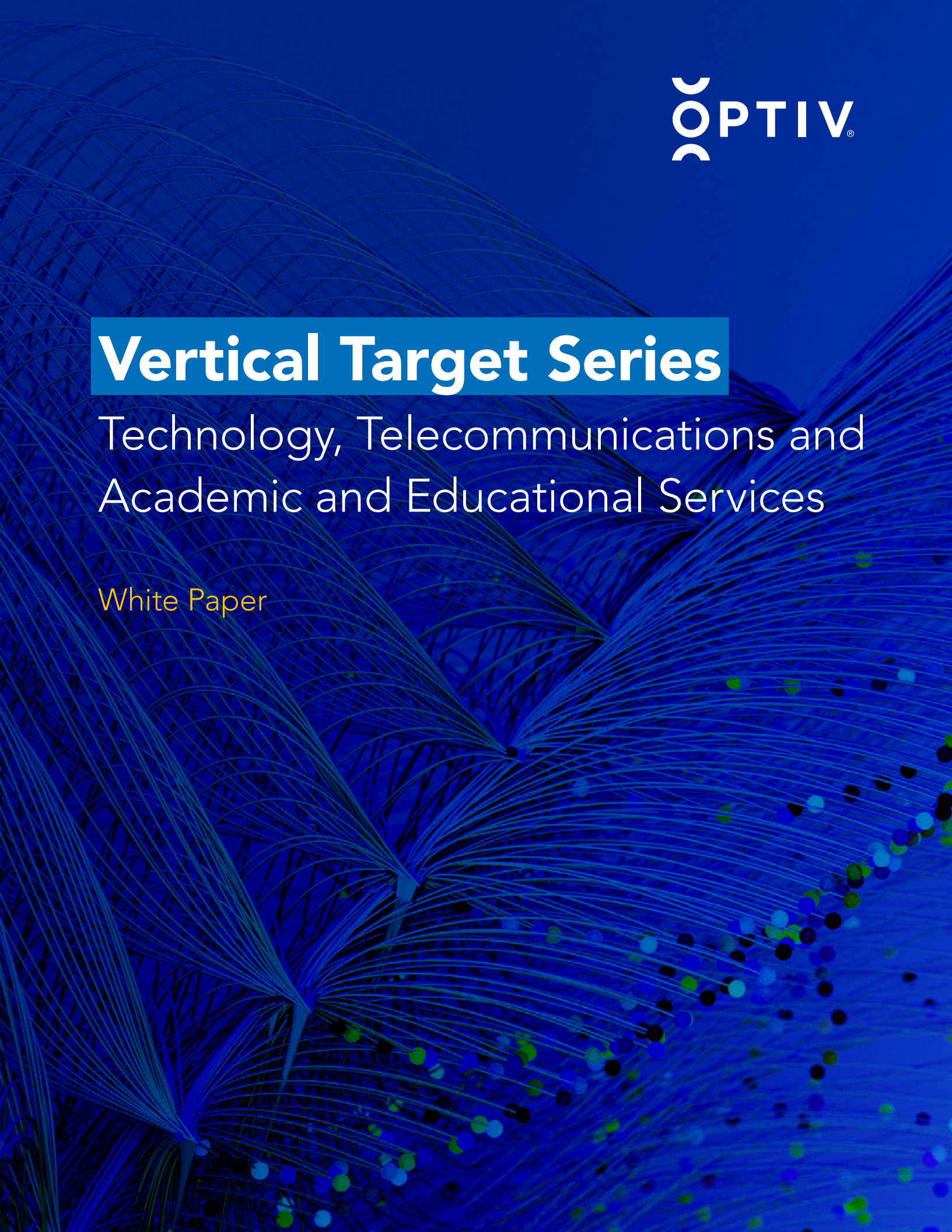

Vertical Target Series

Technology, Telecommunications and Academic and Educational Services

White Paper

Critical infrastructure verticals such as technology and telecommunications, as well as academic and educational services, are attractive targets for cybercriminals and advance persistent threat (APT) groups. These organizations, such as IT services, fintech, universities, professional education institutes, and more, are often targeted by both cybercriminals and APT groups due to the sensitive data these organizations maintain that could help other government bodies. Targeting organizations within these verticals could also lead to potentially negative societal impacts, including the privacy compromise of minors in the education system, as well as the decline of political and economic confidence. Reputational consequences could result from a significant disruption or destruction of availability and integrity of organizations in these verticals. Ransomware operators frequently target these verticals because these organizations have valuable information, including the personally identifiable information (PII) of minors, parents, and staff, connections to other organizations that can be exploited in a supply chain attack, and the inability for these types of organizations to have a significant amount of downtime. Therefore, these actors are more **Likely** to receive a ransom payment. While outside threats are concerning and often make headlines, organizations also face the risk of insider threats. This white paper focuses on the threat actors assessed to pose the biggest threat to technology, telecommunications, and education entities.

An APT group is a malicious actor who is believed to possess significant and dynamic skills, have virtually unlimited resources, and conduct highly targeted attacks. APT groups have more strategic intentions and often aim to gain initial access and remain undetected for long 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 includes data that would be of strategic interest to foreign governments and larger strategic organizations. APT groups have a significant history of targeting education, technology, and telecommunication organizations to collect sensitive information that could be used to gain a strategic advantage for their governments. There are known exceptions in which APT groups also carry out blatant destructive attacks using data and file wiping malware, rather than data exfiltration. The overall intent of APT groups is strategic, rather than financially driven.

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 (legitimate) 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.

Some ransomware programs have been observed by Optiv's gTIC to not only offer ransomware payloads, but also unique stealer malware to siphon off data from victims and directly host them onto the leak page without deploying any encrypting (i.e., ransomware) malware. While some government-sponsored APT groups have been observed deploying ransomware, such as APT10 and APT41, ransomware operators conduct these attacks for the purposes of financial gain.

This white paper leverages the Adversary Risk Matrix developed by Optiv's Global Threat Intelligence Center (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 matrix considers known and assessed non-technical capabilities and intentions.

Table of Contents

Technology

The technology vertical includes technology equipment, software and IT services, and financial technology and infrastructure. Technology organizations are a frequent target for threat actors—including both cybercriminal and APT groups—due to the valuable data they contain including PII and intellectual property (IP). Technology organizations hold sensitive information, such as personal data, personal and corporate card data, access credentials. Technology organizations often hold sensitive data related to the latest technology solutions and research data, and they often take the most risks when using new and cutting-edge technology. IP theft can allow other nations or organizations to develop a competing product, identify vulnerabilities that could be exploited, or enhance their own products without requiring the necessary research and development costs. Technology organizations often have large attack surfaces due to the organizations' use of several different software/solutions, platforms, OS, and smartphones. Additionally, technology companies, including MSSPs and service providers, typically have access to client environments—making technology companies an attractive target for supply chain attacks. Threat actors could gain access to hundreds or thousands of organizations as a result of a single intrusion.

State-backed APT groups and campaigns, particularly from China are the most prevalent threat actors targeting and impacting technology companies with operations and interests in the U.S., Western Europe, Japan, South Korea, and Singapore. The type of information that these organizations host, the impact a cyberattack would have on the organization and the economy, and the ability to gain access to other organizations in a supply chain attack make the technology vertical an attractive target for APT groups worldwide. Three of the APT groups observed targeting the technology vertical include APT39 (Chafer, Cobalt Hickman, Radio Serpens, Remix Kitten), Lazarus Group (Labyrinth Chollima, Zinc, Hidden Cobra, Diamond Sleet), and Volt Typhoon (Bronze Silhouette, Vanguard Panda).

APT41

APT41 is a Chinese state-affiliated threat group that has been active since at least 2012. The group conducts cyber-espionage activity, likely in support of the interests of the Chinese government—particularly the Ministry of State Security (MSS)—as well as financially motivated attacks. It is highly likely that APT41 operates out of Chengdu, the capital of China's Sichuan province. Three of the indicted defendants allegedly operated under the guise of the front company Chengdu 404 Network Technology (Chengdu 404). According to the controversial whistleblowing site, Intrusion Truth, the group also reportedly maintains ties with educational institutions in Sichuan, including Sichuan University and Chengdu University of Information Technology, and may use these links for recruitment purposes.

APT41 is notable for conducting both cyber-espionage and financially motivated attacks. An analysis of the group's operational timing revealed that it usually conducts cyber-espionage attacks during the day and switches to financially motivated cybercriminal operations at night. The latter includes ransomware watering hole attacks, and cryptojacking attacks on gaming companies and systems. This dual focus is likely possible because APT41 is believed to work on a contractual basis for the Chinese government, which turns a blind eye to the group's cybercriminal activity so long as Chinese organizations are not targeted. APT41 is considered extremely technically sophisticated, deploying custom malware and exploiting zero-day vulnerabilities in its attacks.

- In 2019, APT41 reportedly exfiltrated hundreds of GB of data while targeting organizations, including blueprints.
- In 2020, APT41 reportedly targeted victims in the gaming industry with the PipeMon malware. The group compromised the victims' build system to trojanize game executables that would be deployed via a supply chain attack.
- In 2021, APT41 reportedly targeted domains via SQL injection to gain initial access to victim networks and deliver a Cobalt Strike beacon to the endpoints. Post-exploitation activities included establishing persistence, credential theft, and reconnaissance.

Lazarus Group

Although first identified in 2014, Lazarus Group has been found to be active as far back as 2007. The group gained notoriety after targeting Sony Pictures Entertainment in 2014. Lazarus Group is alleged to be associated with two spin-off groups, Andariel and Bluenoroff.

Lazarus Group has been linked with operations that use a wide range of TTPs and pursue a range of objectives, including the acquisition of military and political intelligence, disruption, and destruction. The group is linked to a variety of custom-developed malware, including remote access trojans (RATs), keyloggers, downloaders and destructive wipers. Delivery methods used by the group have included watering holes and spear-phishing email operations.

Lazarus Group has always hovered between an APT and cybercriminal group. The group has been attributed with multiple attacks based on the strategic interests of North Korean government. However, the group has also been attributed with multiple financially motivated cyberattacks.

- In 2014, Lazarus Group was attributed with targeting Sony Pictures Entertainment and stealing sensitive data including personal information about employees and their families, email correspondence between employees, information about salaries, unreleased Sony films, and other information.
- In 2018, Lazarus Group was attributed with sending phishing documents via LinkedIn that masqueraded as a legitimate job advert for a role that matched the employees' skills. When the victim downloaded the document, it deployed an information stealing malware.
- In 2022, Lazarus Group was attributed with exploiting CVE-2022-0609 (CVSS 8.8) to gain initial access to multiple organizations, **Likely** with the goal of stealing sensitive information.
- In 2023, Lazarus Group was attributed with conducting a supply chain attack on 3CX using hacking code that had been observed in previous attacks. The group reportedly modified apps so that they executed malicious commands in the background and downloaded malware that allowed them to steal sensitive information from browsers without the user's knowledge.

APT41 (Barium, Wicked Panda)

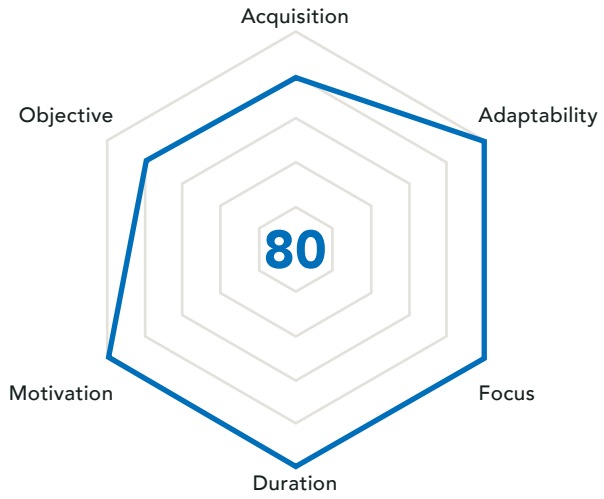

Figure 1: Threat Actor Metric™ for APT41

Lazarus

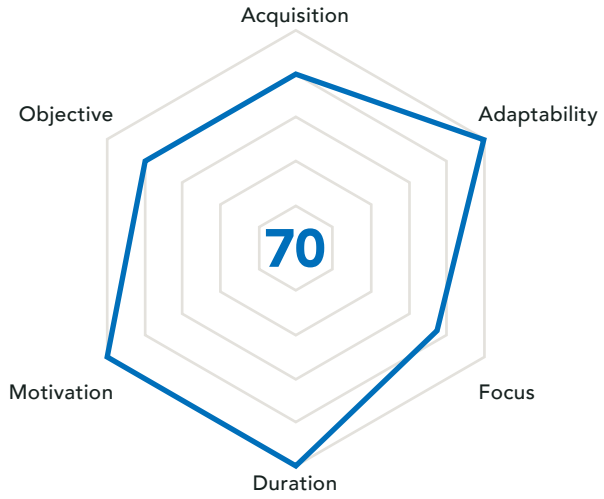

Figure 2: Threat Actor Metric™ for Lazarus Group

Volt Typhoon

Volt Typhoon is an APT group that has been attributed to the Chinese government and has been active since 2021. The group has been observed targeting critical infrastructure organizations in the U.S. and Guam. The group is believed to conduct espionage campaigns and maintain persistent access to victim environments for as long as possible.

