Vertical Target Series

Industrials and Industrial Sub-Verticals

White Paper

Critical verticals, such as industrials, are attractive targets for cybercriminals and advanced persistent threat (APT) groups. The industrials vertical includes the manufacturing, construction and engineering, professional and commercial services, legal services, and transportation verticals. However, Optiv's Global Threat Intelligence Center (gTIC) tracks the threats to those verticals separately. Adversaries often target these industries for numerous reasons, including the type and amount of sensitive information that they can obtain, the amount of money that they perceive these organizations to have available, and the impact that these attacks have. APT groups often target industrial organizations because they have critical information that is likely of strategic interest to government bodies for military, economic, and political advancements. Cybercriminals, such as ransomware groups, frequently target these companies because these verticals cannot suffer significant downtime without having rippling effects on the target countries' economic stability.

An APT group is a malicious actor who is believed to have significant skills, virtually unlimited resources, and experience with conducting highly targeted attacks. APT groups often aim to gain initial access and remain undetected for extended periods of time—allowing the group to steal credentials and sensitive information, as well as deploy backdoors on victim networks. The information targeted from these organizations often includes the type of data that would be of strategic interest to the government the group works for.

As opposed to APT groups, ransomware cybercriminal campaigns focus on the encryption or destruction of files and folders on the targeted endpoint or across the network. Ransomware syndicates have constantly shifted tactics to remain relevant, including rebranding, leveraging known and benign tools to maintain persistence, and building an ecosystem around their own affiliate groups and programs. Such an ecosystem may include hosting and building their own tools, forums, and leak pages.

This white paper leverages the Threat Actor Metric™ developed by Optiv's gTIC - a multi-faceted, qualitative approach to determine an adversary or campaign's potential risk to an organization or industry on a scale of 0 to 100. The metric considers known and assessed non-technical capabilities and intentions.

Table of Contents

Industrials

Threat actors have different motivations for targeting any organization, whether politically, financially, or economically. The industrials vertical is critical to the economy. Threat actors perceive that valuable organizations within this vertical host important data that could benefit competitors and other economies. This data includes sensitive information related to products and employees, which are often interconnected with suppliers, customers, and partners. Personally identifiable information (PII) of employees, suppliers, and customers are likely attractive targets for both APT and cybercriminal groups. APT groups can leverage product designs, blueprints, supply chains, and processes to further production within their sponsored country. Cybercriminal groups can also hold this information for ransom, target additional organizations, or sell the information. The most active APT groups found to target the industrials vertical are APT36 (aka Transparent Tribe, Mythic Leopard, Copper Fieldstone), SiameseKitten (aka Hexane, Lyceum), APT10 (aka Cicada, Stone Panda, menuPass, Red Apollo), and MuddyWater (aka Seedworm, Static Kitten).

APT36

APT36 (aka Transparent Tribe, Mythic Leopard, Copper Fieldstone) is a Pakistan-based group that has been active since at least 2013 and is known for their targeting of the Indian government, military personnel, and defense contractors. The threat actor is known for their use of impersonated websites and documents that mimic legitimate government sites used to obtain user credentials and deliver payloads. The group has also been observed abusing the Google Ads paid search feature to prioritize malicious sites direct users to download their malware.

APT36 is most known for their use of the CrimsonRAT malware. But the group uses a wide array of open-source and custom malware variants to steal information and harvest credentials. The group has conducted phishing attacks with COVID-19-themed lures and installers for government applications, including the Indian multi-factor authentication (MFA) application, Kavach.

- In 2020, APT36 targeted defense organizations in Operation Honey Trap, where they used fake profiles of women to entice targets into opening malicious attachments in their emails or chat messages. Upon opening the attachments, the victims inadvertently downloaded the CrimsonRAT malware used by APT36 to steal sensitive information.

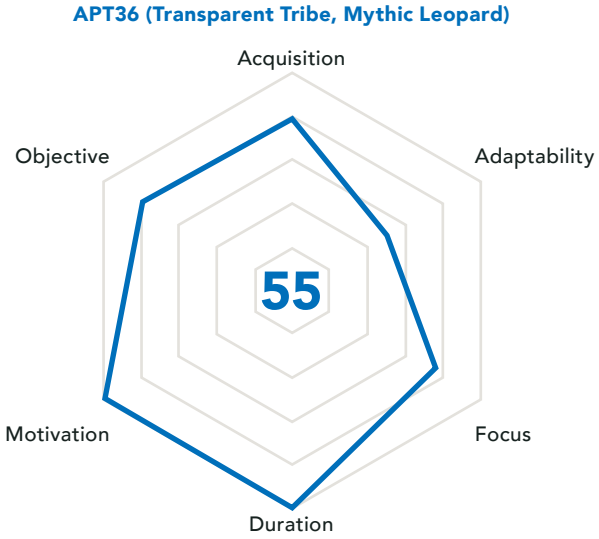

Figure 1: Threat Actor Metric™ for APT36

SiameseKitten

SiameseKitten (aka Hexane, Lyceum) is an Iranian APT group that is likely sponsored by the Iranian state. Active since at least 2017, the group primarily conducts cyber espionage attacks that are likely politically motivated. SiameseKitten has been linked to Iran due to the overlapping infrastructure and tools used by the Iranian threat groups, APT33 (aka Elfin) and APT34 (aka Oilrig).

- In 2021, SiameseKitten targeted various organizations in Israel by impersonating an HR department employee and creating phishing lures. The group contacted potential victims with a fake job offer directing them to a phishing page with a lure file. Victims who clicked the file inadvertently downloaded the Milan or Shark malware variants, which established a connection between the infected machine and the C2 server and eventually downloaded the DanBot RAT. The group then gathered data, conducted espionage, and attempted to spread throughout the network.

APT10

APT10 (AKA Cicada, Stone Panda, menuPass, Red Apollo) has been active since at least 2006. Individual members of APT10 are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Bureau and worked for the Huaying Haitai Science and Technology Development Company.

APT10 concentrates its efforts on cyber espionage, **Likely** in support of the national strategic goals of the People's Republic of China (PRC), and focuses on sensitive proprietary information to support Chinese operations. APT10 has been observed gaining initial access via spear phishing attacks with malicious attachments, conducting supply chain attacks, and exploiting vulnerabilities. APT10 spear phishes have been relatively unsophisticated, leveraging .lnk files within archives, files with double extensions, and, in some cases, simply identically named decoy documents and malicious launchers within the same archive.

- From 2016-2017, APT10 reportedly conducted a campaign targeting organizations in the technology, energy, healthcare, manufacturing, and telecommunications verticals. Utilizing stolen administrative credentials and certificates to target the organizations, the attackers deployed the PlugX and RedLeaves malware variants.
- From 2019-2021, APT10 conducted a campaign targeting Japanese industrial organizations by exploiting the ZeroLogon vulnerability in Microsoft Windows and conducting DLL side-loading techniques. The group deployed the Hartip malware.
- In 2022, APT10 targeted industrial organizations via spear phishing emails with malicious attachments. The attacks included the use of a fake Microsoft Word file and the self-extracting of an archive file in RAR format. The attacks led to the deployment of the LODEINFO malware.

MuddyWater

MuddyWater (aka Seedworm, Static Kitten) is a threat group, active since 2017, that is assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). MuddyWater, like many other APT groups, relies on social engineering to deliver weaponized files hosting embedded macros as an initial infection vector. One of their tactics involves the use of documents, including those with government and intelligence agency branding to add a feeling of legitimacy.

- In 2021, MuddyWater was attributed to a campaign, dubbed "Earth Vetala," that targeted various organizations in the Middle East and neighboring regions. The group used spear phishing emails with embedded links to a legitimate file-sharing service to distribute their malicious package. Once they accessed the victim's system, the attackers downloaded post-exploitation tools that included password and process-dumping utilities, reverse-tunneling tools, and custom backdoors.

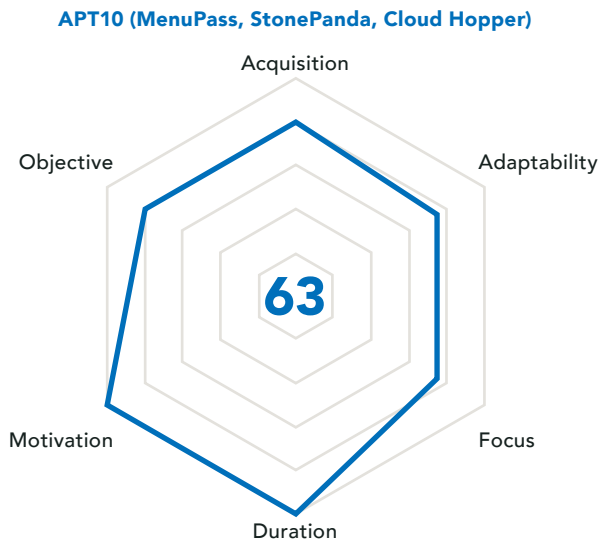

Figure 2: Threat Actor Metric™ for APT10

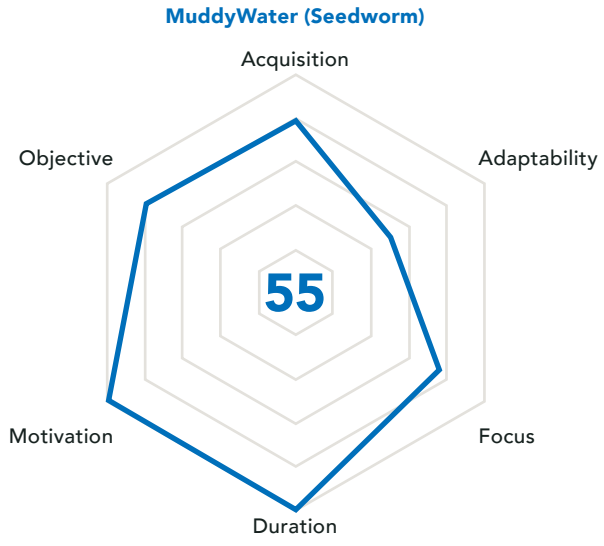

Figure 3: Threat Actor Metric™ for MuddyWater

Ransomware Groups with Industrials Targets

Companies in the industrials vertical cannot afford to be out of service for a significant period, as these downtimes will have direct and secondary impacts on their customers and vendors. This likely results in a perception that organizations in this vertical are more inclined to pay a ransom. Additionally, their systems are often in constant use, which can create a problem because operators may be reluctant to take them offline for routine maintenance and patch applications. Organizations in this vertical are often heavily reliant on systems that are outdated and thus require significant efforts to maintain vulnerability management. Taking these systems offline is likely a significant undertaking. Industrial organizations have been most often targeted by the LockBit, Alphv, Royal, Black Basta, and Clop ransomware operations.

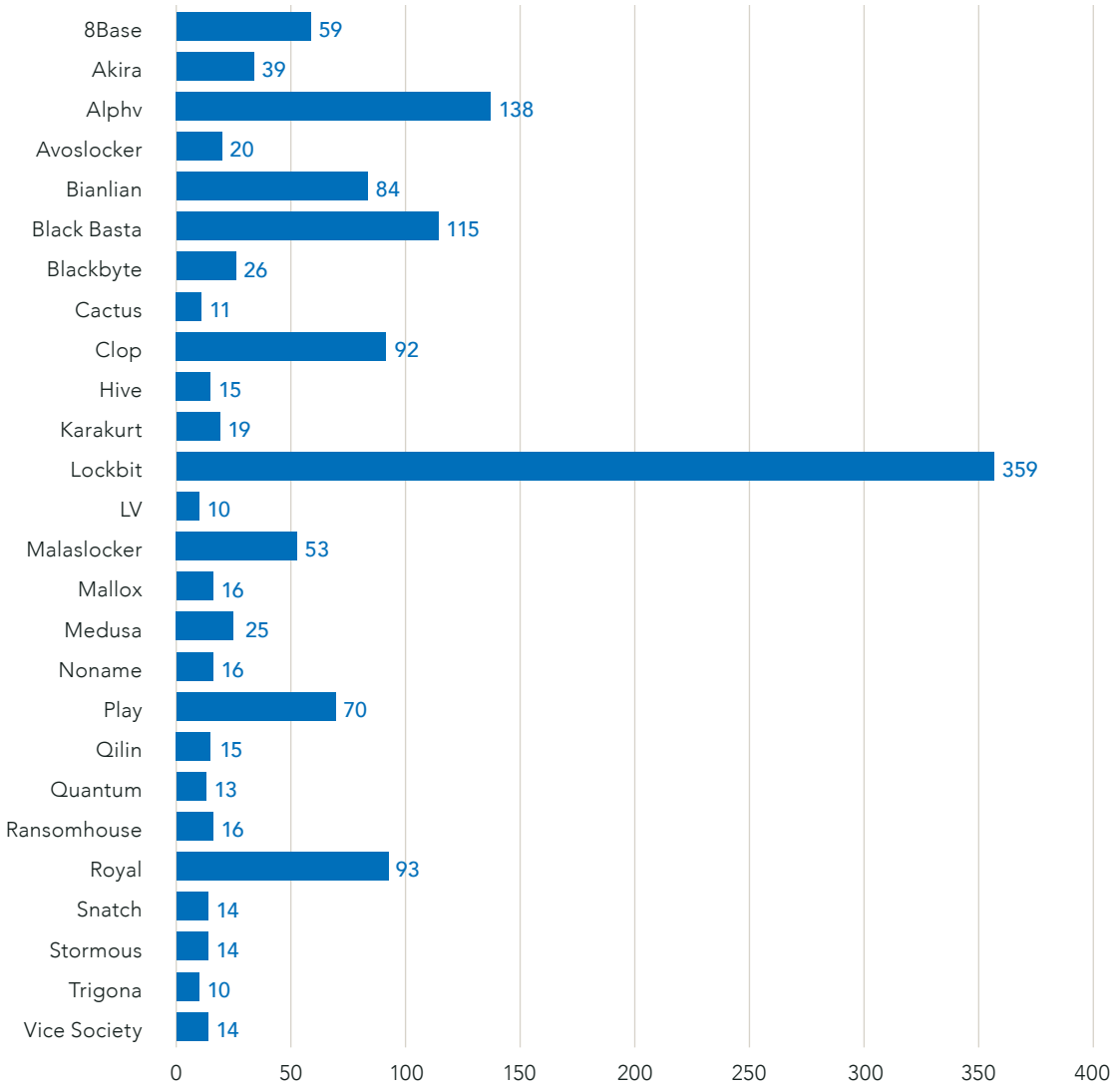

Figure 4: Ransomware variants that listed industrials organizations on their data leak site from August 1, 2022 - July 31, 2023

LockBit

LockBit ransomware was first discovered in September 2019 and was previously known as ABCD ransomware because of the ".abcd virus" extension first observed. LockBit operates as a ransomware-as-a-service (RaaS) model, where affiliates make a deposit to use the tool for a custom attack, and then they split the ransom payout with the LockBit group—up to a 75% payout for some affiliates. LockBit's operators have posted advertisements for their affiliate program on Russian-language criminal forums stating they will not operate in Russia or any CIS countries.

In August 2023, a security researcher with Analyst1, Jon DiMaggio released a detailed report diving into LockBit's operations, including several operational weaknesses. Allegedly, the group is unable to host and leak data to align with their threats. Moreover, affiliates are reportedly leaving the group to work for others and are unable to reach the LockBit leader for up to a week at a time. Multiple organizations within this report that have been listed on LockBit's data leak site have minimal or no screenshots or links to the purported data. This indicates that the group is **Likely** struggling with their operations and is unable to host and leak data as they have in previous years.

Of the 898 victims listed on LockBit's data leak site from August 1, 2022 - July 31, 2023, 359 of them (40%) are in the industrials vertical.

- In October 2022, LockBit 2.0 ransomware hit an Israeli defense firm. The threat actors claimed to gain over 6TB of data and demanded $50 million from the victim organization. At the time of writing, the post included one link to 56.7GB of purportedly stolen data. The post does not include any file folders or screenshots.
- In March 2023, LockBit 3.0 ransomware listed an organization in the U.S. on their data leak site. The group claimed to have stolen nearly 3,000 proprietary schematics developed by the engineers. The ransomware group claimed that a buyer for the documents and reports would be "easy." At the time of writing, the post does not include any links, screenshots, or file folders, but does state that all the data has been published.
- In June 2023, LockBit 3.0 claimed responsibility for a ransomware attack on an organization in Italy and claimed to have stolen 14GB of data. At the time of writing, the post included 8 screenshots, file folders, and one link to 61.5MB of purportedly stolen data.

