



The Rise of Destructive Malware

Modern Bombs Used in Cyberattack

Thomas **ROCCIA**

Security Researcher, **Advanced Threat Research**





Whoami

10001000100
101010101010
01100101011

Thomas ROCCIA



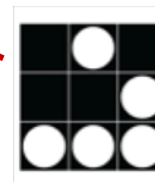
Security Researcher,
Advanced Threat Research



<http://troccia.tdgt.org>



@fr0gger_



Maker, Speaker Whatever...





\$300 Millions

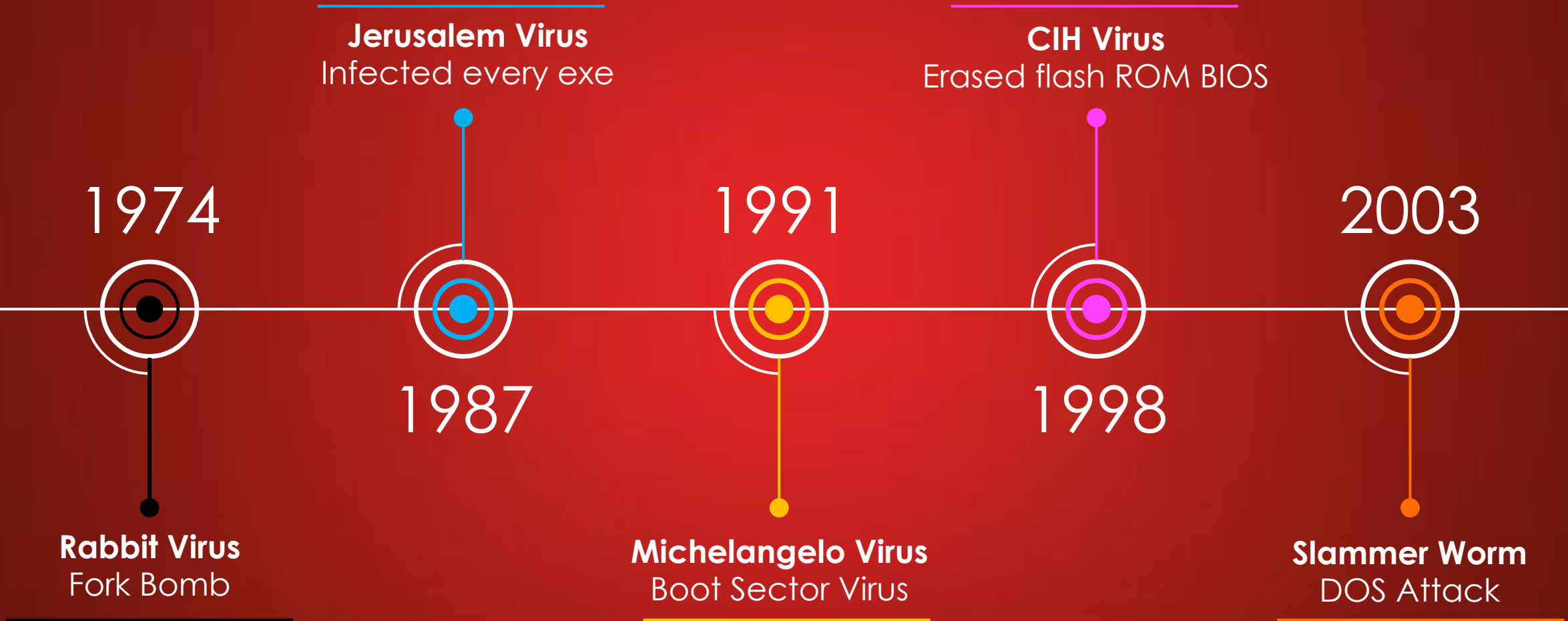
What is a Destructive Malware?



