GLOBAL RESILIENCE FEDERATION

Semiannual Ransomware Report

Jan ‘24 – JUN ‘24

*This document is released as **TLP CLEAR** for public review. **TLP CLEAR** information may be distributed without restriction, subject to copyright controls.*

Global Resilience Federation (GRF) is a nonprofit hub and integrator for support, analysis, and cross-sector intelligence exchange among information sharing and analysis centers (ISACs), organizations (ISAOs), and computer emergency readiness/response teams (CERTs). GRF's mission is to help assure the resilience of critical and essential infrastructure against threats that could significantly impact the orderly functioning of the global economy and general safety of the public. Learn more at www.GRF.org, by visiting @GRFederation on Twitter or Global Resilience Federation on LinkedIn.

Threat information sharing network partners:

LEGAL SERVICES ISAO

OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

K12 SIX

Business Resilience Council
by Global Resilience Federation

MFG-ISAC
Manufacturing Information Sharing and Analysis Center

ProSIX

EASE
Energy Analytic Security Exchange

ONG-ISAC Information Sharing & Analysis Center
Fueling the Exchange of Cyber Intelligence

H-ISAC™
HEALTH - ISAC

Kraft CERT

DNG-ISAC

national council of ISACs

Table of Contents

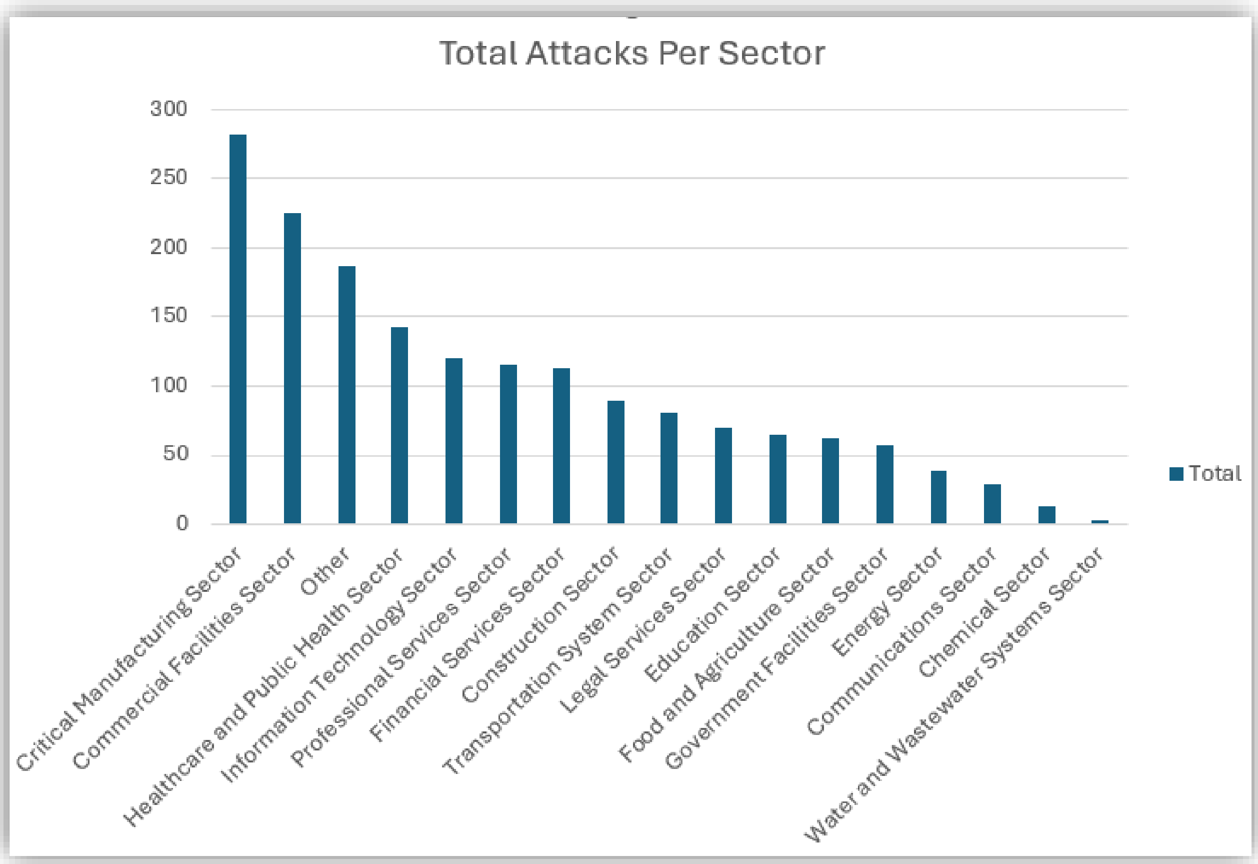
Executive Summary:

The Global Resilience Federation (GRF) Semiannual Ransomware Report analyzes the impact of major ransomware incidents and trends that have changed the security landscape in the first half of 2024 (H1), as well as probable trends and outcomes in the near future.

