CYDERES

Cyber Defense & Response

It's what we do.

STATE OF RANSOMWARE 2022

RANSOMWARE OPERATION ACTIVITY (H1 / '22)

Page of Contents

Executive Summary

EVOLVING TO COUNTER RANSOMWARE

As ransomware continues to be a major threat over time, organizations have demonstrated the ability to become better and faster at detecting and recovering from ransomware events. Despite this however, in the first two fiscal quarters of 2022, there has been an 8% increase in victims paying ransoms of US$1 million or more when compared to last year[1]. Furthermore, ransomware operators continue to mature as they learn lessons from the attacks of the previous ransomware groups who had come before them. The average time-to-encrypt during ransomware attacks has seen a reduction, with multiple groups utilizing techniques such as encrypting files on multiple CPU threads to process more data at once, and automatically exfiltrating stolen files to legitimate cloud service storage accounts with legitimate command line tools.

Crimeware threat groups associated with ransomware attacks continue to use the "double extortion" method; which is the act of exfiltrating sensitive data from the victim's network before the encryption stage of the attack. In the first half of 2022, the sectors the most impacted by data leaks are manufacturing and industry; healthcare and pharmaceutical; and educational institutes. This closely follows trends observed last year around this time; however, the education sector has seen an increase of data leaks while the volume of data leaks observed within the technology sector has slightly declined[2,3].

Interestingly, even though attacks on the education and healthcare sector have increased when compared to last year, these industries have been observed having the lowest average ransomware payouts. Conversely, the highest average ransomware payouts continue to be observed in the manufacturing and industrial sectors[1].

In this report, Cyderes' Special Operations team has analyzed some of most highly effective and prolific ransomware operators observed this far in 2022 including:

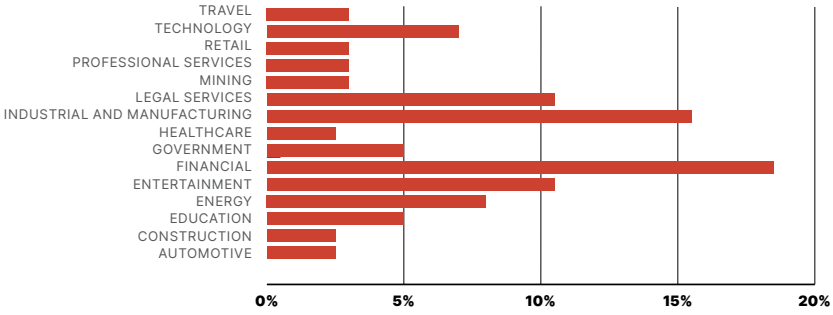
- **BLACKCAT**
- **CONTI**
- **CL0P**
- **HIVE RANSOMWARE**
- **LAPSUS$**
- **LOCKBIT**
- **VICE SOCIETY**

BlackCat

ALPHV, NOBERUS

BlackCat, also known as ALPHV or Noberus is a data-leak Ransomware as a Service (RaaS) operation family which has been active since at least November 2021[4]. BlackCat targets both Windows and Unix-based machines[5]. The group has been seen looking for "Windows / Linux / ESXI pen-testers" and operational "affiliates" on hacking forums such as XSS, Exploit Forum, and RAMP[5]. BlackCat has borrowed a significant amount of code from BlackMatter Ransomware; including parts of BlackMatter's command configurations[6]. According to the FBI, as of March 2022, BlackCat had successfully compromised at least 60 businesses worldwide[7]. The FBI believes BlackCat to be the first officially known successful ransomware operation with an encryptor built in the Rust programming language[7].

BLACKCAT DATA-LEAK VICTIMS BY INDUSTRY



BlackCat's operators have observed been gaining access (TA0001 - Initial Access)[8] via third party frameworks such as Cobalt Strike and/or via exposed and vulnerable Windows and Linux systems with exposed remote services (T1133 – External Remote Services, T1190 – Exploit Public Facing Application)[9-11] and previously compromised user credentials (T1078.002 - Valid Accounts: Domain Accounts, T1110.004 - Brute Force: Credential Stuffing)[12,13]. Following Initial Access and prior to encrypting files, BlackCat exfiltrates sensitive data both from cloud and on-premises sources (T1020 – Automated Exfiltration) to adversary-controlled cloud infrastructure using rclone (T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage)[14]. Following this, BlackCat has been observed using Windows Task Scheduler (T1053.005 – Scheduled Task/Job: Scheduled Task) to configure malicious Group Policy Objects (T1484.001 Domain Policy Modification: Group Policy Modification) which in-turn, will deploy the encryptor across the environment (T1486 – Data Encrypted for Impact).

Like many other ransomware operators, BlackCat's target selection may be opportunity-based, rather than specifically focused on certain industries and countries[15].

BlackCat's victims have included organizations involved in construction, engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components, and pharmaceuticals around the globe.