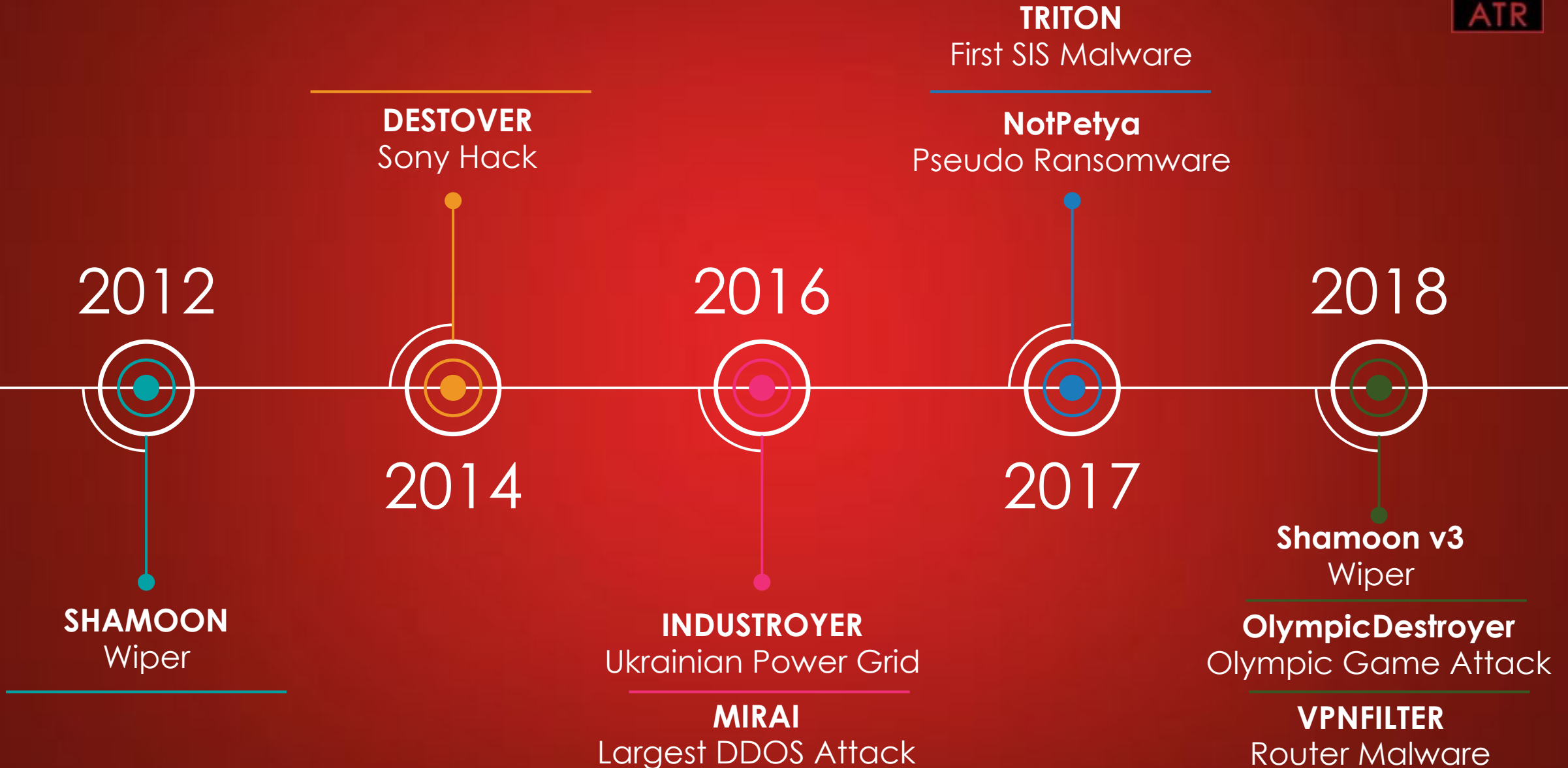
Destructive malware has the ability to destroy data, systems, to put out of service or to have a **physical impact through digital actions**.

Some are associated with propagation capabilities making the threat more destructive.

