



Advanced Security Operations Center
Telelink Business Services
www.telelink.com

Monthly Security Bulletin

February 2020



This security bulletin is powered by

Telelink's

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!

Log Analysis and Correlation	Health Monitoring	Asset Identification and Prioritization	Infrastructure Security Assessment	Infrastructure Security Audit	Automatic Asset Discovery and Service Mapping	Network Devices Configurations Backup
Monthly External Vulnerability Scan and Reports	External Vulnerability Analysis	Monthly Internal Vulnerability Scan and Reports	Internal Vulnerability Analysis	Advanced Vulnerability Analysis	Recommendations for Security Patch	
Automatic Attack and Breach Detection	Human Triage	Threat Hunting				
Recommendations and Workarounds	Recommendations for Future Mitigation	Vulnerability Analysis				
Attack Vector Identification	Reports	Security Surface Exposure	Likelihood Analysis	Impact Analysis		
Network Forensics	Server Forensics	Endpoint Forensics				
Monthly Security Bulletin	Emerging Threats Bulletins	Tailored Bulletin for Customer's Critical Assets	Security Awareness Training			
				Lite Plan	Professional Plan (incl. all from Lite)	Advanced Plan (incl. all from Professional)

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:

Executive summary.....	4
1. DeathRansom Campaign Linked to Malware Cornucopia.....	7
2. Fake Windows 10 Desktop Used in New Police Browser Lock Scam	9
3. Containers in the Cloud: False Assumptions and Security Challenges.....	11
4. Tricky Phish Angles for Persistence, Not Passwords	14
5. The Great \$50M African IP Address Heist.....	18
6. Attackers Are Scanning for Vulnerable Citrix Servers, Secure Now.....	20
7. Mozilla Firefox 72.0.1 Patches Actively Exploited Zero-Day	22
8. Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices	23
9. PoCs for Windows CryptoAPI Bug Are Out, Show Real-Life Exploit Risks.....	26
10. TrickBot Now Uses a Windows 10 UAC Bypass to Evade Detection	29
11. New NetWire RAT Campaigns Use IMG Attachments to Deliver Malware Targeting Enterprise Users	31
12. Windows EFS Feature May Help Ransomware Attackers.....	33
13. BitPyLock Ransomware Now Threatens to Publish Stolen Data	35
14. FTCCODE Ransomware Now Steals Chrome, Firefox Credentials.....	39
15. Russia Blocks ProtonMail and ProtonVPN, Tor to the Rescue	41
16. Microsoft Detects New Evil Corp Malware Attacks After Short Break	43

Executive summary

1. An ongoing DeathRansom malware campaign is part of a larger malicious offensives, all carried out by an actor going by the nickname "scat01." - (very likely) a Russian-speaking cybercriminal living in Italy. [→](#)
2. Scammers have renewed an old browser scam, called a Police Browser Locker and updated it by taking advantage of your web browser's full-screen mode to show a fake Windows 10 desktop stating that your computer is locked. [→](#)
3. As cloud infrastructures become widely adopted across many organizations, some are also moving their software projects to the cloud — specifically containerized environments. While this move brings agility and scale with it, a false assumption can also arise: "My applications are inside containers, so they are secure." In reality, however, it's often the opposite. [→](#)
4. Late last year saw the re-emergence of a nasty phishing tactic that was popular back in 2017, that allows the attacker to gain full access to a user's data stored in the cloud without actually stealing the account password. The phishing starts with a link that leads to the real login page for a cloud email and/or file storage service, however anyone who takes the bait will inadvertently forward a digital token to the attackers that gives them indefinite access to the victim's email, files and contacts — even after the victim has changed their password. [→](#)
5. Ernest Byaruhanga - a top executive at the nonprofit entity responsible for doling out chunks of Internet addresses to businesses and other organizations in Africa has resigned his post following accusations that he secretly operated several companies which sold tens of millions of dollars' worth of addresses to online marketers. The allegations stemmed from a three-year investigation by an U.S.-based researcher. [→](#)
6. Researchers have observed ongoing scans for Citrix Application Delivery Controller (NetScaler ADC) and Citrix Gateway (NetScaler Gateway) servers vulnerable to attacks exploiting CVE-2019-19781 during the last week. This vulnerability impacts multiple Citrix products and it could potentially expose the networks of over 80,000 firms in 158 countries to hacking attacks and despite the fact that there are no public exploits available the risk remains high. [→](#)
7. Mozilla released Firefox 72.0.1 and Firefox ESR 68.4.1 to patch a critical and actively exploited severity vulnerability that could potentially allow attackers to execute code or trigger crashes on machines running vulnerable Firefox versions. The type confusion vulnerability tracked as CVE-2019-17026 impacts the web browser's

IonMonkey Just-In-Time (JIT) compiler and it occurs when incorrect alias information is fed for setting array elements. [→](#)

8. New functionality of the Ryuk ransomware uses the Wake-on-Lan feature to turn on powered off devices on a compromised network to have greater success encrypting them. [→](#)
9. Proof-of-concept exploit code is developed for the Windows CryptoAPI spoofing vulnerability tracked as CVE-2020-0601 by British hardware hacker Saleem Rashid, whom tweeted screenshots of the code and by Swiss cybersecurity outfit Kudelski Security and ollypwn as well. The vulnerability flaw now known as CurveBall was reported by the National Security Agency (NSA), just two days after Microsoft released a patch. Technical details on the vulnerability can be found in Telelink ASOC's issued Emergency Threat Bulletin on the subject. [→](#)
10. The TrickBot Trojan has received an update that adds an UAC bypass targeting the Windows 10 operating system so that it infects users without displaying any visible prompts. The bypass itself is called Fodhelper and was discovered in 2017. [→](#)
11. A new active campaign is targeting organizations with fake business emails that deliver NetWire remote-access Trojan (RAT) variants, hidden inside an IMG file, which is a file extension used by disk imaging software. Such files often are not scanned by the antivirus filters on the e-mail gateway. [→](#)
12. Security researchers have created concept ransomware that takes advantage of a feature in Windows that encrypts files and folders to protect them from unauthorized physical access to the computer. The lab-developed ransomware strain relies on the Encrypting File System (EFS) component in Microsoft's operating system and can run undetected by some antivirus software. [→](#)
13. A new ransomware called BitPyLock, first discovered on the 9th of January 2020 has quickly gone from targeting individual workstations to trying to compromise networks and stealing files before encrypting devices. To make matters worse, as ransomware operators begin stealing data before encrypting victims for use as leverage, BitPyLock actors claim to be adopting this tactic as well. [→](#)
14. FTCODE, a PowerShell-based ransomware that targets Italian-language users and has been around since 2013, has added new capabilities, including the ability to swipe saved credentials from Google Chrome, Internet Explorer and Mozilla Firefox browsers, as well as email clients Mozilla Thunderbird and Microsoft Outlook. [→](#)

15. Proton Technologies', a security-focused ProtonMail end-to-end encrypted email service and ProtonVPN VPN service have been blocked by the Russian government since 29th of January 2020, claiming in a press release from Roskomnadzor that "This email service was used by cybercriminals both in 2019 and especially actively in January 2020 to send false messages under the guise of reliable information about mass mining of objects in the Russian Federation," The block was prompted by Proton Technologies' refusal to register their services with state authorities — something that was asked from all VPN providers operating in Russia — and to provide information about the owners of the mailboxes used to send the bombing threats per Roskomnadzor's statement. [→](#)

16. An ongoing Evil Corp phishing campaign is using novel technique with attachments featuring HTML redirectors for delivering malicious Excel documents with malicious macro. Evil Corp (also tracked as TA505 and SectorJ04) is a financially motivated cybercrime group active since at least Q3 2014 known for focusing on attacks against retail companies and financial institutions via large-sized malicious spam campaigns driven by the Necurs botnet. [→](#)

1. DeathRansom Campaign Linked to Malware Cornucopia

One threat actor appears to be behind several ongoing, related campaigns.

An ongoing DeathRansom malware campaign has been found by researchers to be part of a larger collection of malicious offensives, all carried out by an actor going by the nickname "scat01."

According to Artem Semenchenko and Evgeny Ananin at FortiGuard Labs, evidence found on Russian underground forums and in their forensic investigations points to a significant connection between ongoing DeathRansom and various infostealing malware campaigns, all likely directed by one Russian-speaking individual living in Italy.

The first DeathRansom connection they were able to make was to an ongoing Vidar info-stealing campaign.

"[The samples] share the naming pattern and infrastructure used," researchers explained in a recent blog. "We also found evidence that a Vidar sample tried to download the DeathRansom malware."

Starting with a sample with a file name of "Wacatac_2019-11-20_00-10.exe," the researchers found that it was being downloaded from a Bitbucket directory maintained by someone using the handle "scat01." In looking at other malicious samples that accessed the same directory, they saw that one of them also contained standard Vidar libraries used to extract passwords from different browsers. This particular sample in turn was seen trying to download another DeathRansom variant that also used "Wacatac" in its name.

"DeathRansom uses the name 'Wacatac' to store crypto keys in a registry," Semenchenko and Ananin explained. "Therefore, based on the same malware hosting, the same name pattern, and the fact that the Vidar sample tried to download a DeathRansom sample, we can conclude that the Vidar campaign and the DeathRansom campaign are run by the same actor, who uses scat01 as a Bitbucket profile name as well as a name for some malware samples."

To dig deeper, they then looked for other malware samples containing the string scat01 – which revealed a cornucopia of malware types all apparently connected to this handle. The researchers found samples of the Azorult info-stealer that connects to a command-and-control (C2) server called "scat01[.]tk," for instance, as well as other scat01 connections to the Evrial info-stealer and the 1ms0rryStealer.

The investigation also led them to a website called gameshack[.]ru, controlled by attackers and used to distribute malicious samples with scat01 attribution strings. The domain housed a root folder containing various malicious samples for downloader malware, which in turn

fetches samples of the Evrial stealer and the Supreme cryptominer. The former listed scat01 in its owner field, while the latter was found to contain the Evrial stealer inside its body.

“This sample uses the same iplogger service for counting the infected hosts as the DeathRansom samples,” the researchers noted.

In total, they were able to link scat01 to campaigns using the Vidar stealer, Azorult stealer, Evrial stealer, 1ms0rryStealer and the Supreme miner – and of course DeathRansom, which began as a malicious joke – demanding a ransom without actually encrypting files. Recently though, FortiGuard Labs found that it has evolved into a fully fledged malware with real encryption capabilities.

Who is scat01?

The threat actor, scat01, turns out to (very likely) be a Russian-speaking cybercriminal living in Italy named Egor Nedugov, researchers said.

To find that out, the researchers embarked on a bonanza of web searches, following contact-info breadcrumbs across the internet.

For instance, scat01 was linked to a yandex.ru email address in the owner section of various samples. Semenchenko and Ananin thus decided to search underground forums for “scat01” – and found various additional connections to the malware constellation that they had previously uncovered.

A person with the scat01 nickname provided reviews (in Russian) of the Vidar stealer and Supreme miner; while another scat01 post on another forum has to do with the Evrial stealer. There was also a product review on Yandex.Market using the yandex.ru email address previously seen linked with the malware. This review was geotagged as being posted from Aksay, a small Russian town near Rostov-on-Don. The reviews all had the same profile picture.

“At this point, we are pretty sure that this Yandex profile is related to the scat01 profile we found on the Russian underground forum...as well as to the malware distributed from gameshack[.]ru,” the researchers noted.

From there, the duo attempted to link the scat01 handle with a real person. They got a hit when other searches turned up a YouTube channel advertising the gameshack[.]ru malicious website, with the username “SoftEgorka.” They also turned up a Skype link for the YouTube channel with the same username.

“When we searched for a SoftEgorka Skype user, we found [a] user profile on the same Russian underground forum #4,” the researchers noted. “This time the username ‘Super Info’ is used...By digging further among Super Info posts, we found an announcement about game accounts sales (Steam, WoT, Origin). Here we should note that stealers observed above are capable of stealing passwords from different games and game distribution platforms. This more indirect evidence that Super Info may be connected to the ongoing stealers campaign.”

The profile contained a WebMoney ID, which is also mentioned in another post from the same user, which contains yet another Skype address, "nedugov99." After a search for that address, they found an old advertisement for the sale of a game account. That contained a mobile phone number belonging to the Rostov-on-Don region and an ID corresponding to the name Egor Nedugov.

"The name 'Egor' corresponds to one of the underground nicknames, SoftEgorka, and the surname Nedugov corresponds to the Skype account nedugov99," the researchers said. "According to the profile, this individual lives in Rostov-on-Don. Remember that the Yandex review made by scat01 was done from Aksay – a small town near Rostov-on-Don."

In looking at Instagram and Facebook accounts for Egor Nedugov, researchers found that he had lived in Italy for some time.

Source: <https://threatpost.com/deathransom-campaign-malware-cornucopia/151567/>

2. Fake Windows 10 Desktop Used in New Police Browser Lock Scam

Scammers have taken an old browser scam and invigorated it using a clever and new tactic that takes advantage of your web browser's full-screen mode to show a fake Windows 10 desktop stating your computer is locked.