Conti

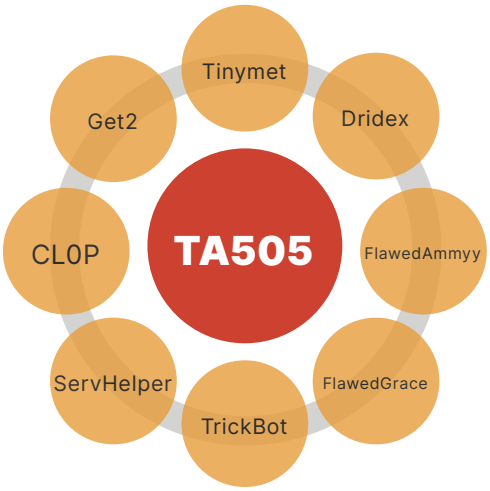
Conti is another "double-extortion" Ransomware-as-a-Service group which operated as the successor to Ryuk ransomware. Conti has been operational since at least December 2020[16]. Conti operated an extremely successful ransomware operation operating up until mid-May 2022, when the group announced they were disbanding the operation in favor of multiple sub-groups[17]. Conti was first publicly observed on December 24, 2020 after successfully breaching the Environment Protection Agency of Scotland[16].

Conti's victims have included government agencies and public entities including 911 dispatch centers, as well as city-hall and court infrastructures, energy distributors and producers, businesses in the financial industry, high-tech and IT service providers, to name a few[18]. In 2022, Conti has been observed gaining Initial Access via phishing emails (T1566 – Phishing) containing adversary-controlled links (T1024.001 – User Execution: Malicious Link) and/or macro-enabled "mal-docs" (T1024.002 – User Execution: Malicious File, T1059.005 – Command and Scripting Interpreter: Visual Basic) which initiate the infection chain upon opening. Additionally, the group has also achieved access via stolen Remote Desktop Protocol Credentials[19,20].

Conti has also exploited a number of vulnerabilities such as "Print Nightmare" (CVE-2021-3457) and "ZeroLogon" (CVE-2020-1472) to facilitate privilege escalation (T1068 – Exploitation for Privilege Escalation) and lateral movement (T1210 - Exploitation of Remote Services)[19]. Before the encrypting stage of the ransomware attack begins, Conti operators have frequently used the opensource command-line storage management tool rclone to exfiltrate data to adversary-controlled cloud storage (T1567.002 - Exfiltrate Over Web Service: Exfiltration to Cloud Storage)[19]. Then, Conti uses the Windows API (T1106 - Native API[21]) to make calls to the Windows Restart Manager to disable security tools (T1562.001 – Impair Defenses: Disable or Modify Tools), delete backups (T1490 – Inhibit System Recovery), and to unlock in-use applications. This is followed by the deletion of shadow copies with vssadmin[22]

Conti's encryptor iterates through the network's shared drives via SMB (T1021.002 SMB/Windows Admin Shares) and supports up to 32-simultaneous CPU threads to speed up the encryption process using an AES-256 encryption key combined with an RSA-4096 public encryption key (T1486 Data Encrypted for Impact)[22].

CL0P



CL0P ransomware is believed to be tied to the threat actor group TA505, a financially motivated threat group which has been active since at least 2014. CL0P ransomware was first discovered in February 2019 as a new variant in the cryptomix family[23]. CL0P infections can be identified through the use of a .CL0P, .ciip, .clip, or .c_l_0_p file extension being appended the encrypted victim files after a successful attack[24,25]. CL0P is another "double-extortion" group which runs a data-leak site named "CL0P^_- LEAKS". Despite the arrest of six suspected CL0P members in Ukraine in June 2021, CL0P has continued to operate uninterrupted [26]. The most targeted sector for CL0P has been the industrial and manufacturing sectors, which are believed to make up approximately 45% of CL0P's attacks, followed by technology industry making up at least 27% of their observed victims[27].

> **CL0P's targets have included organizations across multiple industries including but not limited to transportation, logistics, healthcare, manufacturing, academic institutes, the financial and professional service industries, aerospace, and telecommunication providers[28].**

CL0P operators have been observed obtaining Initial Access via phishing emails containing exploits such as CVE-2021-27101 (Accellion FTA SQL Injection), CVE-2021-27102 (Accellion FTA Command Execution via a local web service call), CVE-2021-27013 (Accellion FTA Server-side request forgery vulnerability), CVE-2021-27104 (Accellion FTA command injection), and CVE-2021-35211 (SolarWinds Serv-U remote memory escape)[26].