Early Destructive Malware

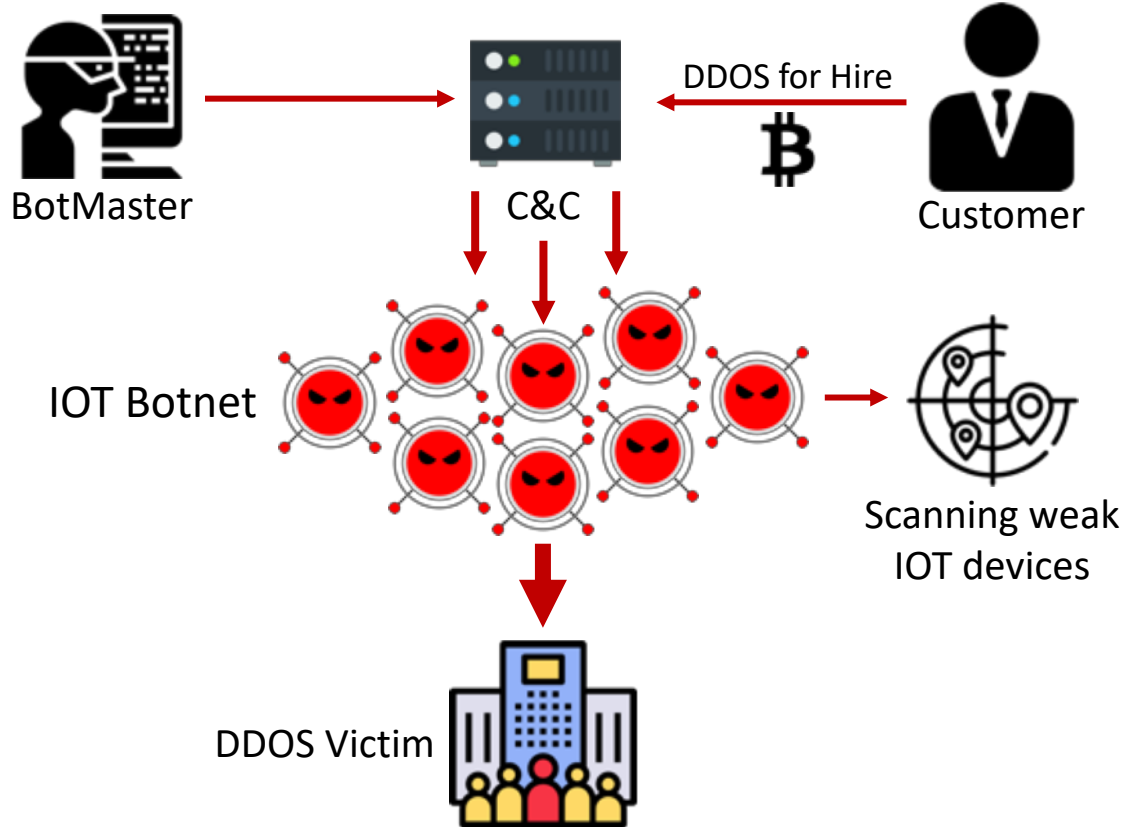


Recent Destructive Attack





MIRAI: The Largest DDOS Botnet



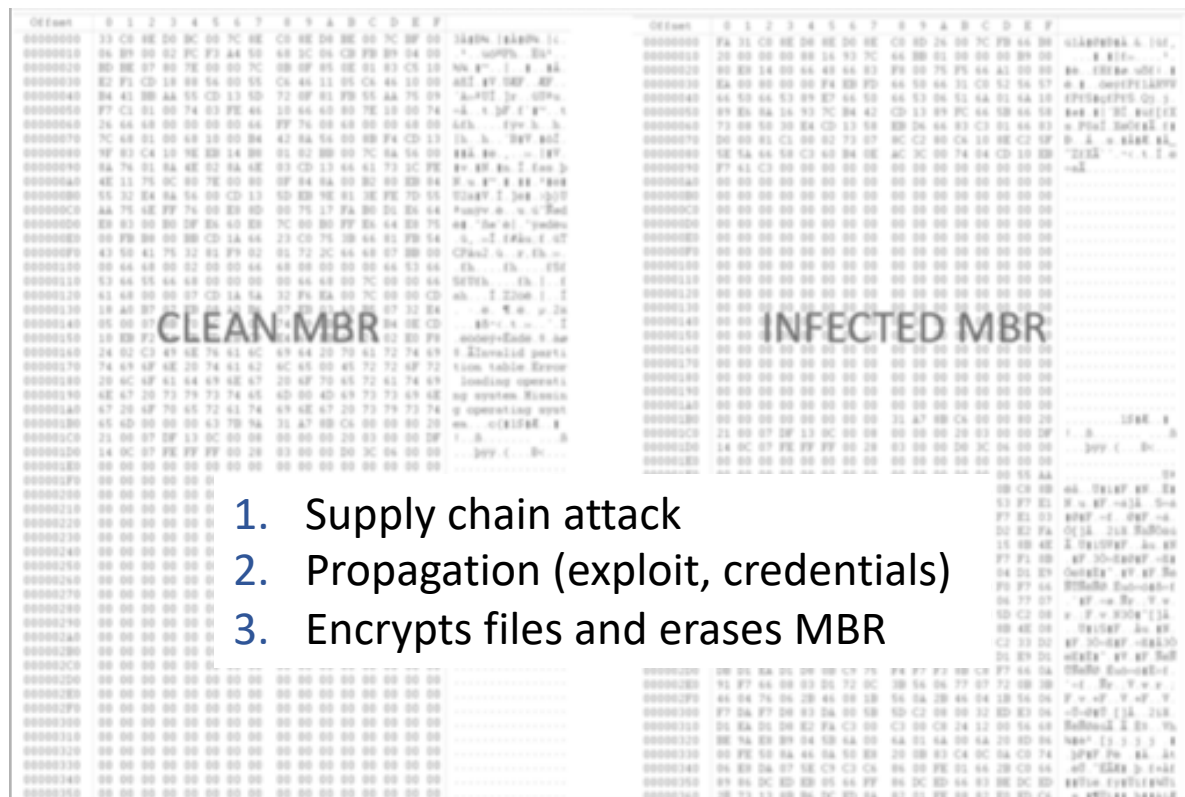
Mirai is responsible of the largest ddos attack in 2016 on Brian Krebs website (660 GBps of traffic)



Mirai was designed for DDOS attack



NotPetya: The Pseudo Ransomware



1. Supply chain attack
2. Propagation (exploit, credentials)
3. Encrypts files and erases MBR

Number of Encrypted files

	Cerber	Locky	Wannacry	Petya 2016	NotPetya
Number of File Types	187	381	176	228	65



PSEUDO-RANSOMWARE

IS A DESTRUCTIVE ATTACK DISGUISED AS RANSOMWARE EITHER TO TAKE DOWN COMPANIES OR TO KEEP THE IT-DEPARTMENT BUSY.



-- CHRISTIAAN BEEK, LEAD SCIENTIST MCAfee

NotPetya was designed for IT destruction

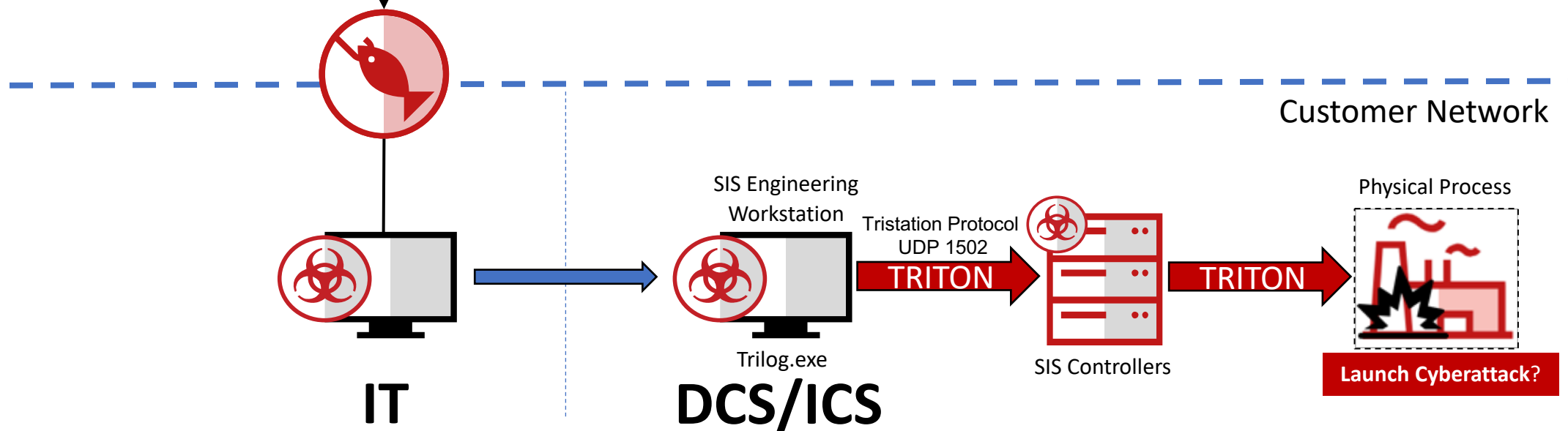


TRITON: The First SIS Malware

10010010010
101010101010
01100101011



An essential danger in this threat is that it moves from mere **digital damage** to risking **human lives**.