This type of scam is called a police browser locker. which pretends to be law enforcement locking your browser because due to illegal activity. These scams then state that if you pay a fine via a credit card, it will unlock your computer so you can use it again.

These types of scams are normally easy to detect as they utilize fake and suspicious URLs and allow you to use other apps on your computer even if the browser is locked.

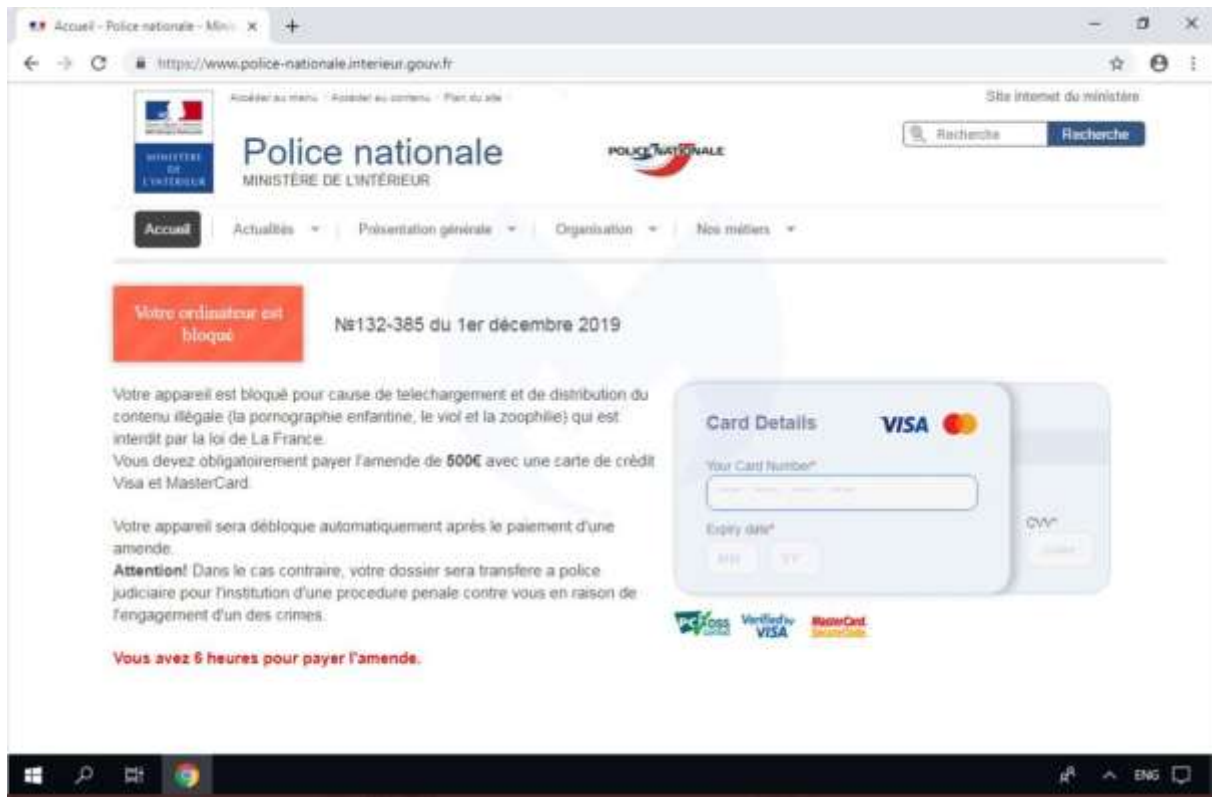
Overlaying a full-screen Windows 10 Desktop image

To make it harder for users to identify these types of scams, attackers are tricking web users into visiting fake sites that display a full-screen image of a Windows 10 desktop with the Chrome browser open.

These fake Windows 10 desktop images will fill up the entire screen and pretend to display the web site for the country's local police force. As the attackers are just displaying an image, they can also display the legitimate government URL to make it more convincing.

These fake web sites state that the police locked the user's computer for conducting illegal activities such as viewing and disseminating pornographic images of children, zoophilia, and

rape. Victims are then prompted to enter their credit card details to pay a fine of approximately \$800.



Fake Windows 10 Desktop shown by French browser locker

When displaying these screens, the scam will show different law enforcement web sites and languages depending on the URL visited or possibly what country you're from.

Malwarebytes who first posted about this new technique saw this scam targeting web users from Qatar, UAE, Oman, Kuwait, and France.

For example, below is some of the text shown in the UAE variant of this scam.

"Your browser has been locked due to viewing and dissemination of materials forbidden by law of [country], namely pornography with pedophilia, rape and zoophilia.

In order to unlocking you should a [amount] [currency] fine with Visa or MasterCard.

Your browser will be unlocked automatically after the fine payment.

Attention! In case of non-payment of the fine, or your attempts to unlock the device independently, case materials will be transferred to [police_force_name] for the institution of criminal proceedings against you due to commitment a crime."

If you enter your credit card details into this form, the attackers will automatically steal the payment information, which will then be sold online at underground criminal forums or used by the attackers for fraudulent purchases.

This tactic makes the scam more convincing

What makes this new variant of the police browser locker so clever is that when the image is shown by the browser in full-screen mode it overlays the entire screen, including the normal Windows 10 desktop.

This could cause users to think that the fake Windows 10 desktop image is their normal desktop. The difference, though, is that clicking on the Start Menu, closing apps, or starting new ones will not work.

What will be usable is an overlaid credit card form, which could make some users think that law enforcement has locked their computer until a fine is paid.

It is important to know that law enforcement will never lock your browser like this and then demand a fine be paid online.

If you ever see a message on your screen like this, press Alt+Tab to see if you can get back to your normal desktop or press Ctrl+Alt+Delete to open the Task Manager and terminate any browser processes.

Source: <https://www.bleepingcomputer.com/news/security/fake-windows-10-desktop-used-in-new-police-browser-lock-scam/>

3. Containers in the Cloud: False Assumptions and Security Challenges

As cloud infrastructures become widely adopted across many organizations, some are also moving their software projects to the cloud — specifically containerized environments. While this move brings agility and scale with it, a false assumption can also arise: “My applications are inside containers, so they are secure.” In reality, however, it’s often the opposite.

Putting applications into containers does not make them secure. For example, legacy applications may include previously unknown vulnerabilities. Container images may have vulnerabilities that date back several years and can rely on older frameworks that have known vulnerabilities. Containerized applications can run with excessive permissions, and the cloud itself can be misconfigured and leak data.

In all cases, applications and images do not gain security benefits simply from being containerized. Vulnerabilities will still exist, but you may just not know about them. Furthermore, managing security in the cloud follows the same basic rules as managing on-premises environments.

What Are Containers?

Before diving deeper into the topic, let's define the word "container." Although containerization in the cloud is a concept that has been gaining momentum across all sectors, not everyone knows what containers are and how they fit into the larger concept of a cloud environment.

The best analogy for containers are those colorful shipping boxes you see on large ships. Each box contains a set of goods, however, since you did not develop or pack the goods, you cannot see them nor know which types of goods are inside each one. Each container is a separate box that does not interact with the other boxes, although they may all be going to the same destination.

Containers in the cloud are similar to those boxes, except they are virtual. Developers build applications and put them inside containers. They can build separate parts of an application into each container and have the different parts essentially "sealed," even though they all run in the same cloud.

But while containers are there to provide isolation, the misconception that containers provide security for the applications inside them is a container security challenge within itself. It is tough to flip a misconception, especially when it involves taking additional steps in the container deployment and management process to integrate security.

Container Security Challenges Start With a Lack of Visibility

Challenges around secure containerization begin with a lack of visibility. Since IT organizations are typically the end receivers of containers — for example, applications were developed by a separate group, who, in turn, included software from other sources — it is tough for the company to know if applications were designed securely. How do you know if secure, up-to-date software was used? How do you know if the applications were tested to find and fix high-risk vulnerabilities that an attacker may exploit?

The simple answer is that unless security was integrated into the process and documented as part of the project, you likely don't know. Without knowing who developed the applications and how, it is nearly impossible to understand their security posture.

To make matters worse, containers tend to be "deploy and forget" assets, which could mean that no one is monitoring them for suspicious activities, outdated applications, lack of tooling and other security components. This lack of visibility into their security posture means fewer eyes on security gaps. When assessing the security of containers, X-Force Red, IBM Security's team of hackers, typically finds security deficiencies, such as misconfigurations, overly permissive access rights and insecure application logic, libraries, middleware and frameworks, to name a few.

Even With Basic Container Security Controls, Challenges Still Arise

Some organizations may be implementing basic container security processes, such as scanning the container environment to identify and fix vulnerabilities that could expose their contents to attackers. The limited number of organizations that do perform container scanning, however, face their own set of challenges. Each scan tends to uncover thousands of vulnerabilities, each with its own priority and risk profile, as well as remedial possibilities.

Buried in an already charged patching program, and often with limited manpower and time, security teams do not know which vulnerabilities pose the highest risk of a compromise, making it nearly impossible to know where to start with remediation. As teams manually try to prioritize the vulnerabilities that matter most, the window of opportunity for an attacker becomes larger. They may also waste resources by chasing down false positives and low-risk vulnerabilities, as the most dangerous ones continue exposing valuable assets or patching gets deferred until it's too late.

Strengthening Container Security in 2020

If just one of those security vulnerabilities enables attackers to gain access to an organization's container(s), attackers could also compromise the organization's internal environment and gain access to all of their assets — those in the cloud and on-premises. So, how can companies strengthen their container security more effectively?

It starts with understanding the container misconception. Just because your applications are inside a container that does not mean they are secure. Companies should then assess their container environment, which includes identifying which kinds of applications are in the containers, how important they are to the business, and what kind of data resides on them or is accessible by them. Companies should also review their containers' existing tools, processes, workflows and technical controls, so that they understand how, if at all, the applications inside are being protected and where gaps exist.

To do that, security teams could begin by performing a scan of their container environment. Scans, however, can typically uncover thousands of vulnerabilities, leaving security teams trying to manually piece together which ones pose the most risk and must be fixed first. That is why a real-world risk ranking capability is essential. Scanning and automated ranking must go hand in hand. After all, what is the point of identifying vulnerabilities if you do not know where to start fixing them?

A risk ranking system that is based on real-world weaponization of vulnerabilities, asset impact and exposure can be used to prioritize vulnerabilities so that the highest risk ones are at the top of the list for remediation. Automating this type of ranking using threat data makes the scan findings actionable so that remediation can begin immediately, and remediators only spend time and resources fixing the vulnerabilities that matter most. From there, steps to fix the vulnerabilities and prevent more in the future begin. That may mean making policy changes, monitoring container activity and analyzing suspicious events that are relevant to that environment.

Those additional steps may sound like a lot of work, but if your organization is scaling up delivery through containerization, then its cloud assets are part of the security program and must be handled as such. To avoid issues down the line, it is worth it to reduce your risk of a container breach.

Source: <http://feedproxy.google.com/~r/SecurityIntelligence/~3/loUCfJwvfSM/>

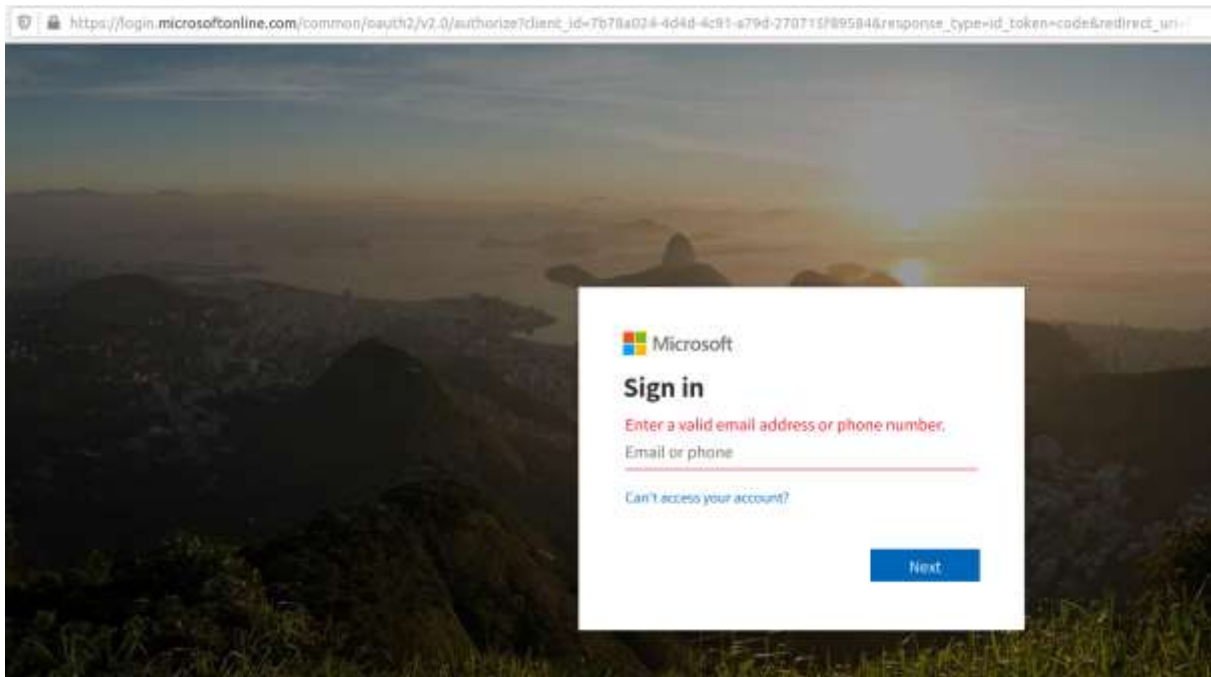
4. Tricky Phish Angles for Persistence, Not Passwords

Late last year saw the re-emergence of a nasty phishing tactic that allows the attacker to gain full access to a user's data stored in the cloud without actually stealing the account password. The phishing lure starts with a link that leads to the real login page for a cloud email and/or file storage service. Anyone who takes the bait will inadvertently forward a digital token to the attackers that gives them indefinite access to the victim's email, files and contacts — even after the victim has changed their password.