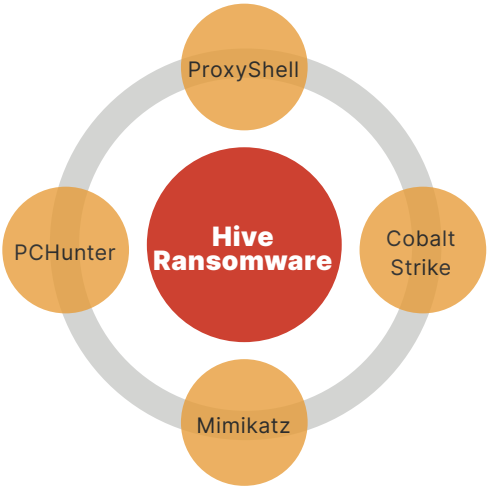
These exploits have also been nested inside of zip files (T1027 - Obfuscated Files or Information), and docx files with malicious macros (T1204.002 - User Execution: Malicious File, T1059.005 - Command and Scripting Interpreter: Visual Basic). CL0P tries to kill process and services related to data backups and security controls T1562.001 – Impair Defenses: Disable or Modify Tools before executing the encrypting stage (T1489 - Service Stop, T1490 - Inhibit System Recovery). The ransomware also further attempts to evade defenses by detecting virtual environments, and by having legitimate code signatures associated with the ransomware from Thawte and Sectigo (T1497.001 – Virtualization/Sandbox Evasion: System Checks, T1553.002 – Subvert Trust Controls)[29,30].

Hive Ransomware

HIVE, DEV-0237

Hive Ransomware, AKA Hive, has been active since at least August 2021. Hive is another RaaS (Ransomware as a Service) group using the "double-extortion" method[31]. Hive has been observed stealing both corporate sensitive information and personally identifying information (PII) with intent to publish this data on their dedicated leak site, HiveLeaks[31]. Hive ransomware group has been observed targeting organizations globally in the energy, healthcare, finance, media, education, manufacturing, telecommunications, and technology industries, as well as government-aligned institutions[32]. Hive has been observed breaching over 350 organizations within a four-month period [31].

During summer 2021, Hive Ransomware Group operators were observed using multiple mechanisms to obtain access to networks; including phishing emails containing malicious attachments used to deploy Cobalt Strike (T1566.001 – Phishing: Spearphishing Attachment, T1204 User Execution: Malicious File)[33,34]. Hive's operators were observed during this time using Cobalt Strike to facilitate persistence and privilege escalation, and Remote Desktop Protocol (T12021.001 Remote Services: Remote Desktop Protocol) to move laterally within the network[31,32,35]. By October 2021, Hive began targeting Unix-based servers such as ESXi and FreeBSD in addition to Windows systems[31].



> **On March 21, 2022, the group alleged they had successfully exfiltrated 400GB of data from Partnership HealthPlan. According to Hive, the data includes more than 850,000 unique records of Protected Health Information (PHI) including names, SSNs, dates of birth, addresses, and contact information[41].**

And, by 2022, Hive operators also began leveraging the ProxyShell attack-chain during their campaigns. ProxyShell is an attack chain that exploits three vulnerabilities in Microsoft Exchange to achieve privileged remote code execution rights: CVE-2021,-34473, CVE-2021-34523, CVE-2021-31207 [36]. After deploying web shells (T1505.003 Server Software Component: Web Shell)[37] on the impacted Microsoft Exchange servers, Hive operators use this newly obtained SYSTEM level access to run obfuscated PowerShell commands (T1059.001 - Command and Scripting Interpreter: PowerShell, T1027 Obfuscated Files or Information) [38] to create a new user with administrator privileges (T1136 - Create Account)[39]. Next, Hive operators use Mimikatz to obtain and supply the access to the Domain Controller account (T1550.002 – Use Alternate Authentication Material: Pass the Hash)[40].

LAPSUS$

LAPSUS, DEV-0537, UNC3661

Summer 2021

Electronic Arts
EE Limited

December 2021

Brazilian Ministry of Health
Claro, NET, Embratal

January 2022

Okta

February 2022

Nvidia

March 2022

Samsung
Ubisoft

March 2022

Microsoft
T-Mobile, Globant

7 Arrests made in London

Lapsus$ is a cyber-extortion group which has been observed since at least Summer 2021, when an affiliate of the group leveraged unsophisticated techniques and social engineering tactics to gain access to the video game publisher Electronic Arts (EA) network environments via EA's Slack Workspace[42]. Unlike other Big Game Hunting-based (BGH) extortion groups who use the "double-extortion" method, LAPSUS$ has exclusively focused on extortion by means of stealing sensitive information and/or acts of data destruction[43].

In comparison to other extortion-based threat actors, Lapsus$ has been particularly public and boastful about their successes, communicating their attacks via an official telegram channel which they also used to antagonise their victims[44,45]. In March 2022, the City of London Police announced they had arrested seven individuals between the ages of 16-21 believed to be associated with the group. In the days following the arrests, the group continued to release leaks on a few more organizations via Telegram before deleting all Telegram messages and becoming dormant[46,47].