Triton was designed to target systems that protect human life



OlympicDestroyer: « Citius, Altius, Fortius »

Deletes all the Shadow Copies

Deletes the backups catalog

No repair possible from recovery console

```
call ds:AdjustTokenPrivileges
push offset aDeleteShadowsA ; "delete shadows /all /quiet"
mov ebx, offset aCWindowsSystem ; "c:\\Windows\\system32\\vssadmin.exe"
call Invoke_CMD
mov ebx, offset aWbadminExe ; "wbadmin.exe"
mov dword ptr [esp+30h+var_30], offset aDeleteCatalogQ ; "delete catalog -quiet"
call Invoke_CMD
mov ebx, offset aBcdeditExe ; "bcdedit.exe"
mov dword ptr [esp+30h+var_30], offset aSetDefaultBoot ; "/set {default} bootstatuspolicy ignoreallfailures &"
; "bcdedit /set {default} recoveryenabled no",0"
call Invoke_CMD
mov ebx, offset aWeventutilExe ; "wevtutil.exe"
mov dword ptr [esp+30h+var_30], offset aClSystem ; "cl System"
call Invoke_CMD
mov dword ptr [esp+30h+var_30], offset aClSecurity ; "cl Security"
call Invoke_CMD
```

Deletes System and Security event logs

SERVICE_DISABLED
0x00000004

A service that cannot be started. Attempts to start the service result in the error code
ERROR_SERVICE_DISABLED.

```
lea ecx, [ebp+dwBytes]
push ecx ; pcbBytesNeeded
push esi ; cbBufSize
push esi ; lpServiceConfig
push eax ; hService
mov [ebp+dwBytes], esi
call ebx ; QueryServiceConfigW
push [ebp+dwBytes] ; dwBytes
push 8 ; dwFlags
call edi ; GetProcessHeap
push eax ; hHeap
call ds:HeapAlloc
push esi ; lpDisplayName
push esi ; lpPassword
push esi ; lpServiceStartName
push esi ; lpDependencies
push esi ; lpdwTagId
push esi ; lpLoadOrderGroup
push esi ; lpBinaryPathName
push 0FFFFFFFh ; dwErrorControl
push 4 ; dwStartType
push 0FFFFFFFh ; dwServiceType
push [ebp+hService] ; hService
mov [ebp+lpServiceConfig], eax
call ds:ChangeServiceConfigW
lea eax, [ebp+dwBytes]
push eax ; pcbBytesNeeded
push [ebp+dwBytes] ; cbBufSize
push [ebp+lpServiceConfig] ; lpServiceConfig
push [ebp+hService] ; hService
call ebx ; QueryServiceConfigW
test eax, eax
jz short loc_4013F5
```

