CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0211

Q42020 MALWARE TRENDS:

# Year Punctuated by Ransomware and Data Breaches Concludes With Sophisticated SolarWinds Attack

*This report continues our quarterly series analyzing trends in malware use, distribution, and development throughout 2020. Insikt Group used the Recorded Future® Platform to look at mainstream news, security vendor reporting, technical reporting around malware, vulnerabilities, security breaches, and dark web and underground forums from October 1 to December 31, 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 Q4 2020, ransomware operators continued to have an opportunistic mindset when conducting campaigns, putting more emphasis on data theft extortion to increase their chances of profitability. There was an increase in Egregor activity throughout the quarter, likely due to Maze ransomware operators shutting down. There was also an increase in Conti ransomware as use of Ryuk, a persistent ransomware family throughout the year, plateaued.

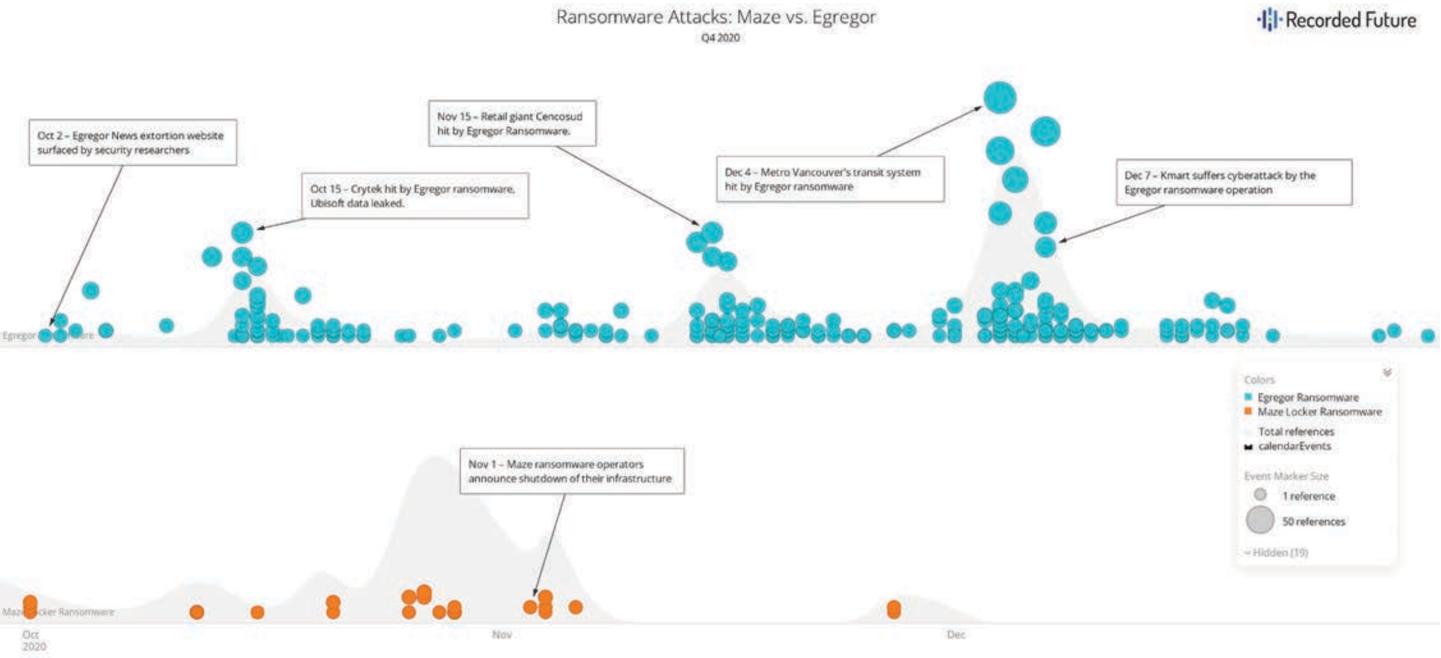
Arguably the most significant malware attack of 2020 was disclosed to the public in this period: the SolarWinds supply chain attack. This attack was significant due to the sophistication of the attack along with the volume of prominent organizations impacted, including United States government entities, along with several prominent technology companies and cybersecurity organizations. As this attack is still being investigated, it is likely that there will be more details released associated with victims targeted and infrastructure used.

