Vertical Target Series

Financial Services, Insurance and Health Care Threats

White Paper

Cybercriminals and APT groups often target organizations in critical infrastructure verticals—including financial services, insurance, and health care—because of the type and amount of sensitive information they can obtain, the amount of money these organizations are perceived to have available, and the potential of an attack. Ransomware groups frequently target these companies because they cannot suffer significant downtime without having rippling effects on the target countries' economic stability.

An APT group is a malicious actor who is believed to possess significant skills, have virtually unlimited resources, and conduct highly targeted attacks. APT groups 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. Ransomware cybercriminal campaigns, on the other hand, focus on the encryption or destruction of files and folders on the targeted endpoint or across the network. Ransomware syndicates have constantly shifted tactics to remain relevant, including rebranding, leveraging known and benign tools to maintain persistence, and building an ecosystem around their own affiliate groups and program. Such an ecosystem may include hosting and building their own tools, forums, and leak pages.

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

Table of Contents

Financial Services

Due to extensive digital transactions, a large attack surface, and the impact a ransomware attack could have on financial services organizations, threat actors find the financial services vertical to be an attractive target. Not only would an attack impact the organization's revenue, but financial services organizations also host customers' personally identifiable information (PII), including names, addresses, social security numbers, phone numbers, email addresses, and more. PII is useful for threat actors to compose convincing social engineering attacks that can lead to the deployment of malware, data exfiltration, and more. Below is the gTIC's analysis of 3 APT groups targeting this vertical.

Granite Typhoon

Granite Typhoon (aka GALLIUM, Alloy Taurus, Soft Cell) is a cyberespionage group that has been active since at least 2012. The group has primarily targeted the telecommunications vertical and has since expanded their targeting to include financial services and government organizations. Granite Typhoon exploits known vulnerabilities and conducts phishing campaigns to gain initial access. The group modifies its tooling to evade antimalware detection, rather than develop custom functionality. Granite Typhoon primarily uses web shells to create persistence in a target network and uses the access to deliver subsequent malware. Granite Typhoon has also developed the capability to target Windows and Linux systems.

From 2021-2022, Granite Typhoon was attributed to multiple campaigns targeting financial services organizations with phishing emails. The group deployed the PingPull malware, which can run commands and access a reverse shell on the compromised host—providing threat actors with remote access to the victim's network.

Blind Eagle

Blind Eagle (aka APT-C-36) has been active since at least 2018, uses spear-phishing emails as their infection vector, and has spoofed legitimate organizations and institutions to deliver backdoor and remote access trojan malware to victims. Their objective is seemingly information theft, including intellectual property. Attribution to a specific country is unconfirmed. Based on the RAR files used in their Spanish-language phishing emails capturing the last modification date, the group appears to be operating within the UTC-4 and adjacent time zones, suggesting a South American origin.

From 2019-2023, Blind Eagle has been attributed to multiple espionage-focused phishing campaigns targeted organizations in Chile, Colombia, Ecuador, Panama, and Spain. The group has been observed impersonating the Colombian government tax agency, Colombia's national directorate of taxes and customs, and more. The goal of the emails has been to deploy RAT malware that can be used to maintain remote access to compromised victim systems, exfiltrate data, and deploy additional malware payloads.

APT38

APT38 (aka Bluenoroff, Stardust Chollima, Sapphire Sleet) is a North Korea-linked financially motivated APT group that has been attributed to the North Korean Reconnaissance General Bureau. The group is most known for their 2016 targeting of the Bangladesh Bank and their use of destructive malware to cover up their fraudulent transactions. APT38 is believed to be a subgroup of the North Korea-linked Lazarus Group and likely targets financial institutions to fund the group's malicious activities and North Korean interests. APT38 often targets known vulnerabilities and uses watering hole attacks and social engineering attacks to gain initial access. The pace of their targeting of financial institutions, as well as their successful theft of millions of dollars from these institutions, highlights North Korea's increasing efforts to gather funds to pursue state interests.

In 2015, APT38 reportedly targeted a Vietnam-based bank and unsuccessfully attempted to transfer $1.36 million out of its accounts via the interbank SWIFT messaging system. However, the group also targeted a bank in the Philippines and a bank in Ecuador, where the group successfully stole $12 million. In 2017, APT38 purportedly sent phishing emails containing Windows shortcut files delivering malware to financial services organizations. The file names were disguised as security or cryptocurrency related files to lure victims into downloading them.

Also in 2017, the group was attributed to the targeting of a commercial banking firm in Taiwan. APT38 moved funds to other accounts and deployed the Hermes ransomware. In 2018, APT38 targeted multiple banks, including a Mexico-based bank where the group attempted to steal $110 million. The group was attributed to a cyberattack targeting Chile's largest financial institution with a wiper malware, destroying 9,000 workstations and 500 servers. The group purportedly used the wiper attack to mask the financial theft of $10 million.

In 2021-2022, the group was attributed to the stalking of a successful cryptocurrency startup. The goal of the infiltration team was to build a map of interactions between individuals and understand possible topics of interest for launching convincing social engineering attacks. In 2022, the group was accused of placing an operative in a tech job with a U.S.-based cryptocurrency startup as a developer – who reported passed multiple interviews – in order to gain access to the internal networks. The alleged goal was to send money and information back to North Korea.

APT38 has been attributed as a subgroup of Lazarus Group and is **Likely** part of the team targeting financial services organizations. The U.S. CISA reported that Lazarus Group distributed the AppleJeus malware in a February 2021 campaign targeting cryptocurrency exchanges and financial institutions spanning over 30 countries. The group used phishing and other social engineering techniques to lure users into downloading cryptocurrency apps compromised by the AppleJeus malware.

Ransomware Groups with Financial Services Targets

According to the Sophos State of Ransomware 2022 report, 55% of financial services organizations were affected by at least one ransomware attack in 2021 – up from 34% in 2020. In 2021, the New York Department of Financial Services stated that "a major ransomware attack could cause the next great financial crisis." Ransomware operators target this vertical due to the perceived amount of money the organization has available to pay a ransom demand. The top ransomware groups that targeted the financial services vertical over the previous 12 months include LockBit, Alphv (aka BlackCat), Clop, Royal, and Black Basta. LockBit targeted 74 organizations, Alphv targeted 30, Clop targeted 17, Royal targeted 16, and Black Basta targeted 14.

