HERJAVEC GROUP

State of Ransomware 2021

Compiled By HG Threat Hunters
Q1-Q2

HERJAVEC GROUP

State of Ransomware

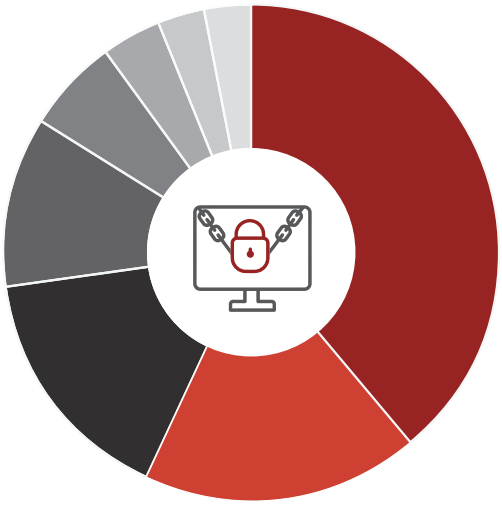
Contents

Evolving Ransomware

In 2021, the average cost of recovery and ransom associated with a ransomware attack has been 2 times more than the 2020 average global ransom demand[1]. During the first two fiscal quarters of 2021, not only did ransomware attacks continue to become more targeted and sophisticated[2], but the most prolific "Double Extortion" ransomware operators have been observed holding enterprise networks hostage for eight figure sums of up to $40M USD[3].

Herjavec Group has analyzed the most active ransomware operations in the first two fiscal quarters of 2021 and created profiles on the highest-impact ransomware families and their victimized industries. As expected, all of these ransomware operators were observed to demand payment via cryptocurrencies and leveraged sensitive data exfiltrated before the encrypting process to apply additional pressure on their victims in an attempt to increase the likelihood of a payout[4], [5].

Victims of Data-Leak Ransomware Operations in the first half of 2021



39% Manufactured Goods

18% Technology & Technology Service Providers

16% Public Sector & Legal Services

11% Finance

6% Healthcare

4% Education

3% Entertainment

3% Energy

Many of these ransomware variants were observed sharing code similarities and Tactics, Techniques, and Procedures (TTPs) related to older variants observed in 2020 and earlier. One such example is Wizard Spider's Conti which contains many code similarities to its predecessor Ryuk[6]. However, developers are continuing to innovate on a technical level. These innovations include encrypting on multiple threads to achieve a faster target takedown time along with using Domain Generation Algorithms (T1568.002 – Dynamic Resolution: Domain Generational Algorithms) for C2 Communications, and common cloud platforms such as Rclone for exfiltration (T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage) [7], [8].

Herjavec Group's research uncovered the following ransomware variants have accrued the most data-leak victims so far in 2021:

Conti

REvil

Avaddon

CL0P

Darkside

DoppelPaymer

Babuk

NetWalker

Conti

Conti is currently the most prominent ransomware of 2021. In the first quarter of 2021, they were second only to Sodinokibi, according to a Conti DFIR ransomware report[9]. Consumables, finance, public sector, and technology are the top targeted sectors by this group. Conti group uses phishing attacks to install TrickBot and BazarLoader trojans that provide remote access to steal credentials and harvest unencrypted data that is stored on workstations and servers[10]. Once Windows domain credentials have been harvested, Conti operators will continue to remain undetected, until they strike and deploy the ransomware on the network to encrypt all of its devices.

The original Conti is a human-operated virus. It is capable of automatically worming its way into a system; however, it can also be manipulated by a human operator. Some prominent ransomware attacks directed by Conti operators in the past include IOT chip maker Advantech, FreePBX, Broward County Public Schools (BCPS), and the Scottish Environment Protection Agency (SEPA). The hit on the SEPA occurred on Christmas Eve, later publishing roughly 1.2 GB of stolen data on Conti's dark web leak site[10]. Conti News site has published data stolen from at least 180 victims thus far[10].

The software uses its own proprietary implementation of AES-256 that uses up to 32 individual logical threads, making it much faster than most ransomware[11]. There are a small number of ransomware families that target the local network to encrypt via SMB. Conti's unique feature is that it allows command line arguments to direct it to encrypt the local hard drive or network shares, even specific, targeted, IP addresses. Conti has an extremely busy and loud methodology for stopping services and inhibiting recovery on the local system. While many ransomware families will simply delete the Windows Volume Shadow Copies using vssadmin, Conti uses vssadmin in unique ways to ensure their deletion. This includes not only deleting the Volume Shadow Copies, but also *resizing all of the available shadow storage volumes to inhibit recovery*[55].

Moreover, the malware will execute 160 individual commands – 146 of which focus on stopping potential Windows services. The entirety of commands mimics those that are found within the Ryuk ransomware family[6]. Conti also targets Windows Restart Manager where it closes applications and services currently running to make them available for encryption and maximize damage.

Once the system has been prepared and files have been identified, Conti will initiate the process of:

- Scanning through each folder
- Encrypting files with AES-256 encryption via a hard-coded public key
- Creating a ransom note named CONTI_README.txt
- Encrypting files to have a file extension of . CONTI.

The use of a hard-coded key allows the malware to encrypt files even if the malware cannot contact its C2.

Conti's unique feature is that it allows command line arguments to direct it to encrypt the local hard drive or network shares, even specific, targeted, IP addresses.

