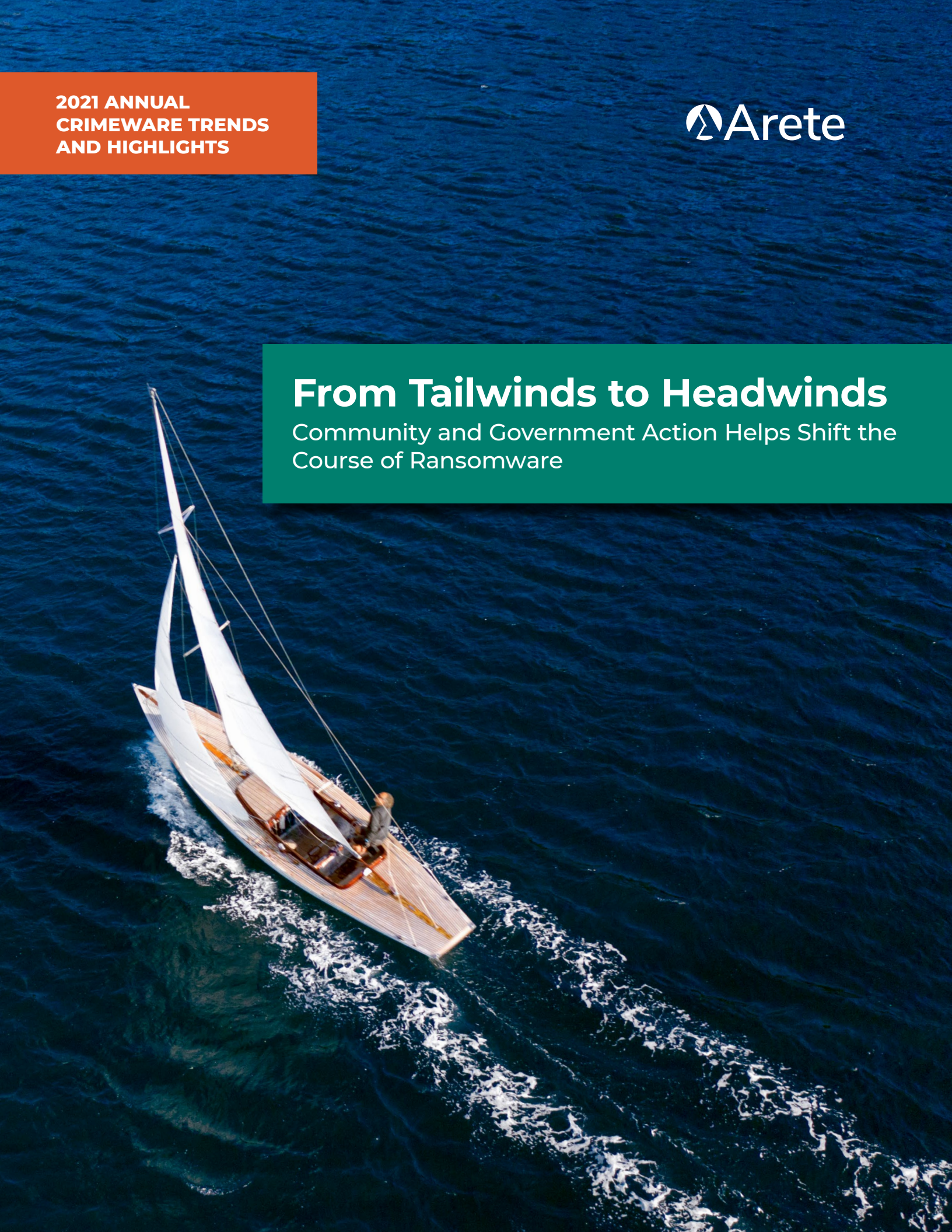
2021 ANNUAL CRIMEWARE TRENDS AND HIGHLIGHTS

Arete

From Tailwinds to Headwinds

Community and Government Action Helps Shift the Course of Ransomware



Executive Summary

At the time of writing this report, the conflict between Ukraine and Russia has been building and in recent weeks, has further escalated with Russia sending "peacekeeping troops" into the Donbas region of Ukraine. As the conflict continues to unfold and governments respond with economic sanctions, it is impossible to predict the cyber ramifications. While it is likely that Russia state-sponsored cyber activities will increase, it remains unclear if targets will be both government agencies and private organizations.

Over the past few years, cybercriminals have safely launched campaigns from the comfort of their home offices. Save for a few large-scale takedowns — for example, the dismantling of Slilpp, the largest marketplace for stolen credentials, and the arrests of REvil and Cl0p affiliates — this trend held steady throughout most of 2021.

Towards the end of the year, after law enforcement agencies — most remarkably, those in previously indifferent nation states, such as Russia and Belarus — became more aggressive in targeting criminal operations, some threat actors began to vocalize the need to stop conducting campaigns or operating forums. And while Russian and Belarusian motivations are unclear, their actions will likely spell change for where and how threat actors operate in Eastern Bloc locales.

This heightened government focus may not stop ransomware, but it will likely help ensure the shakeup of existing Ransomware-as-a-Service (RaaS) operating models. Some threat actors may choose to launch extortion-only campaigns to minimize "disruption" to their own operations, while others may explore new ways to improve their tradecraft to avoid identification. Those actors that do not adapt, however, will become easy targets for law enforcement. This extends to legitimate businesses that turn a blind eye to or do not follow internationally accepted know-your-customer practices.

Based on Arete case data, the commonly observed techniques and vulnerabilities of 2021 will likely not change through most of 2022. Thus, organizations should focus on patching and monitoring edge devices and on-premises Microsoft Exchange systems, which were favorite targets in 2021.

In the Arete Annual Crimeware Report, we will discuss:

- Notable tactics and techniques observed in threat actor campaigns.
- Notable negotiation insights gleaned from ransomware cases.
- How law enforcement has changed its game.
- How the threat landscape will evolve in 2022.

Annual Highlights

2021 HIGHLIGHTS FROM ARETE INCIDENT RESPONSE CASES*

- Phobos wants victims to show them the money — again and again.
- Hive: Their terms are non-negotiable.
- Conti operates like a well-oiled machine.
- Ransomware developers experiment with new coding languages.
- Overall, threat actors consistently exploit vulnerabilities in Microsoft Exchange and Pulse Secure devices.

