Is an Equal and Opposite Reaction

Threat actors react to the actions of their targets as governments and law enforcement agencies seek to protect those targets.

From Q2 to Q3 2021, ransomware gained increasing attention. The government labeled it a national security threat and bolstered efforts to topple top targets, such as REvil/Sodinokibi. The heightened government focus on this group — known for the far-reaching supply chain attack against Kaseya — likely led to law enforcement action, the disappearance of the group's spokesperson "Unkn", the re-appearance of the developers, further enforcement action, and the group's final shutdown.

Unfortunately, REvil/Sodinokibi was not the only highly active group this quarter. While REvil/Sodinokibi may have stolen major media headlines for its massive ransom demands and disappearing acts, Conti exploded onto the scene in Q3 2021 with a consistent cadence of attacks. Its lesser media attention did not stem from increasing ransom demands — those remained relatively steady — but rather, disgruntled affiliates leaking sensitive operation details, including the tactics, techniques, and procedures (TTPs) of Conti ransomware partners. And most recently, in mid-October, Conti released a statement, accusing the United States of "bandit mugging" and comparing U.S. law enforcement's efforts to target groups like REvil/Sodinokibi to U.S. military action in Afghanistan and Iraq.

In Q3 2021, threat actors also continued mass exploitation of vulnerabilities in systems, including those in Microsoft Exchange.

Overview

Q3 2021 HIGHLIGHTS FROM ARETE'S INCIDENT RESPONSE CASES[1]

- Conti takes double extortion techniques a step further, destroying backups to pressure victims into paying ransoms faster.
- REvil/Sodinokibi: Now you see them, now you don't. The group hit hard with a massive supply chain attack, disappeared, reappeared, and went dark once again.
- LockBit 2.0 encrypts faster than any other ransomware variant in the wild — but also pledges to follow a "moral code."

OTHER KEY CYBERSECURITY EVENTS IN Q3 2021

- Early frost hits the cybercrime ecosystem: Data leaks by Conti and Babuk affiliates.
- The ProxyShell exploits: Actors continue to target vulnerabilities that allow them to easily and consistently gain access to victim networks.
- The Karakurt Team is among several new-to-the-scene cyber actors who have adopted the "vintage" extortion-only technique to demand ransom payments from victims.
- Government action could impact the future of Ransomware as a Service (RaaS).

WHAT TO EXPECT

- Expect to see multi-layered, large-scale exploits — for examples, ProxyShell and Kaseya VSA — continue to rise in popularity amongst actors.
- Expect to see threat actors continue to specialize and focus on one aspect of the infection chain, for example, proxy infrastructure or initial infection.
- Expect to see an increase in extortion-only activity driven by multiple factors, including the new view of ransomware as a national security threat along with RaaS operations closing down.
- Expect to see threat actors leverage the same playbook and tooling from victim to victim, thus facilitating actor or group attribution.

Conti
Ups the ante by deleting backups

The Russian-speaking Conti ransomware group has targeted more than 400 organizations worldwide[2], primarily in the healthcare, law enforcement, biotech, critical infrastructure, and engineering sectors, where the need to restore operations is critical if not life-threatening.

While the group has often used double extortion (combining encryption and exfiltration) techniques to demand ransoms upwards of US$25M, it has recently turned to a new tactic to force a victim's hand by destroying a victim organizations' backups — further increasing pressure for prompt payment of ransom demands.

Similar to previous quarters, initial access occurs through various forms of phishing or compromising of remote access services. Most recently, Arete observed Conti exploiting vulnerabilities in unpatched Microsoft Exchange servers.[3] Once inside a victim environment, Conti leverages several tactics — for example, Cobalt Strike, Mimikatz, and exploitation of vulnerabilities in legitimate remote management software — to move laterally and maintain persistence.

The group's average ransom demand starts at just over US$1.6M with the average payment in the US$400k range.

Originally spotted in the wild in February 2020, the Conti ransomware variant is likely operated by the same group that's been conducting Ryuk (formerly Hermes) ransomware attacks since at least 2017.

In Q3 2021, Conti ransomware operators primarily used the following methods to gain initial access to victim networks:

- Spear-phishing campaigns with malicious attachments (or links) with Word documents that deployed IcedID and/or Cobalt Strike through embedded scripts.
- Stolen or weak remote desktop protocol (RDP) credentials.
- ZLoader malware distribution network.
- Common vulnerabilities in external assets, for example, unpatched virtual private network (VPN) or firewall (FW) appliances.