OlympicDestroyer was designed for disruption




VPNFilter: TimeBomb

1000100100
1010101010
0110010101

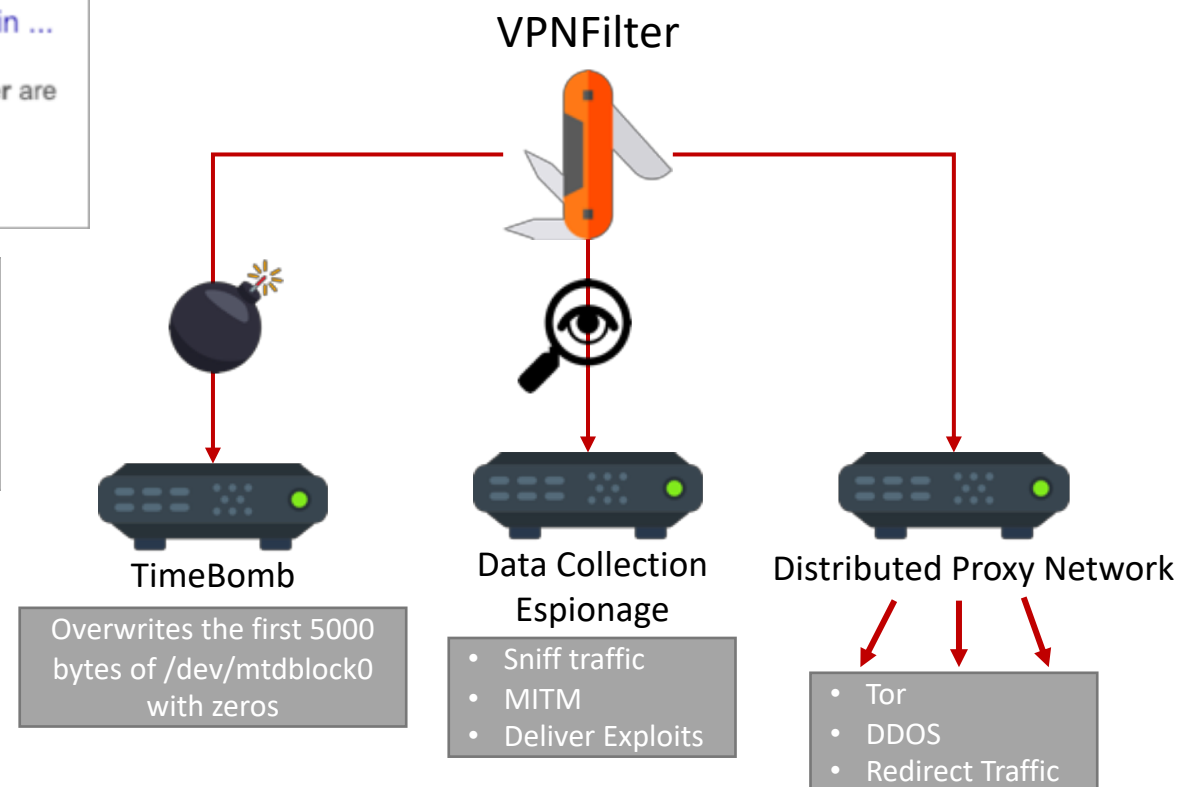


Talos finds new VPNFilter malware hitting 500K IoT devices, mostly in ...
ZDNet - May 23, 2018
According to a blog from Cisco's Talos, the known devices affected by VPNFilter are Linksys, MikroTik, Netgear, and TP-Link networking ...
Advanced VPNFilter malware menacing routers worldwide
The Register - May 23, 2018



VPNFilter – is a malware timebomb lurking on your router?
Naked Security - May 23, 2018
Researchers at Cisco Talos just published a report documenting a giant-sized IoT botnet known as VPNFilter. More than 500,000 devices ...

- ☠️ VPNFilter targets **networking devices**
- ☠️ It has the ability to perform **intelligence collection** and **destructive attack**



VPNFilter has the ability to act as a bomb

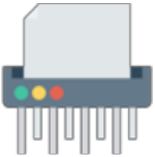


Shamoon V3: Back to the Future



Shamoon Wiper first appears in 2012, back in 2016 then in 2018

- Uses the raw disk driver
- Overwrite every files



Another .Net wiper has been discovered

- Change creation, write, and access date and time to 01/01/3000 at 12:01:01 for each files
- Overwrite 2 times each files

```
private static void changeDateFile(string paths)
{
    try
    {
        DateTime dateTime = new DateTime(3000, 1, 1, 12, 1, 1);
        if (File.Exists(paths))
        {
            File.SetLastWriteTime(paths, dateTime);
            File.SetCreationTime(paths, dateTime);
            File.SetLastWriteTime(paths, dateTime);
            File.SetLastAccessTime(paths, dateTime);
        }
    }
}
```

```
public static void TwoPassFileErase(string path, long blockSize, Random random)
{
    try
    {
        if (path == null)
            throw new ArgumentNullException(nameof(path));
        if (blockSize <= 0L)
            throw new ArgumentOutOfRangeException(nameof(blockSize));
        if (random == null)
```

3724	CloseFile	C:\
3724	CreateFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	QueryStandardI...	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	CloseFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	CreateFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	QueryAttributeT...	C:\WINDOWS\system32\drivers\acpi.sys
3724	SetDispositionI...	C:\WINDOWS\system32\drivers\acpi.sys
3724	CloseFile	C:\WINDOWS\system32\drivers\acpi.sys
3724	CreateFile	C:\
3724	QuerySizeInfor...	C:\
3724	CloseFile	C:\
3724	CreateFile	C:\WINDOWS\system32\drivers\acpiec.sys
3724	QueryStandardI...	C:\WINDOWS\system32\drivers\acpiec.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpiec.sys
3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\acpiec.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpiec.sys
3724	WriteFile	C:\WINDOWS\system32\drivers\acpiec.sys
3724	CloseFile	C:\WINDOWS\system32\drivers\acpiec.sys

sc create hdv_725x type= kernel start= demand
binpath= WINDOWS\hdv_725x.sys 2>&1 >nul

Shamoon was designed for destruction and ideology



Destructive Techniques



Wiper

- Sdelete.exe
- Overwriting files
- Deletes MBR



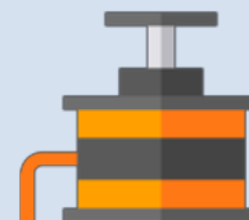
Encryption

- Rewrites MBR
- Encrypts Data
- Encrypts System



Anti-forensic

- Removes Event Logs
- Deletes backups
- Disables services



Physical Impact

Modify internal behavior
Uses exploits
Sabotage or Destruction



DoS

- Botnets/Exploits
- Advanced persistent DoS
- DDoS

Often designed with spreading techniques
To be more efficient, they rarely overwrite the entire hard disk.