Before delving into the details, it's important to note two things. First, while the most recent versions of this stealthy phish targeted corporate users of **Microsoft's Office 365** service, the same approach could be leveraged to ensnare users of many other cloud providers. Second, this attack is not exactly new: In 2017, for instance, phishers used a similar technique to plunder accounts at Google's Gmail service.

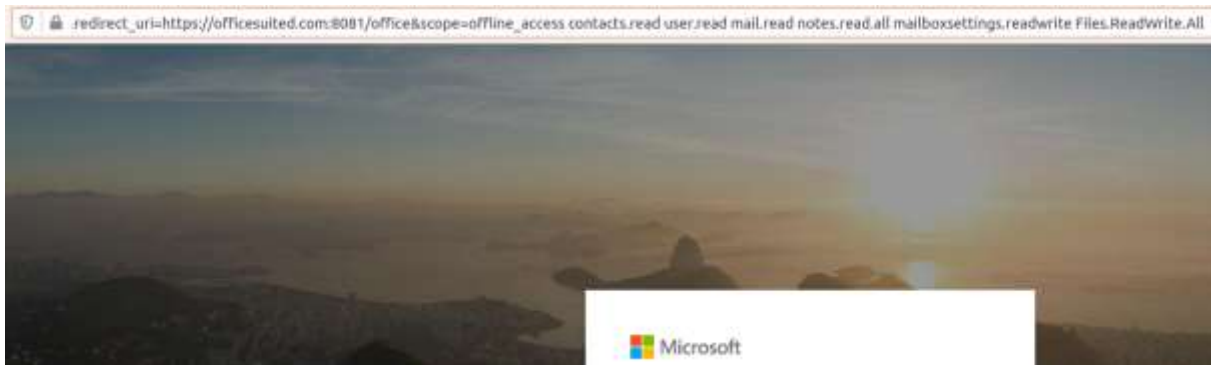
Still, this phishing tactic is worth highlighting because recent examples of it received relatively little press coverage. Also, the resulting compromise is quite persistent and sidesteps two-factor authentication, and it seems likely we will see this approach exploited more frequently in the future.

In early December, security experts at **PhishLabs** detailed a sophisticated phishing scheme targeting Office 365 users that used a malicious link which took people who clicked to an official Office 365 login page — **login.microsoftonline.com**. Anyone suspicious about the link would have seen nothing immediately amiss in their browser's address bar, and could quite easily verify that the link indeed took them to Microsoft's real login page:



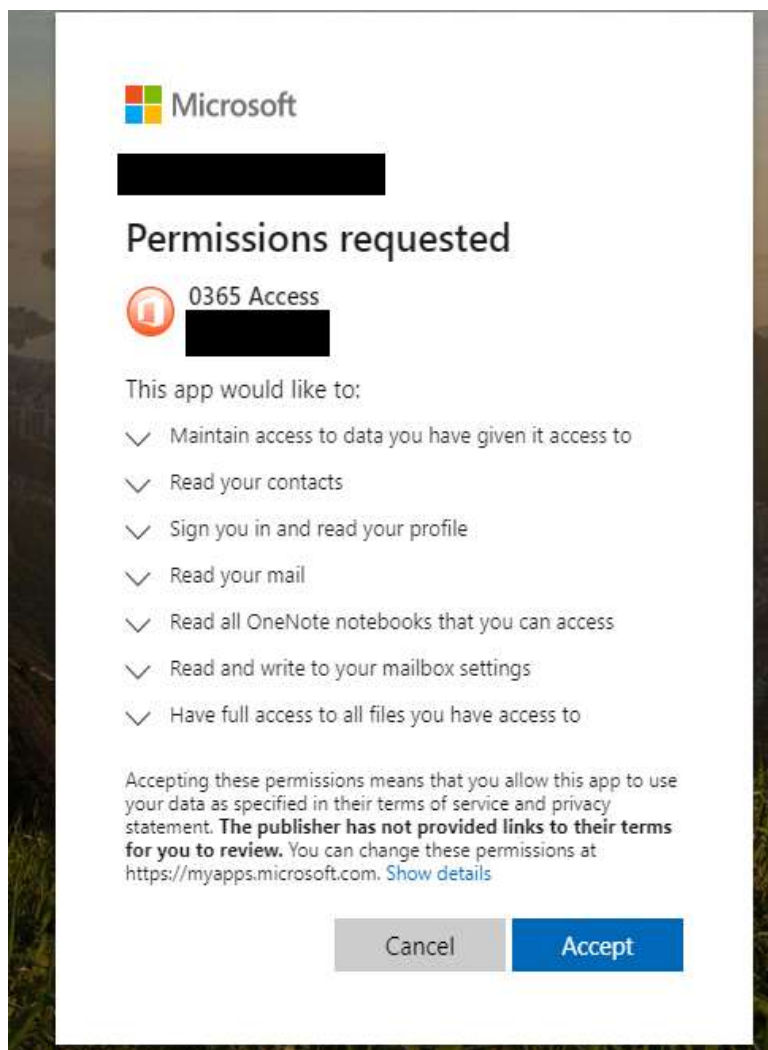
This phishing link asks users to log in at Microsoft's real Office 365 portal (login.microsoftonline.com).

Only by copying and pasting the link or by scrolling far to the right in the URL bar can we detect that something isn't quite right:



Notice this section of the URL (obscured off-page and visible only by scrolling to the right quite a bit) attempts to grant a malicious app hosted at officesuited.com full access to read the victim's email and files stored at Microsoft's Office 365 service.

As we can see from the URL in the image directly above, the link tells Microsoft to forward the authorization token produced by a successful login to the domain **officesuited[.]com**. From there, the user will be presented with a prompt that says an app is requesting permissions to read your email, contacts, OneNote notebooks, access your files, read/write to your mailbox settings, sign you in, read your profile, and maintain access to that data.



PhishLabs

According to PhishLabs, the app that generates this request was created using information apparently stolen from a legitimate organization. The domain hosting the malicious app pictured above — **officemtr[.]com** — is different from the one I saw in late December, but it was hosted at the same Internet address as **officesuited[.]com** and likely signed using the same legitimate company’s credentials.

PhishLabs says the attackers are exploiting a feature of Outlook known as “add-ins,” which are applications built by third-party developers that can be installed either from a file or URL from the Office store.

“By default, any user can apply add-ins to their outlook application,” wrote PhishLabs’ **Michael Tyler**. “Additionally, Microsoft allows Office 365 add-ins and apps to be installed via side loading without going through the Office Store, and thereby avoiding any review process.”

In an interview with KrebsOnSecurity, Tyler said he views this attack method more like malware than traditional phishing, which tries to trick someone into giving their password to the scammers.

“The difference here is instead of handing off credentials to someone, they are allowing an outside application to start interacting with their Office 365 environment directly,” he said.

Many readers at this point may be thinking that they would hesitate before approving such powerful permissions as those requested by this malicious application. But Tyler said this assumes the user somehow understands that there is a malicious third-party involved in the transaction.

“We can look at the reason phishing is still around, and it’s because people are making decisions they shouldn’t be making or shouldn’t be able to make,” he said. “Even employees who are trained on security are trained to make sure it’s a legitimate site before entering their credentials. Well, in this attack the site is legitimate, and at that point their guard is down. I look at this and think, would I be more likely to type my password into a box or more likely to click a button that says ‘okay?’”

The scary part about this attack is that once a user grants the malicious app permissions to read their files and emails, the attackers can maintain access to the account even after the user changes his password. What’s more, Tyler said the malicious app they tested was not visible as an add-in at the individual user level; only system administrators responsible for managing user accounts could see that the app had been approved.

Furthermore, even if an organization requires multi-factor authentication at sign-in, recall that this phish’s login process takes place on Microsoft’s own Web site. That means having two-factor enabled for an account would do nothing to prevent a malicious app that has already been approved by the user from accessing their emails or files.

Once given permission to access the user’s email and files, the app will retain that access until one of two things happen: Microsoft discovers and disables the malicious app, or an administrator on the victim user’s domain removes the program from the user’s account.

Expecting swift action from Microsoft might not be ideal: From my testing, Microsoft appears to have disabled the malicious app being served from officesuited[.]com sometime around Dec. 19 — roughly one week after it went live.

In a statement provided to KrebsOnSecurity, Microsoft Senior Director **Jeff Jones** said the company continues to monitor for potential new variations of this malicious activity and will take action to disable applications as they are identified.

“The technique described relies on a sophisticated phishing campaign that invites users to permit a malicious Azure Active Directory Application,” Jones said. “We’ve notified impacted customers and worked with them to help remediate their environments.”

Microsoft's instructions for detecting and removing illicit consent grants in Office 365 are here. Microsoft says administrators can enable a setting that blocks users from installing third-party apps into Office 365, but it calls this a "drastic step" that "isn't strongly recommended as it severely impairs your users' ability to be productive with third-party applications."

PhishLabs' Tyler said he disagrees with Microsoft here, and encourages Office 365 administrators to block users from installing apps altogether — or at the very least restrict them to apps from the official Microsoft store.

Apart from that, he said, it's important for Office 365 administrators to periodically look for suspicious apps installed on their Office 365 environment.

"If an organization were to fall prey to this, your traditional methods of eradicating things involve activating two-factor authentication, clearing the user's sessions, and so on, but that won't do anything here," he said. "It's important that response teams know about this tactic so they can look for problems. If you can't or don't want to do that, at least make sure you have security logging turned on so it's generating an alert when people are introducing new software into your infrastructure."

Source: <https://krebsonsecurity.com/2020/01/tricky-phish-angles-for-persistence-not-passwords/>

5. The Great \$50M African IP Address Heist

A top executive at the nonprofit entity responsible for doling out chunks of Internet addresses to businesses and other organizations in Africa has resigned his post following accusations that he secretly operated several companies which sold tens of millions of dollars worth of the increasingly scarce resource to online marketers. The allegations stemmed from a three-year investigation by a U.S.-based researcher whose findings shed light on a murky area of Internet governance that is all too often exploited by spammers and scammers alike.

There are fewer than four billion so-called "Internet Protocol version 4" or IPv4 addresses available for use, but the vast majority of them have already been allocated. The global dearth of available IP addresses has turned them into a commodity wherein each IP can fetch between \$15-\$25 on the open market. This has led to boom times for those engaged in the acquisition and sale of IP address blocks, but it has likewise emboldened those who specialize in absconding with and spamming from dormant IP address blocks without permission from the rightful owners.

Perhaps the most dogged chronicler of this trend is California-based freelance researcher Ron Guilmette, who since 2016 has been tracking several large swaths of IP address blocks

set aside for use by African entities that somehow found their way into the hands of Internet marketing firms based in other continents.

Over the course of his investigation, Guilmette unearthed records showing many of these IP addresses were quietly commandeered from African businesses that are no longer in existence or that were years ago acquired by other firms. Guilmette estimates the current market value of the purloined IPs he's documented in this case exceeds USD \$50 million.

In collaboration with journalists based in South Africa, Guilmette discovered tens of thousands of these wayward IP addresses that appear to have been sold off by a handful of companies founded by the policy coordinator for **The African Network Information Centre** (AFRINIC), one of the world's five regional Internet registries which handles IP address allocations for Africa and the Indian Ocean region.

That individual — Ernest Byaruhanga — was only the second person hired at AFRINIC back in 2004. Byaruhanga did not respond to requests for comment. However, he abruptly resigned from his position in October 2019 shortly after news of the IP address scheme was first detailed by **Jan Vermeulen**, a reporter for the South African tech news publication **Mybroadband.co.za** who assisted Guilmette in his research.