OTHER KEY CYBERSECURITY EVENTS IN 2021

- The targeting of critical infrastructure by ransomware actors leads to enhanced government focus.
- Executive Orders drive governmental action on ransomware and international coalitions prioritize the fight against ransomware.
- The targeting of money laundering operations by law enforcement agencies slows cashouts.
- Russia makes moves to arrest cybercriminals involved in multiple aspects of ransomware operations.
- The No More Ransom project takes flight at the end of the year.

WHAT TO EXPECT GOING FORWARD

- To avoid unwanted attention from law enforcement, threat actors are unlikely to adopt further public-shaming tactics or target critical infrastructure. They will, however, look to apply more pressure to pay ransoms by augmenting their existing pressure tactics.
- International law enforcement agencies will increase pressure on actors through their continued targeting of money laundering infrastructure and collaboration with private sector organizations.
- RaaS affiliates will branch out to create their own groups or switch to extortion-only operations, possibly leveraging the successful models of groups like Karakurt and Midas. These changes will likely lead to vanishing "Big Game" RaaS operations.
- Threat actors will continue infecting victims who fail to regularly patch, remove unnecessary access, enable multifactor authentication, and deploy proper security software.

* Disclaimer: Unless otherwise noted, all data within this report is based on Arete incident response cases.

Notable Tactics, Techniques, and Procedures

RaaS: A DARK ENTERPRISE

While not new in 2021, RaaS operations continued expanding throughout the year. Much like with a regular business, RaaS operators create and post marketing content on the dark web, clearnet, and social media to entice affiliates to buy and use their ransomware.

These groups ran efficient operations that allowed them to adapt to every situation quickly, including leaking chats by researchers.

Across the board, ransomware groups upped the ante. Not only did they begin to launch a greater number of attacks with higher ransom demands, but they also began researching victims, adjusting initial intrusion methods, and streamlining operations. Arete commonly observed sophisticated groups completing an entire attack life cycle — from initial intrusion through data exfiltration and encryption — in less than 48 hours.

While members of different groups occasionally changed, the commonly observed tactics, techniques, and procedures did not. Some of these include:

SUPPLY CHAIN DISRUPTION: CRITICAL INFRASTRUCTURE, MANAGED SERVICE PROVIDERS, AND ZERO-DAYS

Throughout 2021, ransomware variants strategically exploited zero-day vulnerabilities, leading to high-impact supply chain disruption via managed service providers (MSPs) and their clients and mounting ancillary effects in the aftermath of initial exploitation, such as increased cost of goods, supply shortages, hospitals turning away patients, and law enforcement actions.

The world witnessed ransomware actors' ability to impact entire industries and supply chains with attacks that caused fuel shortages, led to ransom demands of hundreds of millions of dollars, and one attributed death at a hospital during system outages.[i]

Figure 1 Colonial Pipeline route. Source: CBC News

NOTABLE HIGH-IMPACT BREACHES

Colonial Pipeline

In May 2021, Colonial Pipeline suffered a Darkside ransomware attack that encrypted its network and forced the company to halt operations. The group accessed the network via a legacy VPN solution that lacked two-factor authentication.

The system outages caused gas shortages throughout the southeastern region of the United States, leading to panic buying and price spikes.

Colonial Pipeline purportedly paid nearly US$5 million in cryptocurrency to Darkside and roughly half was recovered by the Federal Bureau of Investigation (FBI). The recovery of funds was one of many efforts made by law enforcement to target how cybercriminals cashout illicitly gained funds.

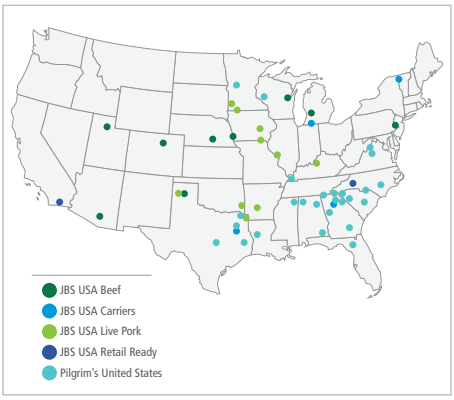


Figure 2 Map of closed JBS Foods processing plants. Source: Bloomberg

JBS Foods

In June 2021, the ransomware group REvil encrypted the networks of JBS Food, the world's largest meat supplier, and exfiltrated more than 45Gb of data via Megasync. Forced to close meat-processing plants throughout the United States, JBS moved quickly to pay the US$11 million ransom demand and avoid further supply chain disruption.[ii]

Kaseya

In July 2021, REvil carried out a large-scale supply chain ransomware attack against multiple MSPs and their customers by leveraging a vulnerability in Kaseya VSA software. The attack affected between 800 and 1,500 businesses and led to an original ransom demand of US$70 million for a universal decryptor.

Soon after, law enforcement targeted the group's infrastructure, causing the group to go dark for a short period before resurfacing. The group continued limited operations over a four-month period before officially halting operations in October 2021.[iii]

Notable Tactics, Techniques, and Procedures

DOUBLE EXTORTION

Threat actors have been using extortion tactics to pressure victims into paying ransoms since as early as 1989.[iv] This expanded to double extortion[v] tactics starting in 2020 and continued escalating in 2021.[vi]

TRIPLE EXTORTION

Throughout 2021, Arete observed multiple instances of triple extortion tactics by actors to pressure victim organizations. In particular, actors leveraged these tactics against victims they perceived to be too slow in their responses. Arete commonly observed actors threatening distributed-denial-of-service (DDoS) attacks against a victim's public-facing website. Suncrypt, for example, is one of many actors that leveraged DDoS threats during campaigns.

QUADRUPLE EXTORTION

Similarly, Arete also observed multiple instances of actors adding another layer. In several cases, threat actors directly reached out to victim employees, partners, or customers — via email, phone, or text — to inform them that they had breached the victim organization or simply, to further harass them.

Depending on many factors, including the pace of law enforcement action, Arete assesses that quadruple extortion will possibly be commonplace before the end of 2022. These tactics increase the chances of victims paying ransoms and, if they do not, actors look to other ways to monetize any stolen data such as the dark web.

"Soon enough, attackers will be doing it all — fully compromising victims, selling off their data in pieces to the highest bidders, sapping their processing power to mine cryptocurrency, threatening to ruin their reputations. Encryption and doxing are just the beginning."

– Roger Grimes,
KnowBe4 data-driven defense analyst[vii]

EXTORTION-ONLY GROUPS

Once commonplace, extortion-only groups had presumably died off, replaced by ransomware groups who could pressure victims into pay ransoms by encrypting systems. With the advancement of extortion tactics, however, Arete observed a resurgence of extortion-only groups in late 2021. These groups focus on exfiltrating data before applying extortion tactics.

