GLOBAL RESILIENCE FEDERATION

Semi-Annual Ransomware Report

June ‘21 – Dec ‘21

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

Hassan Shahzad | Jacob Standley | GRF

Global Resilience Federation (GRF) is a non-profit 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:

DNG-ISAC

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

EASE
Energy Analytic Security Exchange

OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

H-ISAC™
HEALTH - ISAC

ProSIX

K12 SIX

Kraft CERT

Business Resilience Council
by Global Resilience Federation

EE-ISAC

LEGAL SERVICES ISAO

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

NRF® NATIONAL RETAIL FEDERATION®

Elections Infrastructure ISAC®

national council of ISACs

Table of Contents

Executive Summary:

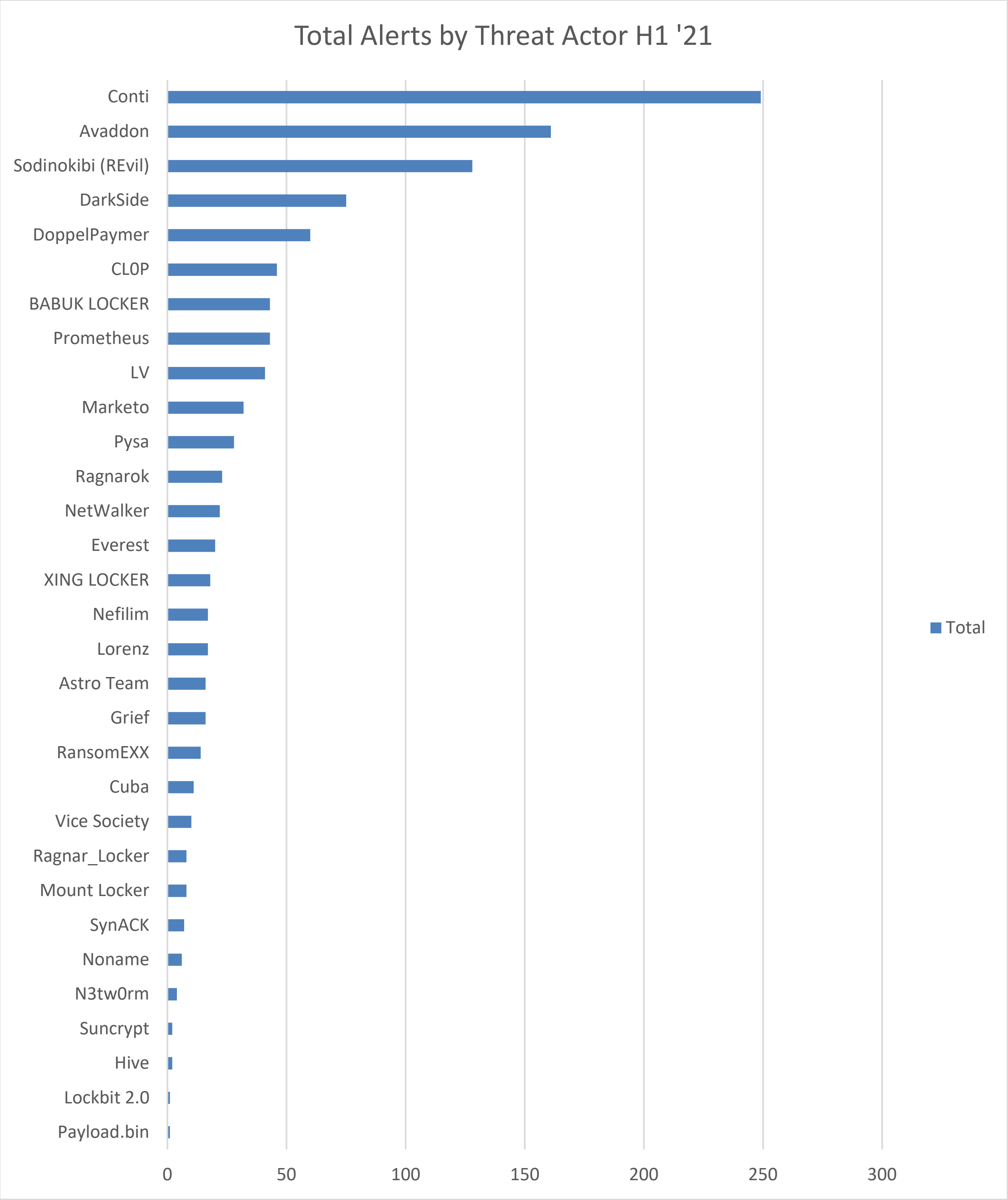
This report analyses the impacts of major ransomware events and outcomes that have shaped the ransomware landscape, as well as probable trends and future activity.