> **Lapsus$' earliest targets primarily were organizations within in the United Kingdom and South America. However, the group quickly began globally targeting organizations in the government, technology, telecom, media, retail, healthcare sectors. In addition to this, the group also targeted cryptocurrency wallets and cryptocurrency exchange user account passwords[45,48,49].**

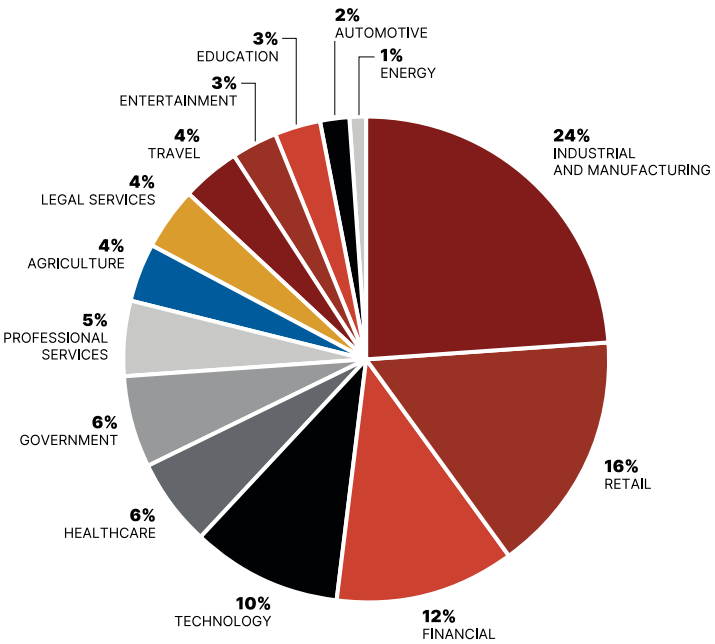
Interestingly, Lapsus$ employed a fairly low-tech operation chiefly consisting of phone-based social engineering, SIM-swapping, personal email account take-over, and bribing employees and/or business partners with money in exchange for access to credentials and multi-factor authentication (MFA) approval[44]. LAPSUS$' public behavior combined with their list of high-profile targets such as Microsoft, EA Sports, Globant, Samsung, Ubisoft and Nvidia[45,48,49] Lapsus$ caused mass disruption and caught global media attention during their short lifespan.

Lockbit

ABCD RANSOMWARE, DEV-0537, UNC3661, BITWISE SPIDER

LockBit ransomware was initially discovered in September 2019. Since then, LockBit has been used in ransomware attacks against a range of industries located across the globe. With the evolution of ransomware operators and their tactics over the past few years, groups like LockBit have implemented successful tactics from other groups to increase their success and/or profits. Since at least June 2021, the LockBit group started advertising "LockBit 2.0" as their new and improved version of the ransomware. Along with this updated version came a slightly updated payment site and information stealing functionality for "double-extortion" purposes and re-branded themselves as the one of the operations with "the fastest encryption speed" in the Ransomware-as-a-Service Industry [50]. As of March 2022, LockBit's ransomware now reads: "LockBit 3.0, The world's fastest ransomware since 2019"[51].

LOCKBIT DATA-LEAK VICTIMS BY INDUSTRY



LockBit has been extremely prolific – The group's data leak site claims that the group has successfully exfiltrated data from nearly 400 victims globally in the first half of 2022, across all industry verticals.

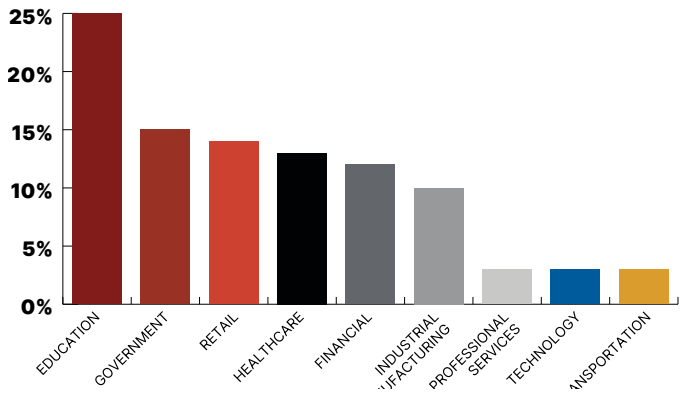
LockBit uses legitimate LOLBAS (Living off the Land Binaries and Scripts) such as sysadmin tools Process Hacker and PC Hunter, to terminate processes and services on the victim systems (T1489 – Service Stop) and[52] weaponizes Active Directory Group Policy Objects (GPOs) to deploy the ransomware across the entire environment (T1481.001 - Domain Policy Modification: Group Policy)[53].

After encrypting all the desired files, LockBit changes the background of all systems to display a message "offering the opportunity to earn millions of dollars to anyone [that provides a method] into a corporate network environment" such as with RDP or VPN login credentials (T1078 - Valid Accounts, T1133 - External Remote Services) after a successful compromise[54].

Vice Society

Vice Society is yet another "double-extortion" ransomware operation which has been active since at least mid 2021[55]. The operation gained notoriety during this time due to their high-volume of successful breaches against healthcare institutions during the COVID-19 pandemic [56] such as Hospital de Castelluccio, Atlanta Perinatal Associates in Georgia, United Health Centers of San Joaquin Valley, and Los Angeles-based Barlow Respiratory Hospital[57-61].