Researchers with Microsoft found that Volt Typhoon uses "living-off-the-land (LOTL) techniques and hands-on keyboard activity" and attempts to "blend into normal activity by routing traffic through compromised small office and home office network (SOHO) equipment." Microsoft also found that the group customized open-source tools to establish a C2 channel over proxy.

While the Volt Typhoon group is purported to only have been active since 2021, there is an **Even Chance** that the group has been active for a longer period of time. APT groups attributed to China have been observed sharing infrastructure and tooling, indicating that Volt Typhoon could have been active under another group or moniker prior to 2021.

- In 2023, Volt Typhoon was attributed with exploiting vulnerabilities in Fortinet FortiOS products to gain initial access to victims' environments. The goal of the attacks was to purportedly gather sensitive information that would be of strategic interest to the Chinese government.

Honorable Mention - APT 10

APT10 has been active since at least 2006. MITRE reports that "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 People's Republic of China (PRC) national strategic goals and focuses 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. According to Mandiant, "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."

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 to 24 months.

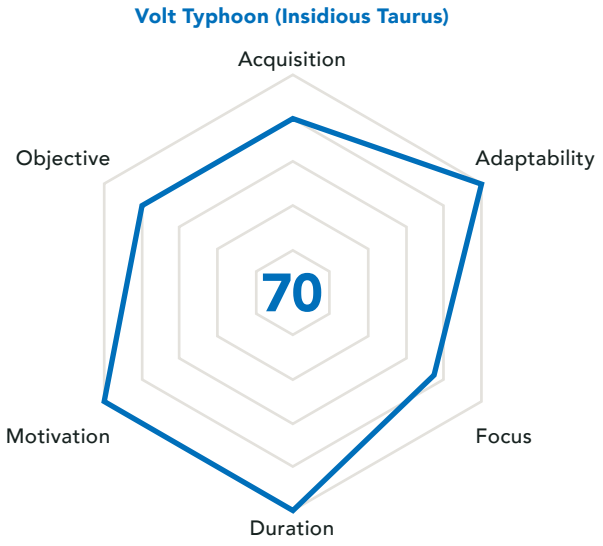

Figure 3: Threat Actor Metric™ for Volt Typhoon

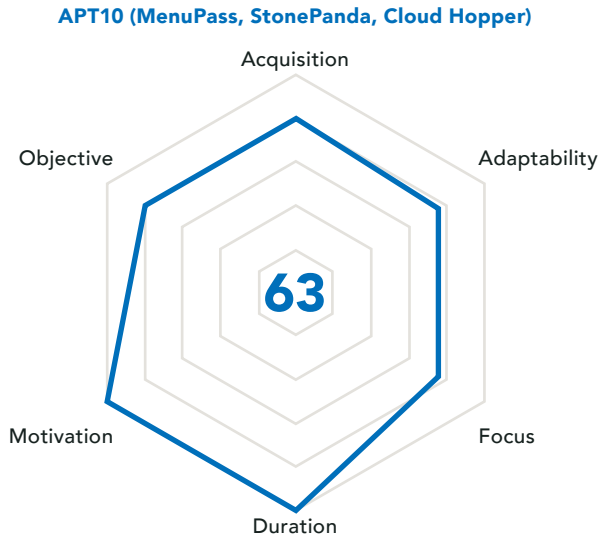

Figure 4: Threat Actor Metric™ for APT10

- In 2017, APT10 was attributed with accessing victims' networks through global service providers. The group used DLL hijacking/DLL side-loading techniques to run payloads in memory, as well as process hollowing techniques to remove and replace code in an executable file with malicious code.
- From 2017 to 2018, APT10 was attributed with using stolen administrative credentials to access Citrix and LogMeIn remote access software before deploying the UPPERCUT and Trochilus malware variants.
- From 2019 to 2021, APT10 was attributed with exploiting the ZeroLogon vulnerability, CVE-2020-1472 (CVSS 10), and conducting DLL side-loading techniques to target Japan-based organizations. The group was observed deploying the Hartip malware.

Ransomware Groups with Technology Targets

In a comparison of data from Q3 2022 through Q2 2023 to Q4 2022 through Q3 2023, ransomware targeting of the technology vertical increased nearly 19%. Technology organizations can be targeted in ransomware supply chain attacks—similar to Clop's targeting of MOVEit and GoAnywhere vulnerabilities in 2023—to target hundreds to thousands of organizations as a result of a single intrusion. It is **Likely** that ransomware groups will continue to target technology organizations over the next 12 months and include a double extortion tactic of stealing sensitive data. The type of data often stolen includes employee data, financial data, human resources data, and client data and will **Likely** remain the target of data exfiltration over the next 12 months.

LockBit

Researchers with *The Hacker News* found that "LockBit ransomware was first discovered in September 2019 and was previously known as ABCD ransomware because of the '.abcd virus' extension first observed." Operating as a RaaS model, LockBit affiliates can earn "a share as high as 75%" and "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, nor will they work with English-speaking developers unless a Russian-speaking 'guarantor' vouches for them."

In July 2022, LockBit released LockBit 3.0 after security vulnerabilities were identified in LockBit 2.0. The new variant was announced on the Russian-language cybercriminal forum XSS. Along with improvements to the variant, the group announced a bug bounty program. The program offered rewards of E1,000 and above for personal identifiable information on sensitive targets, security exploits found, and more.

In September 2022, a disgruntled developer leaked the builder for LockBit 3.0. However, LockBit has continued their operations and did not seem to be severely impacted due to the leak.

Of the 1,012 victims listed on the LockBit data leak site from January 1, 2023 - December 15, 2023, 83 of them (8.2%) are in the technology vertical.

- In 2023, LockBit named Ion Group, a Dublin-based software company, on their data leak site. The cyberattack affected Ion's Cleared Derivatives division, which provides software for automating the trading lifecycle and the derivatives clearing process. The full impact of the ransomware attack remains unknown.
- In 2023, LockBit named Precision Group, an IT solutions company, on their data leak site. The group claimed to have stolen 21.32GB of data from the organization. The listing on the data leak site maintains two screenshots, including a "What We Do" page and a "Representative Client List."
- In 2023, LockBit named PicoSoft Software on their data leak site and claimed to have stolen 6.77Gb of data from the organization. The listing included 14 screenshots of purported data, including passports, financial spreadsheets, and invoices.

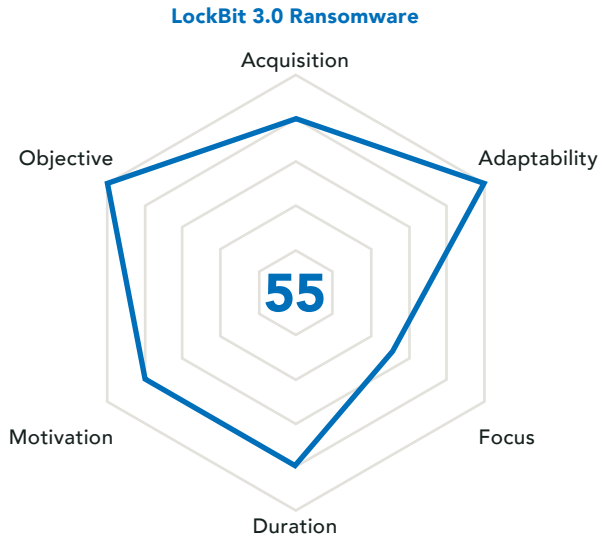

Figure 5: Threat Actor Metric™ for LockBit 3.0 Ransomware

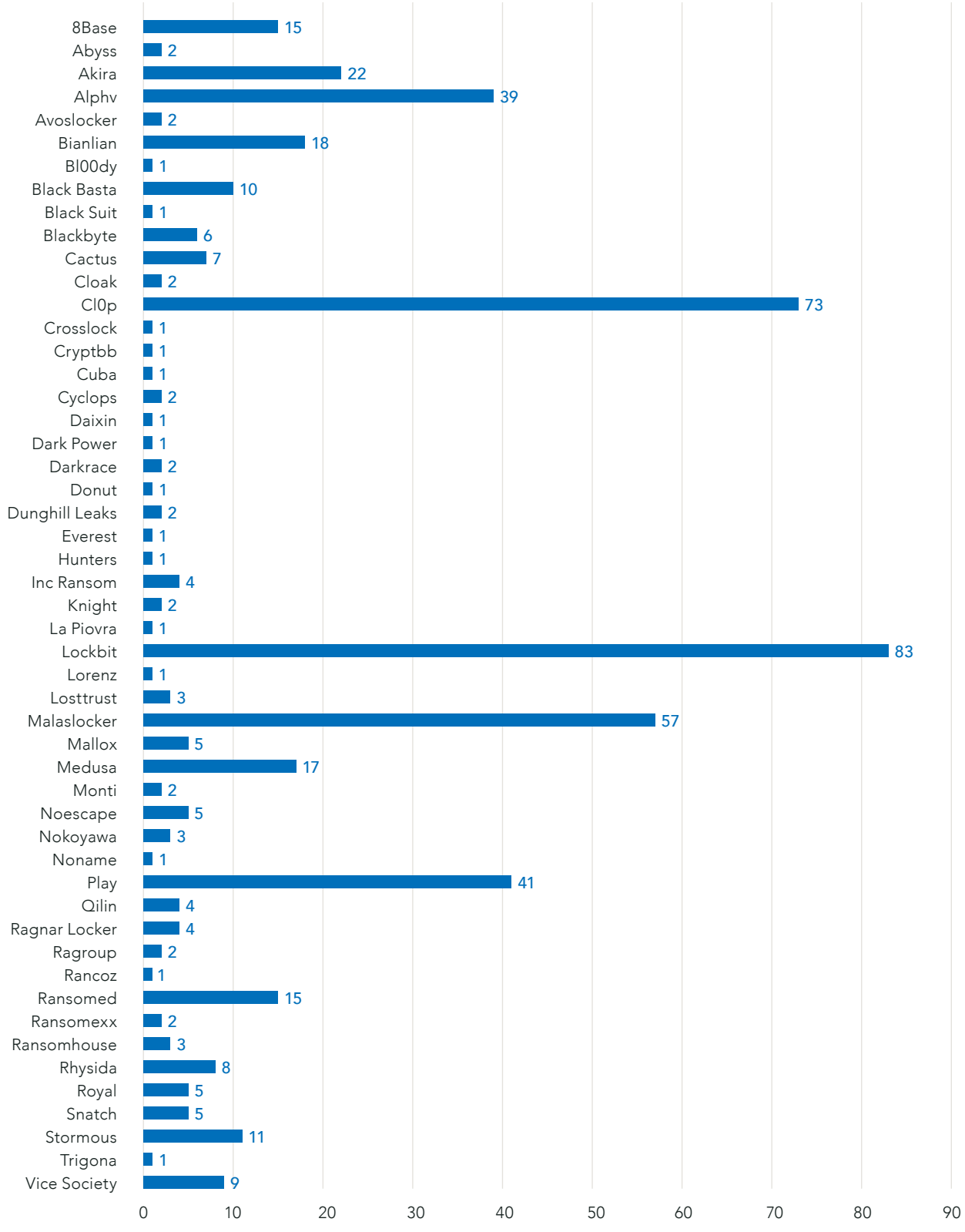

Figure 6: Technology victims listed on data leak sites from January 1, 2023 – December 15, 2023

Cl0p

Clop is a ransomware variant first discovered in February 2019 and is an updated version of the CryptoMix ransomware from 2016. The Clop ransomware has been updated multiple times since it was first identified. In March 2019, the variant was updated to disable services for Microsoft Exchange, Microsoft SQL Server, MySQL, and BackupExec. Clop is a RaaS operation, and therefore the initial access vectors vary depending on the affiliate. Methods observed include phishing attacks, exploiting vulnerabilities, weak passwords, and exposed RDP.