Trickbot, a malware family that has been persistent and prominent throughout the year, went through notable changes in Q4 2020, as multiple organizations worked together to take down the malware's infrastructure before the November 2020 U.S. presidential election. While these efforts temporarily reduced Trickbot activity, the use of QakBot, a discrete loader malware, began to increase, likely as threat actors shifted away from Trickbot.

Lastly, Android malware continued to dominate the mobile malware landscape this quarter, with two new mobile malware variants emerging. While COVID-19-themed mobile malware activity dipped in Q3 after a high during the first half of the year, Insikt Group observed a resurgence of activity in Q4. This was especially true as virus cases increased and digital assets (websites, mobile applications, and so on) regarding the COVID-19 vaccine were released.

## Ransomware

True to their opportunistic outlook, ransomware operators continued to move toward data theft extortion in Q4 2020 to increase the profitability of their campaigns. For example, FIN11 — a financially motivated threat group that has been active since 2016 — recently used Clop ransomware in attacks, threatening to publish victims' data if they did not meet ransom demands. While the group had been using ransomware as a monetization method since 2019, using exfiltrated data to further extort victims was a shift for FIN11. The change is in line with the larger trend of threat actors directing their attention toward capitalizing on stolen data via extortion.



Ransomware Attacks: Maze vs. Egregor

Q4 2020

Oct 2 – Egregor News extortion website surfaced by security researchers

Oct 15 – Crytek hit by Egregor ransomware, Ubisoft data leaked.

Nov 15 – Retail giant Cencosud hit by Egregor Ransomware.

Dec 4 – Metro Vancouver's transit system hit by Egregor ransomware

Dec 7 – Kmart suffers cyberattack by the Egregor ransomware operation

Nov 1 – Maze ransomware operators announce shutdown of their infrastructure

*Figure 1: Timeline showing sunset of Maze ransomware operations and rise of Egregor ransomware attacks (Source: Recorded Future)*

### Egregor on the Rise Following Maze Shutdown Announcement

Egregor ransomware attacks have been on the rise since the beginning of Q4, claiming 133 victims in their first two months of operation. The ransomware is part of the Sekhmet family and first surfaced in mid-September 2020. Organizations impacted by Egregor in Q4 included video game developer Crytek, retail giant Cencosud, Metro Vancouver's transit system Translink, and department store chain Kmart.

There was a large spike in reported Egregor attacks in mid-November 2020 correlating with a "press release" from Maze Team detailing the shutdown of their ransomware affiliate program. Ransom payments have also slowly transferred from Maze to Egregor between September and October 2020, with no new Maze victims during this period. Insikt Group believes many of the affiliates of Maze ransomware have migrated to Egregor and that the ransomware variants are connected due to similarities in code, ransom notes, and payment website names.

### Increase in Conti Activity as Ryuk Activity Plateaus

In Q3 2020, researchers speculated that Conti ransomware, a private ransomware operation, would be a successor to Ryuk ransomware due to similarities in code and ransom notes. This was further supported by a steady decline in Ryuk attacks since July 2020 as Conti operators launched an extortion website, Conti News, and attacked more organizations. The Ryuk decline may have been a result of attempts to take down the infrastructure of TrickBot, a botnet commonly used to distribute Ryuk. After a reduction in attacks throughout Q3 2020 and the first month of Q4 2020, Ryuk activity has plateaued since November 2020. Ryuk's operators continued to claim victims such as the University of Vermont Health Network and K12 Inc in October and November 2020, respectively. Conti activity also flattened but persisted, impacting companies such as Advantech and Total System Services, Inc in November and December 2020, respectively. Both Conti and Ryuk will likely remain active and continue to target organizations across industries as long as it is profitable.

