

Special edition for MWC 2019

# we live security

## MAGAZINE

# RE BOOT



# ROUTER

## HOW TO, WHY, AND WHAT NOT TO DO

---

MACHINE-LEARNING ERA IN CYBERSECURITY:  
A STEP TOWARDS A SAFER WORLD OR THE BRINK OF CHAOS

---

THE TROJAN THAT RAIDS PAYPAL 2FA ACCOUNTS

---

LOJAX:  
FIRST IN-THE-WILD UEFI ROOTKIT FOUND BY ESET

---

# CONTENTS

**02**

The Trojan that raids  
PayPal 2FA accounts

**18**

Router reboot: How to, why, and  
what not to do

**06**

LoJax: First in-the-wild UEFI  
rootkit found by eset

**24**

GreyEnergy:  
A dangerous threat, updated

**12**

Fraudulent iOS apps promise  
fitness, but just steal money

**30**

Machine-learning era in cybersecurity:  
A step towards a safer world or the  
brink of chaos



*ESET researchers discovered a new Android Trojan using a novel Accessibility-abusing technique that targets the official PayPal app, and is capable of bypassing PayPal's two-factor authentication*

# THE TROJAN THAT RAIDS PAYPAL 2FA ACCOUNTS

You can find this article on:  
<https://www.welivesecurity.com/2018/12/11/android-trojan-steals-money-paypal-accounts-2fa/>

There is a new Trojan preying on Android users, and it has some nasty tricks up its sleeve. First detected by ESET in November 2018, the malware combines the capabilities of a remotely controlled banking Trojan with a novel misuse of Android Accessibility services to target users of the official PayPal app.

At the time of writing, the malware is masquerading as a battery optimization tool, and is distributed via third-party app stores.

## How does it operate?

After being launched, the malicious app terminates without offering any functionality and hides its icon. From then on, its functionality can be broken down into two main parts, as described in the following sections.

## Malicious Accessibility service targeting PayPal

The malware's first function, stealing money from its victims' PayPal accounts, requires the activation of a malicious Accessibility service. This request is presented to the user as being from the innocuous-sounding "Enable statistics" service.

If the official PayPal app is installed on the compromised device, the malware displays a notification alert prompting the user to launch it. Once the user opens the PayPal app and logs in, the malicious accessibility service (if previously enabled by the user) steps in and mimics the user's clicks to send money to the attacker's PayPal address.

Because the malware does not rely on stealing PayPal login credentials and instead waits for users to log into the official PayPal app themselves, it also bypasses PayPal's two-factor authentication (2FA). Users with 2FA enabled simply complete one extra step as part of logging in, – as they normally would – but end up being just as vulnerable to this Trojan's attack as those not using 2FA.

The malicious Accessibility service is activated every time the PayPal app is launched, meaning the attack could take place multiple times.

We have notified PayPal of the malicious technique used by this Trojan and the PayPal account used by the attacker to receive stolen funds.

## Banking Trojan relying on overlay attacks

The malware's second function utilizes phishing screens covertly displayed over targeted, legitimate apps.

By default, the malware downloads HTML-based overlay screens for five apps – Google Play, WhatsApp, Skype, Viber, and Gmail – but this initial list can be dynamically updated at any moment.

Four of the five overlay screens phish for credit card details (Figure 1); the one targeting Gmail is after Gmail login credentials (Figure 2). We suspect this is connected to the PayPal-targeting functionality, as PayPal sends email notifications for each completed transaction. With access to the victim's Gmail account, the attackers could delete such emails to remain unnoticed longer. (Figure 1 and Figure 2)

We've also seen overlay screens for legitimate banking apps requesting login credentials to victims' internet banking accounts (Figure 3).

Unlike overlays used by most Android banking Trojans, these are displayed in lock foreground screen – a technique also used by Android ransomware. This prevents the victims from removing the overlay by tapping the back button or the home button. The only way to get past this overlay screen is to fill out the bogus form, but fortunately, even random, invalid inputs make these screens disappear.

According to our analysis, the authors of this Trojan have been looking for further uses for this screen-overlaying mechanism. The malware's code contains strings claiming the victim's phone has been locked for displaying child pornography and can be unlocked by sending an email to a specified address. Such claims are reminiscent of early mobile ransomware attacks, where the victims were scared into believing their devices were locked due

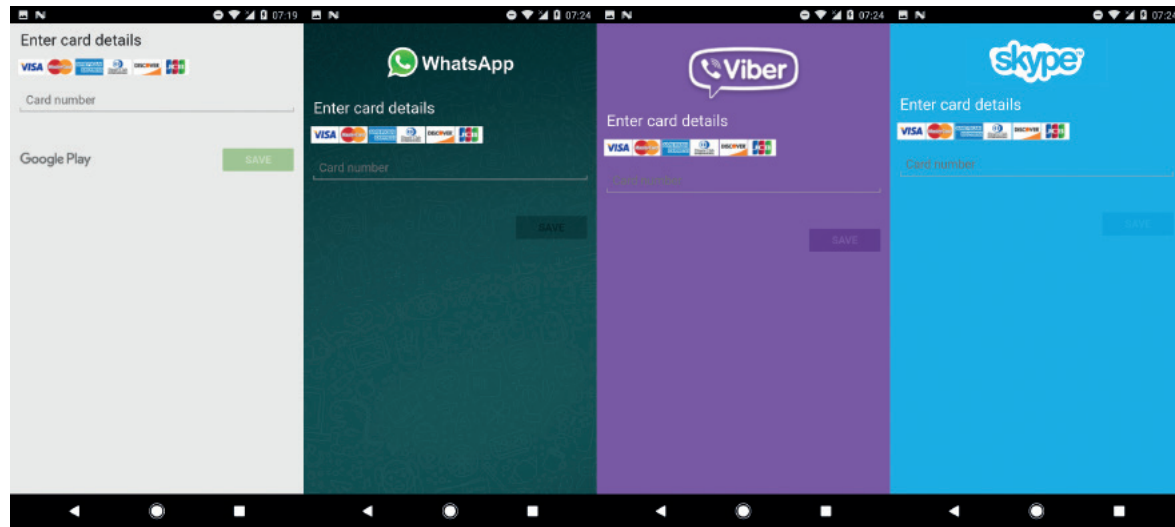


Figure 1 – Malicious overlay screens for Google Play, WhatsApp, Viber and Skype, requesting credit card details

to reputed police sanctions. It is unclear whether the attackers behind this Trojan are also planning to extort money from victims, or whether this functionality would merely be used as a cover for other malicious actions happening in the background.

Besides the two core functions described above, and depending on commands received from its C&C server, the malware can also:

- Intercept and send SMS messages; delete all SMS messages; change the default SMS app (to bypass SMS-based two-factor authentication)
- Obtain the contact list
- Make and forward calls
- Obtain the list of installed apps
- Install app, run installed app
- Start socket communication

### Accessibility Trojans also lurking on Google Play

We also spotted five malicious apps with similar capabilities in the Google Play store, targeting Brazilian users.

The apps, some of them also reported by Dr. Web and now removed from Google Play, posed as tools for tracking the location of other Android users. In reality, the apps use a malicious Accessibility service to navigate inside legitimate applications of several Brazilian banks. Besides that, the Trojans phish for sensitive information by overlaying a number of applications with phishing websites. The targeted applications are listed in the IoCs section of this blogpost

The attackers fail only if the user has insufficient PayPal balance and no payment card connected to the account.