KrebsOnSecurity sought comment from AFRINIC's new **CEO Eddy Kayihura**, who said the organization was aware of the allegations and is currently conducting an investigation into the matter.

"Since the investigation is ongoing, you will understand that we prefer to complete it before we make a public statement," Kayihura said. "Mr. Byaruhanga's resignation letter did not mention specific reasons, though no one would be blamed to think the two events are related."

Guilmette said the first clue he found suggesting someone at AFRINIC may have been involved came after he located records suggesting that official AFRINIC documents had been altered to change the ownership of IP address blocks once assigned to **Infoplan** (now **Network and Information Technology Ltd**), a South African company that was folded into the State IT Agency in 1998.

"This guy was shoveling IP addresses out the backdoor and selling them on the streets," said Guilmette, who's been posting evidence of his findings for years to public discussion lists on Internet governance. "To say that he had an evident conflict of interest would be a gross understatement."

For example, documents obtained from the government of Uganda by Guilmette and others show Byaruhanga registered a private company called **ipv4leasing** after joining AFRINIC. Historic WHOIS records from domaintools.com [a former advertiser on this site] indicate Byaruhanga was the registrant of two domain names tied to this company — **ipv4leasing.org and .net** — back in 2013.

Guilmette and his journalist contacts in South Africa uncovered many instances of other companies tied to Byaruhanga and his immediate family members that appear to have been secretly selling AFRINIC IP address blocks to just about anyone willing to pay the asking price. But the activities of ipv4leasing are worth a closer look because they demonstrate how this type of shadowy commerce is critical to operations of spammers and scammers, who are constantly sully swaths of IP addresses and seeking new ones to keep their operations afloat.

Historic AFRINIC record lookups show ipv4leasing.org tied to at least six sizable blocks of IP addresses that once belonged to a now defunct company from Cameroon called **ITC** that also did business as "**Afriq*Access.**"

In 2013, Anti-spam group **Spamhaus.org** began tracking floods of junk email originating from this block of IPs that once belonged to Afriq*Access. Spamhaus says it ultimately traced the domains advertised in those spam emails back to **Adconion Direct**, a U.S. based email marketing company that employs several executives who are now facing federal criminal charges for allegedly paying others to hijack large ranges of IP addresses used in wide-ranging spam campaigns.

Source: <https://krebsonsecurity.com/2019/12/the-great-50m-african-ip-address-heist/>

6. Attackers Are Scanning for Vulnerable Citrix Servers, Secure Now

Security researchers have observed ongoing scans for Citrix Application Delivery Controller (NetScaler ADC) and Citrix Gateway (NetScaler Gateway) servers vulnerable to attacks exploiting CVE-2019-19781 during the last week.

This vulnerability impacts multiple Citrix products and it could potentially expose the networks of over 80,000 firms to hacking attacks according to a Positive Technologies report from December.

As the security outfit said at the time, "at least 80,000 companies in 158 countries are potentially at risk," with the top 5 countries being "the United States (the absolute leader, with over 38 percent of all vulnerable organizations), the UK, Germany, the Netherlands, and Australia."

"Depending on specific configuration, Citrix applications can be used for connecting to workstations and critical business systems (including ERP)," Positive Technologies added. "In almost every case, Citrix applications are accessible on the company network perimeter, and are therefore the first to be attacked."

No public exploits available

CVE-2019-19781 comes with a 9.8 Critical CVSS v3.1 base score and it could allow unauthenticated attackers to perform arbitrary code execution via Directory Traversal if successfully exploited.

However, as security researcher Kevin Beaumont who shared the info on active CVE-2019-19781 scans on Twitter said, currently no exploitation of this security issue has been observed and no information on an exploit is publicly available so far.

SANS Technology Institute's Dean of Research Johannes B. Ullrich who monitored scans for vulnerable Citrix systems during the last week also confirmed that no active exploitation has been observed and no public exploits are yet available.

Despite this, he also added that credible sources "have indicated that they were able to create a code execution exploit."

According to Citrix, CVE-2019-19781 affects all supported product versions and platforms:

- Citrix ADC and Citrix Gateway version 13.0 all supported builds
- Citrix ADC and NetScaler Gateway version 12.1 all supported builds
- Citrix ADC and NetScaler Gateway version 12.0 all supported builds
- Citrix ADC and NetScaler Gateway version 11.1 all supported builds
- Citrix NetScaler ADC and NetScaler Gateway version 10.5 all supported builds

Mitigation measures

While Citrix hasn't yet released a firmware patch to address this security flaw, the company did publish a set of mitigation measures for standalone systems and clusters and it strongly recommends all impacted customers to apply them as soon as possible.

"Customers should then upgrade all of their vulnerable appliances to a fixed version of the appliance firmware when released," Citrix also says.

To be alerted when updated firmware will be available for impacted Citrix products, customers are also advised to subscribe to bulletin alerts [here](#).

Nextron Systems's Florian Roth also provides a Sigma detection rule for SIEM systems for detecting CVE-2019-19781 exploitation attempts against Citrix Netscaler, Application Delivery Controller, and Citrix Gateway Attack.

This rule will check the web request and if it contains '/../vpns/' or '/vpns/cfg/smb.conf', will log it as a critical alert.

"Citrix applications are widely used in corporate networks. This includes their use for providing terminal access of employees to internal company applications from any device via the Internet," Positive Technologies's Director of Security Audit Department Dmitry Serebryannikov says.

"Considering the high risk brought by the discovered vulnerability, and how widespread Citrix software is in the business community, we recommend information security professionals take immediate steps to mitigate the threat."

Source: <https://www.bleepingcomputer.com/news/security/attackers-are-scanning-for-vulnerable-citrix-servers-secure-now/>

7. Mozilla Firefox 72.0.1 Patches Actively Exploited Zero-Day

Mozilla released Firefox 72.0.1 and Firefox ESR 68.4.1 to patch a critical and actively exploited severity vulnerability that could potentially allow attackers to execute code or trigger crashes on machines running vulnerable Firefox versions.

As Mozilla's security advisory says, the Firefox developers are "aware of targeted attacks in the wild abusing this flaw" which could make it possible for attackers who successfully exploit it to abuse affected systems.

The Firefox and Firefox ESR zero-day flaw fixed by Mozilla was reported by a research team from Qihoo 360 ATA.

BleepingComputer has reached out to the Qihoo 360 ATA researchers for additional details but had not heard back at the time of this publication.

The type confusion vulnerability tracked as CVE-2019-17026 impacts the web browser's IonMonkey Just-In-Time (JIT) compiler and it occurs when incorrect alias information is fed for setting array elements.

This type of security flaw can lead to out-of-bounds memory access in languages without memory safety which, in some circumstances, can lead to code execution or exploitable crashes.

Potential attackers could trigger the type confusion flaw by redirecting users of unpatched Firefox versions to maliciously crafted web pages.

CVE-2019-17026: IonMonkey type confusion with StoreElementHole and FallibleStoreElement

Reporter Qihoo 360 ATA

Impact critical

Description

Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion. We are aware of targeted attacks in the wild abusing this flaw.

References

[Bug 1607443](#)

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) also issued an alert saying that "an attacker could exploit this vulnerability to take control of an affected system," and advising users to review the Mozilla Security Advisory and apply the security update.

While there is no other info related to this 0-day flaw, all users should install the patched Firefox release by manually checking for the new update by going to the Firefox menu -> Help -> About Firefox.

This security patch comes a day after Firefox 72.0 was released with fixes for another 11 security vulnerabilities, give of them being classified as 'High', five classified as 'Medium', and one as 'Low'.

Of the five high severity vulnerabilities, four could potentially be used by attackers for arbitrary code execution after leading victims to specially crafted malicious pages.

In June 2019, Mozilla patched two other actively exploited zero-day vulnerabilities used in targeted attacks against cryptocurrency firms such as Coinbase.

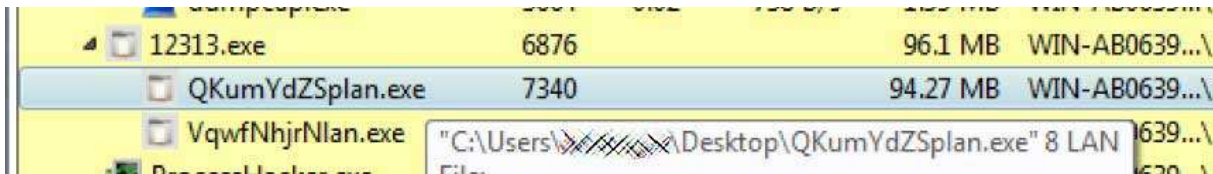
Source: <https://www.bleepingcomputer.com/news/security/mozilla-firefox-7201-patches-actively-exploited-zero-day/>

8. Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices

The Ryuk Ransomware uses the Wake-on-Lan feature to turn on powered off devices on a compromised network to have greater success encrypting them.

Wake-on-Lan is a hardware feature that allows a powered down device to be woken up, or powered on, by sending a special network packet to it. This is useful for administrators who may need to push out updates to a computer or perform scheduled tasks when it is powered down.

According to a recent analysis of the Ryuk Ransomware by Head of SentinelLabs Vitali Kremez, when the malware is executed it will spawn subprocesses with the argument '8 LAN'.



Spawning subprocess with 8 Lan argument

When this argument is used, Ryuk will scan the device's ARP table, which is a list of known IP addresses on the network and their associated mac addresses, and check if the entries are part of the private IP address subnets of "10.", "172.16.", and "192.168."

```

53     IF ( v6 )
54     {
55         while ( 1 )
56         {
57             sub_35004453((WORD *) (v6 + 12), (int)&cp);
58             if ( (char *)arp_rec_cmp_str(xmm0_0, (int)&cp, (const __m128i *)&byte_350111a8) == &cp // 10.
59                 || arp_rec_cmp_str(xmm0_0, (int)&cp, (const __m128i *)"172.16.")
60                 || arp_rec_cmp_str(xmm0_0, (int)&cp, (const __m128i *)"192.168.") )
61             {
62                 v05 = inet_addr(&cp);
63                 IF ( v05 == 0xFFFFFFFF )
64                     return 0xFFFFFFFF;
65                 sub_3500180a(*(BYTE *) (v6 + 44), &u24);
66                 u24 = (unsigned __int64)((255 - BYTE1(u24)) << 24)
67                     + (signed int)((0xFFFFFFFF - (unsigned __int8)u24) << 24)
68                     + (signed __int64)((255 - BYTE2(u24)) << 8) >> 32;
69                 v7 = ((255 - BYTE1(u24)) << 16) + ((0xFFFFFFFF - (unsigned __int8)u24) << 24) + ((255 - BYTE2(u24)) << 8);
70                 u23 = 255 - BYTE3(u24) + v7;
71                 u8 = 255 - BYTE3(u24) + _PAIR_(u24, u7);
72                 u9 = CFADD__((DWORD)u8, *(DWORD *)u3);
73                 *(_DWORD *)u3 += u8;
74                 u24 = HIWORD(u8);
75                 *(_DWORD *) (u3 + 4) += HIWORD(u8) + u9;
76                 IF ( u8 >= 0xFF )
77                     v10 = 0;
78                 else
79                     v10 = BYTE3(u35);

```

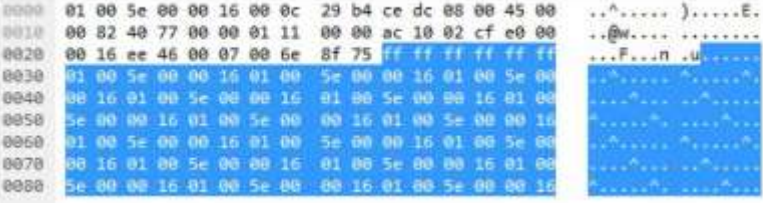
Checking for private network

If the ARP entry is part of any of those networks, Ryuk will send a Wake-on-Lan (WoL) packet to the device's MAC address to have it power up. This WoL request comes in the form of a 'magic packet' containing 'FF FF FF FF FF FF FF FF'.

```

▷ Frame 19: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
# Ethernet II, Src: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
  # Destination: IPv4mcast_16 (01:00:5e:00:00:16)
    Address: IPv4mcast_16 (01:00:5e:00:00:16)
    .... ..0. .... = IG bit: Globally unique address (factory default)
    .... ..1. .... = IG bit: Group address (multicast/broadcast)
  # Source: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc)
    Address: Vmware_b4:ce:dc (00:0c:29:b4:ce:dc)
    .... ..0. .... = IG bit: Globally unique address (factory default)
    .... ..8. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▷ Internet Protocol Version 4, Src: 172.16.2.207, Dst: 224.0.0.22
# User Datagram Protocol, Src Port: 60998, Dst Port: 7
  Source Port: 60998
  Destination Port: 7
  Length: 110
  Checksum: 0x8f75 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 4]
# Echo
  Echo data: ffffffff01005e00001601005e00001601005e000016...