Highly targeted for critical infrastructures

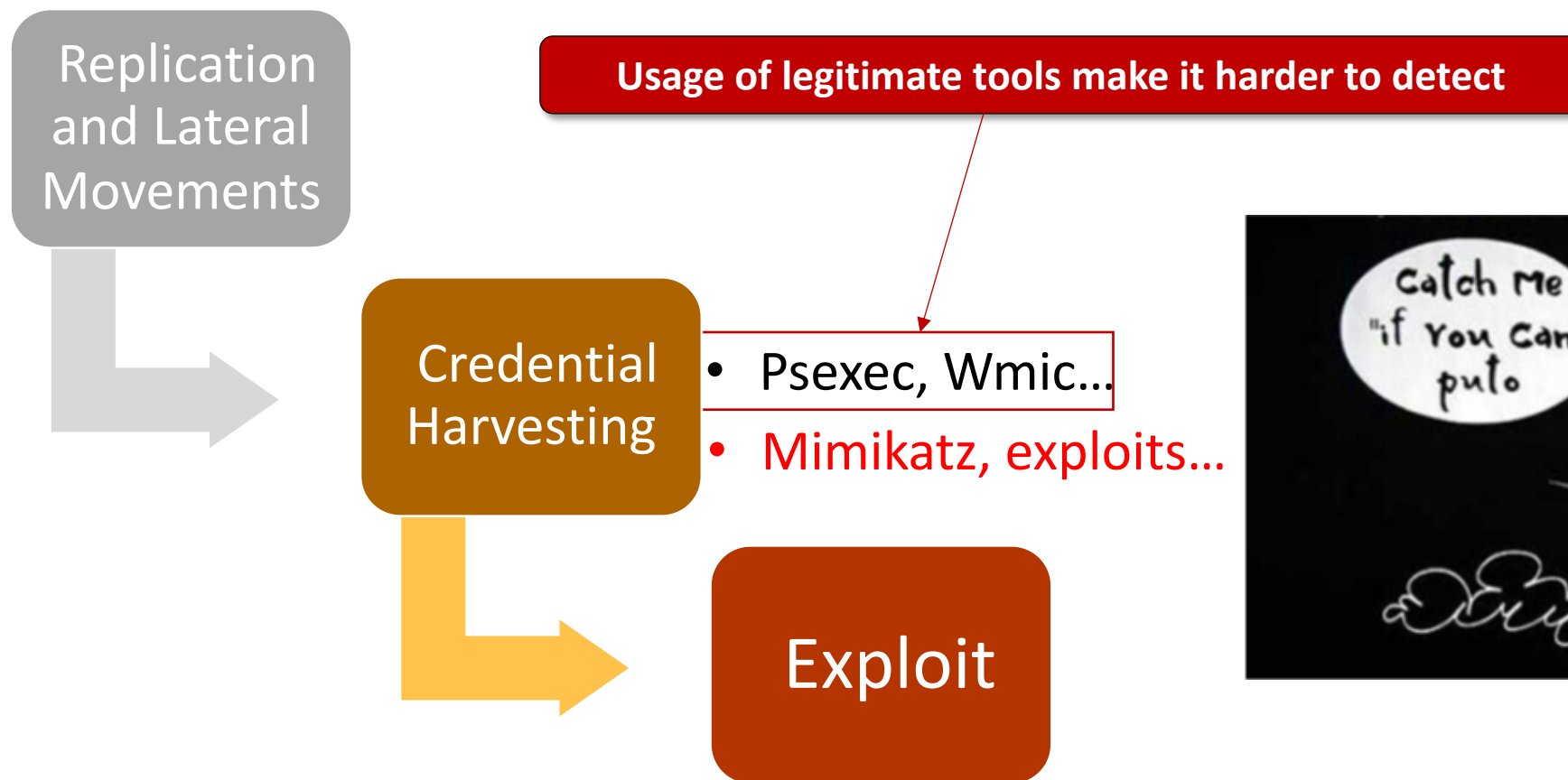
Usually DDOS for Hire



Propagation Mechanisms

100100100
1010101010
01100101011

- Some destructive malware need to be as fast as possible

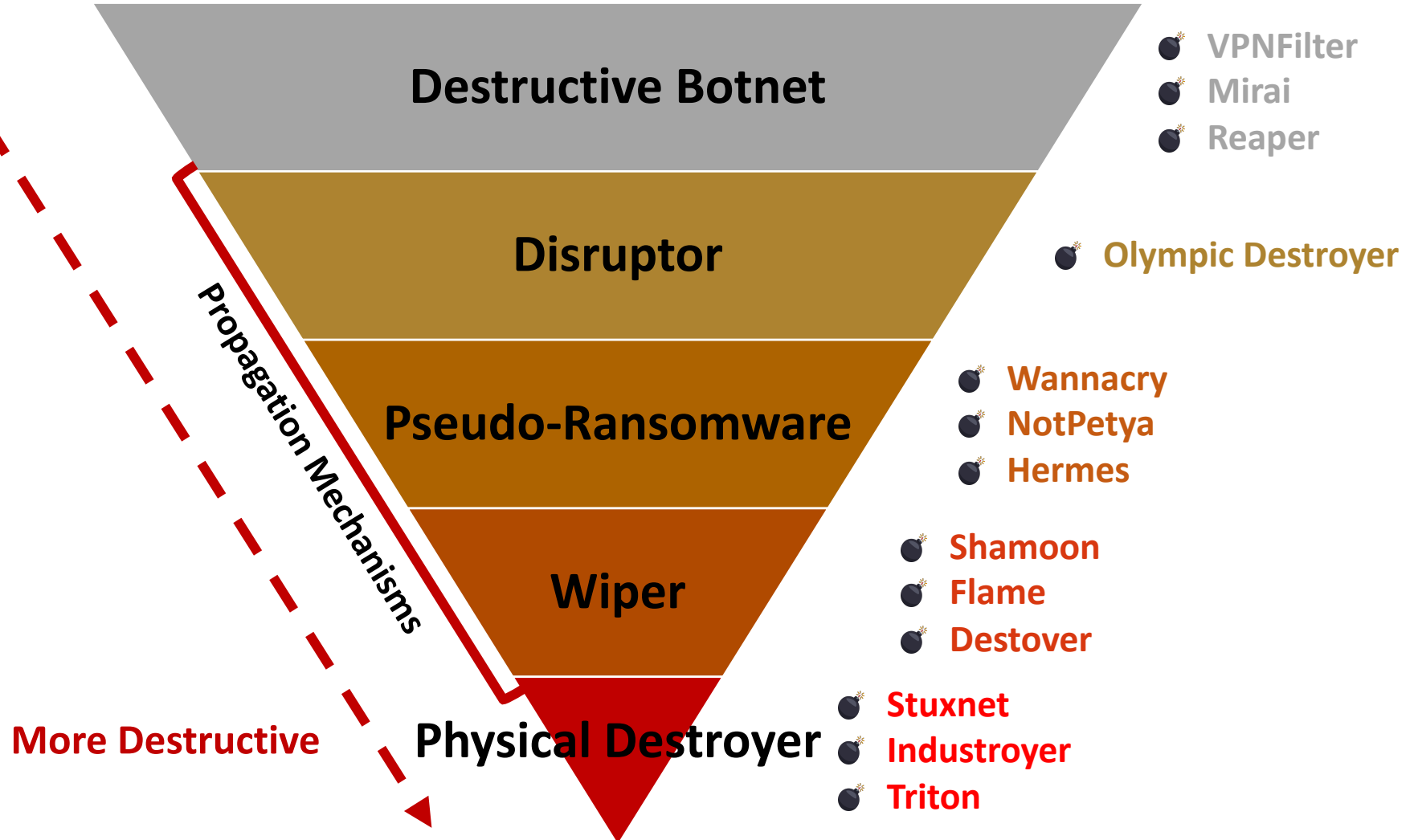




Classification

100100100
1010101010
01100101011

Less Destructive





Business & Cybercrime



We offer services to eliminate the sites and forums of your competitors using

Our service is a quick solution to your problems with **competitors and enemies.**

- Low prices (from \$ 50)
- 24-hour order taking
- Hour monitoring of all attacked resources

Attacked resources during the attack do not show signs of life, as is often the case

- Day - from \$ 50
- Week - from \$ 300
- Month - from \$ 1000

Приветствуем всех, предлагаем вашему вниманию наш сервис.
Мы предлагаем услуги по устранению сайтов и форумов ваших конкурентов при помощи

DDOS атаки.

Берёмся практически за любые проекты начиная от слабых и заканчивая серверами с

высокой защитой!

Наш сервис это быстрое решение ваших проблем с конкурентами и недругами.
Оптовым заказчикам индивидуальные условия!

Почему именно мы?

- Низкие цены (от 50\$)
- Круглосуточный приём заказов
- 100% Анонимность клиента обеспечена.
- Круглосуточный мониторинг всех атакуемых ресурсов
- Работаем со всеми типами атак
- Атакуемые ресурсы во время атаки не показывают признаков жизни, как это часто бывает у

других.

- Регулярные скидки.

Цены

- Сутки - от 50\$
- Неделя - от 300\$
- Месяц - от 1000\$

Способы оплаты

- QIWI
- Bitcoin



Business & Cybercrime



- DDOS As A Service, Powered by Bushido Botnet
- Authors claimed 500 Gbps of Power



Source: <https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered-by-bushido-botnet-.html>