All organizations should maintain offline backups and implement proactive security measures such as multi-factor authentication (MFA) and network segmentation whenever possible to reduce the risk and impact of a ransomware infection.

## Desktop Malware

In Q4 2020, the supply chain attack on SolarWinds, which led to the infection of over 200 organizations, including prominent U.S. government entities as well as well-known technology organizations, was arguably the most significant malware event of the year due to the victims impacted and the sophistication of the attack.

Outside of the SolarWinds supply chain attack ,threat actors shifted away from Trickbot to another persistent downloader, Qakbot ,after Trickbot was targeted in a coordinated takedown effort.

## SolarWinds Supply Chain Attack

The SolarWinds supply chain attack, which was disclosed on December 13, 2020, was a uniquely complex and sophisticated attack, with a diverse set of major victims. The investigation into the attack is still ongoing, with limited details released to the public. What is known is that a sophisticated threat group was able to infect a broad number of victims, many of which were U.S. government entities along with major technology organizations and cybersecurity companies.

### *Technical Details of the Attack*

A SolarWinds digitally signed component of the Orion software framework containing a backdoor, known as SUNBURST (or Solorigate), was delivered via trojanized updates. After an initial dormant period of up to two weeks, SUNBURST retrieves and executes commands, called "Jobs", that include the ability to transfer and execute files, profile the system, reboot the machine, and disable system services. The malware masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity. Multiple trojanized updates were digitally signed from March to May 2020 and posted to the SolarWinds updates website.

After a dormant period of up to two weeks ,the malware will attempt to resolve a subdomain of *avsvmcloud[.]com* created using a custom domain generation algorithm) DGA .(The DNS response will return a CNAME record that points to a command and control) C2 (domain .The C2 traffic is designed to mimic normal SolarWinds API communications .Using SUNBURST, the attackers were identified deploying a previously unseen memory-only dropper to ultimately load Cobalt Strike Beacon.

Following initial access, Microsoft researchers identified the attackers gaining administrative access either using compromised privileged account credentials (such as stolen passwords) or by forging SAML tokens using compromised SAML token-signing certificates. (Security Assertion Markup Language, or SAML, is an open standard, XML-based markup language used for exchanging authentication and authorization data, such as single sign-on authentication.) In some cases, these certificates were obtained through accessing the database which supports the SAML federation server using administrative access and remote execution capabilities. Once the certificate has been acquired, the threat actor can forge SAML tokens and sign them. By doing this, they can access any resources configured to trust tokens signed with that signing certificate. This includes forging a token that claims to represent a highly privileged account in Azure Active Directory.

