CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2020-1105

Q3 MALWARE TRENDS:

RANSOMWARE EXTORTS EDUCATION, EMOTET AND CRYPTO MINING MALWARE EVOLVE, AND ANDROID MALWARE PERSISTS

Recorded Future®

This report is an extension of analysis Recorded Future released, which outlined the trends in malware use, distribution, and development throughout Q1 and Q2 2020. Insikt Group used the Recorded Future® Platform to look at mainstream news, security vendor reporting, technical reporting around malware, vulnerabilities, and security breaches, and dark web and underground forums from July 1 to September 30, 2020, to examine major trends to malware impacting desktop systems and mobile devices. The trends outlined below illustrate the tactics, techniques, and procedures (TTPs) that had a major impact on technology. This report will assist threat hunters and security operations center (SOC) teams in strengthening their security posture by prioritizing hunting techniques and detection methods based on this research and data.

Executive Summary

In the third quarter of 2020, Recorded Future observed major expansions in the tactics, techniques, and procedures (TTPs) of prominent ransomware operators, including the targeting of educational institutions and a continued increase in new ransomware operators using extortion tactics. Between July and October 2020, we identified the development of five new ransomware extortion websites. In addition, we identified a large spike in activity from NetWalker and a decline in Sodinokibi activity over the quarter.

Major trends within the desktop malware threat landscape included a resurgence of the prolific Emotet malware and a shift in the development in cryptocurrency mining malware. Emotet, a trojan malware that has infected targets worldwide, paused activity throughout Q2 but resurfaced in July to target organizations including state and local governments in the United States. And developers of cryptocurrency mining malware are adding additional features, other than simply mining cryptocurrency, to further infections.

Lastly, Android malware dominated the mobile threat landscape again this quarter, with mobile malware such as SpyNote resurfacing and references to Cerberus Banking Trojan spiking in association with the leak of the malware's source code.

Key Judgments

- More threat actors will very likely adopt the ransomware extortion model as long as it remains profitable.
- Educational institutions continue to be a prime target for ransomware operators. We believe that disruptions caused by the COVID-19 pandemic have made the networks of universities and school districts attractive targets because these organizations feel increased pressure to stay operational with minimal disruptions and are therefore more likely to pay ransoms quickly.
- Reports of NetWalker attacks increased, and reports of Sodinokibi attacks decreased. However, it is possible that victims of Sodinokibi attacks are simply paying the ransom more often. Based on activity on underground forums, we suspect that the operators of Sodinokibi are continuing to expand their operations.
- While we expect Emotet's operators to continue to employ major pauses, it is highly likely that Emotet will continue to be a major threat and impact organizations across a variety of industries throughout the end of the year and into 2021.
- In Q3 2020, threat actors have increasingly augmented their cryptocurrency mining malware by adding functionalities such as credential stealing or access capabilities. Assuming this trend continues, it is likely to result in malware that can cause more extensive damage to organizational systems than "traditional" cryptocurrency mining malware.
- It is very likely that threat actors will continue to use Android malware to target users into Q4 2020 based on the widespread use of Android OS devices and the dynamic tool sets distributed within the malware. In addition to general Android malware, banking and financial institutions will likely see a spike in fraud attempts as a result of the Cerberus Banking Trojan source code being released.

Ransomware

Shifts in targeted industries and ransomware extortion website activity were prevalent in ransomware operations throughout Q3 2020, as operators of at least five ransomware families stood up new extortion websites of their own, multiple organizations in the education sector were targeted, and Sodinokibi (also known as REvil) activity decreased while Netwalker (also known as Mailto) activity increased.

Ransomware operators will likely continue to extort educational institutions who not only have the financial resources to pay ransoms, but feel a sense of urgency to do so in order to avoid disruptions during the school year. This sense of urgency is especially heightened as a result of the COVID-19 pandemic, as many schools are doing virtual learning and are thus heavily reliant on digital resources and communications. Additionally, while some educational institutions do have large budgets, they often do not allocate enough towards cybersecurity controls or staff, making them an easier target.

SUNY Erie Community College, the University of Utah, and Las Vegas Clark County School District (CCSD) were among the educational institutions impacted by ransomware attacks. The University of Utah disclosed that they paid the $457,059 USD ransom demanded by the threat actor in order to avoid having their sensitive data published.