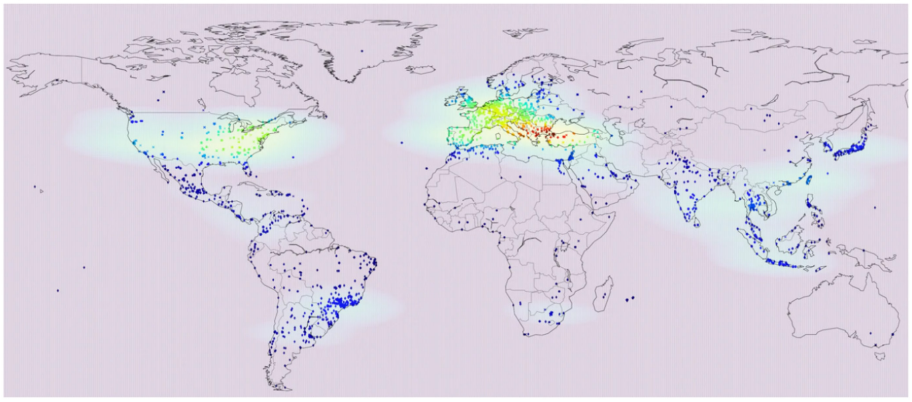
REvil

REvil, also known as Sodinokibi, first appeared in April 2019, and has been observed being distributed through exploit kits, vulnerability exploit, and backdoored software installers[12]. REvil operates as ransomware-as-a-service (RaaS) and has been linked to the GOLD SOUTHFIELD group. It is highly configurable and shares code similarities with the GrandCrab RaaS[13],[14].

REvil Gathers host information (e.g., username, computer name, workgroup) and has the following additional capabilities[15]:

- "Exploit vulnerabilities to elevate privileges" (e.g., CVE-2018-8453)
- "Encrypt non-whitelisted files and folders on local storage devices and network shares."

Geolocation of targets from May 2019 to August 23rd, 2019 illustrate that REvil most frequently targets organizations within North America, Europe, South East Asia, and South America[4]:



Distribution of Targets based on Geolocation (2019)

As of 2021, REvil has been observed most frequently targeting food production organizations such as Dairy Farm and Bakker Logistiek[6]. The next most frequently targeted sector is technology, demonstrated with the compromise of organizations such as MSP Stanley Systems, Acer Computers, and Quanta Computer. REvil has also frequently targeted court systems, lawyers, insurance agencies and to a lesser degree, healthcare[16].

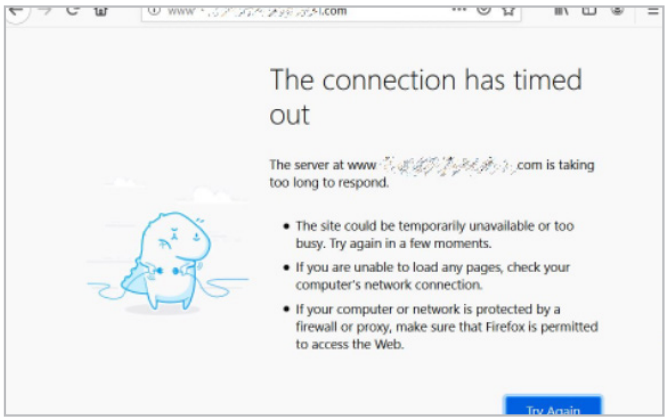
As of 2021, REvil has been observed most frequently targeting food production such as Dairy Farm and Bakker Logistek[6].

Avaddon

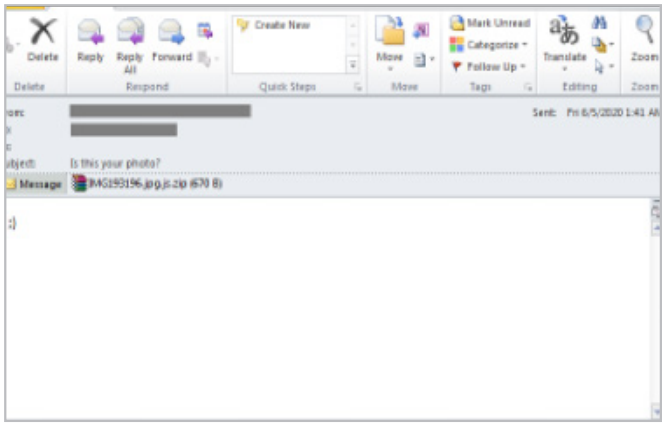
Avaddon Ransomware was reported to begin operations in June 2020[17] and has been observed to target the manufactured consumable and technology industries. This ransomware group has been observed to leverage the double extortion technique[18] which involves threatening the victim into paying a ransom to prevent stolen and often highly sensitive data from being released. In addition, Avaddon was recently observed threatening to DDoS victim sites in addition to encrypting the victim's infrastructure[19].

The double extortion tactic has been observed in the past being leveraged by other ransomware groups such as Maze group[21] and Egregor[22]. Avaddon is initially delivered by email via malicious attachment[23] with the message body containing only a single smiley emoji and subjects were of photo related statements such as "look at this photo!", "photo just for you" or "you look good here"[23].

Once opened and executed, Avaddon will executive via PowerShell commands and encrypt victims files with a focus on Microsoft Exchange Server and Microsoft SQL Server[23]. It will then proceed to delete backup copies of system restore files[23] but will terminate itself if it sees the keyboard layout language is of a Slavic language such as Russian, Ukrainian, Tartar, etc. [23]. Avaddon exhibits similar behavior to that observed in ransomware such as Ryuk[24] and Cl0P[25]. An analysis of Avaddon's recent targets by the team at DarkTrace showed that the top impacted verticals were manufactured consumable and technology[26], with two of its most notable victims being AXA[27], [28] and Acer Finance[28].