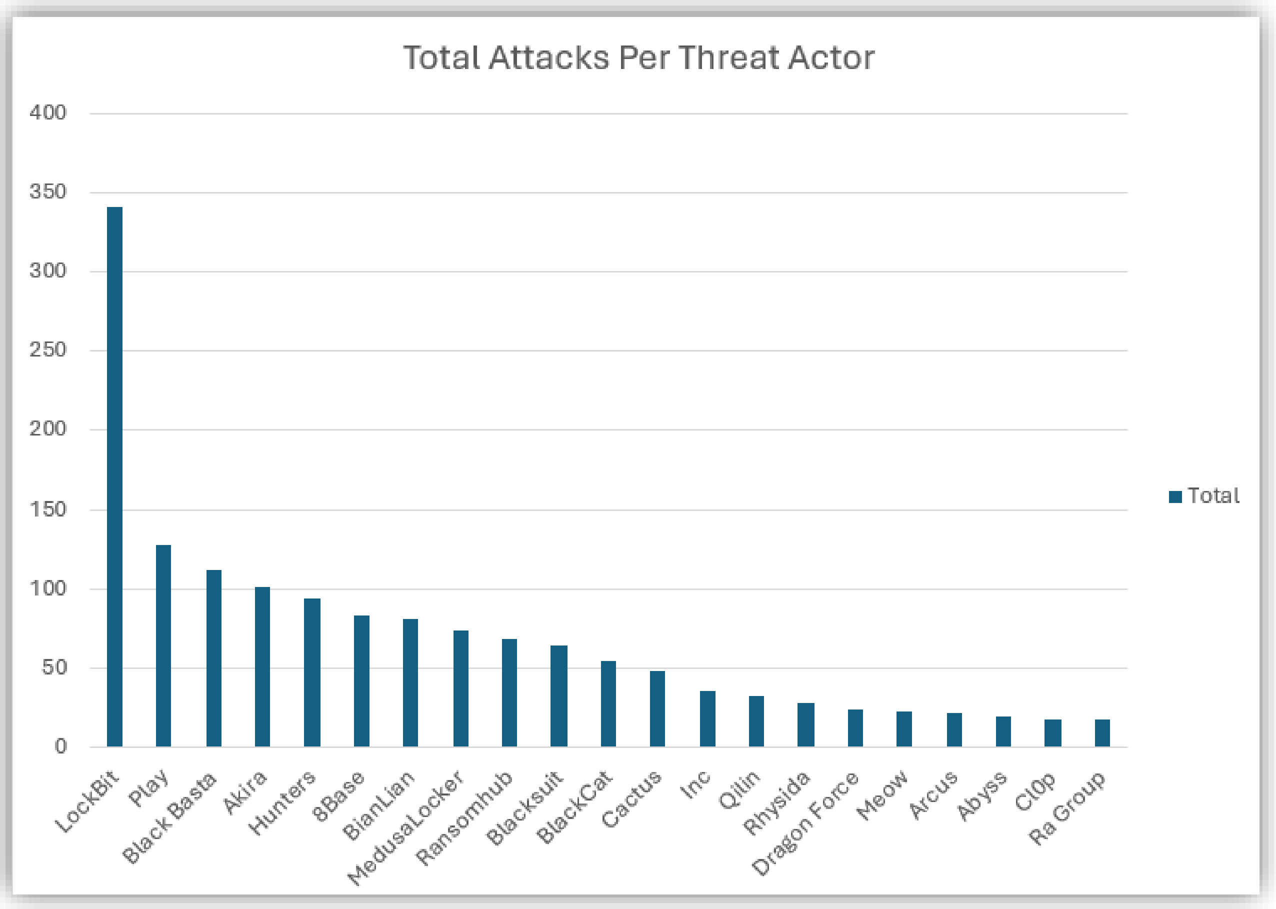
In the first half of 2024, GRF tracked more than 1,690 successful ransomware attacks, hereafter referred to as “attacks” or “incidents.” The top threat actor for H1 was the LockBit group with over 340 successful incidents, followed by the Play ransomware group with just under 130 attacks. The most targeted industry for H1 remained the Critical Manufacturing Sector with over 280 incidents, which is the fifth report in a row this sector was the top targeted sector. The Commercial Facilities Sector followed with over 215 victims.

The information and data in this report were gathered through a combination of open sources and research conducted by GRF analysts on criminal forums and marketplaces. Compromised organizations were categorized according to US Department of Homeland Security (DHS)-designated Critical Infrastructure sectors. Sectors not deemed critical by DHS, yet experiencing a large number of attacks, were broken into appropriate supporting infrastructure (e.g., Legal Services).

