2021 CYBER THREATS TO PUBLIC SAFETY

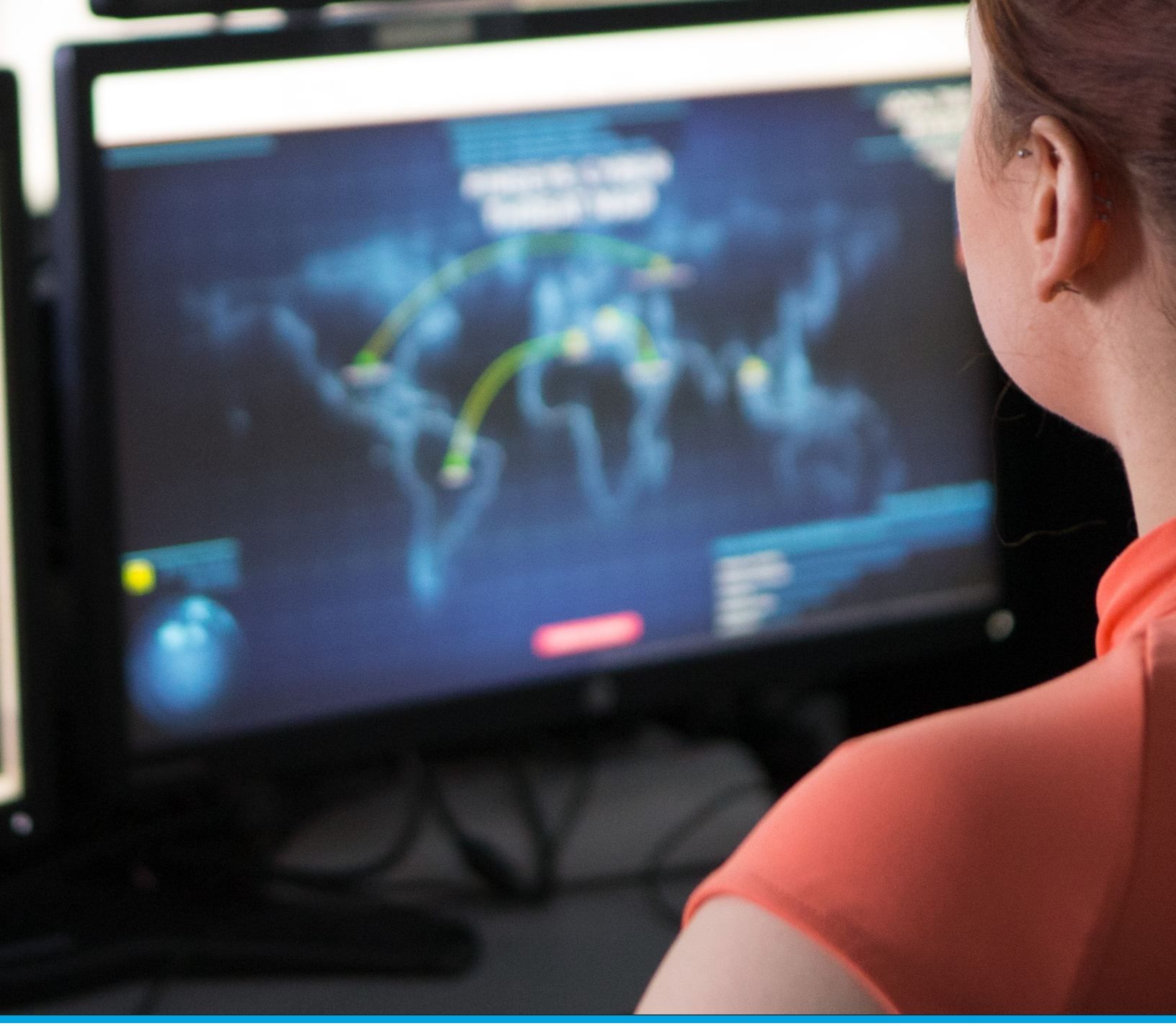
CRIMINAL OPERATIONS FOCUS

Insights from the Motorola Solutions Threat Intelligence Team - Second in a Series