One group to note is Karakurt, an unpredictable group that disappears during negotiations, does not always identify themselves, and is at the forefront of leveraging quadruple extortion in their operations. Karakurt has risen through the ranks to become one of today's most well-known names that targets victims opportunistically.[viii]

Arete assesses that extortion-only groups will continue a consistent pace of attacks, exfiltrating data and contacting victims to "get their files back." Their numbers will directly correlate to the disappearance of large RaaS offerings due to law enforcement action or loss of trust in the model between cybercriminals and money laundering operations, such as mixers, due to governmental sanctions.

Notable Tactics, Techniques, and Procedures

TIME TO LEARN A NEW LANGUAGE

Another notable change in 2021 was the appearance of ransomware variants using non-typical languages as a reaction to security controls increasingly detecting ransomware variants.

Examples include:

- Rust – APLHV BlackCat[ix]
- Dlang – Vovalex
- GoLang – HelloKitty and TellYouThePass[x]

Threat actors will likely continue producing new variants in non-standard programming languages not only because they are harder for security appliances to detect but also allow actors to minimize vulnerabilities in their code.[xi]

COMMONLY OBSERVED TTPs AND TOOLING

The following are the Arete commonly observed TTPs or tooling in ransomware cases:

Cobalt Strike

Cobalt Strike is a commercial software utilized by red teamers and often stolen by ransomware actors, who use the product's beacons (default malware payloads) to create a connection to the team server, which allows them to maintain persistence or deliver other tools, including ransomware payloads, to a victim environment. [xii]

Shadow Copy Deletion

In the past, only the most sophisticated ransomware groups were able to consistently delete shadow copies, which helps prevent restoration from backups. Today, however, shadow copy deletion is a common practice of nearly all ransomware variants. [xiii]

Remote Access

Remote access threats drastically increased as companies shifted employees to working from home and thus, expanded the company attack surface. Unsecure remote desktop protocol (RDP) connections and flaws in virtual private network (VPN) appliances remain a common initial access method for actors.

New Vulnerabilities

In 2021, the attack surface continued to grow as the addition of new systems and technologies, including internet of things (IoT) and cloud services, helped increased the number of potential access points for cybercriminals. Not only was 2021 a record-setting year for new zero-day vulnerabilities but also for the number of vulnerabilities exploited in the wild.[xiv]

Arete's most commonly observed vulnerabilities exploited by ransomware actors included the following:

MICROSOFT EXCHANGE VULNERABILITIES

As one of the most used email servers across the world, Microsoft Exchange was an attractive target for attackers.

PROXYLOGON

ProxyLogon is a series of Microsoft Exchange server vulnerabilities that, when chained together, allow an attacker to achieve full remote-code execution.[xv]

First Disclosed	CVE-ID	MITRE ATT&CK Phase	Threat Actor Types Leveraging	Description
March 2021	CVE-2021-26855	Initial access	APT and ransomware groups	Server-side-request-forgery (SSRF) vulnerability
	CVE-2021-26858 CVE-2021-27065			Arbitrary file write vulnerabilities
	CVE-2021-26857			Insecure deserialization vulnerability

Table 1 ProxyLogon vulnerabilities

PROXYSHELL

ProxyShell refers to another set of Microsoft Exchange Server vulnerabilities that allow threat actors to bypass authentication and execute code as a privileged user.

First Disclosed	CVE-ID	MITRE ATT&CK Phase	Threat Actor Types Leveraging	Description
July 2021	CVE-2021-34473	Initial access	APT and ransomware groups	Microsoft Exchange Server RCE vulnerability
	CVE-2021-34523			Microsoft Exchange Server elevation of privilege vulnerability
	CVE-2021-31207			Microsoft Exchange Server security feature bypass vulnerability

Table 2 ProxyShell vulnerabilities

WINDOWS MSHTML

In September 2021, Microsoft disclosed the Windows MSHTML vulnerability[xvi] CVE-2021-40444 as a zero-day observed in limited attacks. The vulnerability allowed attackers to use specially crafted Microsoft Office documents to perform remote code execution.

After Microsoft published its advisory, threat actors reproduced the exploit and shared detailed technical information on hacking forums. Within a few days, ransomware operators (e.g., Conti, Ryuk, and Magniber) incorporated MSHTML exploits into their arsenals as a new way to gain initial access.[xvii]

PULSE CONNECT SECURE

Malicious actors are known to use VPN appliances as an intrusion vector, and the Pulse Connect Secure VPN[xviii] has a set of vulnerabilities that are widely exploited.

First Disclosed	CVE-ID	MITRE ATT&CK Phase	Threat Actor Types Leveraging	Description
May 2019	CVE-2019-11510	Initial access	APT and ransomware groups	Arbitrary file reading vulnerability
September 2020	CVE-2020-8243			Arbitrary code execution vulnerability
October 2020	CVE-2020-8260			Arbitrary code execution vulnerability
April 2021	CVE-2021-22893			Authentication bypass vulnerability

Table 3 Pulse Connect Secure vulnerabilities

Malicious actors used the vulnerabilities listed in Table 3 to gain initial access into many victim networks throughout 2021, and they continue to leverage all of them as integral components in their arsenals.[xix] Moreover, ransomware operators will continue targeting edge devices, such as VPNs and firewalls, in 2022.

PRINTNIGHTMARE

PrintNightmare[xx] is a class of security vulnerabilities that impact the Windows Print Spooler service, Windows print drivers, and the Windows Point and Print feature.

First Disclosed	CVE-ID	MITRE ATT&CK Phase	Threat Actor Types Leveraging	Description
June 2021	CVE-2021-1675	Privilege escalation	Mainly ransomware groups	Windows print spooler RCE vulnerability
July 2021	CVE-2021-34527			
August 2021	CVE-2021-36958			

Table 4 PrintNightmare vulnerabilities

The PrintNightmare exploitation initially surfaced due to an accidental leak of a proof of concept (PoC) exploit by a security researcher in June 2021. Arete observed groups such as Vice Society and Magniber ransomware leveraging PrintNightmare in operations.

STATE OF ZERO-DAYS

In 2021, the number of disclosed zero-days increased from previous years, a trend that is unlikely to change in 2022. Ransomware actors did, however, focus on a few types of vulnerabilities to exploit as part of their campaigns.

- Vulnerabilities affecting edge devices to bypass authentication and network controls.
- Vulnerabilities easily chained together to gain initial access and maintain persistence in one go.
- Vulnerabilities in software with a high number of known instances.
- Vulnerabilities in software used by managed service providers.