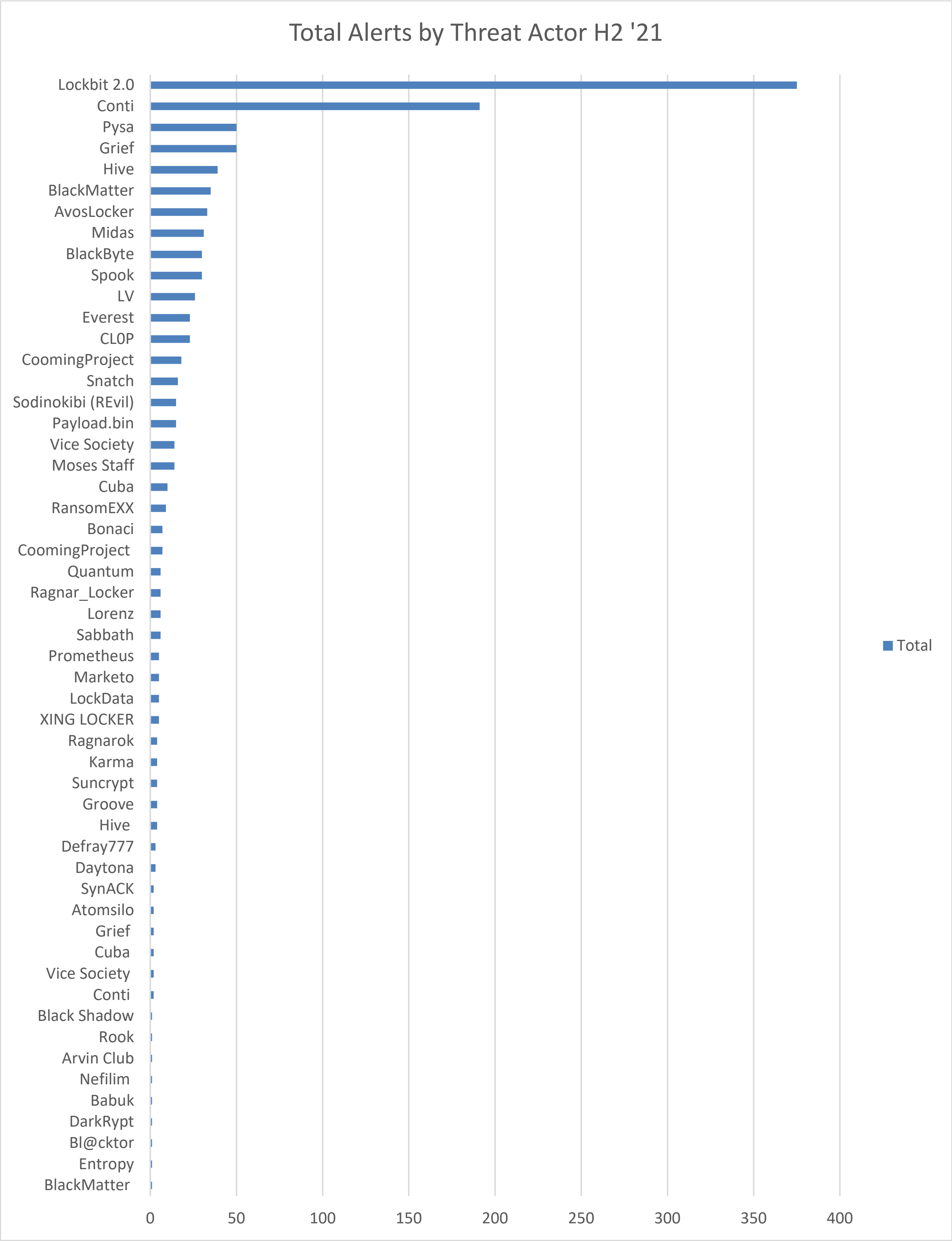
Global Resilience Federation tracked more than 2000 ransomware attacks in 2021 and observed over 1200 in the second half of 2021 (H2). The number of attacks executed in the first half of 2021 (H1) were primarily driven by Conti ransomware. Conti typically seeks targets of opportunity which tend to be small and medium-sized organizations. Conti has generally refrained from "whaling" after large enterprises. However, despite having the largest victim count for the first half of the year, other ransomware operations such as REvil and Darkside (Blackmatter) dominated the news cycle. H2 2021 saw a predominance of LockBit Ransomware as a Service (RaaS), which filled the vacuum left by REvil, Darkside and Avaddon after their closure. Additionally, GRF analysts observed the emergence of small-scale and politically motivated ransomware operations.

Critical Manufacturing, Financial Services, and Retail (Commercial Facilities Sector) continue to be the top three targeted sectors. However, GRF analysts anticipate that the Information Technology Sector will overtake the Financial Services Sector in number of ransomware attacks in 2022.

The information and data in this report were gathered through a combination of open-source intelligence collection and research conducted by Global Resilience Federation on criminal forums and marketplaces. Compromised organizations were categorized by U.S. Department of Homeland Security (DHS) Critical Infrastructure sector. Sectors not deemed critical by DHS, yet have significant number of compromises, were broken out into appropriate supporting infrastructure (e.g. Legal Services).

The charts below represent groups and trends in the ransomware industry, including the most active threat actors and most targeted industries.