Example of DDoS'ed Victim[3]



Sample Avaddon Infection Email[6]

$40,000 USD

Avaddon's average ransom amount is in bitcoin with variations based on annual revenues[29].

CL0P

CL0P was first discovered in February 2019 as a new variant in the cryptomix family. Their first target was German tech firm – Software AG in October 2020[30]. CL0P infections can be detected through the .CL0P file extension, but different extensions of this ransomware have been observed after encryption such as .ciip, .clip, .c_l_0_p[30], [31].

Based on the use of ransomware binary specific to the victim, including an embedded 1024-bit RSA public key and a unique ransom note, multiple processing threads are spawned to each each target file into memory, encrypt the data using the Windows CryptoAPI and then writing this encrypted data to a new file before the original is deleted.

```
CryptAcquireContextW (in: phProv=0x259e1b0, szContainer=0x0, szProvider="Microsoft Enhanced RSA
and AES Cryptographic Provider", dwProvType=0x18, dwFlags=0x0 | out:
phProv=0x259e1b0*=0x2429e8) returned 1
[...]
CreateFileW (lpFileName="C:\\<DIRECTORY>\\<ORIGINAL_FILENAME>.Clop" (normalized:
"c:\\<DIRECTORY>\\<ORIGINAL_FILENAME>.clop"), dwDesiredAccess=0x40000000, dwShareMode=0x2,
lpSecurityAttributes=0x0, dwCreationDisposition=0x2, dwFlagsAndAttributes=0x80,
hTemplateFile=0x0) returned 0x298
[...]
CryptStringToBinaryA (in: pszString="-----BEGIN PUBLIC KEY----- <RSA_PUBLIC_KEY_DATA> -----END
PUBLIC KEY-----", cchString=0x0, dwFlags=0x0, pbBinary=0x259d1b0, pcbBinary=0x259d1a4,
pdwSkip=0x0, pdwFlags=0x0 | out: pbBinary=0x259d1b0, pcbBinary=0x259d1a4, pdwSkip=0x0,
pdwFlags=0x0) returned 1
[...]
CryptEncrypt (in: hKey=0x2439f8, hHash=0x0, Final=1, dwFlags=0x0, pbData=0x255ad8*,
pdwDataLen=0x259d19c*=0x75, dwBufLen=0x80 | out: pbData=0x255ad8*, pdwDataLen=0x259d19c*=0x80)
returned 1
WriteFile (in: hFile=0x298, lpBuffer=0x255ad8*, nNumberOfBytesToWrite=0x80,
lpNumberOfBytesWritten=0x259e1e8, lpOverlapped=0x0 | out: lpBuffer=0x255ad8*,
lpNumberOfBytesWritten=0x259e1e8*=0x80, lpOverlapped=0x0) returned 1
[...]
DeleteFileW (lpFileName="C:\\<DIRECTORY>\\<ORIGINAL_FILENAME>" (normalized:
"c:\\<DIRECTORY>\\<ORIGINAL_FILENAME>")) returned 1
```

Encryption proess (abridged) followed by original file deletion

It was initially discovered that CL0P was tied to the threat actor group, TA505, a financially motivated threat group that has been active since at least 2014, and later to the TA505 spinoff group FIN11. In 2020, FIN11 began using CL0P to target HPH companies, including:

- 20200430: ExecuPharm, Inc., a U.S-based pharmaceutical research company
- 20200505: Carestream Dental LLC, a U.S.-based provider of dental equipment Carestream Dental LLC
- 20201106: Nova Biomedical, a U.S.-based medical device manufacturer

CL0P is often delivered through phishing campaigns via zip files and docx files using malicious macros. This ransomware is known for killing processes and services related to data backups and security controls. It also attempts to detect and not execute within virtual environment to avoid analysis and detection through code signing[32].

CL0P has been linked to threat actors that exploited Accellion File Transfer Appliance (FTA) vulnerabilities such as CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104 in February 2021[33]. The ransomware has created their own tor-based site where victims who do not pay ransom or ignore threats have their confidential data publicly exposed.

Notable targets and victims include Qualys, Shell, Stanford University, Singtel (Singapore telecom), Bombardier, Jonesday, SoftwareAG, and University of California, with the highest ransom being paid by their first target, a German software company named Software AG. Software AG's ransom was a total of $23M USD[3]. CL0P ransomware is also behind the breaches of biopharmaceutical firm, ExecuPharm, Indian business group, Indian bulls, and UK's biggest EV, Cargo Logistics. CL0P ransomware is widely spread. Countries targeted by this threat actor include: Switzerland, Great Britain, Belgium, United States, The Netherlands, Croatia, Porto Rico, Germany, Turkey, Russia, Denmark, Mexico, Canada, and the Dominican Republic.

CL0P is often delivered through phishing campaigns via zip files and docx files using malicious macros.

So far, CL0P has targeted multiple industries including transportation, logistics, healthcare, manufacturing, education, financial, aerospace, telecommunication.

Darkside

Darkside ransomware is a human-operated "double-extortion" ransomware operation that has been active since at least August 2020. One of the very first victims posted on Darkside's data leak site was the North American land developer Brookfield Residential[34]. The operators of Darkside Ransomware claim to have previously earned 1 million dollars of profit through other ransomware-as-a-service products before moving onto making and running their own operation due to dissatisfaction in the RaaS marketplace offerings [35]. Victims who choose not to pay Darkside's ransom have their exfiltrated files freely available on Darkside's data leak site for at least six months before they are removed[35].