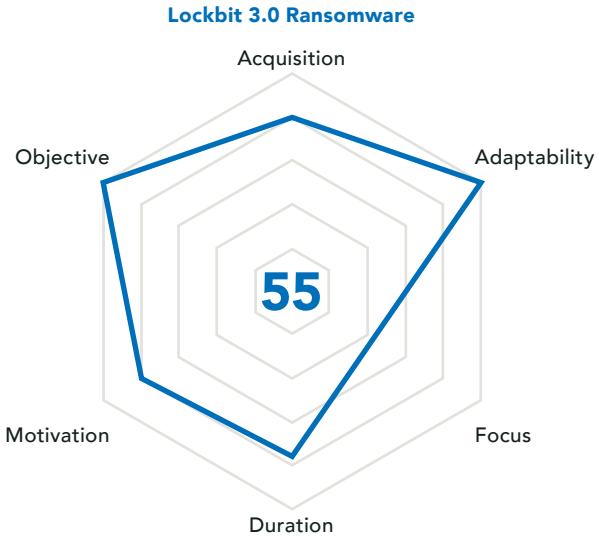

Figure 5: Threat Actor Matrix for LockBit Ransomware

Alphv

Alphv (aka BlackCat) is a ransomware variant that has been active since at least November 2021. This variant involves a RaaS operation, where developers lease ransomware to affiliates who can earn up to $3 million by conducting cyber extortion. Affiliates are often recruited through Russian-speaking cybercriminal forums. Initial access vectors include compromised RDP, phishing attacks, stolen credentials, and vulnerability exploitation.

In September 2022, the operators added wiper functionality to the ransomware. The group was observed using the Exmatter tool to exfiltrate the data and then corrupt and destroy files. This tactic makes it so the only way for a victim to recover the data is to purchase it back from the ransomware operators. The operators use a tool called Eraser to overwrite the files with a selection of code taken from the beginning of another file. It is **Likely** that the group uses this tactic to evade detection, as using legitimate file data to corrupt other files is likely to avoid heuristic-based detection for ransomware and wipers.

Of the 353 victims listed on Alphv's data leak site from August 1, 2022 - July 31, 2023, 138 of them (39.1%) are in the industrials vertical.

- In October 2022, Alphv named a Canada-based organization on their data leak site. The organization stated in an interview that the ransomware was removed, and no ransom was paid. The organization is still listed on the Alphv

data leak site at the time of writing, and their post contains images of purportedly stolen documents from the organization.

- In January 2023, Alphv operators named an India-based company on their data leak site and claimed to have stolen 2TB of data from the organization. The stolen data allegedly includes full descriptions of engineering specifications, drawings, and audits for weapons that the company manufactures, along with customer and employee data. The organization is still listed on Alphv's data leak site at the time of writing, and Alphv's post includes multiple pictures of purported stolen documents.
- In June 2023, Alphv claimed responsibility for the ransomware attack affecting a France-based organization. The group's post on their data leak site includes over a hundred samples of stolen data – ranging from non-disclosure agreements to copies of passports and IDs.

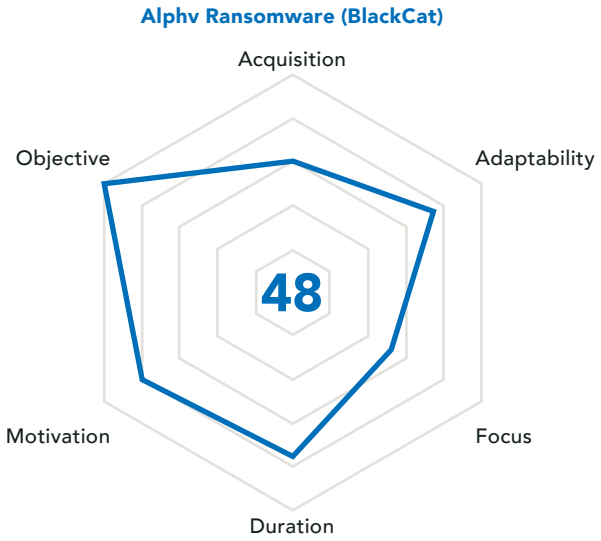

Figure 6: Threat Actor Metric™ for Alphv Ransomware

Royal

Royal is a ransomware operation that was first observed in September 2022, but has likely been active since as early as January 2022. The operators have made a significant impact on the ransomware landscape and have demanded millions of dollars in ransom payments from victims. Unlike other ransomware operations, Royal is a private ransomware group reportedly comprised of former Conti ransomware affiliates. Royal previously used the Alphv (aka BlackCat) encryptor and then switched to using the Zeon encryptor, which has a ransom note resembling the one used by the Conti group.

Royal ransomware operators have been observed gaining initial access via phishing attacks, RDP compromises, credential abuse, vulnerability exploitation, malicious downloaders, and malvertising on Google ads. In March 2023, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released a #StopRansomware alert providing details of the group and their operations. Of the 199 victims listed on Royal's data leak site from August 1, 2022, - July 31, 2023, 93 of them (46.7%) are in the industrials vertical.

- In November 2022, Royal ransomware listed a U.S.-based organization on their data leak site. The organization remains on the site at the time of writing, and the post contains one link to purported data leaked from the organization.
- In January 2023, Royal ransomware listed a U.S. organization on their data leak site and claimed to have stolen data on 3,200 employees, 30,000 customers, and 125 key boarder entry points. The ransom demand was likely not paid because the organization is still listed on the data leak site with one link to purported stolen data.
- In May 2023, Royal ransomware listed a U.K. organization on their data leak site and claimed to have stolen 3GB of data from the organization. The post states that 10% of the stolen data has been published, with one link included in the post.

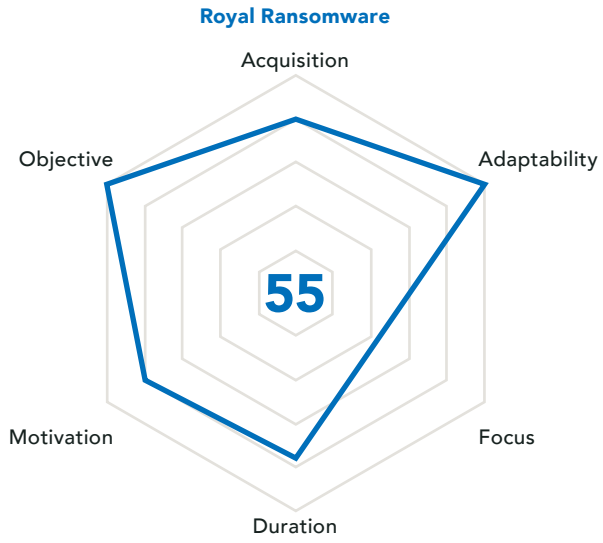

Figure 7: Threat Actor Metric™ for Royal Ransomware

Black Basta

Black Basta is a RaaS operation that has been active since at least April 2022. The group leverages the double extortion method and maintains a data leak site, Basta News. Black Basta is widely believed to be one of the many ransomware variants connected to the former Conti ransomware conglomerate. Black Basta provides victims with a link to the data leak site and a unique "company ID" used to initiate chat sessions for negotiations. Victims are often given seven days to make a payment. Black Basta claims that paying victims will receive a security report to help mitigate future attacks.

Black Basta operators have targeted various organizations across all verticals and geographies. Of the 212 victims listed on Black Basta's data leak site from August 1, 2022 - July 31, 2023, 115 of them (54.2%) are in the industrials vertical.

- In September 2022, Black Basta ransomware operators listed a U.S.-based organization and a subsidiary of an Israeli industrial organization on their data leak site. The operators' post displayed purportedly stolen documents, including a payroll report, an audit report, a confidentiality agreement, and an NDA. The company released a statement that the attack occurred in June 2022 and that 369 people were affected by the stolen data.
- In April 2023, Black Basta listed a U.S. organization on their data leak site and claimed to have stolen information related to their customers and employees. The group posted pictures of driver's licenses, NDAs, compliance statements, and work orders as proof of the data breach. The company is still listed, indicating that no ransom was paid.

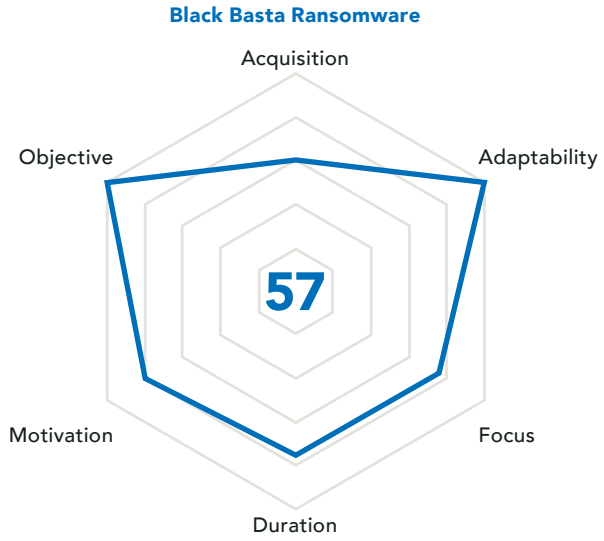

Figure 8: Threat Actor Metric™ for Black Basta Ransomware

Cl0p

Cl0p (aka Clop) is a RaaS operation that has been active since February 2019 and reportedly leverages an updated version of the 2016 CryptoMix ransomware. The Cl0p variant is signed with a legitimate certificate that helps trick security solutions into trusting the binary. Cl0p compares the keyboard of the victim's computer using the "GetKeyboardLayout" function against the hardcoded values. The function returns a "1" if the keyboard belongs to Russia or another CIS country in that case, and the ransomware terminates itself.

In Q1 2023, Cl0p exploited the GoAnywhere vulnerability, CVE-2023-0669, to target a reported 130 organizations. The group did not encrypt the victims, but rather focused on stealing data and holding it for ransom. Cl0p listed the names of organizations that did not pay on their data leak site. This attack resulted in Cl0p being more active in Q1 2023 than the group was in all of 2022. This attack bears similarity to the 2021 Cl0p attack targeting Accellion FTA vulnerabilities. In Q2 2023, Cl0p operators exploited the MOVEit Transfer MTF solution vulnerability, CVE-2023-34362, to target hundreds of organizations. Again, the group did not encrypt the victims, but they did steal sensitive data that they are holding for ransom.

Because Cl0p is a RaaS operation, the initial access vectors vary depending on the affiliate. Methods observed include phishing attacks, exploiting vulnerabilities, weak passwords, and exposed RDP. Cl0p affiliates target a wide range of verticals and geographies. Of the 376 victims listed on Cl0p's data leak site from August 1, 2022 - July 31, 2023, 92 of them (24.5%) are in the industrials vertical.

- In March 2023, Cl0p listed multiple organizations located in the U.S., Canada, Mexico, Chile, and Germany that were purportedly targeted by exploiting CVE-2023-0669. The group did not encrypt the victims' networks, but instead stole sensitive information that was then held for ransom. The information included W-9 tax forms, employee data, and payment orders.
- In June 2023, Cl0p listed multiple global organizations by exploiting a vulnerability in the MOVEit Transfer MFT software. The group did not encrypt victim networks in this attack and stole data to hold for ransom. The information included business plans, tax documents, IDs, passports, and more.

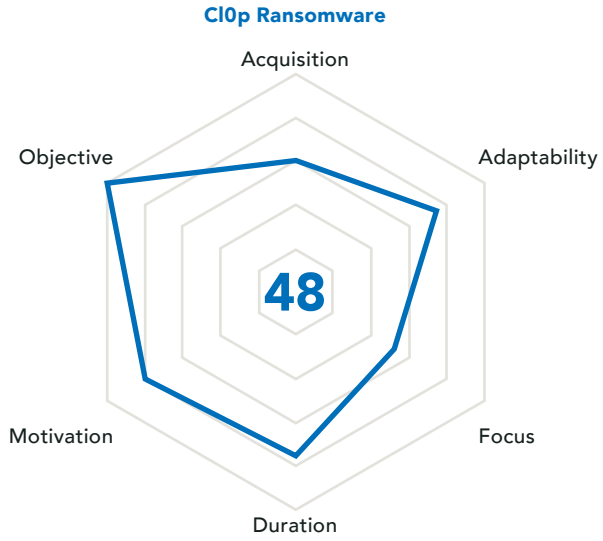

Figure 9: Threat Actor Metric™ for Cl0p Ransomware

Manufacturing

As technology has evolved, manufacturing organizations have become increasingly interconnected with other organizations. This has increased the ability for threat actors to target these organizations. Manufacturing organizations host a great deal of intellectual property (IP) data that could be used to further the manufacturing processes in other organizations and countries. Similar to other industrial organizations, manufacturing organizations often rely on outdated and legacy systems that can open them up to cyberattacks and vulnerabilities. Manufacturing organizations have deadlines, contracts to fulfill, and minimum number units to make. These factors require their equipment to be up and running nearly 24/7, which can hinder the ability to take systems offline to apply patches and updates. If a manufacturing organization has government contracts, they are likely to be targeted by APT groups in espionage attacks. This is because the threat group will **Likely** be able to obtain IP from the manufacturer and compromise the government agencies at the same time. APT groups observed targeting the manufacturing vertical include APT33 (aka Elfin, Holmium, Refined Kitten, Magic Hound), APT32 (aka OceanLotus, SeaLotus, Bismuth Tin, Tin Woodlawn), and APT41 (aka Wicked Panda, Barium, Double Dragon, Brass Typhoon).

APT33

APT33 (aka Elfin, Holmium, Refined Kitten, Magic Hound) is attributed to Iran and has been active since at least 2013. The group has targeted numerous industries worldwide. APT33's goal is apparently to provide long-term access for espionage and exfiltrate data of strategic interest to Iran. The group has utilized several off-the-shelf toolsets, in addition to custom malware. When their TTPs have been compromised, the group has revised tactics and attempted to exploit the target again.

Multiple sources have tied APT33 to the Kavosh Research Center, which is alleged to be a front organization for a unit subordinate to the Iranian Islamic Revolutionary Guards Corps Cyber Electronic Command (IRGC-CEC). Kavosh is allegedly responsible for malware development. Although Kavosh may develop the malware, it is **Likely** that APT33 is comprised of Iranian contractors as well for an added layer of plausible deniability.

APT33 has not had any new, publicly reported activity since 2019. This is **Likely** due to the group's extensive use of open-source, publicly available malware and tools that can make it difficult to distinguish between cybercriminal and APT activity. These factors contribute to the challenge of attribution. It is likely that APT33 has continued to conduct campaigns against the energy, financial services, and industrial verticals. However, APT attacks are often reported much later than the attacks occur, and the use of publicly available tools allows the threat actors to remain anonymous.

- From 2016-2017, APT33 targeted multiple organizations with spear phishing emails with a malicious file attachment. Most of the organizations were located within the U.S. and were **Likely** committed to helping Iran enhance their industrial industry and operations.
- In 2019, APT33 reportedly manipulated domain names associated with U.S.-based organization in phishing attacks to infect victims with malware. The emails were purportedly related to career opportunities to lure victims into downloading the malware.

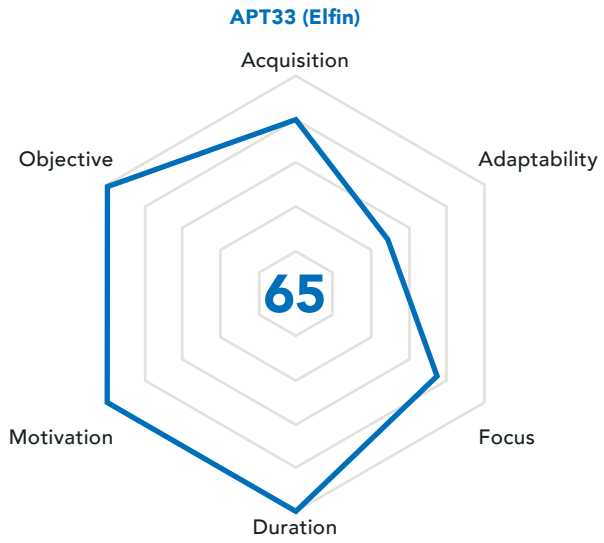

Figure 10: Threat Actor Metric™ for APT33

APT32

APT32 (aka OceanLotus, SeaLotus, Bismuth, Tin Woodlawn) has been active since at least 2014 and has been attributed to Vietnam. APT32 is considered a determined and motivated threat group that continuously changes techniques and upgrades its technology arsenal to remain under the radar. Even in cases where security defenders have identified and disrupted their attacks, APT31 routinely updates TTPs and attempts to target the same organizations again.

To gain initial access, APT32 relies on watering hole and social engineering attacks, specifically phishing emails with malicious attachments. The group has often been observed compromising media websites to compromise victims and monitor the reading habits of other victims. The group has developed malware to target macOS, Android, and Windows operating systems.

