UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 17-CR-124

MARCUS HUTCHINS,

Defendant.

UNITED STATES' SENTENCING MEMORANDUM

The United States of America, by its attorneys, Matthew D. Krueger, United States Attorney for the Eastern District of Wisconsin, and Assistant United States Attorneys Benjamin Proctor and Benjamin Taibleson, files this memorandum in advance of the sentencing hearing set for July 26, 2019.

I. Introduction.

Before he became known internationally for his role in thwarting the WannaCry ransomware attack in 2017, Marcus Hutchins built and sold sophisticated malware packages that had one purpose: to covertly steal personal information, including banking credentials, from unsuspecting victims around the world. He did so because, put simply, he wanted to make money. It is this darker side of Hutchins' life that brings him before the Court for sentencing in this case.

At issue in this case are two of Hutchins' creations: UPAS Kit and Kronos. Hutchins wrote them, and his accomplice, "Vinny," advertised and sold them in

online hacking forums. The FBI began investigating the actors behind UPAS in 2012 and Kronos in 2015. In late 2016, the FBI obtained chat logs establishing that Marcus Hutchins, aka "MalwareTech," created these malware products.

In May 2017, after the FBI obtained Hutchins' chat logs, and while it finalized its investigation, Hutchins was publically credited with stopping the WannaCry ransomware outbreak. WannaCry, while significant, is entirely separate from this investigation and prosecution. In July 2017, Hutchins travelled to the United States and was arrested for his role in marketing and distributing Kronos and UPAS.

In May 2019, Hutchins entered a guilty plea to Counts One and Two of the superseding indictment. Doc. #124. Per the plea agreement, the government agrees not to make a sentencing recommendation. In this memorandum, the government will simply highlight aspects of the offense and the defendant's history that are relevant to the Court's sentencing decision.

II. Analysis of the Factors Under 18 U.S.C. § 3553(a).

The sentence the Court imposes should be sufficient, though not greater than necessary, to reflect the seriousness of the offense, promote respect for the law, adequately punish the crimes committed, deter other criminal conduct, protect the public from the defendant and provide for any particularized needs of the defendant. 18 U.S.C. § 3553(a)(2). In determining the appropriate sentence, the Court must consider the factors set forth in 18 U.S.C. § 3553(a). *United States v. Harris*, 490 F.3d 589, 593 (7th Cir. 2007). In addition to the goals outlined above,

these factors include the nature and circumstances of the offense and the history and characteristics of the defendant; the Sentencing Guidelines range; and the need to avoid unwarranted disparities among similarly situated defendants.

A. The sentencing guidelines.

In the plea agreement, the parties agree on the base offense level for both counts and on several specific guidelines adjustments. These include increases for committing an offense involving at least 10 victims under U.S.S.G. § 2B1.1(b)(2)(A); for committing a substantial part of the offense outside of the United States under § 2B1.1(b)(10); for computer hacking in violation of 18 U.S.C. § 1030 with an intent to obtain personal information under § 2B1.1(b)(18)(A); and for committing an offense in violation of 18 U.S.C. § 1030(a)(5) under § 2B1.1(b)(19)(A)(ii). The parties further agree to recommend a reduction for conspiracy under § 2X1.1(b)(2), and a reduction for timely acceptance of responsibility under § 3E1.1.

The parties disagree over whether there should be an adjustment for loss under § 2B1.1(b)(1). While it is undisputed that Hutchins' malware has been used to infect numerous computers all over the world, loss calculation is challenging because of the very nature of the offense and conduct of the defendant: the defendant and his accomplice communicated via encrypted communications, the malware was sold through encrypted communications, the defendant worked to disguise his role in the offense, the malware was designed to be undetectable on victim computers, the offense was perpetrated overseas, and the defendant's property facilitating the offense was neither turned over to law enforcement nor

recovered. Further, it is challenging to calculate actual monetary losses stemming from others' use of Trojans like Kronos/UPAS to steal personal information. This is true not only due to the nature of the offense, but also because attackers often sell the information they harvest from victim computers to other criminals who will not know how or when the information was obtained. With all of this in mind, however, the government has provided the presentence report writer with several facts relevant to loss as defined under § 2B1.1(b)(1).