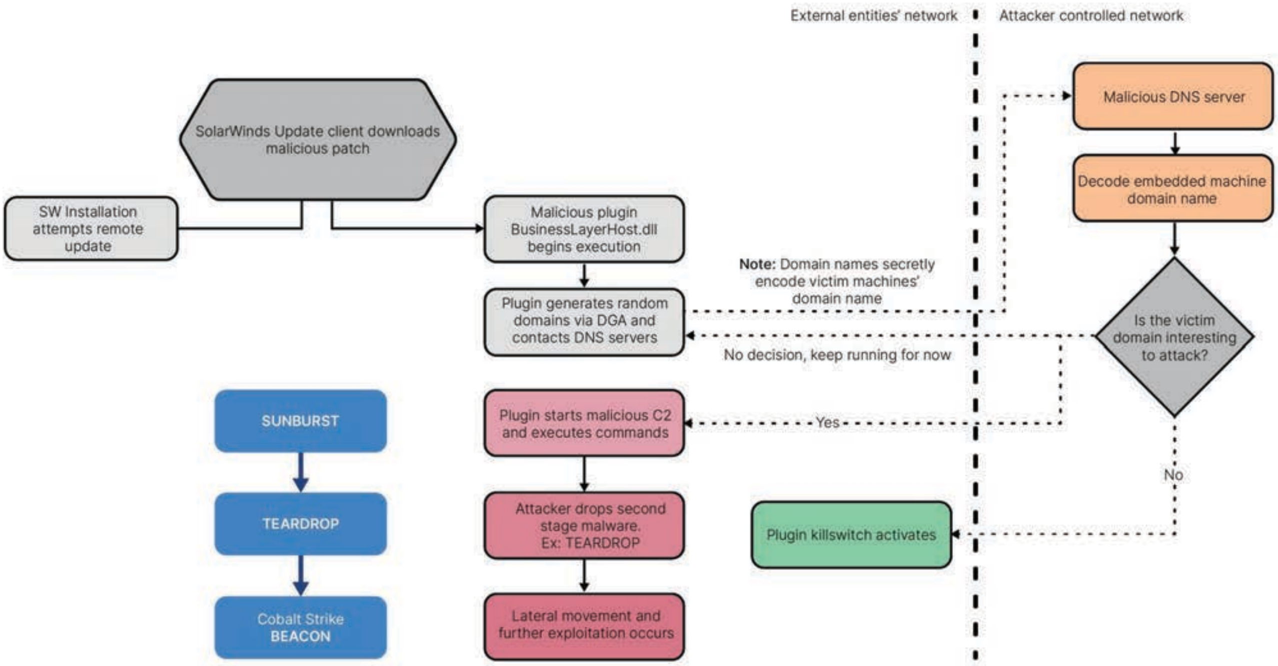

External entities' network
Attacker controlled network
SolarWinds Update client downloads malicious patch
SW Installation attempts remote update
Malicious plugin BusinessLayerHost.dll begins execution
Plugin generates random domains via DGA and contacts DNS servers
Note: Domain names secretly encode victim machines' domain name
Malicious DNS server
Decode embedded machine domain name
Is the victim domain interesting to attack?
No decision, keep running for now
Yes
No
Plugin starts malicious C2 and executes commands
Attacker drops second stage malware. Ex: TEARDROP
Lateral movement and further exploitation occurs
Plugin killswitch activates
SUNBURST
TEARDROP
Cobalt Strike BEACON

*Figure 2: SolarWinds attack topology (Source: Recorded Future)*

Since the disclosure, researchers have identified four discrete malware variants used in the attack: Sunspot, SUNBURST, TEARDROP, and most recently, RAINDROP. On January 19, 2021, Symantec published their findings on an additional malware family used in the SolarWinds attacks called RAINDROP. Unlike TEARDROP, which is delivered by the initial SUNBURST backdoor, Symantec has not seen any evidence of RAINDROP being delivered directly by SUNBURST. Symantec observed RAINDROP elsewhere on infected networks where at least one computer had already been compromised by SUNBURST, indicating that RAINDROP is used by the attackers to move laterally and deploy malicious payloads on computers of interest. Of note, both RAINDROP and TEARDROP act as loaders for Cobalt Strike Beacon; however, they use different packers and Cobalt Strike configurations. In addition, RAINDROP and TEARDROP have minor similarities in the names of exported functions that can be accessed by other programs, which reference the Tcl programming language and its toolkit, dubbed Tk.

At this time, the activity has been attributed to state-sponsored Russian threat actors. Several organizations including FireEye have attributed the activity to UNC2452, while the U.S. government sources have attributed the activity to Russia more generally.

### *SolarWinds Mitigations*

Since the attack, we have observed several instances of individuals attempting to exploit the attack for profit including a threat actor offering a discount for FireEye red team tools, source code, binaries, and documentation on solarleaks[.]net. Some security researchers received the solarleaks offer with suspicion and suggest that it is either a scam or a misinformation campaign. FireEye released YARA rules, making the red team tools binaries unfit to use, but the source code leak creates a potential for obfuscation and further development of it. Additionally, a proof-of-concept exploit for CVE-2020-10148 affecting the SolarWinds Orion was published to GitHub on December 30, 2020. It is highly likely that threat actors will continue to advertise scams or post content as a way to profit from the attack.