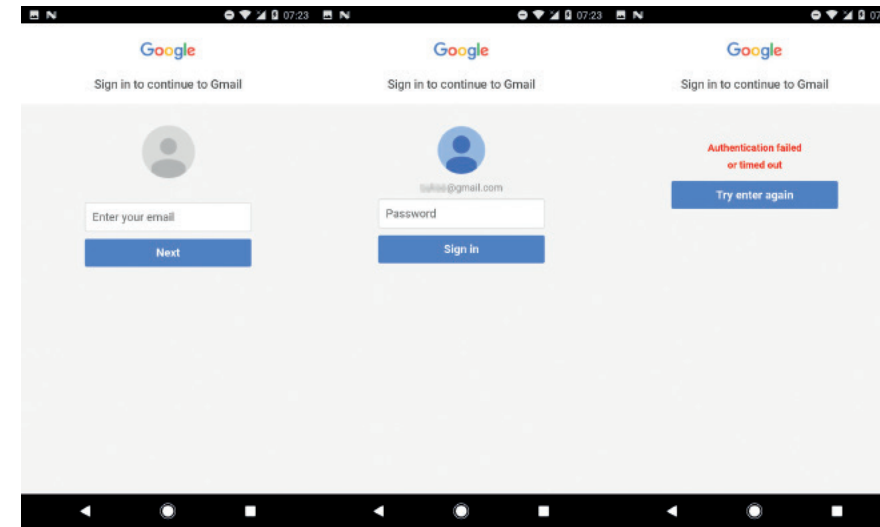


Figure 2 – Malicious overlay screens phishing for Gmail credentials

Interestingly, these Trojans also use Accessibility to thwart uninstallation attempts by repeatedly clicking the “Back” button whenever a targeted antivirus app or app manager is launched, or when strings suggesting uninstallation are detected in the foreground.

### How to stay safe

Those who have installed these malicious apps will have likely already fallen victim to one of their malicious functions.

If you have installed the PayPal-targeting Trojan, we advise you to check your bank account for suspicious transactions and consider changing your internet banking password/PIN code, as well as Gmail password. In case of unauthorized PayPal transactions, you can report a problem via PayPal’s Resolution Center.

For devices that are unusable due to a lock screen overlay displayed by this Trojan, we recommend using Android’s Safe Mode, and proceed with uninstalling an app named “Optimization Android” under Settings > (General) > Application manager/Apps.

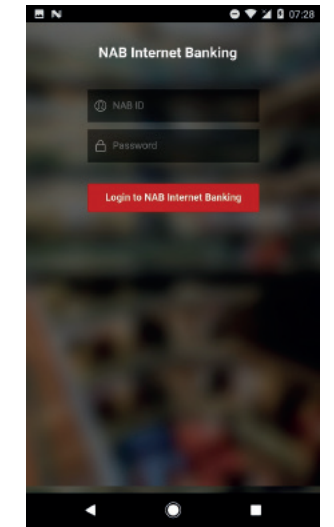


Figure 3 – Malicious overlay screen for the National Australia Bank Mobile Banking app

Uninstalling in Safe Mode is also recommended for Brazilian users who installed one of the Trojans from Google Play.

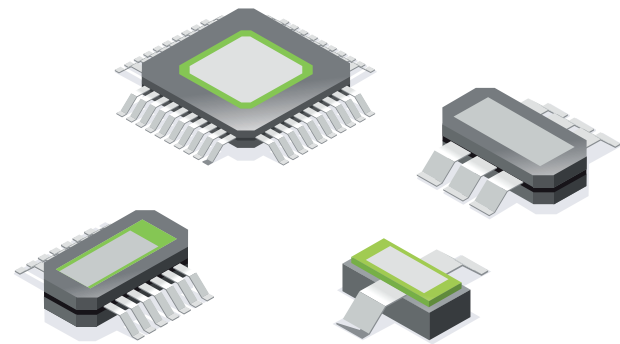
To stay safe from Android malware in the future, we advise you to:

- Stick to the official Google Play store when downloading apps
- Make sure to check the number of downloads, app ratings and the content of reviews before downloading apps from Google Play
- Pay attention to what permissions you grant to the apps you install
- Keep your Android device updated and use a reliable mobile security solution; ESET products detect these threats as Android/Spy.Banker.AJZ and Android/Spy.Banker.AKB



Author  
Lukas Stefanko





# LoJax: FIRST IN-THE-WILD UEFI ROOTKIT FOUND BY ESET

You can find this article on:  
<https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/>

*How the ESET research team uncovered the first ever malware observed to successfully infect the UEFI's firmware component, and was able to attribute the malware with high confidence to the Sednit group.*

UEFI rootkits are widely viewed as extremely dangerous tools for implementing cyberattacks, as they are hard to detect and able to survive security measures such as operating system reinstallation and even a hard disk replacement. Some UEFI rootkits have been presented as proofs of concept; some are known to be at the disposal of (at least some) governmental agencies. However, no UEFI rootkit has ever been detected in the wild – until we discovered a campaign by the Sednit APT group that successfully deployed a malicious UEFI module on a victim's system.

The discovery of the first in-the-wild UEFI rootkit is notable for two reasons. First, it shows that UEFI rootkits are a real threat, and not merely an

attractive conference topic. And second, it serves as a heads-up, especially to all those who might be in the crosshairs of Sednit. This APT group, also known as APT28, STRONTIUM, Sofacy and Fancy Bear, may be even more dangerous than previously thought.

Our analysis of the Sednit campaign that uses the UEFI rootkit was presented September 27 at the 2018 Microsoft BlueHat conference and is described in detail in our "LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group" white paper. In this blog post, we summarize our main findings.

The Sednit group has been operating since at least 2004, and has made headlines frequently in past

years: it is believed to be behind major, high profile attacks. For instance, the US Department of Justice named the group as being responsible for the Democratic National Committee (DNC) hack just before the US 2016 elections. The group is also presumed to be behind the hacking of global television network TV5Monde, the World Anti-Doping Agency (WADA) email leak, and many others. This group has a diversified set of malware tools in its arsenal, several examples of which we have documented previously in our Sednit white paper from 2016.

Our investigation has determined that this malicious actor was successful at least once in writing a malicious UEFI module into a system's SPI flash memory. This module is able to drop and execute malware on disk during the boot process. This persistence method is particularly invasive as it will not only survive an OS reinstall, but also a hard disk replacement. Moreover, cleaning a system's UEFI firmware means re-flashing it, an operation not commonly done and certainly not by the typical computer owner.

## LoJack becomes LoJax

In May 2018, an Arbor Networks blog post described several trojanized samples of Absolute Software's LoJack small agent, rpcnetp.exe. These malicious samples communicated with a malicious C&C server instead of the legitimate Absolute Software server, because their hardcoded configuration settings had been altered. Some of the domains found in LoJax samples have been seen before: they were used in late 2017 as C&C domains for the notorious Sednit first-stage backdoor, SedUploader. Because of this campaign's malicious usage of the LoJack small agent, we call this malware LoJax.

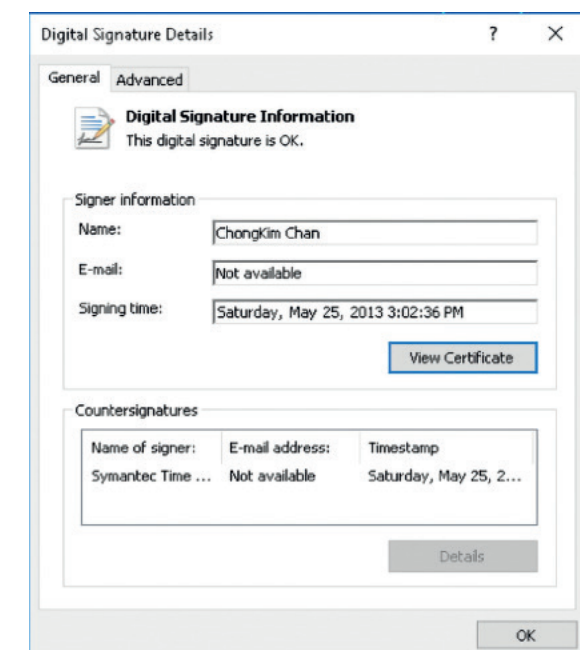
LoJack is anti-theft software. Earlier versions of this agent were known as Computrace. As its former name implies, once the service was activated, the computer would call back to its C&C server and its owner would be notified of its location if it had gone missing or been stolen. Computrace attracted attention from the security community, mostly because of its unusual persistence method. Since this software's intent is to protect a system from theft,

it is important that it resists OS re-installation or hard drive replacement. Thus, it is implemented as a UEFI/BIOS module, able to survive such events. This solution comes pre-installed in the firmware of a large number of laptops manufactured by various OEMs, waiting to be activated by their owners.