APT32 has many custom backdoors and malware variants. But the group also makes use of publicly available tools, such as Cobalt Strike and the Veil framework. APT32 has not been as publicly active since 2020, which is **Likely** due to their operations either not being discovered or disclosed yet. APT campaigns typically evade detection and can last for many years at a time, which contributes to the gap in reporting.

- From 2018-2019, APT32 reportedly targeted organizations via phishing emails with Microsoft Office documents with malicious macros. They also leveraged phishing emails with a RAR archive containing a legitimate program with DLL side-loading. The group reportedly targeted the organizations to deploy the Kerrdown downloader, a custom malware used to download spyware malware on victim networks.
- Throughout 2020, APT32 reportedly targeted multiple organizations in order to collect information related to COVID-19. The information accessed included research and development information related to the virus, a vaccine, and side effects.
- In 2020, APT32 reportedly targeted organizations with an OceanLotus malware variant aimed at macOS environments. OceanLotus is a backdoor that provides threat actors with remote access to victim systems, which can be used to harvest sensitive information.

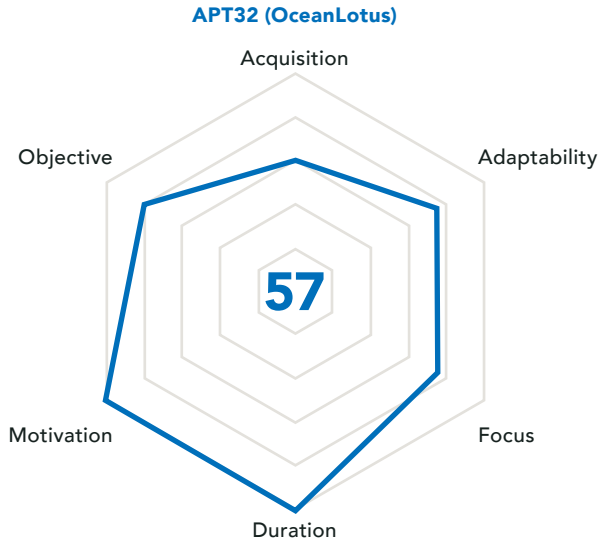

Figure 11: Threat Actor Metric™ for APT32

APT41

APT41 (aka Wicked Panda, Barium, Double Dragon, Brass Typhoon) is a Chinese state-affiliated threat group that has been active since at least 2012. The group has been observed conducting espionage attacks that are **Likely** in support of the interests of the Chinese government, specifically the Ministry of State Security (MSS). The group has also been observed conducting financially motivated attacks that are **Likely** to help fund the group's operations. Analysis of the group's activities has indicated that the group conducts the majority of their espionage attacks during the day and their financially motivated attacks in the evening – outside of typical business hours. This type of work pattern and dual focus indicates an **Even Chance** that APT41 works on a contractual bases for the Chinese government, which then turns a blind eye to the group's cybercriminal activity as long as China-based organizations are not targeted in those attacks.

APT41 is considered to be technically sophisticated, deploying custom malware and exploiting zero-day vulnerabilities in their attacks. MoonBounce, a malware observed being used by APT41, was considered to be the "most advanced" UEFI firmware implant ever identified at the time.

From 2019-2020, the U.S. Department of Justice (DoJ) issued indictments for five members of APT41 for attacks on more than 100 victims. These attacks included stealing source code, code-signing certificates, customer account data, and business

information, in addition to criminal schemes – ransomware deployment and cryptocurrency theft. Additionally, the U.S. DoJ indicted two Malaysian businessmen who were cooperating with APT41. Despite these indictments, APT41 activity has remained consistent.

- In 2019, APT41 reportedly conducted Operation CuckooBees, which targeted organizations in North America, Asia, and Europe. The group reportedly exfiltrated hundreds of gigabytes of data during the attacks, including blueprints, diagrams, formulas, and manufacturing-related proprietary data.
- In 2020, APT41 reportedly attempted to exploit Citrix NetScaler/ADC, Cisco routers, and Zoho ManageEngine Desktop Central at over 75 organizations, including organizations. The group deployed the Speculoos malware that allows threat actors to manipulate files, execute commands and more.
- Throughout 2021, APT41 was attributed to campaigns targeting multiple organizations worldwide to deploy Cobalt Strike beacons and backdoor malware. The group then attempted to steal sensitive data and maintain persistence within the victims' networks.

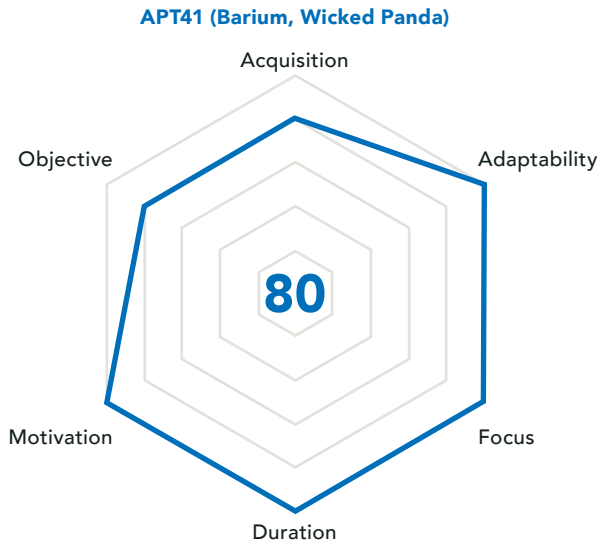

Figure 12: Threat Actor Metric™ for APT41

Ransomware Groups with Manufacturing Targets

Ransomware groups often target manufacturing organizations due to the perceived profits, the amount of information that can be held for ransom, and the potential impact of these attacks. While manufacturing organizations have begun focusing on cybersecurity and risk protection, these organizations have historically been more focused on production and results. This has led to significant opportunities for ransomware operators to target manufacturing companies. Ransomware operators that have targeted the manufacturing vertical most often include LockBit, Alphv, Royal, Black Basta, and Clop.

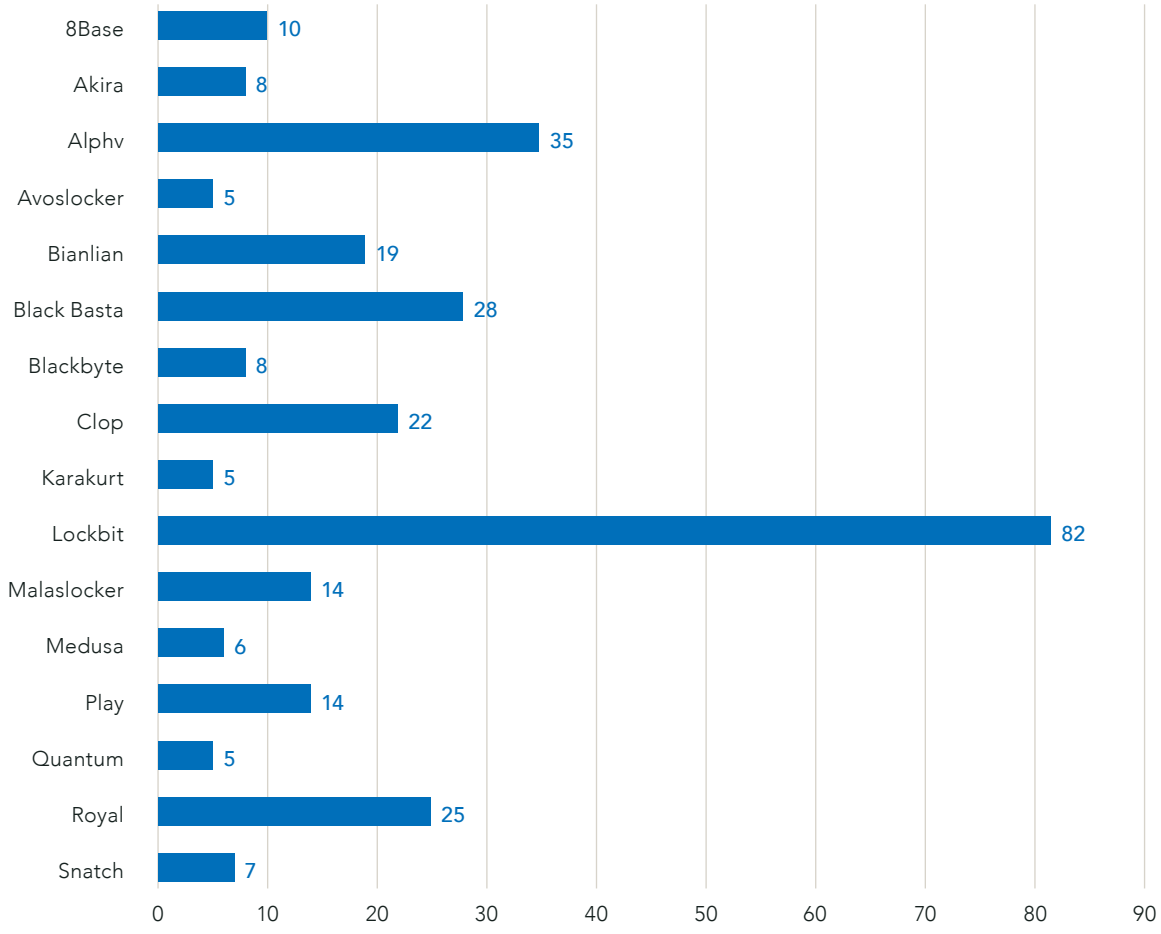

Figure 13: Ransomware variants that listed manufacturing organizations on their data leak site from August 1, 2022 - July 31, 2023

LockBit

LockBit affiliates target organizations in all verticals and around the world. Of the 898 victims listed on LockBit's data leak site from August 1, 2022 - July 31, 2023, 82 of them (9.1%) are in the manufacturing vertical.

- In December 2022, LockBit ransomware operators listed an Italian company on their data leak site and reportedly gave the organization nine days to negotiate the ransom payment. The group reportedly demanded $299,999 for the deletion of all data and $1,000 to extend the countdown timer by one day. The group claimed to have stolen 200GB of data. The post has since been removed, but it is not known if the victim paid the ransom.
- In March 2023, LockBit ransomware operators listed a U.S.-based organization on their data leak site. At the time of writing, the post includes seven screenshots of purportedly stolen data, including financial documents, applications, contact lists, and operations data. The post also includes one link to the purported data.
- In June 2023, LockBit ransomware operators listed the U.S. operations of a Japanese organization on their data leak site. The group claimed to have stolen data from the organization. However, the company released a statement that there was no evidence that personal or financial information or IP was compromised. The group has since removed the company from their data leak site.

Alphv

Of the 353 victims listed on Alphv's data leak site from August 1, 2022 - July 31, 2023, 35 of them (9.9%) are in the manufacturing vertical.

- In December 2022, Alphv ransomware operators listed a U.S.-based organization and posted pictures of five file directories as proof of compromise. The company released a statement that they were targeted, and that access information potentially included personal information including names, emails, addresses, tax ID numbers, and banking information. The same company was purportedly targeted by the Hive ransomware group in December 2022.
- In March 2023, Alphv ransomware operators named a U.S.-based organization on their data leak site. The post did not disclose what type of data the threat actors accessed. The company stated that the attack was on a third-party vendor that does not have access to customer data. While the organization is still listed on Alphv's data leak site at the time of writing, the post does not include any other information besides the company logo.
- In May 2023, Alphv operators listed an Italian organization on their data leak site. The group posted pictures of potential designs, file directories, financial data, and more. The group stated that the company had 72 hours to contact the group and have the data removed. The ransom demand is not known.

Royal

Of the 199 victims listed on Royal's data leak site from August 1, 2022 - July 31, 2023, 25 of them (12.6%) are in the manufacturing vertical.

- In October 2022, Royal ransomware operators listed a U.S.-based organization on their data leak site and claimed to have stolen sensitive data. The group did not indicate the amount or type of data stolen. However, there are six links to purportedly stolen files on the post at the time of writing.
- In February 2023, Royal ransomware operators listed a Brazilian manufacturing organization on their data leak site. The group claimed to have stolen 88GB of data from the organization. The post includes two links to archived data purportedly stolen from the organization.

Black Basta

Of the 212 victims listed on Black Basta's data leak site from August 1, 2022 - July 31, 2023, 28 of them (13.2%) are in the manufacturing vertical.

- In December 2022, Black Basta listed and claimed to have stolen data from a organization based in Canada. The group posted screenshots of credit card applications, schedules, and financial data. The ransom demand is not known.
- In March 2023, Black Basta listed a U.K.-based organization on their data leak site and claimed to have stolen sensitive data from the organization. The group did not post any screenshots or details of the attack other than the organization name and a description. There is an **Even Chance** that the organization paid the ransom demand.

Cl0p

Of the 376 victims listed on Cl0p's data leak site from August 1, 2022 - July 31, 2023, 22 of them (5.9%) are in the manufacturing vertical.

- In March 2023, Cl0p ransomware operators listed an Italy-based organization on their data leak site. The post included nearly 160 links to purportedly stolen data that each contained roughly 700MB of data in them (totaling nearly 100GB). The screenshots on the post included spreadsheets with contact information, passports, and visa paperwork.
- In June and July 2023, Cl0p ransomware operators listed 15 organizations on their data leak site that they targeted as part of a massive campaign exploiting a MOVEit Transfer MTF software vulnerability. The group posted multiple links to purported stolen data and screenshots of spreadsheets, IDs, financial data, and design details.

Transportation

Transportation organizations are an attractive target for threat actors due to the access credentials, customer records, and employee PII that prove valuable for espionage campaigns. The transportation vertical has undergone significant digitization shifts over the last several years to track travel, routes, deliveries, and customers—leading to increased attack surface. As many cyberattacks are opportunistic, the increased attack surface results in an increase in targeting of the transportation organizations. As countries focus on infrastructure bills that include investments to improve transit – such as public transit, airports, rail funding, and electric vehicle chargers – APT actors are **Likely** to target these organizations to obtain information that would be of strategic importance to their sponsored governments. APT groups that have targeted the transportation vertical include TA2541, Tropic Trooper (aka Antlion, Earth Centaur, KeyBoy), and APT27 (aka Bronze Union, LuckyMouse, Threat Group-3390, Budworm).

TA2541

TA2541 has been attributed to Nigeria. This APT group is not considered technically sophisticated due to the fact that they purchase instead of develop their own custom malware. The group is known for the deployment of various remote access trojans (RATs) targeting multiple verticals, including transportation. TA2541 often uses phishing email lures related to transportation and travel. When the group first began operations, they would send macro-laden Microsoft Word attachments that downloaded the RAT payload. However, the group pivoted to focus on sending messages with links to cloud servers that host the payload. In addition to RAT malware variants, the group has been observed using multiple ransomware variants, including Locky, Cerber, and Sage 2.0. There is an **Even Chance** that TA2541 conducted these ransomware attacks to fund further operations or to cover for stealing sensitive information that would be of strategic interest to the Nigerian government.

- In 2019, TA2541 was attributed to a phishing campaign targeting multiple organizations to deploy the Netwire malware. The campaign involved the use of VBScript, PowerShell, and the .NET framework to perform a code injection attack prompting victims to open a Google Drive document.
- From 2019 to 2021, TA2541 was attributed to the Operation Layover campaign targeting the transportation vertical. The group sent phishing emails with malicious attachments that used aviation and transportation lures to deliver the AsyncRAT and njRAT.
- In 2022, TA2541 reportedly conducted a phishing campaign using aviation lures to target organizations. The group deployed various RATs against the victim organizations to maintain remote access and steal information.

Tropic Trooper

Tropic Trooper (aka Antlion, Earth Centaur, KeyBoy) is an APT group attributed to China that has been active since at least 2011. The group has participated in politically motivated cyberespionage activities against countries near the South China Sea. The group focuses on targeting the government, technology, transportation, and consumer cyclicals verticals.

Tropic Trooper attempts to gain initial access to victim networks via phishing or exploiting vulnerabilities in web applications or services. The group is most known for long-lasting campaigns, with up to 250+ days of dwell time in victim networks. Their long game allows them to conduct extensive data exfiltration without detection.