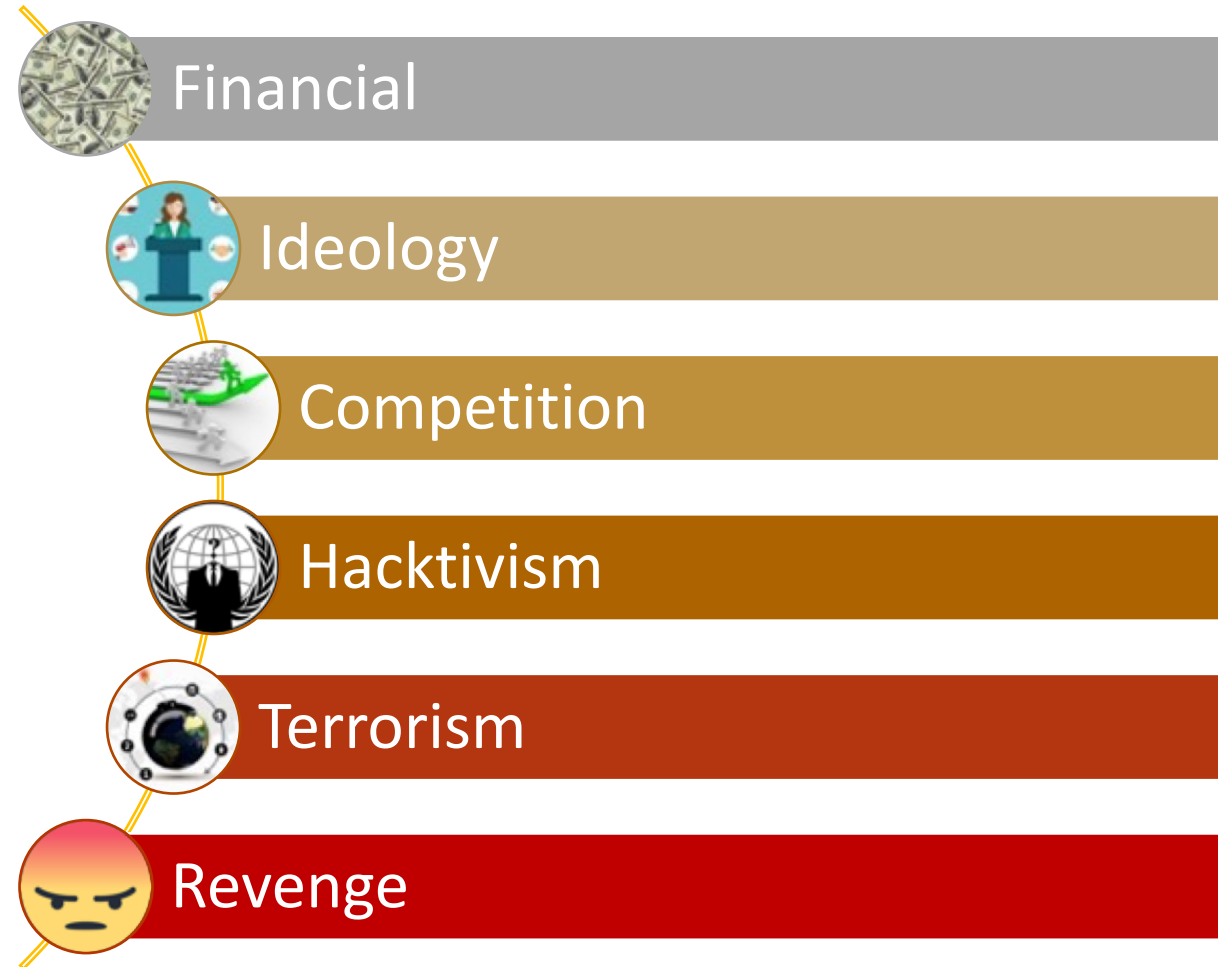




Motivation behind such attacks

100100100100
101010101010
01100101011

Terrorists
APT Hacktivists
Script Kiddies
Nation State
Organized Crime
Insider



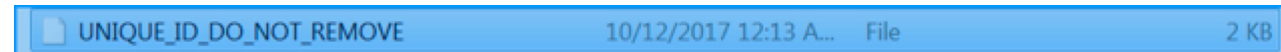
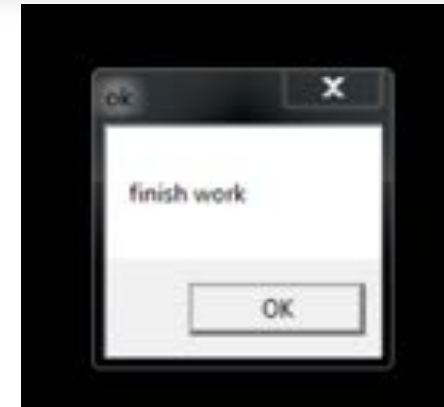


Ransomware for Destruction and Distraction

- Taiwan Bank Hacked in 2017
- Cybercriminals attempted to wire US\$60 million
- Remote access via backdoor on endpoints
- The backdoor contained a copy of the HERMES Ransomware in its resources.
- **The ransomware encrypted the files but no ransom note was printed**

Taiwan Bank Heist and the Role of Pseudo Ransomware

By Christiaan Beek and Raj Samani on Oct 12, 2017





Motivation behind such attacks

- CyanWeb has been targeted in June 2018
- The company experienced a **DDOS attack as a lure**
- In a same time and after gaining access, attackers delivered a **malware wiper** to destroy all the data.

While our server admin was distracted by the DDoS attack, the hackers simultaneously infiltrated the server, escalated their privileges and delivered a seek and destroy payload.

NO RANSOM DEMAND FILES OR CONTACTS WERE FOUND – THIS DOES NOT APPEAR TO BE A RANSOMWARE ATTACK – THIS WAS DELIBERATE DESTRUCTION / CYBER TERRORISM

CYANWEB
sv5.cyanweb.com.au

As many of you may now be aware, sv5.cyanweb.com.au cPanel web hosting server was destroyed in a Cyber Terrorist attack on Wednesday 27th, June 2018.

== What happened? ==

A professional hacking group attacked, infiltrated the server and destroyed all data, including all available backup data.

We highly suspect they were "professionals", as at the time of the infiltration the server was being "overloaded" (DDoS) by a highly suspicious range of sequential Swiss server IP addresses. Some Swiss servers are like Swiss bank accounts and are sometimes used by professional criminal organisations / and other well-funded cyber terrorist groups.

While our server admin was distracted by the DDoS attack, the hackers simultaneously infiltrated the server, escalated their privileges and delivered a seek and destroy payload.

This payload located and destroyed all backup disk drives using the "DD" command, while running a super-fast encryption routine that encrypted all user accounts, while another routine sought out and deleted any core WordPress database tables using the default wp_ prefix.

Once the infiltration was discovered by the then logged in admin, the server was shut off immediately.

Unfortunately, it was too late and only an estimated 12% of customer data survived the attack.

NO RANSOM DEMAND FILES OR CONTACTS WERE FOUND – THIS DOES NOT APPEAR TO BE A RANSOMWARE ATTACK – THIS WAS DELIBERATE DESTRUCTION / CYBER TERRORISM



Motivation behind such attacks: SHAMOON

SHAMOON v1 – 2012



- Shamoon authors have let political messages in each waves:
 - Shamoon v1: Burned American flag
 - Shamoon v2: Syrian refugee
 - Shamoon v3: Phrase from the Quran (Surah Masad, Ayat 1 [111:1])
“perish the hands of the Father of flame”

SHAMOON v2 – 2016



SHAMOON v3 – 2018





What to do?

Destructive Malware are an **aggressive threat** that need to be addressed seriously!

Network and User Segregation

Increase awareness of systems that can be utilized as a gateway to pivot (lateral movement)

Patch Management by Prioritization

Backup

Incident Response Plan



What to expect in the future?

10001000100
101010101010
01100101011

- Destructive malware will continue to evolve and be used as **economical and political weapons** against states and organizations.
- **Supply-chain attack** as spreading technique will become more common.
- **DDOS botnet** will become more powerful.
- Targeted **attack on critical assets** will be more sophisticated.





Take Away

- 💣 Destructive Malware used several techniques.
- 💣 Some of them used propagation mechanisms.
- 💣 Motivation and actors are different.



Destructive Malware are a serious threat that can take down a **whole company or a country.**



References

<https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>

<https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>

<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/>

<https://blog.talosintelligence.com/2018/02/olympic-destroyer.html>

<https://blog.talosintelligence.com/2018/05/VPNFilter.html>

<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europe/>

<https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/>

<https://www.fortinet.com/blog/threat-research/ddos-for-hire-service-powered-by-bushido-botnet-.html>

<https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>

Icon: <https://www.flaticon.com>



Thank You

Thomas ROCCIA

Security Researcher, Advanced Threat Research

<https://securingtomorrow.mcafee.com/author/thomas-roccia/>

 @fr0gger_

Q/A



McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee LLC.