On May 10 2021, Darkside received global attention due to an alleged unintentional attack on Colonial Pipeline which caused a three-day shutdown of the largest refined oil pipeline system in North America[36].

In response to the ransom, the Darkside operators received $4.4M USD from Colonial Pipeline in exchange for the decryption key for their network. On May 13, Darkside announced they were ceasing operations, but on May 20, threat researchers at RISKIQ found that at least one Darkside affiliate, UNC2465, still had an active attack infrastructure [37].

UNC2465 has been observed using phishing emails containing links (T1566.002 – Phishing: Spearphishing Link) to legitimate services Shopify, Google Drive, or Drop Box [38]. These services host a .LNK file (T1204.002 – Malicious Execution: Malicious File) that contacts the adversary owned EMPIRE C2 infrastructure to receive a PowerShell-based .NET backdoor that researchers have named SMOKEDHAM[39] (T1105 – Ingress Tool Transfer). SMOKEDHAM contains keylogging (T1056.001- Input Capture: Keylogging) and screen capture (T1113 – Screen Capture) functionality, as well as the ability to execute arbitrary .NET commands (T1059.001- Command and Scripting Interpreter: PowerShell) [39].

Darkside and its affiliates have claimed to only target companies that can afford to pay their requested ransom. The group also alleges the ransom amount is determined post-intrusion, by figuring out "how much [the company] can pay based on [the company's] net income" [40]. They have also alluded to the fact that they target organizations with ransomware insurance and their ransom does not usually exceed the amount of their insurance coverage [41]. Darkside's average requested payment amount is approximately $6.53M USD and their most frequent targets have been law firms and professional service providers, the producers and distributors of consumable goods, [40], financial institutions, and insurance agencies.

In the first half of 2021, Darkside leaked data from at least 13 legal firms across North America and Europe[16]. Other high-profile leaks have included the financial institution Exim Bank Indonesia[42], insurance brokerage, The Leavitt Group[16], Canadian retailer, Home Hardware[43], and the American clothing retailer, GUESS clothing[41].

$6.53M USD

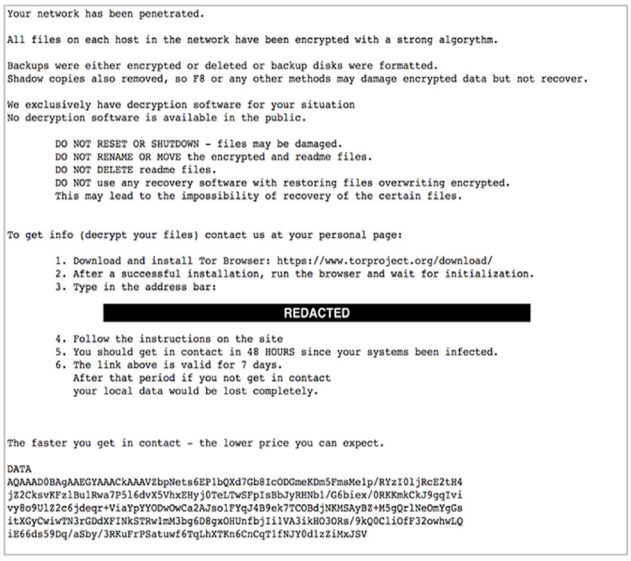
Darkside's approximate average requested payment amount.

"

In the first half of 2021, Darkside leaked data from at least 13 legal firms across North America and Europe[16].

Doppelpaymer

Doppelpaymer ransomware was first observed in 2019 as reported by Trend Micro . It is believed to be based off Bitpaymer ransomware[4], leverages 2048-bit RSA and 256-bit AES encryption[4] and uses threaded file encryption for rapid encryption as an upgrade to Bitpaymer[4]. A new feature included in Doppelpaymer is the use of Process Hacker to terminate services and processes related to security, email, back up, and database software[4]. This is done to prevent access violations during encryption[4] and increase the rate of successful encryption. Doppelpayer's initial infection vector is via malicious emails containing spearphishing links/malicious attachments disguised as a document[4].



```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                        REDACTED

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 7 days.
           After that period if you not get in contact
           your local data would be lost completely.


The faster you get in contact - the lower price you can expect.

DATA
AQAAAD0BAgAAEGYAAACkAAAVZbpNets6EPlbQXd7Gb8IcODGmeKDm5FmsMelp/RYzI0ljRcE2tH4
jZ2CksvKFzlBulRwa7P5l6dvX5VhxEHyj0TeLTwSFpIsBbJyRHNbl/G6biex/0RKKmkCkJ9gqIvi
vy8o9Ul2c6jdeqr+ViaYpYYODwOwCa2AJsolFYqJ4B9ek7TCOBdjNKMSAyBZ+M5qQrlNeOmYgGs
itXGyCwiwTN3rGDdXFINkSTRwlmM3bg6D8gxOHUnfbjIilVA3ikHO3ORs/9kQ0CliOfF32owhwLQ
iE66ds59Dq/aSby/3RKuFrPSatuwf6TqLhXTKn6CnCqTlfNJY0dlzZiMxJSV
```

DoppelPaymer ransom note

Doppelpaymer has also been observed to download other malware during its execution [4]. Once successfully infected and encrypted, Doppelpaymer operators will leverage the double extortion method, threatening to leak stolen files with the hopes of expediting ransom payment. Doppelpaymer operators will often state they will lower the ransom price depending on how quickly the victim pays[4],[5]. A review of data leak victims produced by DarkTrace[26] demonstrates DoppelPaymer has been observed targeting the manufactured consumables industry, with secondary targeting of the public sector. DoppelPaymer has successfully compromised notable victims such as Hyundai Motors of America[44],[45], KIA[46] and the City of Torrance in Los Angeles, California [47]. KIA and Hyundai Motors of America was initially ransomed for approximately $20M USD in Bitcoin but would eventually be ransomed for $30M USD if the initial ransom offer was not paid[45].