- In 2020, Tropic Trooper used COVID-19 themed phishing emails to target multiple organizations with the PoisonIvy malware variant. The group reportedly targeted organizations that would be of strategic interest to the Chinese government, including transportation organizations.
- From 2020-2021, Tropic Trooper targeted organizations by exploiting vulnerabilities in Microsoft Internet Information Services (IIS) and Exchange servers. The group attempted to access flight schedules, documents, and financial data.
- In 2022, Tropic Trooper reportedly targeted organizations in Chinese-speaking countries with SMS Bomber, YAHOYAH, Nimba, and TClient backdoor malware variants. These variants allow the group to maintain remote access and exfiltrate sensitive information. Tropic Trooper

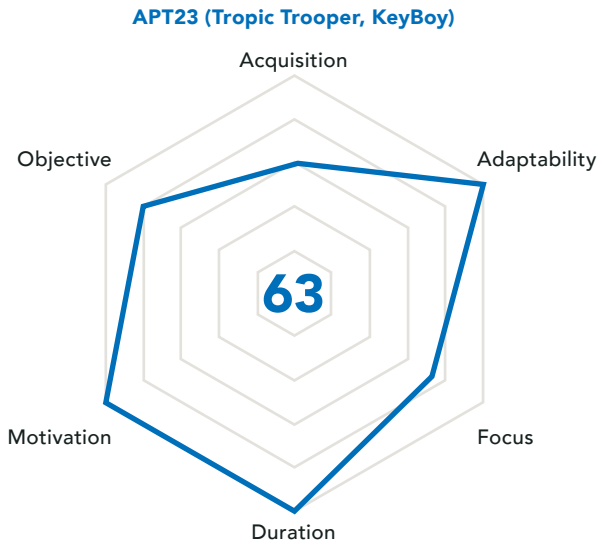

Figure 14: Threat Actor Metric™ for Tropic Trooper

APT27

APT27 (aka Bronze Union, LuckyMouse, Threat Group-3390, Budworm) is a Chinese-speaking threat group that has been active since at least 2015. The group has historically focused on Western targets in cyber espionage campaigns that leverage watering hole attacks. Some reports have referred to this attack vector as strategic web compromises (SWCs), using compromised websites to deliver malware. APT27 has also targeted a national data center in Central Asia, likely to conduct watering hole attacks at a country-wide level. Other attacks saw APT27 installing web shells on Microsoft SharePoint servers to compromise targeted organizations.

Based on the group's domestic security conduct and foreign intelligence gathering operations, there is an **Even Chance** that APT27 is comprised of multiple sub-groups. The fact that their activity timelines coincide with a workday in the People's Republic of China, along with their targeting of both foreign and domestic entities, indicates that the group may be connected to a civilian intelligence service, rather than the People's Liberation Army.

- In 2015, APT27 was attributed to a watering hole attack launched from over 100 compromised legitimate websites, which resulted in data theft from 50 of the organizations across the U.S. and U.K. Sites targeted included organizations in the manufacturing, government, and transportation verticals.
- From 2020-2021, APT27 was attributed to a malicious campaign targeting organizations in India. The threat group reportedly sent phishing emails and exploited vulnerabilities to gain initial access to the victims' networks.

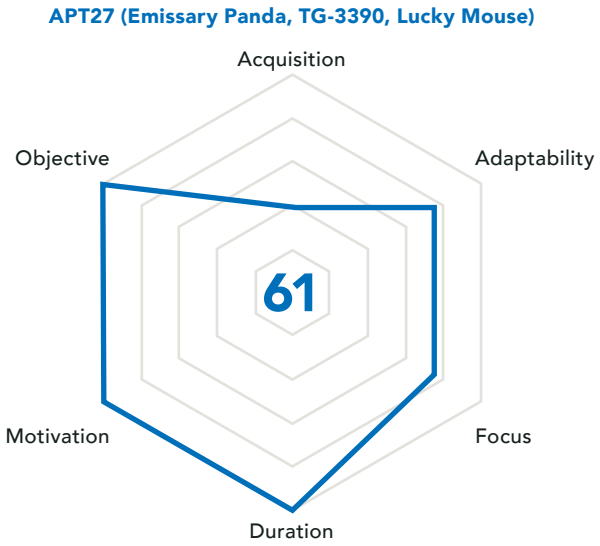

Figure 15: Threat Actor Metric™ for APT27

Ransomware Groups with Transportation Targets

Similar to other industrial verticals, the transportation vertical is an attractive target for ransomware operators. Transportation organizations are **Likely** to pay the ransom demand to avoid any critical business and social impact, as downtimes would have a significant impact on customers, deliveries, partners, and reputation. Transportation organizations typically host a significant amount of PII that they could use to launch additional cyberattacks, sell data on cybercriminal forums, and leverage against the organization. Multiple groups have targeted public transportation organizations, including train operators, airports, and seaports. Ransomware operators have also targeted logistics organizations, resulting in delayed deliveries, delayed troops movements in the Russia-Ukraine war, and more. The top ransomware operators that have targeted the transportation vertical include LockBit, Play, Royal, MalasLocker, and Alphv.

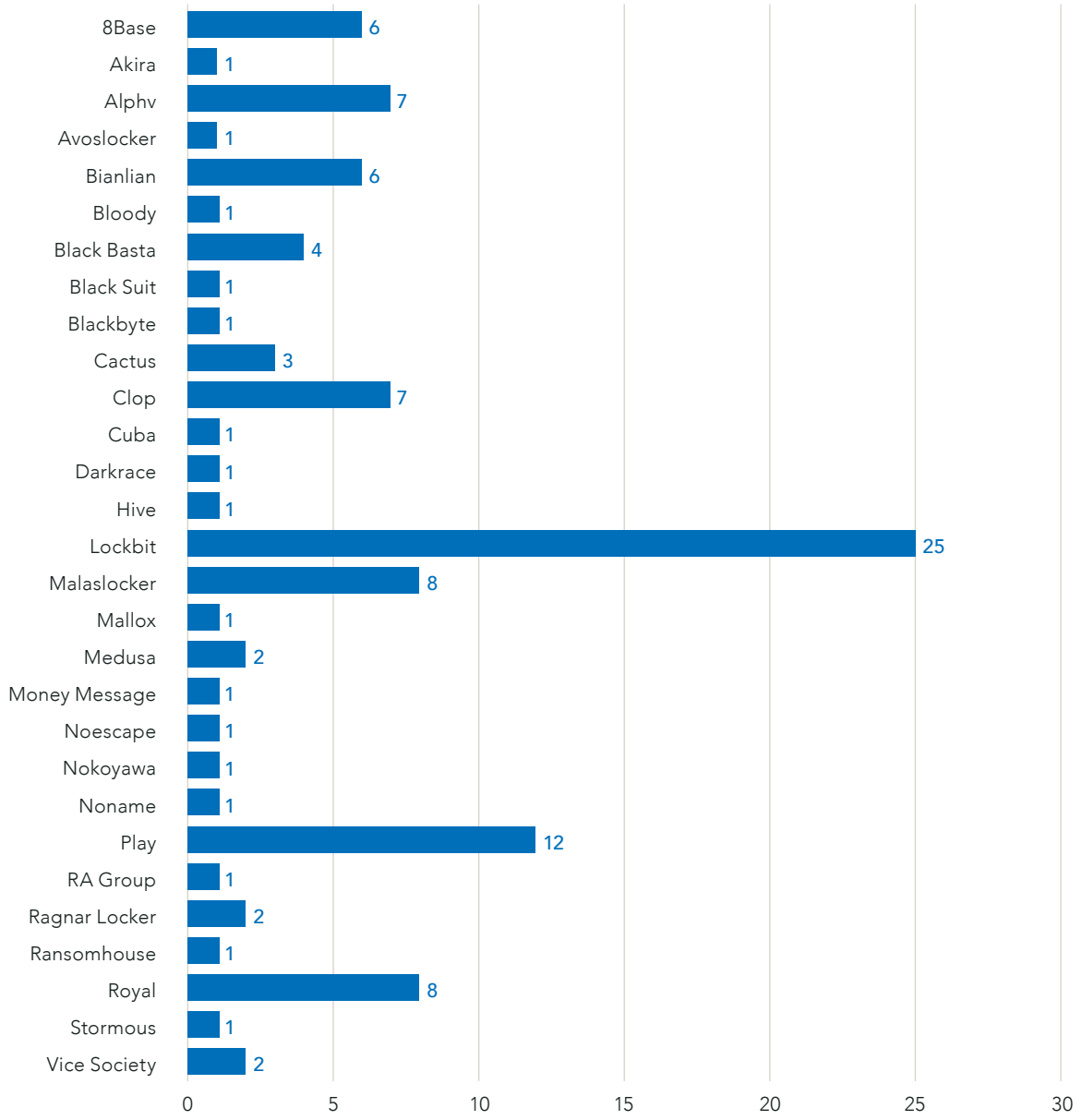

Figure 16: Ransomware variants that listed transportation organizations on their data leak site from August 1, 2022 - July 31, 2023

LockBit

Of the 898 victims listed on LockBit's data leak site from August 1, 2022 - July 31, 2023, 25 of them (2.8%) are in the transportation vertical.

- In December 2022, LockBit operators claimed to have successfully targeted an organization in Portugal. The group reportedly did not impact organizational operations. However, they claimed to have exfiltrated data, including financial reports, budgets, and personal customer data. The operators demanded a ransom of $1.5 million. It is not known if the organization paid the ransom demand. At the time of writing, the post includes one link to download the purported data and 15 screenshots.
- In February 2023, LockBit operators named an Italian organization on their data leak site and set their "countdown" for 11 days before data would be leaked. The operators did not disclose the type or amount of data that they stole, and the ransom demand is not known. The company has since been removed from the site. However, it is not known if the victim paid the ransom.
- In June 2023, LockBit operators named another Italian organization on their data leak site and gave the organization eight days to contact the group to negotiate the ransom. The ransom demand is not known. At the time of writing, the post indicates that all the data is posted. However, it post includes one link, one file, and no screenshots of purported data. The group claims the download is 4.09MB of data.

Play

Play ransomware was first identified in June 2022 and participates in double extortion tactics, where sensitive data is stolen and leaked on the group's data leak site if the ransom demand is not paid. Play gained a reputation within the first few months of operations, indicating that the group is comprised of developers and operators with previous ransomware experience.

Security researchers have discovered that Play uses many tactics that follow the playbook of Hive and Nokoyawa ransomware operations, including similarities in the file names and paths of their tools and payloads. Security researchers also found connections between Play and Quantum ransomware operations. Quantum is known for being a splinter group of the former Conti ransomware operation. The Cobalt Strike beacons used in observed Play ransomware attacks have the same watermark used by the Emotet and SVCReady botnets, which have both been observed in Quantum attacks. Play ransomware is Microsoft Visual C++ based and contains several anti-debugging and anti-analysis features to slow investigations into the malware.

Of the 172 victims listed on Play's data leak site from August 1, 2022 - July 31, 2023, 12 of them (7%) of them are in the transportation vertical.

- In December 2022, Play operators listed a Swedish company on their data leak site and claimed to have stolen personal documents, forms, agreements, passports, crew lists, contracts, shipment information, and archives. The group provided a download link for the purported stolen data with a RAR password when the victim did not pay the ransom demand.
- In March 2023, Play operators listed a company based in the Netherlands and claimed to have stolen sensitive data that included private and personal confidential data, passports, contracts, and more. The group included a download link for the purported data with a RAR password and stated that there was 5GB of compressed data included.
- In July 2023, Play operators named a organization based in Spain and claimed to have stolen 150GB of data. The data included client and employee data, contracts, financial data, and more. The post included a download link for the purported data and a RAR password.

Royal

Of the 199 victims listed on Royal's data leak site from August 1, 2022 - July 31, 2023, 8 of them (4%) are in the transportation vertical.

- In February 2023, Royal operators named a U.S.-based organization on their data leak site. The group included three links to purported stolen data and claimed that data was 100% leaked. Based on the posted links, it is **Unlikely** that the organizations paid the ransom.
- In March 2023, Royal operators named a U.S.-based organization on their data leak site. The group included one link to purported stolen data.
- In May 2023, Royal operators named another U.S.-based organization on their data leak site. The group included one link to purported stolen data and claimed that they had leaked 10% of the 40GB of total stolen data.

MalasLocker

MalasLocker is a new ransomware operation that was first observed in April 2023. The group participates in double extortion methods and maintains a data leak site. MalasLocker claims to have a distaste for corporate entities and economic inequality. Rather than demand a ransom, the group claims to provide a decryption key to companies that donate to a MalasLocker-approved charity. This action, along with the fact that 30% of the group's victims are based in Russia, suggests that the group is politically rather than financially motivated. The operators target Zimbra servers and upload suspicious JSP files to specific directories. Their initial access vector is not known at the time of writing.

Of the 171 victims listed on MalasLocker's data leak site from August 1, 2022 - July 31, 2023, 8 of them (4.7%) are in the transportation vertical.

- In May 2023, MalasLocker named eight organizations located in the U.K., the U.S., South Africa, and Russia on their data leak site. Unlike other threat actors, MalasLocker data leak site posts did not include stolen data. Instead, they included the Zimbra configuration for the targeted organizations. It is not known if any of the listed companies provided donations to MalasLocker-approved charities.

Alphv

Of the 353 victims listed on Alphv's data leak site from August 1, 2022 - July 31, 2023, 7 of them (2%) are in the transportation vertical.

- In September 2022, Alphv posted a U.S.-based organization on their data leak site and claimed to have stolen payment databases, credit card information, PII, driver's licenses, and recorded videos of passengers and accidents. The group claimed to have stolen 2TB of data from the organization. The ransom demand is not known.
- In April 2023, the Alphv operators listed a Brazil-based organization and claimed to have stolen employee and client data, financial and banking data, contracts, partner data, agreements, and internal documents. The group included screenshots of the purported data, including contracts, invoices, passports and IDs, and financial documents. The ransom demand is unknown.

Professional and Commercial Services

Professional and commercial services organizations are an attractive target for threat actors due to the amount of sensitive information they host, the interconnectivity of these organizations with their clients, and the ability to have a significant impact on the organization. These organizations are likely to have a significant number of remote workers, which increases their attack surface. The APT groups that have been most often targeted professional and commercial services organizations include APT19 (aka Codoso, Codoso0, Sunshop Group, Bronze Firestone), APT17 (Deputy Dog, Aurora Panda, Group 72), and APT1 (Comment Crew, Comment Group, Comment Panda, Byzantine Candor). While APT1 has not been active since 2018, it is **Likely** that group members have been consolidated into currently active groups. They are included in this white paper for insight into their TTPs.

APT19

APT19 (aka Codoso, Codoso0, Sunshop Group, Bronze Firestone) is a Chinese threat group that has been active since at least 2010. APT19 has been referred to as Deep Panda. There are inconsistencies on whether these are the same group or not, although both groups are attributed to China's government.

The group has created multiple custom malware variants. Many of them are similar to the Derusbi malware, indicating the group may have access to the Derusbi source code. Although the group's TTPs have remained relatively unchanged, and their malware is like those used by other cybercriminals and APT groups, APT19 remains a credible threat to organizations. APT19 is assessed to conduct cyber espionage against verticals and individuals of strategic interest to the Chinese government.

- In 2015, APT19 reportedly targeted multiple organizations, including a professional services provider, to access sensitive data related to multiple national security personnel. To gain initial access, the threat actors exploited a vulnerability in an SAP enterprise resource planning application.
- In 2016-2017, APT19 reportedly targeted multiple organizations in the professional and commercial services vertical to collect sensitive information for a strategic advantage.
- In 2018, the U.S. Department of Justice charged two Chinese intelligence officers, six hackers, and two aerospace company insiders in a conspiracy to steal confidential information from U.S. and French companies.
- In 2022, APT19 reported began targeting VMware Horizon servers with the Log4Shell vulnerabilities to deploy the Fire Chili rootkit, which was digitally signed using a stolen certificate in order to evade detection.

APT17

APT17 (Deputy Dog, Aurora Panda, Group 72) is a China-based group that has been active since at least 2009 and has been attributed to work for the Jinan bureau of the Chinese Ministry of State (MSS). APT17 has targeted numerous organizations worldwide. However, 52% of their attacks have targeted the U.S. for the purposes of intelligence gathers. The group consistently conducts operations to identify and exfiltrate information from commercial organizations in Japan, South Korea, North Korea, and the U.S. The group has been attributed to attacks leveraging custom malware delivered via spoof profiles, posts, spear phishing emails, zero-day exploits, and watering hole attacks.

APT17 group reportedly does not conduct targeted attacks, but instead targets hundreds of different organizations in multiple verticals. The group is reported to be composed of hackers for hire with capabilities to attack organizations with concurrently running operations. Multiple reports indicate that the group includes at least 50-100 people.

While the group has multiple custom malware variants, these variants are similar to malware used by other groups. One example is Destroy RAT, which is nearly identical to PlugX. The group's two main variants, Naid and Moudoor, have been observed in multiple campaigns. They and were both signed with stolen digital certificates from Bit9, which was targeted in 2012. Many of the campaigns linked to APT17 are based on shared or reused infrastructure, making attribution difficult.