In the end, any calculation of "loss" under § 2B1.1(b)(1) will be an estimate. This is due to limitations noted above, many of which were the direct aim and achievement of defendant. But this court "need only make a reasonable estimate of loss." § 2B1.1(b)(1) Application Note 3(C). The facts the government provided to the PSR writer provide a reasonable basis for a reasonable estimate of that loss.

Finally, § 2B1.1 does not account for the invasion of personal privacy and security inherent in these types of malware cases. Therefore, regardless of the guidelines, "loss" should be considered as part of the overall offense under 18 U.S.C. § 3553(a).

B. Nature and circumstances of the offense.[1]

While computer hacking is often viewed an offense committed by lone wolves, that is not necessarily the reality. In reality, hacking can be organized, with actors exchanging information and working together to better victimize their targets. One

[1] Additional details of the offense are set forth in the plea agreement, Doc. #124, and the presentence report.

form of hacking involves the use of malicious software (malware) to infect computers and steal information. Creating effective malware requires special skills not possessed by all hackers. Thus, marketplaces develop where malware creators can market their wares to those seeking to attack others. Those same markets provide space where attackers can sell the information they steal from victim computers. Moreover, those who create malware may want assistance in effectively marketing it to other hackers. This confluence gives rise to business partnerships intended to maximize sales and profits.

Marcus Hutchins is a skilled malware coder. Between July 2012 and September 2015, Hutchins created and helped market malware known as UPAS Kit and Kronos. Hutchins wanted to make money, but he also wanted to insulate himself from potential capture by delegating the actual sales and servicing of his products. Therefore, he collaborated with an individual known by aliases such as "Aurora123," "Vinny," and "VinnyK," who advertised and sold the malware. Hutchins would periodically update the malware, and Vinny would keep in contact with customers. Hutchins and Vinny agreed to split their profits evenly.

Kronos is a banking Trojan. A Trojan is a type of malware disguised as something else (such as an email attachment) to trick victims into downloading and running malicious code on their computers. The malicious code allows the attacker to steal sensitive information (like financial data, emails, and passwords) from a victim computer without the victims' knowledge. Kronos, in particular, has multiple functions. It was designed to give the attacker the ability to steal banking

credentials from victims' computers using a process called keylogging. It also had "form grabber," "web-inject," and virtual network connection ("VNC") capabilities.

A form grabber intercepts data being sent from a computer's internet browser to a website. For Kronos, this feature gives the attacker the ability to steal banking login credentials and personal information when a victim tries to access online banking services.

Web injects work by intercepting and modifying data being sent from a website to a computer's internet browser. The modifications are typically fraudulent invitations for the victim to provide unnecessary personal and account information. That information is then covertly relayed to the attacker's system. In banking Trojans, web injects can be configured to identify specific banking websites, and then inject content specifically referencing those banks.

VNC is a graphical desktop sharing system that gives users remote access to another computer. For purposes of malware, VNCs establish a connection to the victims' computer, which gives the attacker the ability to perform any task as if the attacker was physically present at the victim computer.

Kronos was configured to work on multiple internet browsers, including Chrome, Internet Explorer, and Firefox. Once installed, it would communicate with the attacker's command-and-control computer, relaying stolen information, downloading more malware, or performing any other malicious activity directed by the attacker. After an attacker purchased the Kronos malware package from

Hutchins and Vinny, the attacker could deploy that malware in a variety of ways to try to infect as many victim computers as desired.

UPAS worked in a manner similar to Kronos as a banking Trojan. An FBI computer scientist who examined both UPAS and Kronos called Kronos an updated version of UPAS with more features and further code development.

In 2012, Hutchins and Vinny (going by "Aurora123"), advertised UPAS Kit on a hacking forum. The advertisement stated in relevant part: "Upas is a modular hxxp bot, with was created with one aim—to save you some headaches. . . . In general the system operates silently without alerting antivirus programs." The advertisement listed the many features of UPAS, including a USB spreader, FTP grabber, form grabber, its ability to work on various internet browsers, and prices. Later, in November 2012, Aurora123 advertised that UPAS was updated to include webinjects. A confidential source working with the FBI purchased UPAS from Aurora123 in 2012.