```



Ryuk sending a WoL packet

If the WoL request was successful, Ryuk will then attempt to mount the remote device's C\$ administrative share.

```

\\172.16.2.208\C$\Program Files\Microsoft Visual Studio\2017\Community\Common7\IDE\CommonExtensions\Platform\Debugger\PerfDebuggerWebViews\loc
\\172.16.2.208\C$\Program Files\Microsoft Visual Studio\2017\Community\Common7\IDE\Extensions\Microsoft\VsGraphics\Assets\Scripts\Hsl\*.

```

Mount drive to the Remote C\$ Share

If they can mount the share, Ryuk will encrypt that remote computer's drive as well.

In conversations with BleepingComputer, Kremez stated that this evolution in Ryuk's tactics allow a better reach in a compromised network from a single device and shows the Ryuk operator's skill traversing a corporate network.

"This is how the group adapted the network-wide ransomware model to affect more machines via the single infection and by reaching the machines via WOL & ARP," Kremez told BleepingComputer. "It allows for more reach and less isolation and demonstrates their experience dealing with large corporate environments."

To mitigate this new feature, administrators should only allow Wake-on-Lan packets from administrative devices and workstations.

This would allow administrators to still benefit from this feature while adding some security to the endpoints.

At the same time, this does not help if an administrative workstation is compromised, which happens quite often in targeted ransomware attacks.

Source: <https://www.bleepingcomputer.com/news/security/ryuk-ransomware-uses-wake-on-lan-to-encrypt-offline-devices/>

9. PoCs for Windows CryptoAPI Bug Are Out, Show Real-Life Exploit Risks

Proof-of-concept exploit code is now available for the Windows CryptoAPI spoofing vulnerability tracked as CVE-2020-0601 and reported by the National Security Agency (NSA), just two days after Microsoft released a patch.

The PoC exploits for the flaw now known as CurveBall (per security researcher Tal Be'ery) were publicly released during the last 24 hours by Swiss cybersecurity outfit Kudelski Security and ollypwn.

British hardware hacker Saleem Rashid also developed a CurveBall PoC exploit but only tweeted screenshots of his exploit code abusing CVE-2020-0601.

What's next? Well, after these working PoC exploits were released, users and organizations should patch their systems by applying the security updates Microsoft released during this month's Patch Tuesday.

While the NSA and Microsoft stated that the flaw hasn't yet been exploited in the wild, the agency's advisory recommends installing the patches as soon as possible to block attackers from defeating "trusted network connections and deliver executable code while appearing as legitimately trusted entities."

DHS' Cybersecurity and Infrastructure Security Agency (CISA) also strongly recommended agencies to "patch all affected endpoints within 10 business days" in its second-ever Emergency Directive.

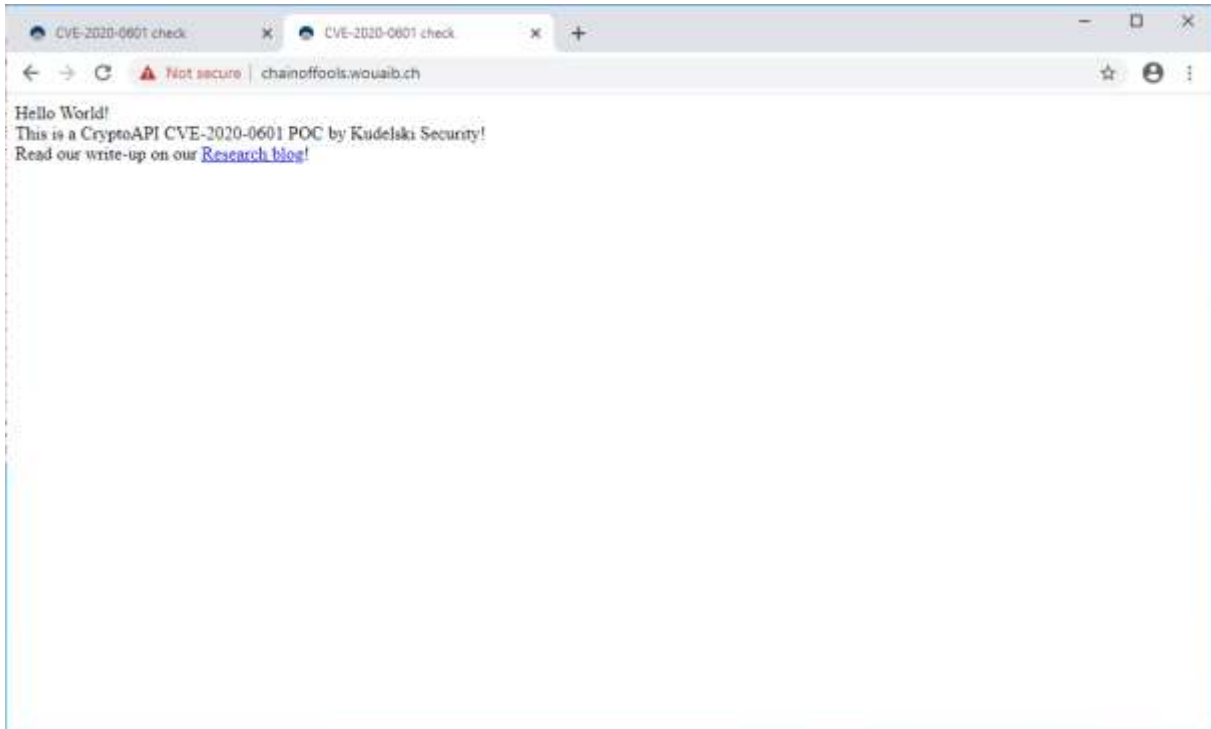
What's the potential impact of an attack exploiting CVE-2020-0601?

The spoofing vulnerability impacts Windows 10, Windows Server 2016 and 2019 versions of CRYPT32.DLL, while "an attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear the file was from a trusted, legitimate source," according to Microsoft.

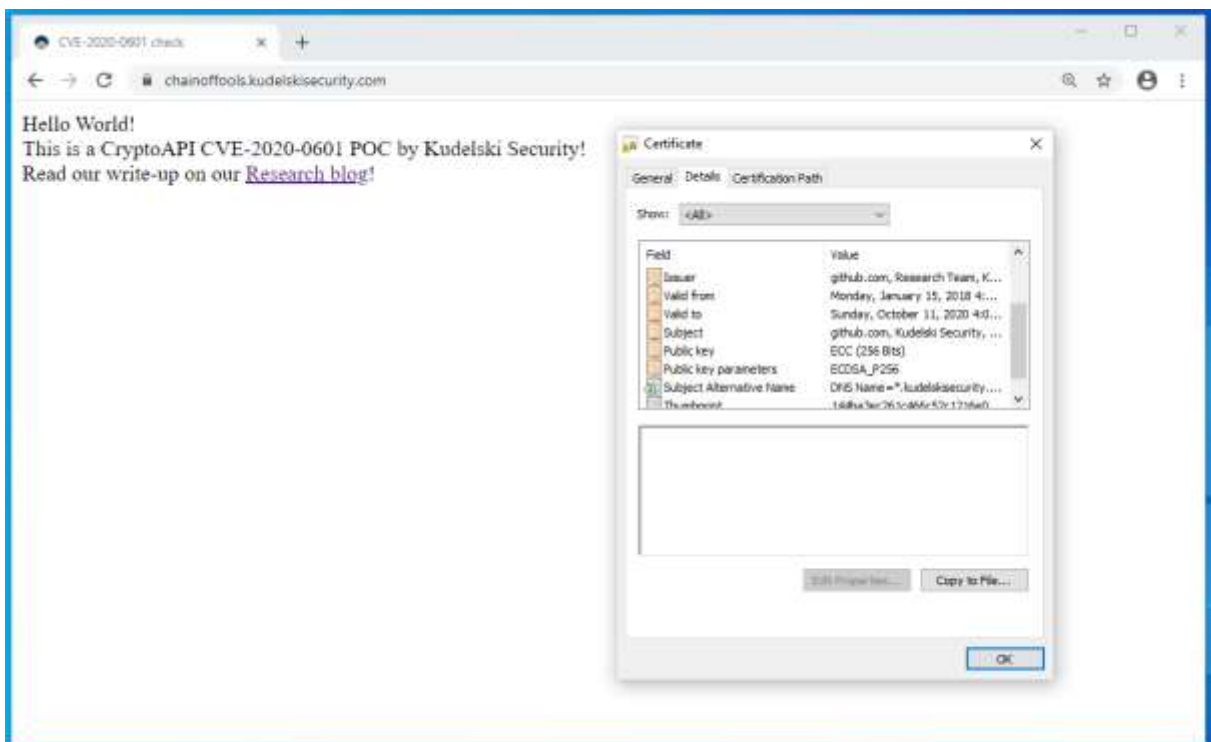
On compromised systems, attackers can launch man-in-the-middle attacks, as well as decrypt confidential info from network connections to impacted software and endpoints.

CERT/CC vulnerability analyst Will Dormann also revealed that "by exploiting this vulnerability, an attacker may be able to spoof a valid X.509 certificate chain on a vulnerable Windows system.

This may allow various actions including, but not limited to, interception and modification of TLS-encrypted communications or spoofing an Authenticode signature."



Chrome PoC on patched system



Chrome PoC on unpatched system

As Crowdstrike co-founder Dmitri Alperovitch further explained, the potential impact of CVE-2020-0601 includes remote code execution (due to auth bypass), compromise of HTTPs authentication, spoofing code signing (in user-mode), and spoofing content signing.

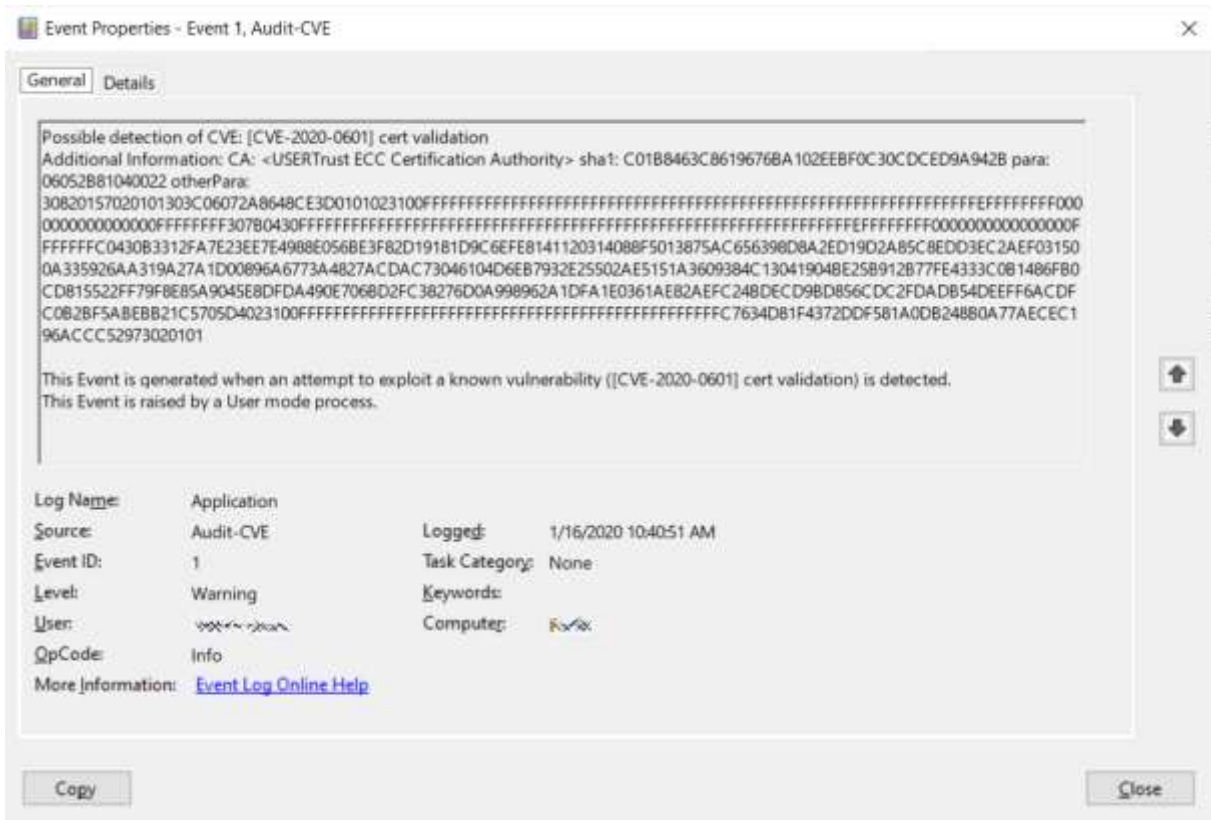
The code execution was also confirmed by the NSA: "The certificate validation vulnerability allows an attacker to undermine how Windows verifies cryptographic trust and can enable remote code execution."

Updated Windows logs exploitation attempts

Crowdstrike's head of EDR, Alex Ionescu and former Project Zero member Matt Tait confirmed yesterday that the Windows Update (WU) system — which was initially thought to have been also impacted — is not affected.