MOTOROLA SOLUTIONS

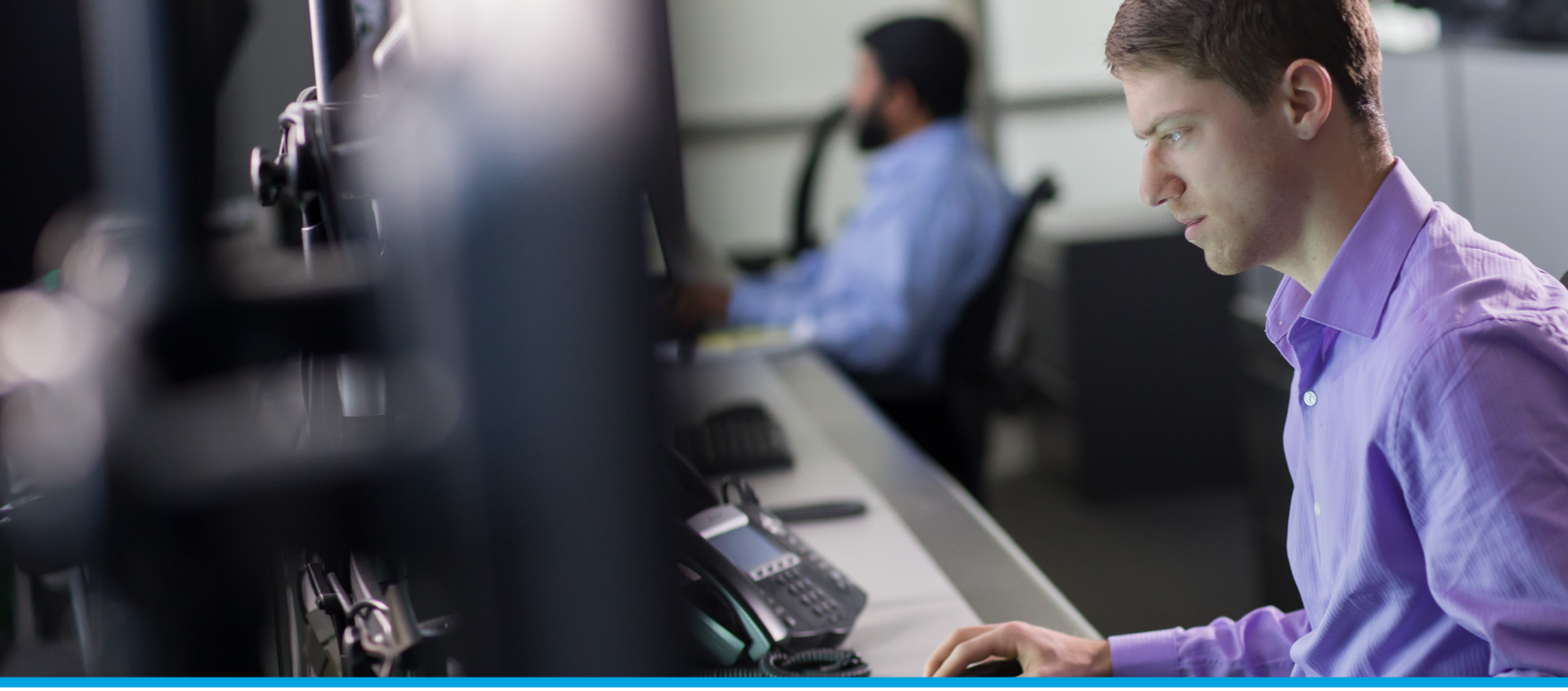
Motorola Solutions continues to grow as a global public safety solution leader. Our commitment to deliver the best products and services for emergency services, with a focus on cybersecurity, gives us direct insight into the cyber threats that uniquely challenge the first responders around the world. To improve the security and awareness of public safety organizations, the Motorola Solutions threat intelligence team has compiled their findings, research and analysis throughout 2021 as part of our Cyber Threats to Public Safety series. Our first report covered the unique cyber threats that threaten the different aspects of a public safety officer's tool kit. In this report, we share our insights on the developments and trends of the cybercrime community as it pertains to public safety. We seek to inform and educate the public safety leaders and practitioners on how criminals view public safety organizations, and how they attempt to compromise their targets. The threat intelligence team used proprietary data, publicly reported and closed source cyber intelligence from Jan. 01 — Nov. 30, 2021 in this paper.

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Cybercriminals are responsible for most of the cyberattacks reported around the world. The criminal industry is flooded with money, organized gangs, and a seemingly endless list of victims being extorted and stolen from for tens of thousands to tens of millions of dollars per attack. The public safety community is not shielded from cybercrime, and faces its own unique challenges to defend itself against the hungry financially motivated extortion actors and ideologically impelled hacktivists. This past year has taught us that proper defenses and response at a federal level can show indications of success, but the criminal world is an agile and creative ecosystem. In addition to building a robust cybersecurity program that incorporates people, processes, and technology, it must be countered by better understanding the motivations and methods behind the acts.



THE CYBERCRIMINAL UNDERGROUND TARGETING PUBLIC SAFETY

To no one's surprise, the ransomware problem did not go away in 2021. Estimates place average ransom payments at a record $570,000 USD[1] and average global attack rates at 235 per month. Within the realm of public safety, defenders planned ahead for extortion attempts by relying on offline backups more often. This led potential victims to increasingly avoid ransom payments in favor of recovering affected systems. However, victim organization payouts increased this year, with public safety entities now having to contend with double, triple, or even quadruple methods of extortion[2].