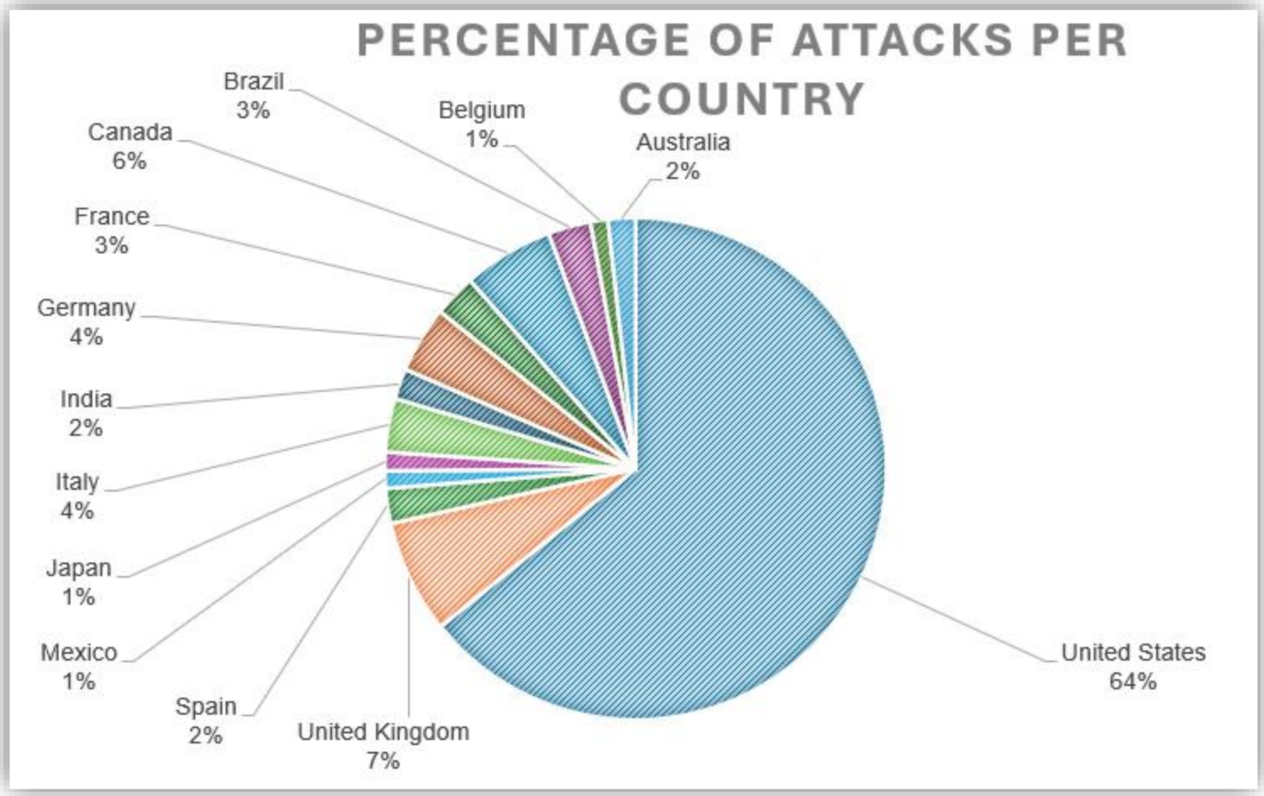
The charts below consist of the latest trends and activity in the ransomware landscape including top threat actor, top targeted sector, and most targeted country.



The top targeted sectors saw considerable overlap with the last Semiannual Ransomware Report, H2 2023. Critical Manufacturing and Commercial Facilities retained the top two spots, though the gap between them shrunk. Healthcare overtook IT, though both remained in the top five, and the Other category bumped Financial Services out of the top five, with it also being overtaken by Professional Services. GRF analysts believe this relative consistency in targeted sectors is due to the success that threat actors are having when attacking these industries. In particular, the top sectors like manufacturing and commercial facilities rely on being physically operational to make a profit, making these sectors a lucrative target for disruption and ransom. Outside of the top four sectors, threat actors seem to spread their attacks across different industries. GRF predicts that we will see a similar attack pattern going into the second half of 2024 unless a new threat actor emerges to heavily target a new sector. As noted, the Other category has risen in the rankings. This category includes all companies that don’t fall into an existing group tracked by GRF analysts. For instance, if an organization like a church were to be hit by a ransomware group, it would be listed under the Other category. The rise of the Other category may indicate a diversification of targets by threat actors, or an increased focus on targets of opportunity.


Total Attacks Per Threat Actor
400
350
300
250
200
150
100
50
0
LockBit
Play
Black Basta
Akira
Hunters
8Base
BianLian
MedusaLocker
Ransomhub
Blacksuit
BlackCat
Cactus
Inc
Qilin
Rhysida
Dragon Force
Meow
Arcus
Abyss
Cl0p
Ra Group
■ Total

The below graph shows the most targeted countries by ransomware threat actors in H1 2024. The United States was targeted by 64% of all ransomware activity tracked by GRF, an 8% increase from 2023. Next, 14% of all ransomware attacks were directed at countries within the EU, with the United Kingdom the next most targeted country at 7% of all activity tracked. The majority of attacks targeting the United States does not come as a surprise, since threat actors see the US as a lucrative environment with companies able to pay larger ransom amounts than smaller and less economically developed countries. Notably, threat actors also don't typically target regions like Russia and their allies, as actors often live in those countries and would be unlikely to be able to continue operations, targeting local industry.