Total Alerts by Threat Actor H1 '21
Conti
Avaddon
Sodinokibi (REvil)
DarkSide
DoppelPaymer
CL0P
BABUK LOCKER
Prometheus
LV
Marketo
Pysa
Ragnarok
NetWalker
Everest
XING LOCKER
Nefilim
Lorenz
Astro Team
Grief
RansomEXX
Cuba
Vice Society
Ragnar_Locker
Mount Locker
SynACK
Noname
N3tw0rm
Suncrypt
Hive
Lockbit 2.0
Payload.bin
0
50
100
150
200
250
300
■ Total


Total Alerts by Threat Actor H2 '21
Lockbit 2.0
Conti
Pysa
Grief
Hive
BlackMatter
AvosLocker
Midas
BlackByte
Spook
LV
Everest
CL0P
CoomingProject
Snatch
Sodinokibi (REvil)
Payload.bin
Vice Society
Moses Staff
Cuba
RansomEXX
Bonaci
CoomingProject
Quantum
Ragnar_Locker
Lorenz
Sabbath
Prometheus
Marketo
LockData
XING LOCKER
Ragnarok
Karma
Suncrypt
Groove
Hive
Defray777
Daytona
SynACK
Atomsilo
Grief
Cuba
Vice Society
Conti
Black Shadow
Rook
Arvin Club
Nefilim
Babuk
DarkRypt
Bl@cktor
Entropy
BlackMatter
0
50
100
150
200
250
300
350
400
Total

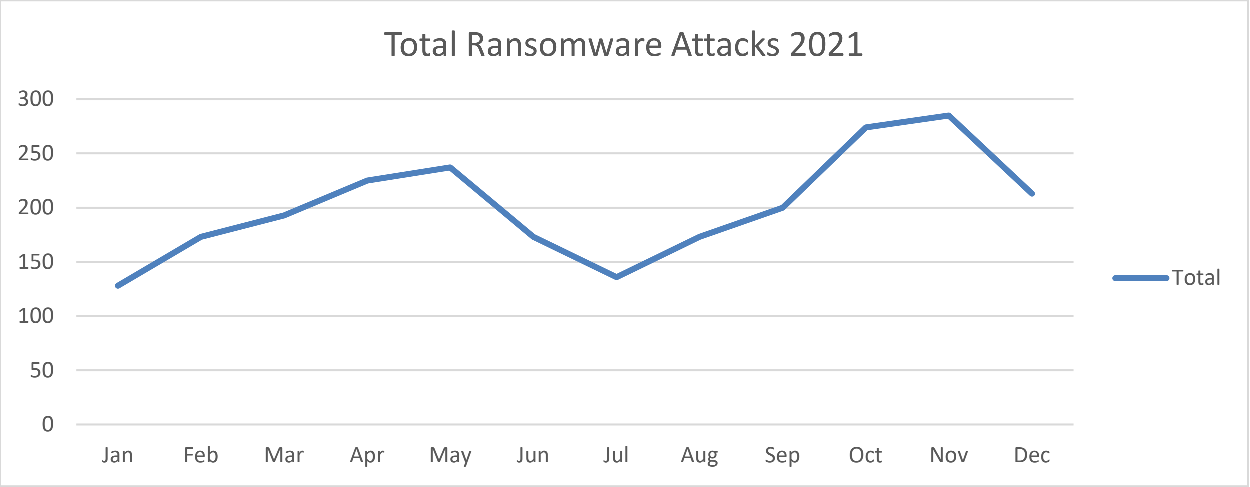
H2 2021 Statistical Trend Analysis:

Global Resilience Federation tracked more than 2000 ransomware attacks in 2021 and observed over 1200 in the second half of 2021 (H2). The number of attacks executed in the first half of 2021 (H1) were primarily driven by Conti ransomware. Conti typically seeks targets of opportunity which tend to be small and medium-sized organizations. Conti has generally refrained from “whaling” after large enterprises. However, despite having the largest victim count for the first half of the year, other ransomware operations such as REvil and Darkside (Blackmatter) dominated the news cycle. H2 2021 saw a predominance of LockBit Ransomware as a Service (RaaS), which filled the vacuum left by REvil, Darkside and Avaddon after their closure. Additionally, GRF analysts observed the emergence of small-scale and politically motivated ransomware operations.

Critical Manufacturing, Financial Services, and Retail (Commercial Facilitates Sector) continue to be the top three targeted sectors. However GRF analysts anticipate that the Information Technology Sector will overtake the Financial Services Sector in number of ransomware attacks in 2022. This is primarily due to the increasing attraction of supply chain attacks and the compromise of heavily leveraged third-party services.

In the previous report published July 2021, GRF analysts proposed that ransomware threat actors are shortening the development cycle to release new features and attack new exploits. In H2 2021, analysts continued to observe major vulnerabilities exploited by ransomware operators just days or even hours after disclosure. Analysts assess with a high degree of confidence that active ransomware operators continue to reinvest in their operations to increase operational and organizational maturity; the GRF team recommends organizations develop procedures to rapidly patch and mitigate critical vulnerabilities. Additionally, with more attacks being carried out through single use infrastructure, and the shuttering of REvil and Darkside, analysts assess that threat actors will invest in concealing and obfuscating attacks in the future, blurring the lines between nation-state and criminal operations.