Municipalities remained the most common public safety victims in 2021, impacted in 55 percent of attacks. Municipalities often have broad network footprints, running systems that range from court services and city functions to citizen portals and utilities. Many of these have connections to the open internet. This often results in municipalities being among the first entities targeted by opportunistic attackers. However, attacks against the federal government and military organizations climbed dramatically this year, too, indicating that some threat actors may be changing their victim profiles. In 2020, federal and military entities represented only 4 percent of public safety victims (4 out of a total of 136). But in 2021, these targets made up 17 percent of the attacks (31 out of all 181 attacks), making them the third-most commonly impacted victims. This trend has yet to abate at the time of this report. Police departments remained the second most targeted public safety entity, consistent with all previous years reporting, representing 18 percent of the attacks (33 of 181 attacks), a 14 percent increase over 2020.

Since 2020, the categories of actors who targeted public service remained largely unchanged through November 2021. Extortion criminals still represent the most common threat, with 53 percent of all attacks (96 total) involving ransomware. This is a 48 percent increase since last year, where there were 65 ransomware infections out of 140 total attacks to public safety. Hacktivism and similarly ideologically motivated attacks remained common in 2021 but fell 18 percent. We believe this is due to fewer large-scale protests than were seen in the spring and summer of 2020. These protests have historically generated hacktivism activity as well as physical attacks motivated by ideology.

We determined that while most extortion groups that attack public service are simply opportunistic, some have a specific preference for our space. DoppelPaymer (recently rebranded as "Grief") was behind 20 percent of all ransomware attacks on public service victims. However, they represented only 3 percent of attacks to worldwide industries in 2021. Compare that with Conti, which made up roughly 22 percent of all attacks worldwide, but were only involved in 11 percent of ransomware attacks on public service. Based on such attack data (See Figure 1), we can say with low confidence that certain groups like Sodinokibi and Conti only incidentally target Public Safety, while groups like DoppelPaymer/Grief and the now-defunct[3] Avaddon gangs are either less wary of, or outright prefer attacking public safety victims.

Some of these gangs, like DoppelPaymer/Grief, are known to use specific tactics, techniques and procedures (TTPs). Targeting domain accounts, stealing data from local systems, discovering system network configurations, and automatically exfiltrating data are all TTPs associated with DoppelPaymer/Grief. Other techniques, while not explicitly demonstrated by the gang, are still highly likely in extortion attacks on public safety, such as, but not limited to, targeting external remote services, lateral tool transfer, service execution and domain account discovery.

[1] https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/
[2] See below: Testing Out Triple and Quadruple Extortion Methods
[3] See below: Extortion Groups Rebrand, In More Ways Than One

RANSOMEWARE GROUP	PERCENTAGE OF GLOBAL RANSOMWARE ATTACKS	PERCENTAGE OF PUBLIC SAFETY RANSOMWARE ATTACKS
DoppelPaymer/Grief	3%	20%
Conti	22%	11%
REvil(Sodinokbi)	14%	5%
Avaddon	12%	13%

Figure 1: Global activity of top extortion groups compared to specific public safety targeting in 2021

Initial Access brokers (IABs), or individuals who use their own methods to breach a company's network to then sell that access to other threat actors for a fee, were prolific in 2021. Currently, IABs selling either verified or likely legitimate access into emergency service environments represent 16 percent of all attacks, a total of 29 attacks. Most IABs are assessed to be opportunistic, attempting to develop access across multiple industry verticals. The likely reason for this is to improve monetization since the more kinds of access there are available, the more likely these IABs are to find a buyer. In addition, IABs often charge more on average for public safety victims than they do other organizations.

While the generic charges for access in 2021 typically ranged from $500-$5,000 USD, it averaged $1,000-$8,000 USD for public safety victims. There are multiple possible explanations for this. The most likely is that intrusions against public safety, particularly government or law enforcement, could be seen as riskier than those against universities or medical research facilities. As such, IABs may believe the effort and risk needed to obtain such access warrants higher pricing. For instance, on Feb. 7, 2021, the prolific IAB 'vasyldn' opened a thread on the top-tier criminal forums Exploit and XSS, which offered access to a virtual private network (VPN) portal belonging to an unnamed Arizona city for approximately $30,000 USD (See Figure 2).