While researching LoJax, we found several interesting artifacts that led us to believe that these threat actors might have tried to mimic Computrace's persistence method.

## Patching SPI flash memory with malware

On systems that were targeted by the LoJax campaign, we found various tools that are able to access and patch UEFI/BIOS settings. All used a kernel driver, RwDrv.sys, to access the UEFI/BIOS settings. This kernel driver is bundled with RWEv-everything, a free utility available on the web that can be used to read information on almost all of a computer's low-level settings, including PCI Express, Memory, PCI Option ROMs, etc. As this kernel driver belongs to legitimate software, it is signed with a valid code-signing certificate.



Our research has shown that the Sednit operators used different components of the LoJax malware to target a few government organizations in the Balkans as well as in Central and Eastern Europe.

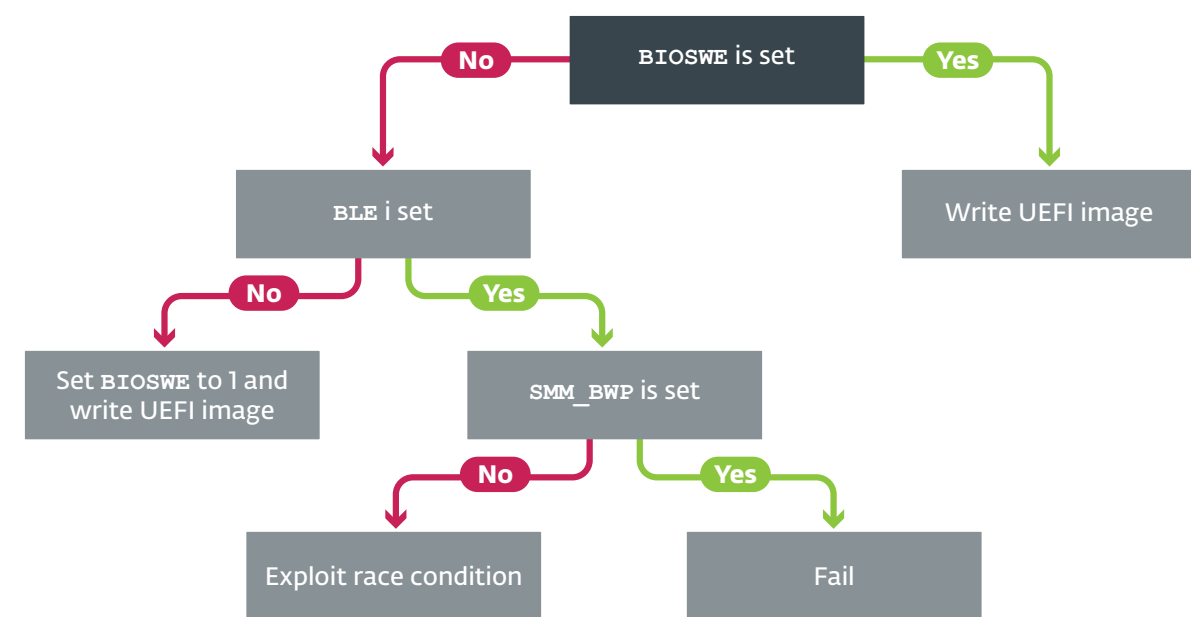
Three different types of tool were found alongside LoJax userland agents. The first one is a tool dumping information about low level system settings to a text file. Since bypassing a platform's protection against illegitimate firmware updates is highly platform-dependent, gathering information about a system's platform is crucial. The purpose of the second tool is to save an image of the system firmware to a file by reading the contents of the SPI flash memory where the UEFI/BIOS is located. The third tool's purpose is to add a malicious UEFI module to the firmware image and write it back to the SPI flash memory, effectively installing the UEFI rootkit on the system. This patching tool uses different techniques either to abuse misconfigured platforms or to bypass platform SPI flash memory write protections. As illustrated in the next figure, if the platform allows write operations to the SPI flash memory, it will just go ahead and write to it. If not, it actually implements an exploit against a known vulnerability.

The UEFI rootkit added to the firmware image has a single role: dropping the userland malware onto the Windows operating system partition and make sure that it is executed at startup.

### How to protect yourself?

While Secure Boot is the first mechanism that comes to mind when we think about preventing UEFI firmware attacks, it wouldn't have protected against the attack we describe in this research. Despite this, we strongly suggest you enable Secure Boot on your systems, through the UEFI setup utility. Secure Boot is designed to protect against malicious components coming from outside of the SPI flash memory. To protect against tampering with the SPI flash memory, the system's root of trust must be moved to hardware. Such technologies exist and Intel Boot Guard is a good example of this. It has been available starting with the Haswell family of Intel processors introduced in 2013. Had this technology been available and properly configured on the victim's system, the machine would have refused to boot after the compromise.

Updating system firmware should not be something trivial for a malicious actor to achieve. There are different protections provided by the platform to prevent unauthorized writes to system SPI flash memory. The tool described above is able to update the system's firmware only if the SPI flash memory protections are vulnerable or misconfigured. Thus,





For more information about how to protect yourself you can visit our website and find out more about the ESET UEFI Scanner.

you should make sure that you are using the latest UEFI/BIOS available for your motherboard. Also, as the exploited vulnerability affects only older chipsets, make sure that critical systems have modern chipsets with the Platform Controller Hub (introduced with Intel Series 5 chipsets in 2008).

Unfortunately for the ambitious end user, updating a system's firmware is not a trivial task. Thus, firmware security is mostly in the hands of UEFI/BIOS vendors. The security mechanisms provided by the platform need to be configured properly by the system firmware in order to actually protect it. Firmware must be built from the ground up with security in mind. Fortunately, more and more security researchers are looking at firmware security, thus contributing to improving this area and raising awareness among UEFI/BIOS vendors.

Remediation of a UEFI firmware-based compromise is a hard problem. There are no easy ways to automatically remove such a threat from a system. In the case we described above: in order to remove the rootkit, the SPI flash memory needs to be re-flashed with a clean firmware image specific to the motherboard. This is a delicate operation that must be performed manually. It is definitely not a procedure that most computer owners are familiar with. The only alternative to reflashing the UEFI/BIOS is to replace the motherboard of the compromised system outright.