Clop ransomware operators manage the dark-website >_CLOP^_-LEAKS, where they leak victims' data if the ransom demand is not met. Ransom notes indicate that the ransom demand amount depends on how quickly the victim organization contacts the operators. In Q1 2023, Clop 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. The organizations that did not pay were leaked on the Clop data leak site. This attack resulted in Clop being more active in Q1 2023 than the group was in all of 2022. Additionally, this attack was similar to the Clop attack targeting Accellion FTA vulnerabilities in 2021.

Of the 384 victims listed on the Clop data leak site from January 1, 2023 - December 15, 2023, 73 of them (19%) are in the technology vertical.

- In March 2023, Clop listed 14 technology organizations located around the world that were reportedly targeted via a vulnerability in the GoAnywhere MFT secure file transfer tool. The group did not encrypt the victim networks in the attack and stole data to hold for ransom. The data included financial data and source code.
- In June 2023, Clop listed 52 global technology organizations that were targeted by exploiting a vulnerability in MOVEit Transfer MFT. The group did not encrypt victim networks in this attack and stole data to hold for ransom. The information included business plans, employee information, source code, and more.

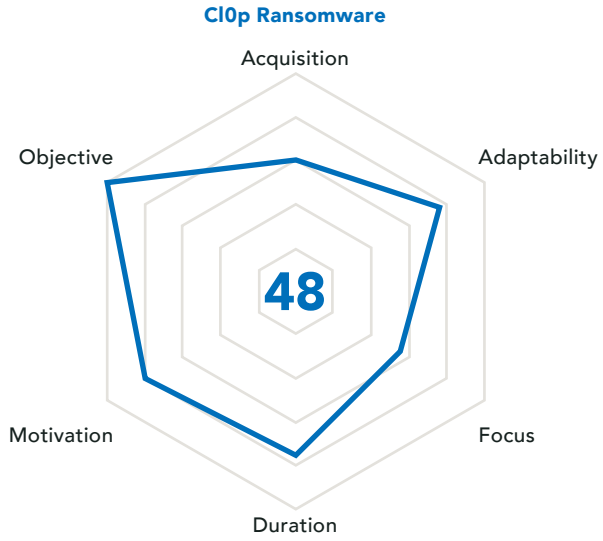

Figure 7: Threat Actor Metric™ for Cl0p Ransomware

MalasLocker

The MalasLocker ransomware operation was first observed in April 2023. The group participates in double extortion methods and maintains a data leak site where victim's information is leaked if the ransom is not paid. The group claims to show disdain for corporations and socio-economic inequality. Rather than demand a ransom like other operations, the group claims that they will provide a decryption key to victim organizations that donate to a MalasLocker-approved charity.

The operators target Zimbra servers and upload suspicious JSP files to specific directories. The initial access vector is not known at the time of writing.

Unlike other ransomware operations, 30% of the group's victims are located in Russia. Moreover, the fact that the group requires donations rather than payment could indicate that the group is politically motivated, rather than financially motivated.

Of the 171 victims listed on the MalasLocker data leak site from January 1, 2023 - December 15, 2023, 57 of them (33%) are in the technology vertical.

- In May 2023, MalasLocker named 49 technology organizations (excluding telecommunications companies) on their data leak site. The posts included a .txt file of purportedly encrypted files. The posts did not appear to contain any screenshots of the purported data or the victim environment.

Play

Play (aka PlayCrypt) 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 with Trend Micro have discovered that Play's tactics are similar to the Hive and Nokoyawa ransomware operations, "including similarities in the file names and file paths of their tools and payloads." These researchers also found connections between Play and Quantum ransomware operations. Play ransomware is Microsoft Visual C++ based and contains several anti-debugging and anti-analysis features to slow investigations into the malware. The payload includes garbage code – code that serves no useful purpose – and function returns that drive execution into a dead end.

In November 2023, security researchers with Adlumin reported that Play ransomware was being sold as a service. Due to nearly identical TTPs leveraged in multiple Play ransomware attack, the researchers concluded that the affiliates were **Likely** using a purchased RaaS variant and following the associated playbooks.

Of the 293 victims listed on the Play data leak site from January 1, 2023 - December 15, 2023, 41 of them (13.9%) are in the technology vertical.

- In June 2023, Play ransomware named the Swiss IT company, Xplain, on their data leak site. The organization released a statement that they did not make contact with the group and would not pay the ransom. The post on Play's data leak site included one download link and a RAR password, and the group alleged to have stolen 907GB of data.
- In August 2023, security researchers reported that Play ransomware operators had been observed sending phishing emails to gain access to MSPs. The purported goal of targeting MSPs is to deploy ransomware to the MSPs' "downstream customers."

Alphv

Alphv (aka BlackCat) is a RaaS variant that has been active since at least November 2021. Affiliates are often recruited through Russian-speaking cybercriminal forums. Alphv operators have been linked to the BlackMatter and DarkSide ransomware operations, However, it is not known if the group is a rebrand of the BlackMatter ransomware or a former affiliate that has started their own operation.

In February 2023, Alphv announced the release of a new variant, dubbed Sphynx. Researchers with the IBM Security X-Force Team reported that the command-line arguments were "reworked," which Alphv denied. Affiliates of the group have been observed targeting Veeam backup software to steal credentials. Initial access vectors include compromised RDP, phishing attacks, stolen credentials, and exploiting known vulnerabilities.

In December 2023, law enforcement agencies from the U.K., Denmark, Germany, Spain, the U.S., and Australia conducted an operation that led to the disruption and seizure of the Alphv data leak site. Additionally, the FBI released a decryption tool that enabled more than 500 victims to restore their systems. However, that same day, the Alphv group reportedly "unseized" the data leak site. They left a message that the law enforcement operation only took down a single domain controller and that the group was able to create a new site to continue operations.

The message left by the group indicated that the group will now allow any affiliates to target any organization outside any CIS countries, where previously the group did not allow the targeting of hospitals or certain critical infrastructure organizations. Additionally, the group stated they would no longer allow discounts for ransom payments. It is not known if the group plans to stick to the new rules or if they are an initial reaction to the disruption.

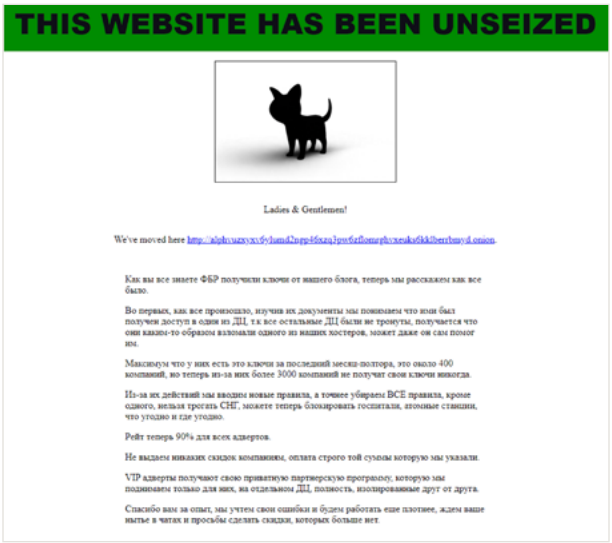

Figure 8: Alphv data leak site claiming it had been "unseized"

Of the 418 victims listed on the Alphv data leak site from January 1, 2023 0 December 15, 2023, 39 of them (9.3%) are in the technology vertical.

- In April 2023, Alphv ransomware named Axure Software Solutions on their data leak site and claimed to have stolen sensitive data. The group claimed to have accessed personal data, banking and financial records, product source codes, and databases. It is not known if the company paid the ransom demand.
- In May 2023, Alphv named Constellation Software to their data leak site and claimed to have access to 1TB of company data. It is not known if the company paid the ransom and since the original Alphv site was taken down, it is not known if the company is still listed.
- In November 2023, Alphv ransomware named Dragos on their data leak site. The group did not list any data, but they stated that Dragos had 24 hours to make contact with the group in order to avoid the data being leaked. However, Dragos reported that there was no evidence of a data breach or a successful attack. Ransomware operators, including RansomedVC, have previously made false claims related to targeting cybersecurity and technology organizations.
  - » In May 2023, Dragos confirmed that an unnamed ransomware attacker had accessed SharePoint and content management system resources. However, the attack failed, and the ransomware was not deployed. It is not known if Alphv was related to that attack.

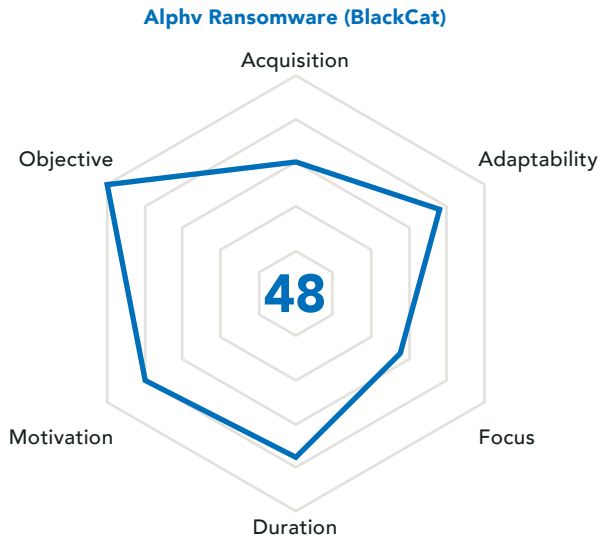

Figure 7: Threat Actor Metric™ for Alphv Ransomware

Telecommunications

The telecommunications vertical has been increasingly targeted by threat actors. This is likely because people use a growing number of mobile devices to store and process both personal and corporate data, as well as activate multi-factor authentication. This vertical includes both internet and cellular service providers, and the vertical plays a critical role in facilitating global communications. As organizations become more connected, it is **Likely** that threat actors will continue to target organizations within this vertical. Telecommunications organizations are often targeted for espionage attacks, technology theft, and data harvesting campaigns. Three of the APT groups observed targeting the telecommunications vertical are APT34 (aka Europium, Hazel Sandstorm, OilRig, Chrysene), APT27 (aka Budworm, Emissary Panda, Threat Group-3390, LuckyMouse), and APT39 (aka Chafer, Cobalt Hickman, Radio Serpens, Remix Kitten).

APT34

APT34 (aka OilRig, Helix Kitten) is an Iranian state-associated threat group that has been in operation since at least 2014. However, attacks attributed to them date back to 2012. The group has targeted several organizations and is most commonly known for sophisticated social engineering scams designed to enable initial access. The group's motivation is believed to be establishing access to target networks that can be used at a later date, conduct supply chain compromise, and move laterally to other targets. APT34 has also been associated with destructive wiper attacks against the energy and ICS industries. APT34 relies on stolen account credentials for lateral movement.

A breach of APT34 associated infrastructure in 2019 revealed the group's organizational structure, toolset, and victim base. Also revealed were aliases of some of the individuals known to be working for the group, which included personnel associated to Iran's Ministry of Intelligence—with several also known to be employees of Iranian cybersecurity company Rahacorp. This was not the first compromise of APT34's infrastructure, as 2019 reports found that the Russian actor, Turla (aka Venomous Bear, Waterbug) compromised APT34's infrastructure in 2017. Turla utilized this intrusion to drop malware on infrastructure owned by APT34, and also on networks known to be previously compromised by APT34. APT34 reportedly did not detect this activity.

- In 2020, APT34 reportedly targeted an organization in the Middle East with the RDAT malware. The attacker's goal was purportedly to maintain persistent access and steal sensitive information.
- In 2022, APT34 reportedly targeted organizations worldwide by using MrPerfectInstaller to drop a backdoor malware and exfiltrate stolen data.
- In 2023, APT34 was attributed with phishing attacks targeting organizations in the Middle East to deploy the Menorah malware. The group's goal was to reportedly steal sensitive information.