UNDERGROUND FORUM DISCUSSIONS

Based on underground and dark net forum observations, cybercriminals were sharing and selling technical details and tools to exploit many of these vulnerabilities. Prices for exploits ranged from $150 and $2,500 depending on the exploit builder kit capabilities and ease of use. Arete assesses that the price range of exploit builders will consolidate further on the higher end. This trend should mimic increasing prices in above-ground, zero-day forums and competitions, where people legally purchase exploits.

Additionally, cybercriminals will continue decreasing the time necessary to leverage exploits by capitalizing on PoC exploits in operations. Cybercriminals also readily leveraged code developed by researchers in their operations, and this is unlikely to change.

Threat Actor Insights

The section provides insights into some of the actors Arete engaged with in 2021.

PHOBOS

Throughout 2021, the ransomware group Phobos continued to show a pattern of re-extortion after victims made a ransom payment, proving themselves to be one of the more unreliable groups in the threat landscape. Typically, once a victim pays a ransom and is waiting for the decryptor, Phobos will ask for more money, claiming "The Developers" were unsatisfied with the agreement. Other highlights include:

- Based on Arete case data, Phobos does not typically exfiltrate data.
- Phobos' ransom demands tend to be relatively low, which may coax victims into paying with little hesitation.

Based on these observed tactics, Arete expects the group to continue their attempts to re-extort future victims for as long as companies show a willingness to pay multiple ransoms to get their data completely decrypted.

PHOBOS DATA EXFILTRATION

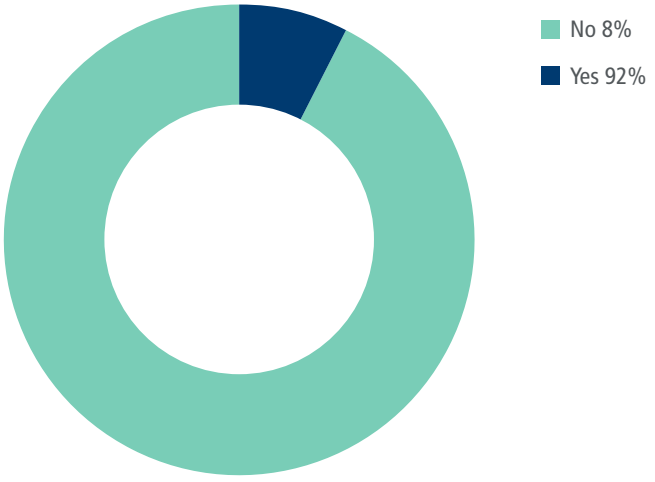


Figure 3 Historical data of Phobos data exfiltration

LOCKBIT 2.0

In June 2021, the Lockbit organization resurfaced as Lockbit 2.0. Not only had the group improved its encryption capabilities — increasing impact to victims — but it also incorporated double extortion pressure tactics. One such pressure tactic included print bombing, whereby they would take control of victims' network printers and print out the ransom notes to ensure victims were aware of the ransomware attack and to demonstrate their physical control over victims' devices.

After resurfacing, the Lockbit 2.0 actors continued demanding the typical ransom demand. However, Arete observed that their initial demands drastically dropped in August 2021 — likely to keep a low profile in response to increased pressure by European law enforcement agencies — only to steadily increased again throughout Q4 2021.

HIVE

Hive first emerged midway through 2021. The group had one standout trait: an unwillingness to negotiate on their initial ransom demands. From July to October 2021, Hive flat out refused to negotiate or compromise on demands and as a result, were known to walk away all together.

Surprisingly, there were a few instances in late 2021 when they softened their stance toward negotiations for unknown reasons. Arete assesses this "softening" trend may become more prevalent in the coming year if the group finds compromise more financially beneficial than walking away when full ransom demands are not met.

PYSA

Throughout 2021, PYSA remained one of the most dominant ransomware groups, especially during Q3 2021 when Arete observed a surge in their attacks. Although PYSA has been consistent in fulfilling their agreements, PYSA victims should be aware that the group typically provides decryptors within 24 hours.

While PYSA is known for targeting the education and healthcare industries[xxi], Arete's analysis has shown that the group's reach is much more comprehensive. In 2021, PYSA also focused on retail and wholesale, alongside heavy machinery industries, such as logistics and building construction companies. Arete assesses that PYSA finds these industries more vulnerable to cyberattacks or more willing to pay to ensure continued operations.

PYSA INDUSTRY DISTRIBUTION

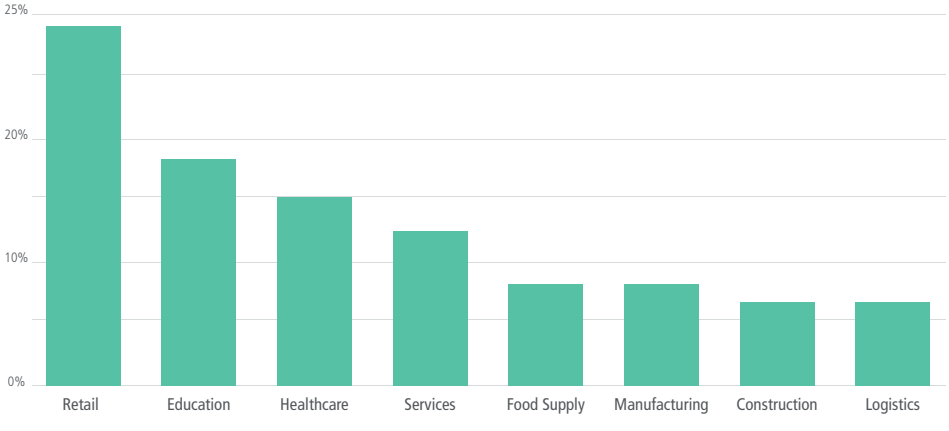


Figure 4

CONTI

Unlike the other groups mentioned, Arete assesses that Conti is a highly "professional" RaaS organization that values both its reputation and most importantly, getting paid. During negotiations, this group tends to operate with a certain business-like professionalism but is also known to use various pressure tactics — they will send emails, make phone calls, and threaten to publish sensitive data — if communication with the victim is slow or inconsistent.

Conti was one of the top three most active ransomware groups in 2021. Their efficient internal operations allow them to target and attack a large variety of business sectors. The group easily increased the pace of their operations after REvil and Maze ceased activity in 2021.

After Conti made a public announcement on October 1 regarding victims releasing details of ransom negotiations to journalists[xxii], Arete observed an uptick in the group's initial demands in several campaigns. The group went from demanding several hundred thousand to a few million dollars in Q3 2021 to demanding between US$5 million and US$10 million in Q4 2021.