VICE SOCIETY DATA-LEAK VICTIMS BY INDUSTRY



After obtaining initial access, the group has been observed using impacket via Remote Windows Management Instrumentation and PsExec to execute batch scripts (T1059.003 - Command and Scripting Interpreter: Windows Command Shell) and PowerShell (T1059.001 – Command and Scripting Interpreter: PowerShell) commands upon other machines within the network (T1021.006 – Remote Services: Windows Remote Management)[55]. To maintain access, Vice Society creates a new service (T1543.003 – Create or Modify System Process: Windows Service) which executes a Base64 encoded (T1027 – Obfuscated Files or Information) PowerShell script upon system start up that disables PowerShell logging (T1562.003 – Impair Defenses: Impair Command History Logging), bypasses AMSI protection (T1562.001 – Impair Defenses: Disable or Modify Tools), in addition to downloading, decrypting, and executing an adversary-controlled backdoor (T1105 – Ingress Tool Transfer, T1140 – Decode/Deobfuscate Information).

Vice Society attempts to obtain credentials by accessing the ntds.dit (T1003.003 – OS Credential Dumping: NTDS) file or by using comsvcs.dll via rundll32.exe to extract LSASS data (T1003.001 - OS Credential Dumping: LSASS Memory)[55]. The group has also used "Print Nightmare" (CVE-2021-34527) to facilitate privilege escalation. Then, Vice Society operators use mstsc.exe to move laterally from system to system via Remote Desktop Protocol (T1021.001 – Remote Services: Remote Desktop Protocol), executing PowerShell scripts as they move through additional systems on the network, clearing windows event logs (T1070.001 – Indicator Removal on Host: Clear Windows Event Logs), disabling remote administration restrictions via the registry (T1112 – Modify Registry, T1562.004 – Impair Defenses: Disable or Modify System Firewall), and exfiltrating data over SMB (T1020 – Automated Exfiltration, T1048 – Exfiltration Over Alternative Protocol) before deploying the encrypting stage of the attack (T1486 Data Encrypted for Impact)[55].

Defensive Recommendations

Common Attack Vectors and Mitigations

- **Exploiting vulnerable systems:** Regularly perform vulnerability scanning and red team assessments to identify exploitable systems[62]. Use a patch management system to ensure all systems, including those externally facing, are up to date with the latest versions available (M1050 – Exploit Protection, M1016 – Vulnerability Scanning, M1051 – Update Software).
- **Phishing:** It is common for threat actors to leverage phishing as an entry point into your environment. Organizations can ensure that extensions known for delivering phishing payloads are blocked (M1054 – Software Configuration, M1049 – Antivirus/Antimalware) along with leveraging a proxy solution to block known bad websites (M1021 – Restrict Web-Based Content). Additionally, implement regular training and educational opportunities for employees to better identify and report phishing emails (M1017 – User Training).

Preparing for Response

- **IR assistance:** Have an incident response team on retainer that can assist in response. This team will be able to supplement and guide your team during an active infection.
- **Insurance:** Obtain cyber insurance and verify what services your policy covers. Understanding what these services are can allow for quicker decisions to be made.
- **Endpoint Protection:** Leverage an advanced endpoint protection solution that utilizes behavior driven analysis. Understand the policies associated with the endpoint protection solution and what actions to take if ransomware activity is observed (M1040 Behavior Prevention on Endpoint).
- **Backups:** Leverage a backup implementation that would not be impacted by ransomware on your corporate network. Practicing disaster recovery with these backups will allow for you to determine challenges and issues with restoration prior to an attack (M1053 – Data Backup).
- **Practice:** Preparing by implementing your incident response plan into tabletop exercises will allow for quicker and more precise action when faced with a ransomware outbreak. During these tabletop exercises, it is important to understand what went well and what needs improvement. These discussions should be used to modify the incident response plan (M1017 – User Training).

Responding to an Active Incident

- **Communication:** In addition to verifying a secure line of communication, it is important to understand who is handling each aspect of the incident response cycle.
- **Backups:** Verify if backups have been impacted. If the backups have not been impacted and are connected to the network, it is recommended to disconnect them from the network to prevent encryption.
- **Analysis:** Review AV/EDR systems to identify if they are successfully blocking execution on some devices. Further review the alerts to determine what needs to be done to block further execution (i.e. hash blocklist, policy misconfiguration, or AV hot patch). If you do not have EDR, consider leveraging your IR retainer for emergency implementation.
- **Containment:** Use the analysis of the malware and infection vector to contain the spread and impact. Items to consider would be data exfiltration indicators, persistence, host and/or network isolation, account deletion, etc.

Cyber Defense & Response

It's what we do.