Starting in 2014, the FBI observed "Vinny" advertising Kronos in various online forums dedicated to the sales of illegal goods and services. In 2014, an FBI confidential source made contact with Vinny and chatted about Kronos' functionality. Vinny directed the source to a video on YouTube that Vinny and Hutchins used to promote sales of Kronos. The video walks through how to easily operate the Kronos control panel, and then demonstrates how the malware collects and stores user credentials after a visit to an Amazon account.

On June 11, 2015, an FBI source arranged the purchase of Kronos from Vinny. After the transfer of funds was complete, Vinny configured the control panel using domains that the source had provided to Vinny, and transferred the Kronos code to the source. A few weeks later, Vinny contacted the source, asking how Kronos was working and whether the source needed crypting services for Kronos. "Crypting" is the process of scanning malware against antivirus tools to see if those tools detect and block the malware. If the malware is blocked, the crypting service makes custom changes to the malware code so that it appears as something benign to the antivirus tools.

As Hutchins acknowledges, since 2014, Kronos has been used to infect numerous computers around the world and steal banking information. *See* Doc. #124 Att. A at 1. Reports of Kronos' impact on banks in Europe were published back in 2014. *See, e.g.,* "New Banking Trojan 'Kronos' Attacks French Banks," *SC Magazine UK*, Aug. 5, 2014, *available at* https://www.scmagazineuk.com/new-banking-trojan-kronos-attacks-french-banks/article/1480575 (last visited July 19, 2019); *see also* "UK Banks Hit with New Zeus Sphinx Variant and Renewed Kronos Banking Trojan Attacks," *Security Intelligence*, Oct. 2, 2015, *available at* https://securityintelligence.com/uk-banks-hit-with-new-zeus-sphinx-variant-and-renewed-kronos-banking-trojan-attacks/ (last visited July 19, 2019).

Authorities in Poland identified Kronos as one of the top four banking Trojans infecting Polish systems in 2014. Later reports noted Kronos' impact on other countries, including Canada and the United States. *See* "Banking Trojans go

Loonie for Toonies: Dridex, Vawtrak and Others Increase Focus on Canada," *Proofpoint*, June 29, 2016, *available at* https://www.proofpoint.com/us/threat-insight/post/banking-trojans-dridex-vawtrak-others-increase-focus-on-canada (noting a spam attack in May 2016 that loaded Kronos, which was configured to target U.S., Canadian, and Australian financial services websites).

Reports of Kronos infections continue through the present. *See, e.g.,* "Kronos Banking Trojan Used to Deliver New Point-of-Sale Malware," *ProofPoint*, Nov. 15, 2016, available at https://www.proofpoint.com/us/threat-insight/post/kronos-banking-trojan-used-to-deliver-new-point-of-sale-malware (last visited July 19, 2019); "Kronos Reborn," *ProofPoint*, July 24, 2018, available at https://www.proofpoint.com/us/threat-insight/post/kronos-reborn (last visited July 19, 2019). The Kelihos botnet, which infected hundreds of thousands of victim computers, was observed loading Kronos on computers through an email phishing campaign in late 2016. *See, e.g.,* Arora, et. al., "Kelihos Botnet: A Never-Ending Saga," *Annual ADFSL Conf. on Digital Forensics, Security and Law* 2017, p. 18, available at https://commons.erau.edu/cgi/viewcontent.cgi?article=1271&context=adfsl.

Leading international cyber security firms have reported hundreds of Kronos alerts over the years. For instance, one leading firm detected more than 600 specific instances of Kronos between 2014 and 2019 around the world, including more than 100 in the United States. The data shows the infections across many sectors, including government, financial services, education, manufacturing, technology, and transportation. Another international firm detected more than 200 different

variations of Kronos between 2014 and 2019, each variation potentially representing numerous infected machines. The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), reports that Kronos botnets have had a modest presence since 2014 and remain active today. CISA and a third-party firm observed thousands of alerts for Kronos between 2014 and 2019, with a significant increase between 2015 and 2017.[2] *See* Exhibit A.[3]

C. History and characteristics of the defendant.

Marcus Hutchins is a young man with an obvious talent for coding. Unfortunately, early on, he decided to use that talent to create devices with the sole purpose of helping steal from innocent victims. He pursued that path because he was greedy and thought he would make around $100,000 per year selling malware. *See* Doc. #124 Att. A at 3. While records show that Vinny and Hutchins sold several packages of malware, Hutchins later complained to a friend that, despite his best efforts, he did not profit as much as he had hoped. Doc. #124 Att. A at 3.

