telelink
BUSINESS SERVICES

Advanced Security Operations Center
Telelink Business Services
www.tbs.tech

Monthly Security Bulletin

June 2022

This security bulletin is powered by Telelink Business Services' Advanced Security Operations Center

The modern cybersecurity threat landscape is constantly evolving. New vulnerabilities and zero-day attacks are discovered every day. The old vulnerabilities still exist. The tools to exploit these vulnerabilities are applying more complex techniques. But are getting easier to use.

Mitigating modern cyber threats require solutions for continuous monitoring, correlation, and behavior analysis that are expensive and require significant amount of time to be implemented. Moreover, many organizations struggle to hire and retain the expensive security experts needed to operate those solutions and provide value by defending the organizations.

The ASOC by Telelink allows organizations get visibility, control, and recommendations on improving their security posture for a fixed and predictable monthly fee.

Why Advanced Security Operations Center (ASOC) by Telelink?

- Delivered as a service, which guarantees fast implementation, clear responsibility in the Supplier and ability to cancel the contract on a monthly basis.
- Built utilizing state of the art leading vendor's solutions.
- Can be sized to fit small, medium, and large business needs.
- No investment in infrastructure, team, trainings or required technology.
- Flexible packages and add-ons that allow pay what you need approach.
- Provided at a fraction of the cost of operating your own SOC.

LITE Plan

425 EUR/mo

- Gain visibility on the security posture of all your company's IT infrastructure
- Analysis of up to 2 GB/day log data
- Optional emergency response team (ERT) and user and endpoint behavior analytics (UEBA)

Get visibility on the cyber threats targeting your company!

PROFESSIONAL Plan

1225 EUR/mo

- Gain visibility on your company's security posture and recommendations on how to deal with security threats, risks, and actors
- Analysis of up to 5 GB/day log data and 100 GB/day network data
- Optional ERT and UEBA

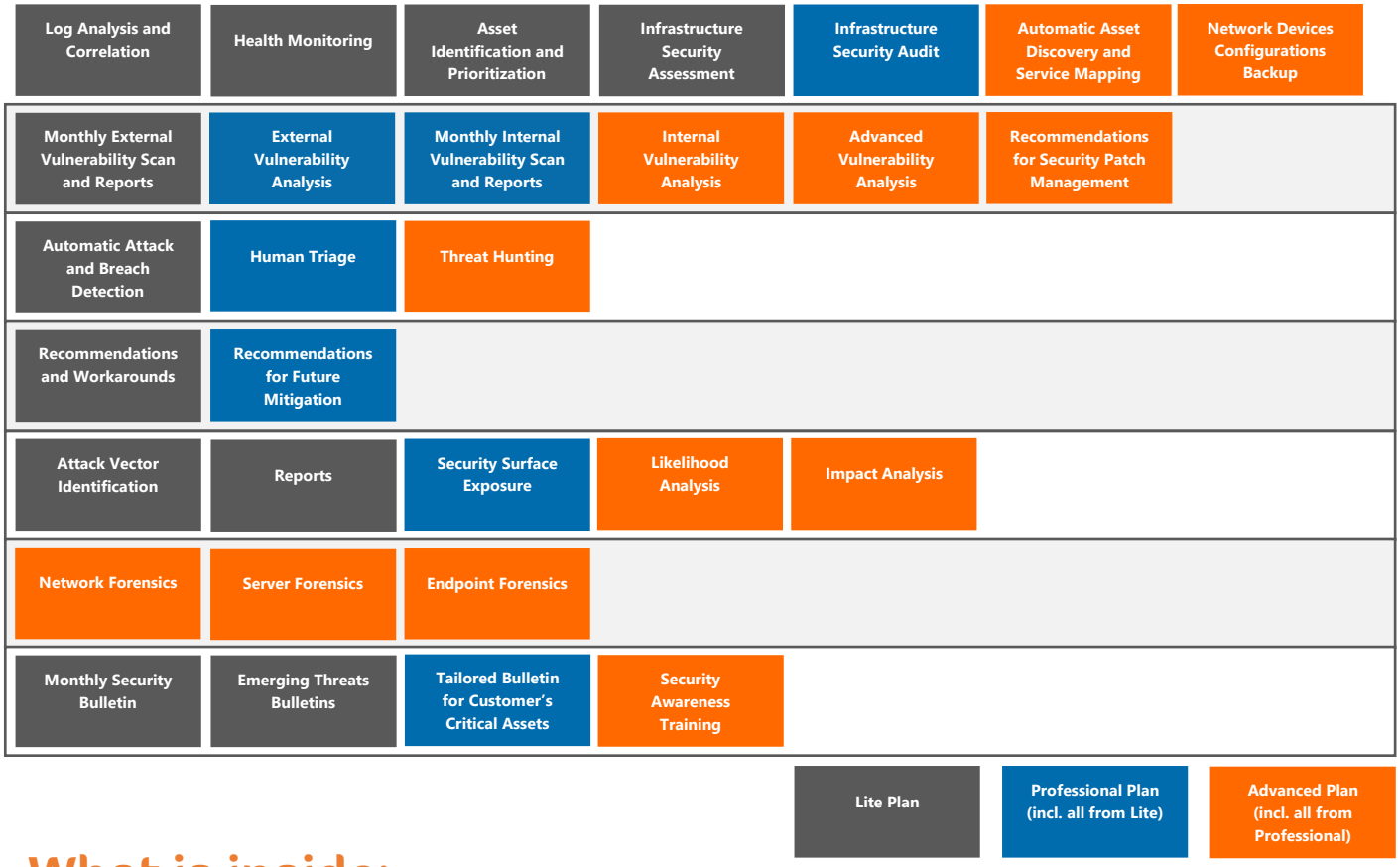
Start to mitigate cyber threats and minimize the risk!

ADVANCED Plan

2 575 EUR/mo

- Gain complete visibility, deep analysis, recommendations, and security awareness trainings for your employees
- Analysis of up to 10 GB/day log data and 200 GB/day network data
- Included ERT and optional UEBA

Complete visibility, deep analysis, and cyber threat mitigation!



What is inside:

- Infrastructure Security Monitoring – the essential minimum to cybersecurity and to detect anomalies is to monitor your infrastructure 24x7x365
- Vulnerability Management – get visibility on the risks new or old vulnerabilities are posing to your IT infrastructure and get recommendations on how to reduce or mitigate those risks
- Attack Detection – get data from state-of-the-art cybersecurity tools, detect attacks and breaches, and involve our ASOC Analytics Team to perform human triage and threat hunting to precisely define the risks of the attack
- Reports and Recommendations – get detailed tailored reports with structured recommendations on how to prevent malicious activities (attacks) and take preventive measures
- Advanced Attack Analysis – get information on the attack vector, the attack surface, potential threat actors, and their objectives and motives for the attack
- Forensic Analysis – in case of severe cybercrimes the ASOC team can perform forensic analysis and/or support the authorities
- Bulletins, Training and Awareness – be timely informed on critical vulnerabilities with tailored and emerging threats bulletins and security awareness trainings to stop people being the weakest link

Table of Contents

1. Instagram Hack Results in $1 Million Loss in NFTs

Imagine – your favorite brand on Instagram just announced a giveaway. You'll receive a free gift! All you have to do is provide your credit card information. Sounds easy, right? This is a brand you've followed and trusted for a while now. You've engaged with them and even purchased some of their items. The link comes directly from their official page, so you don't think to question it.

This is the same mindset that led to several Bored Ape Yacht Club (BAYC) NFTs being stolen by a cybercriminal who had hacked into the company's official Instagram account. Let's dive into the details of this scam.

Sneaking Into the Bored Ape Yacht Club

Bored Ape Yacht Club, the NFT collection, disclosed through Twitter that their Instagram account had been hacked, and advised users not to click on any links or link their crypto wallets to anything. The hacker managed to log into the account and post a phishing link promoting an "airdrop," or a free token giveaway, to users who connected their MetaMask wallets. Those who linked their wallets before BAYC's warning lost a combined amount of over $1 million in NFTs.

Despite the large price tag attached to NFTs, they are often held in smartphone wallets rather than more secure alternatives. MetaMask, the crypto wallet application, only allows NFT display through mobile devices and encourages users to use the smartphone app to manage them. While it may be a good method for display purposes, this limitation provides hackers with a new and effective way to easily steal from users' mobile wallets.

BAYC does not yet know how the hacker was able to gain access to their Instagram account, but they are following security best practices and actively working to contact the users affected.

N.F.T. – Not For Taking

This scam was conducted through the official BAYC account, making it appear legitimate to BAYC's followers. It is incredibly important to stay vigilant and know how to protect yourself and your assets from scams like these. Follow the tips below to steer clear of phishing scams and keep your digital assets safe:

Ensure wallet security

A seed phrase is the "open sesame" to your cryptocurrency wallet. The string of words is what grants you access to all your wallet's assets. Ensuring that your seed phrase is stored away safely and not easily accessible by anyone but yourself is the first step to making sure your wallet is secure.

Protect your privacy

With all transactional and wallet data publicly available, scammers can pick and choose their targets based on who appears to own valuable assets. To protect your privacy and avoid being targeted, refrain from sharing your personal information on social media sites or using your NFT as a social media avatar.

Look out for phishing scams

Phishing scams targeting NFT collectors are becoming increasingly common. Be wary of any airdrops offering free tokens in exchange for your information or other "collectors" doing the same.

Phishing scams tend to get more sophisticated over time, especially in cases like the Bored Ape Yacht Club where the malicious links are coming straight from the official account. It is always best to remain skeptical and cautious, but when in doubt, here are some extra tips to spot phishing scams:

- **Is it written properly?** A few spelling or grammar mistakes can be common, but many phishing messages will contain glaring errors that professional accounts or companies wouldn't make. If you receive an error-filled message or promotion that requires giving your personal information, run in the other direction.
- **Does the logo look right?** Scammers will often steal the logo of whatever brand or company they're impersonating to make the whole shtick look more legitimate. However, rarely do the logos look exactly how they're supposed to. Pay close attention to any logo added in a message or link. Is the quality low? Is it crooked or off-center? Is it almost too small to completely make out? If yes, it's most likely not the real deal.
- **Is the URL legit?** In any phishing scam, there will always be a link involved. To check if a link is actually legitimate, copy and paste the URL into a word processor where you can examine it for any odd spelling or grammatical errors. If you receive a strange link via email, hover over it with your mouse to see the link preview. If it looks suspicious, ignore and delete it. Even on mobile devices, you can press and hold the link with your finger to check out the legitimacy of the URL.

As crypto and NFTs continue to take the world by storm, hackers and scammers are constantly on the prowl for ways to steal and deceive. No matter the source or how trustworthy it may seem at first glance, always exercise caution to keep yourself and your assets safe!

Source: https://www.mcafee.com/blogs/mobile-security/instagram-hack-results-in-1-million-loss-in-nfts/

2. Hackers stole data undetected from US, European orgs since 2019

The Chinese hacking group known as 'Winnti' has been stealthily stealing intellectual property assets like patents, copyrights, trademarks, and other corporate data – all while remaining undetected by researchers and targets since 2019.