### The links with the Sednit APT group

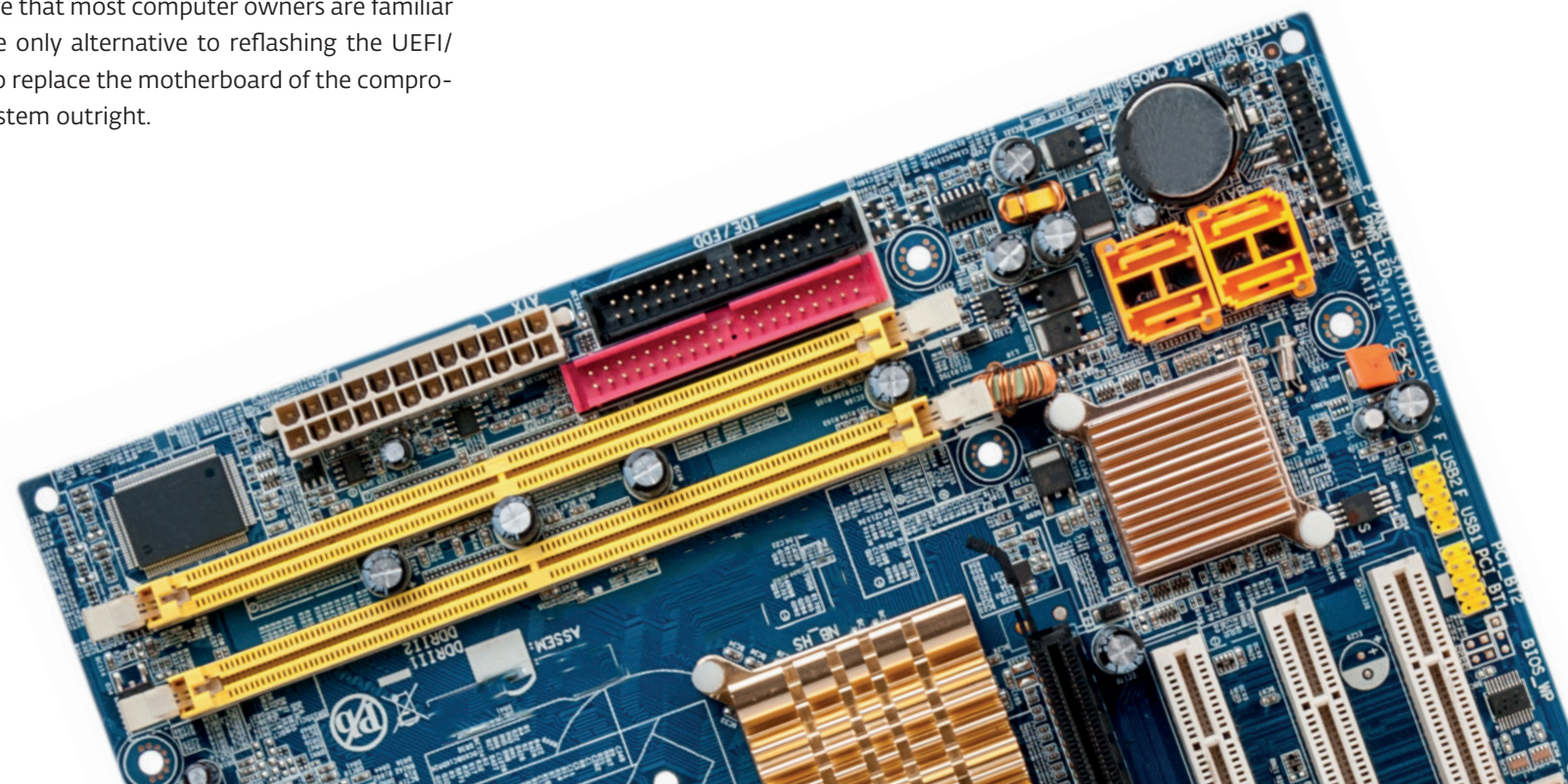
As mentioned above, some of the LoJax small agent C&C servers were used in the past by SedUploader, a first-stage backdoor routinely used by Sednit's operators. Also, in cases of LoJax compromise, traces of other Sednit tools were never far away. In fact, systems targeted by LoJax usually also showed signs of the three examples of Sednit malware below which allow us to attribute LoJax with high confidence to the Sednit group:

- SedUploader, a first-stage backdoor
- XAgent, Sednit's flagship backdoor
- Xtunnel, a network proxy tool that can relay any kind of network traffic between a C&C server on the Internet and an endpoint computer inside a local network

### In conclusion

Through the years we've spent tracking of the Sednit group, we have released many reports on its activities, ranging from zero-day usage to custom malware it has developed, such as Zebrocy. However, the UEFI rootkit component described above is in a league of its own.

The LoJax campaign shows that high-value targets are prime candidates for the deployment of rare, even unique threats and such targets should always be on the lookout for signs of compromise. Also, one thing that this research taught us is that it is always important to dig as deep as you can go! For a detailed analysis of the backdoor, head over to our white paper LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group.



Author  
ESET Research Team



# FRAUDULENT IOS APPS PROMISE FITNESS, BUT JUST STEAL MONEY

You can find this article on:  
<https://www.welivesecurity.com/2018/12/03/scam-ios-apps-promise-fitness-steal-money-instead/>





## Fitness-tracking apps use dodgy in-app payments to steal money from unaware iPhone and iPad users

Multiple apps posing as fitness-tracking tools were caught misusing Apple's Touch ID feature to steal money from iOS users. The dodgy payment mechanism used by the apps is activated while victims are scanning their fingerprint, seemingly for fitness-tracking purposes.

There are many apps that promise to assist users on the way to a healthier lifestyle. The bogus apps were, until recently, available in the Apple App Store. The apps were called "Fitness Balance app" and "Calories Tracker app", and at first glance appeared to put users on the road to fitness – they could calculate the BMI, track daily calorie intake, or remind users to drink more water. These services, however, came with an unexpectedly hefty price tag, according to Reddit users.

After a user fires up any of the abovementioned apps for the first time, the apps request a fingerprint scan to "view their personalized calorie tracker and diet recommendations" (Figure 1). Only moments after the user complies with the request and places a finger on the fingerprint scanner, the apps then display a pop-up showing a dodgy payment amounting to 99.99, 119.99 USD or 139.99 EUR.

This pop-up is only visible for about a second, however, if the user has a credit or debit card directly connected to an Apple account, the transaction is considered verified and money is wired to the operator behind these scams.

Based on the user interface and functionality, both apps are most likely created by the same developer. Users have also posted videos of "Fitness Balance app" and "Calories Tracker app" on Reddit.

If users refuse to scan their finger in "Fitness Balance app", another pop-up is displayed, prompting to tap a "Continue" button to be able to use the app. If they comply, the app tries to repeat the dodgy payment procedure.

Despite its malicious nature, the "Fitness Balance app" received multiple 5-star ratings, had an average rating of 4.3 stars and received at least 18 mostly positive user reviews. Posting fake reviews is a well-known technique used by scammers to improve the reputation of their apps.

Victims already reported both of these apps to Apple, which led to their removal from the market. Users even have tried to contact the developer of "Fitness Balance app" directly, but only received a generic response promising to fix the reported "issues" in the upcoming version 1.1 (Figure 3).

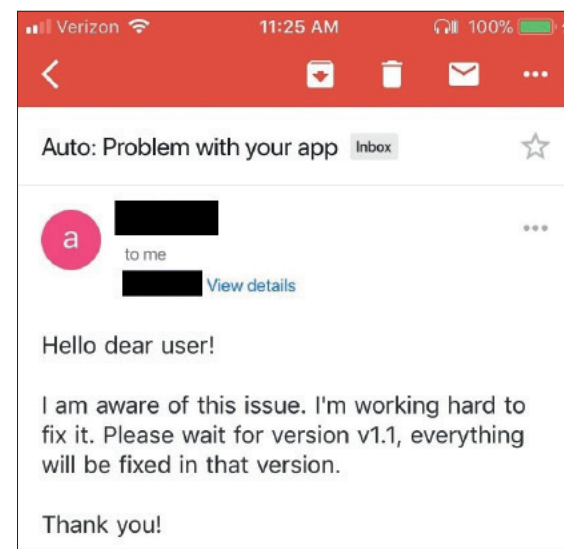


Figure 3 – Users who directly contacted the developer received what seems to be an automatic reply