This is because the updates are signed with RSA certificates rather than ECC-based ones, preventing attackers from abusing as part of MiTM attacks to serve malicious code.

Luckily, as security researcher and co-director of the Open Crypto Audit Project (OCAP) Kenneth White noticed, some vendors including Crowdstrike already updated their security solutions to detect CurveBall exploitation attempts, while Microsoft updated Windows Defender to detect "files w/crafted certificates exploiting the certificate validation vulnerability," per Microsoft Defender ATP Product Manager Amitai Rottem.



Windows Event Viewer logging exploit attempts

To sum it all up, per the NSA "the consequences of not patching the vulnerability are severe and widespread. Remote exploitation tools will likely be made quickly and widely available.

Rapid adoption of the patch is the only known mitigation at this time and should be the primary focus for all network owners."

"In the end, please keep in mind that such a vulnerability is not at risk of being exploited by script kiddies or ransomware," Kudelski Security also added.

"While it is still a big problem because it could have allowed a Man-in-the-Middle attack against any website, you would need to face an adversary that owns the network on which you operate, which is possible for nation-state adversaries, but less so for a script kiddie.

This is why we are releasing this PoC, the exploitability of this vulnerability is not good enough to lead to a sudden ransomware threat (unlike the one we had with Wannacry)."

Source: <https://www.bleepingcomputer.com/news/security/pocs-for-windows-cryptoapi-bug-are-out-show-real-life-exploit-risks/>

10. TrickBot Now Uses a Windows 10 UAC Bypass to Evade Detection

The TrickBot Trojan has received an update that adds a UAC bypass targeting the Windows 10 operating system so that it infects users without displaying any visible prompts.

A UAC bypass allows programs to be launched without displaying a User Account Control prompt that asks users to allow a program to run with administrative privileges.



Example of UAC prompt

In a new TrickBot sample, Head of SentinelLabs Vitali Kremez discovered that the trojan is now using the Windows 10 Fodhelper bypass.

Using Windows 10 UAC bypass

When executed, TrickBot will check if the operating system is Windows 7 or Windows 10.

If it is Windows 7, TrickBot will utilize the CMSTPLUA UAC bypass and if Windows 10, will now use the Fodhelper UAC Bypass.

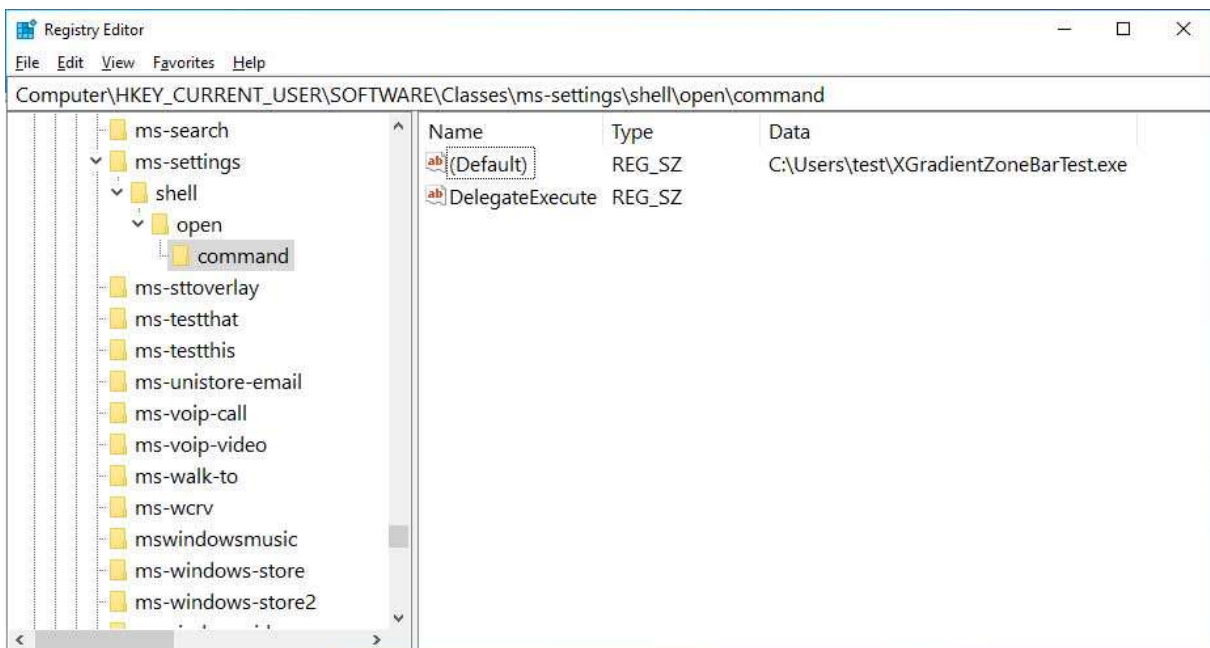
The Fodhelper bypass was discovered in 2017 and uses the legitimate Microsoft C:\Windows\system32\fodhelper.exe executable to execute other programs with administrative privileges.

"Fodhelper.exe is a trusted binary on Windows 10 that TrickBot uses to execute the malware stage bypassing UAC via the registry method," Kremez told BleepingComputer in a conversation.

When properly configured, when executed Fodhelper will also launch any command stored in the default value of the HKCU\Software\Classes\ms-settings\shell\open\command key.

As Fodhelper is a trusted Windows executable, it allows auto-elevation without displaying a UAC prompt. Any programs that it executes will be executed without showing a UAC prompt as well.

TrickBot utilizes this bypass to launch itself without a warning to the user and thus evading detection by the user.



Command executed by the Fodhelper UAC bypass

As more users move to Windows 10 and as Windows Defender matures, more malware has begun to target the operating system and its security features.

In September 2019 we reported how the GootKit banking Trojan also added the Fodhelper bypass in 2019 to execute a command that whitelists the malware executable's path in Windows Defender.

In July 2019, TrickBot also targeted Windows Defender by trying to disable various scan options. With the inclusion of Fodhelper, we continue to see the malware developers attempt to reduce the security features found in Windows 10.

Source: <https://www.bleepingcomputer.com/news/security/trickbot-now-uses-a-windows-10-uac-bypass-to-evade-detection/>

11. New NetWire RAT Campaigns Use IMG Attachments to Deliver Malware Targeting Enterprise Users

IBM X-Force researchers have discovered a new campaign targeting organizations with fake business emails that deliver NetWire remote-access Trojan (RAT) variants.

The RAT is hidden inside an IMG file, which is a file extension used by disk imaging software. Since many attachments can be automatically blocked by email security controls, spammers often carefully choose the type of file extensions they use in malspam messages, and shuffle the types of files they conceal malware in. X-Force's analysis shows that emails delivered by the NetWire RAT in this campaign are being sent from a small number of unique senders supposedly located in Germany.

The NetWire RAT is a malicious tool that emerged in the wild in 2012. This multi-platform malware has since undergone various upgrade cycles and was detected in different types of attacks that range from cybercrime endeavors by Nigerian scammers to advanced persistent threat (APT) attacks. The NetWire RAT is a commercial offering that can be easily purchased on Dark Web markets, which means that it can be used by just about any threat actor.

This isn't the first time NetWire is being delivered in fake business communications. In a previous campaign launched in September 2019, its operators sent booby-trapped fake PDF files to potential victims, indicating it was a commercial invoice. The actual file was an executable that installed the NetWire RAT as soon as the file was clicked.

Extracting a RAT

In one of the samples we looked into, an IMG file named "Sales_Quotation_SQUO00001760.img." was a way for the attackers to archive the malware until the file was clicked open. Once opened, it extracted an executable: the NetWire RAT.

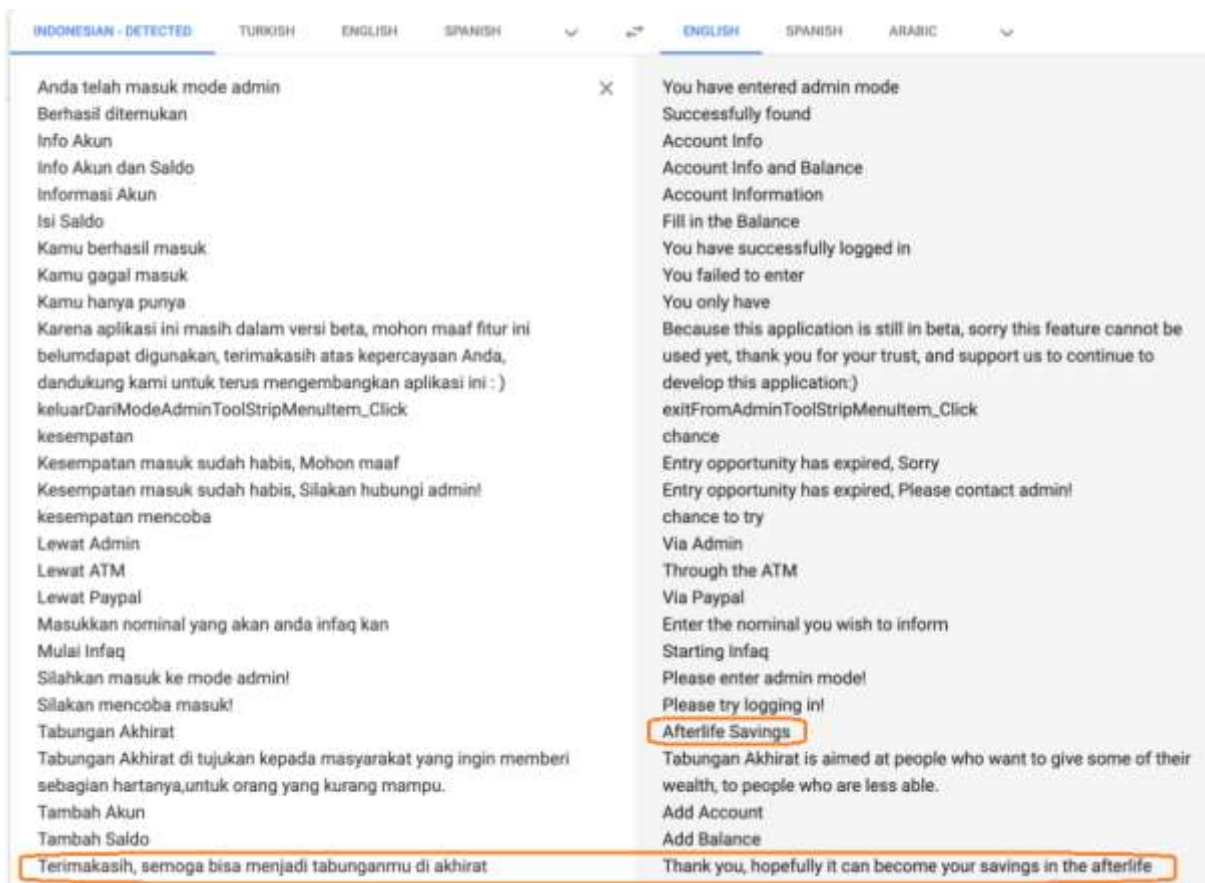
Immediately after this initial execution, the malware established persistence via a scheduled task, a common tactic to many malware developers. Scheduled tasks enable the malware to keep checking that it's active or relaunch itself in a recurring fashion.

Additionally, registry keys are created to store the command-and-control (C&C) server's IP address and save data used by the malware to operate on the infected device. Communication with the C&C server is performed over TCP port 3012.

What's the NetWire RAT Up To?

Since this malware can be used by any group with any motivation, attribution is rather futile. What we did want to figure out was what the NetWire RAT campaign we detected was after this time.

Looking at some unencrypted strings found in memory, we identified a series of strings written in a foreign language, which appears to be Indonesian. Below is a screenshot from Google Translate showing a rough translation of the various identified strings. Many of these terms either relate to a login prompt, payment options, donations or the term "afterlife savings":



Translated malware strings from recent NetWire RAT campaign

This term may relate to permanent life insurance for retirement purposes offered in some parts of the world.

From the overall look of it, this campaign is financially motivated and most likely being carried out by local fraudsters looking to rob account owners in various ways. Although we have not seen the complete post-infection flow, it may be followed up by a 419-type scam, or might also include social engineering or phishing pages to lure the victim to enter their banking credentials and enable the attackers to take over their accounts.

Recent campaigns in the wild show that the NetWire RAT is not the only malware being delivered via disk imaging file extensions. This was somewhat of a trend in late 2019, likely because the same spamming operators were distributing RATs for different threat actors.

Commercial Malware Abounds

Oftentimes, as security professionals, we hear about the larger and more impactful data breaches, ransomware attacks, and destructive campaigns, which are often carried out by sophisticated cybercrime gangs. But while most financially motivated cybercrime is the work of larger, organized crime groups, smaller factions are still very much in business, and they too target businesses to compromise bank accounts and steal money by using commercially available malware year-round.

Indicators of compromise (IoCs) and other information on how to protect networks from the NetWire RAT can be found on IBM X-Force Exchange.