Winnti, also tracked as APT41, is an advanced and elusive cyber-espionage group that is believed to be backed by the Chinese state and operates on behalf of its national interests.

The discovered cybercrime campaign has been underway since at least 2019 and targeted technology and manufacturing firms in East Asia, Western Europe, and North America.

Operation CuckooBees

This criminal operation is known as 'Operation CuckooBees' and was discovered by analysts at Cybereason, who revealed new malware deployed by the notorious group of hackers, the mechanisms they leverage for intrusion, and the intricate payload delivery methods they use.

Winnti's operational steps (Cybereason)

"With years to surreptitiously conduct reconnaissance and identify valuable data, it is estimated that the group managed to exfiltrate hundreds of gigabytes of information.

The attackers targeted intellectual property developed by the victims, including sensitive documents, blueprints, diagrams, formulas, and manufacturing-related proprietary data. - Cybereason.

The financial losses incurred by "CuckooBees" are hard to determine, but the figure should be on a scale that puts the operation among the most damaging cyber campaigns of the past years.

A stealthy operation

The infection chain observed in Operation CuckooBees begins with exploiting known and zero-day vulnerabilities in ERP platforms used by the targets.

Winnti establishes persistence via an encoded WebShell, by abusing the WinRM protocol for remote access, the IKEEXT and PrintNotify Windows services for DLL side-loading, or by loading a signed kernel rootkit.

Once they gain a foothold on networks, the hackers perform reconnaissance using built-in Windows commands like 'systeminfo', 'net start',' net user', and 'dir c:\', that are unlikely to trigger any alerts for suspicious activity, even when run in batch files via a Scheduled Task.

Command	Technique
fsutil fsinfo drives	System Drives Discovery
ipconfig	System Network Configuration Discovery
nbtstat	Remote System Discovery
net accounts	Password Policy Discovery
net group	Permission Groups Discovery
net session	System Network Session Discovery
net share	Network Share Discovery
net start	System Service Discovery
net time	System Time Discovery
net use	System Network Connections Discovery
net user	Account Discovery
net view	Network Share Discovery
netstat	System Network Connections Discovery
nslookup	System DNS Configuration Discovery
ping	Remote System Discovery
query user	System Owner/User Discovery
systeminfo	System Information Discovery
tasklist	Process Discovery
tracert	Remote System Route Discovery
whoami	Logged On User Discovery

Commands used for reconnaissance

(Cybereason)

For credential dumping, Winnti uses either the 'reg save' command to save the stolen passwords in a safe place or a variant of a previously undocumented tool named 'MFSDLL.exe.'

For lateral movement, the hackers continue to abuse the Windows Scheduled Tasks along with a set of special batch files.

```
SCHTASKS /Create /S <IP Address> /U <Username> /p <Password> /SC ONCE /TN test /TR <Path to a Batch File> /ST <Time> /RU SYSTEM
```

Scheduled task for lateral movement (Cybereason)

Finally, for the data collection and exfiltration, the threat actors deploy a portable command-line WinRAR app that features a valid digital signature and uses "rundll32.exe" for its executable.

WinRAR signature (Cybereason)

New findings

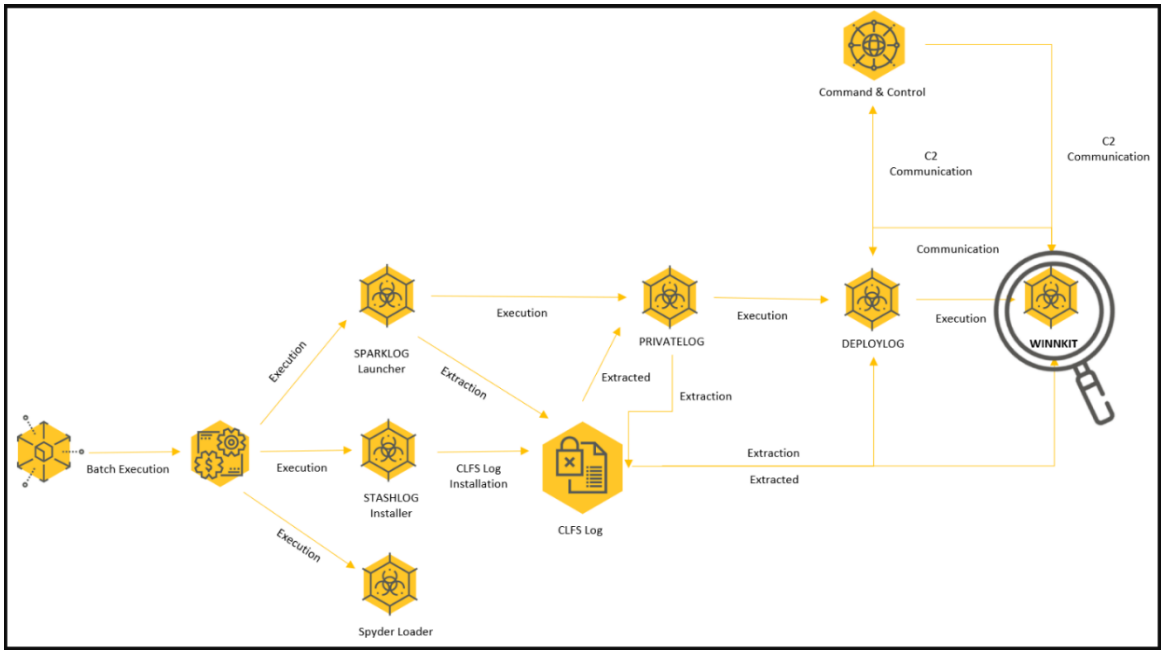
What stands out in Cybereason's report is a new Winnti malware dubbed "DEPLOYLOG" and the method of abuse of the Windows CLFS (Common Log File System) mechanism for payload concealing.

CLFS is an internal logging system for Windows OSes, which uses a proprietary file format that's only accessible through the system's API functions. As such, its log files are skipped by AV scanners while human inspectors don't have a tool that can parse them.

Winnti abuses this system to store and hide its payloads that are dropped on the target system in CLFS log form and then extracted and executed via CLFS API calls.

The DEPLOYLOG malware, which hasn't been documented before, is a 64-bit DLL (masqueraded as "dbghelp.dll") that extracts and executes Winnti's final payload, the WINNKIT rootkit, and then establishes two communication channels with the remote C2 and the kernel-level rootkit.

Some of the malware used to abuse Windows CLFS was previously discovered by Mandiant but had not been attributed to any threat actors.



Malware strains and load steps that lead to Winnkit deployment (Cybereason)

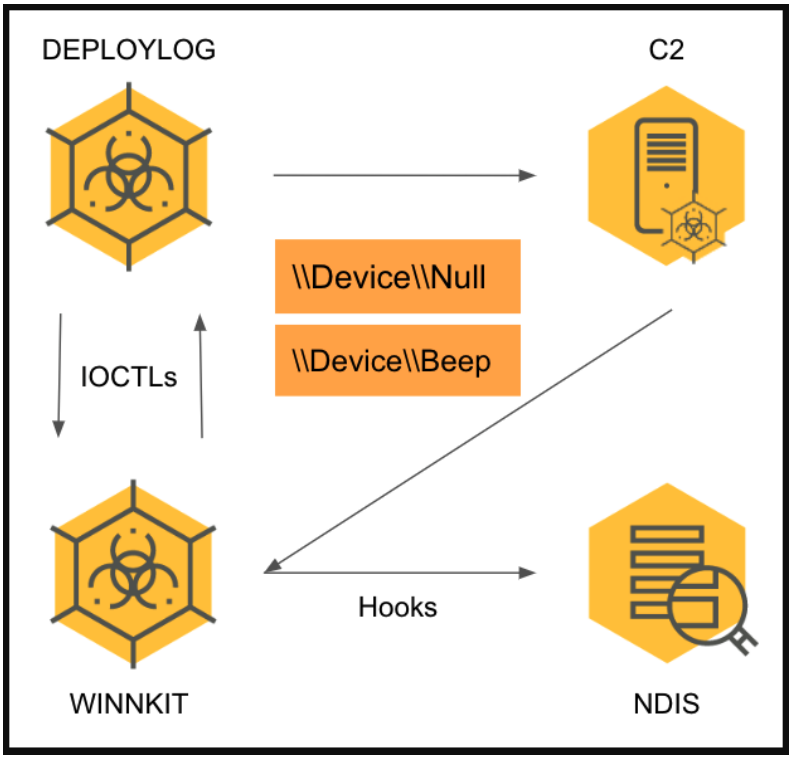
WINNKIT is the threat actor's most evasive and sophisticated payload, which has been extensively analyzed in the past. Still, even after all this time, it remains largely impervious to anti-virus detection.

In Operation CuckooBees, WINNKIT uses reflective loading injection to inject its malicious modules into legitimate svchost processes.

"WINNKIT contains an expired BenQ digital signature, which is leveraged to bypass the Driver Signature Enforcement (DSE) mechanism that requires drivers to be properly signed with digital signatures in order to be loaded successfully," explains the malware report by Cybereason.

"This mechanism was first introduced in Windows Vista 64-bit, and affects all versions of Windows since then."

After successful initialization, WINNKIT will hook the network communication and start receiving custom commands through DEPLOYLOG.



DEPLOYLOG and WINNKIT com interactions (Cybereason)

Defending your network

Despite indictments of Winnti members announced in the past couple of years by the U.S. Department of Justice, and no matter how many technical reports analyzing its tools and tactics have been published, the notorious Chinese cyber-espionage group remains active and industrious.

Cybereason believes that due to the complexity, stealth, and sophistication of Operation CuckooBees, it's very likely that Winnti compromised many more companies than those they were able to verify.

The best bet for defenders against such threats is to update all their software to the latest available version, monitor all network traffic, and use network segmentation.

For more details on Winnti's TTPs, check out an additional Cybereason blog piece that focuses on the techniques, or a third devoted to the malware used in the campaign.

Source: https://www.bleepingcomputer.com/news/security/hackers-stole-data-undetected-from-us-european-orgs-since-2019/

3. Surveillance by Driverless Car

San Francisco police are using autonomous vehicles as mobile surveillance cameras.

Privacy advocates say the revelation that police are actively using AV footage is cause for alarm.

"This is very concerning," Electronic Frontier Foundation (EFF) senior staff attorney Adam Schwartz told Motherboard. He said cars in general are troves of personal consumer data, but autonomous vehicles will have even more of that data from capturing the details of the world around them. "So when we see any police department identify AVs as a new source of evidence, that's very concerning."

Source: https://www.schneier.com/blog/archives/2022/05/surveillance-by-driverless-car.html

4. Third-party web trackers log what you type before submitting

An extensive study looking into the top 100k ranking websites has revealed that many are leaking information you enter in the site forms to third-party trackers before you even press submit.

This leaked data includes personal identifiers, email addresses, usernames, passwords, or even messages entered into forms and then deleted and never actually submitted.