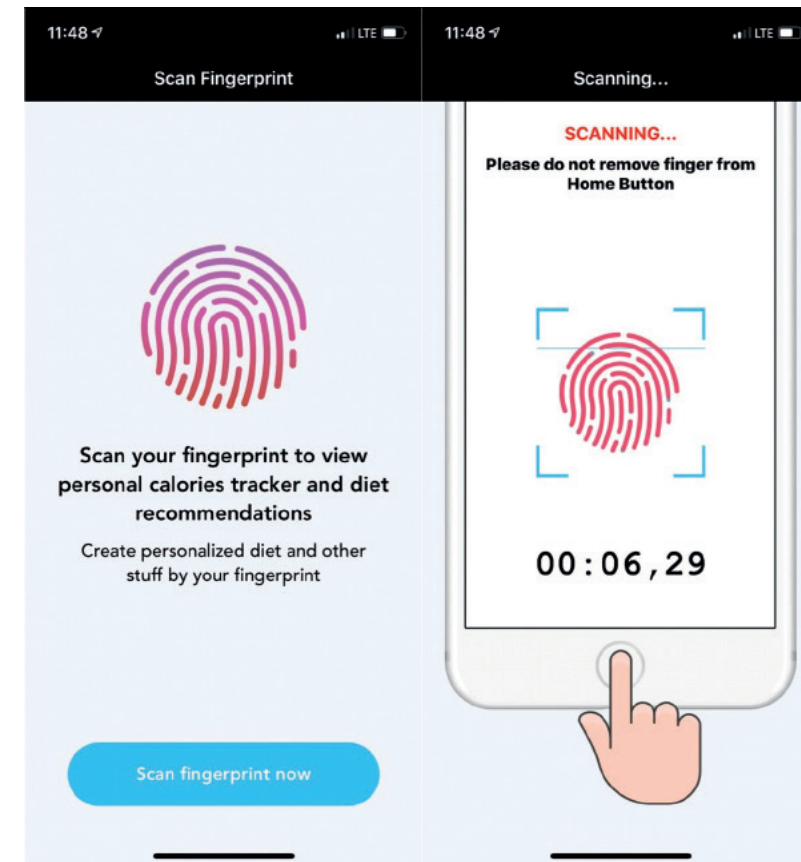


Figure 1 – Scam apps in Apple's App Store require users to scan their fingers for fitness tracking (Image source: Reddit)

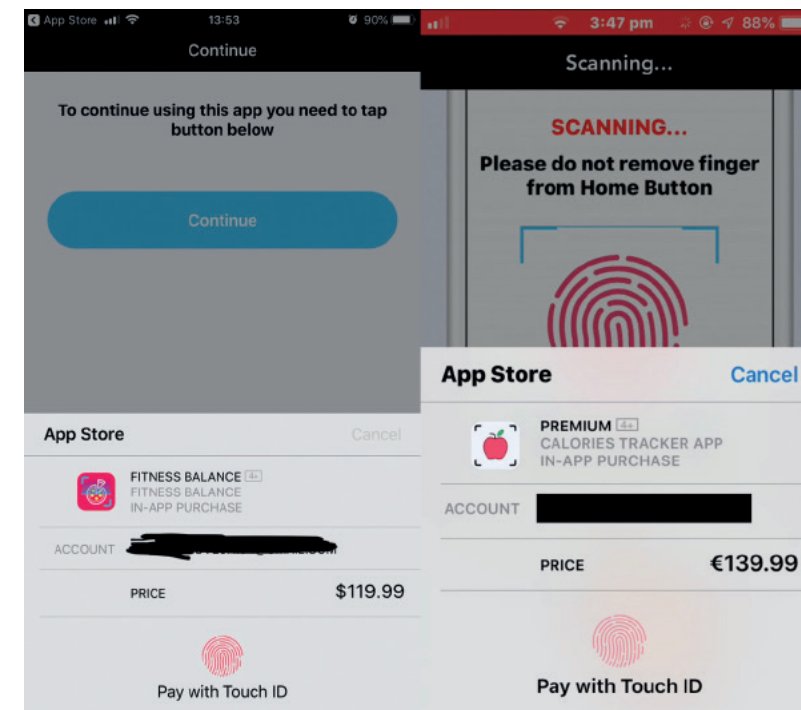


Figure 2 – Dodgy payment popping up in "Fitness Balance app" and "Calories Tracker app" (Image source: Reddit)



Despite its malicious nature, the “Fitness Balance app” received multiple 5-star ratings, had an average rating of 4.3 stars and received at least 18 mostly positive user reviews.

### What can users do to avoid similar threats?

As Apple doesn't allow security products in its App Store, users need to rely on the security measures implemented by Apple.

On top of that, ESET advises users to always read reviews by other users. As positive feedback is easily faked, negative reviews are more likely to reveal the true nature of the app.

iPhone X users are protected from these scams, as this model doesn't have the TouchID feature and instead uses “Double Click to Pay”, which requires the user to double-click the side button (Figure 4) to verify a payment.

Those who already fell victim to this scam can also try to claim a refund from the Apple App Store.

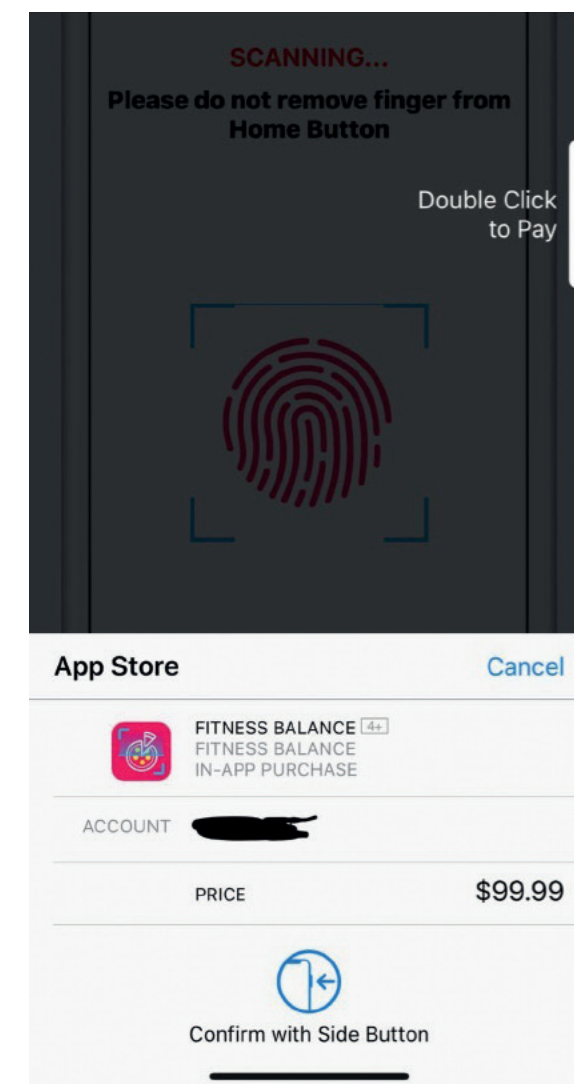


Figure 4



Author  
Lukas Stefanko





## Router reboot: **HOW TO, WHY, AND WHAT NOT TO DO**

You can find this article on:  
<https://www.welivesecurity.com/2018/06/04/router-reboot-how-why-what/>

*The FBI say yes but should you follow this advice? And if you do follow it, do you know how to do so safely?*

Reboot your router! That is the advice put out on May 25, 2018, by one of the world's most widely known law enforcement agencies: the US Federal Bureau of Investigation (FBI). But should you follow this advice? This article provides some answers, both long and short.

### Here are eight short answers.

#### 1. What's going on?

As many as 500,000 routers in more than 50 countries were found to be compromised by malware dubbed VPNFilter.

#### 2. What should I do?

Rebooting your router – turn it off, wait 30 seconds, turn it on again – will help to defeat this particular malware.

#### 3. Who is affected?

This threat mainly affects small office and home office (SOHO) routers. A list of models known to be impacted is located at the end of the article.