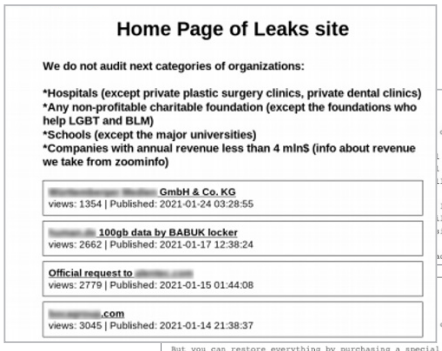
The City of Torrance was ransomed for approximately $700K USD and had 200GB worth of data stolen, none of which was reported to be public personal data[47].

Doppelpayer's initial infection vector is via malicious emails containing spearphishing links/ malicious attachments disguised as a document[4].

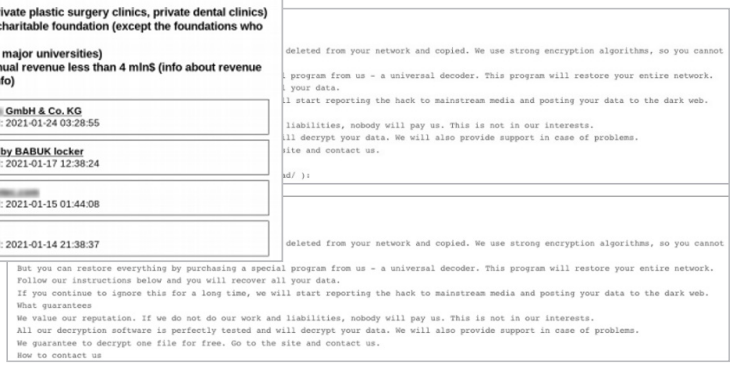
HERJAVEC GROUP

Babuk

Babuk, also known as 'Babuk Locker' and initially 'Vasa Locker', is a new ransomware threat discovered earlier in 2021 and has impacted a total of 38 enterprises, with one successful ransom of $85K USD in Bitcoin after negotiation[48]. The ransom gang also targeted Washington D.C Police, stealing 250 gigabytes of data and later proceeded to dox officers in an effort to extort ransom for the stolen data[49]. The group has been observed to target the consumable industry and like other threat actors, the technology industry is their second preferred target followed by the public sector[50],[16].



Babuk leak site[18]



Babuk and Vasa Ransom Notes

The group has officially stated on their leak website they will not target hospitals, non-profit charities, or schools and will avoid organizations with annual revenues of less than $4M USD[51]. However, they considered private and major universities 'fair game' along with charitable foundations 'who help LGBT and BLM' cause[51]. The ransomware first appeared on raidforums.com with the post "Babuk for press" by user "biba99"[51] According to MacAfee's research team Babuk Locker shares many similarities with Vasa Locker including using the same Ransom note for their victims[52].

Other similarities include:

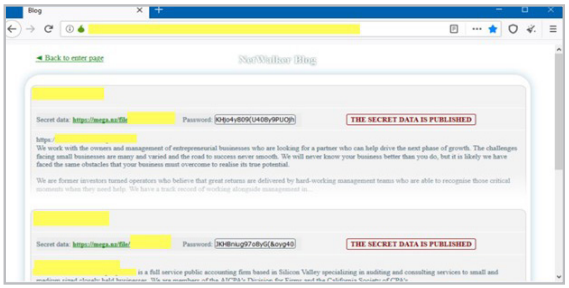
- Use of the same extension added to encrypted files "__NIST_K571__"
- Use of the same cryptographic method
- The process kill list and directories list is

The group was active on famous malware forums XSS[.]is and exploit[.]in to recruit new members to the team and create an affiliate model[53]. During this time, they were also looking for additional initial attack vectors and posted "[Buying] 1-0 day RCE corp vpn [exploit]" on the forum[53]. Babuk is under constant development and have developed newer versions of the malware available for *nix (ESXI, NAS)[53].

38

Total number of enterprises who have been impacted by Babuk, so far.

Netwalker

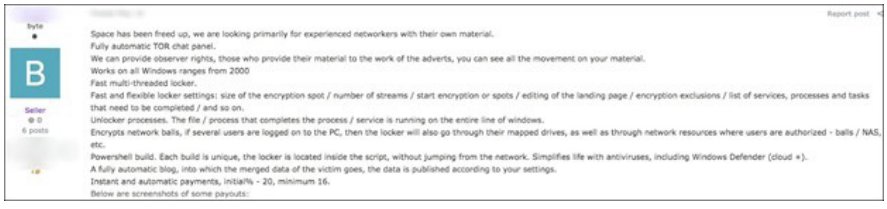


The NetWalker ransomware was created by the cybercriminal group known as 'Circus Spider' and was first discovered in August 2019. On the surface, NetWalker acts like most other ransomware variants, establishing an initial foothold through phishing emails, followed by data extraction, and encrypting sensitive data to hold hostage for a large extorsion[54]. However, this ransomware does more than just hold the victim's data hostage. To show they are serious, the team behind the attack will leak a sample of the data online and threaten to release more to pressure the enterprise to pay the ransom on time.