Marcus Hutchins has since made a good decision to turn his talents toward more positive ends. He has a job in which he focuses on detecting and combating malware. And in May 2017, Hutchins helped stop the WannaCry ransomware attack that was crippling computers around the world. For this act, Hutchins rightly received international acclaim and notoriety. With this in mind, the

[2] Reporting entities note that, due to the nature of the research topic, some false positives are possible.

[3] Exhibit A is a report produced by CISA providing general information regarding Kronos.

government made concessions in the plea agreement to Hutchins' benefit, while still holding him accountable for his criminal conduct.

Also to his credit, Hutchins has accepted responsibility for his illegal conduct and timely entered a guilty plea. This decision was made after Hutchins pursued and lost several pretrial motions to suppress evidence and dismiss counts, but his decision to acknowledge guilt is undoubtedly a positive aspect for the Court to consider.

D. Imposing a sentence that reflects the seriousness of the offense, promotes respect for the law, and provides a measure of deterrence.

In considering the factors under 3553(a), the government believes that the serious nature of the offense, the need to promote respect for the law, and the need to provide a measure of deterrence to other malware developers are particularly important.

It cannot be disputed that this offense is serious. Criminals who develop and sell malware are at the root of computer hacking crimes. Careful development of effective malware is a time consuming effort, demanding special skills possessed by few people. By creating and selling sophisticated malware, actors like Hutchins equip hackers with tools to cause extensive harm on a worldwide scale. For this reason, law enforcement agencies dedicate substantial resources to identifying and prosecuting malware developers, sellers, and users.

Hutchins and his partner dedicated years to developing, updating, and selling dangerous malware to anyone who would buy it. They marketed the malware specifically to criminals, using forums dedicated to illegal activities. The

central purpose of Hutchins' malware was to invade privacy and steal things of value from innocent victims. The malware was expensive and effective because it could do this without being detected, and it was designed to be easy to use. Kronos and UPAS logged the content of typed messages, as well as usernames and passwords for all manner of accounts. Such sensitive information could be used to spy on people, steal their identities, and worse. The malware was configured to detect and target victims' banking credentials, which could be used to steal victims' life savings. That was, inevitably, the primary source of its value – it is why Hutchins thought he would make a lot of money selling it.

Hutchins' malware was purchased and used by hackers. Identifying individual attackers and victims is necessarily difficult because, as noted, sales to attackers were conducted through encrypted communications, the malware was designed to be undetectable on victim computers, and Hutchins' criminal conduct took place while he resided in another country, using devices not recovered by law enforcement. But, there is no confusion as to the criminal purpose behind the development and distribution of UPAS and Kronos. The ramifications of Hutchins' inventions are still being felt today.

By all accounts, Hutchins no longer produces malware and instead uses his skills to combat malware attacks. This is a good thing. But that does not permit him or anyone else to pretend his criminal conduct was insignificant. Like a man who spent years robbing banks, and then one day came to realize that was wrong, and

even worked to design better security systems, he deserves credit for his epiphany. But he still bears responsibility for what he did.

Computer hacking has become a prevalent threat in all aspects of our society. Hacking tools like Kronos and UPAS allow criminals of all skill levels to secretly access, use, and sell victims' personal information. The internet allows these criminals to work remotely and anonymously, making it difficult for law enforcement to identify and apprehend them. It is therefore important that, when malware creators are identified, the public knows these individuals will be held accountable for their actions.

III. Conclusion

This case presents a unique mix of aggravating and mitigating circumstances for the Court to consider in arriving at the appropriate sentence. Counsel for the United States will have additional comments at the hearing.

Dated at Milwaukee, Wisconsin, this 22nd day of July 2019.