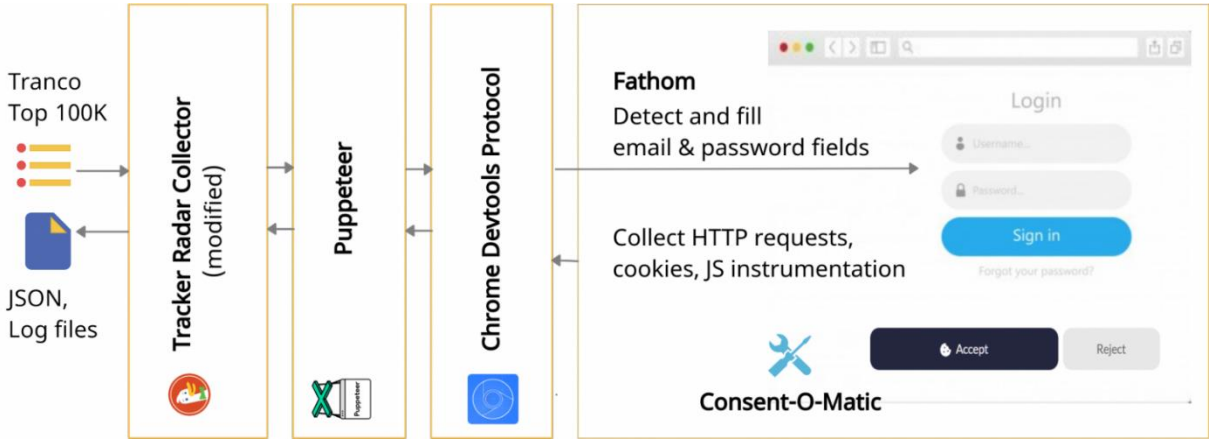
This data leak is sneaky because internet users automatically assume that the information they type on websites isn't saved until they submit it, but for almost 3% of all tested sites, this isn't the case.

Alarming findings

The study was conducted by university researchers who used a crawler based on DuckDuckGo's Tracker Radar Collector tool to monitor exfiltration activities.

The results have been summed up on this webpage, while the researchers also published the detailed technical paper for those who want to dive deeper.

The crawler was equipped with a pre-trained machine-learning classifier that detected email and password fields and intercepted script access to those fields.



Crawler function diagram (GitHub)

The researchers tested 2.8 million pages on the world's top 100,000 highest ranking sites and found that 1,844 websites let trackers exfiltrate email addresses before submission when visited from Europe.

However, when visiting those same websites from the US, the number of sites collecting information before submission jumped to 2,950.

Finally, researchers determined 52 websites to be collecting passwords in the same way, but all of them addressed the problem after receiving the researchers' report.

Who receives the data?

The purpose of website trackers is to monitor visitor activity, derive data points related to preferences, log interactions, and maintain a persistent anonymous (theoretically) ID for each user.

The sites use trackers to provide a more personalized online experience to their users, but they also allow third-party trackers to help advertisers serve targeted ads to their visitors and increase monetary gains.

EU				US			
Rank	**Website**	**Third-party**	**Hash/encoding/compression**	**Rank**	**Website**	**Third-party**	**Hash/encoding/compression**
154	**usatoday.com***	taboola.com	Hash (SHA-256)	95	**issuu.com**	taboola.com	Hash (SHA-256)
242	**trello.com***	bizible.com	Encoded (URL)	128	**businessinsider.com**	taboola.com	Hash (SHA-256)
243	**independent.co.uk***	taboola.com	Hash (SHA-256)	154	**usatoday.com**	taboola.com	Hash (SHA-256)
300	**shopify.com**	bizible.com	Encoded (URL)	191	**time.com**	bouncex.net	Compression (LZW)
328	**marriott.com**	glassboxdigital.io	Encoded (BASE-64)	196	**udemy.com**	awin1.com	Hash (SHA-256 with salt)
567	**newsweek.com***	rlcdn.com	Hash (MD5, SHA-1, SHA-256)			zenaps.com	Hash (SHA-256 with salt)
705	**prezi.com***	taboola.com	Hash (SHA-256)	217	**healthline.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)
754	**branch.io***	bizible.com	Encoded (URL)	234	**foxnews.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)
1,153	**prothomalo.com**	facebook.com	Hash (SHA-256)	242	**trello.com***	bizible.com	Encoded (URL)
1,311	**codecademy.com**	fullstory.com	Unencoded	278	**theverge.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)
1,543	**azcentral.com***	taboola.com	Hash (SHA-256)	288	**webmd.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)

Top sites using leaky trackers (kuleuven.be)

Many of these third-party trackers are using scripts that monitor for keystrokes when inside a form, and save the content, even before the user presses the submit button

The obvious repercussion of having data entered on forms logged is losing the anonymity of trackers, and at the same time, privacy and security risks arise.

The data collected by the university researchers shows that the problem stems from a small number of trackers that are prevalent on the web.

For example, LiveRamp's trackers were found in 662 sites whose email addresses were logged, Taboola was present in 383, Verizon collected data from 255 sites, and Adobe's Bizible ran in 191 sites.

	EU						US					
Leak Type	Entity Name	Tracker Domain	Key by key	Num. sites	Prom.	Min. Rank	Entity Name	Tracker Domain	Key by key	Num. sites	Prom.	Min. Rank
email	Taboola	taboola.com	No	327	302.9	154	LiveRamp	rlcdn.com	No	524	553.8	217
	Adobe	bizible.com	Yes	160	173.0	242	Taboola	taboola.com	No	383	499.0	95
	FullStory	fullstory.com	Yes	182	75.6	1,311	Bounce Exchange	bouncex.net	No	189	224.7	191
	Awin Inc.	zenaps.com*	No	113	48.7	2,043	Adobe	bizible.com	Yes	191	212.0	242
		awin1.com*	No	112	48.5	2,043	Awin	zenaps.com*	No	119	111.2	196
	Yandex	yandex.com	Yes	121	41.9	1,688		awin1.com*	No	118	110.9	196
	AdRoll	adroll.com	No	117	39.6	3,753	FullStory	fullstory.com	Yes	230	105.6	1,311
	Glassbox	glassboxdigital.io*	Yes	6	31.9	328	Listrak	listrakbi.com	Yes	226	66.0	1,403
	Listrak	listrakbi.com	Yes	91	24.9	2,219	LiveRamp	pippio.com	No	138	65.1	567
	Oracle	bronto.com	Yes	90	24.6	2,332	SmarterHQ	smarterhq.io*	Yes	32	63.8	556
	LiveRamp	rlcdn.com	No	11	20.0	567	Verizon Media	yahoo.com*	Yes	255	62.3	4,281
	SaleCycle	salecycle.com	Yes	35	17.5	2,577	AdRoll	adroll.com	No	122	48.6	2,343
	Automattic	gravatar.com*	Yes	38	16.7	2,048	Yandex	yandex.ru	Yes	141	48.1	1,648
	Facebook	facebook.com	Yes	21	14.8	1,153	Criteo SA	criteo.com*	No	134	46.0	1,403
	Salesforce	pardot.com*	Yes	36	30.8	2,675	Neustar	agkn.com*	No	133	45.9	1,403
	Oktopost	okt.to*	Yes	31	11.4	6,589	Oracle	addthis.com	No	133	45.9	1,403
pswd	Yandex	yandex.com	Yes	37	12.12	4,699	Yandex	yandex.ru	Yes	45	17.23	1,688
		yandex.ru		7	2.41	12,989						
	Mixpanel	mixpanel.com	Yes	1	0.12	84,547	Mixpanel	mixpanel.com	Yes	1	0.12	84,547
	LogRocket	lr-ingest.io	Yes	1	0.12	82,766	LogRocket	lr-ingest.io	Yes	1	0.12	82,766

Third-party trackers and their owners (kuleuven.be)

In the password-grabbing category, Yandex tops the list with the highest number of confirmed cases.

Half of the listed first and third parties have responded to the researchers with comments and explanations, attributing the collection to a mistake.

The GDPR factor

The difference between EU and US stats is attributed to the presence of GDPR, a legal regulatory context for protecting the personal data of EU netizens processed by online entities.

The case of compliance here depends on the disclosure of the collection of the data entered in website forms, which needs to be detailed and clearly defined.

For example, the typical 'we share your personal data with selected marketing partners' doesn't cut it for GDPR.

According to the study, the email exfiltration by third parties via trackers breaches at least three GDPR requirements, namely the transparency principle, the purpose limitation principle, and the absence of consent requests.

Confirmed violations of the GDPR are punishable by a fine of up to 20,000,000 Euros or up to 4% of the entity's global annual turnover.

What can users do

The best way to deal with this problem would be to block all third-party trackers using your browser's internal blocker. All major browsers have an in-built blocker, and you will find it in the privacy section of the settings menu.

Additionally, private email relay services give users the capacity to generate pseudonymous email addresses, so even if someone snatches it, identification won't be possible.

Finally, for those who want to take a more involved approach, the researchers have created and released a browser add-on named Leak Inspector, that monitors exfiltration events on any site and warns users accordingly.

Source: https://www.bleepingcomputer.com/news/security/third-party-web-trackers-log-what-you-type-before-submitting/

5. Hackers can steal your Tesla Model 3, Y using new Bluetooth attack

Security researchers at the NCC Group have developed a tool to carry out a Bluetooth Low Energy (BLE) relay attack that bypasses all existing protections to authenticate on target devices.

BLE technology is used in a wide spectrum of products, from electronics like laptops, mobile phones, smart locks, and building access control systems to cars like Tesla Model 3 and Model Y.

Pushing out fixes for this security problem is complicated, and even if the response is immediate and coordinated, it would still take a long time for the updates to trickle to impacted products.

How the attack works

In this type of relay attacks, an adversary intercepts and can manipulate the communication between two parties, such as the key fob that unlocks and operates the car and the vehicle itself.

This places the attacker in the middle of the two ends of the communication, allowing them to relay the signal as if they were standing right next to the car.

Products that rely on BLE for proximity-based authentication protect against known relay attack methods by introducing checks based on precise amounts of latency and also link-layer encryption.

NCC Group has developed a tool that operates at the link layer and with a latency of 8ms that is within the accepted 30ms range of the GATT (Generic ATTribute Profile) response.

“Since this relay attack operates at the link layer, it can forward encrypted link layer PDUs. It is also capable of detecting encrypted changes to connection parameters (such as connection interval, WinOffset, PHY mode, and channel map) and continuing to relay connections through parameter changes. Thus, neither link layer encryption nor encrypted connection parameter changes are defences against this type of relay attack.” - NCC Group

According to Sultan Qasim Khan, a senior security consultant at NCC Group, it takes about ten seconds to run the attack and it can be repeated endlessly.

Both the Tesla Model 3 and Model Y use a BLE-based entry system, so NCC’s attack could be used to unlock and start the cars.

While technical details behind this new BLE relay attack have not been published, the researchers say that they tested the method on a Tesla Model 3 from 2020 using an iPhone 13 mini running version 4.6.1-891 of the Tesla app.

"NCC Group was able to use this newly developed relay attack tool to unlock and operate the vehicle while the iPhone was outside the BLE range of the vehicle" - NCC Group

During the experiment, they were able to deliver to the car the communication from the iPhone via two relay devices, one placed seven meters away from the phone, the other sitting three meters from the car. The distance between the phone and the car was 25 meters.

The experiment was also replicated successfully on a Tesla Model Y from 2021, since it uses similar technologies.