NOTE: *The information and data in this report were gathered through a combination of open-source intelligence collection and research conducted by GRF analysts on criminal forums and marketplaces and may not be comprehensive. Only organizations directly confirmed in these forums to have been attacked were counted as incidents. GRF analysts believe, with a high degree of confidence, that the largest ransomware groups and most impactful attacks and their victims are included in this report.*

H1 2024 Statistical Trend Analysis:

A recent trend that GRF analysts have noticed is that threat actors are re-extorting their victims after they pay a ransom. While this is not a new concept, it was a rare occurrence due to the need for trust from victims, that if they were to pay a ransom demand then the threat actor would provide a decryption key and delete any stolen data; this trust allowed actors to perpetuate their model. In the past, threat actors like LockBit adamantly denied keeping any data after receiving a payment, but during Operation Cronos, law enforcement agent found servers containing sensitive data of victims who had already paid a ransom.[1] In recent months, threat actors have been double extorting their victims in cases involving a large ransom payment. In practice, the threat actor provides the decryption key and then later extorts the victim with the retained, stolen data. If threat actors continue re-extorting their victims, they will likely damage trust with future victims who will determine that paying a ransom, only to be extorted again, is not a feasible path forward. GRF analysts expect to see this tactic continue for new groups seeking a quick infusion of cash, or for groups that plan to shutter operations. It is unlikely that established ransomware groups that seek to continue operations will indulge in re-extortion.

Last Semiannual Report Trends:
In the last issue of the Semiannual Ransomware Report, GRF analysts covered multiple law enforcement takedowns that allowed new groups to emerge to fill the vacuum. Analysts stated that new groups would continue to appear as established groups were shut down by law enforcement. This proved true as groups like DragonForce and RansomHub, among others, began operations and launched worldwide attacks. This trend will likely continue as law enforcement operations continue to take down Ransomware-as-a-Service groups, and threat actors emerge to take advantage of this lucrative criminal strategy.

Another trend mentioned in the last issue of this report was the use of zero-day vulnerabilities. Threat actors continued to use zero-day vulnerabilities to breach victims' networks. This is not surprising as victims are defenseless to these types of attacks, and threat actors can often leverage them to pursue hundreds of victims in the short period before patching. Cl0p's use of zero-days in recent years has shown how successful this approach can be. GRF expects threat actors to continue to weaponize zero-days, and with the use of Generative AI, these attacks will become even faster to execute.

Nation-State Groups:

In this report, GRF analysts will highlight different nation-state groups that pose a major threat to United States-based organizations. While these nation-state groups don't normally leverage ransomware, they do use the same tactics and techniques that ransomware groups use in their campaigns. These nation-state affiliated adversaries include threat actors in China, Iran, and North Korea. While these countries comprise the primary origin of an outsized number of cyber threats, there are also prolific cyber gangs and nation-state actors emerging in other regions of the world, such as in Southeast Asia, Latin America, and Eastern Europe. However, this section of the report will focus on the traditionally prolific actors of major nation-state adversaries.

China – In terms of APTs, China has some of the most prolific actors in the world. They are extremely effective at infiltrating targeted networks and remaining undetected. In the past, Chinese-linked groups have tended to rely on nondestructive tools as they seem to be more interested in information gathering than typical ransomware-oriented motivations. Recently, a Chinese group known as the ChamelGang has started to deploy ransomware payloads in order to distract investigators from their true intentions of data theft.[2] While not new, this is a clever tactic since the group can not only gain the intelligence they seek and distract from their intentions, but gain additional operational financing through the extortion process. Another interesting development in the first half of this year was the adoption of AI in threat actors' attacks. Actors have been abusing AI to hone their scripting, social engineering, and understanding of cybersecurity tools.[3] Going into H2 2024, analysts expect Chinese threat actors to continue using AI models to improve their attacks.

Iran – In H1 2024, Iranian threat actors conducted a wide range of malicious cyber activities leveraging new tactics, from deploying new, custom backdoors to employing generative AI to support campaigns. In January 2024, Microsoft reported the Islamic Revolutionary Guard Corps (IRGC)-linked APT35 (also known as Mint Standstorm and Phosphorus), was observed targeting high-profile researchers from European and American organizations and universities with spear phishing attacks, deploying two new backdoor malwares, MediaPl and MischiefTut.[1]

In February 2024, a group called Homeland Justice claimed to have access to 100 terabytes of geographic information system and population data from Albania's Institute of Statistics (INSTAT). Neither INSTAT nor Albanian cyber officials confirmed Homeland Justice's involvement in the attack, though Albania's cyber agency (AKCESK) reached out to experts and collaborated with state police to help INSTAT recover the affected systems.[2] This incident is reminiscent of the attack on Albanian government networks conducted by the threat group between May and June 2022. In that instance, Homeland Justice launched ransomware on the networks, leaving an anti-Mujahideen E-Khalq (MEK) message on desktops.[3]