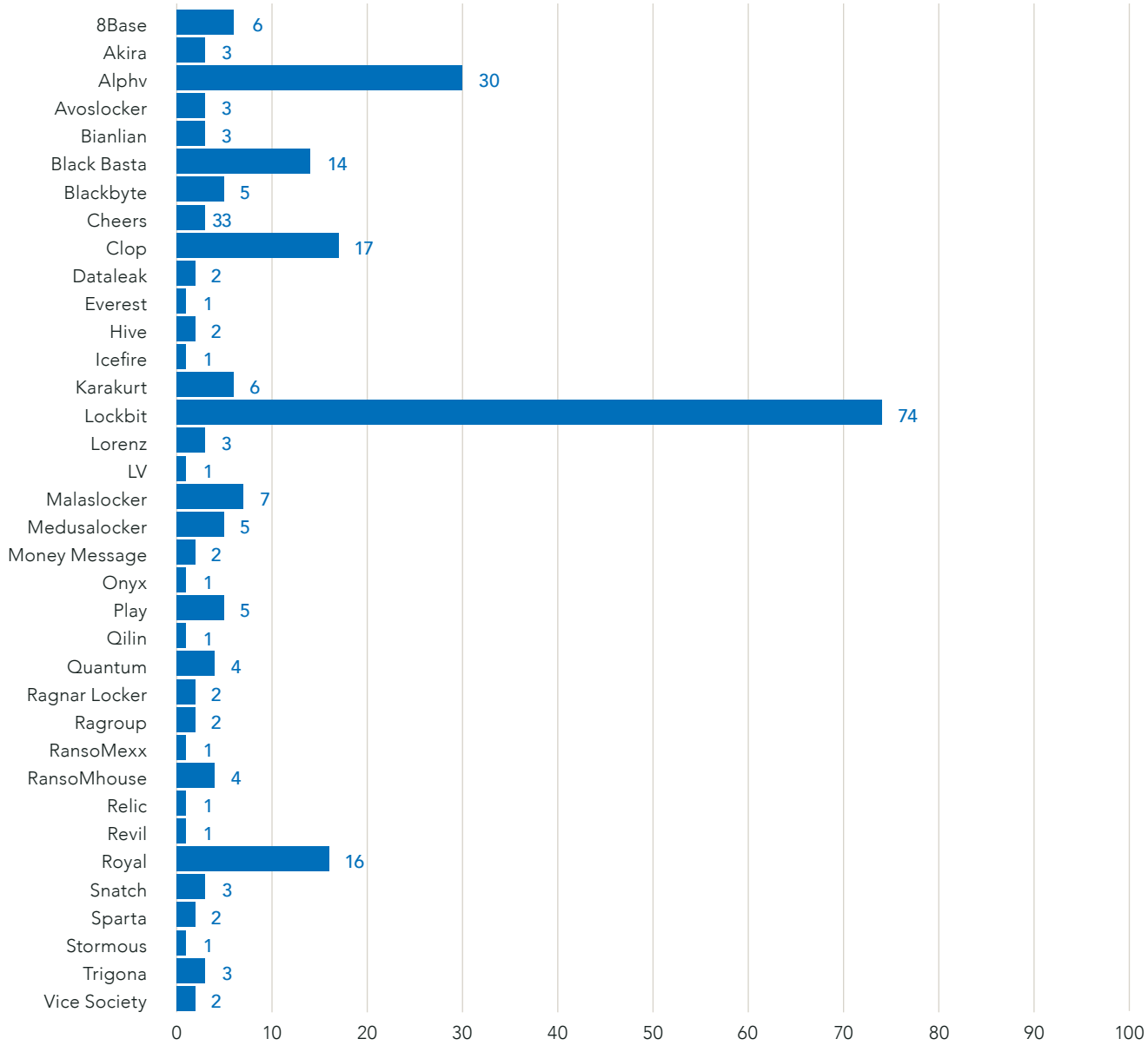

Figure 1: Ransomware variants that listed financial services organizations on their data leak site: June 01, 2022 - May 31, 2023

LockBit

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

In July 2022, LockBit announced the release of LockBit 3.0 on their Russian-language cybercriminal forum, XSS, after security vulnerabilities were identified in LockBit 2.0. Along with improvements to the variant, the group announced a bug bounty program offering rewards of $1,000+ for PII on sensitive targets and found security exploits. LockBit is responsible for nearly half of the reported victims listed on all data sites each quarter.

Of the 890 victims listed on LockBit's data leak site from June 01, 2022, to May 31, 2023, 73 of them (8.2%) are in the financial services vertical. In December 2022, LockBit claimed to have stolen 76GB of data related to databases, confidential data, and financial documents from the California Department of Finance. The California Governor's Office of Emergency Services released a statement that the California Cybersecurity Integration Center (Cal-CSIC) was "actively responding" to the incident and that no state funds had been compromised. In February 2023, LockBit claimed responsibility for a ransomware attack targeting a Dublin-based financial software company that helps financial institutions automate critical business processes. The group removed the organization's name, indicating that a ransom amount was paid.

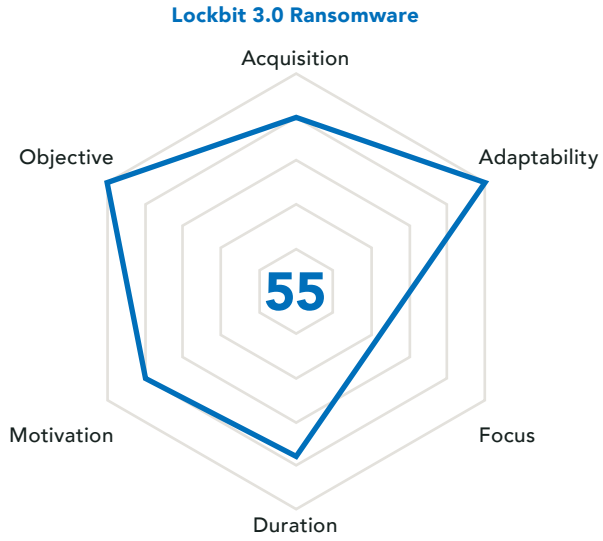

Figure 2: Threat Actor Matrix™ score for LockBit Ransomware

Alphv

Alphv (aka BlackCat) is a ransomware variant that has been active since at least November 2021. In this RaaS operation, where operators often recruit affiliates on Russian-language cybercriminal forums, affiliates earn 80% of payments up to $1.5 million and 90% of payments over $3 million. Initial access vectors include compromised Remote Desktop Protocol (RDP), phishing attacks, stolen credentials, and vulnerability exploitation.

Of the 326 victims listed on Alphv's data leak site from June 01, 2022, to May 31, 2023, 29 of them (8.9%) are in the financial services vertical. In May 2023, Alphv ransomware operators claimed responsibility for targeting a Utah-based mortgage lender with branch offices in over 30 states. Alphv operators posted purported internal documents and indicated that they had been in the organization's network for a "long time" and claimed to have personal, customer, partner, financial, and confidential data. Alphv stated

on their data leak site that the organization refused to pay the ransom demand. In November 2022, Alphv ransomware operators admitted to stealing 2TB of sensitive data from an African banking institution. The bank reportedly refused to pay the ransom demand.

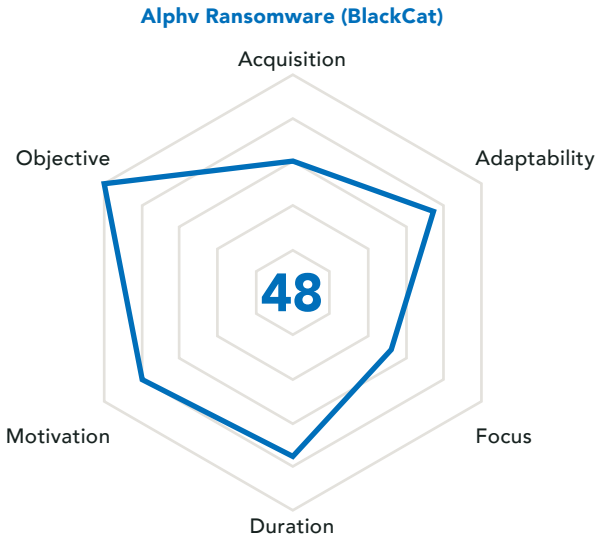

Figure 3: Threat Actor Metric™ score for Alphv Ransomware

Royal

Royal is a private ransomware group reportedly comprised of former Conti ransomware affiliates. Their human-operated ransomware first observed in September 2022, but it was likely active as early as January 2022. Royal has made a significant impact on the ransomware landscape. Unlike other ransomware operations, Royal ransomware operators have gained initial access via phishing attacks, RDP compromises, credential abuse, vulnerability exploitation, malicious downloaders, and malvertising on Google ads. In March 2023, the U.S. CISA released a #StopRansomware alert providing details of the group and their operations.

Of the 197 victims listed on Royal's data leak site from June 01, 2022, to May 31, 2023, 15 of them (7.6%) are in the financial services vertical. In November 2022, Royal ransomware operators targeted a U.S.-based financial services provider, and in December 2022, they targeted an Australia-based mortgage company. In both cases, the ransom demands remain unknown, and the victim organizations were listed on the Royal data leak site—indicating that the organizations either refused payment or that negotiations failed.

In April 2023, Royal claimed responsibility for a ransomware attack on a U.S.-based financial planning organization. Royal claimed to have access to 2TB of company data. In May 2023, Royal ransomware operators claimed they had targeted a U.S.-based financial consultancy organization and said they had access to passports, social security numbers, and confidential documents. Both companies are listed on their data leak site.

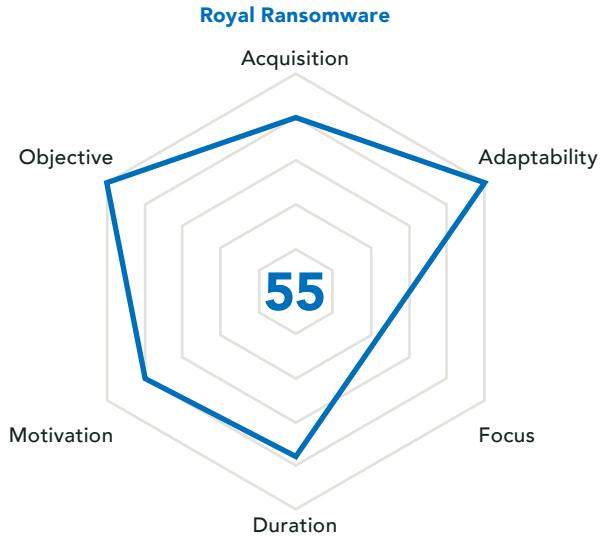

Figure 4: TThreat Actor Metric™ score for Royal Ransomware

Black Basta

Snatch is a ransomware that was first discovered in 2018 that uses the double extortion method, where the victim data is stolen and leaked if the ransom is not paid. Snatch ransomware avoids detection by forcing infected hosts to reboot into Safe Mode. The ransomware installs itself as a Windows service called "SuperBackupMan" that prevents the user from stopping or pausing the service while it is running.