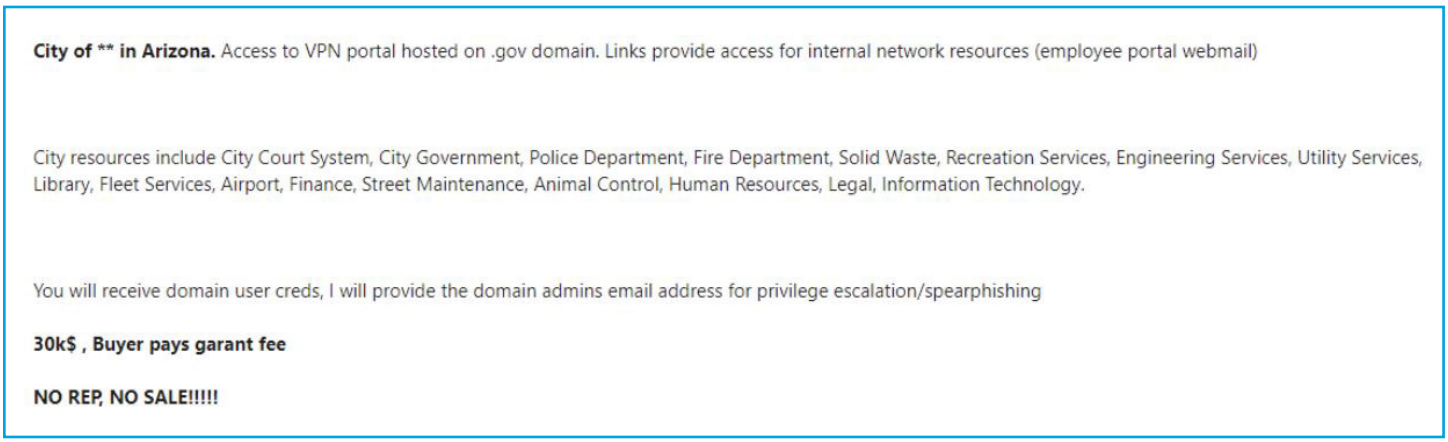


Figure 2: Actor Vasyldn selling access to a city in Arizona

When compromising victims, IABs rely on whatever methods are easy and attractive to potential buyers. This means they often focus on exposed or poorly-secured Windows Remote Desktop Protocol (RDP) ports, Virtual Private Network (VPN) connections, unsuspecting end users, and unpatched external services. In addition, IABs will also often attempt to gain privileges, with the greatest prize being domain administrator accounts or accounts with close access to domain controllers. Domain-level access allows an extreme degree of freedom when executing attacks. It is also the primary vantage point by which extortion groups deploy ransomware. Therefore, IABs that can get elevated privileges are more likely to command the attention of successful groups that may pay more for such quality access.

TESTING OUT TRIPLE AND QUADRUPLE EXTORTION METHODS

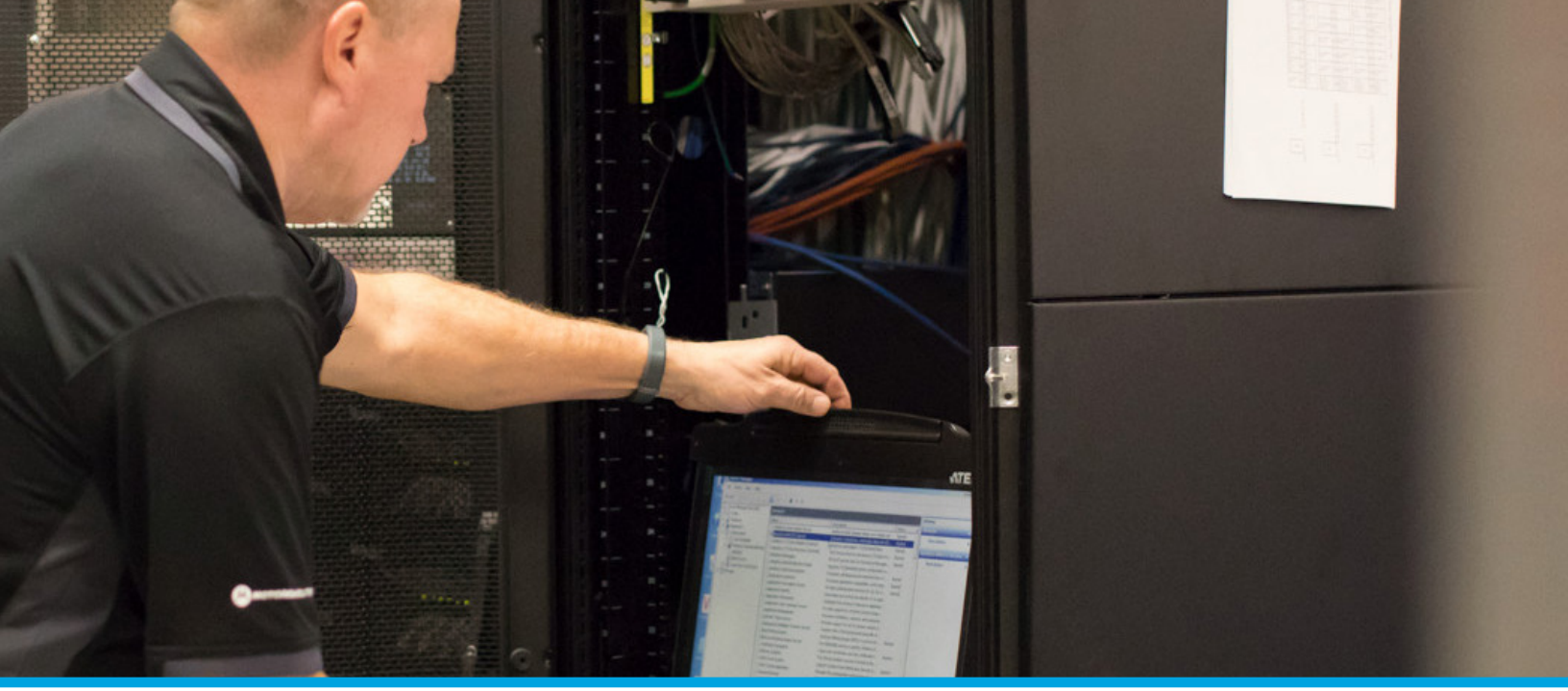
2020 introduced the phenomena of "double extortion," in which criminal groups stole data in addition to encrypting victims' assets. Extortion gangs published this stolen data on name-and-shame blogs as a way to punish organizations that chose not to pay ransoms. The tactic is prevalent across most industries, with a 47 percent increase in stolen company data found on ransomware leak sites in the first three quarters of 2021 compared with all of 2020[4]. However, within the realm of emergency services, double extortion specifically coincided with an increased use of offline backups, which allowed municipal victims to more reliably recover from ransomware attacks.