Anyone using SolarWinds within their technology stack should take the following initial mitigation measures:

- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking illicit connection attempts from — the external IP addresses and domains listed as tagged entities below.
- Review historical log data for the presence of these indicators.
- Consider conducting YARA scans across your organization and deploying Snort and ClamAV rules provided within FireEye’s SUNBURST countermeasures GitHub page.
- Isolate SolarWinds servers while further review and investigation is conducted.

On February ,2021 ,8 US-CERT released malware analysis reports for Teardrop and Sunburst malware .Organizations can use the indicators within the reports for detection and mitigation across their network.

## Trickbot: The Rise, the Fall, and the Shift to QakBot

This quarter ,defenders took a strong ,defensive approach to mitigate prominent and persistent malware ,specifically Trickbot .By October ,2020 Trickbot was such a significant threat that a coalition of cybersecurity firms led by Microsoft orchestrated a global takedown against the Trickbot botnet, taking down 94% of Trickbot‘s C2 infrastructure .While we have observed Trickbot rebuilding their infrastructure and continuing to have significant impacts on major organizations such as Subway UK and Mattel since the takedown ,we have also seen a rise in another downloader ,QakBot ,also sometimes referred to as Qbot.

### *Trickbot Activity in Q4 2020*

Trickbot started as an advanced banking Trojan used to harvest credentials from victim systems and has evolved into a multi-purpose malware downloader and one of the largest botnets in the world .According to Microsoft ,Trickbot had infected over a million computing devices around the world since late.2016 Throughout the year ,Trickbot operators constantly updated the malware ,adding new functionalities and developments .Trickbot was also a prominent downloader for well-known ransomware families including Ryuk and Conti.

On October ,2020 ,12 U.S .Cyber Command and an industry coalition led by Microsoft separately attempted to disrupt Trickbot‘s infrastructure .Both cited the dangers of ransomware being deployed at an aggressive tempo for targeting election infrastructure by Trickbot operators as the reasoning for their actions.

- In September 2020, Cyber Command poisoned Trickbot infections by pointing their command and control configurations to beacon to the localhost, effectively severing Trickbot operators’ access to existing infections.

- On October 12, 2020, Microsoft and its partners ESET, Lumen, Symantec, FS-ISAC, and NTT announced a unique trademark legal filing to seize Trickbot servers located in the U.S. Microsoft claimed Trickbot used Microsoft code and imagery, convincing a U.S. court to grant them access to the servers, crippling a portion of Trickbot's infrastructure.
- On October 18, 2020, Microsoft stated that they had worked with global partners to eliminate approximately 94% of Trickbot's critical operational infrastructure and they had taken down 120 out of 128 servers identified as being related to Trickbot infrastructure around the world. These included both the 62 out of 69 C2 servers and the 58 out of 59 servers that the Trickbot operators tried to bring online after Microsoft's initial takedown.
- And on October 21, 2020, Insikt Group identified activity that indicated Trickbot was rebuilding its infrastructure.

### *The Shift to QakBot*

Trickbot has made a strong comeback since the takedown at the beginning of Q4. However, as Trickbot's activity initially declined from the takedown efforts, QakBot's activity increased.

QakBot is an information-stealing trojan that was first discovered in 2007 and has recently experienced a resurgence. QakBot is typically distributed through exploit kits and weaponized documents delivered through phishing campaigns. QakBot establishes persistence by adding itself to the registry run key and creating a scheduled task. Once executed, QakBot injects itself into a running process, typically explorer.exe, to evade defenses. One of the main capabilities being leveraged by threat actors deploying QakBot is its ability to load and run additional malware.