The Snatch ransomware includes both a ransomware and a data stealer component. The malware is written in Go and can purportedly only run in Windows environments. Snatch operators have been observed advertising open spots on their team on cybercriminal forums—even offering to train the affiliates and provide "the best students" with a customized server running Metasploit. The group advertises for Russian speakers only.

Snatch ransomware operators have been observed automating brute-force attacks against vulnerable applications in the target organizations. Additionally, Snatch ransomware operators have been observed using affiliate partners to gain initial access to victim networks.

Snatch reportedly targeted three energy organizations in February, March, and October 2022 in Asia and North America. However, one organization—listed in October 2022, Oil India Limited—was also listed on REvil's data leak site in April 2022. As of this writing, it is not confirmed if Snatch targeted this organization for a second time or if Snatch repeated a listing from the REvil data leak site.

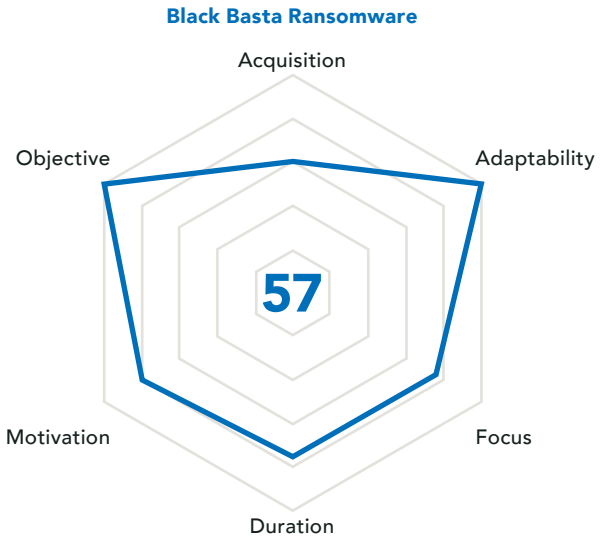

Figure 5: Threat Actor Metric™ score for Black Basta Ransomware

Clop

Clop (aka Clop) is a RaaS operation that has been active since February 2019 and reportedly leverages an updated version of the CryptoMix ransomware from 2016. The Clop variant is signed with a legitimate certificate that helps trick security solutions into trusting the binary. 6 suspected Clop members were arrested in Ukraine in June 2021, but the group's criminal activities have continued. This supports Optiv gTIC's assessment that despite government and law enforcement attention, ransomware operators have very little incentive to halt operations.

Clop ransomware operators manage a data leak website, >_CLOP^_-LEAKS. In Q1 2023, Clop exploited CVE-2023-0669, the GoAnywhere vulnerability, to reportedly target 130 organizations. The group focused on stealing and holding data for ransom. This attack was similar to the Clop attack targeting Accellion FTA vulnerabilities in 2021. In Q2 2023, Clop operators exploited CVE-2023-34362, the MOVEit Transfer MTF solution vulnerability, to target hundreds of organizations. Initial access vectors vary depending on the Clop affiliate. Methods observed include phishing attacks, vulnerability exploitation, weak passwords, and exposed RDP.

Of the 118 victims listed on Clop's data leak site from June 01, 2022, to May 31, 2023, 17 of them (14.4%) are in the financial services vertical. In March 2023, Clop operators exploited the GoAnywhere vulnerability to access a U.S.-based bank's systems from January 30-31. The operators were allegedly able to access over 140,000 social security numbers, and they listed the bank on their data leak site. The bank confirmed the attack. Also in March 2023, Clop operators exploited the GoAnywhere vulnerability to access employee PII at a Canada-based financial services company. In May 2023, Clop operators claimed to have stolen several GB of data, including PII documents, from a U.S. financial services organization.

In June 2023, Clop operators began listing victims that they purportedly targeted via the MOVEit vulnerability. These organizations included 14 financial services organizations – 12 U.S.-based, 1 U.K.-based, and 1 Hong Kong-based organization. Among the organizations listed were banks, investment firms, and financial consultancy organizations. As of this writing, the data has not yet been leaked.

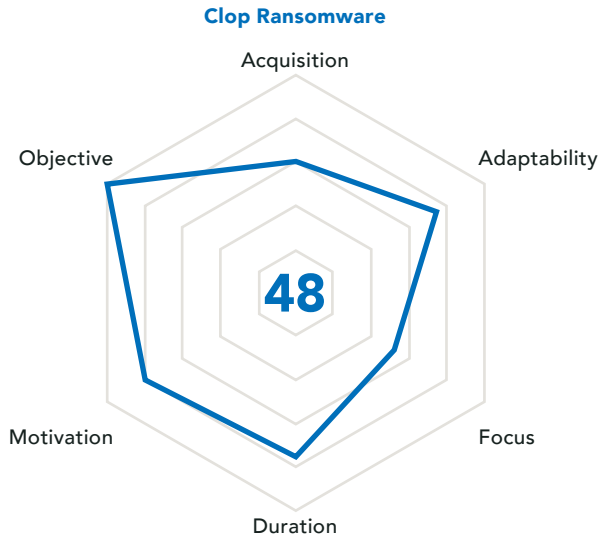

Figure 6: Threat Actor Metric™ score for Clop Ransomware

Insurance

The insurance vertical is a sub-category of the financial services vertical. Insurance organizations often store large amounts of PII, conduct digital transactions, and have applications and 24/7 available staff. APT and cybercriminal groups are attracted to this type of information and attack surface. Nearly every person needs some type of insurance and must provide PII that threat actors could leverage in convincing social engineering attacks. We cover 3 APT groups targeting this vertical below.

Fox Kitten

Fox Kitten (aka Pioneer Kitten, Parasite, Lemon Sandstorm) is an Iran-based threat actor group that has been active since at least 2017 and is linked to the Iranian government. The group is likely focused on seeking material of interest to Iranian intelligence. Researchers have assessed that Fox Kitten is likely a government contract group that gains initial access by leveraging open-source tools and malware, as well as exploits of remote services on web assets.

A purported member of the group has been observed listing accesses to victim networks for sale on cybercriminal forums, which supports the theory that Fox Kitten is a government contract group. Government operated groups usually do not sell access to targeted victims. Multiple Iran-linked threat groups have targeted the same victims and sharing infrastructure and tooling. It is **Likely** that Fox Kitten has previously worked with these groups and acts as an initial access broker (IAB) for criminal groups, including the n3tw0rm and Pay2Key ransomware operations. Although the extent of their relationship is unknown, there is an **Even Chance** that Fox Kitten has provided victims' system access to these operations.

From 2017-2019, Fox Kitten leveraged vulnerabilities in VPN services to target organizations in multiple verticals, including insurance. The group sought to maintain the access by opening communication channels and stealing sensitive data. In 2020, the group was attributed to the targeting of vulnerabilities in the F5 BIG-IP product to gain initial access to victim environments. Fox Kitten was also attributed to the use of the Pay2Key ransomware variant to exploit vulnerabilities in Microsoft Exchange, RDP, and VPNs.

The group has not been publicly active since 2020, but it **Likely** poses a threat to organizations worldwide. This is because many APT groups aim to stay in systems undetected, and not all activity has been identified or publicly reported. It is **Likely** that Fox Kitten members remain active in the cybercriminal landscape, although the extent is unknown.

APT31

APT31 (aka Zirconium, Judgement Panda, Violet Typhoon) is a China-linked APT group that has been active since at least 2010 and is known for cyber espionage. The group has used a wide variety of malware and tools to launch sophisticated cyberattacks, including phishing emails and zero-day exploits to gain initial access to victim networks. The APT31 group is not as widely known as other APT groups—likely operating in the shadows of larger, more well-known groups to remain undetected.

From 2013-2017, APT31 was observed using the EpMe exploit created by Equation Group in 2013. APT31 reportedly replicated the functionality of the EpMe exploit to create a new exploit called Jian, which they used to exploit hundreds of organizations. In 2021, APT31 was attributed to attacks targeting organizations in the government, industrials, and financial services verticals in Russia, Mongolia, Belarus, Canada, and the U.S. The group sent phishing emails to victims laced with RAT malware to maintain remote access to victim organizations and steal sensitive data.