#### 4. What if my router is not on the list?

It may still be at risk from VPNFilter, so current advice is for all SOHO routers to be rebooted.

#### 5. Is a reboot the same as a reset?

NO! A reset wipes out configuration information and returns the router to factory defaults. Do not reset your router unless you know how to configure it and have a record of the configuration information, e.g. admin password, SSID, and so on (see rest of the article for more details).

#### 6. What if my router is supplied by my ISP?

You should contact them for instructions if they have not already alerted you and provided instructions.

#### 7. What other defensive measures can I take?

Consider upgrading your router to the latest firmware, changing the default password, and disabling remote administration. At the end of the article is a table of links to instructions for doing this work on known at-risk routers, along with links on how to reset them to their factory defaults.

#### 8. Does ESET detect this malware?

Yes, it is detected as Linux/VPNFilter. However, ESET recommends that you go ahead and reboot your router – read on for more details.

### What did the FBI say about routers?

On May 25, the FBI issued a statement with this headline: "Foreign cyber actors target home and office routers and networked devices worldwide". This was in response to the discovery that "cyber actors" had used malicious code (malware) to compromise a whole bunch of routers and other equipment, like NAS devices.

In this context, the term "compromise" means these "cyber actors" executed their code on people's devices without their permission. This malware, which has the ability to collect information



flowing through the device but can also render the device inoperable, has been dubbed VPNFilter by the researchers in the Talos threat intelligence group at Cisco.

Fortunately, the part of VPNFilter that could be used to spy on your router traffic, and/or disable the device, can be removed with that classic IT move: turn it off and on again. So the FBI issued this recommendation:

As you may know, booting is the technical term for powering on a computing device, thereby activating basic code that is stored on chips in the device. The very first code to run is that stored in what we call “firmware”, meaning it is considered part of the hardware. Think of the code in firmware as hard to change (in some cases it is practically impossible).

The next code that runs in the boot process is that which has been stored in something called non-volatile memory, a type of memory that retains data even when the device is powered down. That is different from volatile memory, the regular kind of memory that gets wiped clean when you power down your computer (or suffer a power outage).

Remember, your router is a computer, with firmware and memory, both volatile and non-volatile. When a router is compromised by VPNFilter malware, chunks of malicious code are loaded into volatile memory. Rebooting or power cycling your router will clear that out, and that is what the FBI would like you to do.

For some people the easiest way to reboot the router is to unplug the power supply, wait 30 seconds, then plug it back in again. Alternatively, there may be an on/off switch on the back of the router, in which case you can use that to turn it off, wait 30 seconds, and then turn it on again. However, you shouldn't do that unless you are sure the switch you are using is the on/off switch.

## Reboot vs. reset

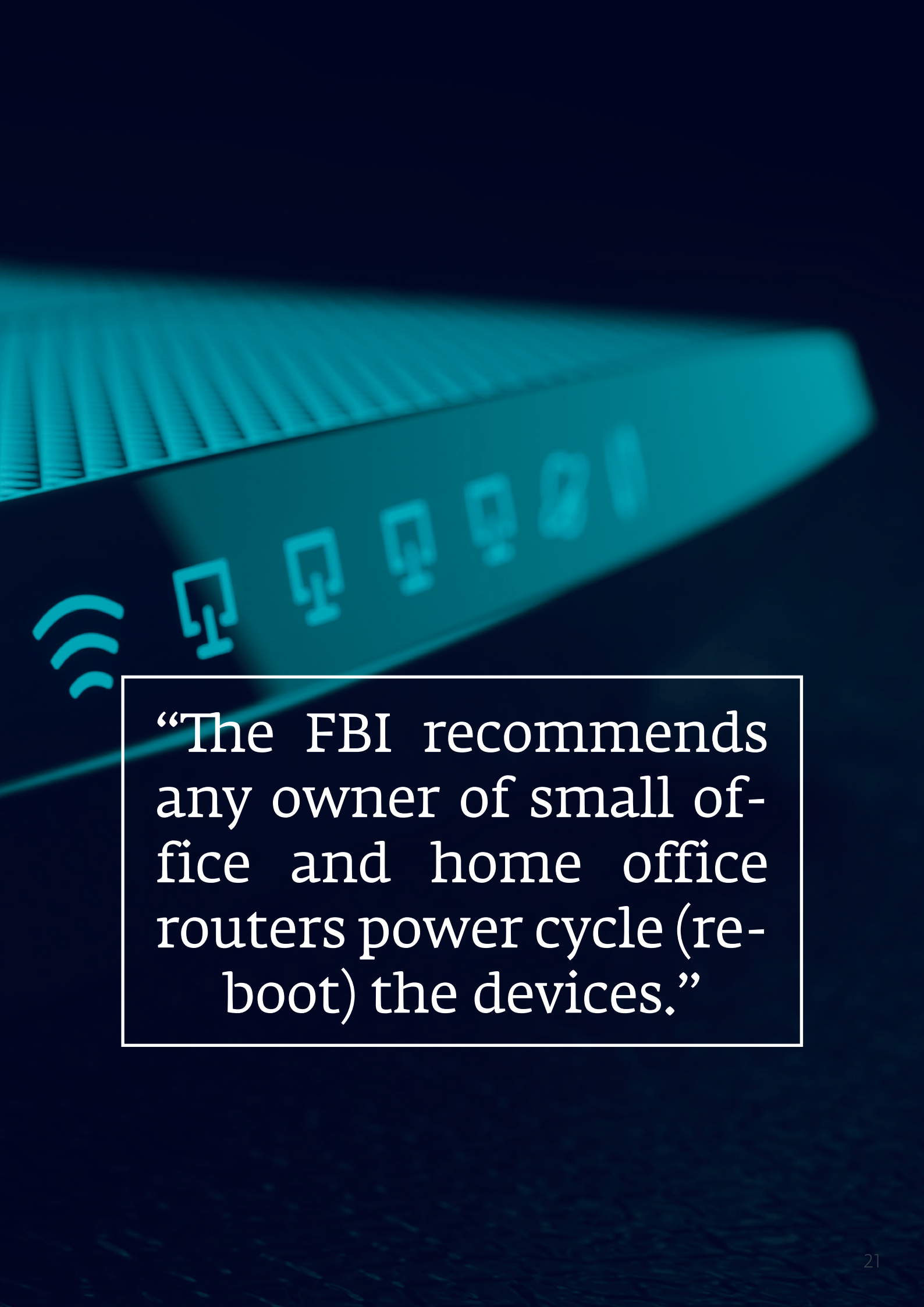
How could you be confused about the on/off switch? Some routers have multiple switches on them; for example, the router on my desk right now has a “Wi-Fi” on/off button as well as a power switch and something called a WPS button. Also, your router may have a reset switch or “Restore Factory Settings” button. Resetting your router and thereby restoring it to the factory configuration is very different from rebooting it.

Performing a reset will erase both volatile memory and non-volatile memory. The latter is where your router stores any changes you have made to its configuration. For example, most routers come with a default administrator name and password that you should change to prevent attackers taking it over. How could they do that? Because the default user names and passwords are widely known. They are often printed on the back of the router and may be discoverable via a Google search based on your model number.

When your router is compromised by VPNFilter malware, part of the code is written into non-volatile memory, so it does not go away when you simply reboot. That remaining code enables the device to reach out to a web domain after a reboot and download fresh malware into memory ... except the FBI now controls that domain. So, even if you have not removed VPNFilter code from non-volatile memory, it is currently prevented from downloading fresh malware.

## How do you perform a router reset?

Taking control of a malware domain is called “sink-holing” and this was clever work by the FBI. However, you may decide that you want to reset your router anyway. This should remove the last of the VPNFilter code from the device.



“The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices.”