Cyberattacks continue to grow in complexity, and the cybersecurity tools required to adequately detect and respond to these threats have grown too numerous to manage without a dedicated team. The cost and shortage of talent have made in-house solutions unworkable for many organizations. Cyderes Managed Services was built to provide practical answers to these common problems with a wide range of cybersecurity solutions that address the needs of the modern digital workforce.

LEARN MORE

100% Cybersecurity Focused

We concentrate on securing your organization, so you can focus on your business while we handle your threats.

Speed & Agility Across Multi-Technology, Complex Environments

Our cyber experts support the world's largest banks, gaming companies, and utility providers, offering customized and flexible solutions.

Award-Winning Expertise

Bringing together the best of two award-winning cybersecurity organizations, Herjavec Group and Fishtech Group, along with partnerships with best-of-breed providers, we're built to protect across any security stack.

Comprehensive Cybersecurity Solutions

With offerings spanning Managed Security Services, Identity & Access Management, and wide-ranging Professional Advisory Services, we have solutions to meet the needs of any enterprise worldwide.

MAKE CYBERSECURITY YOUR COMPETITIVE ADVANTAGE.

Subscribe to our daily intelligence digests to find out how our managed security solutions are ready to meet all your evolving business needs.

CYDERES

cyderes.com

REFERENCES

[1]Sophos, "The State of Ransomware 2022," Sophos, Apr. 2022. Accessed: Jun. 13, 2022. [Online]. Available: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

[2] Herjavec Group Threat Team, "State of Ransomware 2021 Q1-Q2," Herjavec Group, Jul. 2021. Accessed: Oct. 12, 2021. [Online]. Available: https://herjavecgroup.sharepoint.com/sites/ThreatTeam/Shared%20Documents/Resources/Example%20output/Herjavec-Group-State-of-Ransomware-Report-1H-2021.pdf

[3] M. Eng. Luca Mella, Double Extortion Ransomware Tracker. 2022. [Online]. Available: https://doubleextortion.com/

[4] Symantec Threat Hunter Team, "Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware," Symantec Blogs, Dec. 16, 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware (accessed May 30, 2022).

[5] A. SEC, "ALPHV ransomware gang analysis," Cybersécurité - INTRINSEC, Jan. 26, 2022. https://www.intrinsec.com/alphv-ransomware-gang-analysis/ (accessed May 30, 2022).

[6] S2W, "BlackCat : New Rust based ransomware borrowing BlackMatter's configuration," S2W BLOG, Dec. 10, 2021. https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809 (accessed May 30, 2022).

[7] Internet Crime Complaint Center(IC3), "BlackCat/ALPHV Ransomware Indicators of Compromise," Federal Bureau of Investigation, Cyber Division, CU-000167-MW, Apr. 2022. Accessed: May 30, 2022. [Online]. Available: https://www.ic3.gov/Media/News/2022/220420.pdf

[8] "Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/tactics/TA0001/ (accessed Dec. 21, 2020).

[9] MITRE® Corporation, "Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®," Apr. 12, 2021. https://attack.mitre.org/techniques/T1190/ (accessed Jul. 12, 2021).

[10] MITRE® Corporation, "External Remote Services, Technique T1133 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK®, Aug. 19, 2021. https://attack.mitre.org/techniques/T1133/ (accessed Apr. 04, 2022).

[11] J. Walter, "BlackCat Ransomware | Highly-Configurable, Rust-Driven RaaS On The Prowl For Victims," SentinelOne, Jan. 18, 2022. https://www.sentinelone.com/labs/blackcat-ransomware-highly-configurable-rust-driven-raas-on-the-prowl-for-victims/ (accessed May 30, 2022).

[12] "Valid Accounts: Domain Accounts, Sub-technique T1078.002 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK®, Mar. 13, 2020. https://attack.mitre.org/techniques/T1078/002/ (accessed Jan. 02, 2021).

[13] "Brute Force: Credential Stuffing, Sub-technique T1110.004 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1110/004/ (accessed May 30, 2022).

[14] C. Boma, "SpearTip's Investigation into the Emerging BlackCat Ransomware," SpearTip Cyber Counterintelligence, Dec. 10, 2021. https://www.speartip.com/resources/speartips-investigation-into-the-emerging-blackcat-ransomware/ (accessed May 31, 2022).

[15] A. Tanner, A. Hichcliffe, and D. Santos, "Threat Assessment: BlackCat Ransomware," Unit42, Jan. 27, 2022. https://unit42.paloaltonetworks.com/blackcat-ransomware/ (accessed May 31, 2022).

[16] "Conti Ransomware Resurfaces, Targeting Government & Large Organizations," Cyble, Jan. 21, 2021. https://blog.cyble.com/2021/01/21/conti-ransomware-resurfaces-targeting-government-large-organizations/ (accessed Jun. 03, 2022).

[17] AdvIntel, "DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape," AdvIntel, May 20, 2022. https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape (accessed Jun. 03, 2022).