APT34

APT31 (aka Zirconium, Judgement Panda, Violet Typhoon) is a China-linked APT group that has been active since at least 2010 and is known for cyber espionage. The group has used a wide variety of malware and tools to launch sophisticated cyberattacks, including phishing emails and zero-day exploits to gain initial access to victim networks. The APT31 group is not as widely known as other APT groups—likely operating in the shadows of larger, more well-known groups to remain undetected.

In 2018, APT34 was attributed to an attack targeting an insurance agency based in the Middle East. The group used the ThreeDollars delivery document

to deploy the OopsIE malware, as well as socially engineered emails. In 2022, APT34 reportedly conducted a campaign leveraging multiple payloads to harvest credentials from targeted victims across multiple verticals in the Middle East. It is **Likely** that APT34 has gained access to more organizations, and then offered that access to other threat groups. These attacks would likely be attributed to the other groups.

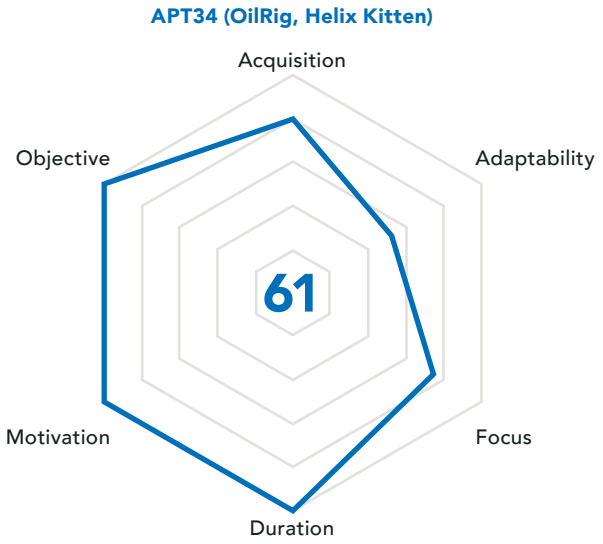

Figure 7: Threat Actor Metric™ score for APT34

Honorable Mention

The MuddyWater APT group, attributed to Iran, receives an honorable for their targeting of insurance organizations. On December 8, 2022, security researchers attributed a spear-phishing campaign to MuddyWater. The campaign began in October 22 and targeted several verticals in the Middle East and Central Asia. The campaign abused both the legitimate remote admin tool, Syncro, and compromised corporate accounts to send phishing emails.

Ransomware Groups with Insurance Targets

In 2022, the insurance vertical profited $69.3 billion, which likely contributes to this vertical being an attractive target for ransomware operators. Threat actors can target an insurance provider and obtain a list of clients they could potentially target. According to a report released by Barracuda, organizations with cyber insurance are more likely to be hit with a ransomware attack. Ransomware operators probably believe that organizations with insurance are more likely to pay the ransom demand than organizations without coverage.

LockBit

LockBit ransomware has remained the most active ransomware operation for the past 12 months. Of the 890 victims listed on LockBit's data leak site from June 01, 2022, to May 31, 2023, 23 of them (2.6%) are in the insurance vertical. In October 2022, LockBit claimed responsibility for a ransomware attack on a U.K.-based insurance organization and their subsidiary offering vehicle insurance. The group claimed to have stolen 1.4TB of data, but the company argued that LockBit could not have stolen that amount of data.

In February 2023, LockBit claimed to have stolen customer driver's licenses and payment data from a U.S.-based insurance company offering commercial auto insurance. In March 2023, LockBit claimed to have stolen over 700GB of patient, policyholder, employee, and financial data from another U.S.-based insurance company data. In both cases, LockBit published the purported data on their data leak site—indicating that the ransoms were not paid. In April 2023, LockBit named an Egypt-based insurance company on their data leak site. Because LockBit later removed the company from the site, either the ransom demand was paid or they mistakenly listed the victim.

Alphv

Of the 326 victims listed on Alphv's data leak site from June 01, 2022, to May 31, 2023, 6 of them (1.8%) are in the Insurance vertical. In February 2022, Alphv named a U.S.-based insurance company and claimed to have stolen over 50GB of data. The operators posted a screenshot of a file directory, which included HR files, reports, and shared data. In January 2023, Alphv claimed responsibility for a ransomware attack targeting a Mexico-based insurance company. Alphv has not leaked any of the purported PII they claimed to have stolen related to clients, partners, and subsidiaries. However, the company is still named, indicating that they have not paid a ransom.

In April 2023, Alphv claimed responsibility for the cyberattack targeting a Venezuelan insurance provider. The listing on the data leak site included 27 screenshots of images of various documents, including ID cards. In May 2023, Alphv claimed responsibility for the ransomware attack exfiltrating 4.7TB of data from a US-based insurance company. The group listed the company on their data leak site and taunted the board members with claims that they failed to protect the privacy of their clients and employees. The sample data included personal sensitive information of patients, financial information, and employee PII.

Royal

Of the 197 victims listed on Royal's data leak site from June 01, 2022, to May 31, 2023, 8 of them (4.1%) are in the insurance vertical. In November 2022, Royal operators named a U.S.-based insurance company on their data leak site. The group claimed to have stolen data related to the county, HR documents, statistics, and general data. Royal said that the data was 100% leaked, indicating the ransom demand was not paid. In December 2022 and May 2023, Royal operators named a Trinidad and Tobago-based insurance company on their data leak site. It is not known if the company was targeted twice or if the data was relisted. The group purportedly stole more than 24GB of data. In April 2023, Royal named a Germany-based insurance company on their data leak site and reportedly leaked 11% of the stolen data. The company is no longer on the site, indicating that a payment was made or that negotiations began.

Black Basta

Of the 222 victims listed on Black Basta's data leak site from June 01, 2022, to May 31, 2023, 6 of them (2.7%) are in the insurance vertical. In September 2022, Black Basta listed a U.S.-based insurance company on their data leak site. The company sent customers a notice of a breach and noted that the attackers may have accessed names and driver's license numbers. In March 2023, the group named a Canada-based insurance company on their data leak site. The group claimed to have leaked the stolen data, indicating that the ransom was not paid.

Clop

Of the 118 victims listed on Clop's data leak site from June 01, 2022, to May 31, 2023, 5 of them (4.2%) are in the insurance vertical. In May and June 2023, Clop listed multiple organizations on their data leak site related to their exploitation of the MOVEit Transfer MFT vulnerability. Of those organizations, 7 are in the insurance vertical – 4 are U.S.-based, 1 is Switzerland-based, 1 is Canada-based, and 1 Brazil-based. As of this writing, the company has not yet released any stolen data.

Health Care

Health care organizations typically cover a diverse range of specialist fields and maintain multiple geographical locations for separate clinics and hospitals. A single organization can have thousands of workstations, specialized medical devices, specialist software, and mobile and cloud-based services. Multiple employees and volunteers with generic or shared credentials can use these workstations. These elements create a large attack surface for threat actors to target. Coupled with the sensitive information stored by health care organizations, such factors make them an attractive target. Below are some of the most active APT groups found to target this vertical.

Kimsuky

The Kimsuky group has been active since at least 2012 and is **Most Likely** tasked by the North Korean regime with a global intelligence gathering mission. Kimsuky is known for their complex infrastructure that uses free-registered, compromised, and private domains registered by the group. The group began by focusing their attacks on South Korean organizations, including government agencies, think tanks, and subject-matter experts. Kimsuky expanded its targets to include the U.S., Russia, Europe, and the U.N. The group focuses its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.

Kimsuky uses spear phishing, malicious attachments, and social engineering methods to obtain initial access to victim networks. The group has been observed sending benign emails to targets, which were likely meant to build trust with the victim and increase the likelihood of a successful attack. Kimsuky has used document lures related to COVID-19, the North Korean nuclear program, and media interviews. Other initial access methods include watering hole attacks, torrent sharing sites, and the directing of victims to install malicious browser extensions. Kimsuky uses a combination of bespoke and open-source or publicly available malware and tools. The use of publicly available tools and malware can make attribution more difficult. Attacks by North Korean-based threat actors are often attributed to Lazarus Group, indicating that Kimsuky may be more active that what is publicly reported.