In November 2020, Egregor ransomware's operators began using QakBot in a similar fashion to Trickbot. It is likely that as Trickbot gained attention in the media and was the target of takedown efforts, threat actors began shifting to a similar loader malware to further their infections.

## Mobile Malware

The 2020 Q4 mobile malware landscape was dominated by Android malware, which is in line with our observations from Q3. Insikt Group continued to observe higher targeting of users in the Middle East, North Africa, and Southeast Asia as compared to users in other regions. Based on the large Android user base in these geographies, this trend will likely continue. Highlights of the quarter include newly discovered Android malware variants WAPDropper and Rana, along with continued discussion around COVID-19-related mobile apps. A common theme among all three of these is the initial access vector, which is usually through trojanized apps such as for games or utilities that are available on third-party app stores. Mobile device users, particularly Android users, should only download applications from trusted developers and verified app stores and to keep device operating systems and applications up to date with the latest versions available. In addition, organizations with bring-your-own-device (BYOD) programs in place should set these rules to ensure that employees minimize the risk of downloading malware that could pose a risk to enterprise data.

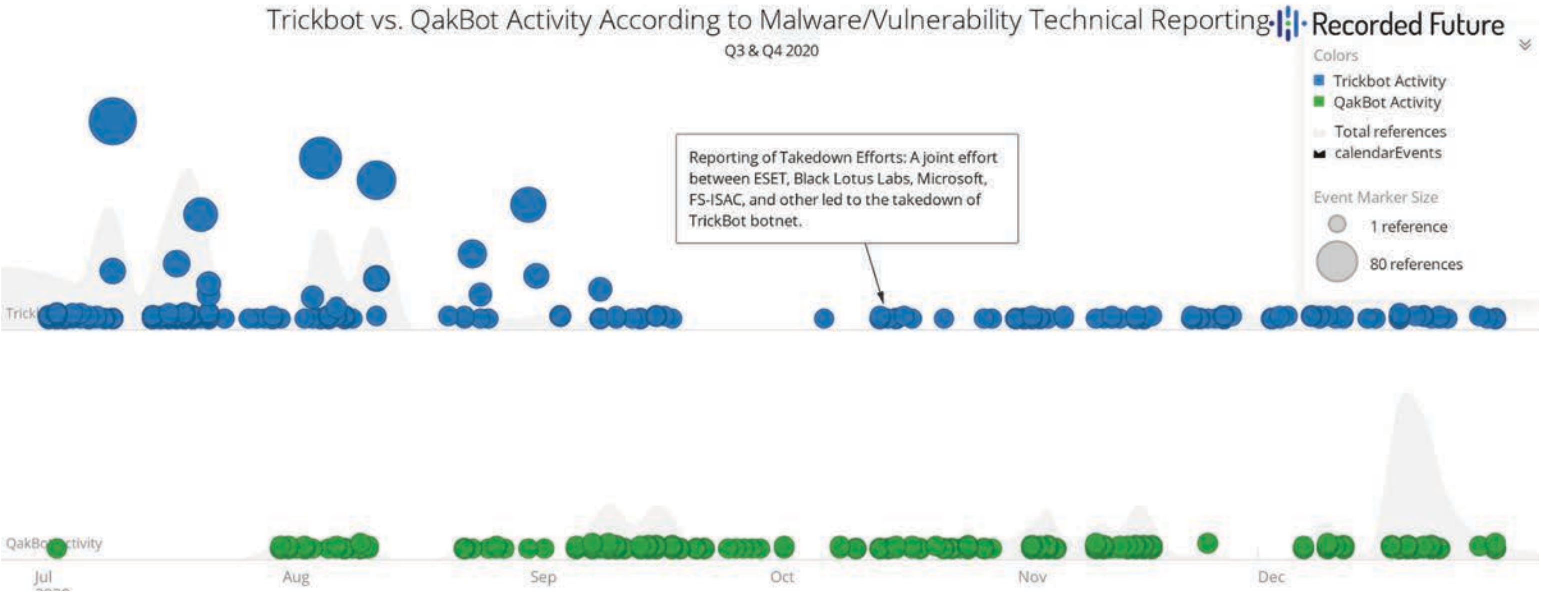
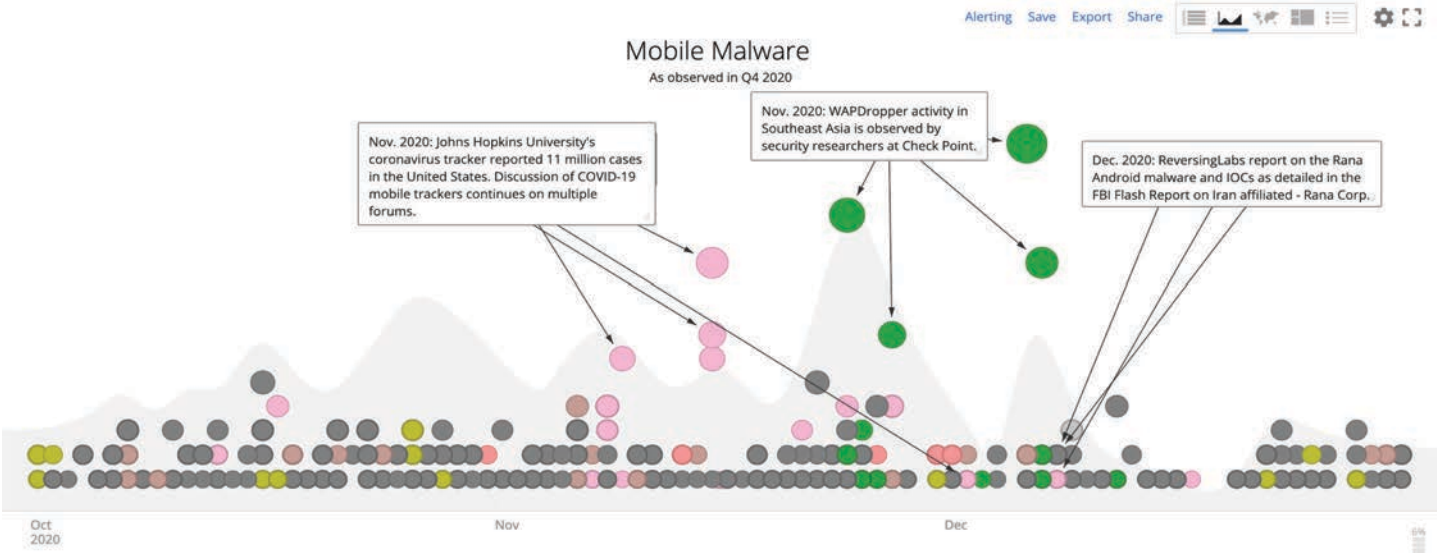


*Figure 3: Trickbot and QakBot activity according to malware/vulnerability technical reporting in Q3 and Q4 2020 (Source: Recorded Future)*



Nov. 2020: Johns Hopkins University's coronavirus tracker reported 11 million cases in the United States. Discussion of COVID-19 mobile trackers continues on multiple forums.

Nov. 2020: WAPDropper activity in Southeast Asia is observed by security researchers at Check Point.

Dec. 2020: ReversingLabs report on the Rana Android malware and IOCs as detailed in the FBI Flash Report on Iran affiliated - Rana Corp.

*Figure 4: Mobile malware timeline in Q4 2020 (Source: Recorded Future)*

## WAPDropper

In November 2020, researchers at Check Point identified a new malware variant, dubbed WAPDropper. The malware was observed on third-party application stores disguised as legitimate apps (such as email or children's games) designed to target Android users in Thailand and Malaysia.