At the end of 2021, this trend eased back, with the group making only a handful of million-dollar demands. Though the trigger behind this trend is unknown, Arete assesses that following a profitable first half of 2021, the group most likely concentrated efforts to restore profitability.

CONTI INITIAL RANSOM DEMAND (USD)

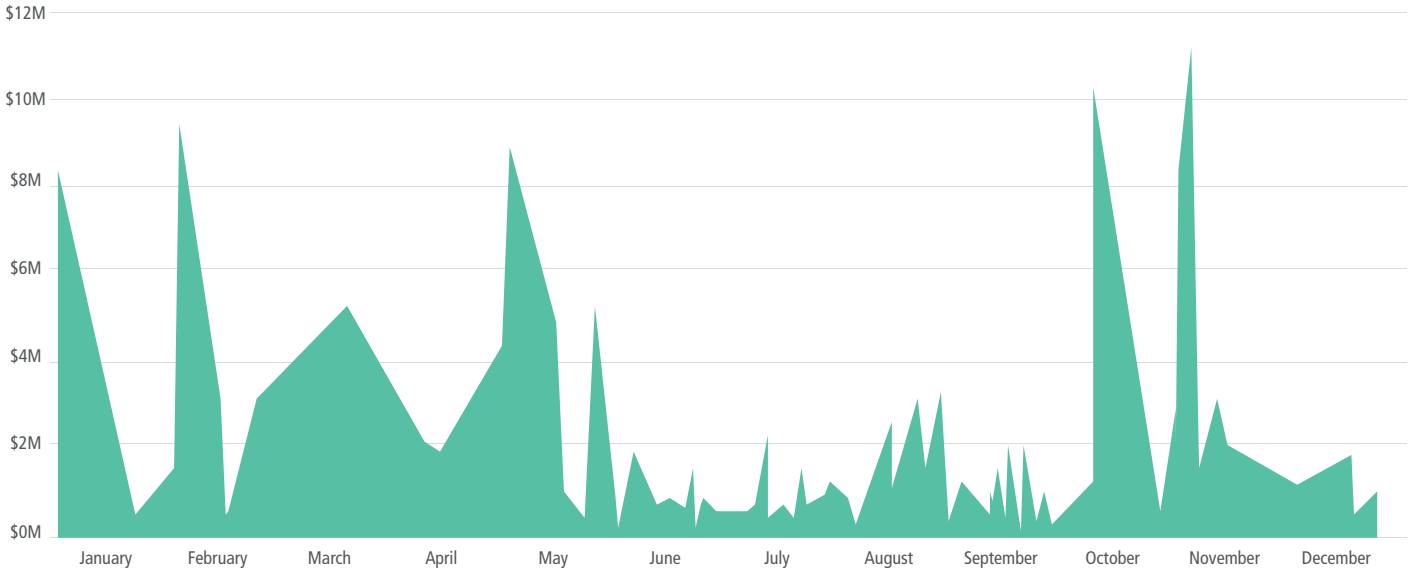


Figure 5 Conti Initial Ransom Demands Throughout 2021

Law Enforcement Involvement

While late 2020 offered a glimmer of hope with global law enforcement's takedown of Emotet and Trickbot operations, 2021 dawned with threat actors bouncing back to business as usual. The pace of threat actor operations increased at the start of the year — and so, too, did the victim count.

This trend would have likely continued throughout 2021 had the Darkside ransomware group not attacked Colonial Pipeline and encrypted its systems. This attack against a critical infrastructure company gave anti-ransomware efforts a shot of adrenaline, catapulting them to the top of the agenda for intelligence and law enforcement agencies and the U.S. White House. Specifically, U.S. law enforcement began to coordinate efforts to combat ransomware after the White House identified the following four key tasks:

- Disrupting ransomware infrastructure and actors.
- Bolstering resilience to withstand ransomware attacks.
- Addressing the abuse of virtual currency to launder ransom payments.
- Leveraging international cooperation to disrupt the ransomware ecosystem and address safe harbors for ransomware criminals.

To help align agencies and prosecutorial initiatives, the Department of Justice (DOJ) began leveraging the National Cyber Investigative Joint Task Force (NCIJTF) by:

- Collaborating with incident response firms.
- Attending international ransomware summits.
- Recommending the first sanctions against a virtual currency exchange.
- Updating ransomware sanctions advisories.
- Creating resources to help private and public organizations combat ransomware attacks.
- Bolstering international cooperation against ransomware.[xxiv, xxv]

Some other notable events in 2021 included:

- G7 leaders and U.S. President Biden issued statements directly asking Russian leaders to help disrupt ransomware gangs from operating within Russia's borders.
- Senior officials from the European Union and 31 other countries around the world issued a joint statement pledging to crack down on payment channels used by ransomware gangs.[xxvi]
- A renewed focus on targeting cybercriminals led to actors shutting down operations, lying low, or looking for new "safe havens."

U.S. President Joe Biden signed Executive Order (EO) 14028 on "Improving the Nation's Cybersecurity" and established a Cyber Safety Review Board.[xxiii] EO 14028 resulted in U.S. government agencies — including the U.S. Department of Justice (DOJ), the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), and U.S. Cyber Command (CYBERCOM) — adjusting their priorities to join the fight.

Law Enforcement Involvement

- The U.S. Department of Treasury officially sanctioned the Suex and Chatex virtual currency exchanges.
- Russia, leveraging its SORM platform, restricted access to 15 VPN providers, some of which are leveraged by threat actors to launch campaigns against victims. These platforms were also likely used by political dissidents and impacted their abilities to organize.[xxvii]
- The No More Ransom project[xxviii] created a central repository of information and tools to help detect, defend against, and educate the public on all things ransomware.
- Security researchers and cybersecurity firms prevented the payment of millions of dollars in ransoms by identifying vulnerabilities in ransomware and developing universal decryptors.
- Editor's note: Unexpectedly Russia and Belarus both joined efforts to combat cybercrime in early 2022, respectively, by arresting members of the REvil ransomware group and actors involved in carding operations.

Arete assesses that the fight to stop ransomware will remain a top priority for the White House and international community throughout 2022. While it is difficult to predict the impact of these efforts, ransomware actors have already begun taking steps to protect themselves. For example, they are forming "ransomware cartels" and sharing TTPs, rebranding often, leveraging initial access brokers, and shifting to extortion-only campaigns.