In 2021, we observed more groups upping the ante, with additional extortion methods applied against targets. Alongside data encryption and data theft, some groups launched distributed denial-of-service (DDoS) attacks. On April 19, 2021, the Avaddon gang compromised the systems of Presque Isle, Maine's police department (PD). Avaddon stated it would launch a DDoS attack in addition to leveraging usual extortion tactics as a way to force Presque Isle to pay the ransom demand. When Presque Isle PD did not pay the ransom, Avaddon subsequently released roughly 200GB of police records and case files. The gang likely also followed through on their threats of a DDoS attack. Avaddon tried this "triple extortion" tactic later against the towns of Villafranca, Italy and Olomouc, Czech Republic — with undetermined success.

Some extortion groups allegedly resorted to harassment[5] as an additional method to place pressure on targeted organizations. Sodinokibi claimed in a post that the group would facilitate voice-over-IP (VoIP) calling against victims' business partners and associates, as well as the media (See Figure 3). The stated purpose of this tactic was to "exert maximum pressure" against targeted entities. While troubling, we have yet to corroborate this claim, since at the time of writing, no businesses have stated they received a call from extortion groups within this context.

In attacks on public safety, we observe that the only tactics that survive as long-term tradecraft are those which reliably help extortion groups make money. Data encryption combined with data theft is successful enough to warrant ransomware gangs leveraging these two tactics in most cases. While DDoS and harassment may make ransomware attacks more stressful, it is unclear whether they result in more frequent extortion payments. We have moderate confidence that neither will remain a staple of ransomware activity, unless one or both result in demonstrable monetary increases for attackers.

[4] https://www.group-ib.com/media/gib-2021-2022-report/?utm_medium=organic&utm_source=press_release&utm_campaign=htct-reports-2021-en&utm_content=global [2] See below: Testing Out Triple and Quadruple Extortion Methods
[5] https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/