WAPDropper contains two modules. The first module is the dropper, which is responsible for downloading the second stage malware. A second module is a premium dialer that subscribes unknowing victims to premium telecommunications services.

The WAPDropper infection chain starts with the user downloading a trojanized app hosted on third-party stores to their mobile device. Upon execution, WAPDropper contacts its C2 server to download the premium dialer module. The module opens a web-view page and contacts premium services such as Super Eagle, a Chinese company that offers machine learning solutions for image recognition. The infected users would also receive large phone bills for using various types of services.

This kind of attack, also known as "WAP fraud" or "WAP billing", was popular in the late 2000s when WAP was a popular method of paying for content online in the early stages of mobile networks, but the technique dissipated as smartphones came out. However, it managed to return in 2017 as cybercriminals realized that many modern phones and telephone companies still supported the older WAP standard.

## Rana Android Malware

A new variant of Rana Android malware was uncovered by researchers at ReversingLabs in December 2020. Their report followed the FBI's threat analysis report on Rana Corp, a front company for activity related to Iranian threat group APT39. ReversingLabs found that the Rana variant has improved surveillance capabilities than its predecessor.

Though the initial infection vector of Rana is unknown, the malware is downloaded when the malicious APK file "com[.]android.providers.optimizer" is executed. Rana requires fewer permissions than its previous version from the local device, what researchers noted is an attempt to avoid detection. Some functions for Rana include collecting SMS data, logging phone call data, and taking photos at login success or failure. On top of this, it can collect location data and application data, including from WhatsApp and Telegram through keystroke logging. While these are not uncommon for Android spyware, a unique feature to Rana is the creation of a custom WiFi access point and forcing the device to connect to it.

Rana is a further iteration of the ever-evolving mobile spyware landscape. Insikt Group reported on the increased observation of spyware in Q2 2020. While the quantity of spyware in the mobile malware landscape has remained consistent, it is clear that threat actors are continuing to improve the quality of their spyware for defense evasion and persistence.

### COVID-19 Mobile Applications

While Q3 2020 did not display nearly as much COVID-19 mobile malware activity as the first half of the year, there was a resurgence of activity in Q4 2020, particularly as cases increased and digital assets (like websites, mobile applications) regarding the COVID-19 vaccine were released. Whether they were created with intentional surveillance capabilities or hastily constructed to fulfill a need, these applications continue to pose security risks for users. While the activity Insikt Group observed was not directly linked to mobile malware instances, we advise continued vigilance as information is released. Insikt Group research on previous uses of the COVID-19 as a lure for malware can be found here.

## Outlook

In 2021, ransomware will likely continue to be a persistent and significant threat to organizations globally, especially those in critical sectors such as organizations working in the vaccination distribution supply chain, as ransomware operators continue to see success in using extortion websites. It is likely that more ransomware families will emerge throughout 2021. Ransomware operators will also continue to find ways to hasten their operations, using central servers to distribute their payloads across an enterprise, through use of multiple offensive security tools and malware families.

It is very likely that new information regarding the SolarWinds supply chain attack will be disclosed in the upcoming months, along with the emergence of additional victims impacted outside of the SolarWinds supply chain attack, as seen with the attack on Malwarebytes' Microsoft Office 365 and Azure environments. Despite the variety of malware families involved, the intrusions all extensively use on-host commands, relying on native tools and credential re-use tactics to remain in victim networks. It is likely that these threat actors are involved in other intrusions that will remain undetected for long periods to facilitate long-term intelligence requirements.

Lastly, it is highly likely that Android malware will continue to dominate the mobile malware landscape throughout 2021 as it is easier to infect compared to other mobile operating systems. In alignment with our findings, we expect some of these new Android mobile malware variants will be used to exfiltrate user data, particularly for financial and espionage purposes as was observed throughout 2020. In addition, it is likely that there will be continued threats from the development of legitimate and malicious apps associated with the COVID-19 pandemic and vaccination distribution throughout 2021, especially as vaccine distributions increase.

## About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.