While the university has not stated which ransomware operators were behind the attack, researchers suspect it to be affiliates of the NetWalker ransomware, which targeted multiple universities in Q2 2020. In the case of CCSD, the Maze ransomware operators stole sensitive data and — after CCSD refused to pay the ransom — published the data, which included employee Social Security numbers, physical addresses, and retirement paperwork, as well as student names, grade levels, birth dates, physical addresses, awards received, years of attendance, and school attended.

Increase in NetWalker Activity, Decrease in Sodinokibi Activity

NetWalker activity spiked in September 2020. Victims named on NetWalker's extortion website, NetWalker Blog, included cybersecurity company Cygilant, Argentina's official immigration agency, Pakistan-based electric supply giant K-Electric, and the College of Nurses of Ontario, with ransom demands consistently in the multimillion dollar range. Data center giant Equinix also reported that it was impacted by NetWalker, though currently there is no evidence of their data being leaked on NetWalker Blog. While it is possible that this is due to Equinix paying the $4.5 million ransom demanded by the NetWalker operators, there is no evidence confirming this.

Reports of activity from Sodinokibi declined over the course of Q3 2020. However, fewer reports of infection does not necessarily mean fewer campaigns have been carried out, and it is possible there is actually an increase in victim organizations who are simply paying the ransom to have their data removed from Sodinokibi's extortion website, Happy Blog. Additionally, on September 28, 2020, UNKN, a member of the Sodinokibi group, announced on XSS Forum that the group is seeking new affiliates to join their operation, which suggests an imminent increase in Sodinokibi campaigns.

New Developments in Ransomware Extortion Websites

In our Q2 Malware Trends report, we stated that more ransomware operators would likely adopt the extortion model, incentivized by the difficulty organizations face in mitigating the threat it poses and potential added income streams from the sale of stolen data. This has proven to be true in Q3 2020, and more ransomware operators will adopt the extortion model as long as it remains profitable.

For example, multiple victims of SunCrypt — a ransomware affiliate program that first surfaced in October 2019 and is operated by the threat actor "SunCrypt" — have had their data exposed on SunCrypt's extortion website, SunCrypt News, since its launch in August 2020, notably North Carolina's Haywood County Schools and University Hospital New Jersey. While both SunCrypt and Maze ransomware have been observed using the IP address 91.218.114[.]31 in their campaigns (SunCrypt recently claimed it had joined the Maze "cartel"), the Maze operators have denied any affiliation with SunCrypt and the reason for the overlap in infrastructure remains unknown.

While SunCrypt ransomware has been known in the threat landscape for a year and has evolved in its TTPs with the launch of SunCrypt News, the three other ransomware extortion websites discovered in Q3 2020 accompany much more recently identified ransomware families. In August 2020, information surfaced regarding a new ransomware operation dubbed DarkSide that targeted various organizations worldwide and posted victim names and samples of stolen data on their extortion website, also named DarkSide. Attacks were initially observed on August 10, 2020, and the threat actors' ransom demands ranged from $200,000 to $2,000,000, depending on the target organization.

While monikers of the threat actors behind DarkSide are unknown, there are some similarities between the DarkSide and Sodinokibi ransomware families, namely their ransom note templates and the PowerShell command used by both families to delete Shadow Volume Copies on the victim machine. DarkSide also uses code similar to both Sodinokibi and GandCrab to check for CIS (Commonwealth of Independed States) countries. Though the DarkSide operators have stated that they were previously affiliates of other ransomware operations that made millions of dollars, the aforementioned similarities to Sodinokibi and GandCrab are not sufficient evidence to link DarkSide to these operations. They also stated that they only target sectors that can afford to pay the specified ransom demand, such as education, government, and medical organizations.