In March 2020, NetWalker shifted to a ransomware-as-a-service (RaaS) model[1], and Circus Spider began looking for affiliates to distribute the NetWalker malware in exchange for a percentage of the ransom collected.

The group published benefits that recruited partners would have access to, including:

- Fully automatic TOR chat Panel
- Observer rights
- Works on all Windows devices from windows 2000 up
- Fast multi-thread locker
- Fast and flexible locker settings
- Unlocker processes
- Adjacent network encryption
- Unique PowerShell builds making it easier to deal with antivirus software.
- Instant payouts



Circus Spider's agenda with NetWalker is to target high paying victims like hospitals, educational institutions, and government. To capitalize on the current pandemic, they have been leveraging phishing emails focused on COVID-19 as a recent threat vector.

As part of RaaS, affiliates would target victims in one of several different methods. The following methods are the most frequently observed:

- Phishing emails with attached malicious files, like VBScript or PowerShell.
- Exposed or vulnerable Remote Desktop Protocol (RDP) services and EXE files.
- Changing encrypted files to a .mailto extension.

Preventing and Responding to a Ransomware Incident

The HG Threat Team suggests the following to deal with active incidents and prevent further breaches:

When responding to an active infection

- **First things, first:** Disrupt any active infections by removing the infected device from the network until it can be re-imaged or cleaned. Do this by unplugging the network cable or turning the device off altogether.

- **You can pay the ransom:** Sometimes it works, but this isn't recommended by Herjavec Group or any law enforcement. This can embolden adversaries and decrypting large amounts of infected data, especially on network volumes, may be slower than restoring from backups.

- **Leverage your proactive resources:** Restore data from back-ups and re-image the infected devices. Re-image the device from known-good images, to eliminate not only the detected ransomware but any other malware that may have been downloaded at the same time.

- **Eradicate the source of the infection:** If you suspect that the malware was delivered via email, it may be useful to find the source email and delete it from all mailboxes to prevent reinfections.

- **Be prepared:** Have an **Incident Response** team on retainer so they can step in and respond in the most effective and efficient way during an active infection.

To further prevent ransomware breaches in the future

- Deploy advanced web and email gateway protection.
- Block potential adversary threat vector such as adware, known bad domains (blacklists for C2 servers), and unknown/unclassified domains by leveraging web content filtering appliances or firewall features. While this can cause minor impacts to business, being intentional about which appliances and firewall features you implement will generally only result in tolerable restrictions.
- Implement advanced endpoint protection including behavior driven analysis. Ensure your endpoint protection examines traffic for behaviors, rather than just file-matching.

HERJAVEC GROUP

Preventing and Responding to a Ransomware Incident

- Deploy a Microsoft Group Policy to restrict software's ability to run from %appdata% and "temp" folders. These are generally used by malware because all users have the ability to write to these locations predictably, and permission cannot be restricted without affecting system function. However, there are few-to-none reasons why software should install or have to run from these directories. If the malware can't run, it can't do any harm.

- Restrict web browsing and email use by privileged users such as administrators. Have separate accounts for administration and day-to-day computing.

- Implement Privileged Access Management best practices. Minimize the permissions to network file shares. Give the ability to write/modify files only to the users that require it, and only to the necessary locations.

- Carry out a policy that no corporate information should be stored on local hard drives, USB drives, or other local storage. Files stored on the network are normally backed up and can be restored with minimal disruption to the business.

- Educate the people using your devices on how to recognize spam and phishing emails and what to do if they receive it.

- Prepare for the worst, and have an Incident Response plan ready. The worst time to decide what to do about an attack is after it has occurred. If your organization doesn't already have one, we suggest using the 10 Point IR Plan from our Cybersecurity Conversations Report as a blueprint to developing one that fits your organization's needs.

Ransomware is constantly evolving and as long as adversaries can keep up with the latest defense tactics, the result is always the same. The best way to stay out of the adversary's shadow is to implement best practices for cyber defense, continuously improve your cybersecurity posture, and be prepared to respond quickly and effectively to any breaches that may occur.

HERJAVEC GROUP

Robert Herjavec founded Herjavec Group in 2003 to provide cybersecurity products and services to enterprise organizations. We have been recognized as one of the world's most innovative cybersecurity operations leaders, and excel in complex, multi-technology environments. We have expertise in comprehensive security services, including Advisory Services, Technology Architecture & Implementation, Identity & Access Management, Managed Security Services, Threat Hunting & Management, Digital Forensics and Incident Response. Herjavec Group has offices and Security Operations Centers across the United States, United Kingdom, Canada and India.
For more information, visit HerjavecGroup.com or contact us at info@herjavecgroup.com.

References

[1] "Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows." https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx (accessed May 26, 2021).

[2] "fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf." Accessed: May 26, 2021. [Online]. Available: https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf

[3] Clop Ransomware Attack Hits German Software Giant Software AG; Confidential Documents Stolen, $23 Million Ransom Demanded," CPO Magazine, Oct. 19, 2020. https://www.cpomagazine.com/cyber-security/clop-ransomware-attack-hits-german-software-giant-software-ag-confidential-documents-stolen-23-million-ransom-demanded/ (accessed May 21, 2021).

[4] "An Overview of the DoppelPaymer Ransomware," Trend Micro, Jan. 05, 2021. https://www.trendmicro.com/en_ca/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html (accessed May 20, 2021).