In 2018 and 2019, Kimsuky was attributed to a spear-phishing campaign that exploited CVE-2017-11882 to target and attempt to steal sensitive information from South Korean organizations. In 2020, Kimsuky was attributed to multiple cyberattacks using phishing emails with COVID-19-related lures and documents laced with the BabyShark malware. Also in 2020, the group was attributed to phishing attacks targeting organizations in various verticals to deploy keyloggers, backdoors, information stealers, and more. In 2022 and 2023, Kimsuky was attributed to phishing attacks designed to deploy malware variants against victim organizations. In 2023, the group sought to steal sensitive information using Microsoft OneNote documents disguised as forms relating to the victims' compensation.

APT22

APT22 (aka Wet Panda, Barista, Bronze Olive, Suckfly) is attributed to the People's Republic of China (PRC) and has been active since at least 2014. The group is most known for targeting government and health care organizations to steal sensitive data of strategic importance and interest to the Chinese government. APT22 reportedly gains initial access by exploiting known vulnerabilities in commonly used software and services. Because APT22's activity has not been tracked or analyzed in detail, the group has likely conducted more attacks than what has been publicly reported. The intelligence gaps do not indicate that the group is incapable of threats with significant malicious intent.

In 2014, APT22 reportedly exploited known vulnerabilities and deployed the Nidiran backdoor to maintain access to target organizations across India, including health care organizations. In 2019, APT22 allegedly targeted biomedical, pharmaceutical, and other health care organizations, including an unnamed U.S.-based cancer research center. The purported goal of these attacks was to steal and use their work to help address growing cancer rates in China.

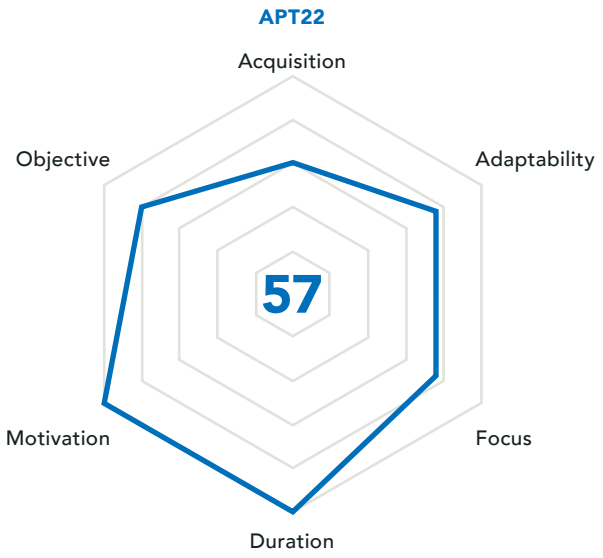

Figure 9: Threat Actor Metric™ score for APT22

APT24

APT24 (aka PittyTiger, Pitty Panda, Earth Aughisky) is a China-linked threat group that has been active since at least 2008, with some reporting suggesting activity since 2011. APT24 develops custom malware variants used exclusively for their activities. However, they are often based on well-known variants, like PlugX and gh0st RAT. Many researchers believe that the group lacks the experience and financial support that many APT groups have. However, their arsenal of tooling suggests the group has access to resources that allow them to continue operating.

The group has been observed conducting phishing attacks to gain initial access, exploiting vulnerabilities during attacks, and focusing on intellectual property theft. Researchers have found that the lures relate to "military, renewable energy, or business strategy themes." While the group appeared to be fairly active until 2019, their activity has either stopped or the group has been able to conduct attacks under the radar. Multiple APT groups attributed to China target the same verticals and geographies, indicating an **Even Chance** that APT24 was absorbed into other groups that are actively conducting campaigns.

In 2012, APT24 reportedly exploited known vulnerabilities and sent phishing emails with malicious attachments to deploy the Taidoor malware. From 2012-2013, APT24 allegedly targeted multiple organizations using the PittyTiger malware variant. From 2015-2016, APT24 reportedly exploited CVE-2015-2545 and sent a phishing email with a malicious attachment to the targeted victim. From 2017-2018, APT24 allegedly expanded their operations to Japanese organizations.

APT35

APT35 (aka Mint Sandstorm, Charming Kitten, Timberworm, UNC788) is an Iranian state-associated cyber-espionage group, specifically attributed to the Islamic Revolutionary Guard Corps (IRGC). The group has been active since at least 2014, with some reports dating them back to 2012. They are known for long-term, resource-heavy attacks. APT35 frequently targets critical organizations in areas of political interest to the Iranian government, like the U.S., Western Europe, and the Middle East. Target sectors include government, defense, transportation, health care, education, media, telecommunications, non-governmental organizations, technology, and energy.

From 2011-2014, APT35 reportedly targeted multiple organizations with compromised websites, phishing emails, and social media messages to gain control over victim devices and/or email accounts. In 2020, APT35 was attributed to Operation Bad Blood, a credential phishing campaign targeting U.S. and Israeli senior medical professionals. The group allegedly impersonated a prominent Israeli physicist.

In 2022, APT35 reportedly conducted phishing campaigns and exploited known vulnerabilities to gain initial access to victim environments. They then deployed ransomware variants, including BitLocker and DiskCryptor. Also in 2022, APT35 purportedly exploited the Log4Shell vulnerabilities to gain initial access to victim environments in the U.S. and the Middle East. The group stole sensitive data and deployed ransomware in the victims' environments. In 2023, APT35 allegedly used ISO images and possibly other archive files to initiate infection chains with victims. The group allegedly used Iraq-themed lures and targeted Israeli organizations, including ones in health care.

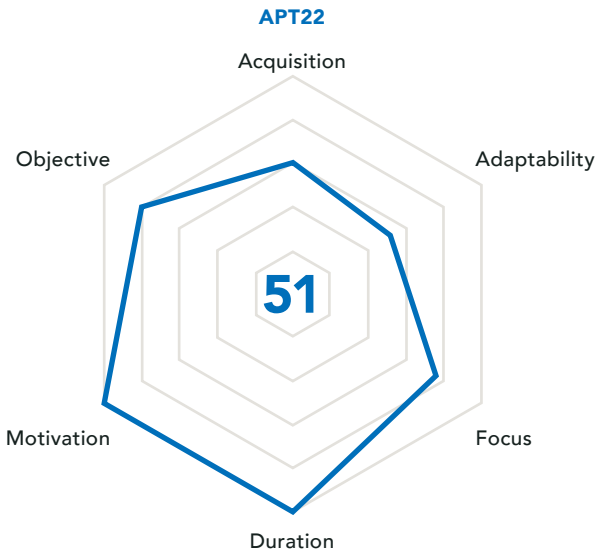

Figure 10: Threat Actor Metric™ score for APT35

Honorable Mentions

Andariel, a purported subgroup of Lazarus Group, receives an honorable mention due to their targeting of health care organizations. From 2016-2018, Andariel conducted Operation GoldenAxe, which involved a watering hole attack against at least 10 organizations' websites in the government, aerospace, education, health care, legal services, and financial services verticals. The group used ActiveX programs related to these verticals to infect the website visitors with multiple malware variants used to collect information. In 2018, Lazarus Group conducted Operation GhostSecret, which reportedly targeted organizations in the telecommunications, health care, financial services, media, and critical infrastructure verticals with spear-phishing emails containing a Destover-like implant designed to steal sensitive data.

APT41, a Chinese state-sponsored group, also receives an honorable mention for their targeting of the health care vertical. The group has targeted U.S.-based organizations focused on cancer research and biomedical and pharmaceutical companies. In 2019, APT41 reportedly targeted the same U.S.-based cancer research company targeted by APT22.

Ransomware Groups with Health Care Targets

In March 2020, when the COVID-19 pandemic hit, ransomware operators – including Clop, DoppelPaymer, Maze, Nefilim, and NetWalker ransomware – posted on their data leak sites and social media that they would not target hospitals and health care facilities during the pandemic. The impact on an already strained vertical would likely have had a significant and potentially fatal impact. Ransomware operators claimed that they "cared" and wanted health care professionals to focus on the virus and the care that citizens needed at the time. However, certain groups, including Clop, clarified that pharmaceutical organizations were not included in that exemption. They claimed that these companies made significant profits off the pandemic and thus would still be targeted. Ransomware operators that did target health care facilities often offered the decryption key for free and issued public apologies.

However, by April 2020, ransomware operators began targeting health care facilities again via VPNs—likely due to the significant increase in remote workers due to the pandemic. Additionally, April 2020 reports found that ransomware operators were using COVID-19 as lures to conduct successful phishing attacks. In September 2020, the DoppelPaymer ransomware operators targeted a Germany-based hospital. The attack caused the hospital to delay their care of a patient with a life-threatening condition—resulting in the patient's death.