These findings were reported to Tesla on April 21st. A week later, the company responded by saying "that relay attacks are a known limitation of the passive entry system."

The researchers also notified Spectrum Brands, the parent company behind Kwikset (makers of the Kevo line of smart locks).

What can be done

NCC Group's research on this new proximity attack is available in three separate advisories, for BLE in general, one for Tesla cars, and another for Kwikset/Weiser smart locks, each illustrating the issue on the tested devices and how it affects a larger set of products from other vendors.

The Bluetooth Core Specification warns device makers about relay attacks and notes that proximity-based authentication shouldn’t be used for valuable assets.

This leaves users with few possibilities, one being to disable it, if possible, and switch to an alternative authentication method that requires user interaction.

Another solution would be for makers to adopt a distance bounding solution such as UWB (ultra-wideband) radio technology instead of Bluetooth.

Tesla owners are encouraged to use the 'PIN to Drive' feature, so even if their car is unlocked, at least the attacker won't be able to drive away with it.

Additionally, disabling the passive entry functionality in the mobile app when the phone is stationary would make the relay attack impossible to carry out.

If none of the above is possible on your device, keep in mind the possibility of relay attacks and implement additional protection measures accordingly.

Source: https://www.bleepingcomputer.com/news/security/hackers-can-steal-your-tesla-model-3-y-using-new-bluetooth-attack/

6. This World Password Day, Here's How a Password Manager Can Simplify Your Life

Passwords: we entrust our most important data to these strings of letters, numbers, and special characters. So, we should make sure our passwords are words or phrases that we can easily remember, right? While this might be the most convenient option, there are more secure ways to digitally lock up your most sensitive personally identifiable information (PII). In celebration of World Password Day, we're diving into how you can practice top-notch password security without compromising convenience.1

The Nature of the Password

Over the years, the password has remained a good first line of defense against cyberattacks. However, most of us tend to choose passwords based on memorable things from our lives, like family names or our pets' birthdays. As it turns out, these details are easy for hackers to find on social media sites like Facebook or LinkedIn. It's also human nature to opt for convenience, and for many people that means setting easy-to-remember and easy-to-guess passwords. Plus, out of convenience, people often reuse passwords across multiple accounts and services. The downside is that if one account becomes compromised, all accounts become compromised.

As an alternative to single-word passwords, many security experts advocate for passphrases over passwords. Passphrases are longer strings of words and characters that are easier for you to remember and harder for nefarious software and cybercriminals to guess than random strings of upper and lowercase letters, numbers and symbols. But, according to a study, the average American internet user was projected to have 300 online accounts by 2022.2 Can you

imagine memorizing 300 different passphrases? We can all agree that sounds pretty unrealistic, so users tend to look for other solutions.

Do You Save Your Password in a Browser?

If the answer is yes, you may want to reconsider, as there are several risks associated with this practice. Although it's convenient to have your browser save your passwords, they tend to do a lousy job of safeguarding your passwords, credit card numbers and personal details, such as your name and address.

Let's take Google Chrome, for example. Unlike most dedicated password managers, Chrome doesn't use a primary password to encrypt all your credentials. (Note that some browsers do use one, and are therefore more secure, though you'll still need to trust your browser provider.) This makes your Chrome-stored passwords relatively weak to "local" attacks. For example, if someone gets hold of—or guesses—your Windows password, they can then see all the logins stored in your browser's password manager.

Another consideration to note is that the security of all your accounts is tied to your browser account's security. Let's say you use the sync option to make your credentials available on all your devices. This means that logins are stored in the cloud and, though encrypted, if someone manages to hack into your browser account, they will gain access to all your logins.

Keep Your Accounts Secure Without Compromising Convenience

What can you do to help ensure your online profiles are kept safe without spending hours managing a complex list of passwords? Here are some easy ways to lock down your digital life without sacrificing convenience:

Use a password manager to store unique, complex passwords for all your accounts

A password manager is a software application that stores your passwords and other sensitive information. You can install it on computers or mobile devices and store all passwords in an encrypted file (or database). The best option is to use a password manager like McAfee True Key to store and create strong, random passwords for each site you visit. You'll have one primary password that grants access to the rest of them—ideally, a long and random passphrase that you can remember. Once everything is set up, it should be seamless. As you log in to new sites, the password manager will offer to save your credentials for later use.

Turn on two-factor authentication for every site that offers it

One of the best ways to protect your accounts against unauthorized access is to turn on two-factor authentication for every site that offers it. Using two-factor authentication means a site will prompt you for a unique security code, in addition to your password, whenever you log in to an account for which you have enabled this feature.

Two-factor authentication adds an extra layer of security by requiring another form of identification after you enter your username and password. Some services send a temporary passcode over text message. Others require the user to approve login attempts from new devices using an app. If someone steals your device or gains access to your account details, they're out of luck unless they also have access to this second piece of information. Two-factor authentication is available on a wide range of websites and can help keep your accounts safe from would-be hackers, so you should always use it when available.

Use a virtual private network (VPN) when out and about

A VPN, or virtual private network, encrypts your data and masks your online behavior from snooping third parties. When you go to a website, your computer connects to the server where the site is hosted, and that website can see a certain amount of data about you and your computer. With a VPN, you connect to a private server first, which scrambles your data and makes it more difficult for digital eavesdroppers to track what you're doing online.

VPNs can provide users with greater peace of mind when on the go. Say you're traveling on a business trip and need to connect to the Wi-Fi network provided by your hotel. Shifty characters often lurk on unprotected, free networks (such as those provided by hotels, coffee shops, airports, etc.) to lift PII from people handling sensitive emails, making banking transactions, or shopping online. McAfee Safe Connect VPN encrypts your online activity with bank-grade encryption to protect your data from prying eyes. With a premium paid plan, you can protect up to five devices at once and enjoy unlimited data protection.

The Best of Both Worlds: Security and Convenience

With your growing number of accounts all requiring passwords—emails, social media profiles, online banking—it's no wonder that people tend to reuse passwords across multiple sites. This may be convenient, but it creates significant security risks if a suspicious actor manages to obtain one of your passwords and attempts to use it elsewhere. That's why having strong passwords matters.

Do yourself a favor and opt for a dedicated password manager that will auto-save and store your credentials for you, so you only have one password to remember. Who says security and simplicity can't coexist?

Source: https://www.mcafee.com/blogs/internet-security/this-world-password-day-heres-how-a-password-manager-can-simplify-your-life/

7. Chinese 'Space Pirates' are hacking Russian aerospace firms

A previously unknown Chinese hacking group known as 'Space Pirates' targets enterprises in the Russian aerospace industry with phishing emails to install novel malware on their systems.

The threat group is believed to have started operating in 2017, and while it has links to known groups like APT41 (Winnti), Mustang Panda, and APT27, it is thought to be a new cluster of malicious activity.

Russian threat analysts at Positive Technologies named the group "Space Pirates" due to their espionage operations focusing on stealing confidential information from companies in the aerospace field.

In the wild detections

The Space Pirates APT group has been seen targeting government agencies and enterprises involved in IT services, aerospace, and electric power industries located in Russia, Georgia, and Mongolia.

The threat analysts first discovered signs of Space Pirates' activity last summer during incident response and quickly confirmed that the threat actors used the same malware and infrastructure against at least four more domestic entities since 2019.

Two of these cases concern Russian companies with state participation, which the hackers successfully compromised.

In the first case, the threat actors maintained their access to 20 servers for ten months, stealing over 1,500 documents, employee details, and other sensitive data.

In the second case, the Chinese hackers stayed in the network of the compromised company for over a year, siphoning confidential information and installing their malware to 12 corporate network nodes in three distinct regions.

Novel malware

The arsenal of Space Pirates consists of custom loaders hiding behind decoy documents, slightly modified backdoors that have been around for years, the Chinese trademark malware PlugX, and tailored spins of the PcShare backdoor.

Moreover, Space Pirates' attacks have also employed ShadowPad, Zupdax, PoisonIvy, and ReVBShell in attacks.

In addition to the above, the newly discovered APT uses three previously undocumented modular malware tools, namely Deed RAT, BH_A006, and MyKLoadClient.

MyKLoadClient is a loader using SFX archives combined with DLL side-loading through an auxiliary launcher library signed by McAfee Inc. The launcher supports commands that give the threat actors close control over the infection.

BH_A006 is a heavily modified version of the Gh0st backdoor, featuring many layers of obfuscation to bypass security protections and thwart analysis.

Its features include network service creation, UAC bypassing, and shellcode unpacking and launching in the memory.

```
18  if ( !load_imports() )
19    return -1;
20  (imports.kernel32_SetErrorMode)(2);
21  memset(v14, 0, sizeof(v14));
22  (imports.kernel32_GetModuleFileNameW)(0, v14, 260);
23  v1 = (imports.kernel32_GetCommandLineW)();
24  debug(L"Argv12%s", v1);
25  debug(L"GetModuleFileName %s", v14);
26  if ( wcsstr(v1, L"InsertS") )
27  {
28    create_and_start_service();
29    (imports.kernel32_Sleep)(1000);
30    v2 = (imports.kernel32_GetCurrentProcess)(0);
31    (imports.kernel32_TerminateProcess)(v2);
32  }
33  else if ( wcsstr(v1, L"runsvc") )
34  {
35    debug(L"svchost.exe %s", v14);
36    kernel32_DeleteFileA = imports.kernel32_DeleteFileA;
37    (imports.kernel32_DeleteFileA)("C:\\ProgramData\\Sandboxie\\SbieMsg.dll");
38    kernel32_DeleteFileA("C:\\ProgramData\\Sandboxie\\SbieMsg.dat");
39    kernel32_DeleteFileA("C:\\Windows \\System32\\SSPICLI.dll");
40    kernel32_DeleteFileA("C:\\Windows \\System32\\perfmon.exe");
41    kernel32_DeleteFileA("C:\\Windows \\System32\\dxva2.dll");
42    kernel32_DeleteFileA("C:\\Windows \\System32\\dccw.exe");
43    kernel32_RemoveDirectoryA = imports.kernel32_RemoveDirectoryA;
44    (imports.kernel32_RemoveDirectoryA)("C:\\Windows \\System32\\");
45    kernel32_RemoveDirectoryA("C:\\Windows \\");
46    kernel32_CreateThread = imports.kernel32_CreateThread;
47    (imports.kernel32_CreateThread)(0, 0, inject_payload, 0, 0, 0);
48    (imports.kernel32_Sleep)(2000);
49    kernel32_CreateThread(0, 0, check_mapping, 0, 0, 0);
50  }
51  else if ( wcsstr(v1, L"ByPassUAC") )
52  {
53    v6 = alloc_and_lock(dword_1387B78);
54    memset(v6, 0, dword_1387B78);
```

BH_A006 shellcode loading (PT)

Another interesting custom tool is Deed RAT, which features an unusual, intelligent method of transferring control to the shellcode.

Deed RAT's functions depend on which plugins are fetched and loaded. For example, PT has seen eight plugins for startup, C2 config, installation, code injection into processes, network interactions, connection management, registry editing, registry monitoring, and proxy sniffing.

The supported protocols for C2 communication include TCP, TLS, HTTP, HTTPS, UDP, and DNS, so there's generally a high level of versatility.