Respectfully submitted,

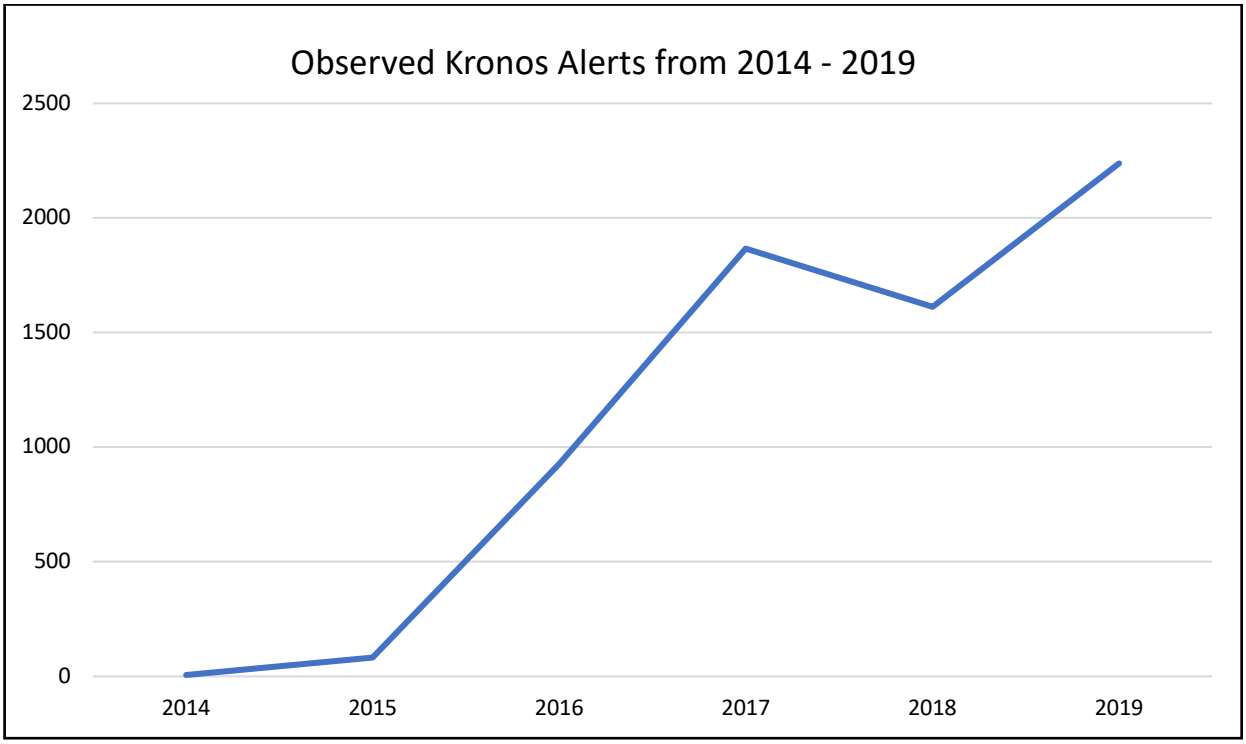
MATTHEW D. KRUEGER
United States Attorney

By: *s/ Benjamin Proctor*
BENJAMIN PROCTOR
BENJAMIN TAIBLESON
Assistant United States Attorneys
Benjamin Proctor Bar No.: 1051904
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Ave. Suite 530
Milwaukee, Wisconsin 53202
Tel: (414) 297-1700
Email: benjamin.proctor@usdoj.gov

Kronos Trojan Still Active – June 2019

Kronos is a banking malware capable of intercepting web browsing data, injecting its own malicious code into webpages, and downloading additional payloads, while also employing a user-mode rootkit to hide its presence on an infected system.

The Department of Homeland Security and a trusted third party observed Kronos activity in the United States from 2015 – 2019, with increases observed in mid-November 2016 and in quarter two of 2019. Additionally, a spike was observed on federal, state and local networks in quarter four of 2018. It is noted by the trusted third party that it is possible some of the detections are false positives.