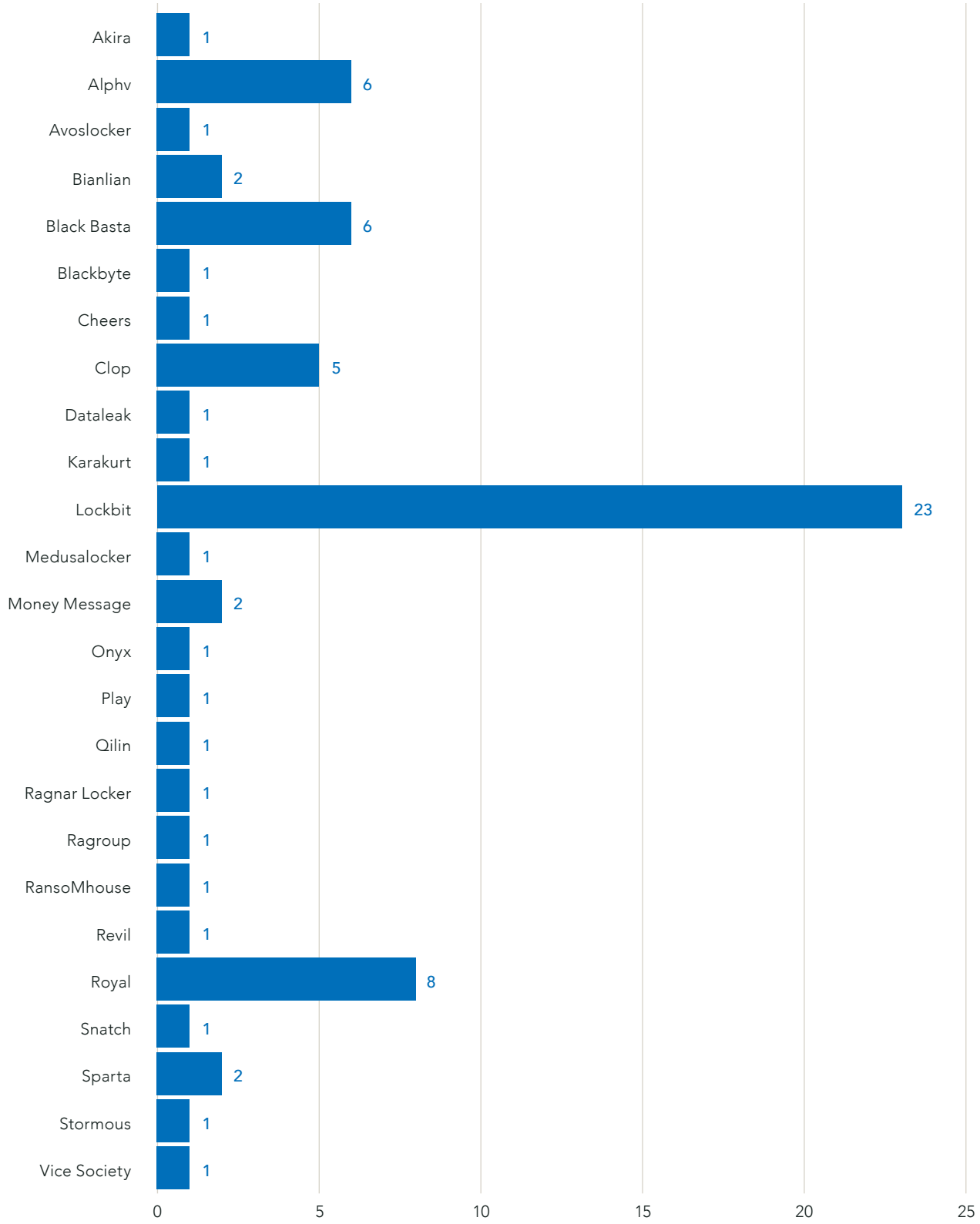

Figure 8: Ransomware variants that listed insurance organizations on their data leak site: June 01, 2022 - May 31, 2023

LockBit

Of the 890 victims listed on LockBit's data leak site from June 01, 2022, to May 31, 2023, 60 of them (6.7%) are in the health care vertical. In May 2022, LockBit operators named a Belgian private hospital group on their data leak site. The attack reportedly crippled their operating capacity severely and made patient records unavailable, while also reverting many processes to manual. LockBit operators threatened to publish 400GB of hospital and patient data if the ransom demand was not paid. Given that the victim was named on the site, the ransom was not paid.

In August 2022, LockBit operators named an Argentina-based medical care service provider on their data leak site and demanded a ransom of $300,000 to purchase or remove all exfiltrated data. They leaked the data—approximately 139.07GB of files. In December 2022, LockBit named a Canada-based hospital on their data leak site. Researchers report that the incident impacted "internal and corporate systems, hospital phone lines, and the website." LockBit later issued a public apology for the attack, claiming that the affiliate violated the group's rules, and released a free decryptor to the organization.

In January 2023, LockBit named a U.S.-based health care facility on their data leak site and gave them 13 days to pay $150,000 in ransom. The organization posted a press release on their website warning patients of a data breach. In April 2023, LockBit named a U.S.-based eye care provider on their data leak site and claimed to have exfiltrated their full database of medical records for all patients and data. The organization is no longer listed on the data leak site, indicating that the organization paid the ransom or began negotiations.

Alphv

Of the 326 victims listed on Alphv's data leak site from June 01, 2022, to May 31, 2023, 19 of them (5.8%) are in the health care vertical. In February 2022, Alphv named a U.S.-based eye care center on their data leak site and claimed to have stolen PII. The organization did not pay the ransom and the group leaked the purportedly stolen data, including screenshots of payment cards, insurance cards, and patient data. In April 2022, Alphv listed a U.S.-based physical therapy provider and claimed to have stolen nearly 90GB of data. The victim reported the data breach and stated that the potentially accessed information included names, social security numbers, electronic signatures, and credentials. The organization is no longer listed, but it is unknown if a ransom was paid. In September 2022, Alphv named a U.S.-based behavioral health provider on their data leak site and claimed to have stolen 313GB of data. The victim is still listed on the data leak site with screenshots of health assessments, patient information, and more.

In February 2023, Alphv named a U.S.-based health care provider on their data leak site and claimed to have been in the network "for a long time". The organization posted a notice on their website warning of the breach and that the attackers targeted a computer system used for patient images for radiation oncology treatment. The organization did not pay the ransom, and Alphv leaked the data on their site.

In March 2023, Alphv named an India-based pharmaceutical company on their data leak site, claimed to have 17TB of data, and argued that they were still active in the network. The organization's operations were interrupted due to required network isolation and recovery. Following the attack, the organization had a manufacturing problem and recalled thousands generic medication bottles, likely influenced by the interruption of processes. The company is still listed on the data leak site, indicating that no ransom has been paid. In May 2023, the group made two additional posts about the victim and leaked additional purportedly stolen data. In May 2023, Alphv named a U.S.-based health care provider and claimed to have stolen 4.7TB of data. The company released updates indicating that the incident was still under investigation, and they were close to resuming normal operations. The victim is listed on the data leak site, with 87 screenshots of purportedly stolen documents.

BianLian

BianLian ransomware, which has been active since at least July 2022, is written in Go, Google's open-source programming language. BianLian likely gets its name from an ancient Chinese dramatic art, where performers quickly alternate costume face masks "in the blink of an eye"—possibly alluding to the speed of a ransomware attack. The operators are not as active as LockBit, Alphv, and Black Basta. But they participate in double extortion, maintain a data leak site, and use a custom toolkit inclusive of homemade encryptors and encryption backdoors.

In March 2023, security researchers reported that BianLian had switched tactics from ransoming encrypted files to focus more on data-leak extortion. This change is **Likely** due to the January 2023 release of the decryption tool by Avast. Unlike other groups, BianLian operators appear to extensively research

their victims to tailor the threats. Initial access vector includes vulnerability exploitation, RDP, and weak credentials. The group has been observed dwelling on a victim network for up to 6 weeks prior to stealing data and encrypting files.

Of the 166 victims listed on BianLian's data leak site from June 01, 2022, to May 31, 2023, 25 of them (15.1%) are in the health care vertical. In October 2022, BianLian operators named a U.S.-based health care provider on their data leak site and claimed to have stolen sensitive information. The company reported the attack, and the Health and Human Services (HHS) disclosed that the breach impacted nearly 34,000 patients. In December 2022, BianLian named a U.S.-based hospital on their data leak site and claimed to have stolen 1.7TB of data. BianLian claimed that the victim began negotiations and then refused the payment, so the attackers leaked the purportedly stolen data.