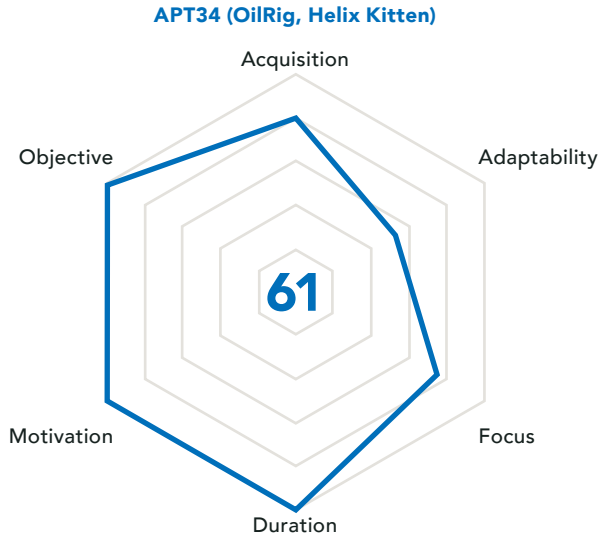

Figure 10: Threat Actor Metric™ for APT33

APT27

APT27 is a Chinese group that has been active since at least 2015. The group has historically focused on Western targets in cyber-espionage operations. APT27 has targeted a national data center in Central Asia, likely to conduct nationwide watering hole attacks. APT27 has also installed web shells on SharePoint servers to compromise targeted organizations. APT27 uses spear-phishing emails to gain initial access to targets before harvesting account credentials, escalating privileges, and deploying web shells.

- In 2023, APT27 reportedly used an updated version of SysUpdate to target organizations with the intent of stealing sensitive information, including harvesting credentials. The group used living-off-the-land (LOTL) techniques to evade detection.

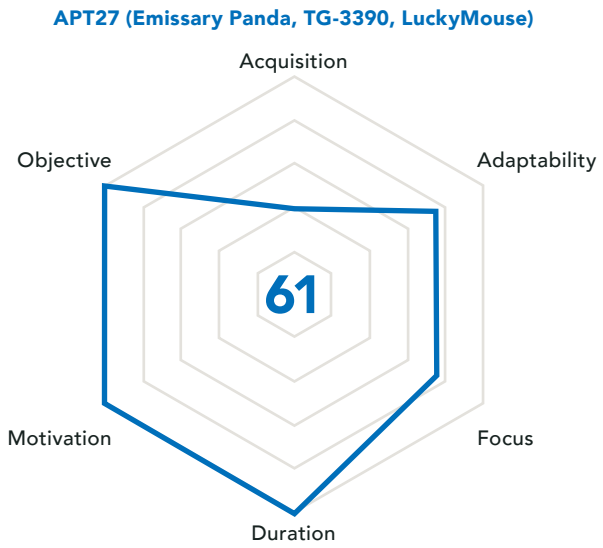

Figure 11: Threat Actor Metric™ for APT27

APT39

According to MITRE, "APT39 is one of several names for cyber-espionage activity by the Iranian Ministry of Intelligence and Security (MOIS) through the front company Rana Intelligence Computing since at least 2014." Mandiant further writes that "APT39's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns."

- In 2017, APT39 reportedly used malicious Excel documents to deliver malware to multiple organizations with the goal of gathering sensitive information.
- From 2018 - 2019, APT39 was attributed with cyberattacks targeting organizations to gather personal information. APT39 **Likely** targets personal information to aid Iranian state operations. Additionally, the group can use the victims' personal information to execute social engineering and impersonation tactics.

Sandman

Sandman is an APT group that was first discovered in August 2023, but malware development indicates the threat actor has been active since 2022. The group was observed targeting telecommunications providers in the Middle East, Europe, and South Asia. Researchers with SentinelLabs argue that the group has focused on "strategic lateral movements and minimal engagements, likely to minimize the risk of detection."

The group has not been attributed to a specific location. According to SentinelLabs, "While the development style is historically associated with a specific type of advanced threat actor, inconsistencies between the high-end development of the malware and poor segmentation practices lead us towards the possibility of a private contractor or mercenary group."

- In 2023, Sandman was attributed with the targeting of organizations in Africa, Asia, and Europe with the LuaDream malware to collect sensitive information.
- In 2023, Sandman was attributed with targeting organizations with the LuaDream and KEYPLUG malware variants with the goal of stealing sensitive information.

Honorable Mentions - Volatile Cedar

Volatile Cedar (aka Lebanese Cedar) is a Lebanese-linked APT group that has been active since at least 2012. The attackers rely on locating exploitable vulnerabilities in the target's public facing web servers before injecting a web shell code. They then inject their custom 'Explosive' malware so that they can compromise victims' servers and access credentials.

- In 2025, Volatile Cedar was attributed with the targeting of hundreds of organizations with the Explosive malware variant with the intent of collecting sensitive information.
- In 2020, Volatile Cedar was attributed with the exploitation of CVE-2012-3152 (CVSS 6.4) in Oracle Fusion Middleware to gain initial access to multiple organizations. The group deployed both the Explosive and Caterpillar malware variants with the intention to steal sensitive information.

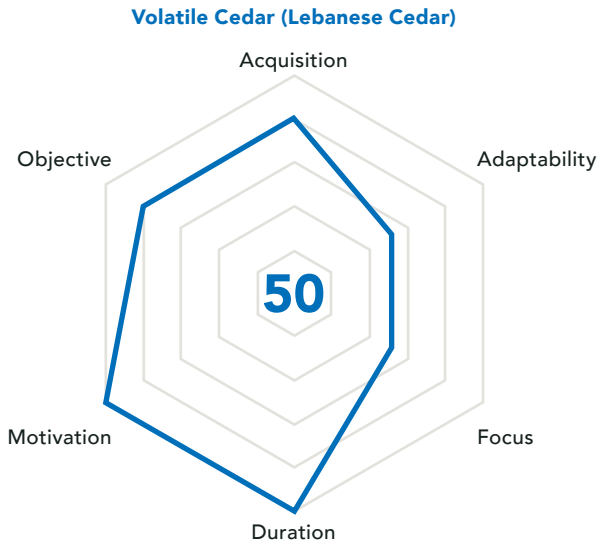

Figure 12: Threat Actor Metric™ for Volatile Cedar

LightBasin

LightBasin is a Likely state-sponsored threat actor, attributed to China, that has been observed targeting the telecommunications vertical since 2017. The group is known to use custom tools and their knowledge of telecommunications protocols and architecture to launch successful attacks. According to CrowdStrike, LightBasin has been observed "leveraging external DNS (eDNS) servers…to connect directly to and from other compromised telecommunications companies' General Packet Radio Service (GPRS) network."

- In October 2021, LightBasin was observed targeting telecommunications companies worldwide in a campaign designed to collect information. CrowdStrike reported that "LightBasin deployed their SLAPSTICK PAM backdoor on the systems to siphon credentials." LightBasin then elevated privileges and deployed additional malware, including TinyShell and SIGTRANslator, to steal data that would be of interest to intelligence organizations.

Ransomware Groups with Telecommunications Targets

While the overall number of ransomware attacks and targeting the telecommunications vertical is lower than most others, telecommunications organizations do remain attractive targets for multiple groups. In a comparison of data from Q3 2022 - Q2 2023 to Q4 2022 - Q3 2023, ransomware targeting of the telecommunications vertical increased nearly 20%. Telecommunications organizations maintain sensitive PII that would be of interest to threat actors attempting to extort the organizations, including names, addresses, email addresses, payment data, and more. Not only can this data be used to extort the company, but it would be of value to many other threat actors willing to purchase the data to use in future malicious attacks. It is **Likely** that ransomware groups will continue to target telecommunications organizations over the next 12 months.

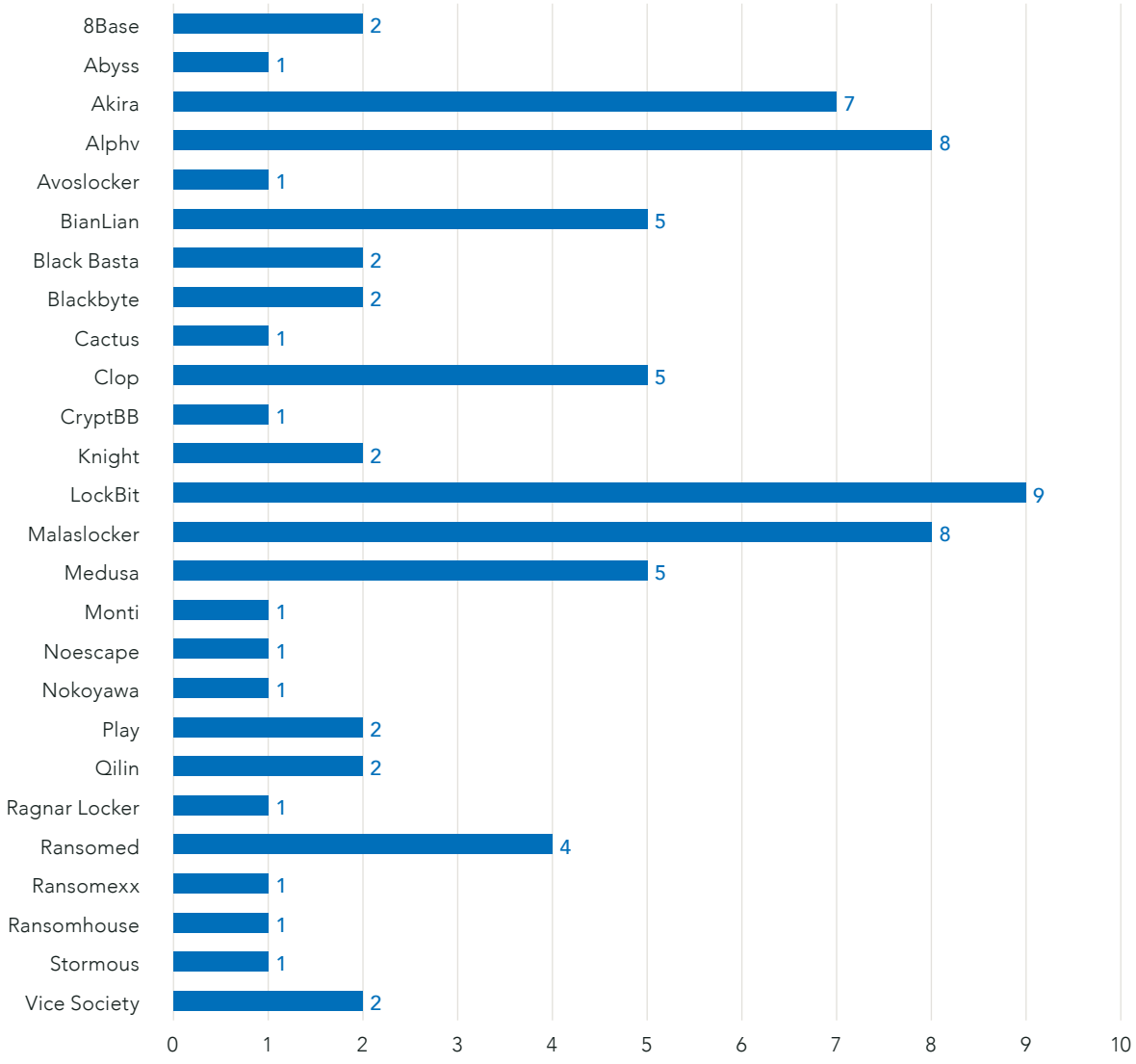

Figure 13: Telecommunications victims named on data leak sites from January 1, 2023 – December 15, 2023

LockBit

Of the 1,012 victims listed on the LockBit data leak site from January 1, 2023 - December 15, 2023, 9 of them (0.9%) are in the telecommunications vertical.