**What follows is a generic guide that you use at your own risk.**

For many routers the reset operation is more than flipping a switch, it involves the classic “paper clip poker” and a small hole on the device. This may be referred to in the manufacturer’s documentation as “Restore Factory Settings” or something similar. It is often printed on the back of the device, along with the default values, like this:

To proceed with the reset, first make sure:

1. You know the default user name and password for the device because you will need these to access the device after the reset.
2. You have recorded any adjustments you made to the factory settings, like changing the router password, as well as the wireless SSID name and password.
3. The router is powered on.
4. You have warned everyone who is using the network to save their work.
5. The router is disconnected from the internet (if the reset reverts the router password to a known default and the router is on the internet it instantly becomes a soft target).

Now grab your poking implement – a straightened paperclip, or something similar, like the pin you got with your smartphone or tablet to pop the microSD card or SIM-tray – and follow these three steps to perform the reset:

1. Gently insert poker into the reset hole where you can feel it depress a button.
2. Hold the button down for 10 seconds
3. Release.

This will cause the lights on the router to flash a lot, but after a minute or so they will settle down. However, before reconnecting the router to the internet you should log into the router to change the router admin password from the default and make other changes, like setting the wireless SSID name and password.

The VPNFilter malware poses a serious threat to the security and availability of small office and home office networks.

**Summary**

Summing up: the VPNFilter malware poses a serious threat to the security and availability of small office and home office networks. Even if you are not using one of the routers in the list below, you need to take action. The following is the minimum response:

- If your router is supplied by your ISP, turn it off and then back on again, then check for further advice from your ISP.
- If you own/maintain a router, reboot it, change the default password, and check if any firmware updates are available from the router manufacturer; if so, install them.

If you are someone who knows their way around network hardware you may also want to do the following:

- Disconnect your router from the internet and perform a router reset.
- Re-install the most recent firmware.

For ongoing protection – and hopefully, it goes without saying these days – you need to run reputable security software on all your networked devices like laptops, PCs, Macs, Android tablets, smartphones, and yes, even your smart TV.

In addition, everyone should stay tuned for further news about VPNFilter and other malicious code that targets network connected devices.

**List of router models known to be at risk (but there could be more)**

<b>Linksys</b>	E1200 E2500 WRVS4400N
<b>Mikrotik Routers Versions for Cloud Core Routers</b>	1016 1036 1072
<b>Netgear</b>	DGN2200 R6400 R7000 R8000 WNR1000 WNR2000
<b>QNAP</b>	TS251 TS439 Pro other QNAP NAS devices running QTS software
<b>TP-LINK</b>	R600VPN



Author  
Stephen Cobb



## GreyEnergy: **A DANGEROUS THREAT, UPDATED**

You can find this article on:  
<https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/>

*ESET research reveals a successor to the infamous BlackEnergy APT group targeting critical infrastructure, quite possibly in preparation for damaging attacks*

Recent ESET research has uncovered details of the successor of the BlackEnergy APT group, whose main toolset was last seen in December 2015 during the first-ever blackout caused by a cyberattack. Around the time of that breakthrough incident, when around 230,000 people were left without electricity, we started detecting another malware framework and named it GreyEnergy. It has since been used to attack energy companies and other high-value targets in Ukraine and Poland for the past three years.

It is important to note that when we describe 'APT groups', we're making connections based on technical indicators such as code similarities, shared C&C infrastructure, malware execution chains,

and so on. We're typically not directly involved in the investigation and identification of the individuals writing the malware and/or deploying it, and the interpersonal relations between them. Furthermore, the term 'APT group' is very loosely defined, and often used merely to cluster the abovementioned malware indicators. This is also one of the reasons why we refrain from speculation with regard to attributing attacks to nation states and such.

We have already extensively documented the threat actors' transition towards TeleBots in cyberattacks on high-value targets in the Ukrainian financial sector, the supply-chain attacks against Ukraine and in an analysis of TeleBot's cunning



backdoor. All from the group most notable for the NotPetya ransomware outbreak. At the same time, we have also been keeping a close eye on GreyEnergy – a subgroup operating in parallel, but with somewhat different motivations and targeting.

Although ESET telemetry data shows GreyEnergy malware activity over the last three years, this APT group has not been documented until now. This is probably due to the fact that those activities haven't been destructive in nature, unlike the numerous TeleBots ransomware campaigns (not only NotPetya), the BlackEnergy-enabled power grid attack, and the Industroyer-caused blackout – which we recently linked to these groups for the first time. The threat actors behind GreyEnergy have tried to stay under the radar, focusing on espionage and reconnaissance, quite possibly in preparation of future cybersabotage attacks or laying the groundwork for an operation run by some other APT group.

GreyEnergy's malware framework bears many similarities to BlackEnergy, as outlined below. It is similarly modular in construction, so its functionality is dependent on the particular combination of modules its operator uploads to each of the targeted victim's systems. The modules that we have observed were used for espionage and reconnaissance purposes (i.e. backdoor, file extraction, taking screenshots, keylogging, password and credential stealing, etc.). We have not observed any modules that specifically target Industrial Control Systems (ICS). We have, however, observed that the GreyEnergy operators have been strategically targeting ICS control workstations running SCADA software and servers, which tend to be mission-critical systems never meant to go offline except for periodic maintenance.

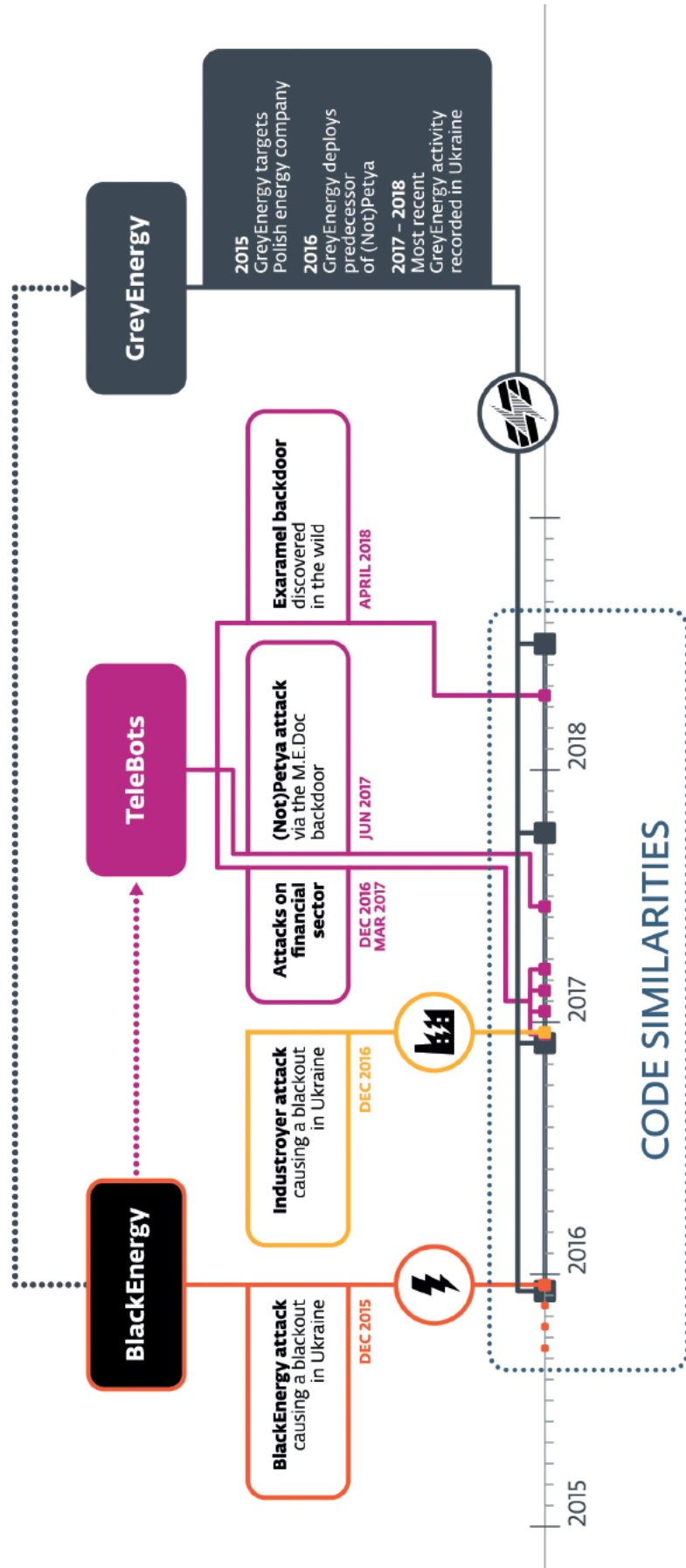
### Links to BlackEnergy and TeleBots

Some of the reasons ESET researchers consider BlackEnergy and GreyEnergy related are listed below:

- The appearance of GreyEnergy in the wild coincides with the disappearance of BlackEnergy.
- At least one of the victims targeted by GreyEnergy had been targeted by BlackEnergy in the past. Both subgroups share an interest in the energy sector and critical infrastructure. Both have had victims primarily in Ukraine, with Poland ranking second.
- There are strong architectural similarities between the malware frameworks. Both are modular, and both employ a "mini", or light, backdoor deployed before admin rights are obtained and the full version is deployed.
- All remote C&C servers used by the GreyEnergy malware were active Tor relays. This has also been the case with BlackEnergy and Industroyer. We hypothesize that this is an operational security technique used by the group so that the operators can connect to these servers in a covert manner.

Compared to BlackEnergy, GreyEnergy is a more modern toolkit with an even greater focus on stealth. One basic stealth technique – employed by both families – is to push only selected modules to selected targets, and only when needed. On top of that, some GreyEnergy modules are partially encrypted using AES-256 and some remain fileless – running only in memory – with the intention of hindering analysis and detection. To cover their tracks, typically, GreyEnergy's operators securely wipe the malware components from the victims' hard drives.

The threat actors behind GreyEnergy have tried to stay under the radar, focusing on espionage and reconnaissance, quite possibly in preparation of future cybersabotage attacks or laying the groundwork for an operation run by some other APT group.



In addition to the outlined similarities with BlackEnergy, we have observed another link between GreyEnergy and the TeleBots subgroup.

In December 2016, we noticed an instance of GreyEnergy deploying an early version of the TeleBots' NotPetya worm – half a year before it was altered, improved, and deployed in the most damaging ransomware outbreak in history.

There is significant code reuse between this ransomware component and the GreyEnergy core module. We call this early version "Moonraker Petya", based on the malware writers' choice of filename – most likely a reference to the James Bond movie. It didn't feature the infamous EternalBlue spreading mechanism, as it had not been leaked at that time.

### GreyEnergy Tactics, Techniques and Procedures

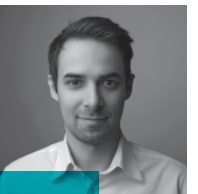
We have observed two distinct infection vectors: "traditional" spearphishing, and the compromise of public-facing web servers. When such a vulnerable web server was hosted internally and connected to the rest of a targeted organization's network, the attacker would attempt to move laterally to other workstations. This technique is used not only as a primary infection vector but also as a backup reinfection vector.

The attackers typically deploy internal C&C proxies within the victims' networks. Such proxy C&Cs redirect requests from infected nodes inside the network to an external C&C server on the internet. This is another stealth tactic, as it is less suspicious to a defender to see that multiple computers are "talking" to an internal server, rather than a remote one.

A very curious observation – one that is also indicative of the group's targeting – is that some of the GreyEnergy samples we detected were signed with a certificate from Advantech, a Taiwanese manufacturer of industrial and IoT hardware. These were most likely stolen from the company, just as in the case of Stuxnet and a recent Plead malware campaign.

The GreyEnergy operators also employ common external tools in their arsenal, such as Mimikatz, PsExec, WinExe, Nmap, and a custom port scanner.

For a detailed analysis of the GreyEnergy toolset and operations refer to our white paper GreyEnergy: A successor to BlackEnergy. A full list of Indicators of Compromise (IoCs) and samples can be found on Github. For any inquiries, or to make sample submissions related to the subject, please contact us at: [threatintel@eset.com](mailto:threatintel@eset.com). For more information about how to protect yourself you can visit [www.eset.com](http://www.eset.com) and find out more about GreyEnergy.



Authors  
Anton Cherepanov  
Robert Lipovsky



# Machine-learning era in cybersecurity: A STEP TOWARDS A SAFER WORLD OR THE BRINK OF CHAOS

While artificial intelligence (AI) and machine learning (ML) have been transforming various fields of human activity for some time now, their full transformative potential is yet to be realized. AI-based technologies will increasingly help fight fraud, evaluate and optimize business processes, improve testing procedures and develop new solutions to existing problems. However, like most disruptive innovations, even AI and machine learning will have their drawbacks.

With business, critical infrastructure, as well as our personal lives becoming ever more entwined with the digital realm, new risks will emerge. Attackers can employ AI in multiple ways: to power their malware, to target specific victims and extract valuable data, to hunt for zero-day vulnerabilities or protect hijacked infrastructure such as botnets.

Machine-learning solutions deployed by legitimate organizations can become another attractive target. By creating poisoned data sets, attackers can try to manipulate otherwise beneficial systems to make incorrect decisions or to provide a distorted view of the monitored environment, potentially causing chaos.

## Misusing ML for translations and targeting

The first signs that these scenarios are crossing from theory to reality are already appearing on the radar. One good example are spammers, who have been (mis)using legitimate ML-based translation services to improve their messaging in a wide array of local languages (of course, unless the attackers are sending spam by day, and learning those new languages by night).

Another in-the-wild example that shows AI-like signs is the currently prevalent downloader Emotet, suspected of using this type of technology to improve its targeting. Despite infecting thousands of victims daily, it has become surprisingly effective in avoiding honeypots and botnet trackers.

To achieve this, Emotet collects telemetry of its potential victims and sends it to the attacker's C&C server for analysis. Based on these inputs, the malware not only picks the modules included in the payload, but also distinguishes human operators from virtual machines used by researchers.

Similar self-defense mechanisms would be very complex and expensive and Emotet's operators would have to invest extraordinary resources to achieve the malware's current abilities without utilizing machine learning.

## Not enough layers, not enough security

Tampering with the ML model by feeding it poisoned inputs – aka adversarial machine learning – is another risk that will become more pressing in the future, especially in the cybersecurity field. If less-advanced, purely ML-based scanning engines were fooled into incorrect decisions by attackers, it could diminish the security of the victim company and potentially cause serious damage.

ESET has over 30 years' experience specializing in cybersecurity and more than 20 years of focus on machine learning implementations. This makes our experts more than able to build a robust, resilient and cutting-edge machine learning engine.

Integration of this ML engine into our cloud reputation system, ESET LiveGrid®, has made the benefits of this technology available to all our customers, including regular users as well as companies of all sizes. Enterprises might also consider ESET Dynamic Threat Defense, providing another layer of security by utilizing a cloud-based sandboxing technology to detect new, never before seen threats.

However, ESET is aware that machine learning is no silver bullet and that the risks of adversarial machine learning will grow with time. To avoid such potential issues ESET ML is integrated within an array of highly effective detection technologies such as DNA Detections, Advanced Memory Scanner, Network Attack Protection and UEFI Scanner. We believe that only multilayered solutions can offer reliable protection from ever-developing cyberthreats.



Author  
Juraj Janosik



ENJOY SAFER TECHNOLOGY™

[WWW.ESET.COM](http://WWW.ESET.COM)