Law Enforcement Involvement

2021 TIMELINE

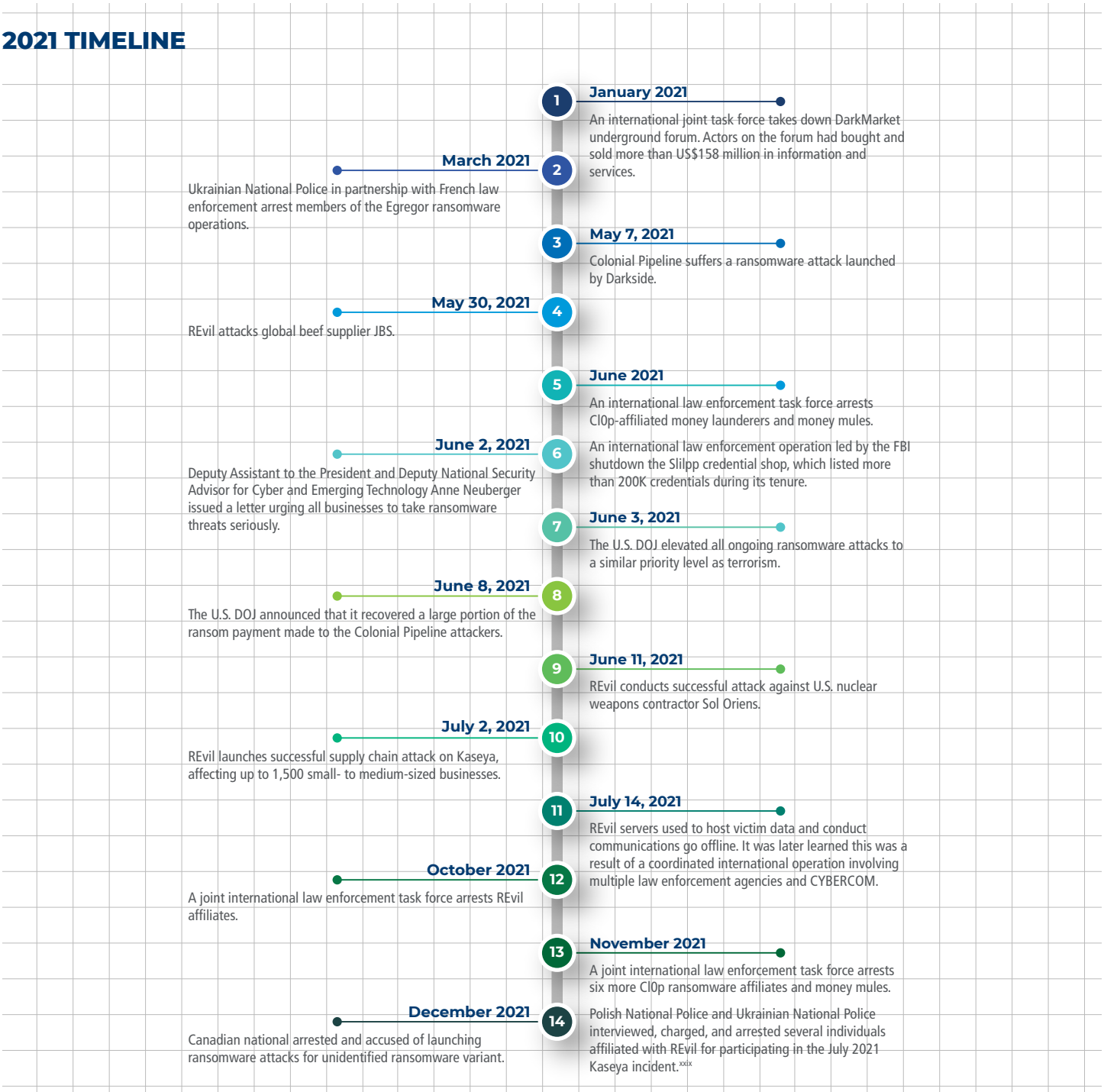


Figure 6

Overall Ransomware Stats

Source: Arete Cases from 2021

AVERAGE RANSOM DEMAND VS. AVERAGE RANSOM PAID BY MONTH (TOP 10 VARIANTS)

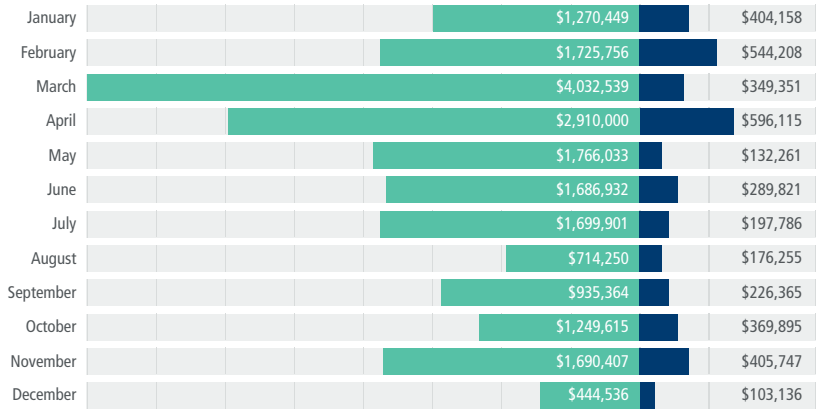


Figure 7

AVERAGE RANSOM DEMAND VS. AVERAGE RANSOM PAID BY QUARTER (TOP 10 VARIANTS)