- In July 2023, LockBit named HGC Global Communications on their data leak site and claimed to have stolen sensitive data. The post stated, "change the negotiator." Documents claiming to include company financial data, employee information, and more were posted on August 3, 2023.
  - » On August 04, 2023, HGC Global Communications posted a statement that, after analyzing the leaked documents, the company did not believe the compromise was related to their organization and was likely another organization. Additionally, they stated that an attack had not disrupted their daily business operations.
- In October 2023, LockBit claimed to have targeted Tata Tele Business Services and named them on their data leak site. The group threatened to leak the stolen data if the company did not pay the ransom demand. On October 14, 2023, the group posted 17 images of the breached data that purportedly included financial data and confidential correspondence.
  - » On October 15, 2023, security researchers with CloudSEK determined that the leaked data was not related to Tata Tele Business Services, but rather an India-based real estate company.

Alphv

Of the 418 victims listed on the Alphv data leak site from January 1, 2023 - December 15, 2023, 8 of them (1.9%) are in the telecommunications vertical.

- In May 2023, Alphv named KDDI Indonesia on their data leak site and claimed to have stolen data from the organization. The group attached 34 screenshots to the post and stated that the data included employee personal data, financial and accounting data, passports, and more. It is not known if a ransom payment was made.
- In October 2023, Alphv named Innovattel LLC on their data leak site. As the original Alphv site was seized, it is not known if the company is still listed or if they removed due to negotiations or ransom payment.

MalasLocker

Of the 171 victims listed on the MalasLocker data leak site from January 1, 2023 - December 15, 2023, 8 of them (4.7%) are in the telecommunications vertical.

- In May 2023, MalasLocker named 8 telecommunications organizations on their data leak site. The posts all appeared to contain a .txt file of the files that were encrypted. It is not known if any of the companies paid a ransom demand.

Akira

Akira is a ransomware variant that was identified in 2017. Analysis of Akira's behaviors resulted in security researchers linking Akira to the leaked Conti ransomware source code. Akira ignores the same file types and directories as Conti and has functions that are similar as well. Security researchers with Arctic Wolf analyzed cryptocurrency transactions related to Akira and Conti and found that in "at least three separate transactions, Akira threat actors sent the full amount of their ransom payment to Conti-affiliated addresses." In June 2023, Avast researchers released a decryptor for Akira ransomware. However, Akira quickly changed the encryption routine since the decryptor was published.

In August 2023, an Akira ransomware variant, Megazord, was identified that Trend Micro argues "appears to be referencing a Power Rangers formation because it encrypts files with the 'POWERRANGES' file extension. The ransom note, which is named 'powerranges.txt,' instructs victims to contact the ransomware actor via TOX messenger."

Of the 170 victims listed on the Akira data leak site from January 1, 2023 - December 15, 2023, 7 of them (4.1%) are in the telecommunications vertical.

- In June 2023, Akira listed GC&E on their data leak site and claimed to have stolen data. While the company was listed in their news section, there is no corresponding leak in their leaks section. It is not known if the company paid the ransom demand or if the data was not leaked for another reason.
- In August 2023, Akira listed Cequint, Inc. on their data leak site and claimed to have stolen 800GB from the organization. The group claimed to have obtained source code, company projects, and financial data. There is no listing in the leaks section, and it is not known if the company paid a ransom demand.

- In December 2023, Akira listed SmartWave Technologies on their data leak site and claimed to have stolen 65GB of data that included confidential personal information, human resources documents, and financial documents. It is not known if the company has paid a ransom demand or entered negotiations with the group.

BianLian

BianLian is a ransomware written in Google's Go programming language. BianLian has been active since at least July 2022. The operators are not as active as some of the more prolific groups, such as LockBit, Alphv, and Black Basta. The operators do participate in double extortion and maintain a data leak site. BianLian uses a custom toolkit, including homemade encryptors and encryption backdoors.

In March 2023, security researchers with [redacted] reported that BianLian has switched tactics from ransoming encrypted files to focus more on data leak extortion. This change is **Likely** due to the decryption tool that was released by Avast in January 2023. The group, similar to other groups, uses tactics – email, phone calls, and general harassment – to put additional pressure on the victims. However, unlike other groups, BianLian operators appear to do extensive research on their victims in order to tailor the threats to the specific victim.

BianLian appears to post the masked data (purported stolen data that is not publicly available to see) on their data leak site within 48 hours of the compromise – compared to other groups that wait 3-21 days.

Of the 194 victims listed on the BianLian data leak site from January 1, 2023 - December 15, 2023, 5 of them (2.6%) are in the telecommunications vertical.

- In April 2023, BianLian named Commerce Pundit on their data leak site and claimed to have stolen 400GB of data. The data reportedly included human resources documents, financial data, and more. The post includes 199 .zip links to purportedly stolen data.
- In August and September 2023, BianLian named two hidden companies on their data leak site. Both have been removed, and it is not known if the ransom demand was paid.
- In September 2023, BianLian named Smartfren Telecom on their data leak site and claimed to have stolen 1.2TB of data from the organization. The group claimed the information included financial data, technical data, and more. The post includes 917 files for download that contain purported stolen data.

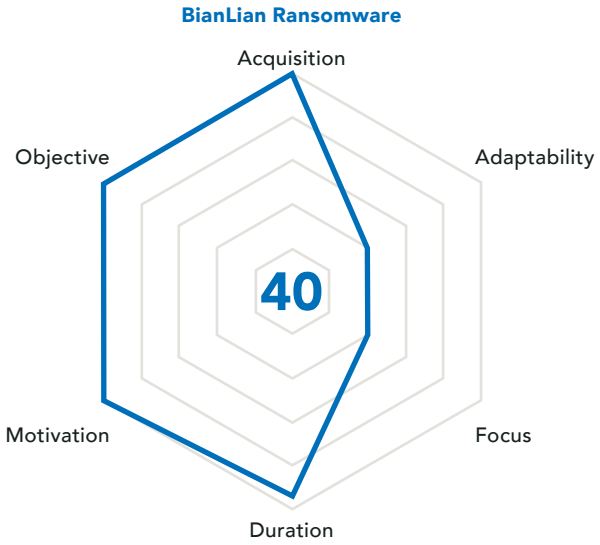

Figure 14: Threat Actor Metric™ for BianLian Ransomware

Academic and Educational Services

The academic and educational services vertical includes public and private school districts, primary and secondary schools, universities, and professional and business education services and providers. Despite many defensive frameworks and policies that academic and educational services institutions have adopted to improve security, institutions in this vertical remain an attractive target for threat actors due to the high-value information and critical nature of these organizations. Often the goal of state-sponsored attacks targeting these organizations is for strategic gain by collecting sensitive intellectual property, such as research or stealing credentials for future malicious activities. Three of the APT groups observed targeting the education vertical are Mustang Panda (aka Bronze President, Camero Dragon, Stately Taurus, TA416), Deep Panda (aka KungFu Pandas, Pink Panther, Shell Crew), Earth Lusca (aka Aquatic Panda, Bronze University, Charcoal Typhoon, Chromium).

Mustang Panda

Mustang Panda (aka Bronze President, HoneyMyte, TEMP.Hex) is a China-linked APT group that has been active since at least 2014. The group is notable for their social engineering attacks using lure documents related to current global events, including the Russia-Ukraine war, COVID-19, and human rights conditions in China. Mustang Panda is known for using both open-source and custom malware variants.

- In 2022, Mustang Panda was attributed with launching spear-phishing attacks to target organizations. The phishing emails included embedded links that victims could click to download the custom malware.

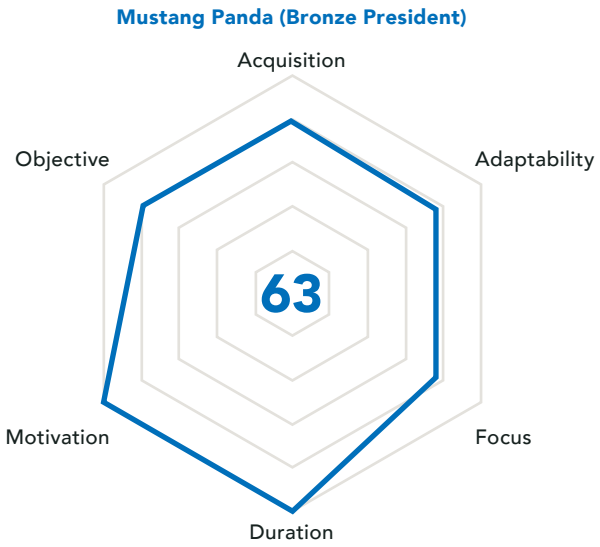

Figure 15: Threat Actor Metric™ for Mustang Panda

Deep Panda

Deep Panda (aka Black Vine, Shell Crew, KungFu Kitten, PinkPanther, WebMasters) is a Chinese threat group that has likely been active since at least 2011. The group is known for conducting persistent, politically motivated cyber-espionage campaigns against high-profile targets, but it has not been directly attributed to the Chinese government. It is likely that the group also conducts intellectual property theft. Deep Panda has previously been linked to Topsec, a Chinese cybersecurity research company.

From 2017-2022, Deep Panda's publicly known activity decreased significantly. However, in March 2022, the group was linked to a widespread phishing campaign. The campaign reportedly exploited the Log4Shell (CVE-2021-44228) vulnerability in VMware Horizon servers to deploy a rootkit called "Fire Chili." The rootkit was allegedly signed using a stolen digital certificate previously deployed by Deep Panda.

Deep Panda is sometimes referred to as "APT19." However, although it is realistically possible that the two groups share certain tools and infrastructure, it is more likely that they are distinct groups. The inconsistency in public reporting means that it is difficult to attribute campaigns to either group with certainty. For example, CrowdStrike initially attributed the 2015 US Office of Personnel Management breach to Deep Panda, but FireEye subsequently countered this claim.

- In 2015, Deep Panda was attributed with compromising a website used to sell software that helps Windows system administrators parse and understand Windows event logs. Deep Panda used the platform to deliver malicious versions of the software to more than 175 organizations.
- In 2022, Deep Panda was attributed with exploiting the Log4Shell vulnerability to gain initial access to vulnerable organizations. The goal of the attacks was to purportedly steal sensitive data by using the Fire Chili rootkit and Milestone backdoor.

Earth Lusca

Discovered in mid-2021 – but believed to be active since 2019 – "Earth Lusca" is a threat group motivated by espionage and financial gain. Trend Micro argues that the group's is primary motivated by cyber espionage, given the group's targets that include "government and educational institutions, religious movements, pro-democracy and human rights [organizations] in Hong Kong, and [COVID-19 research organizations.]" Moreover, according to Trend Micro, "the threat actor also seems to be financially motivated, as it also took aim at gambling and cryptocurrency companies." Trend Micro further notes that Earth Lusca's main attack vectors include spear phishing, watering hole attacks, and vulnerability exploitation.

Earth Lusca has exploited vulnerabilities in public-facing applications, like ProxyShell, which Sophos states "enables an actor to bypass authentication and execute code as a privileged user."

- In 2019, Earth Lusca was attributed with attacks targeting Asian universities using the ShadowPad backdoor. It was assessed that the attacks were Likely to obtain information related to the protests in Hong Kong occurring at the time of the attacks.

Honorable Mention - SparklingGoblin

SparklingGoblin is a suspected Chinese-based APT group related to the Winnti Group – an umbrella group that has been active since 2010. SparklingGoblin mainly targets institutions in the academic and educational services vertical in East and Southeast Asia. However, other targets have been identified in the U.S. and Canada. The activities of SparklingGoblin **Likely** overlap with activities of other Chinese cyberthreat groups and institutions. Observed and analyzed SparklingGoblin payloads suggest the reuse of malware and implants taken from the Equation Group leak from 2017.

- Between 2020 and 2021, SparklingGoblin targeted multiple academic and education services institutions in Hong Kong, Taiwan, Canada, and the U.S. These organizations' respective backdoors communicated with the attackers' C2, which allowed the threat actor to collect information and load plugins.