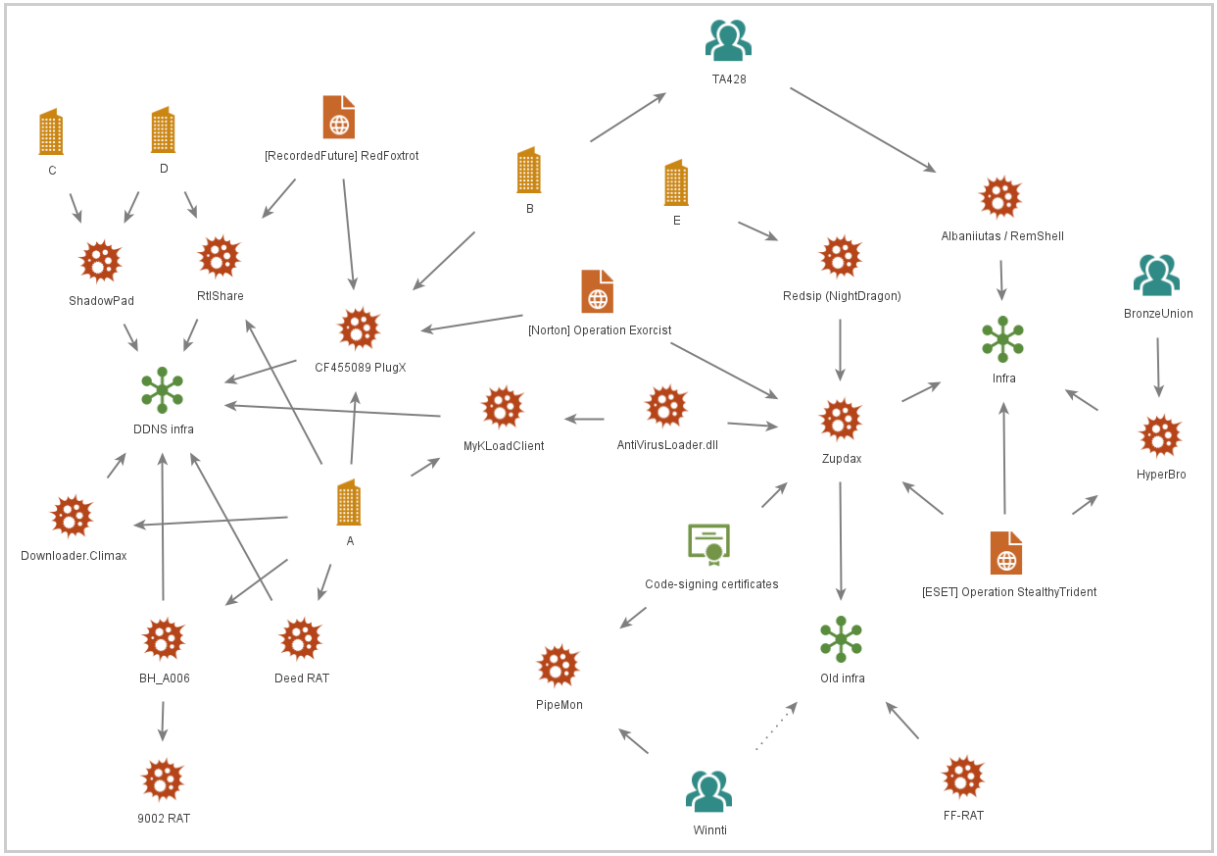
The commands supported by Deed RAT are the following:

- Collect system information
- Create a separate communication channel for a plugin
- Self-remove
- Ping
- Deactivate connection
- Update the shellcode for an injection stored in the registry
- Update the main shellcode on disk and delete all plugins

Chinese convolution

The threat analysts believe that the overlaps between various Chinese APTs are due to tool exchanges, a common phenomenon for hackers in the region.

Using shared tools further obscures the traces of distinct threat groups and makes the work of analysts a lot harder, so Chinese APTs have multiple reasons to follow this practice.



Various links between Chinese APTs (PT)

Space Pirates has also been seen deploying their custom malware on some Chinese firms for financial gains, so the threat group might have a dual function.

Chinese hackers have been very aggressive against Russian targets lately, as confirmed by recent findings of analysts at Secureworks and Google.

Espionage is a standard operation for Chinese APTs, and Russia is a valid target that excels in aerospace, weapons, electrical engineering, shipbuilding, and nuclear technology.

Source: https://www.bleepingcomputer.com/news/security/chinese-space-pirates-are-hacking-russian-aerospace-firms/

8. Microsoft Teams, Windows 11 hacked on first day of Pwn2Own

During the first day of Pwn2Own Vancouver 2022, contestants won $800,000 after successfully exploiting 16 zero-day bugs to hack multiple products, including Microsoft's Windows 11 operating system and the Teams communication platform.

The first to fall was Microsoft Teams in the enterprise communications category after Hector Peralta exploited an improper configuration flaw.

The STAR Labs team (Daniel Lim Wee Soong, Poh Jia Hao, Li Jiantao, and Ngo Wei Lin) also demonstrated a Teams zero-click exploit chain of 2 bugs (injection and arbitrary file write).

Microsoft Teams was hacked a third time by Masato Kinugawa, who exploited a 3-bug chain of injection, misconfiguration, and sandbox escape.

Each of them earned $150,000 for successfully demonstrating their Microsoft Teams zero-days.

STAR Labs also earned an extra $40,000 after elevating privileges on a system running Windows 11 using a Use-After-Free weakness and an additional $40,000 by achieving privilege escalation on Oracle Virtualbox.

Manfred Paul (@_manfp) also successfully demoed 2 bugs (prototype pollution and improper input validation) to hack Mozilla Firefox and an out-of-band write on Apple Safari to earn $150,000.

Other highlights from the first day of Pwn2Own include Marcin Wiązowski, Team Orca of Sea Security, and Keith Yeo demonstrating more zero-days in Windows 11 and Ubuntu Desktop.

On the second day, Pwn2Own competitors will attempt to exploit zero-days in the Tesla Model 3 Infotainment System (with Sandbox Escape) and Diagnostic Ethernet (with Root Persistence), Windows 11, and Ubuntu Desktop.

After the security vulnerabilities are demonstrated and disclosed during Pwn2Own, software and hardware vendors have 90 days to develop and release security fixes for all reported flaws.

During the Pwn2Own Vancouver 2022 contest, security researchers will target products in the web browser, virtualization, Local Escalation of Privilege, servers, enterprise communications, and automotive categories.

Between May 18 and May 20, they will be able to earn more than $1,000,000 in cash and prizes, including a Tesla Model 3 and a Tesla Model S. The top award for hacking a Tesla is now $600,000 (and, maybe, the car itself).

Team Fluoroacetate was the first to go home with a Tesla Model 3 at Pwn2Own Vancouver 2019 after hacking the car's Chromium-based infotainment system.

Source: https://www.bleepingcomputer.com/news/security/microsoft-teams-windows-11-hacked-on-first-day-of-pwn2own/

9. Emulation of Kernel Mode Rootkits With Speakeasy

In August 2020, we released a blog post about how the Speakeasy emulation framework can be used to emulate user mode malware such as shellcode. If you haven't had a chance, give the post a read today.

In addition to user mode emulation, Speakeasy also supports emulation of kernel mode Windows binaries. When malware authors employ kernel mode malware, it will often be in the form of a device driver whose end goal is total compromise of an infected system. The malware most often doesn't interact with hardware and instead leverages kernel mode to fully compromise the system and remain hidden.

Challenges With Dynamically Analyzing Kernel Malware

Ideally, a kernel mode sample can be reversed statically using tools such as disassemblers. However, binary packers just as easily obfuscate kernel malware as they do user mode samples. Additionally, static analysis is often expensive and time consuming. If our goal is to automatically analyze many variants of the same malware family, it makes sense to dynamically analyze malicious driver samples.

Dynamic analysis of kernel mode malware can be more involved than with user mode samples. In order to debug kernel malware, a proper environment needs to be created. This usually involves setting up two separate virtual machines as debugger and debugee. The malware can then be loaded as an on-demand kernel service where the driver can be debugged remotely with a tool such as WinDbg.

Several sandbox style applications exist that use hooking or other monitoring techniques but typically target user mode applications. Having similar sandbox monitoring work for kernel mode code would require deep system level hooks that would likely produce significant noise.

Driver Emulation

Emulation has proven to be an effective analysis technique for malicious drivers. No custom setup is required, and drivers can be emulated at scale. In addition, maximum code coverage is easier to achieve than in a sandbox environment. Often, rootkits may expose malicious functionality via I/O request packet (IRP) handlers (or other callbacks). On a normal Windows system these routines are executed when other applications or devices send input/output requests to the driver. This includes common tasks such as reading, writing, or sending device I/O control (IOCTLs) to a driver to execute some type of functionality.

Using emulation, these entry points can be called directly with doped IRP packets in order to identify as much functionality as possible in the rootkit. As we discussed in the first Speakeasy blog post, additional entry points are emulated as they are discovered. A driver's DriverMain entry point is responsible for initializing a function dispatch table that is called to

handle I/O requests. Speakeasy will attempt to emulate each of these functions after the main entry point has completed by supplying a dummy IRP. Additionally, any system threads or work items that are created are sequentially emulated in order to get as much code coverage as possible.

Emulating a Kernel Mode Implant

In this blog post, we will show an example of Speakeasy's effectiveness at emulating a real kernel mode implant family publicly named Winnti. This sample was chosen despite its age because it transparently implements some classic rootkit functionality. The goal of this post is not to discuss the analysis of the malware itself as it is fairly antiquated. Rather, we will focus on the events that are captured during emulation.

The Winnti sample we will be analyzing has SHA256 hash c465238c9da9c5ea5994fe9faf1b5835767210132db0ce9a79cb1195851a36fb and the original file name tcprelay.sys. For most of this post, we will be examining the emulation report generated by Speakeasy. Note: many techniques employed by this 32-bit rootkit will not work on modern 64-bit versions of Windows due to Kernel Patch Protection (PatchGuard) which protects against modification of critical kernel data structures.