- In 2012, APT17 reportedly conducted Operation Voho, an information-stealing campaign that targeted over 1,000 companies. The group conducted a watering hole attack to deploy gh0st RAT, which was disguised as Microsoft or Symantec software.
- In 2013, APT17 reportedly targeted multiple organizations in Japan and the U.S. to deploy the McRAT Trojan, HiKit rootkit, and more. The goal of the attacks was to purportedly steal sensitive information that would be of strategic interest to the Chinese government.
- In 2018, APT17 reportedly targeted multiple organizations in South Korea with the goal of stealing sensitive information. The threat actors deployed the 9002 RAT by compromising the update server of a remote support solutions provider.

APT1

APT1 (Comment Crew, Comment Group, Comment Panda, Byzantine Candor) is a Chinese threat group, active since at least 2006, that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. APT1 has reportedly targeted 141 organizations, with their longest known access lasting for 1,764 days (4 years and 10 months).

APT1 has an incredibly large infrastructure, including nearly 1,000 C2 servers hosted on nearly 850 distinct IP addresses in 13 countries – including 109 in the U.S. Mandiant researchers have identified three personas associated with APT41, including UglyGorilla, DOTA, and SuperHard.

- APT1 has historically been observed revisiting the victims' networks over several months or years and stealing intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victims' leadership. The group's largest theft included 6.5 terabytes of compressed data from a single organization over a 10-month period. The majority of APT1 victims match industries that China has identified as strategic to their growth, and 87% of the victims have been headquartered in English-speaking countries.

From 2010-2016, APT1 reportedly conducted a large-scale campaign, Operation Dust Storm, targeting multiple industries in Japan, South Korea, the U.S., and Europe – including professional and commercial services organizations. The operation included spear phishing, watering hole attacks, and zero-day exploits. APT41 leveraged multiple backdoors in an alleged effort to collect sensitive information that would be of strategic interest to the Chinese government and related to China's Five-Year Plan.

- In 2014, APT1 reportedly conducted Operation Siesta, where threat actors sent spear phishing emails with malicious attachments addressed to executives.
- In 2018, APT1 allegedly targeted organizations in South Korea, the U.S., and Canada, with the goal of stealing sensitive information via spear phishing attacks with malicious attachments.

Ransomware Groups with Professional and Commercial Services Targets

Professional and commercial services organizations handle valuable information that typically includes client data, research, and intellectual property used to deliver insights and solutions that can be delivered to other organizations. As organizations in this vertical increasingly rely on cloud-based services to conduct business, ransomware operators can conduct a single intrusion that could lead to supply-chain attacks targeting hundreds or thousands of other organizations. Ransomware operators that have targeted the professional and commercial services vertical include LockBit, Clop, Alphv, Black Basta, and BianLian.

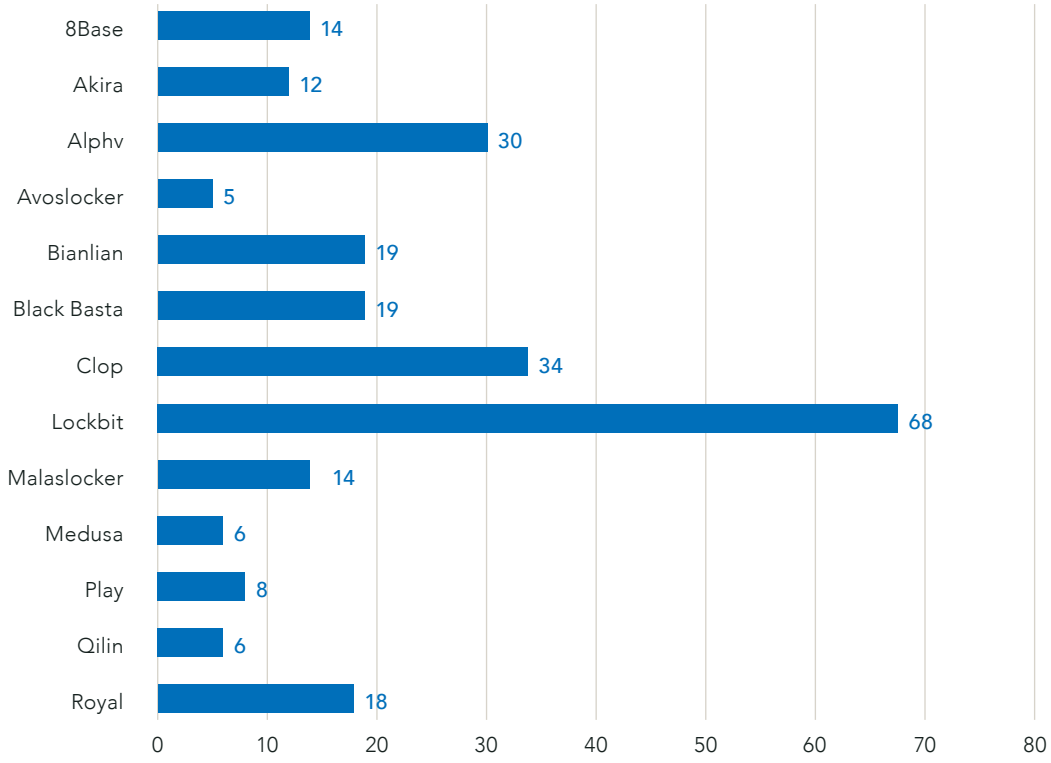

Figure 17: Ransomware variants that listed professional and commercial services organizations on their data leak site from August 1, 2022 - July 31, 2023

LockBit

Of the 898 victims listed on LockBit's data leak site from August 1, 2022 - July 31, 2023, 68 of them (7.6%) are in the professional and commercial services vertical.

- In October 2022, LockBit operators listed an organization based in Spain on their data leak site and gave the company 10 days to pay the ransom or contact the group. The group claimed to have stolen data that included client and financial information. The ransom demand is not known. At the time of writing, the post included 10 screenshots of purported data accessed and nine links to the purportedly stolen data.
- In January 2023, LockBit operators named a Morocco-based organization on their data leak site and gave the company 14 days to contact the group. The post has been removed since posting. However, it is not known if the victim paid the ransom.
- In April 2023, LockBit operators named a Romania-based organization on their data leak site and gave the organization four days to contact the group or pay the ransom. The group claimed to have stolen 216GB of data that included email correspondence, PII, and other sensitive documents. At the time of writing, the group claims that the data has been published, the group has posted 8 screenshots, one file, and one link to download the purported 53.6GB of stolen data.

Cl0p

Of the 376 victims listed on Cl0p's data leak site from August 1, 2022 - July 31, 2023, 34 of them (9%) are in the professional and commercial services vertical.

- In March 2023, Cl0p named a U.S-based consulting company on their data leak site as part of the purported victims targeted by exploiting the vulnerability in GoAnywhere software. The post on the data leak site includes screenshots of log files, one download link, and claims to include presentations, videos, and xlsx databases.
- In April 2023, Cl0p named a U.S.-based employment services company on their data leak site. The operators posted 397 links to purported stolen data. Additionally, the screenshots included insurance information, job descriptions, an Excel sheet that includes email addresses, names, phone numbers, and positions held.
- In July 2023, Cl0p operators named a U.S.-based information services organization on their data leak site as part of the organizations targeted via the MOVEit vulnerability. The post includes screenshots of insurance documents and archives, and states that 99GB of data was stolen.

Alphv

Of the 353 victims listed on Alphv's data leak site from August 1, 2022 - July 31, 2023, 30 of them (8.5%) are in the professional and commercial services vertical.

- In August 2022, the Alphv ransomware group targeted an Italian consulting company. The ransom demand is not known. The post on the group's data leak website hosted screenshots of employee IDs, passports, invoices, contracts, and more.
- In August 2023, Alphv targeted a U.S.-based business support services organization on their data leak site. The group claimed to have leaked 57.7GB of data from the organization. The screenshots included screenshots of IDs, passports, applications, contracts, invoices, emails, and more. The ransom demand is unknown.

Black Basta

Of the 212 victims listed on Black Basta's data leak site from August 1, 2022 - July 31, 2023, 19 of them (8.9%) are in the professional and commercial services vertical.

- In November 2022, the Black Basta group named an India-based consulting company on their data leak site. The group did not include any screenshots or disclose the type of data that was purportedly stolen. The company is still named on the data leak site. However, no data has been leaked. There is an **Even Chance** that the ransom was paid or that another threat actor purchased the data.
- In April 2023, the Black Basta operators named a U.S.-based business support services organization on their data leak site. The group included pictures of agreements, financial documents, and applications. The ransom demand is not known.

BianLian

Of the 193 victims listed on BianLian's data leak site from August 1, 2022 - July 31, 2023, 19 of them (9.8%) are in the professional and commercial services vertical.

- In August 2022, BianLian operators listed an Australia-based organization on their data leak site. The group claimed to have stolen 10,662 folders that contained personal and medical data, monthly business reports, and operational files.
- In December 2022, BianLian operators listed an India-based consulting company on their data leak site and claimed to have stolen 110GB from the organization—including company projects, financial documents, personal data, technical data, and fileserver archives.
- In January 2023, BianLian operators listed an Australia-based professional services organization on their data leak site. The ransom demand is not known.

Legal Services

Legal services organizations are often attractive targets for threat actors due to the amount of information hosted, the impact an attack could have, and the access to potential client data. Legal services organizations connect with and support clients, including other organizations, which could give threat actors access to a significant amount of data. As law firms often deal with confidential and time sensitive business, threat actors can use their access to victims' networks to send phishing emails to other organizations. Not only do legal services organizations have to worry about their reputation, but they also must be concerned with compliance mandates and confidentiality laws. Legal services organizations, especially smaller firms, are **Unlikely** to have a significant security budget, which could lead to opportunistic attacks. APT groups that have been observed targeting the legal services vertical include APT29 (aka Cozy Bear, DarkHalo, Midnight Blizzard, BlueBravo), APT10 (AKA Cicada, Potassium, Stone Panda, menuPass, Red Apollo, CVNX, and HogFish), and APT5 (aka PittyTiger, Mulberry Typhoon, Poisoned Flight).

APT29

APT29 (aka Cozy Bear, DarkHalo, Midnight Blizzard, BlueBravo) is attributed to the Russian Federation that has been active since at least 2008. The group conducts espionage and intelligence gathering activity using highly sophisticated techniques and malware against government and government-affiliated entities in the U.S. and globally. APT29 is **Almost Certainly** a politically motivated threat group.

Custom tools used by APT29 include the malware "WellMess," "WellMail," and "SoreFang," which were used in attempted thefts of COVID-19 vaccine data from the U.S., U.K., and Canada in July 2020. Other notable custom malware includes the "SUNBURST" backdoor used in the SolarWinds attack, the custom Cobalt Strike loader, "TEARDROP," and the C2, backdoor "GoldMax".

APT29 is considered highly professional, with high levels of technical expertise and custom malware. The group's operations include two categories. The first is a "smash and grab" technique focused on rapidly exfiltrating data with later transitions to stealthier surveillance, credential access, and lateral movement. The second consists of slower, and stealthier methods that establish persistence and harvest credentials before eventually compromising the entire domain.

- In 2016, APT29 reportedly targeted organizations in the U.S. with spear phishing attacks that deployed malware to assist the threat actors with stealing sensitive information.
- In 2019, APT29 reportedly sent phishing emails targeting U.S. organizations with the goal of stealing sensitive information.
- From 2019-2020, APT29 was attributed to the targeting SolarWinds networks to inject test code into the organization's network management and monitoring suite of products. Then, in 2020, the group reportedly injected trojanized code into a file that was later included in updates. The code provided APT29 with a backdoor to gain initial access to multiple organizations, including those the professional and commercial services vertical.
- In 2021, APT29 reportedly conducted multiple campaigns that included the use of phishing emails with malicious attachments to deploy malware in multiple organizations' networks, with the purported goal of stealing sensitive information.
- In 2023, APT29 has continued to launch attacks involving the use of phishing emails with malicious attachments to deploy backdoor and information stealing malware against organizations worldwide. The purported goal of these attacks is to collect information that would be of strategic interest to the Russian government.

APT10

APT10 (AKA Cicada, Potassium, Stone Panda, menuPass, Red Apollo, CVNX, and HogFish) has been active since at least 2006. Individual members of APT10 are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Bureau and worked for the Huaying Haitai Science and Technology Development Company.

APT10 concentrates its efforts on cyber espionage, likely in support of the strategic national goals of the People's Republic of China (PRC) in their focus on sensitive proprietary information to support Chinese operations. APT10 has been observed gaining initial access via spear phishing attacks with malicious attachments, supply-chain attacks, and vulnerability exploitations. APT10 spear phishing attacks have been relatively unsophisticated, leveraging .lnk files within archives, files with double extensions, and, in some cases, simply identically named decoy documents and malicious launchers within the same archive.

The group has used dozens of backdoors and other malware in their campaigns since 2006. While the group is considered highly sophisticated, many of the tools and malware variants (including custom variants) observed in their attacks have been used in other APT campaigns and cybercriminal cyberattacks.

Despite charges and international law enforcement attention, APT10 is still active and remains a credible threat to organizations worldwide. The group has been observed using both custom and publicly available tools and will likely continue to develop and improve their malware and capabilities in order to conduct campaigns undetected over the next 12-24 months.

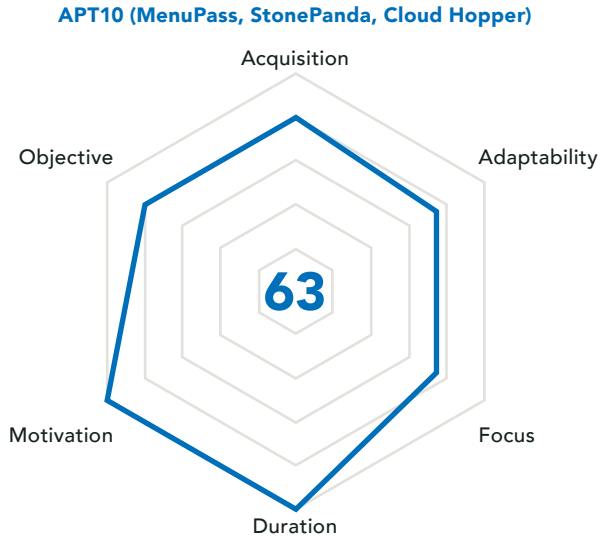

Figure 18: Threat Actor Metric™ for APT10

APT5

APT5 has been attributed to the People's Republic of China and has been active since at least 2007 and appears to consist of several subgroups, each with its own infrastructure and TTPs. APT5 has been known to exploit zero-day vulnerabilities in virtual private network (VPN) devices, with the goal of gaining initial access and stealing sensitive data. Few APT5 attacks have been reported, but the group is believed to be highly sophisticated. It is thus **Highly Likely** that the group has been responsible for attacks that have gone undetected. TTPs used by the group include compromising network devices, initial access via vulnerability exploitation or malware, and information harvesting.

- In 2019, APT5 reportedly exploited the Fortinet vulnerability, CVE-2018-13379, and the Pulse Secure flaw, CVE-2019-11510, in the attempt to steal files storing password information or VPN session data.
- In 2021, APT5 reportedly targeted a Pulse Secure VPN vulnerability, CVE-2021-22893, to target U.S. organizations. The group deployed malware to harvest AD credentials and bypass multifactor authentication on the devices that could then be used to access victim networks.

Ransomware Groups with Legal Services Targets

Threat groups often seek out legal services organizations because they are considered "easy targets" – with less security protocols in place and significantly valuable data to harvest. Law firms keep many different types of data, including PII of clients, sensitive information from organizations, case information, and data that is often not publicly available. When this type of data is exfiltrated, a unique situation emerges where the firm must weigh the options of paying the ransom or facing the legal and reputation consequences of the attack. Ransomware operators that have been observed targeting the legal services vertical include LockBit, Alphv, Black Basta, 8Base, and BianLian.