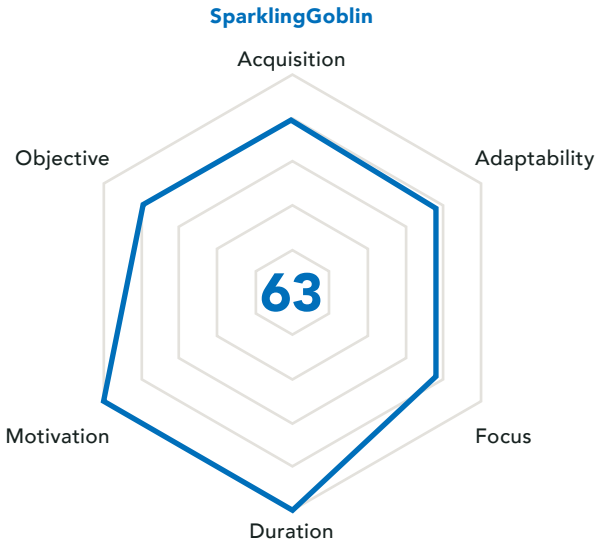

Figure 16: Threat Actor Metric™ for SparklingGoblin

Ransomware Groups with Academic and Educational Services Targets

Academic and educational services organizations remain an attractive target for ransomware victim due to the perception that these institutions are more likely to pay a ransom payment. According to researchers with Sophos, the academic and educational services vertical had one of the highest rates of ransom payment, with over half of higher education victims and 47% of schools (K-12) paying the demand. In a comparison of data from Q3 2022 - Q2 2023 to Q4 2022 - Q3 2023, ransomware targeting of the academic and education services vertical increased nearly 18%. Most schools do not have the profits that some other verticals, such as manufacturing or technology organizations, have. Yet, the sensitive nature of the data that can be stolen makes these institutions a highly visible and attractive target. It is **Likely** that ransomware groups will continue to target academic and educational services organizations over the next 12 months.

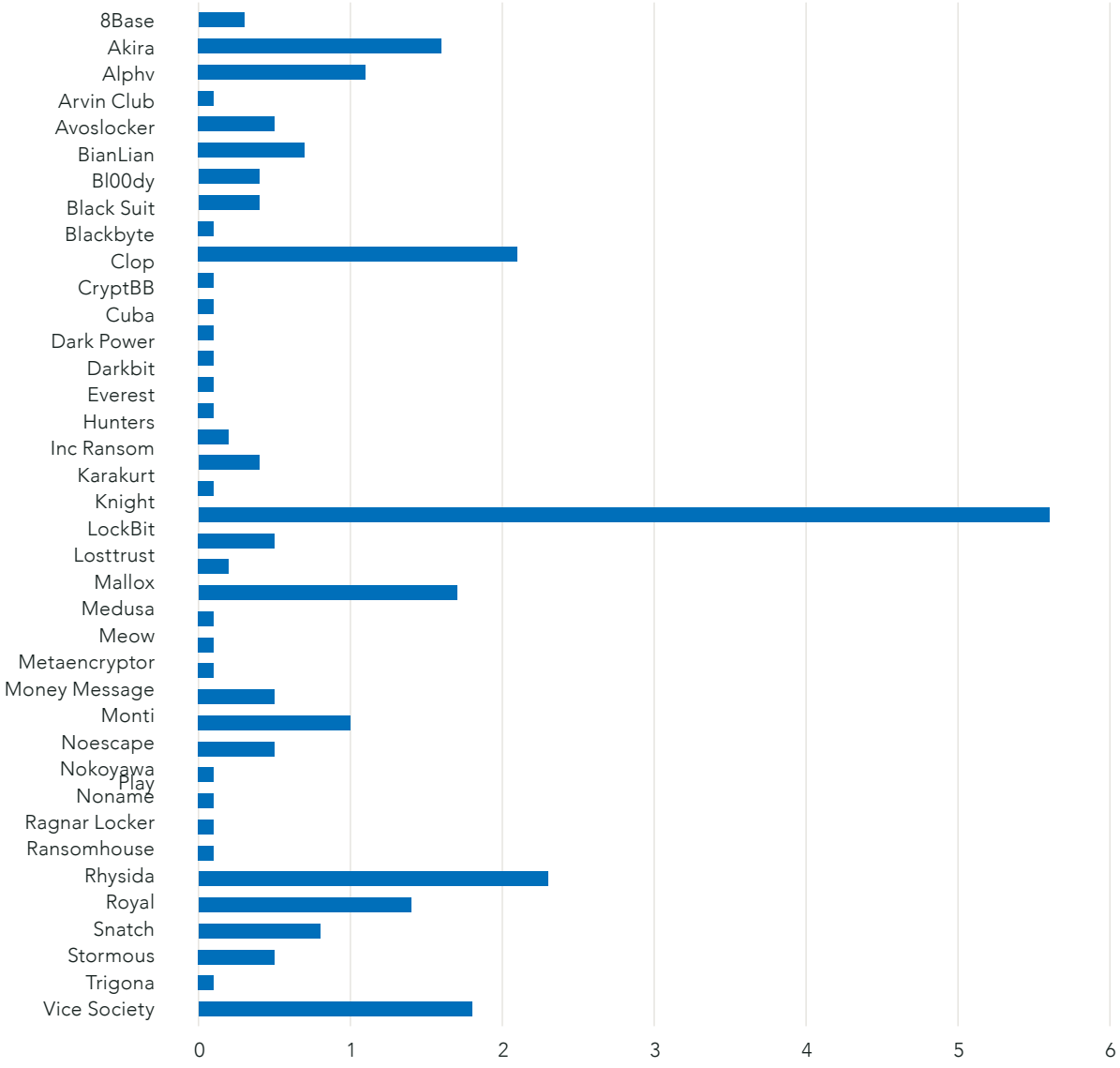

Figure 17: Academic and educational services victims named on data leak sites from January 1, 2023 - 15 December 15, 2023

LockBit

Of the 1,012 victims listed on the LockBit data leak site from January 1, 2023 - December 15, 2023, 56 of them (5.5%) are in the academic and educational services vertical.

- In February 2023, Illinois' Olympia Community Unit School District 16 was targeted in a LockBit ransomware attack. In April 2023, the school was named on LockBit's data leak site and shortly after, LockBit posted an apology to the school district and offered to provide the decryption keys for free. The LockBit leader also stated the affiliate that hit the school had been blocked from the affiliate program with LockBit.
- In April 2023, LockBit named New Jersey's Pinelands Regional School District on their data leak site and claimed to have stolen 64GB of data from the school. The group later added screenshots of purported data that included student and personnel data and directories.
- In September 2023, LockBit named Florida's Hillsborough County Public School and claimed to have stolen 2TB of data. The school superintendent informed the students' parents of the breach and investigation in August 2023.

Rhysida

Rhysida is a RaaS group that was first observed in May 2023 and gained notoriety in May 2023 after launching an attack against the Chilean army. The U.S. Department of Health and Human Services indicates that the name, "Rhysida," refers to the Rhysida Longpipes centipede genus, which is also displayed on their data leak site.

At the time of writing, it is not known how the operators gain initial access. However, it is **Likely** similar to other groups via the use of social engineering, vulnerability exploitations, and initial access brokers.

Of the 73 victims listed on the Rhysida data leak site from January 1, 2023 - December 15, 2023, 23 of them (31.5%) are in the academic and educational services vertical.

- In May 2023, Rhysida targeted Oklahoma's Northeastern State University (NSU) and named the university on their data leak site in June 2023. NSU temporarily disabled their network—preventing students from accessing the school network or accessing electronic grades.
- In July 2023, Rhysida named the University of the West of Scotland on their data leak site and demanded 20 Bitcoin (approximately $44,119) for the decryption key. The group claimed to have accessed personnel data and internal documents.
- In November 2023, Rhysida named Bangkok University on their data leak site and claimed to have stolen 180GB of data. The post included screenshots of student IDs and financial data, as well as the statement that that they had uploaded 60% of the stolen data.

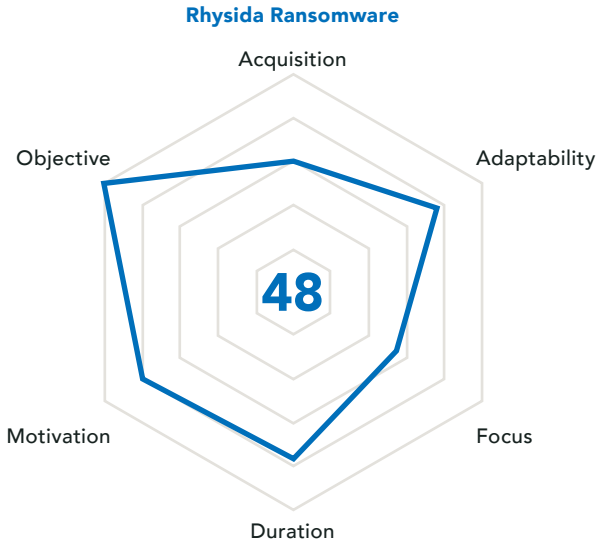

Figure 18: Threat Actor Metric™ for Rhysida Ransomware

Clop

Of the 384 victims listed on the Clop data leak site from January 1, 2023 - December 15, 2023, 21 of them (5.5%) are in the academic and educational services vertical.

- Clop named 17 academic and educational services institutions throughout June and July 2023 that were purportedly targeted via the MOVEit Transfer vulnerability. The data purportedly stolen included personnel and student data, financial data, and more.
- In November 2023, Clop and Rhysida both named North Carolina Central University on their data leak sites. The school suspended online courses and school network access. It is not known if both groups targeted the school, shared information, or conducted the attack together.

Vice Society

Vice Society was first discovered in June 2021 and uses double extortion methods. Vice Society has previously deployed third-party ransomware payloads, such as HelloKitty, Five Hands, RedAlert, and Zeppelin ransomware. However, in December 2022, it was reported that the Vice Society group had created a custom variant, PolyVice.

In September 2022, the U.S. CISA released an advisory warning of the threat posed by the Vice Society ransomware group. Vice Society was the top ransomware operation targeting the education vertical in 2022.

The group's data leak site has not been updated since June 2023, indicating that they are no longer active. There is an **Even Chance** that the group has dissolved and joined other groups, or that the group remains active without a data leak site.

Of the 45 victims listed on the Vice Society data leak site from January 1, 2023 - December 15, 2023, 18 of them (40%) are in the academic and educational services vertical.

- Vice Society began their data leak site in 2021, and the Whitehouse Independent School District in Texas was one of the first listed victims. The group posted more than 18,000 files containing purported data related to employees, students, financial data, and more. The group stated they posted the data because the school had ignored their messages to negotiate a ransom payment.
- In January 2023, Vice Society named the University of Duisburg-Essen on their data leak site months after a November 2022 cyberattack that reportedly forced the university to "reconstruct the entire IT infrastructure." This reconstruction was ongoing at the time they were publicly named on the data leak site. The leaked files included financial and research papers.
- In March 2023, Vice Society named West Virginia's Berkeley County Schools on their data leak site. The school temporarily closed as a result.

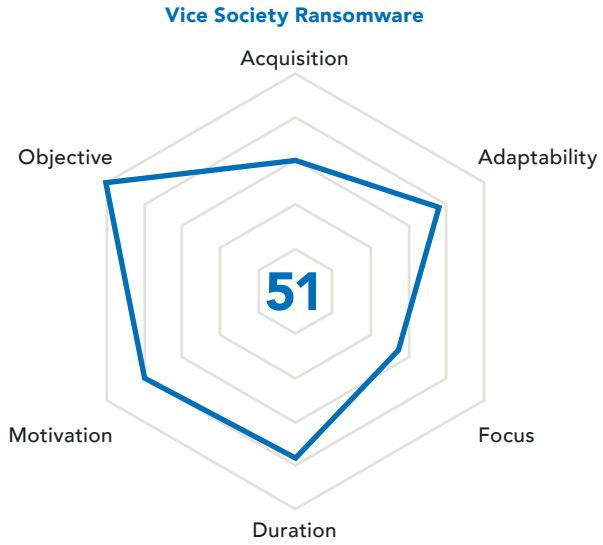

Figure 19: Threat Actor Metric™ for Vice Society Ransomware

MedusaLocker

rebrand of the Ako ransomware variant. Affiliates are responsible for compromising their own victim, which leads to a wide variety of initial access vectors. The most commonly reported initial access vector has been internet-facing RDP servers. MedusaLocker developers required their affiliates to meet a set of skills, which included "practical experience with ransomware, confident user of Cobalt Strike, able to escalate local administrator and domain administrator privileges, working knowledge of backup systems, and understanding of OpSec."