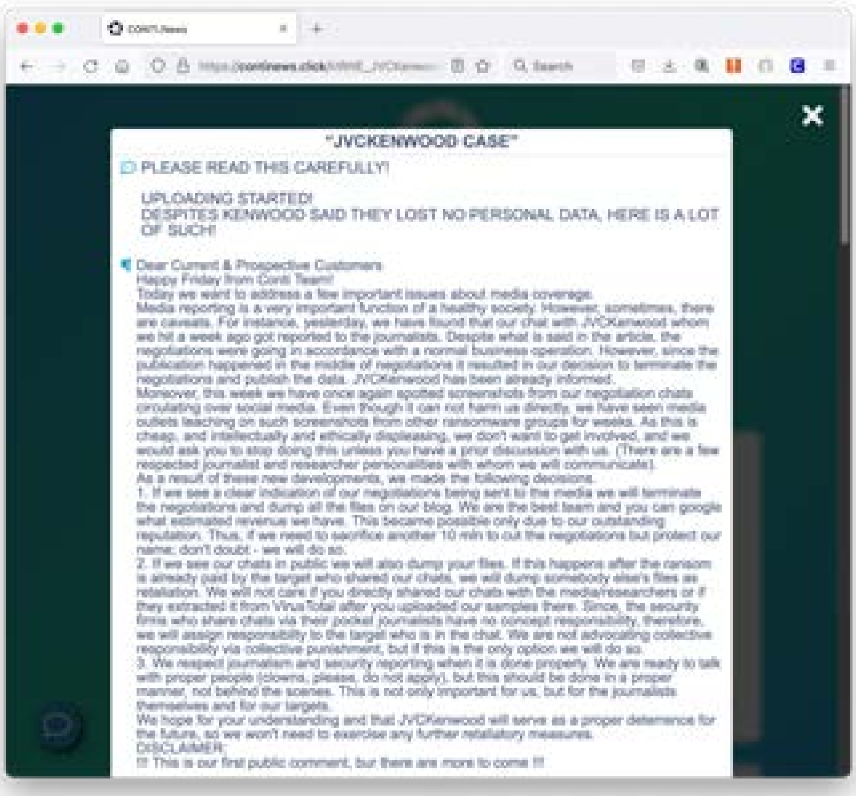
Conti
Ups the ante by deleting backups

The Conti playbook, which an alleged "disgruntled former Conti member" leaked in August 2021, also confirmed Arete forensic findings from prior cases. Moreover, the playbook showed that Conti operators typically use open-source Rclone software for data exfiltration and can exploit the following vulnerabilities for lateral movements and privilege escalation:

- 2017 Microsoft Windows Server Message Block 1.0 server vulnerabilities.
- "PrintNightmare" vulnerability (CVE-2021-34527) in Windows Print spooler service.
- "Zerologon" vulnerability (CVE-2020-1472) in Microsoft Active Directory Domain Controller systems.

Arete did not observe any significant changes in ransomware negotiation tactics. In Q3 2021, Conti continued to call or email victims to increase pressure during negotiations. Based on the Arete Cyber Threat Intelligence (CTI) team's assessment, Conti is most likely using a third-party provider for those services.

On October 7, 2021, Conti released the following announcement:



"JVCKENWOOD CASE"

PLEASE READ THIS CAREFULLY!

UPLOADING STARTED!
DESPITES KENWOOD SAID THEY LOST NO PERSONAL DATA, HERE IS A LOT OF SUCH!

Dear Current & Prospective Customers
Happy Friday from Conti Team!
Today we want to address a few important issues about media coverage.
Media reporting is a very important function of a healthy society. However, sometimes, there are caveats. For instance, yesterday, we have found that our chat with JVCKenwood whom we hit a week ago got reported to the journalists. Despite what is said in the article, the negotiations were going in accordance with a normal business operation. However, since the publication happened in the middle of negotiations it resulted in our decision to terminate the negotiations and publish the data. JVCKenwood has been already informed.
Moreover, this week we have once again spotted screenshots from our negotiation chats circulating over social media. Even though it can not harm us directly, we have seen media outlets leaching on such screenshots from other ransomware groups for weeks. As this is cheap, and intellectually and ethically displeasing, we don't want to get involved, and we would ask you to stop doing this unless you have a prior discussion with us. (There are a few respected journalist and researcher personalities with whom we will communicate).
As a result of these new developments, we made the following decisions.
1. If we see a clear indication of our negotiations being sent to the media we will terminate the negotiations and dump all the files on our blog. We are the best team and you can google what estimated revenue we have. This became possible only due to our outstanding reputation. Thus, if we need to sacrifice another 10 mln to cut the negotiations but protect our name: don't doubt - we will do so.
2. If we see our chats in public we will also dump your files. If this happens after the ransom is already paid by the target who shared our chats, we will dump somebody else's files as retaliation. We will not care if you directly shared our chats with the media/researchers or if they extracted it from VirusTotal after you uploaded our samples there. Since, the security firms who share chats via their pocket journalists have no concept responsibility, therefore, we will assign responsibility to the target who is in the chat. We are not advocating collective responsibility via collective punishment, but if this is the only option we will do so.
3. We respect journalism and security reporting when it is done properly. We are ready to talk with proper people (clowns, please, do not apply), but this should be done in a proper manner, not behind the scenes. This is not only important for us, but for the journalists themselves and for our targets.
We hope for your understanding and that JVCKenwood will serve as a proper deterrence for the future, so we won't need to exercise any further retaliatory measures.
DISCLAIMER:
!!! This is our first public comment, but there are more to come !!!

See the trend in Conti cases from Q1 to Q3.

REvil/Sodinokibi
Now you see them, now you don’t

Since April 2019, the suspected Russian-based ransomware group REvil (also known as Sodinokibi) has been targeting victims in the wild — primarily managed service providers (MSPs) and other high-impact targets across multiple sectors.

In Q3 2021, the group’s targets included the MSP Kaseya, the Brazilian meat-processing company JBS SA, the electronics corporation Acer, and even, political candidates. On average, the group demanded ransoms of ~US$1.4M with average payment in the US$270k range.

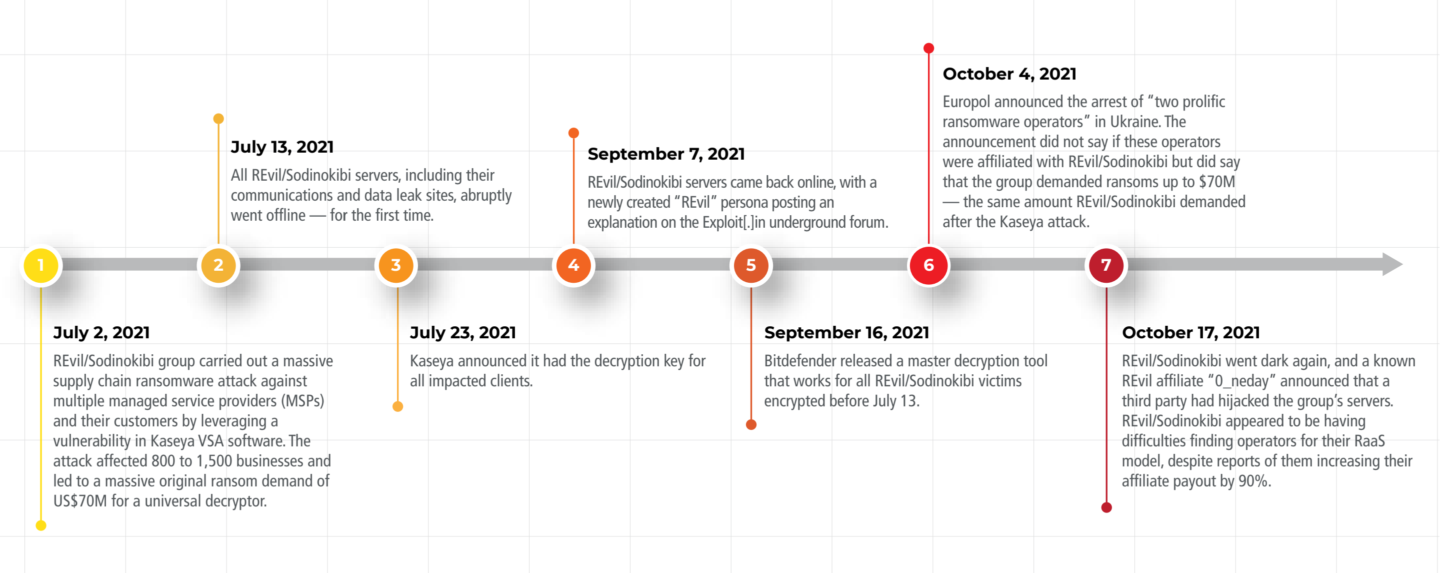
More recently, REvil/Sodinokibi has quickly become known for their disappearing acts.