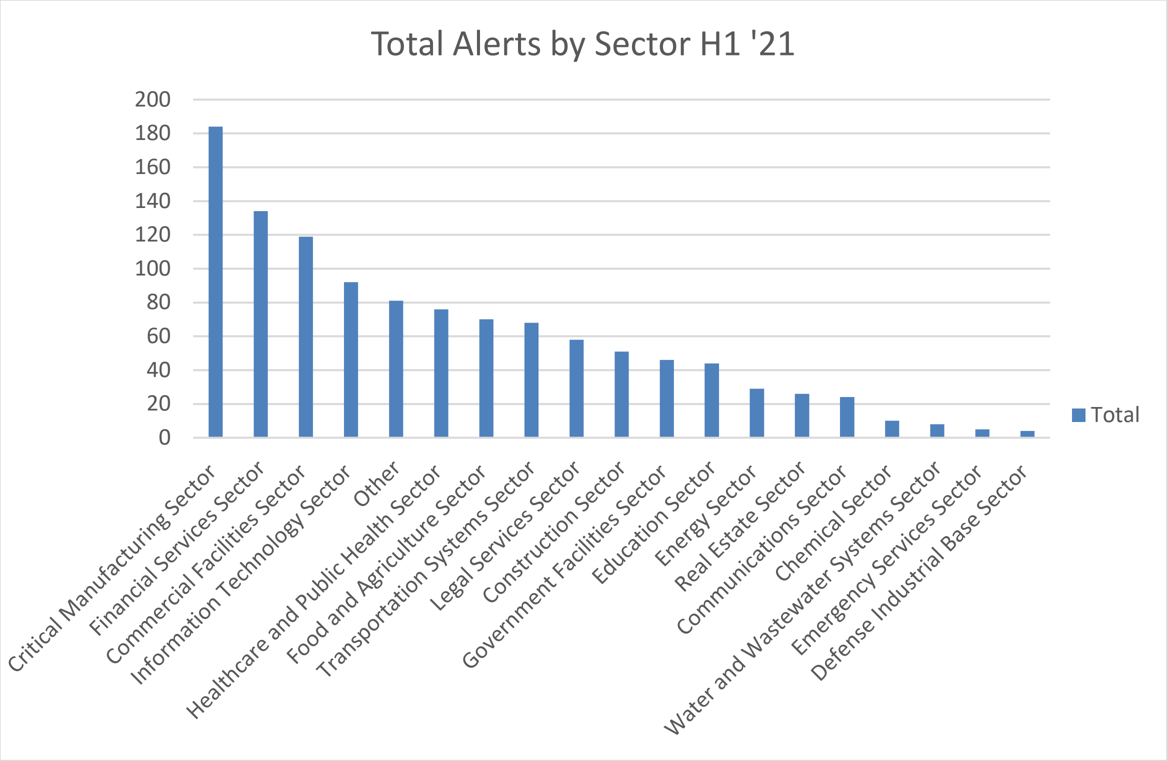
GRF analysts also believe that more medium-sized business will continue to be heavily targeted and that ransomware operators will avoid “whaling” operations against enterprises for much of 2022. This assessment is primarily due to ongoing law enforcement and intelligence agency actions against ransomware operators that have targeted Critical Infrastructure. If law enforcement activities continue to generate arrests and disrupt operations, analysts expect this trend to hold throughout 2022.