To start, we will instruct Speakeasy to emulate the kernel driver using the command line shown in Figure 1. We instruct Speakeasy to create a full memory dump (using the "-d" flag) so we can acquire memory later. We supply the memory tracing flag ("-m") which will log all memory reads and writes performed by the malware. This is useful for detecting things like hooking and direct kernel object manipulation (DKOM).

```
→  speakeasy git:(master) ✗ python3 run_speakeasy.py -t ~/0b105cd6ecdfe5724c7db52135aa47ef -o
 /tmp/output.json -d ~/Desktop/mem.zip -m
```

Figure 1: Command line used to emulate the malicious driver

Speakeasy will then begin emulating the malware's DriverEntry function. The entry point of a driver is responsible for setting up passive callback routines that will service user mode I/O requests as well as callbacks used for device addition, removal, and unloading. Reviewing the emulation report for the malware's DriverEntry function (identified in the JSON report with an "ep_type" of "entry_point"), shows that the malware finds the base address of the Windows kernel. The malware does this by using the ZwQuerySystemInformation API to locate the base address for all kernel modules and then looking for one named "ntoskrnl.exe". The malware then manually finds the address of the PsCreateSystemThread API. This is then used to spin up a system thread to perform its actual functionality. Figure 2 shows the APIs called from the malware's entry point.

```
0x10499: 'ntoskrnl.wcscpy(0x1200f6c, "tcprelay.sys")' -> 0xc
0x104a4: 'ntoskrnl.wcschr("tcprelay.sys", ".")' -> 0x1200f7c
0x10e09: 'ntoskrnl.wcscat("\\Device\\", "tcprelay")' -> 0x1200d6c
0x10e19: 'ntoskrnl.wcscat("\\DosDevices\\", "tcprelay")' -> 0x1200e6c
0x10a35: 'ntoskrnl.ZwQuerySystemInformation(0xb, 0x1200cf4, 0x10, 0x1200ce8)' -> 0xc0000004
0x10a45: 'ntoskrnl.ExAllocatePoolWithTag(0x0, 0xa00, "Ddk ")' -> 0x3f8000
0x10a57: 'ntoskrnl.ZwQuerySystemInformation(0xb, 0x3f8000, 0xa00, 0x1200ce8)' -> 0x0
0x10a81: 'ntoskrnl.strrchr("\\??\\C:\\Windows\\system32\\ntoskrnl.exe", "\\")' -> 0x3f8037
0x10a97: 'ntoskrnl._stricmp("ntoskrnl.exe", "ntoskrnl.exe")' -> 0x0
0x10ad3: 'ntoskrnl.ExFreePoolWithTag(0x3f8000, 0x0)' -> None
0x10a35: 'ntoskrnl.ZwQuerySystemInformation(0xb, 0x1200d18, 0x10, 0x1200d0c)' -> 0xc0000004
0x10a45: 'ntoskrnl.ExAllocatePoolWithTag(0x0, 0xa00, "Ddk ")' -> 0x3f8000
0x10a57: 'ntoskrnl.ZwQuerySystemInformation(0xb, 0x3f8000, 0xa00, 0x1200d0c)' -> 0x0
0x10a81: 'ntoskrnl.strrchr("\\??\\C:\\Windows\\system32\\ntoskrnl.exe", "\\")' -> 0x3f8037
0x10a97: 'ntoskrnl._stricmp("ntoskrnl.exe", "ntoskrnl.exe")' -> 0x0
0x10ad3: 'ntoskrnl.ExFreePoolWithTag(0x3f8000, 0x0)' -> None
0x10e48: 'ntoskrnl.RtlInitUnicodeString(0x1200d58, "\\Device\\tcprelay")' -> None
0x10e58: 'ntoskrnl.RtlInitUnicodeString(0x1200d50, "\\DosDevices\\tcprelay")' -> None
0x10e75: 'ntoskrnl.IoCreateDevice(0x3f7c20, 0x0, "\\Device\\tcprelay", 0x22, 0x0, 0x1, 0x1200d60)' -> 0x0
0x10e91: 'ntoskrnl.IoCreateSymbolicLink("\\DosDevices\\tcprelay", "\\Device\\tcprelay")' -> 0x0
0x10ef9: 'ntoskrnl.PsCreateSystemThread(0x1200d68, 0x1f03ff, 0x0, 0x0, 0x0, 0x1096e, 0x0)' -> 0x0
```

Figure 2: Key functionality in the tcprelay.sys entry point

Hiding the Driver Object

The malware attempts to hide itself before executing its main system thread. The malware first looks up the "DriverSection" field in its own DRIVER_OBJECT structure. This field holds a linked list containing all loaded kernel modules and the malware attempts to unlink itself to hide from APIs that list loaded drivers. In the "mem_access" field in the Speakeasy report shown in Figure 3, we can see two memory writes to the DriverSection entries before and after itself which will remove itself from the linked list.


```
    {
        "tag": "emu.object._Driver_0b105cd6ecdfe5724c7db52135aa47ef.DriverSection.0x3f7de0",
        "base": "0x3f7de0",
        "reads": 4,
        "writes": 0,
        "execs": 0
    },
    {
        "tag": "emu.object._Driver_Ndis.DriverSection.0x1be0",
        "base": "0x1be0",
        "reads": 0,
        "writes": 1,
        "execs": 0
    },
    {
        "tag": "emu.object._Driver_volmgr.DriverSection.0x1640",
        "base": "0x1640",
        "reads": 0,
        "writes": 1,
        "execs": 0
    }
```


Figure 3: Memory write events representing the tcprelay.sys malware attempting to unlink itself in order to hide

As noted in the original Speakeasy blog post, when threads or other dynamic entry points are created at runtime, the framework will follow them for emulation. In this case, the malware created a system thread and Speakeasy automatically emulated it.

Moving on to the newly created thread (identified by an "ep_type" of "system_thread"), we can see the malware begin its real functionality. The malware begins by enumerating all

running processes on the host, looking for the service controller process named services.exe. It's important to note that the process listing that gets returned to the emulated samples is configurable via JSON config files supplied at runtime. For more information on these configuration options please see the Speakeasy README on our GitHub repository. An example of this configurable process listing is shown in Figure 4.

Figure 4: Process listing configuration field supplied to Speakeasy

Pivoting to User Mode

Once the malware locates the services.exe process, it will attach to its process context and begin inspecting user mode memory in order to locate the addresses of exported user mode functions. The malware does this so it can later inject an encoded, memory-resident DLL into the services.exe process. Figure 5 shows the APIs used by the rootkit to resolve its user mode exports.

```
0x106b0: 'ntoskrnl.ZwQuerySystemInformation(0x5, 0x0, 0x0, 0x1200dd8)' -> 0xc0000004
0x1063e: 'ntoskrnl.ExAllocatePoolWithTag(0x0, 0xb72, "4321")' -> 0x3fa000
0x106ee: 'ntoskrnl.ZwQuerySystemInformation(0x5, 0x3fa000, 0xb72, 0x1200dd8)' -> 0x0
0x10707: 'ntoskrnl.RtlInitUnicodeString(0x1200dc0, "services.exe")' -> None
0x1071d: 'ntoskrnl.RtlEqualUnicodeString("System", "services.exe", 0x1)' -> 0x0
0x1071d: 'ntoskrnl.RtlEqualUnicodeString("smss.exe", "services.exe", 0x1)' -> 0x0
0x1071d: 'ntoskrnl.RtlEqualUnicodeString("csrss.exe", "services.exe", 0x1)' -> 0x0
0x1071d: 'ntoskrnl.RtlEqualUnicodeString("wininit.exe", "services.exe", 0x1)' -> 0x0
0x1071d: 'ntoskrnl.RtlEqualUnicodeString("services.exe", "services.exe", 0x1)' -> 0x1
0x1063e: 'ntoskrnl.ExAllocatePoolWithTag(0x1, 0x10e, "4321")' -> 0x3fab80
0x107a2: 'ntoskrnl.ExFreePoolWithTag(0x3fa000, 0x0)' -> None
0x116ba: 'ntoskrnl.PsLookupProcessByProcessId(0x46c, 0x1200e48)' -> 0x0
0x116e8: 'ntoskrnl.ObOpenObjectByPointer(0xe0004000, 0x200, 0x0, 0x1f0fff, 0x0, 0x0, 0x1200e40)' -> 0x0
0x116f7: 'ntoskrnl.PsGetProcessPeb(0xe0004000)' -> 0x11c0
0x11707: 'ntoskrnl.KeStackAttachProcess(0xe0004000, 0x1200e18)' -> None
0x113ca: 'ntoskrnl.ZwAllocateVirtualMemory(0x228, "0x1200bdc->0x0", 0x0, 0x1200bc4, 0x1000, 0x40)' -> 0x0
0x10f61: 'ntoskrnl._wcsicmp("ntdll.dll", "KERNEL32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("kernel32.dll", "KERNEL32.dll")' -> 0x0
0x10f61: 'ntoskrnl._wcsicmp("ntdll.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("kernel32.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("ws2_32.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("wininet.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("winhttp.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("advapi32.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("psapi.dll", "USER32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("user32.dll", "USER32.dll")' -> 0x0
0x10f61: 'ntoskrnl._wcsicmp("ntdll.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("kernel32.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("ws2_32.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("wininet.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("winhttp.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("advapi32.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("psapi.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("user32.dll", "GDI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("gdi32.dll", "GDI32.dll")' -> 0x0
0x10f61: 'ntoskrnl._wcsicmp("ntdll.dll", "ADVAPI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("kernel32.dll", "ADVAPI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("ws2_32.dll", "ADVAPI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("wininet.dll", "ADVAPI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("winhttp.dll", "ADVAPI32.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("advapi32.dll", "ADVAPI32.dll")' -> 0x0
0x10f61: 'ntoskrnl._wcsicmp("ntdll.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("kernel32.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("ws2_32.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("wininet.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("winhttp.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("advapi32.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("psapi.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("user32.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("gdi32.dll", "MSVCRT.dll")' -> 0x1
0x10f61: 'ntoskrnl._wcsicmp("msvcrt.dll", "MSVCRT.dll")' -> 0x0
0x11727: 'ntoskrnl.KeUnstackDetachProcess(0x1200e18)' -> None
0x11747: 'ntoskrnl.ObfDereferenceObject(0xe0004000)' -> None
0x11756: 'ntoskrnl.ExFreePoolWithTag(0x3fab80, 0x0)' -> None
0x11764: 'ntoskrnl.ZwClose(0x228)' -> 0x0
```

Figure 5: Logged APIs used by tcprelay.sys rootkit to resolve exports for its user mode implant

Once the exported functions are resolved, the rootkit is ready to inject the user mode DLL component. Next, the malware manually copies the in-memory DLL into the services.exe process address space. These memory write events are captured and shown in Figure 6.

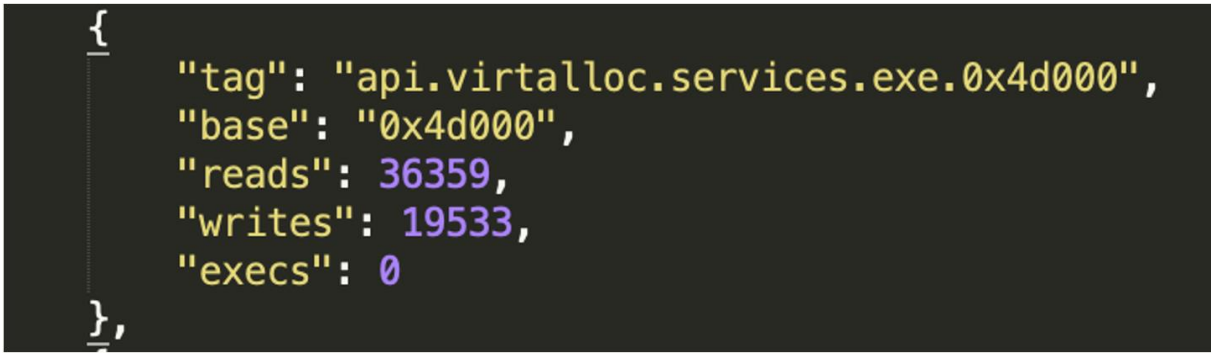


Figure 6: Memory write events captured while copying the user mode implant into services.exe

A common technique that rootkits use to execute user mode code involves a Windows feature known as Asynchronous Procedure Calls (APC). APCs are functions that execute asynchronously within the context of a supplied thread. Using APCs allows kernel mode applications to queue code to run within a thread's user mode context. Malware often wants to inject into user mode since much of the common functionality (such as network communication) within Windows can be more easily accessed. In addition, by running in user mode, there is less risk of being detected in the event of faulty code bug-checking the entire machine.