The same month as the Homeland Justice attack, Crimson Sandstorm (also known as TA456 or Imperial Kitten), also linked to IRGC, was observed targeting critical sectors with malware, weaponizing generative AI to improve the quality of phishing emails, developing code to evade detection, and enhancing scripting techniques to support application and web development.[4]

MuddyWater (also known as Mango Sandstorm and Static Kitten), once again tied to the IRGC, conducted a phishing campaign in early March 2024 targeting Israeli employees at large multinational organizations.[5] The campaign revealed some changes in MuddyWater's tactics, such as delivering malicious URLs in a PDF rather than linking the file in an email, and using a sender email account that matches the lure content.[6]

These attacks have not gone without response. As Iranian actors continue to target the US and other countries with ransomware, spear phishing, and social engineering attacks, the Department of the Treasury's Office of Foreign Assets Control (OFAC) acted by sanctioning six officials in the IRGC Cyber-Electronic Command in February 2024, and two companies and four more IRGC members in April 2024.[7,8]

Based on these recent activities, it is likely Iranian threat groups will continue to focus on critical infrastructure in adversary nations, using sophisticated malware and spear-phishing techniques, deploying ransomware for financial gain and operational disruption, and targeting military, government, and private sector entities to gather intelligence and strategic information. Lastly, amid ongoing geopolitical tensions, it is predicted that Iran will leverage cyber operations to attempt to sway public opinion and disrupt political processes ahead of the 2024 US presidential election, as seen by Iranian threat groups prior to the 2020 election.[9,10]

North Korea – North Korean cyber operations continue to be a global concern, characterized by sophistication, evolving tactics, and coordinated strategic objectives. North Korean cyber operations have advanced significantly, demonstrating increased technical sophistication and adoption of new tactics, techniques, and procedures (TTPs). Cyber operations conducted by North Korea are primarily aimed at furthering the regime's objectives, which include generating revenue through illicit means like cryptocurrency theft, gathering of intelligence, disrupting adversaries, and supporting broader geopolitical goals.

Groups like Moonstone Sleet, identified by Microsoft in May, have emerged and showcased advanced capabilities in ransomware deployment and complex malicious toolsets. The addition of ransomware capabilities, resembling other North Korean actors Storm-0530 and Onyx Sleet, suggests a shift towards disruptive operations.[4] Moonstone Sleet has demonstrated the capability to conduct multiple concurrent campaigns, utilizing robust malicious tools, and deploying custom ransomware variants, which indicates significant resourcing. The group also leverages techniques previously used by other North Korean actors, like the use of malicious npm packages observed in campaigns targeting software developers. Despite being a newcomer, Moonstone Sleet shows potential to mature and become a prominent threat actor conducting sophisticated cyber-attacks on behalf of North Korea.[5]

Notable Incidents:

Optum Subsidiary UnitedHealth Hacked by BlackCat

In February, UnitedHealth Group, a subsidiary of Optum health, was impacted by an attack from an affiliate of the ALPHV ransomware group.[6] The healthcare company provides a platform that is commonly used across the healthcare system for payment processing, care coordination, data analytics, and electronic health records in hospitals, pharmacies, and health clinics. The attack led to a major disruption in healthcare operations where their platform was used. The attacker leveraged compromised credentials to remotely access a Citrix portal which did not have MFA enabled. The ALPHV ransomware was deployed nine days after initial access, exfiltrating an alleged 6TB of data. UnitedHealth ultimately paid the ransom demand to ALPHV.

The ALPHV affiliate that originally launched the attack goes by the name “Notchy.” Notchy stated on RansomHub’s data leak site, a rival of ALPHV, that they would extort UnitedHealth again because ALPHV stole the full ransom demand of $22 million. Notchy threatened to leak data on the RansomHub site if a ransom demand was not paid, since they still had the data exfiltrated from the attack.[7] Notchy did ultimately leak data on RansomHub’s site which contained patient and billing information.

This incident has caused major repercussions in the ransomware industry as ALPHV broke the Ransom-as-a-Service (RaaS) model that operators have built up over the last few years. This RaaS model functioned on the premise that an affiliate would rent ransomware tools from a group like ALPHV, and after a ransom was paid the RaaS operator would keep a percentage of the money and forward the rest to the affiliate. With that business relationship broken by ALPHV, affiliates might be reluctant to work with other RaaS groups. This changing environment could lead to a few outcomes, including affiliates demanding more control over the ransom payment process or relying solely upon extortion after the RaaS group absorbs the ransom payment.

Ransomware Payments Drop to Record Low

Ransomware payments have declined to a record low in 2024, even as the number of ransomware attacks has continued to increase. Recent Coveware statistics showed that the average ransomware payment has dropped by 32%, even as the median ransomware payment increased by 25%.[8] Coveware reports threat actors may be avoiding high dollar demands of most victims, instead seeking smaller amounts to keep victims engaged and more likely to pay a ransom. This could be a reason why the average is dropping, but it is more likely due to victims not paying a ransom, with the percentage of companies choosing to pay dropping to an all-time low of 28% in 2024.[9] The reasons why ransom payments are down compared to earlier years are most likely due to better prepared victims, with better backups and greater security controls in place. Another reason is that organizations are becoming more skeptical that threat actors are truly deleting the exfiltrated data after receiving a payment, as highlighted by recent incidents in which a victim has been extorted again after payment.