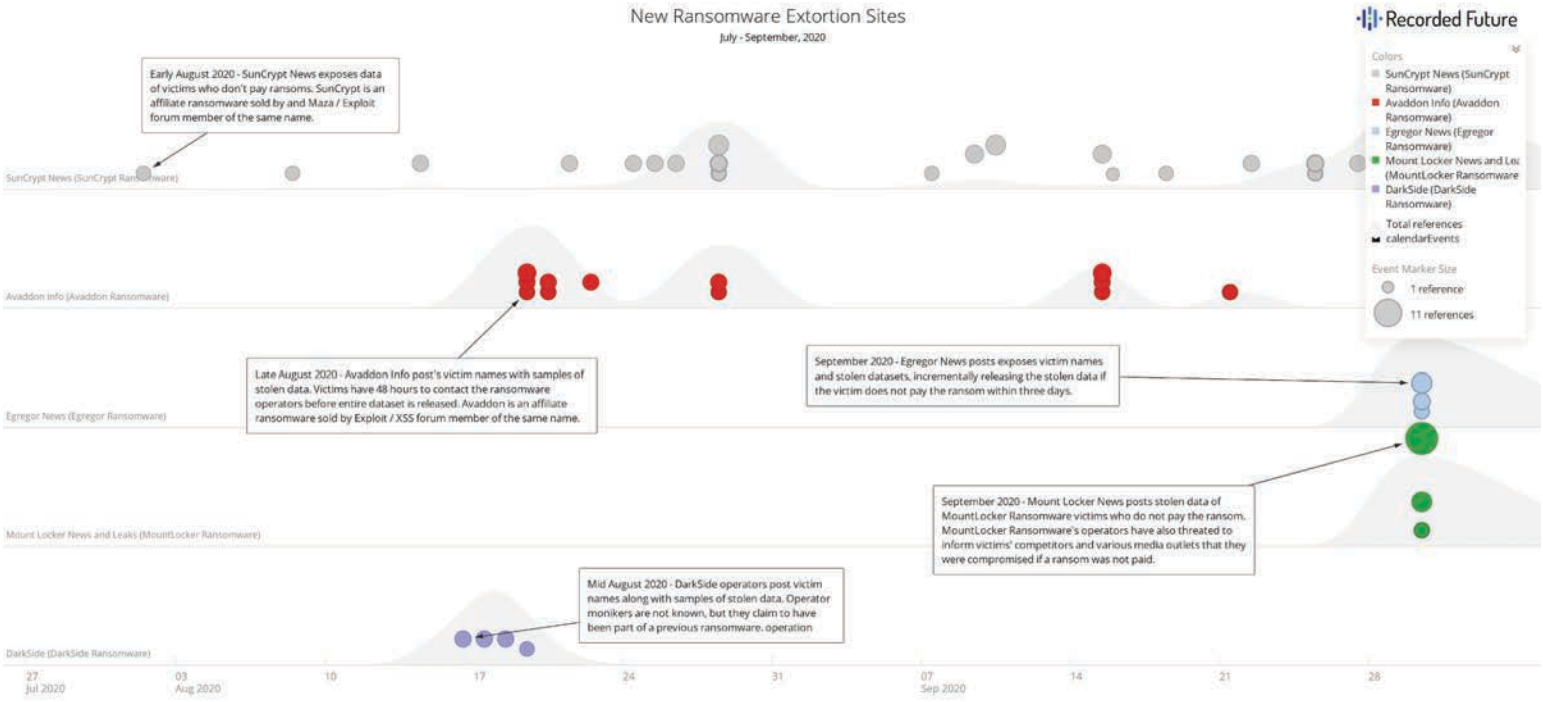

Figure 1: Ransomware extortion websites added to the Recorded Future Portal from July to September 2020 (Source: Recorded Future)

On June 8, 2020, reports emerged of an Avaddon ransomware malspam campaign which targeted users globally. The reports came less than a week after the announcement of the Avaddon ransomware affiliate program on Exploit and XSS forums by a threat actor using the moniker "Avaddon." Avaddon targets data such as financial information, databases, and credit card information, posting samples of victims' stolen data on their extortion website, Avaddon Info. Victims have 48 hours to contact the operators before their stolen data is published.

Also targeting organizations globally in Q3 2020 were operators associated with the ransomware family Egregor. Egregor campaigns were first observed in late September 2020 and have since impacted over a dozen companies, including France-based global logistics company GEFCO. Victims of Egregor will have samples of their stolen data posted on Egregor News and are given three days to pay the ransom before the operators continue to leak some or all of the dataset onto Egregor News. Egregor's payload also requires a decryption key be passed to the command line to run properly on the victim machine, which means that the file cannot be analyzed, either manually or by a sandbox, unless the same command line that the attackers used to run the ransomware is provided.

Finally, in late September 2020, reports surfaced of attacks targeting corporate networks with a new ransomware dubbed MountLocker. MountLocker's operators reportedly demanded ransom payments of $2 million and threatened to publish stolen data on their extortion website, "MountLocker News & Leaks," if they were not paid. The threat actors have also threatened to inform victims' competitors, the media, TV channels, and newspapers that they were compromised if a ransom was not paid.