When not leveraging zero-day vulnerabilities to encrypt large-scale supply chain networks, REvil/Sodinokibi exploited known vulnerabilities in firewalls, phished for user credentials, and used brute-forcing techniques against remote access services to gain initial access into victim environments.

Much like Conti, REvil/Sodinokibi leveraged Mimikatz and Cobalt Strike in victim environments and was also identified installing the remote access tool ConnectWise on up to one-third of a victim’s environment to maintain persistence if removed or blocked.

The Arete CTI team will continue to follow developments related to REvil/Sodinokibi but based on the latest shutdown, it is highly likely this group will close operations for good.

KEY REVIL/SODINOKIBI HIGHLIGHTS FOR Q3 2021



1

July 2, 2021

REvil/Sodinokibi group carried out a massive supply chain ransomware attack against multiple managed service providers (MSPs) and their customers by leveraging a vulnerability in Kaseya VSA software. The attack affected 800 to 1,500 businesses and led to a massive original ransom demand of US$70M for a universal decryptor.

2

July 13, 2021

All REvil/Sodinokibi servers, including their communications and data leak sites, abruptly went offline — for the first time.

3

July 23, 2021

Kaseya announced it had the decryption key for all impacted clients.

4

September 7, 2021

REvil/Sodinokibi servers came back online, with a newly created “REvil” persona posting an explanation on the Exploit[.]in underground forum.

5

September 16, 2021

Bitdefender released a master decryption tool that works for all REvil/Sodinokibi victims encrypted before July 13.

6

October 4, 2021

Europol announced the arrest of “two prolific ransomware operators” in Ukraine. The announcement did not say if these operators were affiliated with REvil/Sodinokibi but did say that the group demanded ransoms up to $70M — the same amount REvil/Sodinokibi demanded after the Kaseya attack.

7

October 17, 2021

REvil/Sodinokibi went dark again, and a known REvil affiliate “0_neday” announced that a third party had hijacked the group’s servers. REvil/Sodinokibi appeared to be having difficulties finding operators for their RaaS model, despite reports of them increasing their affiliate payout by 90%.

See the trend in Revil/Sodinokibi cases from Q1 to Q3.

LockBit 2.0
Has the fastest encryption method

In operation since at least September 2019, the Russian-speaking RaaS group LockBit returned in June 2021 after a brief hiatus with a new variant dubbed LockBit 2.0. Since that time, the group has continued to expand their operations, recruit new affiliates through their data leak site, and primarily target organizations in Chile, Italy, Taiwan, and the United Kingdom. Accenture became one of its most high-profile victims with a suspected US$50M demand to decrypt the company's files.[5]

To date, LockBit 2.0 has the fastest encryption method of ransomware variants in the wild. The group uses a unique encryption method that proliferates across devices in the Windows domain by abusing Active Directory group policies and only partially encrypting the files. The group uses speed results benchmarks for self-promotion.

LockBit 2.0 affiliates are responsible for obtaining initial access into victim environments, typically via RDP account credentials. To establish and maintain persistence, LockBit 2.0 terminates security tools, enables RDP connections, and uses legitimate tools, such as Process Hacker and PC Hunter. Once persistence is established, LockBit 2.0 moves laterally and executes the ransomware using Windows Active Directory group policies.

Encryption speed comparative table for some ransomware – 02.08.2021

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHZ \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472
LOCKBIT 2.0	**5 Jun, 2021**	**373 MB/s**	**4M 28S**	**7H 26M 40S**	**Yes**	855 KB	109964
LOCKBIT	**14 Feb, 2021**	**266 MB/s**	**6M 16S**	**10H 26M 40S**	**Yes**	146 KB	110029
Cuba	8 Mar, 2020	**185 MB/s**	**9M**	**15H**	No	1130 KB	110468
BlackMatter	2 Aug, 2021	**185 MB/s**	**9M**	**15H**	No	67 KB	111018
Babuk	20 Apr, 2021	**166 MB/s**	**10M**	**16H 40M**	**Yes**	79 KB	109969
Sodinokibi	4 Jul, 2019	**151 MB/s**	**11M**	**18H 20M**	No	253 KB	95490
Ragnar	11 Feb, 2020	**151 MB/s**	**11M**	**18H 20M**	No	40 KB	110651
NetWalker	19 Oct, 2020	**151 MB/s**	**11M**	**18H 20M**	No	902 KB	109892
MAKOP	27 Oct, 2020	**138 MB/s**	**12M**	**20H**	No	115 KB	111002
RansomEXX	14 Dec, 2020	**138 MB/s**	**12M**	**20H**	No	156 KB	109700
Pysa	8 Apr, 2021	**128 MB/s**	**13M**	**21H 40M**	No	500 KB	108430
Avaddon	9 Jun, 2020	**119 MB/s**	**14M**	**23H 20M**	No	1054 KB	109952
Thanos	23 Mar, 2021	**119 MB/s**	**14M**	**23H 20M**	No	91 KB	81081
Ranzy	20 Dec, 2020	**111 MB/s**	**15M**	**1D 1H**	No	138 KB	109918
PwndLocker	4 Mar, 2020	**104 MB/s**	**16M**	**1D 2H 40 M**	No	17 KB	109842

LockBit 2.0
Has the fastest encryption method

LockBit 2.0 has been identified targeting organizations in the manufacturing, hospitality, and financial services sectors. On average, the group demanded ransoms of US$70k with average payment just over US$35k.