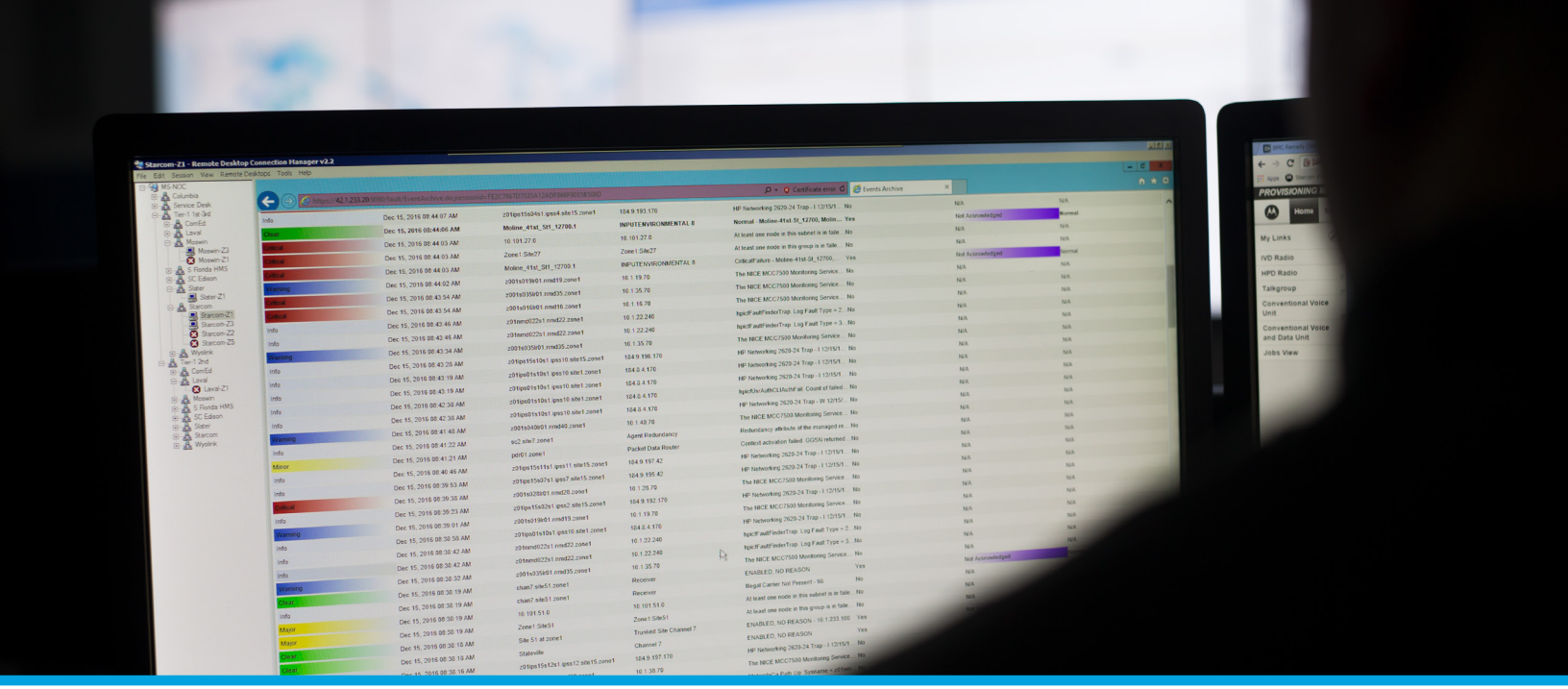
We assess that the addition of DDoS, harassment, and data theft into the extortion methodology is the result of organizations successfully implementing security controls across their environments. As most industries quickly learned that having updated, offline and tested backups could help them consistently recover from ransomware attacks, cybercriminals had to adapt in order to continue receiving payouts. As a result, threat actors began to rely on data theft to force victims into paying to protect their data from exposure. Moving into 2021, we observed an increased number of both public and private organizations able to defend their data and quickly recover with backups, which we assess has led to the development of the triple and quadruple extortion methods.

We now have the opportunity to ring your networks (calls to the media, company counterparties) to exert maximum pressure. To do this, indicate in the description of the network the domain of the company, with whom it communicates, and so on. You can also write to the chat contacts for spam and dialing (phone numbers).
Also, **DDoS** (L3, L7) works in test mode on sites and networks (various services of companies). More information in the "news" section.
DDoS is paid, calls and spam are free for adverts of our PP.
I also remind you about the development of solutions for * nix (VM ESXi), a polymorphic engine for win *.
Other wishes, please indicate in the tickets.

There is one place. Let's also take in the "Red Team" 1 team of network providers and 1 team of network workers. Experience is required. Maximum rate, work directly.

A complaint Like + Quote Answer

Figure 3: Sodinokibi advertising phone calls to exert pressure against victims



INTERNATIONAL ATTENTION AND BACKLASH

One extortion attack drew the eyes of the world, much to the criminal underground's seeming displeasure. On May 7, 2021, DarkSide ransomware affiliates encrypted the IT networks of Colonial Pipeline, the main conduit of refined oil from the Gulf Coast in the United States. After the initial infection, Colonial Pipeline halted the operational technology (OT) networks that govern oil movement and handling as a precaution. Aside from frustrating Americans at the gas pump, the attack drew the scrutiny of the United States government. President Biden indicated[6] he spoke to Russia's Vladimir Putin about the attack, and later stated "We do not believe the Russian government was involved in this attack, but we do have strong reason to believe that the criminals who did the attack are living in Russia, that's where it came from,".[7]

More action from the United States followed. The U.S. Department of Justice (DOJ) granted ransomware investigations a similar legal priority as terrorism cases.[8] The Biden administration acknowledged the importance of protecting critical infrastructure and pointedly didn't rule out the possibility of retaliation against groups targeting U.S. interests. The White House also created an anti-ransomware task force in which disruptive attacks against extortion groups were reportedly considered.[9]

As a result of the increased cybersecurity investment across United States government and public safety organizations, and the anti-ransomware response from the federal government, we have observed a significant shift in extortion attacks to public safety. In 2020, the United States public safety organizations represented 80 percent of all public safety extortion victims. However, in 2021 the U.S. only makes up 40 percent of the victims, and that is with a 60 percent increase in overall attacks. What occurred was a drastic shift in targeting by the eCrime community, who moved their sights on European, Asian and South American targets. As a result, attacks to EMEA increased 273 percent in 2021, where extortion actors are having higher success at receiving an extortion payment.