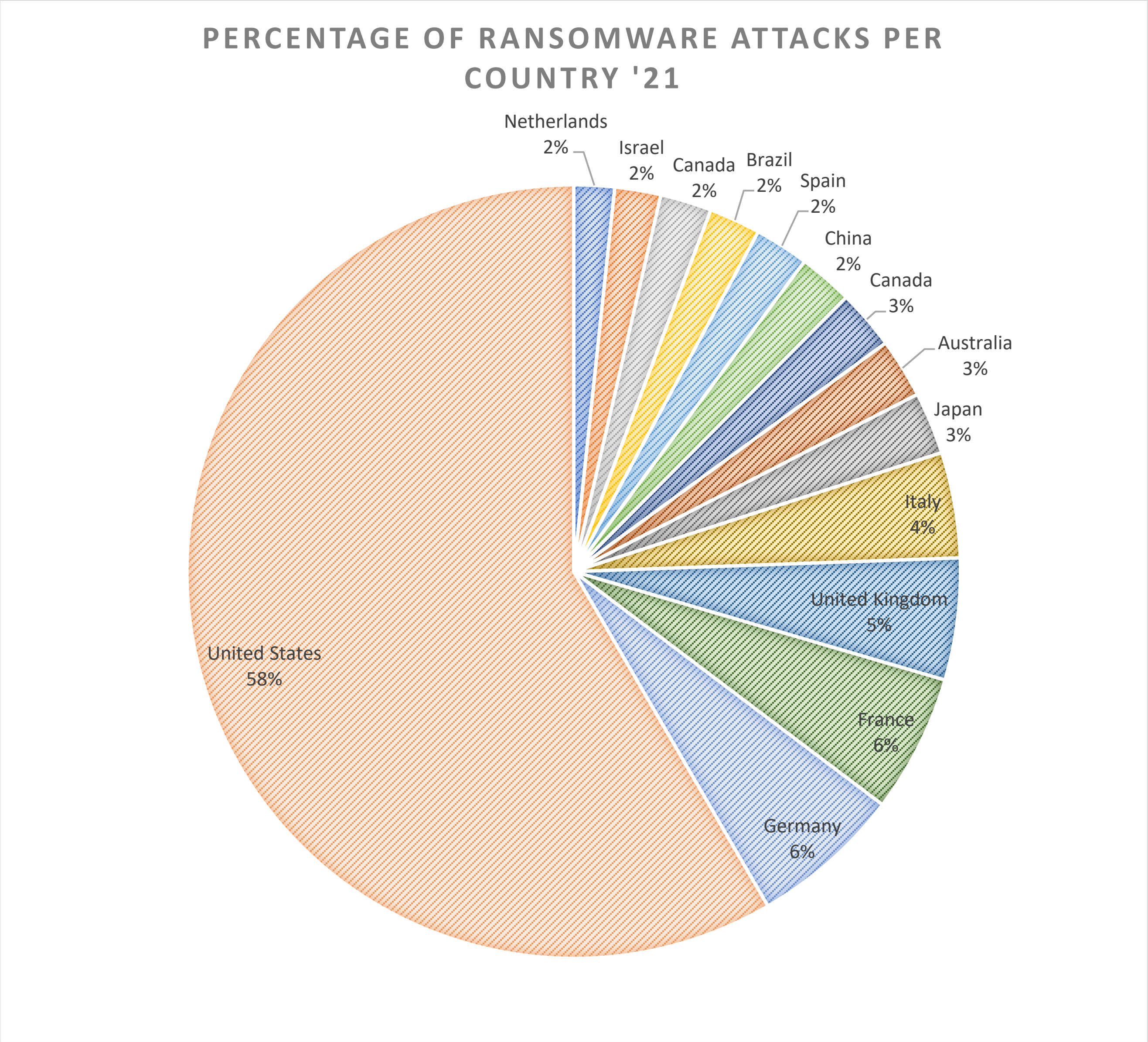


The above graph shows a climb in ransomware activity three months after the attack on Colonial Pipeline (May 2021). During the May to July period, several ransomware groups ceased operations due to media attention and increased pressure from law enforcement. However, beginning in August groups reemerged and operations such as LockBit 2.0 became the primary Ransomware as a Service (RaaS). This led GRF analysts to assess that ransomware group affiliates are becoming increasingly flexible with which RaaS operations they leverage. This trend could hinder investigative efforts as the number of initial access vectors and TTPs of ransomware operations are compounded by the willingness of affiliates to change “vendors” depending on needs.

GRF analysts have also observed the emergence of politically motivated ransomware being leveraged by extremist groups. Analysts assess with a high degree of certainty that ransomware will be further leveraged by extremist groups to carry out politically motivated attacks and fund operations with ransomware payouts. Moses Staff is one such group that security researchers have placed in this category and has been tentatively attributed to Palestinian or Iranian threat actors.[1] Moses Staff routinely carries out attacks against Israeli businesses and governmental organizations. It has also posted political messages on its blog site.

Some of the most targeted sectors by ransomware gangs continue to be Critical Manufacturing, Financial Services, and Commercial Facilities. The GRF team assess with a high degree of certainty that downtime-sensitive organizations will continue to be highly targeted. In addition, analysts anticipate financially mature organizations will continue to be targeted because of COVID-19 and economic turmoil. GRF analysts recommend planning for ransomware events in terms of both security and crisis management, and strongly recommend having business resilience plans in place in the event operations are impacted.





Some of the most hostile nations to U.S. Critical Infrastructure and supporting infrastructure remain Russia, China, Iran and North Korea. While these countries comprise the primary origin of a large number of threats, there are also prolific cyber gangs and nation-state actors emerging in other regions of the world such as Southeast Asia, Latin America, and Eastern Europe. However, in this section of the report we will focus on traditional and prolific actors, trends and targeting.

Russia – Russia continues to be a clear and immediate threat to western cyber interests. This threat has been further exacerbated by geopolitical tensions surrounding Ukraine. GRF assesses that Russia could leverage cyber-criminal organizations or ransomware tactics to disrupt U.S. and allied Critical Infrastructure in the event of a Ukrainian invasion. Russia continues to play host to a large cybercriminal ecosystem though recent efforts by U.S. and international law enforcement appear to be disrupting some elements. Operations including Avaddon, Darkside, and REvil have been successfully ended. However, despite these efforts, GRF analysts assess that Russian cyber-criminal organizations will continue to thrive. Other RaaS operations have filled the vacuum and continue to infect larger numbers of organizations. Analysts have also seen a shift on Russian speaking forums to collaboration with Chinese threat actors. A Conti spokesperson posted on elite criminal forums saying the group is looking for new threat actors to work with and would consider working with Chinese-speaking actors.