On August 23, 2021, a representative of the LockBit ransomware group "LockBitSupp" did an interview with "Russian OSINT." Highlights included:

- LockBit primarily targets organizations in the United States and European Union and has leveraged the COVID-19 pandemic to breach more victims.

  "Many employees started working remotely from personal computers, which are easier to infect with a virus and steal account information used to access the companies."

- LockBit follows a "moral code":

  "We do not attack healthcare, education, charitable organizations, social services - everything that contributes to the development of personality and sensible values from the 'survival of the species' perspective ... Healthcare, medicine, education, charitable organizations and social services remain intact."

Arete confirmed that several victims throughout Q3 received free decryptors.

See the trend in LockBit/LockBit 2.0 cases from Q1 to Q3.

Key Cybersecurity Events

Data leaks: early frost hits the cybercrime ecosystem

Fall arrived with a distinct chill as alleged affiliates of the Conti and Babuk RaaS platforms signaled long-held grievances by leaking sensitive operational details, tooling, and techniques of the ransomware proprietors to the broader cybercrime community and subsequently, the public at large.

CONTI SUFFERED OPERATIONAL SECURITY BREACH

On August 5, 2021, an alleged affiliate ("m1Geelka")[6] of the Conti ransomware operation leaked an archive containing files that described the TTPs of Conti ransomware partners to attain the most effective ways to distribute and deploy the ransomware.

ATT&CK Tactic		ATT&CK Technique
1	**RESOURCE DEVELOPMENT** T1608 – Stage capabilities	• Instructions for how to install and configure Metasploit OST on a private (actor-controlled) server.
2	**INITIAL ACCESS** T1190 – Exploit public-facing application T1200 – Hardware additions	• Instructions for how to leverage ZeroLogon/ProxyLogon vulnerabilities. • Instructions for how to brute force network storage devices, routers, and network-enabled security cameras.
3	**PERSISTENCE** T1133 – External remote services	• Instructions for how to use/configure AnyDesk as a persistence mechanism within victim environment. • Instructions for how to use/configure Ngrok for secure tunneling via RDP - ingress/egress of compromised network.
4	**PRIVILEGE ESCALATION** T1484 – Domain policy modification	• Instructions for how to elevate privileged access up to Domain Admin.
5	**DEFENSE EVASION** T1562 – Impair defenses	• Instructions for how to disable Windows Defender.
6	**CREDENTIAL ACCESS** T1003 – OS credential dumping T1558 – Steal or forge Kerberos tickets T1110 – Brute force	• Instructions for how to dump credentials from Microsoft Active Directory. • Instructions for how to execute 'Kerberoasting' attack on weakly secured credentials. • Instructions for how to brute force server message bus (SMB) authentication.
7	**DISCOVERY** T1046 – Network service scanning	• Instructions for how to use NetScan OST for enumeration within victim environment.
8	**COMMAND & CONTROL (C2)** T1219 – Remote access software	• Instructions for how to deploy/use Cobalt Strike agent.
9	**EXFILTRATION** T1567 – Exfiltration over Web service	• Instructions for how to use/configure Rclone COTS tool in conjunction with MegaUpload for data.
10	**IMPACT** T1490 – Inhibit system recovery	• Instructions for how to delete Windows shadow volumes.

Highlighted TTPs observed in tutorials provided to Conti ransomware affiliates

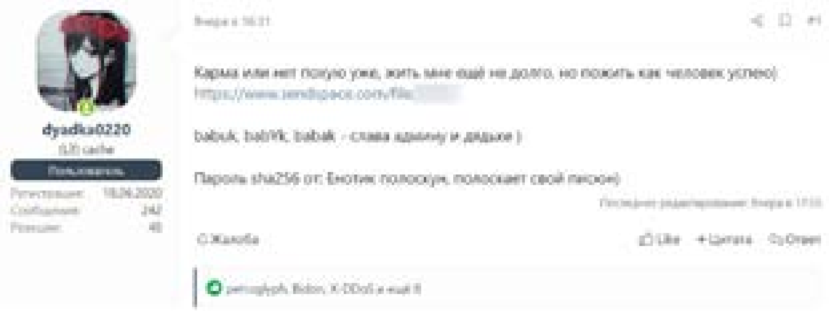
Additionally, m1Geelka disclosed four IPv4 addresses corresponding to Cobalt Strike C2 servers that Conti affiliates use to access compromised networks:

- 162[.]244[.]80[.]235
- 85[.]93[.]88[.]165
- 185[.]141[.]63[.]120
- 82[.]118[.]21[.]1

BABUK RANSOMWARE SOURCE CODE LEAKED

On September 3, 2021, a self-described affiliate ("dyadka0220") of the Babuk ransomware operation leaked the ransomware source code on a popular Russian-language cybercrime forum.

The Arete CTI team analyzed the content of the Babuk ransomware source code leak, searching for any decryption utilities. After uncovering additional leak details, the team delivered tailored response and recovery approaches to impacted clients.



dyadka0220

Пользователь

Регистрация: 18.06.2020

Сообщения: 242

Реакции: 40

Вчера в 16:21

Карма или нет похую уже, жить мне ещё не долго, но пожить как человек успею)
https://www.sendspace.com/file/[redacted]

babuk, babyk, babak - слава админу и дядьке)

Пароль sha256 от: Енотик полоскун, полоскает свой писюн)

Последнее редактирование: Вчера в 17:10

petroglyph, Bidon, X-DDoS и ещё 8

Forum post announcing Babuk ransomware leak, with corresponding download link. Source: BleepingComputer[7]

Many factors are likely to influence the behavior of ransomware affiliate operators who leak data and techniques of their partnered platform. Though the most pronounced motivation is often manifested through claims of retribution, the dynamics underlying such criminal partnerships and their dissolution are opaque by design.