[18] "Conti Ransomware Gang Claims 50+ New Victims including Oil Terminal...," eSentire. https://esentire-backup.frb.io/security-advisories/conti-ransomware-gang-claims-50-new-victims-including-oil-terminal-operator-sea-invest (accessed Jun. 03, 2022).

[19] "Conti Ransomware | CISA." https://www.cisa.gov/uscert/ncas/alerts/aa21-265a (accessed Jun. 03, 2022).

[20] "Conti Ransomware Attacks Impact Healthcare and First Responder Networks," p. 4.

[21] "Native API, Technique T1106 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1106/ (accessed Sep. 23, 2021).

[22] B. Baskin, "TAU Threat Discovery: Conti Ransomware," Jul. 08, 2020. https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/ (accessed Jul. 08, 2020).

[23] P. E. T. Intelligence, "Operation TA505: how we analyzed new tools from the creators of the Dridex trojan, Locky ransomware, and Neutrino botnet," May 20, 2020. https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/operation-ta505/ (accessed Jun. 05, 2020).

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

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

[26] Trend Micro Research, "Ransomware Spotlight: Clop - Security News," Ransomware Spotlight, Feb. 22, 2022. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop (accessed Jun. 11, 2022).

[27] NCC Group, "NCC Group Monthly Threat Pulse – April 2022," NCC Group, May 25, 2022. https://www.mynewsdesk.com/nccgroup/news/ncc-group-monthly-threat-pulse-april-2022-448500 (accessed Jun. 12, 2022).

[28] "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).

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

[30] MITRE® Corporation, "Subvert Trust Controls: Code Signing, Sub-technique T1553.002 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK®, Feb. 10, 2020. https://attack.mitre.org/techniques/T1553/002/ (accessed Jun. 12, 2022).

[31] Trend Micro Research, "Ransomware Spotlight: Hive - Security News," Trend Micro, Mar. 18, 2022. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive (accessed May 31, 2022).

[32] C. Glover, "Hive ransomware gang strikes Indonesian gas giant PGN," Tech Monitor, Apr. 04, 2022. https://techmonitor.ai/technology/cybersecurity/hive-ransomware-gang-pgn (accessed May 31, 2022).

[33] MITRE® Corporation, "User Execution: Malicious File, Sub-technique T1204.002 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK®, Mar. 11, 2020. https://attack.mitre.org/techniques/T1204/002/ (accessed Jun. 25, 2021).

[34] MITRE® Corporation, "Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK, Jan. 04, 2022. https://attack.mitre.org/techniques/T1566/ (accessed Apr. 25, 2022).

[35] Federal Bureau of Investigation, Cyber Division, "Indicators of Compromise Associated with Hive Ransomware," Federal Bureau of Investigation, Alert MC-000150-MW, Aug. 2021. Accessed: May 31, 2022. [Online]. Available: https://www.ic3.gov/Media/News/2021/210825.pdf

REFERENCES

[36] B. Posey, "Everything you need to know about ProxyShell vulnerabilities," WhatIs.com, Dec. 29, 2021. https://www.techtarget.com/whatis/feature/Everything-you-need-to-know-about-ProxyShell-vulnerabilities (accessed Jun. 02, 2022).

[37] "Server Software Component: Web Shell, Sub-technique T1505.003 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK®, Jul. 26, 2021. https://attack.mitre.org/techniques/T1505/003/ (accessed Jun. 02, 2022).

[38] "Obfuscated Files or Information, Technique T1027 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1027/ (accessed Dec. 02, 2020).

[39] MITRE® Corporation, "Create Account, Technique T1136 - Enterprise | MITRE ATT&CK®," MITRE ATT&CK, Aug. 12, 2021. https://attack.mitre.org/techniques/T1136/ (accessed May 30, 2022).

[40] "Use Alternate Authentication Material: Pass the Hash, Sub-technique T1550.002 - Enterprise | MITRE ATT&CK®." https://attack.mitre.org/techniques/T1550/002/ (accessed Jun. 02, 2022).

[41] M. Espinoza, "Hackers Claim Responsibility for California Ransomware Attack," GovTech, Mar. 31, 2022. https://www.govtech.com/security/hackers-claim-responsibility-for-california-ransomware-attack (accessed May 31, 2022).

[42] "MENACES LIÉES AUX VOLS DE COOKIES ET CONTRE-MESURES," CERT-FR, CERTFR-2022-CTI-005, mai 2022. Accessed: Jun. 02, 2022. [Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2022-CTI-005.pdf

[43] Microsoft Threat Intelligence Center and MIcrosoft 365 Defender Threat Intelligence Team, "Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself," Microsoft Security Blog, May 09, 2022. https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/ (accessed May 31, 2022).

[44] Microsoft Threat Intelligence Center, Microsoft Detection and Response Team, and Microsoft Defender Threat Intelligence Team, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction," Microsoft Security Blog, Mar. 22, 2022. https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/ (accessed May 31, 2022).