The post [New NetWire RAT Campaigns Use IMG Attachments to Deliver Malware Targeting Enterprise Users](#) appeared first on Security Intelligence.

Source: <http://feedproxy.google.com/~r/SecurityIntelligence/~3/WbKg8pSkPs/>

12. Windows EFS Feature May Help Ransomware Attackers

Security researchers have created concept ransomware that takes advantage of a feature in Windows that encrypts files and folders to protect them from unauthorized physical access to the computer.

The lab-developed ransomware strain relies on the Encrypting File System (EFS) component in Microsoft's operating system and can run undetected by some antivirus software.

Abusing a legitimate feature

EFS allows users to encrypt specific files and folders with a symmetric key known as File Encryption Key, which is then encrypted with a public key (asymmetric encryption). This process and its reversal is done at a layer below the NT file system (NTFS).

The component is available in Professional and above editions of Microsoft's operating system starting Windows 2000. It is different than Bitlocker, which encrypts the entire drive.

Researchers at Safebreach Labs developed concept ransomware that relies on EFS to lock files on a Windows computer. The way it functions is described in the steps below:

1. The ransomware generates a key (using AdvApi32!CryptGenKey) to be used by EFS and records the file name used by CAPI for this key.
2. The ransomware generates a certificate for this key, using Crypt32!CertCreateSelfSignCertificate, and adds it to the personal ("MY") certificate store using Crypt32!CertAddCertificateContextToStore.
3. The ransomware sets the current EFS key to this certificate using AdvApi32!SetUserFileEncryptionKey.
4. Now the ransomware can invoke AdvApi32!EncryptFile on every file/folder to be encrypted.
5. The ransomware saves the key file (whose name was recorded in step 1) to memory and deletes it from the following two folders:
 - %APPDATA% \Microsoft\Crypto\RSA\sid\ (where sid is the user SID)
 - %ProgramData% \Microsoft\Crypto\RSA\MachineKeys\
6. The ransomware flushes the EFS data from memory using the undocumented AdvApi32!FlushEfsCache (available since Windows Vista). At this time, the encrypted files become unreadable to the user (and operating system).
7. Ideally, the ransomware wipes the slack parts of the disk to ensure that data from the deleted the EFS key files and temporary files used by EncryptFile cannot be salvaged. This can also be done before the previous step.
8. The ransomware can now encrypt the key file data collected in step 5, for example, using an asymmetric (public) key hard-wired into the ransomware and send the encrypted data to the attacker directly (or instruct the victim to do so).

Source: <https://www.bleepingcomputer.com/news/security/windows-efs-feature-may-help-ransomware-attackers/>

13. BitPyLock Ransomware Now Threatens to Publish Stolen Data

A new ransomware called BitPyLock has quickly gone from targeting individual workstations to trying to compromise networks and stealing files before encrypting devices.

BitPyLock was first discovered by MalwareHunterTeam on January 9th, 2020 and has since seen a trickle of new victims daily.

What is interesting is that we can compare the ransom notes of earlier versions with the latest versions to see a clear progression in the types of victims that are targeted.

To make matters worse, as ransomware operators begin stealing data before encrypting victims for use as leverage, BitPyLock actors claim to be adopting this tactic as well.

The BitPyLock Ransomware

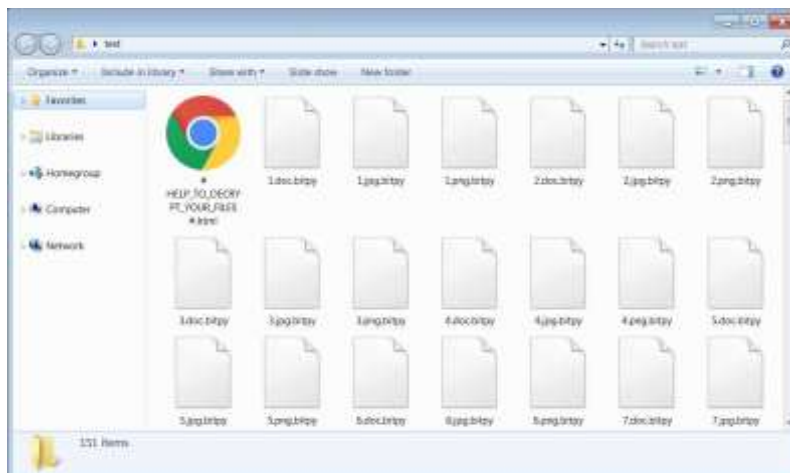
Based on our analysis, when first launched, BitPyLock will attempt to terminate any processes that contain the following strings. This is done to terminate security software and close files being used by backup software, web server daemons, virtual machines, and databases so that they can be encrypted.

```
backup, cobain, drop, drive, sql, database, vmware, virtual, agent, anti, iis,
web, server, apache
```

While encrypting files, BitPyLock will target 346 extensions (listed in the IOCs section) and will skip any files located in the following folders.

```
windows
windows.old
program files
program files (x86)
program data
$recycle.bin
system volume information
```

For every encrypted file, the ransomware will append the **.bitpy** extension as shown below. For example, a file named 1.doc will be encrypted and renamed to 1.doc.bitpy.



Encrypted BitPyLock files

In each folder and on the Windows desktop, BitPyLock will create a ransom note named # **HELP_TO_DECRYPT_YOUR_FILES** #.html that instructs the users to send a bitcoin ransom to the enclosed bitcoin address. It then instructs the victim to email the listed address to get a decryptor.

In the sample BleepingComputer analyzed, the ransom amount was hardcoded to .8 bitcoins.

The language in the original ransom note also indicated that the attackers were targeting individual machines rather than networks.



Original ransom note

Strangely, the sample that we saw had a static bitcoin address in the executable, which means every victim would have the same bitcoin address and thus it could make it impossible to determine who paid the ransom.

Evolves to network attacks and the publishing of stolen data

In a more recent version discovered by MalwareHunterTeam, the actors have changed their targeting to focus on network compromise and the claims of stealing data before encrypting devices.



All your files are encrypted!

If you read this message. That means we've been able to break into your network and encrypt all your machines.

All your files on all network machines, including, but not limited to:
Documents, databases, and office projects have been encrypted using strong military grade encryption algorithm **RSA-4096**.
Break it is impossible! and any effort is a waste of time!

Recovery tools and other software will not help you!
Don't find your backups? because they have been successfully encrypted too or securly wiped!

The only way to recover your files, are to meet our demand.

1. Create a Bitcoin wallet (we recommend you to create on [Blockchain.com](#))
2. Register on [LocalBitcoins.com](#) (or any other Bitcoin exchange), then buy [redacted] Bitcoin (BTC).
3. Send Bitcoins to our wallet below (in case sensitive. Make sure you copy past it):
[redacted]
4. Send Bitcoin Transaction ID to our e-mail address along with our wallet address you pay!
[redacted]
5. You will receive the tools needed to decrypt all of your machines and files!
Note: Before payment you can contact with us for 1 free small file as decryption test!

Be warned, we won't be able to recover your files if you start fiddling with them!
If you do not wish to negotiate with us. We will make your company's private papers and databases public. This's not a joke!

You have 72 hours from this moment to send us payment, or you files and the way we communicate will be lost in eternity!

New ransom note targeting networks

In this version of the ransom note, we can see that the attackers are targeting "all your files on all network machines".

For entire network decryption, BitPyLock's ransom amounts are also fairly low compared to other targeted ransomware at only approximately 5 bitcoins for the entire network.

The ransom note further states that they will release stolen data if a ransom payment is not made.

"If you do not wish to negotiate with us. We will make your company's private papers and databases public. This's is not a joke!"

Unlike Maze Ransomware and Sodinokibi Ransomware who have already released stolen files belonging to non-paying victims, BitPyLock has not done so at this time.

This could also just be an empty threat like ransomware operators used to make in the past. Unfortunately, there is no way to tell anymore as more ransomware actors begin to actually release stolen data.

IOCs:

Hashes:

```
274011aaa97fd19ad6d993a5555c9306090da6a9b16c991739033ebb7673a244
```

Associated file names:

```
# HELP_TO_DECRYPT_YOUR_FILES #.html
```

Targeted Extensions:

```
.frx, .jin, .xls, .xlsx, .pdf, .doc, .docx, .ppt, .pptx, .log, .txt, .gif, .png, .conf, .data, .dat, .dwg, .asp, .aspx, .html, .tif, .htm, .php, .jpg, .jsp, .js, .cnf, .cs, .vb, .vbs, .mdb, .mdf, .bak, .bkf, .java, .jar, .war, .pem, .pfx, .rtf, .pst, .dbx, .mp3, .mp4, .mpg, .bin, .nvram, .vmdk, .vmsd, .vmx, .vmxf, .vmsn, .vmem, .gz, .3dm, .3ds, .zip, .rar, .3fr, .3g2, .3gp, .3pr, .7z, .ab4, .accdb, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .ads, .agdl, .ai, .ait, .al, .apj, .arw, .asf, .asm, .asx, .avi, .awg, .back, .backup, .backupdb, .pbl, .bank, .bay, .bdb, .bgt, .bik, .bkp, .blend, .bpw, .c, .cdf, .cab, .chm, .cdr, .cdr3, .cdr4, .cdr5, .cdr6, .cdrw, .cdx, .ce1, .ce2, .cer, .cfp, .cgm, .cib, .class, .cls, .cmt, .cpi, .cpp, .cr2, .craw, .crt, .crw, .csh, .csl, .csv, .dac, .db, .db3, .dbf, .db-journal, .dc2, .dcr, .dcs, .ddd, .ddoc, .ddrw, .dds, .der, .des, .design, .dgc, .djvu, .dng, .dot, .docm, .dotm, .dotx, .drf, .drw, .dtd, .dxb, .dxg, .jse, .dxg, .eml, .eps, .erbsql, .erf, .exf, .fdb, .ffd, .fff, .fh, .fmb, .fhd, .fla, .flac, .flv, .fpx, .fxg, .gray, .grey, .gry, .h, .hbk, .hpp, .ibank, .ibd, .ibz, .idx, .iif, .iiq, .incpas, .indd, .jpe, .jpeg, .kc2, .kdbx, .kdc, .key, .kpdx, .lua, .m, .m4v, .max, .mdc, .mef, .mfw, .mmw, .moneywell, .mos, .mov, .mrw, .msg, .myd, .nd, .ndd, .nef, .nk2, .nop, .nrw, .ns2, .ns3, .ns4, .nsd, .nsf, .nsg, .nsh, .nwb, .nx2, .nx1, .nyf, .oab, .obj, .odb, .odc, .odf, .odg, .odm, .odp, .ods, .odt, .oil, .orf, .ost, .otg, .oth, .otp, .ots, .ott, .p12, .p7b, .p7c, .pab, .pages, .pas, .pat, .pcd, .pct, .pdb, .pdd, .pef, .pl, .plc, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .pptm, .prf, .ps, .psafe3, .psd, .pspimage, .ptx, .py, .qba, .qbb, .qbm, .qbr, .qbw, .qbx, .qby, .r3d, .raf, .rat, .raw, .rdb, .rm, .rw2, .rwl, .rwz, .s3db, .sas7bdat, .say, .sd0, .sda, .sdf, .sldm, .sldx, .sql, .sqlite, .sqlite3, .sqlitedb, .sr2, .srf, .srt, .srw, .st4, .st5, .st6, .st7, .st8, .std, .sti, .stw, .stx, .svg, .swf, .sxc, .sxd, .sxd, .sxi, .sxi, .sxm, .sxw, .tex, .tga, .thm, .tlg, .vob, .wallet, .wav, .wb2, .wmv, .wpd, .wps, .x11, .x3f, .xis, .xla, .xlam, .xlb, .xlm, .xlr, .xlsb, .xlsm, .xlt, .xltm, .xltx, .xlw, .ycbcra, .yuv
```

Source: <https://www.bleepingcomputer.com/news/security/bitpylock-ransomware-now-threatens-to-publish-stolen-data/>

14. FTCODE Ransomware Now Steals Chrome, Firefox Credentials

New versions of the ransomware now sniff out saved credentials for Internet Explorer, Mozilla Firefox, Mozilla Thunderbird, Google Chrome and Microsoft Outlook.

FTCODE, a PowerShell-based ransomware that targets Italian-language users, has added new capabilities, including the ability to swipe saved web browser and email client credentials from victims.

Samples of the ransomware, which has been around since 2013, were recently observed in September 2019. After further analysis, researchers say new versions of the ransomware now aim to steal credentials from Internet Explorer and Mozilla Firefox, as well as email clients Mozilla Thunderbird, Google Chrome and Microsoft Outlook.

“The FTCODE ransomware campaign is rapidly changing,” said researchers Rajdeepsinh Dodia, Amandeep Kumar and Atinderpal Singh with Zscaler, in an analysis last week. “Due to the scripting language it was written in, it offers multiple advantages to threat actors, enabling them to easily add or remove features or make tweaks much more easily than is possible with traditionally compiled malware.”