What is clear, however, is that while some of these relationships may be on ice, the competition in the ransomware space remains hot. Criminal organizations are likely to defy longstanding conventional codes of conduct in favor of more agile, business-like methods of seizing opportunities in an unregulated market.

New Vulnerabilities

Arete observed the exploitation of multiple vulnerabilities across its case data in Q3 2021. Similar to Q1 and Q2 2021, actors continue targeting vulnerabilities that allow them to easily and consistently gain access to victim networks.

THE PROXYSHELL EXPLOITS

When linked together, a series of three unique vulnerabilities in Microsoft Exchange Servers (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) have been dubbed ProxyShells. Originally exploited by the state-sponsored Chinese threat group Hafnium, ProxyShells have become a staple for ransomware groups as they can lead to pre-authenticated remote code execution (RCE) and arbitrary code execution (ACE) over port 443. They are most notably used by the ransomware group Conti, as revealed in their leaked manuals.

CVE-2021-34473: Microsoft Exchange Server Remote Code Execution Vulnerability

- The CVE-2021-34473 vulnerability allows for pre-authenticated RCE, which enables threat actors to remotely execute code on an affected system.
- The vulnerability exists in a feature called Explicit Logon of Microsoft Exchange, which allows a browser to embed or display a specific user's mailbox or calendar with a single URL.
- The vulnerability causes the Microsoft Exchange Server to not perform adequate checks on URLs, which can lead to arbitrary access to backend URLs, access to the NT Authority\System account, and an ability to conduct further attacks.

CVE-2021-34523: Microsoft Exchange Server Elevation of Privilege Vulnerability

- Due to a flaw in the PowerShell service that causes improper token validation, the CVE-2021-34523 vulnerability allows for arbitrary code post-authentication on Microsoft Exchange Servers.
- The vulnerability exists in a feature called Exchange PowerShell remoting, which allows users to send and read emails as well as update the Outlook configuration from the command line.

CVE-2021-31207: Microsoft Exchange Server Security Feature Bypass Vulnerability

- The CVE-2021-31207 vulnerability enables post-authenticated actors to execute arbitrary PowerShell commands in the context of system and write arbitrary files.
- The vulnerability exists in the Import Export Mailbox that is assigned to the impersonated user, which allows the malicious actors to export mailboxes where they previously created emails with Web shells.

New Vulnerabilities

WEB SHELLS IN NON-STANDARD LOCATIONS

Attackers can modify the configuration file for the Exchange internet service to include a new “virtual directory” that redirects one URL endpoint to another location on the filesystem. This modification allows a threat actor to hide a Web shell in uncommon locations outside of known ASP directories. LockFile was the first ransomware group observed exploiting this attack.

Virtual Web shells can be hidden in:

- C:\Users\All Users\
- C:\Windows\System32\
- C:\ProgramData\

TARGET SECTORS AND GEOGRAPHIES

ProxyShells have targeted a broad spectrum of organizations within these sectors:

- Education
- Government
- Business Services
- elecommunications

And across these geographies:

- United States
- Europe
- Middle East

These organizations are most frequently targeted by Conti and LockFile ransomware groups.

MULTI-LAYERED, LARGE-SCALE EXPLOITS WILL CONTINUE TO RISE

ProxyShell exploitation was a well-planned, strategic follow-on to the original Hafnium exploits that both old and new ransomware groups have used to target a broad spectrum of sectors and countries.

Arete assesses with high confidence that such strategic, multi-layered, large-scale exploits and attacks at both the state-sponsored level and in the ransomware sector will continue to rise.

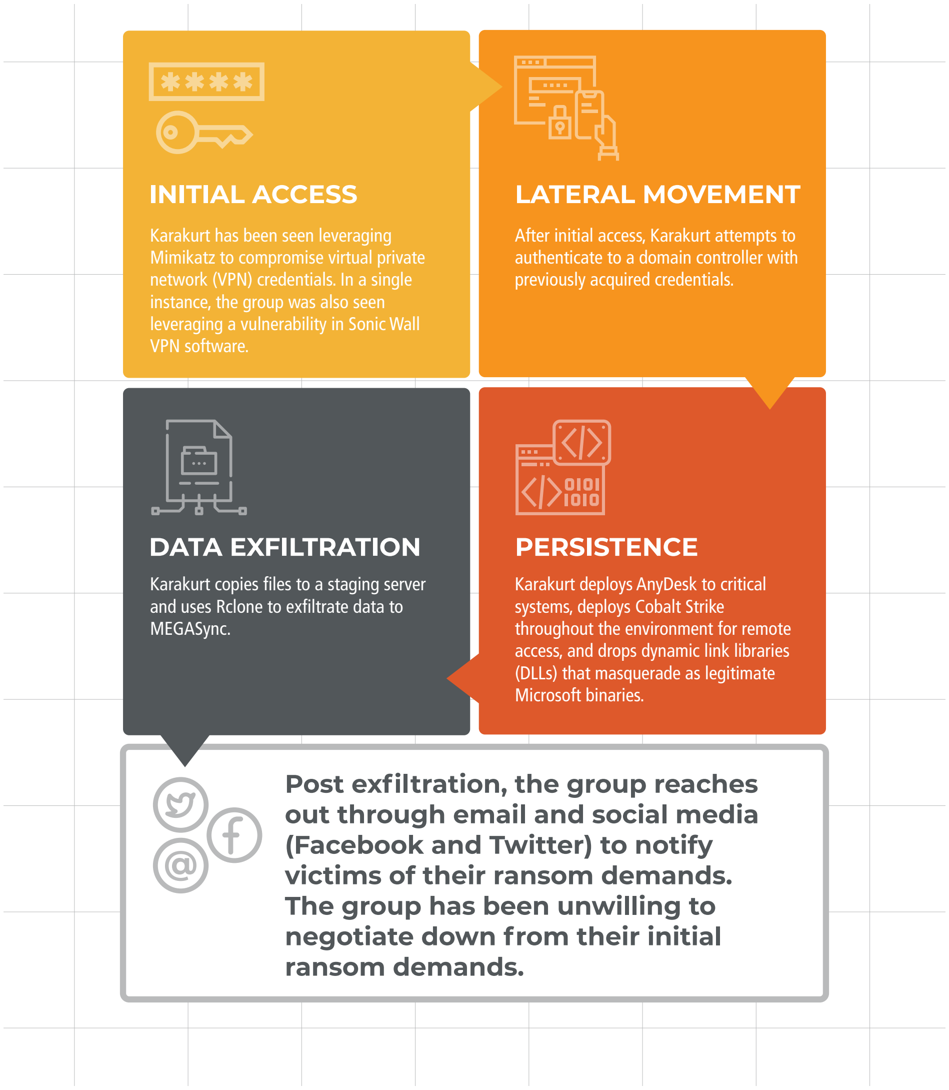
New Notable Extortion Groups and Ransomware Variants