Iran – In H1 2021 the GRF team covered Iran's capability and use of destructive ransomware operations, and the Project Signal leak by Lab Dookhtegan detailing Iran's Islamic Revolutionary Guard Corps (IRGC) approach to ransomware activity.[2] In H2 2021 analysts began to observe some of these tactics against organizations in Israel. This activity coupled with retaliatory attacks has furthered the ongoing cyber conflict between Israel and Iran. This conflict has seen suspected Iranian threat actors leverage destructive ransomware attacks on Israeli organizations, and Israeli counter attacks on Iranian Critical Infrastructure. It is important to note that neither side has claimed responsibility, however GRF analysts assess that both nation-states either directly conducted the attacks or carried out attacks through third-party organizations. Some of the major operations include a shutdown of the Iranian railway system by a new wiper malware and later, a similar attack on the nation's gas stations which disrupted operations in more than 3,500 locations around the country. Both attacks have been attributed to Israel. On the other hand, we have seen major attacks from the group Moses Staff which has disrupted operations in multiple Israeli government organizations including the Israeli Ministry of Defense, with personal identifiable information leaked about Israel Defense Forces members. Although the group has not been directly linked to Iran, there have been connections made with groups like Pay2Key and BlackShadow, which are known Iranian nation-state threat actors.

China – Chinese state-sponsored cyber actors remain agile and mindful of the information security community's practices. These actors take effort to mask their activities and utilize critical vulnerabilities to infiltrate networks. They have been seen exploiting major applications like Pulse Secure, Apache, F5 Big-IP, and Microsoft products. Most recently it was reported that cyber groups originating from China were seen exploiting the critical vulnerability (CVE-2021-44288) in Apache Log4j. According to the U.S. NSA, CISA, and FBI these cyber actors have been routinely observed using a VPS as an encrypted proxy. The cyber actors use the VPS as well as small office and home office (SOHO) devices as operational nodes to evade detection.

North Korea – North Korean actors have been active since the beginning of the year, starting with targeting security researchers around the world using a zero-day, as well as breaching a South Korean atomic research agency by utilizing a VPN exploit. Their primary strategic goal is to further the Kim family rule through development of the economy and nuclear weapons program. All cyber-attacks by North Korean threat actors follow that pattern. For meeting their economic goals they have looked towards ransomware and within the last year have relied heavily on COVID-19 themed attacks. These operations are carried out by North Korea's supposed 9,000 cyber warriors, with a major portion enacted by the Bureau 121 threat group.[3]

Notable Incidents:

In the second half of 2021 we have seen significant incidents impacting multiple sectors. Some incidents have even crippled organizations around the world.

Kaseya Breach

At the beginning of July, one of the most significant ransomware attacks to date was conducted by REvil, a major ransomware groups at the time, and breached almost 60 MSPs. This was done by breaching Kaseya's VSA on-premises product through an update called "Kaseya VSA Agent Hot-fix." After breaching the MSPs, it spread to an estimate 1,000 businesses worldwide. REvil demanded $70 million USD in exchange for decrypting all devices. However, the victims did not pay the ransom and Kaseya was eventually able to obtain the decryptor through a trusted third party. Shortly thereafter REvil mysteriously shut down operations, briefly came back that September but has now stopped activities again.

Accenture Breach

The ransomware group LockBit reportedly breached the global IT consulting company Accenture in early August. It demanded $50 million USD in ransom for stolen data. The theft amounted to 6 TB of data which was then offered for sale. Accenture said it restored affected systems from back-ups and that there was no impact to operations or any of its clients' systems. In October 2021 Accenture confirmed theft of proprietary data during its fiscal reporting.

PrintNightmare

In July, Microsoft disclosed a critical zero-day vulnerability called PrintNightmare. The vulnerability could allow for a Windows domain server take over to deploy malware on a network. The vulnerability occurs within the print spooler service. There are two variants, one permitting remote code execution (CVE-2021-34527), and the other leading to privilege escalation (CVE-2021-1675). A third vulnerability was announced July 15 and upgraded to remote code execution by Microsoft in August.[4] Technical details and a proof of concept were leaked and the vulnerability has been seen exploited in the wild. Microsoft released an out-ofband patch and due to the severity of the exploit it also released patches for Windows 7 and Windows server 2012.