MedusaLocker ransomware participates in the double extortion method where victims' data is stolen, and the data is leaked if the ransom is not paid.

Of the 142 victims listed on the MedusaLocker data leak site from January 1, 2023 - December 15, 2023, 17 of them (12%) are in the academic and educational services vertical.

- In March 2023, MedusaLocker named Minnesota's Minneapolis Public Schools on their data leak site and demanded a $1 million ransom. The leaked files included more than 189,000 files totaling more than 143GB of data. The information included sensitive emails, student data, complaint information, and financial data with dates ranging from 2018-2023.
- In April 2023, MedusaLocker named New York's Uniondale Union Free School District on their data leak site and claimed that the school could pay $1,000 to extend the deadline by one day or pay $1,000,000 to delete all of the data.

The data purportedly included student information, including grades and parent income forms.

- In December 2023, MedusaLocker named three U.S. school districts on their data leak site and posted sensitive documents for each district—including student, parent, and staff data. MedusaLocker demanded $1 million from one of the schools and $600,000 from the other two.

Honorable Mention - Akira

Of the 170 victims listed on the Akira data leak site from January 1, 2023 - December 15, 2023, 16 of them (9.4%) are in the academic and educational services vertical.

- In June 2023, Akira named Virginia's Middlesex County Public Schools on their data leak site. Reportedly, daily operations were minimally impacted due to the attack. Akira claimed to have stolen 543GB of data.
- In August 2023, Akira named Arkansas' Jasper High School on their data leak site and claimed to have stolen 60GB of sensitive information.
- In October 2023, Akira named Stanford University on their data leak site and claimed to have stolen 430GB of data limited to Stanford University Department of Public Safety (SUDPS).

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 techniques 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-2012-0158	Buffer Overflow Vulnerability	MSCOMCTL.OCX library	9.3	APT10, APT27, APT34, APT41, Deep Panda
CVE-2012-4792	Use-After-Free Vulnerability	Internet Explorer 6-9	9.3	APT27, Deep Panda
CVE-2013-0322	XSS Vulnerability	Ubercart module 7.x-3.x before 7.x-3.4 for Drupal	4.3	APT41, Cl0p
CVE-2015-5119	User-After-Free Vulnerability	Adobe Flash Player	10	APT10, APT27
CVE-2017-0144	RCE Vulnerability	Microsoft SMBv1	8.1	APT27, Lazarus Group
CVE-2017-0199	RCE Vulnerability	Microsoft Office/WordPad	7.8	APT27, APT34, APT41, Lazarus Group, Mustang Panda
CVE-2017-11882	Memory Corruption Vulnerability	Microsoft Office	7.8	APT27, APT34, APT41
CVE-2018-13379	Credential Exposure Vulnerability	Fortinet FortiOS SSL VPN	9.8	Alphv, LockBit, Mustang Panda, Play
CVE-2019-0604	RCE Vulnerability	Microsoft SharePoint	9.8	APT27, APT24
CVE-2021-26857	Deserialization Vulnerability	Microsoft Unified Messaging	7.8	APT27, SparklingGoblin
CVE-2021-26858	RCE Vulnerability	Microsoft Exchange Server	7.8	APT27, SparklingGoblin
CVE-2021-27065	RCE Vulnerability	Microsoft Exchange Server	7.8	APT27, SparklingGoblin
CVE-2021-4034	Out-of-Bounds Read and Write Vulnerability	Red Hat Polkit	7.8	BianLian, Lazarus Group
CVE-2021-40539	Authentication Bypass Vulnerability	Zoho ManageEngine ADSelfService Plus	9.8	APT27, Volt Typhoon
CVE-2022-26134	RCE Vulnerability	Atlassian Confluence Server and Data Center	9.8	APT41, Cl0p

Vulnerability	Description	Affected Product	CVSS	Groups Observed Targeting
CVE-2022-27925	Arbitrary File Upload Vulnerability	Zimbra Collaboration (ZCS)	7.2	BianLian, Lazarus Group, MalasLocker
CVE-2022-31199	Insecure Object Deserialization Vulnerability	Netwrix Auditor	9.8	Cl0p, LockBit
CVE-2022-37042	Authentication Bypass Vulnerability	Zimbra Collaboration (ZCS)	9.8	Lazarus Group, MalasLocker
CVE-2022-40684	Authentication Bypass Vulnerability	Fortinet FortiOS	9.8	Earth Lusca, Volt Typhoon
CVE-2023-27350	Improper Access Control Vulnerability	PaperCut MF/NG	9.8	BianLian, Cl0p, LockBit
CVE-2023-27351	Improper Authentication Vulnerability	PaperCut NG 22.0.5	7.5	Cl0p, LockBit
CitrixBleed (CVE-2023-4966)	Sensitive Information Disclosure Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	9.4	LockBit, Medusa
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, APT27, APT41, Deep Panda, Lazarus Group, LockBit
ProxyLogon (CVE-2021-26855)	RCE Vulnerability	Microsoft Exchange	9.8	APT10, APT27, APT41, Alphv, Earth Lusca, SparklingGoblin
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	Alphv, APT10, BianLian, Earth Lusca, LockBit
Spring4Shell (CVE-2022-22965)	RCE Vulnerability	Spring Framework JDK 9+	9.8	Alphv, LockBit, Vice Society
ZeroLogon (CVE-2020-1472)	Privilege Escalation Vulnerability	Netlogon	10	APT10, BianLian, Cl0p, Earth Lusca

Tool	Description	Groups Observed Using Tool
Acunetix	An automated web application security testing tool that audits web applications by checking for vulnerabilities.	APT41, Earth Lusca
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.	Akira, APT10, APT27, Earth Lusca, Lazarus Group, LockBit, Mustang Panda, Play
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.	Akira, Alphv, LockBit, Rhysida, Vice Society
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, Rhysida, Vice Society
AnyDesk	A remote desktop application that provides remote access to computers and other devices.	Akira, BianLian, LockBit, Rhysida
BloodHound	An Active Directory reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.	APT10, LockBit, Play
certutil	A command-line program used to dump and display certification authority configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains.	APT10, APT27, APT34, APT41, Earth Lusca, Medusa Panda, SparklingGoblin
cmd	A program used to execute commands on a Windows computer.	APT10, Rhysida, Volt Typhoon
Cobalt Strike	A post-exploitation tool that is often used during cyberattacks to deploy beacons.	Alphv, APT10, APT27, APT41, Clop, Deep Panda, Earth Lusca, Lazarus Group, Medusa, Mustang Panda, Play, Rhysida, SparklingGoblin, Vice Society, Volt Typhoon
CrackMapExec	An open-source tool that leverages Mimikatz to enable users to harvest credentials and move laterally through an Active Directory environment.	APT39, LightBasin
Dnscmd	A program used to change values in the registry for the DNS server and individual zones; the command also modifies the configuration of the specified server.	APT41, Volt Typhoon
Dropbox	A cloud storage service that allows users to save files online and sync them to other devices.	APT10, APT27, APT39, APT41, Lazarus Group
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.	APT41, Play, Vice Society
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.	Akira, APT41, LockBit
FScan	A comprehensive internal network scanning tool that provides numerous functions including network scanning, vulnerability scanning, building reverse shells, and brute forcing common services.	APT41, Earth Lusca, SparklingGoblin

Tool	Description	Groups Observed Using Tool
GitHub	An internet hosting service for software development and version control that has been used by threat actors to host malware.	APT41, Earth Lusca, Lazarus Group, SparklingGoblin
GMER	A tool used to detect and remove rootkits.	LockBit, Play
gsecdump	A publicly available credential dumper used to obtain password hashes and LSA secrets from Windows OS.	APT10, APT27
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.	Alphv, APT10, APT27, BianLian, Lazarus Group, LightBasin, LockBit, Mustang Panda, Vice Society, Volt Typhoon
ipconfig	A command line utility that is used to display and manage the IP address assigned to the machine.	APT27, APT34, APT41, Volt Typhoon
JuicyPotato	A local privilege escalation tool.	APT27, Earth Lusca, Volatile Cedar
LaZagne	An open-source application used to retrieve passwords stored on a local computer.	Akira, Alphv, APT27, APT34, LockBit
Ligolo	A simple and lightweight tool for establishing SOCKS5 or TCP tunnels from a reverse connection in complete safety.	Alphv, LockBit
LSASS	A Windows process that takes care of security policy for the OS.	Akira, Alphv, APT41, BianLian, Earth Lusca, Play, Rhysida, Volt Typhoon
MEGA/ MEGASync	A cloud storage and file hosting service and a cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.	Alphv, BianLian, Earth Lusca, LockBit
Metasploit	A tool that can be used by threat actors to probe systematic vulnerabilities on networks and servers.	Alphv, APT27, APT39, LockBit, SparklingGoblin, Volt Typhoon
Meterpreter	A Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.	APT39, APT41, Mustang Panda, SparklingGoblin
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.	Akira, Alphv, APT10, APT27, APT34, APT39, APT41, Earth Lusca, Lazarus Group, LockBit, Mustang Panda, Play, SparklingGoblin, Volt Typhoon
NBTScan	An open-source tool that has been used to conduct internal reconnaissance within a compromised network.	APT27, APT39, APT41, Earth Lusca, Mustang Panda, SparklingGoblin

Tool	Description	Groups Observed Using Tool
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.	APT10, APT27, APT34, APT41, Clop, Deep Panda, SparklingGoblin, Volt Typhoon
NetScan	A utility that scans within a subnet or IP range to check for devices.	LockBit, Play
netsh	A scripting utility used to interact with networking components on local or remote systems.	Lazarus Group, Volt Typhoon
netstat	A tool that generates displays that show network status and protocol statistics.	APT27, APT34, APT41, SparklingGoblin, Volt Typhoon
Ngrok	A tool that exposes local servers behind NATs and firewalls to the public internet over secure tunnels.	Akira, Alphv, BianLian, LockBit
Nirsoft	A collection of tools that include password recovery utilities, network monitoring tools, command-line utilities, and more.	Alphv, APT41
Nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.	Earth Lusca, Play, Volt Typhoon
Nmap	An open-source utility for network discovery; it 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, Mustang Panda
Non-Sucking Service Manager	A service manager that manages background and foreground services and processes.	APT39, BianLian
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, Volt Typhoon
PC Hunter	A toolkit for Windows with various powerful features for kernel structure viewing and manipulating.	Akira, LockBit, Play
Ping	A tool used to test whether a particular host is reachable across an IP network.	APT10, APT41, Deep Panda, SparklingGoblin, Volt Typhoon
Plink	A common utility used to tunnel RDP sessions and can be used to establish SSH network connections to other systems using arbitrary source and destination ports.	APT34, APT39, Lazarus Group
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.	Akira, Alphv, APT10, APT27, APT39, APT41, BianLian, Deep Panda, Earth Lusca, Lazarus Group, LockBit, Medusa, Mustang Panda, Play, Rhysida, SparklingGoblin, Vice Society, Volt Typhoon

Tool	Description	Groups Observed Using Tool
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 anti-virus, recon, and exfiltration.	Alphv, APT10, APT41, Earth Lusca, LightBasin, Medusa, SparklingGoblin, Vice Society, Volt Typhoon
PowerTool	A security tool that scans and analyzes files at kernel level; can help threat actors remove and disable security services/software.	Akira, LockBit, Play
PowerView	A PowerShell tool used to gain network situational awareness of Windows domains.	APT10, Mustang Panda
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, it also can serve as a general process dump utility that you can embed in other scripts.	Alphv, APT27, APT39, Earth Lusca, Lazarus, LightBasin, LockBit, Rhysida
Process Hacker	An open-source tool that allows users to see what processes are running on a device and identify network connections that are associated with a process.	LockBit, Play
PsExec	A utility tool that allows users to control a computer from a remote location.	Akira, Alphv, APT10, APT27, APT34, APT39, APT41, Deep Panda, LightBasin, LockBit, Medusa, Play, Rhysida, Vice Society, Volt Typhoon
PuTTY	A free and open-source terminal emulator, serial console, and network file transfer application.	Alphv, APT39, Lazarus, LockBit, Rhysida
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.	APT10, APT27, APT39, APT41
Rclone	A command-line program for syncing files with cloud storage services such as Dropbox, Google Drive, Amazon S3, and MEGA.	Akira, Alphv, BianLian, LockBit
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.	Akira, Alphv, APT27, APT41, BianLian, Cl0p, Deep Panda, Earth Lusca, LightBasin, LockBit, Medusa, Play, Rhysida, SparklingGoblin, Vice Society
Responder	A penetration tool that can do poisoning on LLMNR, NBT-NS, and MDNS and can be used to obtain credentials from compromised devices.	Lazarus Group, LightBasin
Rubeus	A C# toolset for raw Kerberos interaction and abuses.	APT10, Vice Society
ScreenConnect	A remote management software used to gain access to a remote computer.	Alphv, LockBit