THE KARAKURT TEAM: THEIR TECHNIQUES AREN'T OLD, THEY'RE VINTAGE

First identified in September 2021, the Karakurt Team (Karakurt Lair) is a new-to-the-scene, extortion-only group that shows significant ties to Russia and refuses to negotiate.

They have been observed in victim networks for as long as two months, significantly longer than the average ransomware variant in today's threat landscape. And while known to exfiltrate data over longer-than-average periods, the extortion-only group does not deploy ransomware to victim environments.

ATTACK LIFECYCLE



INITIAL ACCESS

Karakurt has been seen leveraging Mimikatz to compromise virtual private network (VPN) credentials. In a single instance, the group was also seen leveraging a vulnerability in Sonic Wall VPN software.

LATERAL MOVEMENT

After initial access, Karakurt attempts to authenticate to a domain controller with previously acquired credentials.

PERSISTENCE

Karakurt deploys AnyDesk to critical systems, deploys Cobalt Strike throughout the environment for remote access, and drops dynamic link libraries (DLLs) that masquerade as legitimate Microsoft binaries.

DATA EXFILTRATION

Karakurt copies files to a staging server and uses Rclone to exfiltrate data to MEGASync.

Post exfiltration, the group reaches out through email and social media (Facebook and Twitter) to notify victims of their ransom demands. The group has been unwilling to negotiate down from their initial ransom demands.

Karakurt Team Twitter page

EXFILTRATION: WHAT'S OLD IS NEW AGAIN

The combination of cyber espionage, exfiltration, and theft of state secrets is nothing new. In fact, it was likely the first form of a cyberattack.

Recently, several new-to-the-scene cyber actors have adopted this "old" extortion-only technique to demand ransom payments from victims — and it isn't completely clear why just yet.

These exfiltration-only groups use TTPs that have become standard throughout the ransomware industry and are the epitome of not re-inventing the wheel.

Community Action

OFAC UPDATES ITS ADVISORY ON POTENTIAL SANCTIONS RISKS ASSOCIATED WITH RANSOMWARE PAYMENTS

On September 21, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,"[8] which superseded its previous guidance on facilitating ransomware payments.[9] Within the update, OFAC designated SUEX OTC S.R.O., a virtual currency exchange, and 25 digital currency addresses for inclusion to its Specially Designated Nationals and Blocked Persons List (SDN) in connection with malicious cyber-enabled activities associated with ransomware payments.

OFAC's actions were a positive step toward shutting down virtual currency exchanges that permit sanctioned actors to move, store, and convert cryptocurrencies into physical cash.

As mentioned in the updated advisory, reporting ransomware attacks and payments to law enforcement and/or the U.S. Department of Treasury not only increases the likelihood of recovering access to stolen data through other means and/or recovering some of the ransomware payments, but it may also allow organizations to receive significant mitigation from OFAC in the event a sanctions nexus is subsequently found in connection with a ransom payment.

GOVERNMENT ACTION COULD IMPACT THE FUTURE OF RAAS

Government action could cause the RaaS market to fracture into smaller platforms or see individual actors running these campaigns — for example, extortion-only groups or source-code sales.

Furthermore, it is possible that threat actors are reacting to a combination of factors and changing tactics to minimize the chances of government attention. Another possibility is that actors no longer trust the RaaS model after recent leaks and accusations of admin backdoors.