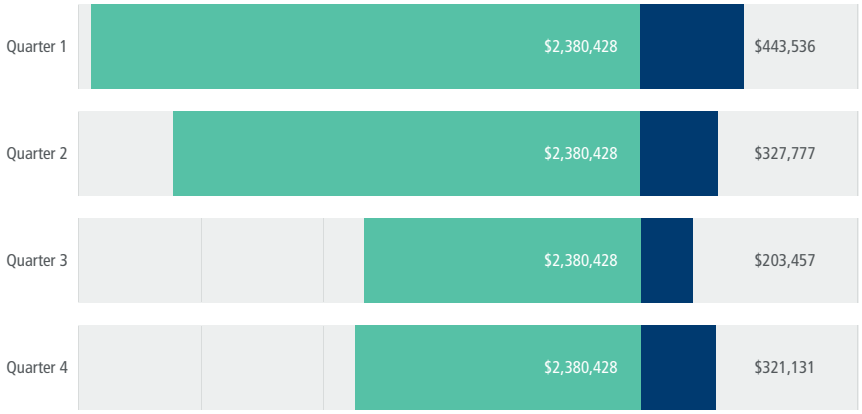


Figure 8

AVERAGE RANSOM DEMAND VS. AVERAGE RANSOM PAID BY INDUSTRY

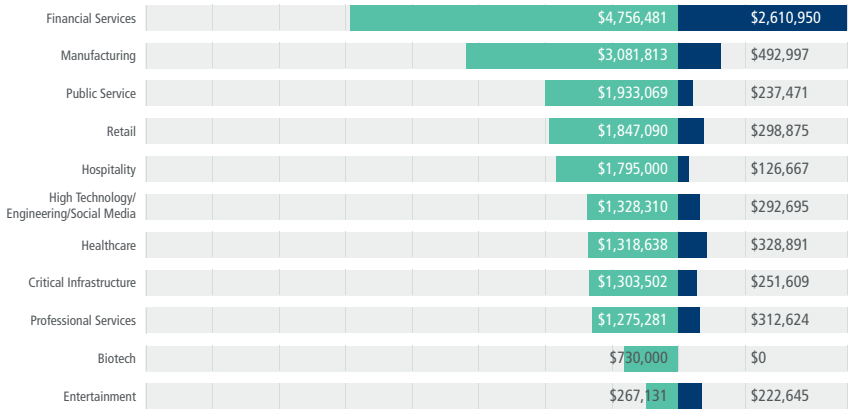


Figure 9

Overall Ransomware Stats

Source: Arete Cases from 2021

AVERAGE RANSOM DEMAND VS. AVERAGE RANSOM PAID BY TYPE OF MALWARE

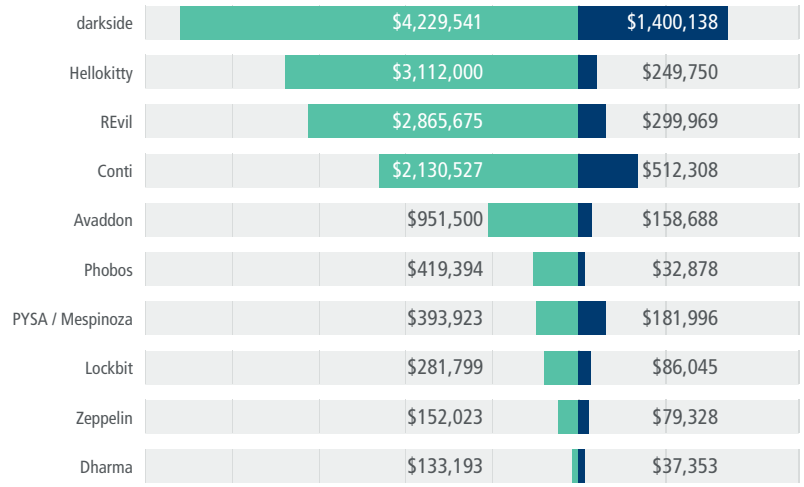


Figure 10

VARIANTS OBSERVED IN PROFESSIONAL SERVICES

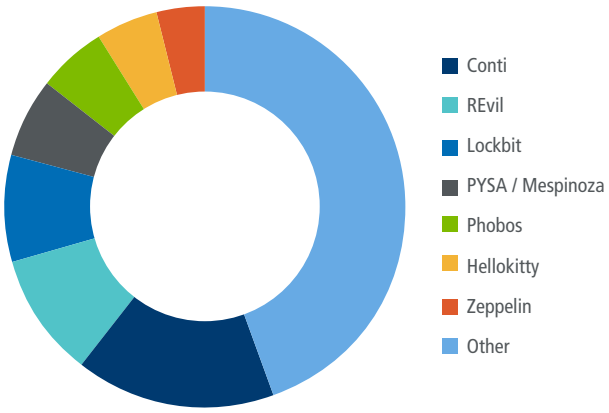


Figure 11

VARIANTS OBSERVED IN PUBLIC SERVICES

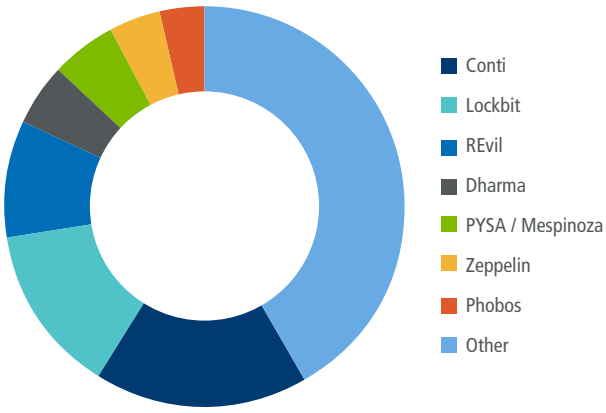


Figure 12

VARIANTS OBSERVED IN MANUFACTURING INDUSTRY

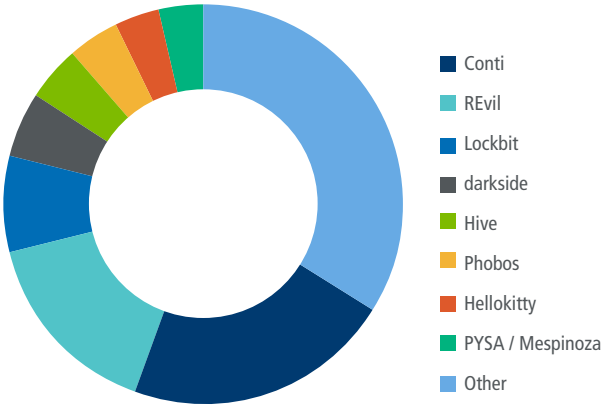


Figure 13

Overall Ransomware Stats

Source: Arete Cases from 2021

DATA EXFILTRATION BY MONTH

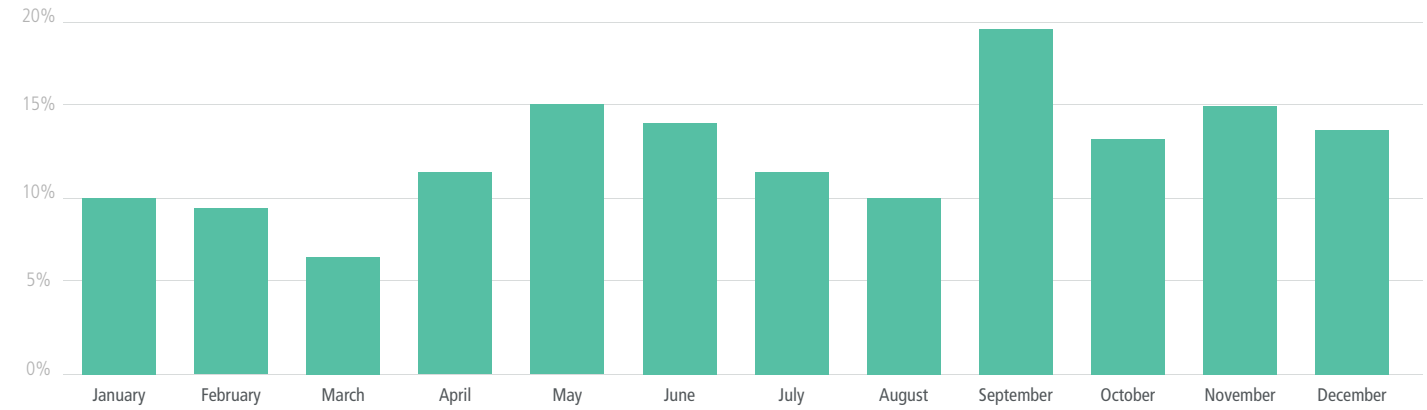


Figure 14

AVERAGE 1ST RANSOM PAID AMOUNT AND AVERAGE 1ST RANSOM PAID AMOUNT BY MONTH AND YEAR

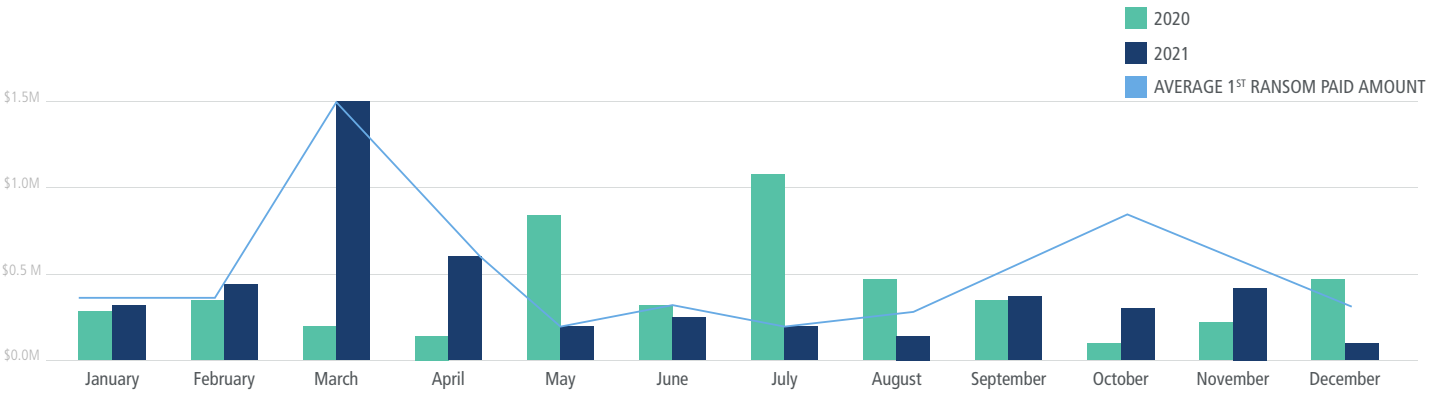


Figure 15

What to Expect

While 2021 began with an uptick in ransomware activity and demands, it closed with a renewed effort from governments, law enforcement agencies, and IR firms to combat cyberthreats. These efforts must continue into the new year. Otherwise, if left unchecked, ransomware could prove to put more and more victim organizations out of business, whether they have cyber insurance or not.

The key to resolving the issue is disruption. As a community, we must continue to band together to increase pressure and exact the same toll on ransomware actors as they do on their victims. Though recent global events, such as the Ukraine and Russia tensions, may hamper efforts to sustain cybercriminal disruptions, we can still make it more difficult for actors to operate and thus, help to slow the pace of attacks. To do this, we must increasingly target cashout operations and those sanctioning entities with lax compliance while also remaining focused on individual arrests. Otherwise, the threat will continue to proliferate and businesses across the globe will remain at risk.

i. https://www.blackfog.com/the-state-of-ransomware-in-2021/

ii. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers

iii. https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/

iv. https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/#:~:text=AIDS%20Trojan%2FPC%20Cyborg%20(1989,instance%20of%20a%20ransomware%20attack