[6] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/
[7] https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/
[8] https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/
[9] https://www.politico.com/news/2021/07/14/white-house-ransomware-task-force-499723

HOW AND WHY CRIMINAL FORUMS "BANNED" RANSOMWARE

The criminal community has not been too fond of the increased public attention and government backlash from the increasingly frequent and impactful ransomware attacks. Immediately after the Colonial Pipeline attack, cybercriminals from ransomware operators to forum administrators had to deal with the attack's fallout. First, DarkSide's infrastructure went down, potentially being disabled by outside actors, though this is unconfirmed. Despite this setback, DarkSide was able to continue several ongoing attacks in which it likely had already been engaged. The disruption of Darkside's infrastructure happened despite the previous apology (See Figure 4) put forth by the group.

> We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined government and look for other our motives.
> Our **goal is to make money, and not creating problems for society.**
> From today we introduce moderation and check each company that our partners want to encrypt to advoid social consequences in the future.

Figure 4: Darkside group attempts to absolve themselves of the Colonial Pipeline attack

Additionally, two top-tier dark web criminal forums took action to distance themselves from the increasing attention DarkSide's attack provided. On Exploit, administrators made a post (See Figure 5) that stated that "all [ransomware] affiliate programs" would be banned from the site moving forward. The administrators specifically welcomed "pentesters, specialists, [and] coders" to post instead. Penetration testers, or pentesters, are individuals who evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities in the organization, and are therefore an easy cover for a malicious initial access broker. Meanwhile, the XSS forum administrators had only just finished making a similar announcement: discussions surrounding ransomware were unwelcome[10] on the site.

Good day,

We are glad to see pentesters, specialists, coders.
But lockers are not happy, they attract a lot of attention. The very type of activity is not pleasant to us in view of the fact that everything is located in a row, we do not consider it advisable to be present on our forum, partner programs of lockers.

It was decided to remove all affiliate programs and prohibit them as a type of activity on our forum.

All topics related to lockers will be deleted.

Figure 5: Exploit administrators ban ransomware activity in May 2021

That doesn't mean ransomware discussions and transactions stopped on the XSS and Exploit forums. Extortion groups began hiring IABs for "pentesting" work, a term associated with non-malicious security testing conducted in legitimate business, rather than the previously stated objectives of gaining access to and control over victim environments. For public safety targets, this amount was higher than the industry norm, as mentioned above. The shift to seeking "pentesters" without mentioning data encryption — and the associated social engineering for non-action against ransomware on the criminal forums — helped ransomware gangs circumvent bans by avoiding open discussions of ransomware deployment while still forging relationships with new IABs and dedicated affiliates (See Figure 6).

Figure 6: English and Russian-language post seeking pentesters for inital access activity

[10] https://www.flashpoint-intel.com/blog/darkside-faces-xss-ban-servers-seized/

EXTORTION GROUPS REBRAND, IN MORE WAYS THAN ONE

The Colonial Pipeline attack and following scrutiny it evoked coincided with multiple extortion groups appearing to cease operation, some dissolving, and others likely only hiding their tracks. On June 11, 2021, Avaddon deactivated their data leak site and halted operations. As part of this shutdown, Avaddon released 2,934 decryption keys, each associated by name with a specific victim, though this was too late for almost all organizations who had already begun rebuilding their IT infrastructure. Since the beginning of 2021, Avaddon was responsible for at least eight attacks against public safety entities, though the true number is likely higher. These eight events equal eight percent of overall compromises since Jan. 1, 2021 — however, this figure is only for the 103 attacks where the threat actor is attributed.

Avaddon wasn't the only casualty. Sodinokibi shuttered on July 13, 2021. The latter gang's so-called "happy blog," which Sodinokibi used to publish stolen data as part of ongoing attacks, went offline, indicating the group followed suit. Additionally, the different communication channels the group used to negotiate with victims became inactive — leaving organizations in the process of ransom negotiations with no way to obtain decryption keys. There were also zero communications from *'Unknown'*, the alias of the group's dark web spokesperson, regarding the disruption. Sodinokibi was behind several attacks on public safety, including a July 2, 2021 compromise against North Beach Maryland and the massive August 2019 campaign[11] which hit more than 22 Texas municipalities and police departments.