Trend by Industries

Source: Arete Cases from Q1-Q3

INDUSTRIES TARGETED BY RANSOMWARE

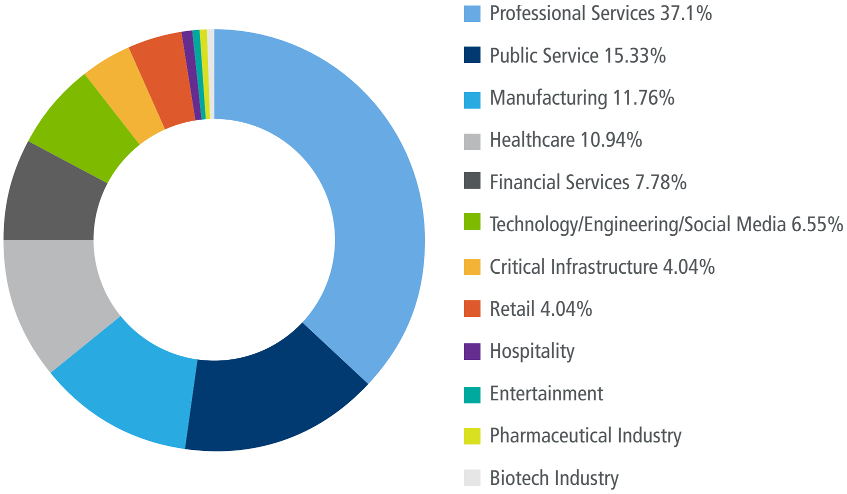


Figure 1

VARIANTS OBSERVED IN PROFESSIONAL SERVICES

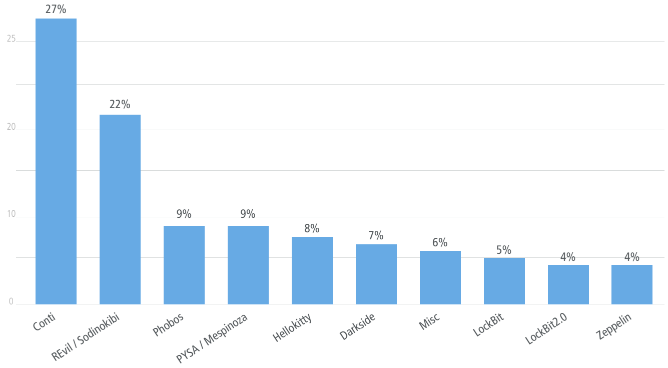


Figure 2

VARIANTS OBSERVED IN PUBLIC SERVICES

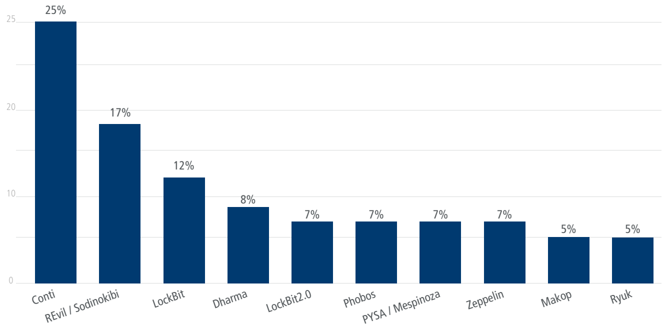


Figure 3

VARIANTS OBSERVED IN MANUFACTURING SERVICES

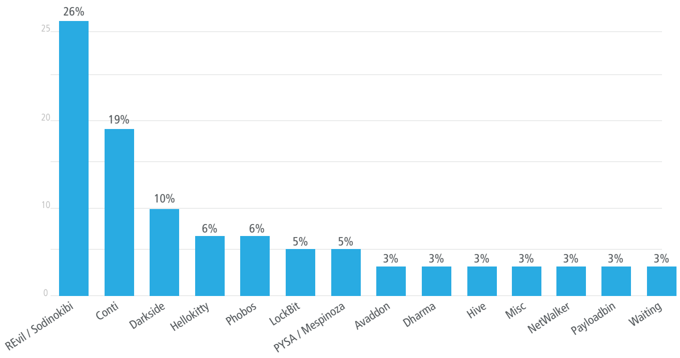


Figure 4

Overall Ransomware Stats

Source: Arete Cases from Q1-Q3

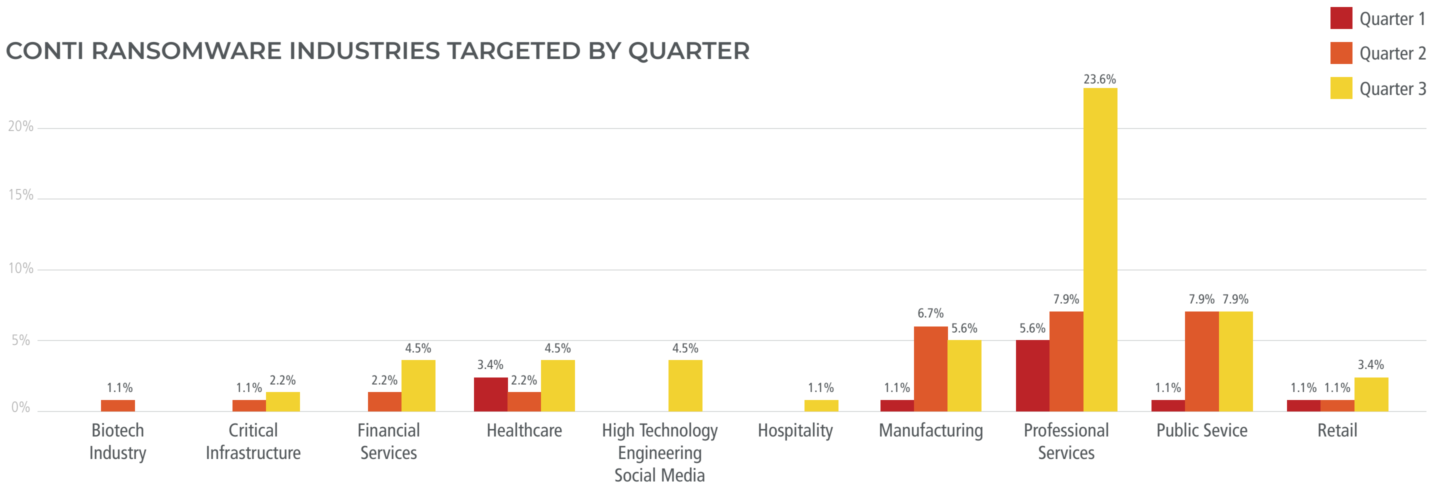

CONTI RANSOMWARE INDUSTRIES TARGETED BY QUARTER

Figure 5

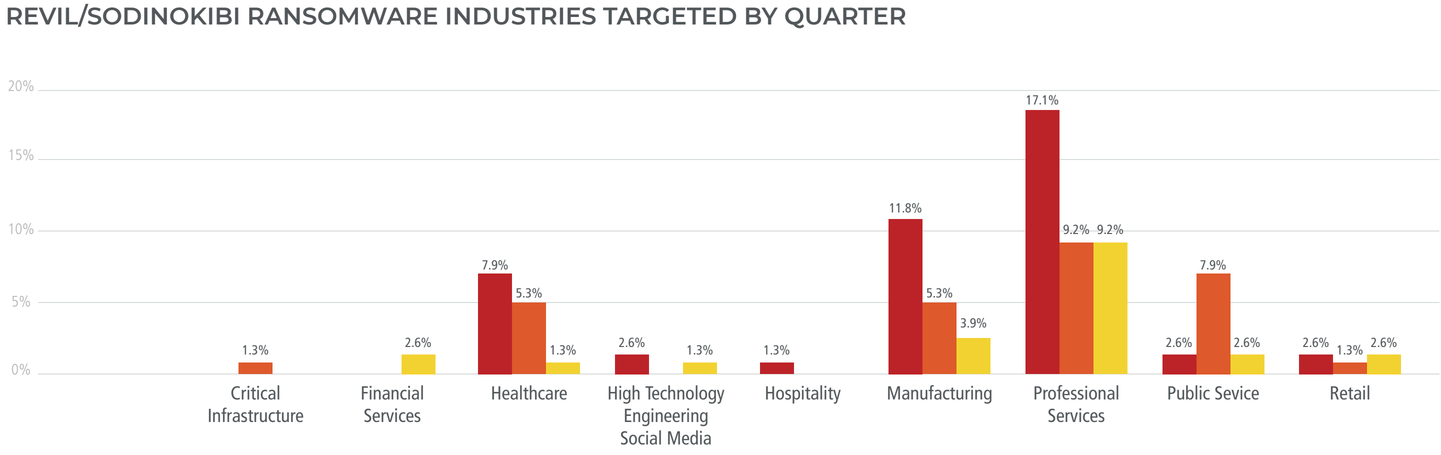

REVIL/SODINOKIBI RANSOMWARE INDUSTRIES TARGETED BY QUARTER

Figure 6

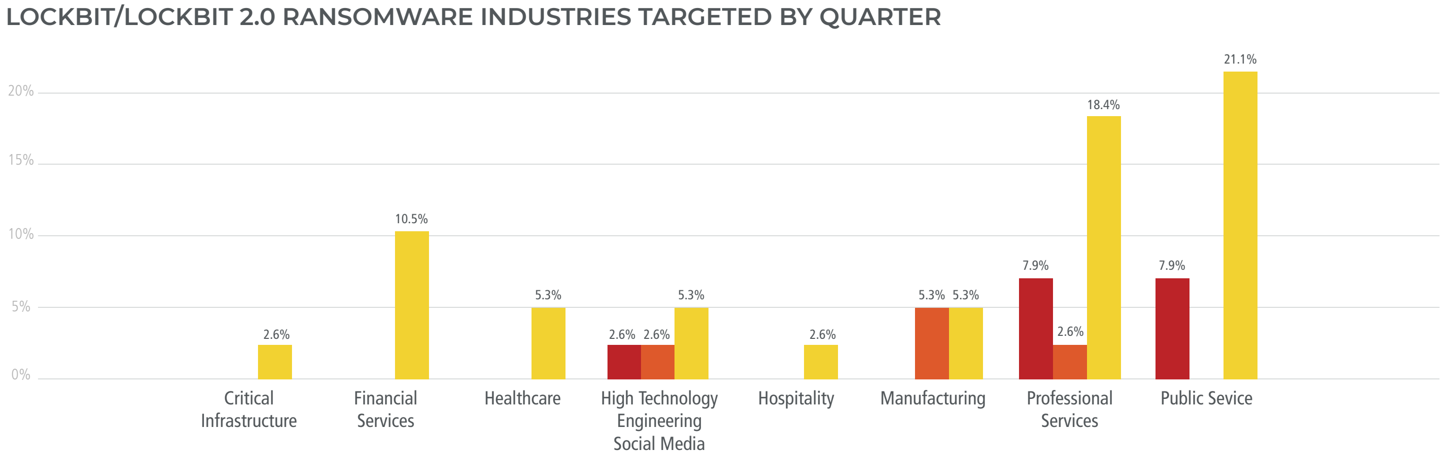

LOCKBIT/LOCKBIT 2.0 RANSOMWARE INDUSTRIES TARGETED BY QUARTER

Figure 7

What to Expect

Cybercrime is in a constant state of evolution and revolution. Threat actors continue to react to the actions of their targets as well as the governments and law enforcement agencies trying to protect those targets.

While the updated advisory from the U.S. Department of Treasury bolstered ransomware awareness, the longer term effects on the cybercrime ecosystem is unclear. Takedowns or sanctioning of exchanges may lead threat actors to temporarily scramble to other exchanges or underground forums, but threat actors always reinvent themselves when law enforcement intervenes. Where one, such as REvil/Sodinokibi, shuts down, others will step in.

Arete assesses that government action may begin to fracture the ransomware ecosystem and expects to see a continued trend of threat actors moving away from RaaS offerings toward solo acts, likely leading to an acceleration of data as hostage (DasH) extortion campaigns. Additionally, RaaS operators and affiliates are likely to respond with a mix of fear, anger, or disbelief akin to Conti's statement on the REvil/Sodinokibi shutdown. What remains to be seen, however, is whether these groups will punish victims in retaliation for government action.