[45] B. Krebs, "A Closer Look at the LAPSUS$ Data Extortion Group – Krebs on Security," Krebs on Security, Mar. 23, 2022. https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/ (accessed May 31, 2022).

[46] J. Tidy, "Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal," BBC News, Mar. 24, 2022. Accessed: Jun. 03, 2022. [Online]. Available: https://www.bbc.com/news/technology-60864283

[47] C. Page, "Lapsus$ claims Globant as its latest breach victim," TechCrunch, Mar. 30, 2022. https://social.techcrunch.com/2022/03/30/lapsus-globant-breach/ (accessed Jun. 03, 2022).

[48] R. Lakshmanan, "IT Firm Globant Confirms Breach after LAPSUS$ Leaks 70GB of Data," The Hacker News, Mar. 30, 2022. https://thehackernews.com/2022/03/lapsus-claims-to-have-breached-it-firm.html (accessed May 31, 2022).

[49] N. Coppinger, "Defending Your Cloud Environment Against LAPSUS$-style Threats," Inside Out Security Blog, Mar. 29, 2022. https://www.varonis.com/blog/lapsus (accessed May 31, 2022).

[50] Zaib, "LockBit 2.0 Ransomware Attacks Increase Worldwide," Cyclonis, Aug. 19, 2021. https://cyclonis.com/lockbit-2-0-ransomware-attacks-increase-worldwide/ (accessed Jun. 09, 2022).

[51] V. Rieß-Marchive, "Ransomware : LockBit 3.0 commence à être utilisé dans des cyberattaques," LeMagIT. https://www.lemagit.fr/actualites/252516821/Ransomware-LockBit-30-commence-a-etre-utilise-dans-des-cyberattaques (accessed Jun. 09, 2022).

[52] J. P. Bernardo, J. Chong, N. Madayag, M. Marti, C. Tomboc, and S. Torre, "LockBit Resurfaces With Version 2.0 Ransomware Detections in Chile, Italy, Taiwan, UK," Trend Micro, Aug. 2021. Accessed: Aug. 18, 2021. [Online]. Available: https://www.trendmicro.com/en_us/research/21/h/lockbit-resurfaces-with-version-2-0-ransomware-detections-in-chi.html

[53] "LockBit 2.0, the first ransomware that uses group policies to encrypt Windows domains," Security Affairs, Jul. 29, 2021. Accessed: Aug. 18, 2021. [Online]. Available: https://securityaffairs.co/wordpress/120664/cyber-crime/lockbit-2-0-ransomware-group-policies.html

[54] L. Abrams, "LockBit ransomware recruiting insiders to breach corporate networks," BleepingComputer, Aug. 04, 2021. Accessed: Aug. 18, 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

[55] E. Brumaghin and A. Zobec, "Vice Society leverages PrintNightmare in ransomware attacks," Aug. 12, 2021. http://blog.talosintelligence.com/2021/08/vice-society-ransomware-printnightmare.html (accessed Oct. 13, 2021).

[56] C. Glover, "'Ruthless' Vice Society claims responsibility for Spar ransomware attack," Tech Monitor, Jan. 04, 2022. https://techmonitor.ai/technology/cybersecurity/vice-society-spar-hack-ransomware (accessed Jun. 10, 2022).

[57] J. Greig, "Ransomware groups continue assault on healthcare orgs as COVID-19 infections increase," ZDNet, Sep. 11, 2021. https://www.zdnet.com/article/ransomware-groups-continue-assault-on-healthcare-orgs-as-covid-19-infections-increase/ (accessed Jun. 10, 2022).

[58] J. Davis, "Ongoing ransomware, data theft, leaks pummel health care organizations," Sep. 28, 2021. https://www.scmagazine.com/analysis/ransomware/ongoing-ransomware-data-theft-leaks-prove-problematic-in-health-care (accessed Jun. 10, 2022).

[59] H. Mitchell, "Hackers leak California hospital patients' data online after ransomware attack," Becker's Health IT, Sep. 13, 2021. https://www.beckershospitalreview.com/cybersecurity/hackers-leak-california-hospital-patients-data-online-after-ransomware-attack.html (accessed Jun. 10, 2022).

[60] U.S. Department of Health and Human Services, "Health Sector Ransomware Trends for Third Quarter 2021," Department of Health & Human Services, 202110131200, Oct. 2021. Accessed: Jun. 10, 2022. [Online]. Available: https://www.hhs.gov/sites/default/files/hph-ransomware-trends-analyst-note.pdf

[61] L. Whitney, "United Health Centers reportedly compromised by ransomware attack," TechRepublic, Sep. 28, 2021. Accessed: Jun. 10, 2022. [Online]. Available: https://www.techrepublic.com/article/united-health-centers-reportedly-compromised-by-ransomware-attack/

[62] Cybersecurity and Infrastructure Security Agency, "Ransomware Guide," Stop Ransomware, Sep. 2020. https://www.cisa.gov/stopransomware/ransomware-guide (accessed May 31, 2022).