Log4j

In early December a critical vulnerability was discovered in Apache Log4j Java-based logging library. CVE-2021-44228, also known as Log4Shell, is an unauthenticated remote code execution vulnerability which can give threat actors complete access to a victim system. Additional exploits related to Log4j were discovered in December. CVE-2021-45046 could allow attackers to craft malicious input data using a JNDI Lookup pattern, which resulted in a denial-of-service attack. GRF analysts also saw another vulnerability in December, CVE-2021-44832. The vulnerability makes victims susceptible to an RCE attack when the configuration uses a JDBC Appender with a JNDI LDAP data source URI, when an attacker has control of the target LDAP server. The impact of the vulnerabilities in Log4j have been massive, with advisories from multiple government agencies. Major companies like Apple, Twitter, Tencent, Amazon, Tesla, Cisco, and others are known to have been affected. And in a quick turnaround, major ransomware groups like Conti and state sponsored groups like APT35 and APT28 have leveraged CVE-2021-44228 as an attack vector.[5] It is highly recommended to apply the most recent patch from Apache. [6]

Notable Sector Activity:

Energy Sector:

In H2, the electrical utility sector has seen a roughly similar level of targeting by ransomware operators, potentially because of the real or perceived downside risk of causing a significant outage event. Analysts believe these groups now fear the resulting repercussions from governments of victim nation-states. When utilities have ransomware incidents the corporate enterprise IT systems are typically the main target. This often has a major impact on company operations especially in the billing and customer service departments but does not usually result in utility service disruption to customers. As mentioned, government action is believed to have decreased the targeting of some Critical Infrastructure and there is reason to think that trend may continue.

Legal Sector:

The Legal Sector is still being heavily targeted by ransomware actors; the services law firms provide are extended to multiple industry verticals and present a third-party target for threat actors. Firms continue to be the target of sophisticated phishing campaigns but these attacks are widespread and don't tend to target specific people in an organization. Threat actors have been employing a tactic of spoofing another organization's email to give more credibility. Analysts predict that this method will become even more common as it has been successfully used to offer greater legitimacy.

Professional Services:

Accounting and consulting firms have become more common victims of ransomware attacks due to the sensitive data they retain and the high ransom amounts cybercriminals can collect. Last year, ransomware group LockBit 2.0 breached the global IT consulting company Accenture and demanded $50 million USD in ransom for stolen data. Professional Services companies in the UK alone have experienced 62 cyberattacks in the last 12 months, according to Keeper Security's 2021 Cybersecurity Census Report.[7] For these sometimes colossal organizations, work from home has also been considered a significant cybersecurity challenge. It has made the human security element more problematic. Clear IT policies and solutions such as zero-trust, segmentation and compartmentalization approaches to cybersecurity are now even more essential to preventing spread and limiting damage from an attack.

Manufacturing Sector:

Critical manufacturing continues to be a highly targeted subsector for several reasons. First the perception is that the risk of repercussions to the ransomware operator is not as high as a more directly vital sector like energy or water. Second, where IT manufacturing orders often result in the start of an OT process, the crippling of an enterprise IT network can have operational effects even if the operational network is not compromised which is an appealing and potentially easier to achieve impact for a threat actor. Third, the likelihood of victim payment is higher if operational impacts can be achieved. The future prospects for the manufacturing sector are likely more targeting, especially as IT/OT convergence increases.

Manufacturing represents an appealing target as its cybersecurity lags behind more mature sectors like the financial industry. A Varonis Manufacturing Data Risk Report highlighted that manufacturing was the 5th most targeted industry in 2020 and it is still underprepared for disruptive attack.[8]

Retail Sector:

In the summer of 2020, the IT services company SolarWinds was breached by threat actors affiliated with Russian intelligence. The actors were able to steal sensitive data by implementing compromised code into a software update which affected thousands of customers. Like SolarWinds, many other businesses including Accellion, Codecov, and Kaseya became software supply chain attack victims, which affects the third-party services used by hundreds or even many thousands of companies. A software supply chain is the code within the software and how it is traced back to original sources. It represents a method of penetrating one company to then impact all of its customers. Facing the seriousness of the threat, in May 2021, the Biden administration released a cybersecurity Executive Order which focused on improving software supply chain security, including creating new standards that companies must follow to sell to the federal government. With these threats at hand, retail companies must make software supply chain security part of their overall cybersecurity strategy. This is a difficult solution as retailers can have a large number of third-party operations within IT enterprises. However, companies can implement software maturity frameworks like NIST's Secure Software Development Framework to make key security practices part of their protocol.

Education Sector:

Ransomware gangs regularly target large networks belonging to firms, companies, hospitals, and cities in the United States. During the last few years however, K-12 schools have been increasingly targeted with cyberattacks. This can in part be credited to increased virtual learning due to the pandemic, and hackers' knowledge that most schools lack robust security measures to protect students, parents, and teachers. Because of a lack of regulatory requirements, parents are not always informed when schools are attacked, which can raise the risk of successful phishing emails or vishing calls from threat actors, or even worsen the threat of blackmail. For example, one parent in the Allen Independent School District of Dallas, Texas received messages that if his son's school did not pay a ransom, both his and his son's information would be released in the Dark Web.

It is important for schools to inform parents when any personal information is compromised; the number of education-related cyberattack incidents has increased and as of August 2021, ransomware attacks have hit 58 different education organizations and school districts[9]. Successful attacks damage K-12 school systems by not only holding personal information hostage, but also by disrupting students' education, causing increased financial costs to taxpayers for ransom payments and remediation, as well as increased insurance premiums.