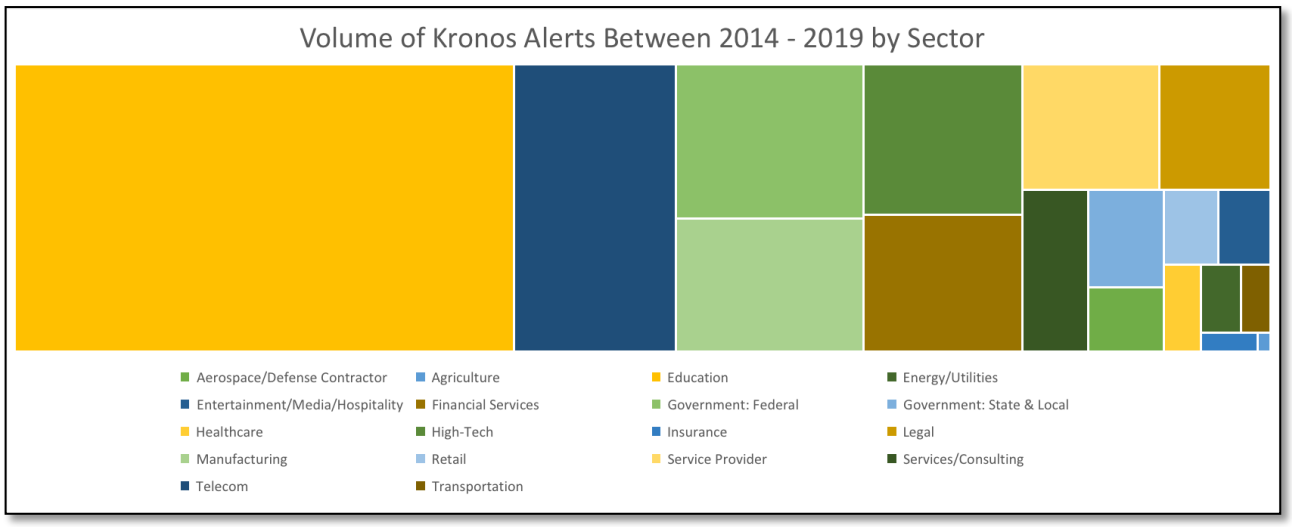
MALWARE HISTORY

The Department of Homeland Security and trusted third parties first observed Kronos advertised on an established Russian cyber-criminal forum by the actor "VinnyK" in June 2014. Like most new banking Trojans to emerge, forum actors were skeptical of its reliability, particularly Russian - speaking actors as VinnyK likely does not speak Russian and was new to the forum. However, it appears that VinnyK commands an adept technical skillset and connections to well-known cyber crime operators.

Kronos botnets have had a modest presence since its initial release in 2014 and are still active today. More recent discussions on underground forums indicate that Kronos licenses cost $3,000 USD, a decrease from its initial price point of $7,000 USD. One Kronos botnet was observed loading a new point-of-sale (POS) malware known as ScanPOS in November 2016. Currently, it appears that several different actors are deploying and maintaining separate Kronos botnets. Several malware customers have been identified hosting C&C on notorious bulletproof hosting infrastructure.

TARGETING

Kronos malware is almost certainly being distributed by multiple customers and, therefore, financial targeting is somewhat geographically distributed. For example, one Kronos botnet hosted on Fluxxy revealed malware infecting hosts in Spain, Romania, Germany, Greece, and the U.S., though overall geographical targeting is more widespread than this. Campaigns have also been observed targeting Canadian and Australian financial institutions. As seen in the below chart, between 2014 – 2019 industries ranging from education, telcom, energy, healthcare and others have been impacted the Kronos Trojan.