Operation Cronos Disrupts LockBit

In February of this year, law enforcement officials executed an operation dubbed Cronos against the major ransomware group LockBit.[10] Law enforcement was able to infiltrate the ransomware group’s operation and gain control over the group’s data leak site and admin portal, later using the leak site to post information about the group and the arrest of some of its members. The disruption was a major blow to the group, with many affiliates departing to work with other Ransomware-as-a-Service offerors. Law enforcement was also able to seize around 200 cryptocurrency wallets, along with cryptographic keys to decrypt victim files, damaging the group’s financial position. While this operation did hinder LockBit for weeks, the group has set up new infrastructure.

Notable Sector Activity:

Legal Services Sector:

In H1 2024, GRF has tracked 70 ransomware attacks on the legal sector. The most active threat actors against the sector were BianLian and LockBit, both with 12 victims. Since the last GRF ransomware report, the sector has continued to be heavily hit by phishing attacks. This has been the largest threat to the sector for many years as it is commonly used to gain initial access or gather credentials for future attacks. With generative AI being used widely by threat actors, phishing attacks have become more challenging to spot, as once common grammar mistakes have dwindled. Threat actors will continue to target the legal sector since the type of data possessed by law firms can be highly sensitive in nature. Going into the second half of 2024, the legal space should focus on user education on ever-changing phishing practices.

Energy Sector:

The energy sector is not one of the top targeted sectors. The victimology tends to be outside on the ring of energy production, distribution, and retail sales. Most of the sector's victims are support service providers offering consulting, specialty equipment sales and services, and trade association benefits. It is not clear from the data that the victims were chosen because they were associated with the energy industry. Like with manufacturing, most of the victims were small organizations, lacking a strong information security or cybersecurity capability, and were most often in the United States.

However, in the last six months of 2023 there were several very large energy firms with gross revenue over $10 billion that fell victim to the Cl0p ransomware gang, including Siemens Energy, Hess Energy, and Energy Transfer Partners. In the first six months of 2024 there were 18 Cl0p victims, none in the energy space, and none that are global industry giants. The lone standout in 2024 was Brazilian electrical grid operator Equatorial Energia, and it was not attacked by Cl0p.

Equatorial Energia was unique as a victim in the energy space for at least three reasons. First, Equatorial Energia is a major producer and grid distribution operator of electricity in Brazil, with their grid providing electricity to 31% of the territory and 13% of all customers in the country.[11] Second, they are a large company with revenue around $5B in 2023. Third, they were attacked by a relatively unknown ransomware gang called Cloak. Cloak became active in August of 2023, gainging 28 victims over the five-month period to finish the year.

Until late March when Equatorial Energia was hit, Cloak had never had any Brazilian victims, nor have they since. This may be due to the suspicion that Cloak uses the services of Russian initial access brokers (IABs) for their activities.[12] These brokers allow them to gain access to numerous organizations around that world as IABs provide the initial foothold that threat actors need to access a network. These IABs typically don't target any specific sector or country. They simply seek to maximize their profits. Equatorial Energia is the exception to the rule that energy sector victims tend to be third parties. In the future victims will likely continue to be small firms, and non-energy producers and distributors.

Professional Services:

Trustwave SpiderLabs' 2024 report highlights a significant increase in cyber threats targeting the Professional Services sector, which includes consulting, legal, accounting, and management firms (Note: GRF separates Legal Services as its own industry vertical). The Professional Services industry's appeal stems from its wealth of sensitive data, including intellectual property and client information, which makes it a prime target for ransomware, supply chain attacks, and other sophisticated cyber threats.[13]

Ransomware attacks have notably surged within this sector, particularly in the United States where at least 142 firms were impacted in the past year. As noted in previous reports, cybercriminals view these firms as lucrative targets capable of paying substantial ransoms to restore critical client data and minimize operational disruptions.

Partner exposures are a concern in the sector, with attackers exploiting vulnerabilities in trusted third-party vendors to gain unauthorized access to sensitive data held by Professional Services firms. This approach capitalizes on the interconnected nature of business relationships within the industry.

In H1 2024, GRF saw a slight decrease in the number of attacks against the Professional Services sector. In H2 2023, there were 150 attacks compared to 116 in H1 2024. The top threat actors targeting Professional Services were Play with 19 victims, LockBit with 18 victims, Akira with 11 victims, and Black Basta with 9 victims. Play and Akira appear to be very interested in the Professional Services industry, with 15% and 11% of their total attacks targeting this sector, respectively.