[5] B. Stone-Gross, S. Frankoff, and B. Hartley, "CrowdStrike Discovers New DoppelPaymer Ransomware & Dridex Variant," Jul. 12, 2019. https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/ (accessed Jan. 07, 2021).

[6] S. Kalollu, "The Ryuk-Conti Connection: A Ransomware Blog | Blog eScan." http://blog.escanav.com/2020/07/the-ryuk-conti-connection-a-ransomware-blog/ (accessed May 25, 2021).

[7] "Conti Ransomware Resurfaces, Targeting Government & Large Organizations | Cyble." https://cybleinc.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/ (accessed May 27, 2021).

[8] N. Craig-Wood, rclone/rclone. rclone, 2021. Accessed: Feb. 18, 2021. [Online]. Available: https://github.com/rclone/rclone

[9] The DFIR Report, "Conti Ransomware," The DFIR Report, May 12, 2021. https://thedfirreport.com/2021/05/12/conti-ransomware/ (accessed May 25, 2021).

[10] R. Lanigan, "Conti Ransomware: Facts, Figures and Advice — Smarttech247," Smarttech247 - Innovative Managed Security Provider, May 17, 2021. https://www.smarttech247.com/news/conti-ransomware-facts-figures-and-advice/ (accessed May 25, 2021).

[11] A. I. Response, "Is Conti the New Ryuk?," Arete, Aug. 2020. Accessed: Aug. 25, 2020. [Online]. Available: https://areteir.com/wp-content/uploads/2020/08/Arete_Insight_Is-Conti-the-new-Ryuk_August2020.pdf

[12] L. Constantin, "REvil ransomware explained: A widespread extortion operation," CSO Online, Nov. 17, 2020. https://www.csoonline.com/article/3597298/revil-ransomware-explained-a-widespread-extortion-operation.html (accessed May 25, 2021).

[13] SecureWorks, "GOLD SOUTHFIELD," 2020. https://www.secureworks.com/research/threat-profiles/gold-southfield (accessed May 23, 2020).

[14] Counter Threat Unit Research Team, "REvil/Sodinokibi Ransomware," SecureWorks, Sep. 24, 2019. https://www.secureworks.com/research/revil-sodinokibi-ransomware (accessed May 25, 2021).

[15] Trend Micro, "Sodinokibi Ransomware Information," Trend Micro Business Success, Jan. 21, 2020. https://success.trendmicro.com/solution/000238277-Sodinikibi-Ransomware-Information (accessed May 25, 2021).

[16] DarkTracer, "List of victim organizations attacked by ransomware gangs released on leak sites." May 17, 2021. Accessed: May 20, 2021. [Online]. Available: https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3/edit#gid=1321518761

[17] "List of ransomware that leaks victims' stolen files if not paid," BleepingComputer. https://www.bleepingcomputer.com/news/security/list-of-ransomware-that-leaks-victims-stolen-files-if-not-paid/ (accessed May 19, 2021).

[18] P. Arntz, "Avaddon ransomware campaign prompts warnings from FBI, ACSC," Malwarebytes Labs, May 11, 2021. https://blog.malwarebytes.com/ransomware/2021/05/avaddon-ransomware-campaign-prompts-warnings-from-fbi-acsc/ (accessed May 19, 2021).

[19] "Another ransomware now uses DDoS attacks to force victims to pay," BleepingComputer. https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/ (accessed May 19, 2021).

[20] Australian Cyber Security Centre, "2020-003: Ongoing campaign using Avaddon Ransomware," p. 6, May 2021.

[21] "Maze Ransomware – Double Extortion Attack," Check Point Software. /cyber-hub/threat-prevention/ransomware/maze-ransomware-double-extortion-attack/ (accessed May 19, 2021).

[22] "Egregor Ransomware Launches String of High-Profile Attacks to End 2020," Trend Micro, Dec. 14, 2020. https://www.trendmicro.com/en_ca/research/20/l/egregor-ransomware-launches-string-of-high-profile-attacks-to-en.html (accessed May 19, 2021).

[23] T. M. T. R. Team, "Ransomware Report: Avaddon and New Techniques Emerge, Industrial Sector Targeted," Jul. 08, 2020. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted (accessed Jul. 30, 2020).

[24] A. Hanel, "Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware," Jan. 10, 2019. https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/ (accessed Dec. 20, 2019).

[25] A. Mundo and M. R. López, "Clop Ransomware," Aug. 01, 2019. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/clop-ransomware/ (accessed Jan. 06, 2020).

[26] "[DarkTracer] List of victim organizations attacked by ransomware gangs released on the Dark-Web.xlsx - Google Sheets." https://docs.google.com/spreadsheets/d/1MI8Z2tBhmqQ5X8Wf_ozv3dVjz5sJOs-3/edit#gid=1321518761 (accessed May 20, 2021).

[27] "Insurer AXA hit by ransomware after dropping support for ransom payments," BleepingComputer. https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/ (accessed May 19, 2021).

[28] "Avaddon Ransomware gang hacked France-based Acer Finance and AXA Asia," Security Affairs, May 16, 2021. https://securityaffairs.co/wordpress/117991/cyber-crime/avaddon-ransomware-acer-finance-axa.html (accessed May 19, 2021).

[29] "Avaddon Ransomware Incident Response," BeforeCrypt. https://www.beforecrypt.com/en/avaddon-ransomware-removal-decryption-and-data-recovery/ (accessed May 21, 2021).

[30] "CL0P Ransomware." https://blog.cyberint.com/cl0p-ransomware (accessed May 21, 2021).