v. Double extortion is when threat actors exfiltrate sensitive data before encryption and threaten to publish or sell the data.

vi. https://www.darktrace.com/en/blog/double-extortion-ransomware/

vii. https://www.scmagazine.com/analysis/leadership/roger-grimes-says-quintuple-extortion-is-the-new-ransomware-reality-and-its-getting-worse

viii. https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation

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

x. https://therecord.media/the-fbi-believes-the-hellokitty-ransomware-gang-operates-out-of-ukraine/

xi. https://therecord.media/alphv-blackcat-is-the-first-professional-ransomware-gang-to-use-rust/

xii. https://www.mandiant.com/resources/defining-cobalt-strike-components

xiii. https://docs.microsoft.com/en-us/troubleshoot/windows-server/backup-and-storage/shadow-copies-deleted-run-file-classification-infrastructure

xiv. https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/view#gid=2129022708

xv. Notably, the threat actor Hafnium exploited ProxyLogon vulnerabilities in the HTTP proxy and Unified Message Service (UMS) component of the Client Access services layer two months before the vulnerabilities were publicly disclosed.

xvi. https://www.microsoft.com/security/blog/2021/09/15/analyzing-attacks-that-exploit-the-mshtml-cve-2021-40444-vulnerability/

xvii. https://asec.ahnlab.com/en/27264/

xviii. https://www.mandiant.com/resources/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day

xix. https://bishopfox.com/blog/breaching-the-trusted-perimeter

xx. https://www.bleepingcomputer.com/news/security/ransomware-gang-uses-printnightmare-to-breach-windows-servers/

xxi. https://www.cisa.gov/sites/default/files/publications/PYSA%20Flash.pdf FBI Flash, "Alert Number: CP-000142-MW," March 16, 2021

xxii. https://therecord.media/conti-gang-threatens-to-dump-victim-data-if-ransom-negotiations-leak-to-reporters/

xxiii. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

xxiv. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

xxv. https://www.npr.org/2021/10/13/1045248842/white-house-brings-together-30-nations-to-combat-ransomware

xxvi. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/

xxvii. https://en.wikipedia.org/wiki/SORM

xxviii. https://www.nomoreransom.org

xxix. https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya

Arete

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
Arete911@AreteIR.com

www.areteir.com