Manufacturing Sector:

The threat of ransomware to the global manufacturing ecosystem remains very high. Manufacturing continues to be the top targeted sector for ransomware operators. The reasons for manufacturing being the most targeted have remained consistent over several years. Small and medium organizations in the US that lack cybersecurity and network segmentation between the front office IT systems and the plant floor OT system can quickly see manufacturing output impacted, while also having the insurance plans or funds to pay a ransom.

Historically, the demographics of manufacturing victims have remained fairly consistent, consisting primarily of midsized organizations. However, in this most recent period there has been a slight shift in the market, with small manufacturers becoming the most attacked group. The reason for this shift may not be financial incentives but rather that midsized manufacturers are increasingly hardening their systems, forcing a shift to easier targets.

The reasons that ransomware gangs target manufacturers are fundamental commonalities and challenges in the industry, and as such are not quickly changed. Cybersecurity posture and the logical and physical segmentation of networks will gradually change but still present an opportunity for threat actors. Despite this, there seems to be a growing awareness of both the problem and the corresponding set of solutions that need to be employed by the manufacturing community as a whole.

This understanding seems to be reflected in the data from the GRF ransomware reports. The last six months of 2023 saw 350 manufacturing victims while the first six months of 2024 saw 281, a 20% reduction in victims. It is too soon to make long-term predictions based solely on this data, but it is a welcome statistic that backs analysts' anecdotal experience with the sector. Hopefully this represents the first significant shift for the industry's security posture and resilience.

Education Sector:

Ransomware continued to be a significant threat for the Education Sector in H1 2024. Attacks against US school districts resulted in significant operational disruptions and school closures.[14] In response, in March 2024, the US Department of Education launched a Government Coordinating Council to facilitate cybersecurity collaboration across federal and local governments and agencies.[15] The Federal Communications Commission also approved a $200 million K-12 Schools and Libraries pilot program to provide eligible K-12 districts with universal service funds for cybersecurity improvements over the next three years.[16]

According to Trustwave SpiderLabs researchers, the top three ransomware threat actors targeting the sector in the last year – defined by Trustwave as K-12 schools, colleges and universities, and corporate training companies- were LockBit 3.0, Rhysida, and Cl0p.[17] In H1 2024, GRF saw 65 total ransomware incidents against the Education sector compared to 110 in H2 of 2023. The top threat actor was LockBit with 30 victims, which accounted for 9% of the group's total victims. Blacksuit had the second most victims with 7, accounting for 11% of their total victims. In the GRF H2 2023 report, it was noted that Rhysida ransomware group, the reported rebrand of Vice Society ransomware, had the second most attacks against the sector. They had previously been known to specifically target Healthcare and Education. However, in H1 2024 Rhysida had no victims in the Education sector and their total number of victims decreased from 49 in H2 2023 to 28 in H1 2024.

Operational Technology Sector:

In the first half of 2024, ransomware activity in the Operational Technology (OT) sector has exposed a complex landscape of both challenges and progress. The industrial sector, notably manufacturing, remains a prime target, suffering extensive disruptions from ransomware attacks. (Note: GRF separately tracks the component sectors in the OT category. This section of the report groups them together for trend analysis.) LockBit continues to dominate as the most active ransomware group despite a significant law enforcement intervention in February, Operation Cronos, that temporarily hampered their operations. Other prominent groups like Black Basta, Phobos, and 8Base have also shown resilience and adaptability, quickly exploiting new vulnerabilities and employing sophisticated attack methods.

The overall number of ransomware incidents in the industrial sector decreased in the first quarter of 2024 compared to the end of 2023. This reduction is linked to ransomware groups shifting their focus towards other sectors such as healthcare, and increased law enforcement actions. Despite this, the impact on OT systems remains severe, with many attacks causing significant operational disruptions. Notably, 37% of ransomware attacks affected both IT and OT systems, underscoring the critical interdependence of these infrastructures and the downtime that can result from penetration of just one side of technology.

The decline in attack numbers does not necessarily indicate a reduced threat. Instead, ransomware groups are evolving their strategies, focusing on more impactful and high-profile targets within the OT sector.[18] The rapid deployment of new ransomware variants and the exploitation of vulnerabilities in widely used platforms highlight the need for continued vigilance and advanced cybersecurity measures. Organizations in the OT sector must prioritize proactive security strategies, including regular vulnerability assessments and robust incident response plans, to mitigate the ongoing and evolving ransomware threats.

Oil and Gas Sector:

From January through June 2024, GRF analysts were able to track 78 ransomware attacks on the Oil and Natural Gas (ONG) industry from 26 unique ransomware groups. Of the attacks, 43 victims were ONG-related vendors, three were gas station chains, 12 were ONG upstream companies, 11 were ONG midstream companies, and three were identified as downstream companies. Additionally, three victim companies conducted both upstream and midstream operations and three other victims operated in both upstream, midstream, and downstream. (Note: GRF has chosen to break out the ONG sector for its own analysis as many of the threats to the sector are unique to what is seen in other energy verticals.)