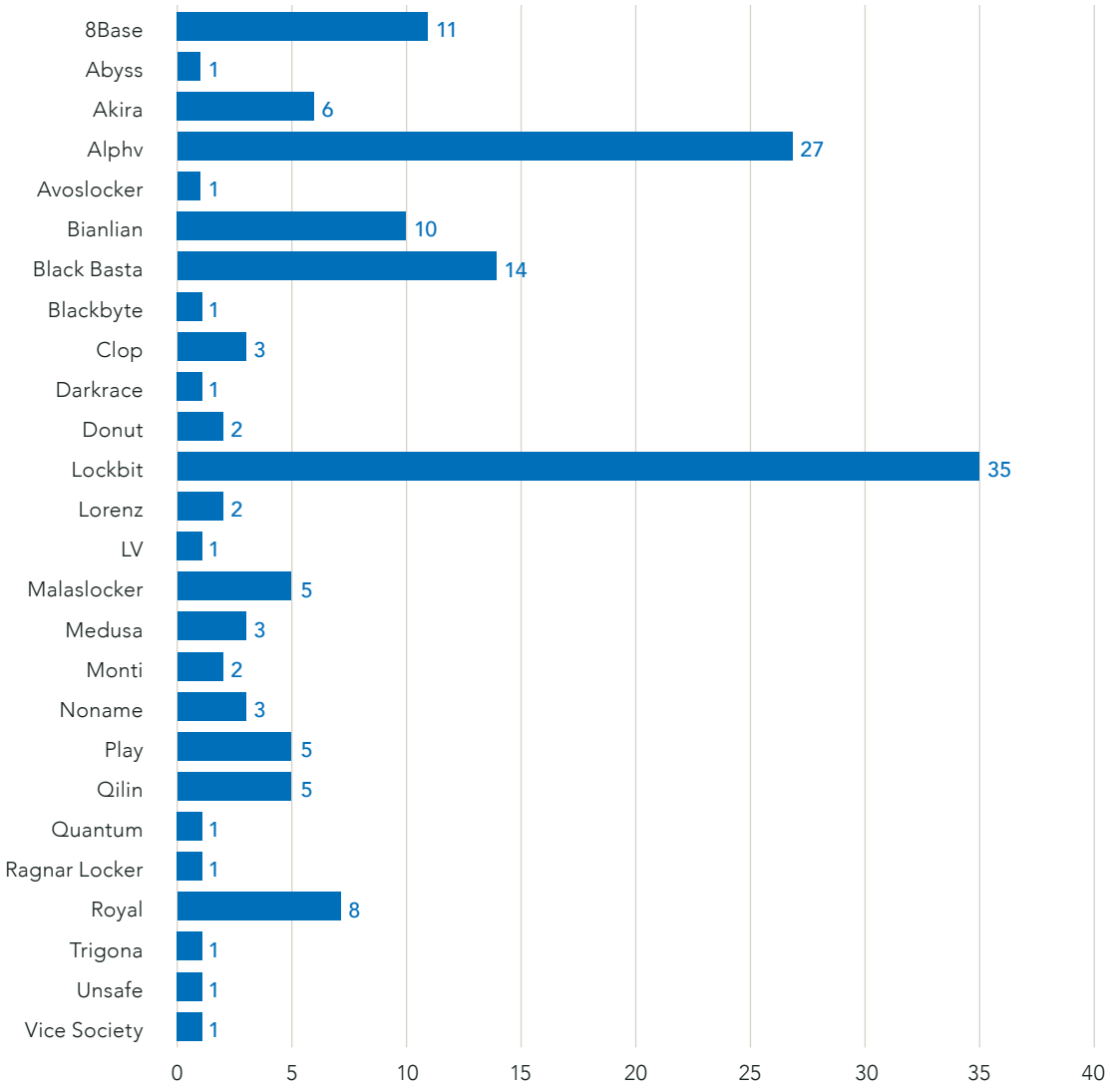

Figure 19: Ransomware variants that listed legal services organizations on their data leak site from August 1, 2022 - July 31, 2023

LockBit

Of the 898 victims listed on LockBit's data leak site from August 1, 2022 - July 31, 2023, 35 of them (3.9%) are in the legal services vertical.

- From August-October 2022, LockBit operators named 17 organizations on their data leak site across North America, Europe, Oceania, and Europe. The group claimed to have stolen data from the organizations, including client lists, staff PII, financial data, and more.
- In July 2023, LockBit operators named a Lebanon-based organization on their data leak site. The group claimed to have obtained client information, invoices, case-related documentation, and financial documentation. The victim is listed on the data leak site at the time of writing. LockBit has demanded $5,000 to extend the timer for 24 hours and $400,000 to destroy or download the data.

Alphv

Of the 353 victims listed on Alphv's data leak site from August 1, 2022 - July 31, 2023, 27 of them (7.6%) are in the legal services vertical.

- In October 2022, Alphv ransomware operators named a U.S.-based organization on their data leak site. The group claimed to have stolen 200GB of data, including emails and client information. The company's listing on the data leak site hosts one link to 121GB of purportedly stolen data.
- In February 2023, Alphv operators named a U.K.-based organization on their data leak site and claimed to have stolen 446GB of data. The group claimed to have obtained staff and client PII, as well as a complete network map, including credentials. The post on the data leak site hosts screenshots of case documentation, IDs, passports, and a payment card.
- In April 2023, Alphv operators named an Australia-based organization. The group claimed to have stolen 4TB of data that included employee PII, accounting data, insurance contracts, agreements, client documentation, and credentials. The company is no longer listed on the data leak site. However, it is not known if the victim paid the ransom or was removed for another reason.

Black Basta

Of the 212 victims listed on Black Basta's data leak site from August 1, 2022 - July 31, 2023, 14 of them (6.6%) are in the legal services vertical.

- In December 2022, Black Basta operators named a U.S.-based organization on their data leak site and claimed to have stolen data, including contact information, emails, and financial information.
- In May 2023, Black Basta operators named a Germany-based organization on their data leak site and posted screenshots of purportedly stolen data, including client documentation, invoices, medical information, and employee PII.

8Base

Of the 140 victims listed on 8Base's data leak site from August 1, 2022 - July 31, 2023, 11 of them (7.9%) are in the legal services vertical.

- In March 2023, 8Base ransomware operators named an Australia-based organization on their data leak site. The post includes one link to a third-party data hosting website that hosts the purported stolen data.
- In June 2023, 8Base operators named a U.S.-based organization on their data leak site. The group claimed, via the post, to have obtained passports, checks, personal data, client data, and communications. While the company is still listed on the data leak site, the post is listed as "EXPIRED" and does not include any links or screenshots of purported data.
- In July 2023, 8Base operators named a German-based organization on their data leak site. The group claimed to have stolen 200GB of data that included internal documents, customer data, tax documents, and client data. The post includes multiple links to a third-party data hosting site where the purported data is hosted.

BianLian

Of the 193 victims listed on BianLian's data leak site from August 1, 2022 - July 31, 2023, 10 of them (5.2%) are in the legal services vertical.

- In August 2022, BianLian operators named a U.S.-based organization on their data leak site. The group posted 15 links to purported stolen data and claimed that the information included projects, financial documentation, and staff PII.
- In February 2023, BianLian operators named a U.S.-based organization on their data leak site and claimed to have received 500GB of data, including financial documents, staff PII, human resources information, and archived data.
- In June 2023, BianLian operators named three organizations across North America on their data leak site. The group claimed to have stolen staff PII, transcripts, and more.

Construction and Engineering

Construction and engineering organizations have been increasingly targeted by threat actors, often due to the perceived lack of security measures and the potential access to other organizations' data. Historically, these organizations have been immune to the cyberattacks faced by the rest of the world. This is mainly due to the belief that, unlike legal or transportation organizations, construction and engineering organizations host little personal information. However, construction and engineering organizations often host client and partner data, as well as leverage machine learning and other new technologies—making them attractive targets. APT groups observed targeting the construction and engineering vertical include BlackTech (aka Palmerworm, Circuit Panda, Earth Hundun), Energetic Bear (aka Dragonfly, Crouching Yeti, Group 24, Havex, Koala Team, IRON LIBERTY), and Bronze Starlight (aka Cinnamon Tempest, Emperor Dragonfly).

BlackTech

BlackTech (aka Palmerworm, Circuit Panda, Earth Hundun), a group that has been active since 2010, is attributed to the People's Republic of China. The group is known for their cyber espionage attacks against East Asian countries, particularly Taiwan, that appear to be motivated by the political interests of the Chinese government. BlackTech often uses custom malware for their attacks and are considered to be technically sophisticated. In 2020, Taiwanese government officials stated that BlackTech threat actors were working for, and aligned with, the Chinese Communist Party. BlackTech often abuses legitimate software tools and processes to achieve its goals, including the use of stolen digital certificates and API hooking.

- In 2018, BlackTech reportedly used a stolen digitally signed certificate from D-Link Corporation to deploy malware against an unnamed organization. The malware, PLEAD, was used to collect saved passwords from Google Chrome, Internet Explorer, Outlook, and Mozilla Firefox.
- From 2020-2021, BlackTech reportedly targeted Japanese organizations with the Flagpro malware variant. The group reportedly spread the malware via phishing emails with a malicious attachment.
- In 2022, BlackTech reportedly exploited CVE-2022-1388 in F5 BIG-IP to target organizations with the TSCookie and BIFROSE malware variants. The group reportedly conducted these attacks to steal sensitive information that would be of strategic value to the Chinese government.

Energetic Bear

Energetic Bear (aka Dragonfly, Crouching Yeti, Group 24, Havex, Koala Team, IRON LIBERTY) has been active since at least 2010. Energetic Bear is known to primarily conduct operations targeting the control systems of critical infrastructure in the energy and industrial sectors. The group has been linked to Russia's Federal Security Service (FSB) Center 16 by U.S. authorities. Energetic Bear's primary goal is to collect intelligence and steal intellectual property that would be of strategic interest to the Russian government.

The main tactics of the group include sending phishing emails with malicious documents and infecting various servers. The group uses some of the infected servers for auxiliary purposes – to host tools and logs. Others are deliberately infected to use them in watering hole attacks to reach the group's main targets.

Energetic Bear increased their attacks targeting Ukraine in 2016-2017, which is in line with targeting by Russia-linked threat groups. Energetic Bear has reportedly been an integral part of the Russian cyberattacks against Ukraine and Western allies since the start of the Russia-Ukraine war.

- From 2016-2017, Energetic Bear was attributed to a campaign targeting servers in multiple countries, including construction and engineering organizations in Russia and Ukraine. The group deployed data gathering tools and vulnerability scanners.
- From 2015-2019, Energetic Bear was attributed to campaigns that involved the group sending phishing emails, conducting watering hole attacks, and exploiting zero-day vulnerabilities to target global organizations, including construction organizations. The group's goal is assessed as data theft of information that would be of strategic interest to the Russian government.

- After 2022, Energetic Bear's activity has been primarily focused on Russia's war efforts against Ukraine, including the targeting of multiple industrial organizations – including construction and energy organizations in Ukraine and Western-supporting countries.

Bronze Starlight

Bronze Starlight (aka Cinnamon Tempest, Emperor Dragonfly) has been active since 2021 and attributed to China. The group is most known for their use of ransomware, including custom ransomware and RaaS operations. However, the victimology and operations of these ransomware variants are different than many of the present-day ransomware operations. The group uses specific ransomware variants for a short time before rebranding or switching to another affiliate program to target organizations of strategic interest to the Chinese government. These factors indicate that the group **Likely** conducts ransomware attacks to both fund their operations and as a cover for exfiltrating sensitive data that could be of interest to the Chinese government.

In addition to developing their own ransomware, Bronze Starlight has also used the "LockBit 2.0" (now LockBit 3.0) affiliate program to conduct ransomware attacks. The group has exploited vulnerabilities in public-facing applications to deploy ransomware, including the Log4Shell zero-day vulnerability (CVE-2021-44228), as well as vulnerabilities in Confluence (CVE-2021-26084) and on-premises Microsoft Exchange servers (CVE-2021-34473).

- From August-October 2021, Bronze Starlight was attributed to ransomware attacks deploying the LockFile ransomware variant. The group used the ransomware to target financial services, construction and engineering, consumer cyclicals, manufacturing, and legal services organizations.
- Beginning in April 2022, Bronze Starlight deployed the LockBit 2.0 ransomware variant in attacks. The group reportedly targeted manufacturing, retail, consumer cyclicals, construction and engineering, and professional and commercial services organizations.
- Bronze Starlight was attributed to ransomware attacks deploying the Cheers ransomware variant. The group reportedly targeted industrials, health care, transportation, technology, construction and engineering, and consumer cyclicals organizations.

Ransomware Groups with Construction and Engineering Targets

Ransomware groups often target construction and engineering organizations due to the perceived profits and impact of an attack. Ransomware attacks that shut down a company's network often delay projects and risk data being stolen, which impacts the victims' reputation. Construction and engineering organizations that maintain government and military contracts are **Likely** to be targeted due to the type of information that they host related to the agency. The construction and engineering vertical often has limited industry regulations and guidelines, especially related to cybersecurity measures. Employees in this vertical are often part of a distributed workforce spread across different job sites. This type of work environment can lead to an increased attack surface and a bigger opportunity for successful social engineering attacks. Ransomware operators observed targeting the construction and engineering vertical include LockBit, Alphv, Black Basta, Royal, and Play.

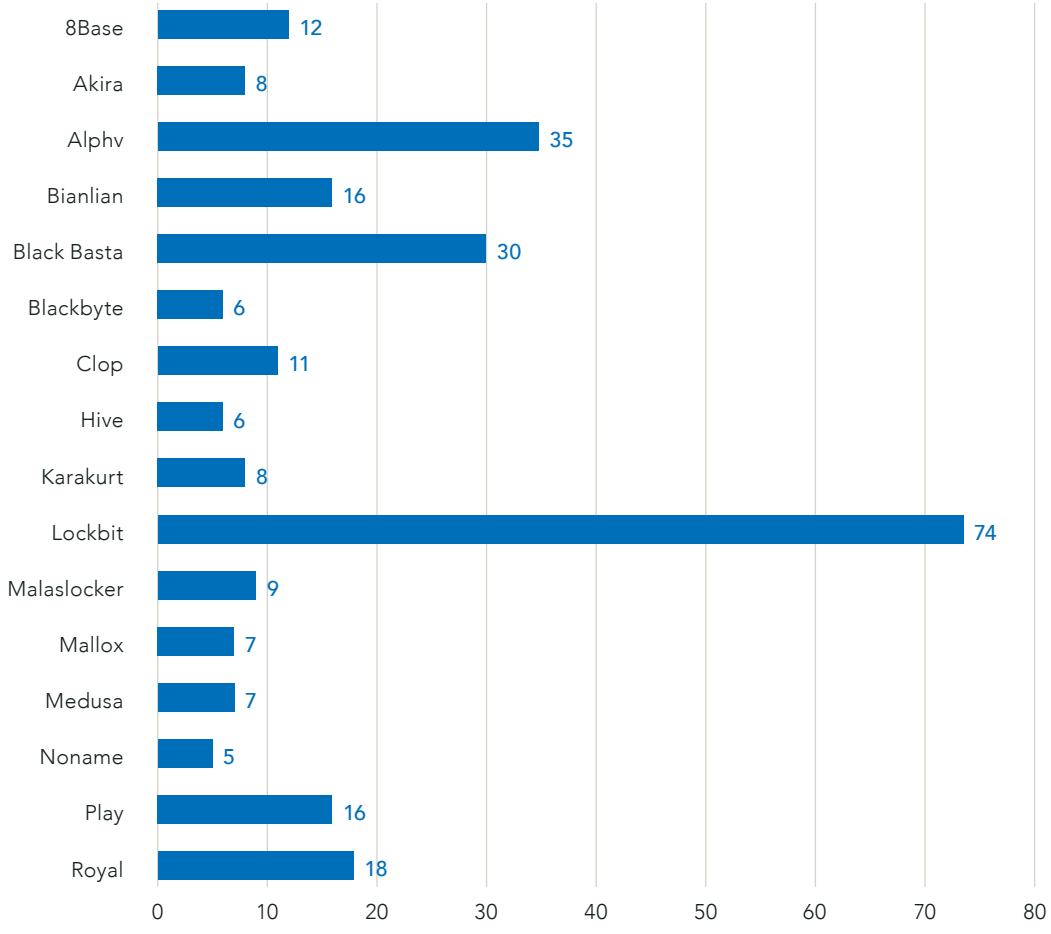

Figure 20: Ransomware variants that listed construction and engineering organizations on their data leak site from August 1, 2022 – July 31, 2023

LockBit

Of the 898 victims listed on LockBit's data leak site from August 1, 2022 – July 31, 2023, 74 of them (8.2%) are in the construction and engineering vertical.

- In August 2022, LockBit operators posted a U.S.-based organization on their data leak site. The group posted screenshots of purportedly accessed file directories, including financial folders and files related to recruiting, insurance, audits, and more. The listing includes one file with 4KB of purported data and screenshots.
- In October 2022, LockBit operators posted a New Zealand-based organization on their data leak site. The company is still listed on the data leak site. The post includes one file with 4KB of purported data and a link to another purported 2.6GB of data.
- In February 2023, LockBit operators named a U.S.-based organization on their data leak site. The group includes one link to purportedly stolen data.
- In May 2023, LockBit operators named a Scotland-based company on their data leak site. The company is no longer listed on the data leak site, but it is not known if the company paid the ransom demand.