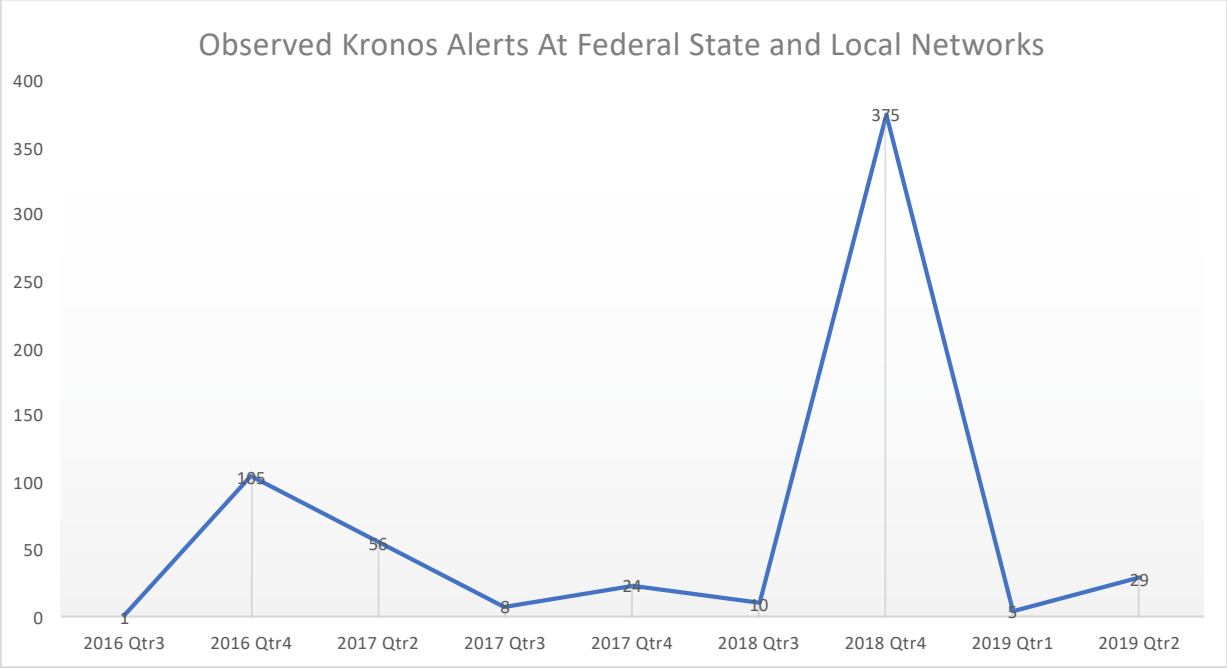
Currently, most Kronos campaign targeting appears to be opportunistic. However, it is noteworthy that a Kronos campaign in 2016 – 2017 delivering ScanPOS appeared to specifically target retail and hospitality sectors in the U.S.

Federal, State and Local Networks

According to a source with first hand access to the information, between the August of 2016 and December of 2017, officials identified Kronos malware activity on U.S. State and local government information systems.

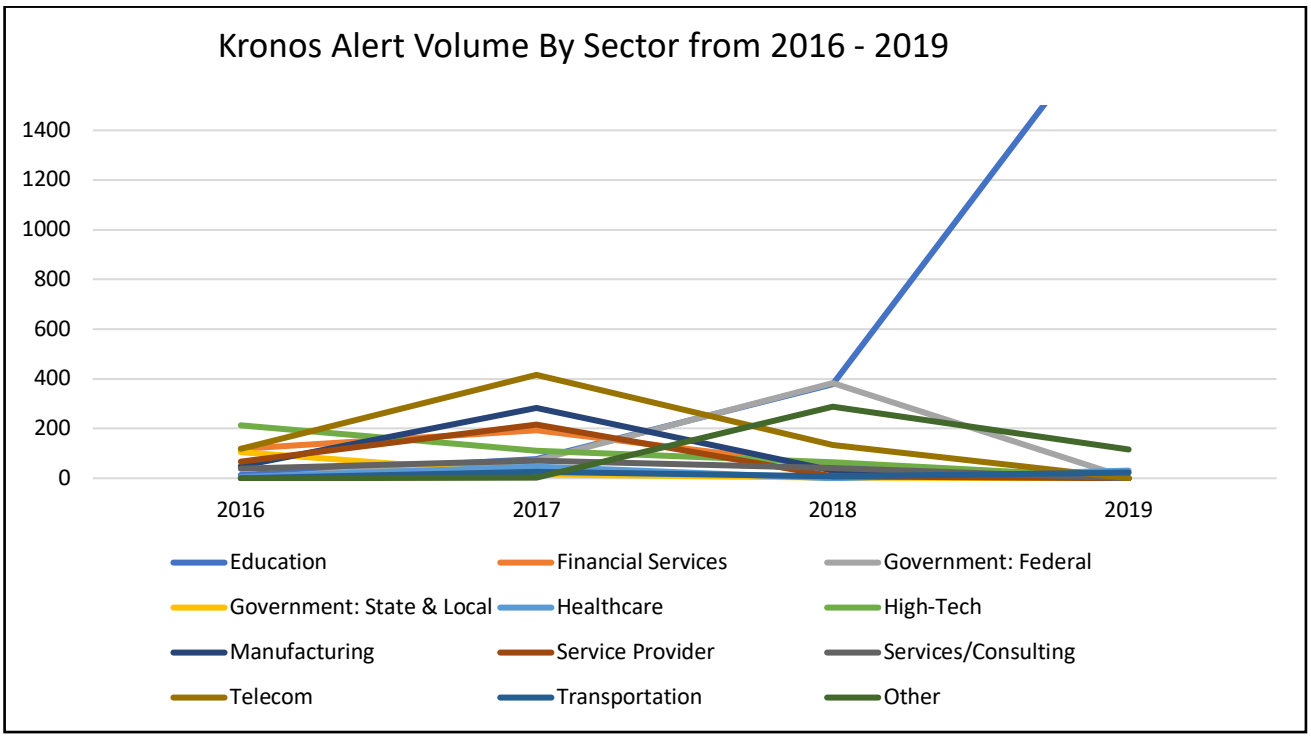
Additionally, multiple states detected and reported cyber reconnaissance and intrusion activity targeting their network that resolved to domains hosting a Kronos C2.