LockBit was the most active ransomware organization with 16 separate attacks, primarily targeting ONG vendors, though the group also targeted upstream and midstream organizations. Black Basta followed LockBit with 10 claims, with victims ranging from ONG vendors to upstream, midstream, and downstream organizations. Hunters International and Play tied with seven attacks each, targeting a variety of ONG vendors, upstream, midstream, and downstream organizations.

The most attacks were made in May 2024 with 16 attacks followed by January and March which saw 15 attacks each, and 14 in February. The drop in attacks from March (15) to April (9) may be attributed to AlphV/BlackCat's exit scam that began in early March 2024. Interestingly, AlphV/Blackcat claimed a victim operating in the midstream space on February 12, 2024, and the same company was claimed again by LockBit in May 2024.[19] It is unknown if the victim's data was recycled from the AlphV/BlackCat claim or if they suffered a new attack by LockBit. It is also notable that no ONG ransomware incidents conducted by LockBit were found in June, which only saw nine total ransomware attacks in total. This may be due to the US Federal Bureau of Investigation, which reported ongoing efforts to disrupt LockBit operations, including obtaining over 7,000 decryption keys now being used to help victims reclaim data.[20] [21]

Ransomware Group Highlights:

LockBit

LockBit has remained the top ransomware group since the shutdown of Conti in 2022. The group has remained dominant, doubling the second highest threat actor's victim count. The group had 20% of all the tracked ransomware activity in the first half of 2024. This report has referenced the operation conducted by law enforcement that disrupted the group in February, but months later the group still seems to be operating, albeit not as smoothly. Going into the second half of 2024, analysts expect LockBit to continue operating and launching worldwide attacks. The group has proven to be resilient despite law enforcement efforts. It will be interesting to see if LockBit remains a top threat actor in H2 once the dust settles from Operation Cronos.

Play

Play is a ransomware group that tends to keep a low profile, avoiding media attention. When they do appear in the news, it often is related to a high-profile target such as critical infrastructure or a government entity. For instance, Play was behind the attack on Rackspace, a cloud computing provider.[22] This attack caused major outages in cloud-hosted Microsoft Exchange servers when the group exploited the ProxyNotShell vulnerability. Play also made headlines when they leaked files belonging to the Swiss government after attacking a Swiss technology and software company.[23] Play will most likely continue to keep a low profile in order to avoid major law enforcement action. While continuing operations they may choose to avoid critical infrastructure.

Black Basta

One group that has seen a lot of attention from law enforcement and media has been Black Basta. They are comprised of former members of Conti that split off in 2022.[24] CISA released an alert detailing TTPs and how the group executes attacks, relying heavily on phishing campaigns and recently using zero-day vulnerabilities to breach victims' networks. During the first half of 2024, the group had just over 110 victims. Going into H2 of 2024, GRF analysts expect this group will continue to be a major threat to organizations, worldwide. Black Basta has consistently been a top threat for the past few years.

This report was made possible with the support of GRF partners Accenture and Polyswarm.

accenture

POLYSWARM

Fresh Malware Intelligence

Appendix:

Open-Source Intelligence References

[1] https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html

[2] https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/

[3] https://www.bleepingcomputer.com/news/security/openai-blocks-state-sponsored-hackers-from-using-chatgpt/

[4] https://www.microsoft.com/en-us/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

[5] https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

[6] https://www.unitedhealthgroup.com/ns/changehealthcare/faq.html

[7] https://www.bleepingcomputer.com/news/security/ransomware-gang-starts-leaking-alleged-stolen-change-healthcare-data/

[8] https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024

[9] https://www.coveware.com/blog/2024/4/17/raas-devs-hurt-their-credibility-by-cheating-affiliates-in-q1-2024

[10] https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html

[11] https://www.equatorialenergia.com.br/home/

[12] https://cyberint.com/blog/other/cloak-ransomware-whos-behind-the-cloak/

[13] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/professional-services-sector-under-attack-trustwave-spiderlabs-report-2024/

[14] https://www.darkreading.com/vulnerabilities-threats/freehold-township-district-closes-due-to-cyber-incident, https://upnorthlive.com/news/local/traverse-city-area-public-schools-close-for-cyber-breach-investigation, https://www.kgw.com/article/news/education/oregon-central-school-district-cyberattack/283-b3ae13dc-f770-48f0-a0f5-fcb60629e772

[15] https://statescoop.com/department-education-k12-cyberattacks/

[16] https://www.govtech.com/education/k-12/fcc-approves-200m-pilot-program-for-k-12-cybersecurity

[17] https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2024_Trustwave_Education_Sector_Threat_Landscape.pdf

[18] https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q1-2024/

[19] https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html

[20] https://www.infosecurity-magazine.com/news/operation-cronos-lockbit-takedown/

[21] https://www.theregister.com/2024/06/06/lockbit_fbi_decryption_keys/

[22] https://www.bleepingcomputer.com/news/security/rackspace-confirms-play-ransomware-was-behind-recent-cyberattack/

[23] https://www.bleepingcomputer.com/news/security/switzerland-play-ransomware-leaked-65-000-government-documents/

[24] https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/black-basta