As previously stated, Arete also assesses with high confidence that strategic, multi-layered, large-scale exploits, such as ProxyShell, will continue to drive initial access for both state-sponsored and cybercriminal campaigns.

In short, Arete expects to see no decrease in criminal activity in the coming quarters.

[1] Disclaimer: Unless otherwise noted, all data within this report is based on Arete incident response cases.

[2] https://us-cert.cisa.gov/ncas/alerts/aa21-265a

[3] https://siliconangle.com/2021/09/05/conti-ransomware-gang-targeting-unpatched-microsoft-exchange-servers/

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

[5] https://www.infosecurity-magazine.com/news/accenture-tied-up-in-50m-ransom/

[6] https://therecord.media/disgruntled-ransomware-affiliate-leaks-the-conti-gangs-technical-manuals/

[7] https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/

[8] https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/

[9] Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

Arete

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
Arete911@AreteIR.com

www.areteir.com

Arete Advisors, LLC makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents of this report and expressly disclaims liability for errors and omissions in the content. Neither Arete Advisors, LLC, nor its employees and contractors make any warranty, express or implied or statutory, including but not limited to the warranties of non-infringement of third-party rights, title, and the warranties of merchantability and fitness for a particular purpose, with respect to content available from this report. Arete Advisors, LLC assumes no liability for any direct, indirect, or any other loss or damage of any kind for the accuracy, completely, or usefulness of any information, product, or process disclosed herein, and does not represent that the use of such information, product, or process would not infringe on privately owned rights.