According to a trusted third party, an increase in Kronos alerts on Federal, State and Local networks occurred in quarter 4 of 2018. (Figure 2)



2019 Increase at Education

According to a trusted third party, a large spike in Kronos traffic was observed within the education sector, as noted by figure 4.



MALWARE TECHNICAL OVERVIEW

Kronos is a banking malware capable of intercepting web browsing data, injecting its own malicious code into webpages, and downloading additional payloads. The malware also employs user-mode rootkit code to hide its presence on infected systems.

Upon initial execution, the malware injects its malicious content into a new svchost.exe process and performs several anti-analysis checks. It collects a variety of system information to report back to the C&C server. The original executable is copied into the %APPDATA%\Microsoft\<GUID>\ directory as a hidden file and an associated AutoRun key is generated for persistence.

A new thread is created for opening two sockets: one listening on localhost (127.0.0.1) port 32767 to receive the malware's webinject configuration and intercepted browsing traffic, while the other listens on localhost port 32768 to forward intercepted data to a C&C server or its intended destination after being injected. The local listeners create a proxy that allows the malware to evaluate captured browser traffic, inject its own code into browser webpages, and forward stolen browser data to a C&C server. While these port numbers are hardcoded in the malware, they are incremented during execution as new connections from infected processes are created.

Next, an embedded DLL capable of stealing browsing data from popular browsers is loaded into memory. The malware creates a new thread that injects the DLL into any instance of iexplore.exe, chrome.exe, firefox.exe, or opera.exe. It hooks numerous specified functions, which allows the malware to hijack browser socket connections and redirect their data to a local listener on a specified port. Next, the malware begins hooking functions within browser and system DLLs based on the process into which it was injected. Intercepted network traffic is directed to the local listening port written to the DLL prior to its injection.

The injected svchost.exe process attempts to hide the existence of the malware on the system by injecting user-mode rootkit shellcode into all running processes. The shellcode accomplishes this by hooking several ntdll.dll functions. The hooking code hides the currently running malware process, based on process ID, and other malware artifacts, such as registry keys used and the location of the malware binary on disk.

The malware attempts to communicate with a C&C server every 10 seconds. Each C&C URL is contacted up to three times. If a valid response is not received in three attempts, the next C&C URL is contacted. This continues until the C&C list is exhausted or a valid C&C response is received, at which point the malware sleeps for 15 minutes and begins this process again.

The malware decodes a C&C server's response using a single-byte XOR key found at offset 0x01 within the response.

Once the configuration is successfully downloaded from the C&C and written to disk, the malware sends the plaintext configuration to its own socket listening on a localhost port. The decrypted configuration likely contains webinject HTML code used to perform man-in-the-browser (MiTB) attacks, which allow the malware to alter communications to webpages and steal browsing-related information.

CONCLUSION

The Kronos Trojan has persisted globally from 2014 to 2019.