Alphv

Of the 353 victims listed on Alphv's data leak site from August 1, 2022 - July 31, 2023, 35 of them (9.9%) are in the construction and engineering vertical.

- In August 2022, Alphv operators named a U.S.-based organization on their data leak site and claimed to have stolen 200GB of data from the organization. The group gave the organization three days to contact the group and begin negotiations or pay the ransom. The company is still listed on the data leak site. However, no screenshots, links, or files are listed.
- In December 2022, Alphv operators named a U.K.-based company on their data leak site and claimed to have leaked 41.9GB of data across multiple links to third-party data hosting websites.
- In June 2023, Alphv named a Canada-based organization on their data leak site. The group posted a link to a third-party data hosting website as proof of compromise. However, the link has since been removed from the data leak site. The company is still listed without any purported stolen data linked or posted.

Black Basta

Of the 212 victims listed on Black Basta's data leak site from August 1, 2022 - July 31, 2023, 30 of them (14.2%) are in the construction and engineering vertical.

- In October 2022, Black Basta operators listed a U.S.-based organization on their data leak site. The group posted screenshots of purportedly stolen data that included information status forms, staff contact information, financial information, IDs, and employment onboarding documents.
- In April 2023, Black Basta operators named a U.S.-based organization on their data leak site, where they posted screenshots of passports, IDs, work orders, financial documents, and staff contact lists.
- In June 2023, Black Basta operators listed a U.K.-based construction company on their data leak site, where they posted screenshots of staff's education degrees, confidentiality agreements, financial documents, and invoices.

Royal

Of the 199 victims listed on Royal's data leak site from August 1, 2022 - July 31, 2023, 18 of them (9%) are in the construction and engineering vertical.

- In November 2022, Royal ransomware operators named a U.S.-based company on their data leak site. The company has since been removed, but it is not known if a ransom demand was paid. The group appears to have removed any named companies listed prior to May 2023. There is an **Even Chance** that the company was removed during the site cleanup.
- In March 2023, Royal operators named a U.S.-based company on their data leak site. The company is no longer named on the data leak site, and it is unknown if the company paid the ransom.
- In May 2023, Royal operators named a U.K.-based architectural company on their data leak site and claimed to have stolen 100GB of data. At the time of writing, the post includes one link to purported stolen data.

Play

Of the 172 victims listed on Play's data leak site from August 1, 2022 - July 31, 2023, 16 of them (9.3%) are in the construction and engineering vertical.

- In March 2023, Play ransomware operators named a U.S.-based company on their data leak site. The group claimed to have stolen personal and corporate confidential information, IDs, passports, contracts, and more. The company is still listed on the data leak site, and the post includes one link and RAR password to download the purportedly stolen data.
- In June 2023, Play ransomware operators named a U.S.-based organization on their data leak site and claimed to have stolen 33GB of data. The group claimed that the data included PII of staff, projects, passports, financial data, and client documentation. The company is still listed on the data leak site, with one link and a RAR password to the purportedly stolen data.

The Overlap

Both APT and ransomware groups have been observed using similar TTPs and have multiple overlapping tools, targeted vulnerabilities, and techniques. Optiv's gTIC recognizes that post-incident attribution and malware identification take less priority than proactive detection and defensive measures against known behaviors and overlapping techniques. Therefore, we performed manual research of processes and behaviors obtained for 19 different ransomware strains and 26 APT groups from Iran, China, North Korea, Russia, Vietnam, and Pakistan during active campaigns. Optiv's gTIC acknowledges there are exceptions amongst notable groups who modify or create bespoke post-exploitation malware. However, it is important to note that in most instances, initial access, persistence, lateral movement, and credential access are achieved via commonly observed tools and techniques. The tables below detail the overlap between the groups mentioned in this white paper.

Vulnerability	Description	Affected Product	CVSS	Groups Observed Targeting
CVE-2009-3129	Memory Corruption Vulnerability	Microsoft Excel Featheader Record	9.3	APT1, APT29, APT5
CVE-2010-3333	Stack-based Buffer Overflow Vulnerability	Microsoft Office	9.3	APT29, APT36, Tropic Trooper
CVE-2011-0611	RCE Vulnerability	Adobe Flash Player	9.3	APT1, APT19, Energetic Bear
CVE-2012-0158	Buffer Overflow Vulnerability	MSCOMCTL.OCX library	9.3	APT10, APT29, APT32, APT36, APT41, APT5, BlackTech, Tropic Trooper
CVE-2012-1723	Arbitrary Code Execution Vulnerability	Oracle Java SE Runtime Environment (JRE)	10	APT17, Energetic Bear
CVE-2012-1856	RCE Vulnerability	Microsoft Office MSCOMCTL.OCX library	9.3	APT36, Tropic Trooper
CVE-2012-1889	Memory Corruption Vulnerability	Microsoft XML Core Services	9.3	APT1, APT17
CVE-2013-0322	XSS Vulnerability	Ubercart module 7.x-3.x before 7.x-3.4 for Drupal	4.3	APT41, Cl0p
CVE-2015-1641	Memory Corruption Vulnerability	Microsoft Office	9.3	APT36, APT41, Tropic Trooper
CVE-2015-1770	Memory Use Vulnerability	Microsoft Office	9.3	APT36, Tropic Trooper
CVE-2015-5119	User-After-Free Vulnerability	Adobe Flash Player	10	APT10, BlackTech
CVE-2016-7255	Elevation of Privilege Vulnerability	Microsoft Windows Vista, 7, 8.1, 10 and Windows Server 2008, 2012, and 2016 Win32k	7.8	APT29, APT32
CVE-2017-0199	RCE Vulnerability	Microsoft Office/Wordpad	7.8	APT19, APT32, APT36, APT41, BlackTech, MuddyWater, Tropic Trooper
CVE-2017-0213	Elevation of Privilege Vulnerability	Microsoft Windows	4.7	APT27, APT33

Vulnerability	Description	Affected Product	CVSS	Groups Observed Targeting
CVE-2017-11882	Memory Corruption Vulnerability	Microsoft Office	7.8	APT32, APT41, MuddyWater, Tropic Trooper
CVE-2017-7269	Buffer Overflow Vulnerability	Microsoft Internet Information Services (IIS)	9.8	APT17, BlackTech
CVE-2018-0798	Backdoor Exploitation Chain	Microsoft Office 2007-2016	8.8	APT27, Tropic Trooper
CVE-2018-0802	Backdoor Exploitation Chain	Microsoft Office 2007-2017	7.8	APT32, Tropic Trooper
CVE-2018-13379	Credential Exposure Vulnerability	Fortinet FortiOS SSL VPN	9.8	Alphv, APT29, APT5, Energetic Bear, LockBit, MuddyWater, Play
CVE-2019-11510	Arbitrary File Reading Vulnerability	Pulse Connect Secure VPN	10	APT29, APT41, APT5
CVE-2019-1653	Improper Access Control Vulnerability	Cisco RV320 and RV325 Routers	7.5	APT29, APT41
CVE-2019-19781	Directory Traversal Vulnerability	Citrix Application Delivery Controller and Citrix Gateway	9.8	APT29, APT41, Energetic Bear
CVE-2020-0688	Static Key Vulnerability	Microsoft Exchange	8.8	APT1, APT29, Energetic Bear, MuddyWater
CVE-2021-26084	Confluence Server Webwork OGNL Injection Vulnerability	Confluence Server and Data Center	9.8	APT10, Bronze Starlight
CVE-2021-26857	Deserialization Vulnerability	Microsoft Unified Messaging	7.8	APT27, APT29
CVE-2021-26858	RCE Vulnerability	Microsoft Exchange Server	7.8	APT27, APT29
CVE-2021-27065	RCE Vulnerability	Microsoft Exchange Server	7.8	APT27, APT29
CVE-2021-40539	Authentication Bypass Vulnerability	Zoho ManageEngine ADSelfService Plus	9.8	APT27, Bronze Starlight
CVE-2022-1388	Missing Authentication Vulnerability	F5 BIG-IP	9.8	APT5, BlackTech
CVE-2022-26134	RCE Vulnerability	Atlassian Confluence Server and Data Center	9.8	APT41, Cl0p, Tropic Trooper
CVE-2022-30190	RCE Vulnerability	Microsoft Windows Support Diagnostic Tool (MSDT)	7.8	Black Basta, Tropic Trooper
CVE-2023-27350	Improper Access Control Vulnerability	PaperCut MF/NG	9.8	Cl0p, LockBit, MuddyWater
CVE-2023-27351	Improper Authentication Vulnerability	PaperCut NG 22.0.5	7.5	Cl0p, LockBit

Vulnerability	Description	Affected Product	CVSS	Groups Observed Targeting
Log4Shell (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832)	RCE, DoS, DoS, RCE Vulnerabilities	Apache Log4j Java Library	10, 9, 5.9, 6.6	Alphv, APT10, APT19, APT41, Bronze Starlight, Karakurt, MuddyWater
ProxyLogon (CVE-2021-26855)	RCE Vulnerability	Microsoft Exchange	9.8	Alphv, APT10, APT27, APT29, APT41, Tropic Trooper
ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207)	Pre-Auth Path Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities	Microsoft Exchange	9.8, 9.8, 7.2	APT10, Alphv, BianLian, Bronze Starlight
Spring4Shell (CVE-2022-22965)	RCE Vulnerability	Spring Framework JDK 9+	9.8	Alphv, Black Basta
ZeroLogon (CVE-2020-1472)	Privilege Escalation Vulnerability	Netlogon	10	APT10, BianLian, Black Basta, Cl0p, Energetic Bear, MuddyWater

Tool	Description	Groups Observed Using Tool
AdFind	A free command-line query tool that can be used for gathering information from Active Directory (AD).	APT10, APT29, LockBit, Play, Royal
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.	Alphv, LockBit
Advanced Port Scanner	A free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.	BianLian, LockBit, Royal
All In One	A live desktop distribution that can be used to recover files and reset Windows passwords.	APT17, APT5
AnonFiles	An online file storage provider that allows users to store and share files anonymously.	LockBit, MuddyWater
AnyDesk	A remote desktop application that provides remote access to computers and other devices.	BianLian, Black Basta, Karakurt, LockBit, Tropic Trooper
Arp	A communication protocol used for discovering the link layer address, such as MAC address, associated with a given internet layer address.	APT32, BianLian
Atera	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.	BianLian, Black Basta, LockBit, Royal
Backstab	A tool that terminates antimalware-protected processes. It can be used to terminate EDR-protected processes.	Black Basta, LockBit

Tool	Description	Groups Observed Using Tool
BITSAdmin	A command-line tool used to create, download, or upload jobs, and to monitor their progress.	Alphv, APT41, Black Basta, SiameseKitten, Tropic Trooper
BloodHound	An Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.	APT10, APT29, LockBit, Play
certutil	A command-line program used to dump and display certification authority (CA) configuration information, configure certificate services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.	APT10, APT27, APT41
cmd	A program used to execute commands on a Windows computer.	APT10, SiameseKitten
Cobalt Strike	A post-exploitation tool that is often used during cyberattacks to deploy beacons.	Alphv, APT10, APT19, APT27, APT29, APT32, APT41, Black Basta, Bronze Starlight, Cl0p, Karakurt, MuddyWater, Play, Royal
Connectwise	Formerly ScreenConnect. A self-hosted remote desktop software application that can be used to remotely access victim environments.	MuddyWater, Royal
CrackMapExec	An open-source tool that leverages Mimikatz to enable users to harvest credentials and move laterally through an Active Directory environment.	Energetic Bear, MuddyWater
Dropbox	A cloud storage service that allows users to save files online and sync them to other devices.	APT10, APT19, APT27, APT29, APT41, Tropic Trooper
dsquery	A command-line tool that can be used to query Active Directory for information from a system within a domain.	APT17, APT41
Empire	A tool that is similar to Metasploit but specific to PowerShell. It allows you to run PowerShell scripts in memory and make a connection back to your machine.	APT19, APT33, APT41, MuddyWater, Play, SiameseKitten
FileZilla	A free open-source file transfer protocol software tool that allows users to set up FTP servers or connect to other FTP servers to exchange files.	APT41, Karakurt, LockBit
fscan	A comprehensive internal netowrk scanning tool that provides numerous functions including network and vulnerability scanning, reverse shell building, and common services brute-forcing.	APT41, Tropic Trooper
GitHub	An internet hosting service for software development and version control that has been used by threat actors to host malware.	APT41, MuddyWater, TA2541, Tropic Trooper
GMER	A tool used to detect and remove rootkits.	LockBit, Play, Royal
gsecdump	A publicly available credential dumper used to obtain password hashes and LSA secrets from Windows OS.	APT1, APT10, APT27, APT5
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.	Alphv, APT10, APT27, BianLian, Bronze Starlight, Energetic Bear, LockBit, MuddyWater

Tool	Description	Groups Observed Using Tool
ipconfig	A command-line utility that is used to display and manage the IP address assigned to the machine.	APT1, APT27, APT29, APT32, APT41, SiameseKitten
Koadic	A Windows post-exploitation framework and penetration testing tool that is publicly available on GitHub.	Alphv, MuddyWater
LaZagne	An open-source application used to retrieve passwords stored on a local computer.	Alphv, APT33, APT36, LockBit, MuddyWater
Ligolo	A simple and lightweight tool for establishing SOCKS5 or TCP tunnels from a reverse connection in complete safety.	Alphv, LockBit, MuddyWater
LSASS	A Windows process that takes care of security policy for the OS.	Alphv, APT1, APT41, BianLian, Play, Tropic Trooper
MEGAsync	A cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.	Alphv, BianLian, Karakurt, LockBit
Meterpreter	A Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.	APT41, Bronze Starlight, MuddyWater
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.	Alphv, APT1, APT10, APT17, APT27, APT29, APT32, APT33, APT41, APT5, Black Basta, Energetic Bear, Karakurt, LockBit, MuddyWater, Play, SiameseKitten, Tropic Trooper
NBTScan	An open-source tool that has been used to conduct internal reconnaissance within a compromised network.	APT27, APT41
Net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.	APT1, APT10, APT19, APT27, APT29, APT32, APT33, APT41, Energetic Bear
Netscan	A utility that scans within a subnet or IP address range to check for devices.	Play, Royal
netsh	A scripting utility used to interact with networking components local or remote systems.	APT32, Energetic Bear
Netstat	A tool that generates displays that show network status and protocol statistics.	APT27, APT41, SiameseKitten
Ngrok	A tool that exposes local servers behind NATs and firewalls to the public internet over secure tunnels.	Alphv, BianLian, LockBit
NirCmd	A command-line tool that can be used to manipulate a variety of setting son a computer, modify the registry, add shortcuts, and open the default internet connection.	Black Basta, Royal
NirSoft	A collection of tools that include password recovery utilities, network monitoring tools, command-line utilities, and more.	Alphv, Kimsuky, APT24

Tool	Description	Groups Observed Using Tool
Nmap	An open-source utility for network discovery that runs on all major computer operating systems and includes multiple tools that can be used to transfer data, compare scan results, and generate packets.	APT41, Energetic Bear
Nsudo	An open-source tool used to disable AV solutions.	Black Basta, Royal
ntdsutil	A command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).	APT10, APT41
PasteBin	A text storage site used by threat actors to host malware.	APT41, TA2541
PC Hunter	A toolkit for Windows with various powerful features for kernel structure viewing and manipulating.	LockBit, Play
Ping	A tool used to test whether a particular host is reachable across an IP network.	APT10, APT19, APT41, SiameseKitten
PoshC2	An open-source remote administration and post-exploitation framework that is publicly available on GitHub. The server-side components of the tool are primarily written in Python, while the implants are written in PowerShell.	APT33, SiameseKitten
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.	Alphv, APT10, APT19, APT27, APT29, APT33, APT41, BianLian, Black Basta, BlackTech, MuddyWater, Play, Royal, TA2541, Tropic Trooper
PowerSploit	An open-source, offensive security framework comprised of PowerShell modules and scripts that perform a wide range of tasks related to penetration testing such as code execution, persistence, bypassing antivirus, recon, and exfiltration.	APT10, APT32, APT33, APT41, MuddyWater
PowerTool	A security tool that scans and analyzes files at the kernel level; can help threat actors remove and disable security services/software.	LockBit, Play, Royal
ProcDump	A command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that can be used to determine the cause of the spike. Itt also can serve as a general process dump utility that you can embed in other scripts.	Alphv, APT27, APT33, LockBit, Tropic Trooper
Process Hacker	An open-source tool that allows users to see which processes are running on a device and identify network connections that are associated with a process.	LockBit, Royal
PsExec	A utility tool that allows users to control a computer from a remote location.	Alphv, APT10, APT17, APT27, APT29, APT41, APT5, Black Basta, BlackTech, Energetic Bear, LockBit, Play, Royal, Tropic Trooper
Putty	A free and open-source terminal emulator, serial console and network file transfer application.	Alphv, BlackTech, LockBit