Desktop Malware

Two major trends are impacting general desktop malware development and distribution in Q3 2020: the resurgence of Emotet malware, and the development of additional malicious functionalities within cryptocurrency mining malware.

Emotet Malware Makes a Major Comeback

Emotet, which has been observed infecting victims globally since at least 2014, has had numerous iterations, with periods of activity that have ebbed and flowed, especially over the past two years. Emotet spam activity paused between mid-March 2020 and July 17, 2020, when a new spam campaign delivering Emotet was observed targeting users worldwide. It seems, at least for the last two years, that Emotet's operators stick to a fairly consistent schedule; in 2019, researchers observed a decrease in Emotet activity in Q2, followed by a resurgence in Q3.

While Emotet is not a novel malware variant, this resurgence of Emotet campaigns has impacted entities globally, including Quebec's Department of Justice and French companies and administrations. In addition, we have observed its operators using major events (such as the COVID-19 pandemic and U.S. elections) as phishing lure themes to assist in delivery.

Major shifts in Emotet's TTPs included:

- The replacement of TrickBot with QakBot as a final payload
- A 1,000 percent increase in Emotet downloads, correlating with Emotet's packer change, which causes the Emotet loader to have a lower detection rate across anti-virus software
- Operators using new Word document templates
- Operators using password protected archives containing malicious macros to bypass detections

While we expect Emotet's operators to continue to employ major pauses, we believe it is highly likely that Emotet will continue to be a major threat and impact organizations across a variety of industries throughout the end of the year and into 2021.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) issued an alert highlighting Emotet's recent activity throughout Q3 2020. In the alert, MS-ISAC and CISA shared Snort signatures for use in detecting network activity associated with Emotet. In addition, CISA and MS-ISAC provided numerous best practices that they recommend security teams follow to mitigate against Emotet attacks.

Figure 2: Emotet activity throughout Q3 2020 (Source: Recorded Future)

Cryptocurrency Mining Malware Develops Dangerous Functionalities

Cryptocurrency mining malware steals resources on a system to mine cryptocurrency for monetary gain. Threat actors have used this malware to target individual systems and major corporate networks. Until recently, cryptocurrency mining malware was mainly used for this purpose; however, in Q3 2020, threat actors have increasingly augmented their cryptocurrency mining malware by adding functionalities such as credential stealing or access capabilities.

This shift renders cryptocurrency mining malware more dangerous to organizations, rather than solely as a tax on corporate digital resources. Because the cryptocurrency mining malware operators are financially motivated, it is possible they will use these new functionalities to further any profit by selling stolen victim data. In Q3 2020, we observed multiple cryptocurrency mining malware operators adding functions beyond cryptomining to their malware:

- On July 28, 2020, a new malware variant, dubbed Doki, was reported to be infecting Docker Servers using the Dogecoin cryptocurrency blockchain to dynamically generate command and control (C2) domains. Instead of delivering cryptocurrency mining malware, the botnet began delivering Doki.
- On August 17, 2020, researchers identified activity from a cybercriminal group, tracked as TeamTNT, conducting what appears to be the first cryptomining malware operation that steals Amazon Web Services (AWS) credentials from infected servers.
- On August 21, 2020, reports emerged detailing a Monero mining script that was found to be embedded in the Elastic Cloud Compute (EC2) servers of AWS Community Amazon Machine Instances (AMI). While the primary goal of the malware is cryptocurrency mining, it also allows attackers to connect to Windows machines and use it to access other sensitive areas of the environment, such as accessing the entire EC2 infrastructure of the affected AWS account.
- On August 25, 2020, a new variant of the Lemon_Duck cryptomining malware was observed targeting Linux-based systems via SSH bruteforce attacks to infect servers running Redis and Hadoop instances. The new version of Lemon_Duck added a module that exploits CVE-2020-0796, also known as SMBGhost, a Windows SMBv3 Client remote code execution (CE) vulnerability that allows attackers to collect information on compromised machines.

The added malicious functionalities outlined above have potential to cause more extensive damage to organizational systems than "traditional" cryptocurrency mining malware. Organizations can familiarize themselves with prevalent cryptocurrency mining malware variants outlined by the New Jersey Cybersecurity & Communications Integration Cell here.