It’s unclear how many victims have been targeted as part of FTCODE’s recent campaign; Threatpost has reached out to researchers for more details.

Attack Chain

The attack chain for FTCODE previously started with spam emails being sent to victims containing malicious macro documents, which when clicked downloaded the ransomware. However, in more recent campaigns, the bad actor has been sending victims links to VBScripts, which then download FTCODE. Once a user executes the VBScript, it in turn executes a PowerShell script, which then downloads and opens up a decoy image (saved into the **%temp%folder**).

This image, which purports to be an outline of prices (the image is titled “Dettaglio dei costi” in Italian, translated to “cost details”), attempts to convince users that they simply received an image. However, in the background, the ransomware is downloaded (saved in **%Public%\Libraries\WindowsIndexingService.vbs**) and executed.

The ransomware then searches for all drives with at least 50 KB of free space and starts encrypting the files with various extensions (see picture below for a full list of the extensions).


```
*.sql","*.mp4","*.7z","*.rar","*.m4a","*.wma","*.avi","*.wmv","*.csv","*.d3dbsp","*.zip"
"*.sie","*.sum","*.ibank","*.t13","*.t12","*.gdf","*.gdb","*.tax","*.pkpass","*.bc6","*.
oc7","*.bkp","*.qic","*.bkf","*.sidn","*.sidd","*.mddata","*.itl","*.itdb","*.icxs","*.hv
pl","*.hplg","*.hkdb","*.mdbbackup","*.synodb","*.gho","*.cas","*.svg","*.map","*.wmo","*.
itm","*.sb","*.fos","*.mov","*.vdf","*.ztmp","*.sis","*.sid","*.ncf","*.menu","*.layout",
"*.dmp","*.blob","*.esm","*.vcf","*.vtf","*.dazip","*.fpk","*.mlx","*.kf","*.iwd","*.vpk"
"*.tor","*.psk","*.rim","*.w3x","*.fsh","*.ntl","*.arch00","*.lvl","*.snx","*.cfr","*.ff
"*.vpp_pc","*.lrf","*.m2","*.mcmeta","*.vfs0","*.mpqge","*.kdb","*.db0","*.dba","*.rofl
"*.hxx","*.bar","*.upk","*.das","*.iwi","*.litemod","*.asset","*.forge","*.ltx","*.bsa"
"*.apk","*.re4","*.sav","*.lbf","*.slm","*.bik","*.epk","*.rgss3a","*.pak","*.big","*.wal
let","*.wotreplay","*.xxx","*.desc","*.py","*.m3u","*.flv","*.js","*.css","*.rb","*.png",
"*.jpeg","*.txt","*.p7c","*.p7b","*.p12","*.pfx","*.pem","*.crt","*.cer","*.der","*.x3f",
"*.srw","*.pef","*.ptx","*.r3d","*.rw2","*.rwl","*.raw","*.raf","*.ori","*.nrw","*.mrwref
"*.mef","*.erf","*.kdc","*.dcr","*.cr2","*.crw","*.bay","*.sr2","*.srf","*.arw","*.3fr"
"*.dng","*.jpe","*.jpg","*.odr","*.indd","*.ai","*.eps","*.pdf","*.pdd","*.psd","*.dbf",
"*.mdf","*.wb2","*.rtf","*.wpd","*.dxg","*.xf","*.dwg","*.pst","*.acodb","*.mdb","*.pptm"
"*.pptx","*.ppt","*.xlk","*.xlsb","*.xlsm","*.xlsx","*.xls","*.wps","*.docm","*.docx","*
.doc","*.odb","*.odc","*.odm","*.odp","*.ods","*.odt|
```

Credential Theft

Once downloaded, FTCODE takes history details from Internet Explorer and decrypts the stored credentials from information in the registry (HKCU:\Software\Microsoft\Internet Explorer\IntelliForms\Storage2).

For Mozilla Firefox and Thunderbird, the script checks four paths and steals any credentials in them (SystemDrive\Program Files\Mozilla Firefox, SystemDrive\Program Files\Mozilla Thunderbird, SystemDrive\Program Files (x86)\Mozilla Firefox, SystemDrive\Program Files (x86)\Mozilla Thunderbird). For Google Chrome, the ransomware steals files from the file %UserProfile%\AppData\Local\Google\Chrome\User Data*\Login Data.

And, in Microsoft Outlook, the ransomware accesses the registry key below to steal the credentials:

- HKCU:\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles*\9375CFF0413111d3B88A00104B2A6676*
- HKCU:\Software\Microsoft\Office\1[56].0\Outlook\Profiles*\9375CFF0413111d3B88A00104B2A6676*

All your files was encrypted!

Yes, You can Decrypt Files Encrypted!!!

Your personal ID: %guid%

1. Download Tor browser - <https://www.torproject.org/download>

2. Install Tor browser

3. Open Tor Browser

4. Open link in TOR browser:

<http://qvo5td7p5yazubrgioiky7rlu4vslxrcasrnhjr7rtn3t2pihp56w1qd.onion/?guid=%guid%>

5. Follow the instructions on this page

***** Warning*****

Do not rename files

Do not try to hack your data using third-party software, it may cause permanent data loss.(If you do not believe us, and still try to - make copies of all files so that we can help you if third-party software harms them)

As evidence, we can for free back one file

Decoders of other users is not suitable to back your files - encryption key is created on your computers when the program is launched - it is unique.

After encryption, the ransomware drops the ransom note "READ_ME_NOW.htm" in the directory that contains the encrypted files. The ransom note gives instructions to download a Tor browser and follow the instructions on the browser for next steps.

As ransomware attacks can be extremely damaging to businesses, more ransomware strains are continuously evolving to update their targeting and capabilities.

"This trend toward more creative ways to exploit... is a compelling reason to focus on stronger preventative measures and not just the ability to quickly restore files after the infection occurs," Erich Kron, security awareness advocate at KnowBe4, said in an email.

Source: <https://threatpost.com/ftcode-ransomware-steals-chrome-firefox-credentials/152022/>

15. Russia Blocks ProtonMail and ProtonVPN, Tor to the Rescue

Proton Technologies' security-focused ProtonMail end-to-end encrypted email service and ProtonVPN VPN service have been blocked by the Russian government since yesterday.

"On January 29, based on the requirements of the General Prosecutor's Office of the Russian Federation, Roskomnadzor will restrict access to the mail service Protonmail.com (Switzerland)," Roskomnadzor, Russia's telecommunications watchdog, said in a press release.

"This email service was used by cybercriminals both in 2019 and especially actively in January 2020 to send false messages under the guise of reliable information about mass mining of objects in the Russian Federation," Roskomnadzor added.

The block was prompted by Proton Technologies' refusal to register their services with state authorities — something that was asked from all VPN providers operating in the country as we reported last year — and to provide information about the owners of the mailboxes used to send the bombing threats per Roskomnadzor's statement.

"In accordance with the procedure enshrined in the legislation, Roskomnadzor consistently restricts access to resources used by criminals to destabilize the situation in the country and increase tension, and expects effective interaction with all parties involved," the press release further explains.



ProtonMail and ProtonVPN service status

Proton Technologies' response

The Swiss company behind ProtonMail and ProtonVPN published an incident on its status page, which currently lists partial outages for most services needed by the company's products to work properly.

"We have received reports that Proton is currently blocked in Russia. We are reaching out to the appropriate authorities to get the block lifted as soon as possible," the company says.

"This block affects ProtonMail and ProtonVPN users who were not logged in before the block was implemented. For now, we recommend using the TOR network (via the TOR Browser) to access our services."

ProtonMail also said in a statement to Reuters that they "condemn this block as a misguided measure which only serves to harm ordinary people."

Although access to both services is restricted for any Russian users, Proton Technologies says that ways to get around this block are available.

ProtonMail and ProtonVPN users are advised to access the two services using the Tor service specifically is designed to help circumvent censorship.

To get access to Proton's services using the Tor Browser you will have to follow these steps:

1. Download the TOR browser for your device here: <https://www.torproject.org/download/>
2. Install the TOR browser
3. Once the browser is installed, launch it and you will be able to access the Proton websites

ProtonVPN users who cannot log in into the app will have to manually set up an OpenVPN connection for their device until the block is lifted:

1. Open the TOR browser
2. Navigate to the ProtonVPN Knowledge Base: <https://protonvpn.com/support/>

3. Search for the OpenVPN guide for your OS, for instance type "Windows OpenVPN"
4. Open the guide and follow the steps to set up a manual connection on your device
5. Connect using your OpenVPN/IKEv2 credentials

Source: <https://www.bleepingcomputer.com/news/security/russia-blocks-protonmail-and-protonvpn-tor-to-the-rescue/>

16. Microsoft Detects New Evil Corp Malware Attacks After Short Break

Microsoft says that an ongoing Evil Corp phishing campaign is using attachments featuring HTML redirectors for delivering malicious Excel documents, this being the first time the threat actors have been seen adopting this technique.

The new campaign is detailed in a series of tweets from the Microsoft Security Intelligence account, with the researchers saying that the final payload is being dropped using an Excel document that bundles a malicious macro.

Evil Corp (also tracked as TA505 and SectorJ04) is a financially motivated cybercrime group active since at least Q3 2014 [1, 2] known for focusing on attacks against retail companies and financial institutions via large-sized malicious spam campaigns driven by the Necurs botnet.

This threat actor distributed remote access Trojans (RATs) and malware downloaders that delivered the Dridex and Trick banking Trojans as secondary payloads, as well as Locky, BitPaymer, Philadelphia, Globelmposter, Jaff ransomware strains on their targets' computers. [1, 2]

TA505 back from vacation

"The new campaign uses HTML redirectors attached to emails. When opened, the HTML leads to the download Dudear, a malicious macro-laden Excel file that drops the payload," Microsoft Security Intelligence's researchers explain. "In contrast, past Dudear email campaigns carried the malware as an attachment or used malicious URLs."

As mentioned in the beginning, this campaign also marks the adoption of HTML redirectors as this is the first time Microsoft observed this technique being used by Dridex's authors as part of their attacks.

Past email campaigns distributing the malware would deliver the payload onto the victim's computer within the attachment or via malicious download URLs.

The phishing messages come with HTML attachments which will automatically start downloading the Excel file used to drop the payload.

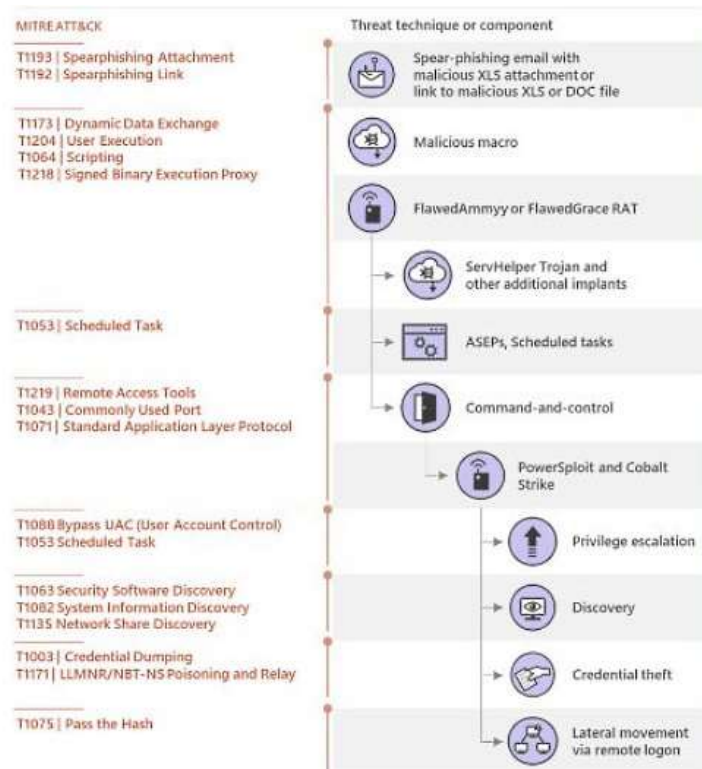


The victims are instructed to open the Excel document on their computer as online previewing is not available and to enable editing to get access to its contents.

"Once you have enabled editing, please click Enable Content from the yellow bar above," the bait Microsoft Office doc adds.

The operators behind this phishing campaign also use localized HTML files in different languages for victims from all around the world.

Also, the attackers make use of an IP traceback service that enables them to "track the IP addresses of machines that download the malicious Excel file."



Threat Analytics report (Microsoft)



Once executed on the victim's computer, the malware will also attempt to drop an info-stealing Trojan tracked by Microsoft as GraceWire.

Like most other info stealers, this will also start collecting sensitive information from the victim's device and send it to its masters via a command-and-control server.

Microsoft Security Intelligence provides a full list of indicators of compromise (IOCs) including SHA-256 hashes of the malware samples used in the campaign [here](#) and [here](#).

Source: <https://www.bleepingcomputer.com/news/security/microsoft-detects-new-ta505-malware-attacks-after-short-break/>



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

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.