In April 2023, BianLian named a U.S.-based ophthalmology provider on their data leak site and claimed to have stolen 170GB of files, including health information of patients, financial data of the practice, and human resources files. The incident was reported to HHS and allegedly affected nearly 36,000 patients. In May 2023, BianLian listed 4 U.S.-based health care providers on their data leak site. These included a clinic provider, an oncology provider, an ENT specialist, and a non-profit offering health care services to intellectually disabled adults and children. The group claimed to have stolen hundreds of GB of files, such as patient data, employee data, financial data, and more.

Clop

Of the 118 victims listed on Clop's data leak site from June 01, 2022, to May 31, 2023, 21 of them (17.8%) are in the health care vertical. Throughout March 2023, Clop ransomware operators listed victims compromised by exploiting the Fortra GoAnywhere vulnerability. A named victim was one of the largest health care providers in the U.S., who reported that the sensitive data of more than 1 million people was stolen. A Mexico-based pharmaceutical company also made Clop's list. The group has leaked a downloadable file of purportedly stolen PHI data.

In June 2023, Clop ransomware operators began listing organizations purportedly targeted by exploiting the MOVEit Transfer MFT solution. Victims included 3 health care organizations and a U.S.-based biotechnology company providing testing designed to identify viral and bacterial diseases. The company reported that Clop had acquired the confidential information of 2.47 million patients, including names, test information, and 600,000 social security numbers. A French diagnostic services company disclosed a Clop attack via a press release and stated that 4 laboratories, a small number of patients and staff, and old health data were accessed. Clop named an Austrian pharmaceutical company on their data leak site, but they have not disclosed the type of information accessed.

Karakurt

Karakurt is an English-speaking cybercriminal group, identified in June 2021, that conducts data extortion attacks without an encryptor. The group operates a data leak site, Magazine. Karakurt does not post proof of compromise or samples of the stolen data, but multiple victims have verified attacks. In February 2022, the group announced its intent to begin auctioning off victims' data on Magazine. Karakurt typically targets smaller US-based organizations and amends its TTPs depending on its victims' infrastructure. The group leverages PowerShell or Mimikatz if it cannot escalate privileges using valid credentials. Karakurt has reportedly attempted to escalate privileges through the ZeroLogon vulnerability, a flaw in the cryptography of Microsoft's Netlogon process that allows an attack against Microsoft Active Directory domain controllers.

In April 2022, Karakurt was linked to the Conti ransomware group. Researchers reportedly obtained access to a Russian-hosted Conti VPS server using credentials found on a threat actor's breached ProtonMail account. There, evidence on FileZilla confirmed that the Conti group accessed Karakurt's C2 server. While Conti operated as a typical ransomware variant, Karakurt has been assessed to act as the data extortion arm of the Conti umbrella. This is likely the result of diversification strategies by Conti. Blockchain analysis further confirmed the connection between Karakurt and Conti, as well as a potential connection between the Diavol, Conti, and Karakurt cybercriminal groups.

Of the 118 victims listed on Karakurt's data leak site from June 01, 2022, to May 31, 2023, 13 of them (6.6%) are in the health care vertical. In February 2022, Karakurt operators named a U.K.-based pharmaceutical company on their data leak site. The organization is no longer named on the site, but it is unknown if the ransom demand was paid. There is also an **Even Chance** that Karakurt auctioned off the data. In August 2022, Karakurt named a U.S.-based hospital network on their data leak site and claimed to have stolen 367GB of data, including

invoices, contracts, prescription scans, patient cards, and financial documents. The company released a breach notice and stated that some of the accessed information included patient PII and medical history, diagnosis, and treatment information.

In April 2023, Karakurt operators named a U.S.-based health care center on their data leak site and claimed to have stolen 453GB of files, including financial data, PHI, and PII of patients and employees. The organization released a breach notification confirming numerous types of stolen data. At the time of writing, the data has not been leaked. In May 2023, Karakurt operators named another U.S.-based hospital on their data leak site and claimed to have stolen 158GB of files. The data purportedly included PHI and PII of staff and patients, financial data, and more. The threat actors have not leaked the data at the time of writing, despite passing the ransom deadline of May 27, 2023. There is an **Even Chance** that the data is being or has been auctioned.

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	Type	Affected Software/Device	CVSS	Groups Observed Targeting
CVE-2012-0158	Buffer Overflow Vulnerability	MSCOMCTL.OCX library	9.3	APT24, APT34, APT41
CVE-2017-0199	RCE Vulnerability	Microsoft Office/WordPad	7.8	APT38, APT34, Andariel, APT41, MuddyWater
CVE-2017-11882	Memory Corruption Vulnerability	Microsoft Office	7.8	Kimsuky, APT34, APT41
CVE-2018-13379	Credential Exposure Vulnerability	Fortinet FortiOS SSL VPN	9.8	LockBit, Alphv, APT35, Fox Kitten, MuddyWater
CVE-2020-0688	Static Key Vulnerability	Microsoft Exchange	8.8	Kimsuky, APT34, MuddyWater
CVE-2021-26857	Deserialization Vulnerability	Microsoft Unified Messaging	7.8	APT35, APT31
CVE-2021-26858	RCE Vulnerability	Microsoft Exchange Server	7.8	APT35, APT31
CVE-2021-27065	RCE Vulnerability	Microsoft Exchange Server	7.8	APT35, APT31
CVE-2023-27350	Improper Access Control Vulnerability	PaperCut MF/NG	9.8	LockBit, Clop, APT35
CVE-2023-27351	Improper Authentication Vulnerability	PaperCut NG 22.0.5	7.5	LockBit, Clop
Log4Shell	RCE, DoS, DoS, RCE Vulnerabilities	Apache Log4j Java Library	10, 9, 5.9, 6.6	Karakurt, Alphv, APT35, Lazarus, Andariel, MuddyWater
ProxyLogon	RCE Vulnerability	Microsoft Exchange	9.8	Alphv, APT35, APT31
ProxyShell	Pre-Auth Path Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities	Microsoft Exchange	9.8, 9.8, 7.2	BianLian, Alphv, APT35
Spring4Shell	RCE Vulnerability	Spring Framework JDK 9+	9.8	Alphv, Black Basta
ZeroLogon	Privilege Escalation Vulnerability	etlogon	10	BianLian, Clop, Black Basta

Tool	Description	Groups Observed Using Tool
AdFind	A free command-line query tool that can be used for gathering information from Active Directory.	Royal, LockBit
Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.	Alphv, LockBit
Advanced Port Scanner	A free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.	BianLian, Royal, LockBit, Andariel
AnyDesk	A remote desktop application that provides remote access to computers and other devices.	BianLian, Karakurt, Black Basta, LockBit
Atera	A remote monitoring and network discovery tool that provides a comprehensive security scan and complete view of all your end-user networks and devices.	BianLian, Royal, Black Basta
Backstab	A tool that terminates antimalware-protected processes. It can be used to terminate EDR-protected processes.	Black Basta, LockBit
cmd	A program used to execute commands on a Windows computer.	Kimsuky, APT35, Granite Typhoon, Blind Eagle
Cobalt Strike	A post-exploitation tool that is often used during cyberattacks to deploy beacons.	Clop, Karakurt, Alphv, Royal, Black Basta, Granite Typhoon, APT38, APT31, APT41, MudyWater
DropBox	A cloud storage service that allows users to save files online and sync them to other devices.	APT35, APT31, Lazarus
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.	LockBit, Karakurt
FRPC	A modified version of the open-source FRP tool. It allows a system to provide network access to operators outside the victim network.	APT35, Fox Kitten, APT41
GitHub	An internet hosting service for software development and version control that has been used by threat actors to host malware.	APT35, APT31, Lazarus, APT41
GMER	A tool used to detect and remove rootkits.	Royal, LockBit
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.	LockBit, BianLian, Alphv, APT35
ipconfig	A command-line utility that is used to display and manage the IP address assigned to the machine.	APT35, Granite Typhoon, APT34, APT41
LaZagne	An open-source application used to retrieve passwords stored on a local computer.	Alphv, APT34, LockBit, MuddyWater
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 the security policy for the OS.	BianLian, Alphv, APT35, Granite Typhoon, Fox Kitten, APT31