Ransomware group "deaths" are rarely permanent. Multiple groups rebranded in 2021 (See Figure 7), continuing operations under new names. DoppelPaymer, a gang responsible for eight attacks on public safety in the first quarter of 2021, changed its designation to Grief in May 2021. Since then, Grief has conducted multiple attacks on public safety entities. This includes the July 22 compromise against the city of Thessaloniki, Greece in which the extortion group demanded $20 million USD after encrypting Thessaloniki's systems and stealing private letters and confidential financial reports.

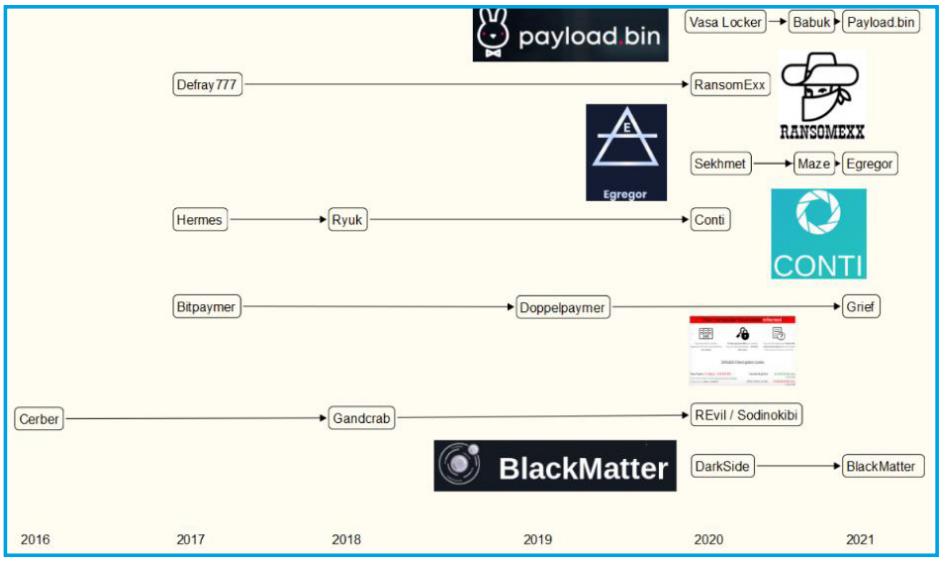


Figure 7: Graph posted by KrebsOnSecurity, detailing rebranded extortion groups

In addition to name changes, some extortion groups attempted a more conceptual rebranding. Different gangs stated they would tighten the reins on the types of entities their affiliates were allowed to target. Prior to its closure, Avaddon prohibited attacking victims within the "public" sector. Sodinokibi stated they would no longer allow the targeting of the "government" sector. Yet Sodinokibi quickly and publicly reversed that decision and Avaddon's attacks against public safety did not stop. On June 8, 2021, Avaddon attacked the town of Freeport, Maine which resulted in the subsequent disruption of municipal services.[12] Based on our available attack data, we are highly suspicious of any claims made by threat actors stating that certain entities are "off limits."

New groups targeting public safety also emerged in 2021. Among them was a potential successor to previously discussed and now-defunct DarkSide. A ransomware strain called 'BlackMatter' appeared months after DarkSide's disappearance and its creators claimed to have combined the most important features of DarkSide and Sodinokibi. Since the code is not identical, it is unknown whether BlackMatter is a rebranding of DarkSide. As we have yet to observe any attacks from BlackMatter against public safety targets, it is similarly uncertain whether the gang will mimic its apparent predecessor or refrain from targeting public safety altogether. We assess the latter possibility to be unlikely, simply due to the opportunistic nature of extortion gangs and their affiliates.

[11] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/texas-municipalities-hit-by-revil-sodinokibi-paid-no-ransom-over-half-resume-operations
[12] https://www.pressherald.com/2021/06/15/freeport-town-computer-network-back-up-following-ransomware-attack/

CONFRONTING THE CRIMINAL ELEMENT

The continued shift for more integrated and intelligent public safety tools and technology, which offers tremendous advancements to a first responder's situational awareness and ability, must be done with security at the forefront. The critical public safety tools can be just as secure as legacy systems, but security teams must understand the challenges posed as they defend against criminals, nation states, hacktivists and others.

These bad actors know that dependable, secure emergency services are essential to combat the pandemic and keep citizens safe from other everyday dangers. That is what makes them such enticing targets. Our intent is that the knowledge contained in this report empowers public safety organizations to understand the methods, techniques, and operations of adversaries.

Today, this knowledge is a core building block of every product and service Motorola Solutions offers. Our customers face increasingly sophisticated and dangerous cyber threats. However, they are not facing this threat alone. Armed with insights such as those found in the Motorola Solutions 2021 Cyber Threats to Public Safety reports, they can confront today's cyber challenges with confidence.

For more information, visit motorolasolutions.com/cybersecurity

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, Il 60661 U.S.A. **motorolasolutions.com**