Operational Technology Sector:

GRF analysts have seen more ransomware and exfiltration attacks on operational technology-using sectors, especially healthcare which according to U.S. Department of Health and Human Services saw a 170% increase in incidents from 2020 to 2021.[10] This could be due to medical systems and devices not being built with security in mind, thus presenting easy targets for threat actors. But according to a Sophos report, Healthcare is one of the sectors that is willing to pay ransoms. [11] This willingness to pay to restore system functionality may factor into to the popularity of this sector for threat actors.

The U.S. government has recognized the cybersecurity threats to operational technology using sectors and has sought industry partners to provide guidelines to enhance security. Thus far there have been guides created for healthcare, water, and transportation, with more guides to be published in 2022.

Ransomware Group Highlights:

Ransomware: BlackCat

A new ransomware group that goes by the name ALPHV or BlackCat popped up in early to mid-December. It has been dubbed one of the most sophisticated groups to emerge this year, with its ransomware seen promoted on major Russian-speaking sites. This group operates on the RaaS business model with affiliates earning up to 90% of the payout. The ransomware operates solely through command line and is highly configurable. It allows up to four different encryption modes ranging from fast encryption to slow-but-secure encryption. Unlike other ransomware operators, BlackCat has a separate login portal for third-party intermediaries to use for negotiations.[12] Within the past month analysts have confirmed more than 10 victims.

Ransomware: Rook

Rook is another new ransomware that arrived in December. Its most interesting trait is that it appears to be based off the infamous Babuk ransomware; researchers were able to find numerous similarities between the two. For example, it uses the same API calls to terminate processes. It also uses the same hardcoded list for terminated processes and Windows Services. The similarities continue to how it deletes shadow copies and uses the Windows Restart Manager API. Based on all of these similarities, researchers believe that Rook is based on the leaked code of Babuk rather than the idea that the Babuk operators started a new operation.[13] It is likely we will see Rook operations increase and fill the slots left behind by other infamous groups.

Ransomware: LockBit 2.0

LockBit had seen a major decline in activity due to increased attention from law enforcement. However, in H2 2021 GRF analysts have seen a return after an increase in recruitment and changed infrastructure. LockBit's reemergence in July filled gaps left behind by other major groups like Darkside, Avaddon, and REvil. With its return and revamped ransomware, it also listed of a number of new features including things like print bombing ransom notes on all printers on a network and utilizing group policies to encrypt a network. LockBit 2.0 is offering affiliates 80% of a ransom payment. Within six months of its return, the group has infected hundreds of networks putting it right behind Conti for the most victims in 2021.

Ransomware: Conti

Conti continues to be one of the largest ransomware groups currently active, if not the largest group. It has been very consistent with new victims counts. For targeting, this group appears to attack all sectors but has a focus on retail and manufacturing businesses. Conti has mostly remained the same from a TTP standpoint except it has recently become one of the ransomware groups using the Log4j exploit as an attack vector. It has been seen using this vulnerability to gain quick access to internal VMware vCenter Server instances and to encrypt virtual machines. Going into 2022 it is likely Conti will remain one of the most active groups.

Ransomware: Hive

Hive ransomware emerged midway through the year when there was a vacuum to be filled after the closure of Darkside and Avaddon. This new group flew under the radar for some time before becoming acknowledged as a sophisticated RaaS group that has since infected over 350 victims. Hive utilizes an admin panel to conduct all ransomware related tasks like ransomware deployment and negotiations. Regardless of its sophistication in some ways, victims have reported that even with the use of the decryption key some drives remained encrypted and unrecoverable.[14] Victims have appeared worldwide, in all sectors, but with a focus on the U.S.

Ransomware: Cuba

Cuba ransomware first popped up in late 2019 as an unknown group with few victims. However, it has since increased activity significantly. The U.S. Federal Bureau of Investigation has stated Cuba has targeted almost 50 organizations from U.S. Critical Infrastructure sectors and has collected over $40 million USD in ransom payments.[15] The ransomware itself is distributed through the loader called Hancitor. Once a victim is infected, the ransomware installs and runs Cobalt Strike while also downloading two executable files for password collection and writing to compromised systems TMP file. The ransomware uses stolen credentials to access RDP to compromise a network and runs a PowerShell script to allocate memory for the next payload. This payload is used to reach the C2 and deploy the next stage of files for the ransomware. Cuba is known for targeting companies and organizations in South America, the U.S, and Europe.

Appendix:

Open-Source Intelligence References

[1] https://www.cybereason.com/blog/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations

[2] https://www.flashpoint-intel.com/blog/second-iranian-ransomware-operation-project-signal-emerges/

[3] https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

[5] https://www.securityweek.com/chinese-iranian-state-hackers-exploiting-log4j-flaw-mandiant

[6] https://logging.apache.org/log4j/2.x/security.html

[7] https://www.keepersecurity.com/uk-cybersecurity-census-report-2021.html

[8] https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Manufacturing-Data-Risk-Report.pdf?hsLang=en

[9] https://www.edweek.org/technology/opinion-what-can-be-done-about-k-12s-looming-tech-nightmare/2022/01

[10] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[11] https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf

[12] https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/

[13] https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/

[14] https://blog.group-ib.com/hive

[15] https://www.ic3.gov/Media/News/2021/211203-2.pdf