[31] "Threat Assessment: Clop Ransomware," Unit42, Apr. 13, 2021. https://unit42.paloaltonetworks.com/clop-ransomware/ (accessed May 21, 2021).

[32] "Detecting Clop Ransomware | Splunk." https://www.splunk.com/en_us/blog/security/detecting-clop-ransomware.html (accessed May 21, 2021).

[33] "Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion," FireEye. https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html (accessed May 21, 2021).

[34] L. Abrams, "DarkSide Ransomware hits North American real estate developer," BleepingComputer, Aug. 25, 2020. Accessed: May 24, 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/darkside-ransomware-hits-north-american-real-estate-developer/

[35] L. Abrams, "DarkSide: New targeted ransomware demands million dollar ransoms," Bleeping-Computer, Bleeping Computer, Aug. 21, 2020. Accessed: Aug. 24, 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/

[36] M.-A. Russon, "US fuel pipeline hackers 'didn't mean to create problems,'" BBC News, May 10, 2021. Accessed: May 24, 2021. [Online]. Available: https://www.bbc.com/news/business-57050690

[37] Team RISKIQ, "DarkSide is Standing Down, But Its Affiliates Live On | RiskIQ," External Threat Management, May 20, 2021. https://www.riskiq.com/blog/external-threat-management/darkside-affiliates/ (accessed May 24, 2021).

[38] J. Grob, "Analysis of Infrastructure used by DarkSide Affiliates," RiskIQ, May 2021. Accessed: May 24, 2021. [Online]. Available: https://community.riskiq.com/article/fdf74f23

[39] J. Nuce et al., "Shining a Light on DARKSIDE Ransomware Operations," Threat Research, May 11, 2021. https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html (accessed May 24, 2021).

[40] Arete Cyber Threat Intelligence Team, "Darkside Ransomware: Caviar Taste on Your Big-Game Budget," Arete, Feb. 23, 2021. https://www.areteir.com/darkside-ransomware-caviar-taste-on-your-big-game-budget/ (accessed Apr. 26, 2021).

[41] Dissent, "A chat with DarkSide," The Office of Inadequate Security, Apr. 21, 2021. https://www.databreaches.net/a-chat-with-darkside/ (accessed May 24, 2021).

[42] A. Nugroho, "Yang Perlu Diketahui tentang Peretasan Colonial Pipeline," cyberthreat.id, May 11, 2021. https://cyberthreat.id/read/11577/Yang-Perlu-Diketahui-tentang-Peretasan-Colonial-Pipeline (accessed May 24, 2021).

[43] H. Solomon, "Canadian retailer Home Hardware hit by ransomware," IT World Canada, Apr. 02, 2021. Accessed: May 24, 2021. [Online]. Available: https://www.itworldcanada.com/article/canadian-retailer-home-hardware-hit-by-ransomware/445416

[44] F. Bajak, "Kia and Hyundai recovering from days-long network outages," CTVNews, Feb. 18, 2021. https://www.ctvnews.ca/autos/kia-and-hyundai-recovering-from-days-long-network-outages-1.5315317 (accessed May 20, 2021).

[45] S. STAHIE, "DoppelPaymer Gang Reportedly Attacked Kia Motors America with...," HOTforSecurity, Feb. 19, 2021. https://hotforsecurity.bitdefender.com/blog/doppelpaymer-gang-reportedly-attacked-kia-motors-america-with-ransomware-25363.html (accessed May 20, 2021).

[46] "Kia Motors America suffers ransomware attack, $20 million ransom," BleepingComputer. https://www.bleepingcomputer.com/news/security/kia-motors-america-suffers-ransomware-attack-20-million-ransom/ (accessed May 20, 2021).

References

[47] "DoppelPaymer Ransomware hits Los Angeles County city, leaks files." https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-hits-los-angeles-county-city-leaks-files/ (accessed May 20, 2021).

[48] A. Mundo, T. Seret, T. Roccia, J. Fokker, and V. Mairet, "Babuk Ransomware," McAfee Blogs, Feb. 24, 2021. /blogs/other-blogs/mcafee-labs/babuk-ransomware/ (accessed May 21, 2021).

[49] L. Vaas, "Babuk Ransomware Gang Targets Washington D.C. Police | Threatpost," Threatpost, Apr. 27, 2021. Accessed: May 21, 2021. [Online]. Available: https://threatpost.com/babuk-ransomware-washington-dc-police/165616/

[50] D. Galov, L. Bezvershenko, and I. Kwiatkowski, "Ransomware world in 2021: who, how and why," May 12, 2021. https://securelist.com/ransomware-world-in-2021/102169/ (accessed May 21, 2021).

[51] biba99, "Babuk for Press," Raid Forums, 2021. https://raidforums.com/Thread-Babuk-for-press

[52] A. Mundo, T. Seret, T. Roccia, and J. Fokker, "Technical Analysis of Babuk Ransomware," McAfee, Feb. 2021. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-babuk-ransomware.pdf

[53] Cyberint Research, "Industry Security Bulletin: Babuk Ransomware," Security Bulletin, Jan. 2021. Accessed: May 21, 2021. [Online]. Available: https://e.cyberint.com/hubfs/Babuk_Bulletin_January_2021.pdf

[54] N. Coppinger, "Netwalker Ransomware Guide: Everything You Need to Know," Inside Out Security, Nov. 17, 2020. https://www.varonis.com/blog/netwalker-ransomware/ (accessed May 25, 2021).

[55] Brian Baskin, "TAU Threat Discovery: Conti Ransomware," Carbon Black, July 8, 2020. https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/ .