Tool	Description	Groups Observed Using Malware
Pwdump	A Windows utility that outputs the LM and NTLM password hashes of local user accounts from the Security Account Manager database and from the Active Directory domain's users' cache on the operating system.	APT1, APT10, APT27, APT41
Rclone	A command-line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.	Alphv, BianLian, Black Basta, Karakurt, LockBit, Royal, Tropic Trooper
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.	Alphv, APT1, APT27, APT29, APT41, BianLian, Black Basta, Cl0p, LockBit, Play
ReadFile	Reads data from a specified file or input/output device.	Alphv, Royal
ScreenConnect	A remote management software used to gain access to a remote computer.	Alphv, LockBit
SharpHound	The official data collector for BloodHound; it is written in C# and uses native Windows API functions and LSAP namespace functions to collect data from domain controllers and domain-joined Windows systems.	APT17, Tropic Trooper
Sliver	An open-source cross-platform adversary emulation/red team framework. It has been increasingly used by threat actors due to the number of tools available, including dynamic code generation, staged and stageless payloads, secer C2, and more.	APT29, Bronze Starlight, Tropic Trooper
SMB	A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.	Black Basta, Bronze Starlight, LockBit, Tropic Trooper
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices.	Alphv, BianLian, LockBit
Splashtop	A remote desktop application that allows users to remotely access their Windows, Mac, and Linux computers from any Windows, Mac, iOS, Android, and Chromebook device.	BianLian, Black Basta, LockBit, Royal
Sqlmap	An open-source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws.	APT41, Energetic Bear
Syncro	A fully featured remote file browser tool that gives users access to virtually every native file function. It can be used to remotely create, rename, copy, delete, or compress files and folders without needing to share screens.	MuddyWater, Royal
SystemBC	A malware written in C that turns infected computers into SOCKS5 proxies.	Black Basta, Play
SystemInfo	A Windows utility that can be used to gather detailed information about a computer.	APT27, APT29
tasklist	A utility that displays a list of applications and services with their process IDs for all tasks running on either a local or a remote computer.	APT1, APT19, APT27, APT29
tcping	A tool that allows you to use a TCP connection to ping a service.	APT10, APT41

Tool	Description	Groups Observed Using Malware
TeamViewer	A comprehensive, remote access, remote control and remote support solution that works with almost every desktop and mobile platform, including Windows, macOS, Android, and iOS.	Alphv, APT41, BianLian, LockBit
Windows Credential Editor	A security tool to list logon sessions and add, change, list and delete associated credentials.	Alphv, APT27, APT41, APT5, BianLian
WinRAR	A trialware file archiver utility for Windows devices that can back up data and reduce the size of email attachments, open and unpack RAR, ZIP and other files downloaded from Internet, and create new archives in RAR and ZIP file format.	APT5, BlackTech, MuddyWater, Play, Tropic Trooper
WinSCP	A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.	Black Basta, Karakurt, LockBit, Play
WMI/WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.	Alphv, APT10, BianLian, Black Basta, Bronze Starlight, Play, Tropic Trooper
WMIExec	A tool that allows threat actors to execute commands on a remote system and/or establish a semi-interactive shell on a remote host.	APT10, APT41

Malware	Description	Groups Observed Using Malware
9002 RAT	A RAT that has been used to remotely access compromised devices and deploy additional malicious payloads from the threat actors' server.	APT17, APT19, APT41
Atomsilo	A ransomware variant first discovered in September 2021. Operated the double extortion method and exploited vulnerabilities to gain initial access. The variant maintains similarities to LockFile and has been observed in campaigns attributed to APT10.	APT10, Bronze Starlight
BATLOADER	Initial access malware that heavily uses batch and PowerShell scripts to gain a foothold on a victim machine and deliver other malware.	MuddyWater, Royal
BlackCoffee	A backdoor that obfuscates IT communications as normal traffic to legitimate websites such as GitHub and Microsoft's Technet portal.	APT17, APT41
China Chopper	A web shell used to provide access back to an enterprise network that does not rely on an infected system calling back to a remote C2 server.	APT10, APT17, APT19, APT27, APT32, APT41
Coroxy	A malware used to gain access to a server or computer.	Black Basta, Play
Derusbi	A DLL backdoor capable of obtaining directory, file, and drive listing, creating a reverse shell; performing screen captures; recording video and audio; listing, terminating, and creating processes; and collecting system and user information.	APT17, APT19, APT41

Malware	Description	Groups Observed Using Malware
gh0st RAT	A publicly available RAT that has the ability to take full control of the remote screen, keylogging, download remote binaries, take control of remote shutdown, disable infected computer remote pointer and keyboard input, list active processes, and clear all existing SSDT of all existing hooks.	APT10, APT27, APT41, APT5, BlackTech, Tropic Trooper
HUI Loader	A custom DLL loader that is loaded by legitimate programs that are vulnerable to DLL search order hijacking. The malware decrypts and loads a third file containing an encrypted payload that is also deployed to the compromised host.	APT41, Bronze Starlight
Lilith	A RAT that is capable of executing commands, manipulating files and directories, and deleting itself.	APT36, Tropic Trooper
LockFile	A ransomware first observed in July 2021 that had been observed targeting ProxyShell vulnerabilities to encrypt data.	APT10, Bronze Starlight
Netwire	A RAT that is designed to focus on password stealing and keylogging, but also allows attackers to remotely access compromised systems.	APT36, TA2541
Night Sky	A ransomware first observed in December 2021 that uses the double extortion method and maintains a data leak site.	APT10, Bronze Starlight
njRAT	A RAT that will silently collect and steal information, including credentials. The malware can perform keylogger monitoring, remote desktop control, additional malicious software installation, and many other malicious activities on the victim's computer.	APT36, APT41, TA2541
Pandora	A ransomware variant that the threat actors deployed via the Log4Shell vulnerabilities. The ransomware is a RaaS operation that rebranded frequently and maintained a data leak site.	APT27, APT10, Bronze Starlight
PlugX	A modular malware that calls back to a C2 server for tasking and is capable of download additional plugins and gather system information.	APT10, APT17, APT19, APT27, APT41, Black Basta, Bronze Starlight
PoisonIvy	A publicly available remote access trojan that can monitor victims remotely and steal user credentials and files.	APT1, APT10, APT17, APT19, APT5, Tropic Trooper
QakBot	A banking trojan that has been used to steal victims' data, including keystrokes and credentials, and to deploy additional payloads.	Black Basta, Royal
QUADAGENT	A PowerShell-based backdoor that has the ability to maintain persistence and gather usernames and current domain.	APT32, MuddyWater
Quasar RAT	A legitimate open-source RAT written in C# that has been used to remotely access compromised devices.	APT10, APT32, APT36, APT41, Tropic Trooper
RevengeRAT	A freely available RAT that automatically gathers system information and allows attackers to access system components, such as webcams, microphones, and other utilities.	APT36, TA2541
Rook	A ransomware operation that was based on the leaked source code of the Babuk ransomware operation.	APT10, Bronze Starlight

Malware	Description	Groups Observed Using Malware
Sakula	A RAT that has been active since at least 2012. Used by multiple China-based APT groups. Can be disguised as legitimate applications and can create a remote shell, download and execute payloads, upload a file, update the C2 server, query malware status, and uninstall malware and itself.	APT17, APT19
Scanbox	A modular, reusable JavaScript-based exploit kit that allows an attacker to first compromise a website using basic attacks such as SQL injection or WordPress bugs and set up a waterhole attack.	APT10, APT19
ShadowPad	AKA Barlaiy, POISONPLUG. A backdoor widely believed to be the successor of the PlugX malware that can download additional payloads and gather system information.	APT41, Tropic Trooper
ZxShell	A publicly available backdoor that can launch port scans, run a keylogger, capture screenshots, set up an HTTP or SOCKS proxy, launch a reverse shell, cause SYN floods, and manipulate files.	APT17, APT27, APT41

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
T1566 – Phishing (Initial Access) T1204 – User Execution (Execution) T1589 – Gather Victim Identity Information (Reconnaissance) T1598 – Phishing for Information (Reconnaissance)	Phishing emails with malicious attachments and links requiring users to enable macros or interact.	Google Docs Microsoft Office Documents ISO Files Embedded Links
T1583 – Acquire Information (Resource Development) T1585 – Establish Accounts (Resource Development) T1588 – Obtain Capabilities (Resource Development)	Attackers acquire accounts and tools to help conduct the attacks.	Purchase servers Dropbox Google Drive GitHub Facebook/Twitter/LinkedIn Mimikatz Cobalt Strike
T1190 – Exploit Public-Facing Application (Initial Access) T1133 – External Remote Services (Initial Access)	Attackers often exploit known vulnerabilities in external remote services and public-facing applications to gain access.	Microsoft Exchange Cisco Fortigate VPN Citrix PulseSecure Outlook Web Access RDP

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
T1053 – Scheduled Task/ Job (Execution) T1112 – Modify Registry (Defense Evasion) T1543 – Create or Modify System Process (Persistence) T1055 – Privilege Injection (Privilege Escalation)	Utilize processes and scheduled tasks to repeatedly execute malicious payloads.	StorSyncSvc Nwsapagent svchost.exe Win7Elevate Rundll32.exe Windows task scheduler schtasks HKEY_CURRENT_USER\ Software\Classes\ HKLM\SYSTEM\ CurrentControlSet\services
T1547 – Boot or Logon Autostart Execution (Persistence) T1543 – Create or Modify System Processes (Persistence) T1546 – Event Trigger Execution (Persistence) T1505 – Server Software Component (Persistence)	Gain persistence by using system mechanisms and creating processes, servers, and boot/logon to execute events and malware deployments.	HKLM\SOFTWARE\Microsoft\ Windows NT\CurrentVersion\Svchost WMI C:\Windows\System32\sethc.exe HKEY_LOCAL_MACHINE\ SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows "AppInit_DLLs"="pserver32.dll" HKLM\Software\Microsoft\ Windows NT\CurrentVersion\ Windows\AppInit_DLLs – %APPDATA%\Intel\ResN32.dll HKLM\Software\Microsoft\ Windows NT\CurrentVersion\ Windows\LoadAppInit_DLLs – 0x1
T1078 – Valid Accounts (Initial Access) T1110 – Brute Force (Credential Access) T1003 – OS Credential Dumping (Credential Access) T1552 – Unsecured Credentials (Credential Access) T1555 – Credentials from Password Stores (Credential Access)	Obtain credentials that allow attackers to use valid accounts to conduct malicious activities.	Mimikatz PsExec Wmic Ncrack CrackMapExec GetPassword_x64 ProcDump ntdsutil.exe Gpppassword
T1562 – Impair Defenses (Defense Evasion)	Stop/disable Windows and AV services.	cmd.exe /c sc.exe stop*/y cmd.exe taskkill /im * net.exe stop * /y net stop security center net stop WinDefend

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
T1564 – Hide Artifacts (Defense Evasion) T1036 – Masquerading (Defense Evasion) T1070 – Indicator Removal on Host (Defense Evasion)	Hide or manipulate features of artifacts to appear legitimate; delete or modify artifacts to remove evidence of their presence.	HKLM\SOFTWARE\ Microsoft\Windows NT\ CurrentVersion\Winlogon\ SpecialAccounts\UserList' /v -WindowStyle Hidden esentutl mshta.exe wscript.exe \Microsoft\Windows\ SoftwareProtectionPlatform\ EventCacheManager Remove-MailboxExportRequest KernelCallbackTable wevtutil cl System wevtutil cl Security
T1087 – Account Discovery (Discovery) T1083 – File and Directory Discovery (Discovery) T1082 – System Information Discovery (Discovery) T1018 – Remote system Discovery (Discovery) T1057 – Process Discovery (Discovery) T1016 – System Network Configuration Discovery (Discovery) T1033 – System Owner/User Discovery (Discovery) T1046 – Network Service Discovery (Discovery) T1049 – System Network Connections Discovery (Discovery)	Perform network/directory/user reconnaissance and enumeration.	Get-ManagementRoleAssignment net user net localgroup administrators net.exe users ipconfig /all >> %temp%\download NBTscan AdFind Net View Ping PlugX "cmd.exe" /C whoami Systeminfo file /bin/pwd tasklist /v

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
T1005 – Data from Local System (Collection) T1074 – Data Staged (Collection) T1056 – Input Capture (Collection)	Collect, stage, and capture data from the system and user inputs.	Forfiles Cobalt Strike njRAT C:\Program Files\Common Files\System\Ole DB\ %TEMP% KEYLIME GEARSHIFT Cobalt Strike MECHANICAL SetWindowsHookE
T1041 – Exfiltration Over C2 Channel (Exfiltration) T1567 – Exfiltration Over Web Service (Exfiltration)	Attackers use known public services to stage and exfiltrate data to their servers.	Google Drive GitHub OneDrive DropBox HTTP HTTP POSTS
T1485 – Data Destruction (Impact) T1490 – Inhibit System Recovery (Impact)	Delete or resize shadow volumes.	vssadmin delete shadows /all /quiet vssadmin shadowcopy delete /all /quiet vssadmin resize shadowstorage wbadmin DELETE SYSTEMSTATEBACKUP wbadmin DELETE SYSTEMSTATEBACKUP –deleteoldest wbadmin delete catalog –quiet
T1529 – System Shutdown/ Reboot (Impact)	Modify/disable boot configuration or system recovery.	bcdedit.exe /set {default} recoveryenabled no bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures bcdedit.exe /set {current} safeboot minimal
T1569 – System Services (Execution) T1574 – Hijack Execution/ Flow (Persistence)	System/file hijack.	takeown.exe /f *

Outlook

Despite high-profile ransomware incidents and government/law enforcement attention on ransomware operations and facilitators, there is currently little motive for ransomware operations to cease. Ransomware operators have continued to operate and adapt throughout 2023 and are assessed to focus on continuing to build infrastructure and capabilities around themselves as a one-stop shop, with less reliance on marketplaces and forums. This includes a shift from encryption to data theft that is stolen and held for ransom. Both Cl0p and BianLian operators have been observed conducting attacks in this manner, which makes the attack faster and still gives the threat actors leverage to begin negotiations.

State-backed and cybercriminal APT groups and campaigns usually involve data and systems destruction via wiper malware or exfiltration of sensitive information for espionage and data harvesting campaigns. Optiv's Global Threat Intelligence Center (gTIC) assesses with **High Confidence** that the motivation behind targeting these companies is for strategic economic and political gain by collecting sensitive information or outright disrupting or destroying information technology and operational technology (IT/OT) systems.

The gTIC assesses with **High Confidence** that both cybercriminal and state-sponsored groups will continue to leverage known vulnerabilities in popular software and services that provide elevated privileges and access to sensitive data. Many of these tools and exploits have been in use for years and are usually available on open-source repositories and forums. The techniques will **Likely** continue to rely on internal risks that may not have been known or remediated by the victim organization. Enabling multifactor authentication (MFA), enforcing a least-privilege user policy, and leaving ports and

services (e.g., Remote Desktop Protocol [RDP], Server Message Block [SMB], Universal Plug and Play [UPnP]) exposed and insecure allow easy access from simple brute-force and credential guessing.

Optiv's gTIC assesses with **Moderate Confidence** that state-sponsored adversaries will increase the use of destructive wiper malware and ransomware as part of their campaigns over the next 12 months. Although the overall probability of a targeted state-sponsored attack across all verticals and organizations is **Unlikely**, the industrials vertical and sub-verticals have a historical record of being targeted by state-sponsored APT groups.

Geopolitics is one of the main driving factors of APT activity. As countries continue to have conflict and search for ways to make economic advancements, APT activity will **Likely** continue over the next 12 months. APT groups are observed to employ what Optiv's gTIC refers to as a "weakest-link" approach to reconnaissance and initial access in most campaigns. These include using opportunistic phishing campaigns with malicious Microsoft Office attachments or links distributed to multiple organizations and potential victims, as well as the exploitation of older (2+ year-old) vulnerabilities in popular public-facing software and services like VPN clients, RDP, Microsoft Exchange, and Oracle WebLogic. It is **Likely** that APT and ransomware groups will continue to target the industrials vertical and sub-verticals over the next 12 months.

Want to learn more?

Visit **optiv.com**

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com

Secure greatness®

Optiv is the cyber advisory and solutions leader, delivering strategic and technical expertise to nearly 6,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential. For more information, visit www.optiv.com.