Mobile Malware

Android-based malware dominated the mobile threat landscape during Q3 2020. This is a continuation of the observations from Q2 2020, with some mobile malware like SpyNote resurfacing. Toward the end of the quarter, Recorded Future observed a spike in references to Cerberus Banking Trojan, likely due to the leak of the malware's source code. While the functionalities of these malware differ, their core functionality of stealing Android user data without their knowledge is a testament to the continuous development of mobile malware, from spyware to trojans, as reflected in the previous two quarters.

SpyNote

Among the instances of mobile malware, Recorded Future observed discussions of SpyNote occurring on multiple underground forums during Q3 2020. SpyNote, also referred to as SpyMax Android RAT, is a malware with many surveillance features, including keylogging, location details, and remote command execution. The tool's developer, known as "Scream," is highly likely to be a native Arabic speaker based in the Middle East who is active on the Arabic-language hacker forum — Sa3ka (شبكة الصاعقة العربية, "Arab Thunderbolt Network").

In Q2 2020, we covered major trends in the distribution of fake COVID-19 tracing apps, some of which used SpyNote malware. While we witnessed a decline of COVID-19-related mobile malware lures, SpyNote remained a prominent topic of discussion in Q3 2020 on underground forums such as Cracked Forum. Forum posts indicate continued development of SpyNote, with the advertisement of version 6.4 and claims that the new version adds increased application stability and encryption functionality and an improved graphical user interface. SpyMax is another Android RAT by the same author.

Based on the observed underground activity, **Insikt Group believes that SpyNote will continue to be used by threat actors, particularly in regions with high volumes of Android users such as the Middle East and Southeast Asia.**

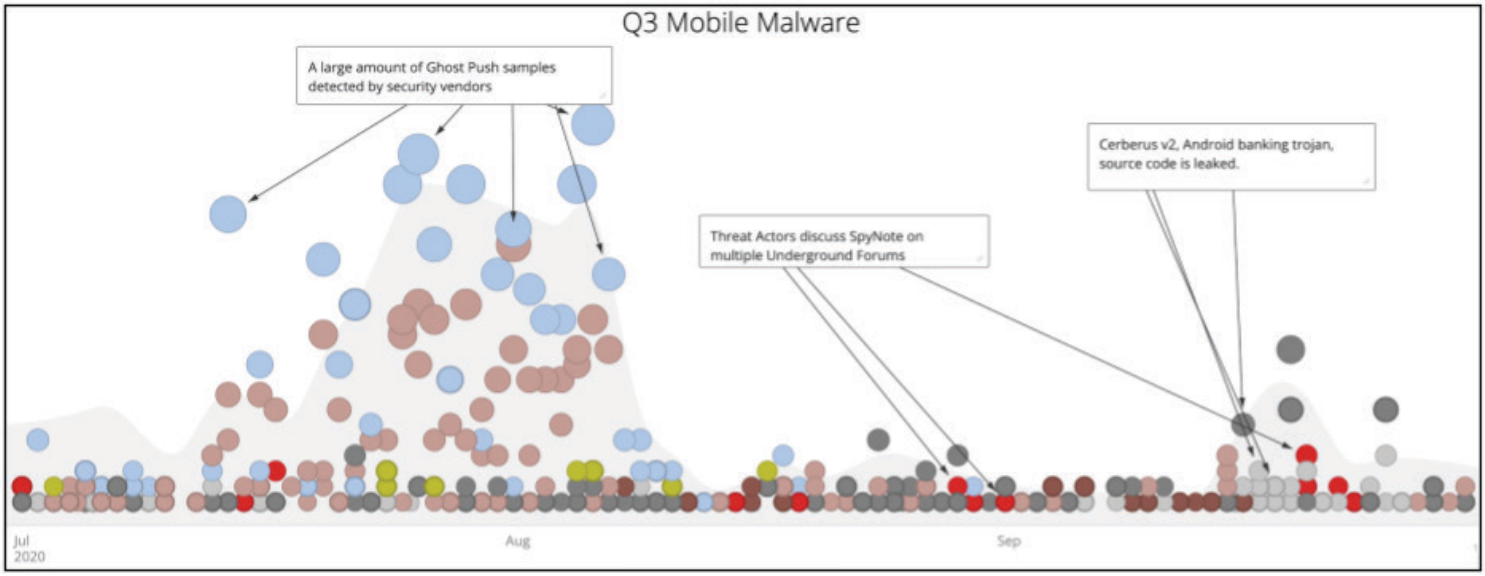

Figure 3: Mobile malware trends in Q3 dominated by Android malware (Source: Recorded Future)