In order to queue an APC to fire in user mode, the malware must locate a thread in an "alertable" state. Threads are said to be alertable when they relinquish their execution quantum to the kernel thread scheduler and notify the kernel that they are able to dispatch APCs. The malware searches for threads within the services.exe process and once it detects one that's alertable it will allocate memory for the DLL to inject then queue an APC to execute it.

Speakeasy emulates all kernel structures involved in this process, specifically the executive thread object (ETHREAD) structures that are allocated for every thread on a Windows system. Malware may attempt to grovel through this opaque structure to identify when a thread's alertable flag is set (and therefore a valid candidate for an APC). Figure 7 shows the memory read event that was logged when the Winnti malware manually parsed an ETHREAD structure in the services.exe process to confirm it was alertable. At the time of this writing, all threads within the emulator present themselves as alertable by default.

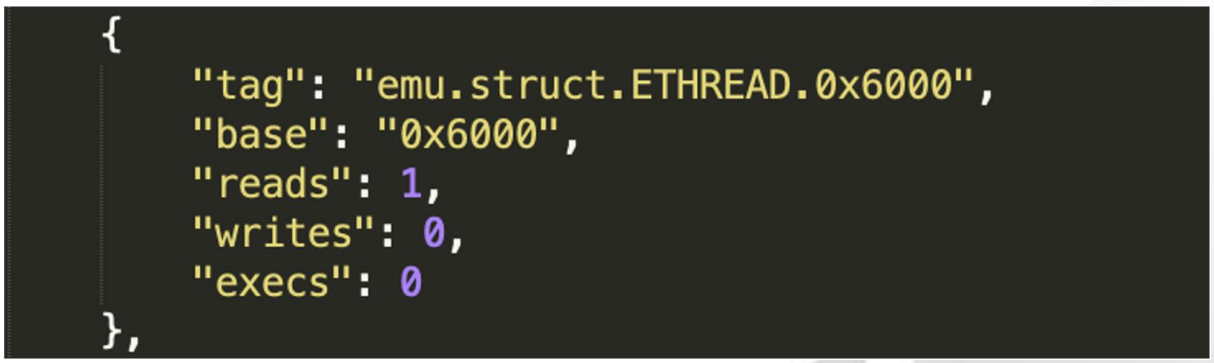


Figure 7: Event logged when the tcprelay.sys malware confirmed a thread was alertable

Next, the malware can execute any user mode code it wants using this thread object. The undocumented functions KeInitializeApc and KeInsertQueueApc will initialize and execute a user mode APC respectively. Figure 8 shows the API set that the malware uses to inject a user mode module into the services.exe process. The malware executes a shellcode stub as the target of the APC that will then execute a loader for the injected DLL. All of this can be recovered from the memory dump package and analyzed later.

```
0x11995: 'ntoskrnl.PsLookupThreadByThreadId(0x480, 0x1200e10)' -> 0x0
0x1189b: 'ntoskrnl.RtlGetVersion(0x266c8)' -> 0x0
0x119d5: 'ntoskrnl.ExFreePoolWithTag(0x7e7b80, 0x0)' -> None
0x11a8f: 'ntoskrnl.ObOpenObjectByPointer(0xe0004000, 0x200, 0x0, 0x1f0fff, 0x0, 0x0, 0x1200df8)' -> 0x0
0x11ab6: 'ntoskrnl.ZwAllocateVirtualMemory(0x22c, "0x1200df0->0x0", 0x0, 0x1200dec, 0x1000, 0x40)' -> 0x0
0x11ace: 'ntoskrnl.KeStackAttachProcess(0xe0004000, 0x1200dd0)' -> None
0x11af2: 'ntoskrnl.KeUnstackDetachProcess(0x1200dd0)' -> None
0x1063e: 'ntoskrnl.ExAllocatePoolWithTag(0x0, 0x30, "4321")' -> 0x7e7020
0x11b26: 'ntoskrnl.KeInitializeApc(0x7e7020, 0x6000, 0x0, 0x11a1e, 0x0, 0x7e7000, 0x1, 0x0)' -> None
0x11b30: 'ntoskrnl.KeInsertQueueApc(0x7e7020, 0x0, 0x0, 0x0)' -> 0x1
0x11b72: 'ntoskrnl.ZwClose(0x22c)' -> 0x0
```

Figure 8: Logged APIs used by tcprelay.sys rootkit to inject into user mode via an APC

Network Hooks

After injecting into user mode, the kernel component will attempt to install network obfuscation hooks (presumably to hide the user mode implant). Speakeasy tracks and tags all memory within the emulation space. In the context of kernel mode emulation, this includes all kernel objects (e.g. Driver and Device objects, and the kernel modules themselves). Immediately after we observe the malware inject its user mode implant, we see it begin to attempt to hook kernel components. This was confirmed during static analysis to be used for network hiding.

The memory access section of the emulation report reveals that the malware modified the netio.sys driver, specifically code within the exported function named NsiEnumerateObjectsAllParametersEx. This function is ultimately called when a user on the system runs the “netstat” command and it is likely that the malware is hooking this function in order to hide connected network ports on the infected system. This inline hook was identified by the event captured in Figure 9.

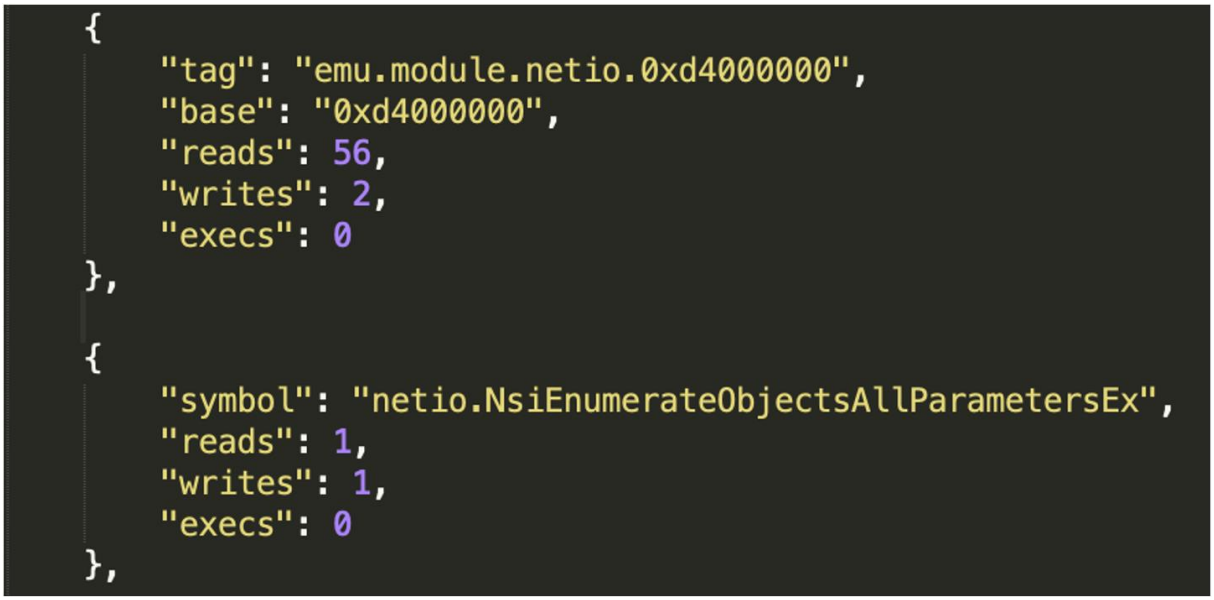


Figure 9: Inline function hook set by the malware to hide network connections

In addition, the malware hooks the Tcpip driver object in order to accomplish additional network hiding. Specifically, the malware hooks the IRP_MJ_DEVICE_CONTROL handler for the Tcpip driver. User mode code may send IOCTL codes to this function when querying for active connections. This type of hook can be easily identified with Speakeasy by looking for memory writes to critical kernel objects as shown in Figure 10.

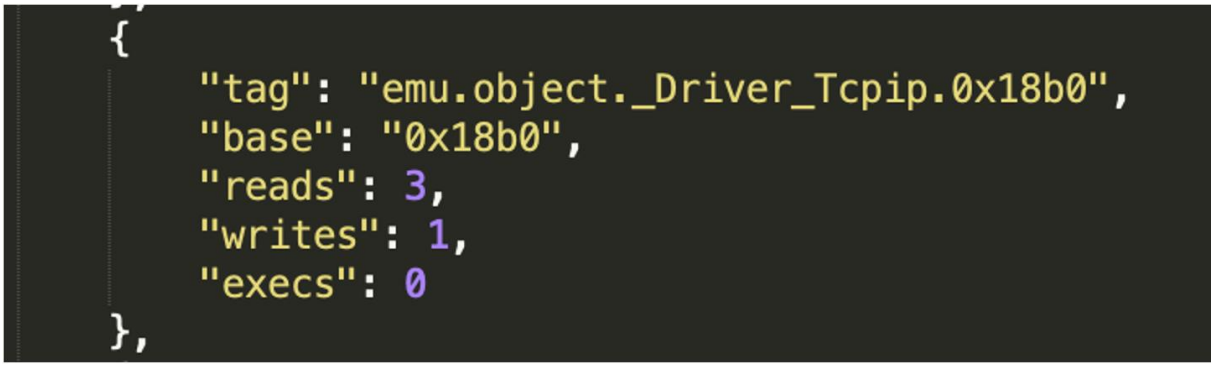


Figure 10: Memory write event used to hook the Tcpip network driver

System Service Dispatch Table Hooks

Finally, the rootkit will attempt to hide itself using the nearly ancient technique of system service dispatch table (SSDT) patching. Speakeasy allocates a fake SSDT so malware can interact with it. The SSDT is a function table that exposes kernel functionality to user mode code. The event in Figure 11 shows that the SSDT structure was modified at runtime.