Tool	Description	Groups Observed Using Tool
SecretsDump	A publicly available tool that can perform various techniques to dump secrets from the remote machine without executing any agent.	APT27, Volt Typhoon
SMB	A client-server communication protocol used for sharing access to files, printers, serial ports, and other resources on a network.	APT39, Medusa, LockBit
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, LockBit
sqlmap	An open-source penetration testing tool that can be used to automate the process of detecting and exploiting SQL injection flaws.	APT41, Earth Lusca
SystemBC	A malware written in C that turns infected computers into SOCKS5 proxies.	Play, Rhysida, Vice Society
SystemInfo	A Windows utility that can be used to gather detailed information about a computer.	APT27, APT34, Volt Typhoon
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.	APT27, APT34, Deep Panda, Earth Lusca, Volt Typhoon
TCPing	A tool that allows you to use a TCP connection to ping a service.	APT10, APT41, SparklingGoblin
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, Mustang Panda
VSSAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.	Alphv, Clop, Medusa, Rhysida
Windows Credential Editor	A security tool to list logon sessions and add, change, list and delete associated credentials.	APT27, APT39, APT41
WinRAR	A trialware file archiver utility for Windows devices that can backup 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.	Akira, APT34, APT39, Earth Lusca, Play
WinRM	Microsoft's version of the WS-Management protocol, which is a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows interoperation between hardware and operating systems from different vendors.	APT27, BianLian, Rhysida
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.	Akira, BianLian, LockBit, Play, Rhysida
WMI/WMIC	A utility that allows script languages to manage Microsoft Windows personal computers and server.	Alphv, APT10, BianLian, Deep Panda, Earth Lusca, Lazarus Group, Medusa, Play, Volt Typhoon
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, Mustang Panda

Malware	Description	Groups Observed Using Malware
Antak	A web shell that is written in .NET and allows attackers to send PowerShell commands to the remote computer.	APT27, APT34, APT39
ASPXSpy	A web shell that allows threat actors to maintain persistence and move laterally through the victim network.	APT27, APT39, APT41, Volatile Cedar
BIOPASS RAT	A malware that possesses basic features found in other malware, such as file system assessment, remote desktop access, file exfiltration, and shell command execution. It can compromise the private information of its victims by stealing web browser and instant messaging client data.	APT41, Earth Lusca
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, APT27, APT41, Deep Panda, Mustang Panda
CrossWalk	A backdoor that gathers system information and can execute shell code in response to C2 messages.	APT41, SparklingGoblin
Derusbi	A DLL backdoor capable of obtaining directory, files, 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.	APT41, Deep Panda
EdgeBender	An ASPX webshell written in C# that functions as a dropper, decrypts an embedded payload using a key supplied via an HTTP request. The malware supports self-update and self-delete.	APT34, APT39
FunnySwitch	A .NET framework backdoor that usually uses DLL Search Order Hijacking and executes inside a legal process.	APT41, Earth Lusca, SparklingGoblin
gh0st RAT	A publicly available RAT that can 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, Deep Panda, Lazarus Group
HDRoot	A backdoor that installs a bootkit that infects the OS during the boot stage with an arbitrary backdoor specified as a parameter.	APT41, SparklingGoblin
HTTPBrowser	A malware that can establish persistence, manipulate files, capturing keystrokes, and more.	APT27, Deep Panda
KEYPLUG	A modular backdoor written in C++ that supports multiple network protocols for C2 traffic including HTTP, TCP, KCP, over UDP, and WSS.	APT41, Sandman
MessageTap	A data miner initially loaded by an installation script that is designed to monitor and save SMS traffic from specified phone numbers, IMSI numbers, and keywords for subsequent theft.	APT39, APT41
NJRat	A RAT that will silently collect and steal information, including credentials. The malware can perform keylogger monitoring, remote desktop control, installing additional malicious software, and many other malicious activities on the victim's computer.	APT27, APT41, Earth Lusca
Pandora	A multi-stage kernel rootkit with backdoor that has the ability to gain privileged escalation, load additional drivers, monitor processes, inject code, and install itself as a service.	APT10, APT27
PipeMon	A backdoor that persists as a Print Processor that has been used to target video game companies in South Korea and Taiwan.	APT41, SparklingGoblin

Malware	Description	Groups Observed Using Malware
PlugX	Also known as SOGU. A RAT that is used by multiple threat groups and has the ability to manipulate files, capture screenshots, establish persistence, and enumerate drives.	APT10, APT27, APT41, Deep Panda, Mustang Panda, SparklingGoblin
PoisonIvy	Also known as Spivy. A publicly available remote access trojan that can monitor victims remotely and steal user credentials and files.	APT10, Mustang Panda
PowBat	A backdoor malware that can be used to establish persistence in a victim network.	APT34, APT39
Quasar RAT	A legitimate open-source RAT written in C# programming language and has been used to remotely access compromised devices.	APT10, APT41
RedXOR	A backdoor that masquerades itself as polkit daemon.	APT41, SparklingGoblin
RemCom	A lateral movement tool written in C/C++ that reimplements the logic of the Sysinternals PsExec application. The malware supports creating an interactive command prompt on a remote system as well as executing files and shell commands. It can also be used to copy files to a remote system.	APT27, Mustang Panda
Scanbox	A capable of collecting information about the victims visiting the site, including but not limited to keystrokes, Adobe Flash versions, Microsoft Office versions, Acrobat Reader versions, and Java versions. Other collected system information includes installed anti-virus (AV) products, operating system (OS) patch levels, and IP address.	APT10, APT27, Deep Panda
ShadowHammer	A backdoor that was deployed via a modified version of the ASUS Live Update Utility software and was used to deploy additional payloads.	APT41, SparklingGoblin
ShadowPad	Also known as Barlaiy, POISONPLUG. A backdoor widely believed to be the successor of the PlugX malware that can download additional payloads and gather system information.	APT41, Earth Lusca, Mustang Panda, SparklingGoblin
Spyder	A module backdoor written in C++ and designed to run on 64-bit Windows. Its purpose is to decrypt files and load additional payloads.	APT41, Earth Lusca, SparklingGoblin
Trochilus	An RAT that is primarily spread through emails with a malicious .RAR attachment containing the malware. The malware can move laterally, operates in memory only, and does not write to the disk.	APT10, APT27, APT41, Earth Lusca, Lazarus Group
TwoFace	Also known as Minion, HyperShell, SEASHARPEE. A two stage webshell written in C# that is designed to run on webservers with ASP.NET. The web shell can execute commands, download and delete files, and manipulate MAC timestamps.	APT27, APT34
Winnti for Linux	A trojan that specifically targets Linux systems and can deploy modules and has used a passive listener.	APT39, APT41, SparklingGoblin
XMRig	An open source cryptomining malware that hijacks the user's computer and uses its resources to mine cryptocurrency, such as Monero.	APT27, APT41, Earth Lusca, SparklingGoblin
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.	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) T1068 – Exploitation for Privilege Escalation (Privilege Escalation) T1203 – Exploitation for Client Execution (Execution)	Attackers often exploit known vulnerabilities in external remote services and public-facing applications to gain access, privilege escalation, and execution.	Microsoft Exchange Cisco Fortigate VPN Citrix PulseSecure Outlook Web Access RDP
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

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
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) T1218 – System Binary Proxy Execution (Defense Evasion) T1027 – Obfuscated Files or Information (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) T1012 – Query Registry (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 Reg Query reg query "HKEY_CURRENT_USER\ Software\Microsoft\Terminal Server Client\Default"

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
T1005 – Data from Local System (Collection) T1074 – Data Staged (Collection) T1056 – Input Capture (Collection) T1560 – Archive Collected Data (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) T1102 – Web Services (Command and Control)	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 *

Based on the tables above, attribution can be difficult to ascertain when attacks occur, which **Likely** results in fewer attacks being linked to group activity. This indicates that groups are **Likely** more active than public reporting indicates due to many attacks remaining unattributed.

Outlook

Technology, telecommunications, and academics and educational services verticals are attractive targets for both APT and cybercriminal groups due to the criticality of their operations to an economy, the public, the type of information that could be obtained, and the perception that threat actors are more likely to get a ransom payment. Despite many defensive frameworks and policies that these institutions have adopted to improve security, organizations in these verticals remain an attractive target for ransomware operations due to the high-value information, company revenues, and critical nature of these organizations. These factors contribute to the likelihood of ransom payments or negotiations.

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.

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 multi-factor 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**, these 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. There has been a spike in APT activity since the beginning of the Russia/Ukraine war. 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 malicious links distributed to multiple organizations and potential victims, as well as the exploitation of older (2+ years) 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 technology, telecommunications, and academic and educational services verticals over the next 12 months.

Appendix A: Probability/ Confidence Statements

Intelligence and Cyber Intelligence Frameworks

MITRE ATT&CK: The framework developed by the MITRE organization which illustrates technical, endpoint-based activity and behaviors of threats and adversaries. Activities and behaviors are organized into 14 Tactics, which are further broken down into Techniques. A wide range of procedures are the actions and behaviors to achieve the Technique, while the Techniques are the actions to achieve the main Tactics.

Optiv Threat Actor Metric™: The Optiv Threat Actor Metric™ was developed by Optiv's gTIC and is a multi-faceted, qualitative approach to determine a cyber adversary's or campaign's potential threat to an organization or industry. The metric considers known and assessed non-technical capabilities and intentions and is scored out of a total possible of 100. The purpose of this metric is to provide an added layer of depth to risk-based intelligence analysis and support proactive and remediating recommendations by presenting a visualization of non-technical, qualitative risk factors of adversaries and threat campaigns. It is similar in function to the U.S. Department of Defense's CARVER targeting scale.

Analytical Comments, Statements, and Best Practices

Most Likely Course of Action (MLCOA): The expected and probable tactics, techniques, and actions carried out by a threat actor. COA statements are well established and accepted in estimative and predictive intelligence assessments.

Most Dangerous Course of Action (MDCOA): The tactics, techniques, or actions carried out or taken by an adversary that result in a worst-case scenario outcome or impact, regardless of probability. COA statements are well established and accepted in estimative and predictive intelligence assessments.

Words of Estimated Probability: The gTIC employs the use of both probability statements for likelihood of events or actions and confidence levels for analytic assessments and judgments. Probability statements and confidence statements are inherently subjective; however, the gTIC leverages professional experience and intelligence fundamentals to deliver reasonable and relevant statements and assessments. Probability statements and the degree of likelihood of an assessed event/incident are modeled after the Intelligence Community Directive (ICD) 203: Analytic Standards, published by the United States' Office of the Director of National Intelligence (ODNI), and are as follows:

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain(ly)
Remote	Highly Improbable	Improbable (Improbably)	Roughly Even Odds	Probable (Probably)	Highly Probable	Nearly Certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence statements, as defined by Optiv's gTIC, apply to the reliability and relevance of information reported and are as follows:

Confidence Level	Optiv gTIC Definition	Factors	Quantitative Relevance
High Confidence	Information and/or intelligence is assessed to be of high reliability and value to drive operations and decision	Established history, repeated observations and patterns, strong precedence to form professional assessment and prediction/ extrapolation	75%+
Moderate Confidence	Information and/or intelligence is reasonable and warrants consideration or action or response where applicable	Sporadic observations, limited historical references (too recent or too long of a gap to be considered "established")	45-65% (+/- 10%)
Low Confidence	Information and/or intelligence is unreliable or less relevant and provided as situational awareness	Lack of established history or observations, unreliable or circumstantial evidence	< 35%

Per *ICD 203* standards, confidence-level statements are not combined with probability and degree of likelihood terms proposed in the above chart.

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.