Cerberus Banking Trojan

In July 2020, Recorded Future observed "ANDROID-Cerberus," the developer or seller of the Cerberus Android bot project, auctioning it off on Exploit and XSS forums. The threat actor was selling malware that included the source code, administrative panel source code, payload servers, and the customer database with all active licenses and contact information. The starting price of the auction was $25,000 or the malware could be purchased directly for $100,000. The threat actor shut down their criminal enterprise on August 11, 2020, allegedly due to a lack of time to devote to the malware, and shared the source code of the Cerberus Android Bot infrastructure, including "Cerberus v1 + Cerberus v2 + install scripts + admin panel + SQL DB." The threat actor also shared the full set of available web injects.

The source code included multiple well-crafted web pages impersonating banks, financial institutions, and social networks. Since Cerberus is abusing the accessibility functionality of Android to perform web injections and appears to have access to a wide variety of data on the user's phone (including text messages, Google Authenticator codes, and the unlock pattern for the device), two-factor authentication (2FA) will not fully mitigate the threat. Hundreds, if not thousands, of threat actors will likely use the leaked code and methodology in their daily fraudulent activity. **Banking and financial institutions will likely see a spike in fraud attempts as a result of the source code being released.**

Outlook

On October 1, 2020, the U.S. Treasury Department issued a pair of advisories in an attempt to raise awareness on ransomware attacks and outline the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. The advisories illustrate the assertive stance the U.S. is taking in response to extortionary ransomware attack payments. The U.S. government has recommended that organizations do not pay the ransom as payments benefit illicit threat actors and can undermine the national security and foreign policy objectives of the U.S. However, guidance from the U.S. government and other global agencies has been inconsistent, according to the security intelligence news website The Record by Recorded Future: "There are no unified federal rules that address how organizations should handle the rapidly growing problem of ransomware attacks."

It is highly likely that ransomware operators will continue to persist, impact industries, and continue using extortion tactics. However, the Treasury Department advisories may impact the proliferation of organizations who are involved in facilitating the ransomware payments and will likely shift the calculations of cyber insurance companies who have frequently been willing to pay the ransom even in cases where an alternative existed, based on overall cost calculations. Despite the advisory, victims are likely to continue to face few options other than paying the ransom for fear of facing the public relations and legal repercussions of the sensitive data of their clients being leaked on the extortion sites.

Emotet operators are likely to continue distributing the malware indiscriminately to a large number of victims throughout Q4 2020; however, it is possible that the threat operators take a hiatus similar to that observed at the end of 2019, when researchers observed a decrease in activity between December until mid-January 2020. Nonetheless, Emotet remains a major threat to organizations as it is now primarily a dropper for additional malware, including different ransomware families. This was highlighted in an alert published by CISA and MS-ISAC on October 6, 2020 which warned of a significant increase in malicious cyber threat actors targeting state and local governments with Emotet phishing emails. Organizations should familiarize themselves with Emotet's TTPs and follow the mitigations outlined by CISA and MS-ISAC.

While cryptocurrency mining malware has often been low on the list of prioritized threats for security teams, the abovementioned developments demonstrate the potential for this malware category to take on dangerous functionalities that could have major repercussions for organizations. If threat actors began using preexisting cryptocurrency mining malware infections or used cryptocurrency mining malware as an initial infection vector, malware operators could take advantage of the infection to distribute more dangerous malware, such as ransomware or another variant to exfiltrate proprietary data. If the trend of added functionality to cryptocurrency mining malware continues, it is likely that we will see more threat actors using these infections as a jumping point to further malicious capabilities in different malware variants into Q4 2020 and the beginning of 2021.

Android mobile malware continues to be a prevalent issue affecting users banking information and general surveillance. Because of the widespread use of Android OS devices, making up 75% of all smartphone users, and the dynamic tool sets distributed within the malware, it is likely that threat actors will continue to use Android malware to target users into Q4 2020. In addition to general Android malware, we believe that banking and financial institutions will see a spike in fraud attempts as a result of the Cerberus Banking Trojan source code being released. Organizations impacted by this trojan should familiarize themselves with the associated TTPs to strengthen their defense surrounding compromised customer accounts.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.