Tool	Description	Groups Observed Using Tool
MEGASync	A cloud-based synchronization tool that is designed to work with the MEGA file-sharing service.	LockBit, Alphv, BianLian, Karakurt
Metasploit	A tool that can be used by threat actors to probe systematic vulnerabilities on networks and servers.	Alphv, APT35, APT38, APT31
Meterpreter	A Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.	Blind Eagle, APT31, APT41, MuddyWater
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.	LockBit, Karakurt, Alphv, Black Basta, Kimsuky, APT35, APT24, Granite Typhoon, APT38, Fox Kitten, APT34, APT31, Lazarus, APT41, MuddyWater
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.	APT35, Granite Typhoon, APT38, APT34, APT41
netcat	A utility tool that uses TCP and UDP connections to read and write in a network.	Black Basta, Granite Typhoon
NetScan	A utility that scans within a subnet or IP range to check for devices.	Royal, Granite Typhoon
Ngrok	A tool that exposes local servers behind NATs and firewalls to the public internet over secure tunnels.	LockBit, BianLian, Alphv, Fox Kitten
NirCmd	A command-line tool that can be used to manipulate a variety of setting son a computer, modify the registry, add shortcuts, and open the default internet connection.	Royal, Black Basta
NirSoft	A collection of tools that include password recovery utilities, network monitoring tools, command-line utilities, and more.	Alphv, Kimsuky, APT24
Nsudo	An open-source tool used to disable AV solutions.	Royal, Black Basta
PC Hunter	A toolkit for Windows with various powerful features for kernel structure viewing and manipulating.	LockBit, Royal
Ping	A tool used to test whether a particular host is reachable across an IP network.	APT35, Granite Typhoon, APT41
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.	APT35, Fox Kitten, Lazarus
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.	BianLian, Alphv, Royal, Black Basta, Kimsuky, APT35, Blind Eagle, APT31, Lazarus, APT41, MuddyWater

Tool	Description	Groups Observed Using Malware
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.	LockBit, Alphv, Kimsuky, Fox Kitten, APT31, Lazarus
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, Royal
PsExec	A utility tool that allows users to control a computer from a remote location.	LockBit, Alphv, Royal, Black Basta, Kimsuky, APT35, Granite Typhoon, Fox Kitten, APT34
PsList	Utility for viewing a list of processes currently running in the operating system.	APT35, APT34
PuTTY	A free and open-source terminal emulator, serial console, and network file transfer application.	LockBit, Alphv, Fox Kitten, Lazarus, Andariel
Rclone	An open-source, multi-threaded, command-line computer program to manage or migrate content on cloud and other high latency storage.	LockBit, BianLian, Karakurt, Alphv, Royal, Black Basta
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.	LockBit, BianLian, Clop, Alphv, Black Basta, Kimsuky, APT35, Granite Typhoon, Blind Eagle, APT38, Fox Kitten, APT41
ReadFile	A Windows API function that reads data from a specified file or input/output device.	Alphv, Royal
Reg	A Windows utility used to interact with the Windows Registry; it can be used at the command-line interface to query, add, modify, and remove information.	Granite Typhoon, APT34
ScreenConnect	Aka ConnectWise. A remote management software used to gain access to a remote computer.	Alphv, LockBit
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices.	BianLian, Alphv, 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.	LockBit, BianLian, Royal, Black Basta
SystemInfo	A Windows utility that can be used to gather detailed information about a computer.	APT35, APT34
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.	BianLian, Alphv, Kimsuky, LockBit

Tool	Description	Groups Observed Using Malware
TightVNC	A remote desktop software that allows users to access and control a computer over the network.	BianLian, APT38
Various Social Media Platforms	Twitter, Discord, Telegram, Facebook, LinkedIn, etc. These are often used to create fake personas, leak stolen data, claim responsibility for attacks, and more.	Kimsuky, APT35, Blind Eagle, Karakurt, 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.	Granite Typhoon, Blind Eagle, Fox Kitten, APT34, MuddyWater
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.	LockBit, Karakurt, Black Basta
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.	BianLian, Alphv, Black Basta, APT35, Granite Typhoon, Fox Kitten, Lazarus

Malware	Description	Groups Observed Using Malware
China Chopper	A web shell backdoor that allows threat groups to remotely access an enterprise network.	APT22, Granite Typhoon, Fox Kitten, APT31, APT41
DistTrack	AKA Shamoon. A worm that targets a system's MBR. Additionally, it has been used as a wiper malware.	APT35, APT34
gh0st RAT	A publicly available backdoor that was observed in Andariel attacks from 2015-2016.	Kimsuky, APT24, Granite Typhoon, APT31, Lazarus, Andariel, APT41
PlugX	A modular malware that calls back to a C2 server for tasking and is capable of download additional plugins and gather system information.	APT22, Granite Typhoon, Black Basta, APT31, APT41
PoisonIvy	A publicly available remote access trojan that can monitor victims remotely and steal user credentials and files.	APT24, Granite Typhoon
Qakbot	A banking trojan that has been used to steal victims' data, including keystrokes and credentials. Additionally, the malware has been used to deploy additional payloads.	Royal, Black Basta
Quasar RAT	A legitimate open-source RAT written in C# programming language and has been used to remotely access compromised devices.	Kimsuky, Blind Eagle

MITRE ATT&CK Technique	Behavior Category	Command/Process/Tool
T1566 – Phishing (Initial Access) T1204 – User Execution (Execution) T1589 – Gather Victim Identity Information (Reconnaissance) T1598 – Phishing for Information (Reconnaissance)	Phishing emails with malicious attachments and links requiring users to enable macros or interact.	Google Docs Microsoft Office Documents ISO Files Embedded Links
T1583 – Acquire Information (Resource Development) T1585 – Establish Accounts (Resource Development) T1588 – Obtain Capabilities (Resource Development)	Attackers acquire accounts and tools to help conduct the attacks.	Purchase servers Dropbox Google Drive GitHub Facebook/Twitter/LinkedIn Mimikatz Cobalt Strike
T1190 – Exploit Public-Facing Application (Initial Access) T1133 – External Remote Services (Initial Access)	Attackers often exploit known vulnerabilities in external remote services and public-facing applications to gain access.	Microsoft Exchange Cisco Fortigate VPN Citrix PulseSecure Outlook Web Access RDP
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)	Hide or manipulate features of artifacts to appear legitimate; delete or modify artifacts to remove evidence of their presence.	HKLM\SOFTWARE\ Microsoft\Windows NT\ CurrentVersion\Winlogon\ SpecialAccounts\UserList' /v -WindowStyle Hidden esentutl mshta.exe wscript.exe \Microsoft\Windows\ SoftwareProtectionPlatform\ EventCacheManager Remove-MailboxExportRequest KernelCallbackTable wevtutil cl System wevtutil cl Security
T1087 – Account Discovery (Discovery) T1083 – File and Directory Discovery (Discovery) T1082 – System Information Discovery (Discovery) T1018 – Remote system Discovery (Discovery) T1057 – Process Discovery (Discovery) T1016 – System Network Configuration Discovery (Discovery) T1033 – System Owner/User Discovery (Discovery) T1046 – Network Service Discovery (Discovery) T1049 – System Network Connections Discovery (Discovery)	Perform network/directory/user reconnaissance and enumeration.	Get-ManagementRoleAssignment net user net localgroup administrators net.exe users ipconfig /all >> %temp%\download NBTscan AdFind Net View Ping PlugX "cmd.exe" /C whoami Systeminfo file /bin/pwd tasklist /v

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

Outlook

Despite high-profile ransomware incidents and government/law enforcement attention on ransomware operations and facilitators, there is currently little motive for ransomware operations to cease. Ransomware operators have continued to operate and adapt throughout 2022 and into 2023. They are assessed to focus on continuing to build infrastructure and capabilities around themselves as one-stop shops, with less reliance on marketplaces and forums. This includes a shift from encryption to the theft of data that is stolen and held for ransom. Both Clop and BianLian operators have been observed conducting attacks in this manner, which makes the attack faster and still gives the threat actors leverage to begin negotiations.

State-backed and cybercriminal APT groups and campaigns usually involve data and systems destruction via wiper malware or the 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**, the financial services and health care 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+ year-old) vulnerabilities in popular public-facing software and services like VPN clients, RDP, Microsoft Exchange, and Oracle WebLogic. It is **Likely** that APT and ransomware groups will continue to target the financial services, insurance, and health care verticals over the next 12 months.

Want to learn more?

Visit **optiv.com**

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

800.574.0896 | optiv.com

Secure greatness®

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