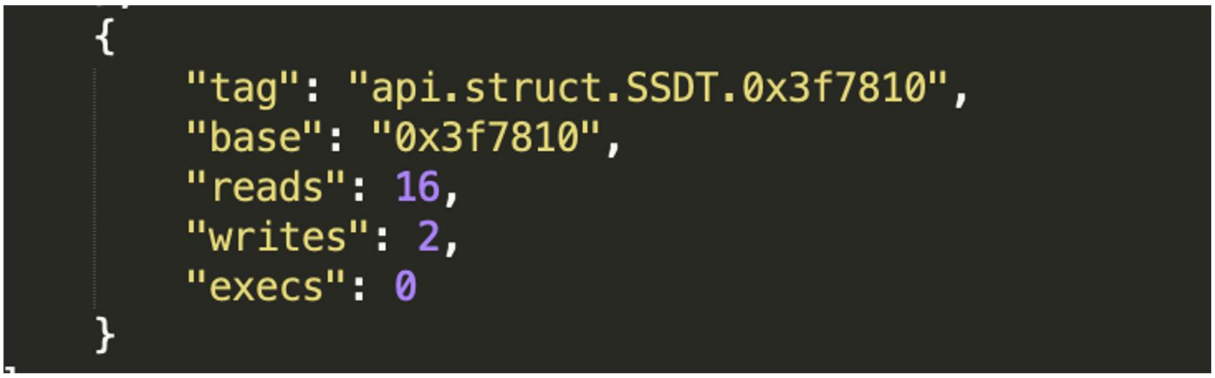


Figure 11: SSDT hook detected by Speakeasy

If we look at the malware in IDA Pro, we can confirm that the malware patches the SSDT entry for the ZwQueryDirectoryFile and ZwEnumerateKey APIs that it uses to hide itself from file system and registry analysis. The SSDT patch function is shown in Figure 12.

```
int set_file_hide_hook()
{
  dword_267E4 = wcslen(L"tcprelay.sys");
  return patch_func(
           *(_BYTE **)(*(_DWORD *)ssdt + 4 * *(_DWORD *)((char *)&ZwQueryDirectoryFile + 1)),
           11,
           (int)file_hook);
}
```

Figure 12: File hiding SSDT patching function shown in IDA Pro

After setting up these hooks, the system thread will exit. The other entry points (such as the IRP handlers and DriverUnload routines) in the driver are less interesting and contain mostly boilerplate driver code.

Acquiring the Injected User Mode Implant

Now that we have a good idea what the driver does to hide itself on the system, we can use the memory dumps created by Speakeasy to acquire the injected DLL discussed earlier. Opening the zip file we created at emulation time, we can find the memory tag referenced in Figure 6. We quickly confirm the memory block has a valid PE header and it successfully loads into IDA Pro as shown in Figure 13.

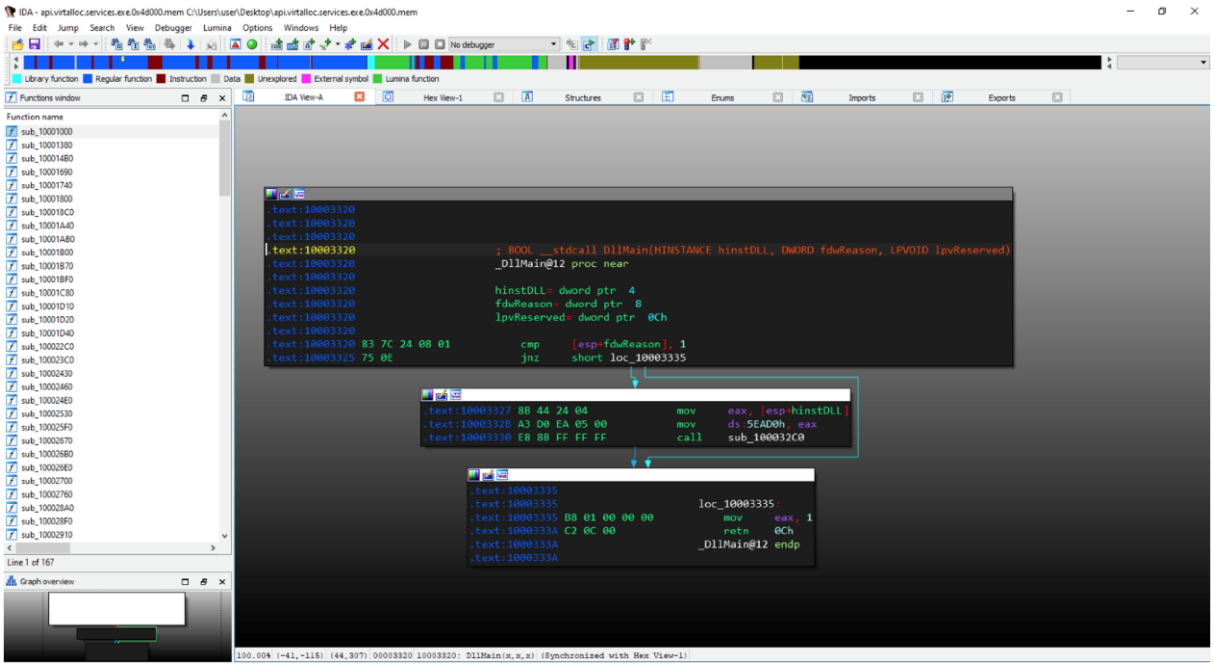


Figure 13: Injected user mode DLL recovered from Speakeasy memory dump

Conclusion

In this blog post, we discussed how Speakeasy can be effective at automatically identifying rootkit activity from the kernel mode binary. Speakeasy can be used to quickly triage kernel binaries that may otherwise be difficult to dynamically analyze. For more information and to check out the code, head over to our GitHub repository.

Source: https://www.fireeye.com/blog/threat-research/2021/01/emulation-of-kernel-mode-rootkits-with-speakeasy.html

10. Google shut down caching servers at two Russian ISPs

Two Russian internet service providers (ISPs) have received notices from Google that the global caching servers on their network have been disabled.

A caching server is an ISP-bound node for fast serving Google content faster to internet subscribers and maintain high access reliability even during outages.

The caching is most important for popular YouTube content that ISPs can store on servers and load quicker, giving their subscribers a better connection experience.

Russian news outlets attempted to confirm which entities have been affected by this sudden move and verified that Radiosvyaz (Focus Life) and МФТИ-Телеком (MIPT Telecom) are currently affected by Google's decision.

MTS, the largest mobile network provider in Russia, and MegaFon providers report seeing no changes for now, while VimpelCom, T2 RTK Holding, and ER-Telecom have declined to comment on the matter.

The two ISPs confirmed as impacted had their caching servers shut down on May 19, 2022, but received Google's notification only a few days after that date.

MIPT Telecom has shared a copy of the notice they received from Google with RBC.ru that confirmed the validity of the reports and the provided justification.

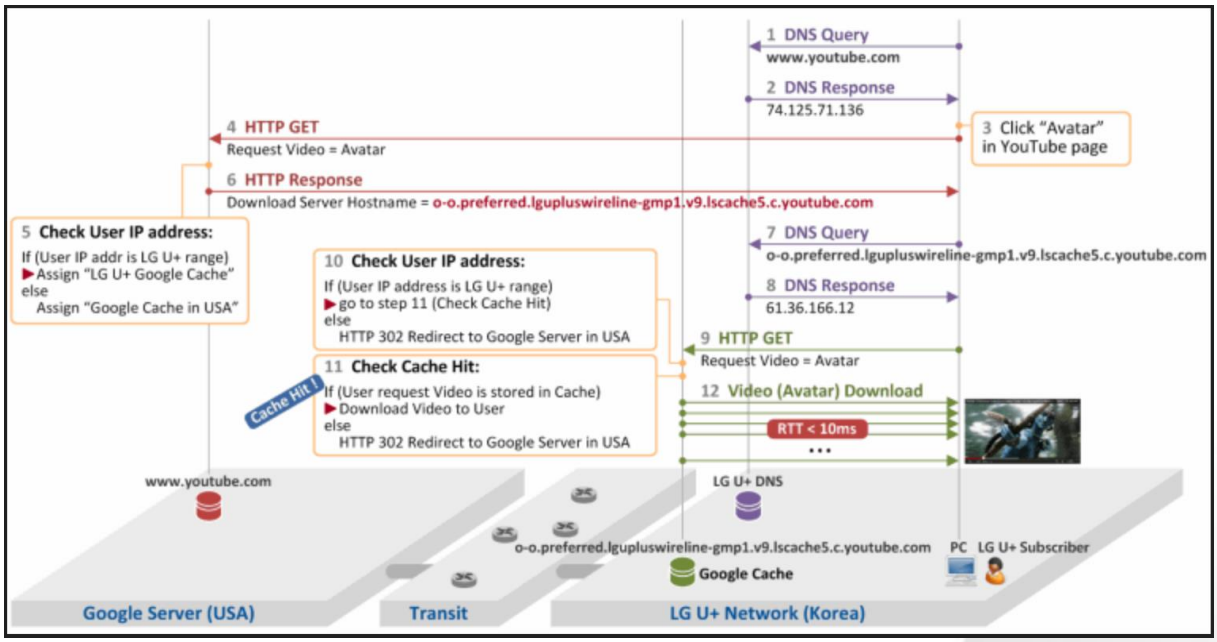
In the notice, Google states the reason for turning off the caching servers was changes in legal practices, pointing to the inclusion of firms and key persons on sanctions lists.

Estimating the impact

The impact on the two Russian ISPs is significant but the two companies have a relatively small market share, which makes the effects unlikely to affect a large number of internet users in the country.

However, if Google expands the ban to all Russian internet providers, the conditions will change dramatically for both companies and their customers.

Google's Global Cache reduces external traffic between 70% to 90%, depending on the content consumption patterns of the end-users of ISP operators.



How Google's caching servers work (Netmanias)

Losing the service would increase their operational cost, and this may trickle into the subscribers' monthly bill.

Apart from that, shutting down the caching servers doesn't only threaten to make YouTube video loading slower. It will also affect servers such as Google CAPTCHA that is stored on the same systems.

If ISPs are deprived of this service, the system that tells humans and bots apart might not work on Russian sites.

Google subsidiary bankrupt

It is worth noting that Google's subsidiary in Russia initiated bankruptcy procedures right before the first caching servers in the country were shut down.

The entity stated incapacity to continue business in Russia due to a massive ($100,000,000) fine imposed by a court on claims from Roskomnadzor on lack of compliance with blocking demands.

This was combined with the confiscation of its local assets worth roughly $32,500,000 approved by the Moscow Arbitration Court in response to several motions submitted by YouTube channel owners like NTV, TNT, ANO TV-Novosti (RT), TV Channel 360, VGTRK, Zvezda, OTR, TV Center and Moscow 24, who had their channels removed by Google.

However, Google's local subsidiary was not involved in the provision of caching services in Russia, as these are part of Google's global operations, so the two issues are not connected, at least at a technical level.

BleepingComputer has requested more information from Google on the matter and the company's future plans but haven't received an answer by publishing time.

Source: https://www.bleepingcomputer.com/news/technology/google-shut-down-caching-servers-at-two-russian-isps/

If you want to learn more about ASOC and how we can improve your security posture, **contact us at tbs.sales@tbs.tech**.

This Bulletin contains information, articles, news, reports or other materials from external sources (links to website sources stated herein above). All information and materials are provided "as is" and TELELINK BUSINESS SERVICES makes no warranty or representations, expressed or implied, for their accuracy, completeness, fitness for particular use, reliability, legality or non-infringement of copyrights.

The content in this Bulletin is provided for informational purposes only do not constitute or represent TELELINK BUSINESS SERVICES's expressed or implied endorsement, recommendation, advertisement, merchandising or solicitation to purchase any of the products or services, described therein, or making any other investment decisions.

TELELINK BUSINESS SERVICES is not responsible for the contents of any linked site or any link contained in a linked site. The hypertext links provided herein are meant only as a convenience and the inclusion of any link does not imply endorsement of or by the referenced site.