WISDOM AND LIFE LESSONS LEARNED IN THE BUSINESS OF CYBER SECURITY

DefCamp November 2017

ABOUT ME AND IXIA

Steve McGregory – Senior Director of Application and Threat Intelligence
@stevemcgregory

I'm human. I have a family. I love spending time with my children and working on our farm.

After that, I focus on building products to help protect the cyber world.

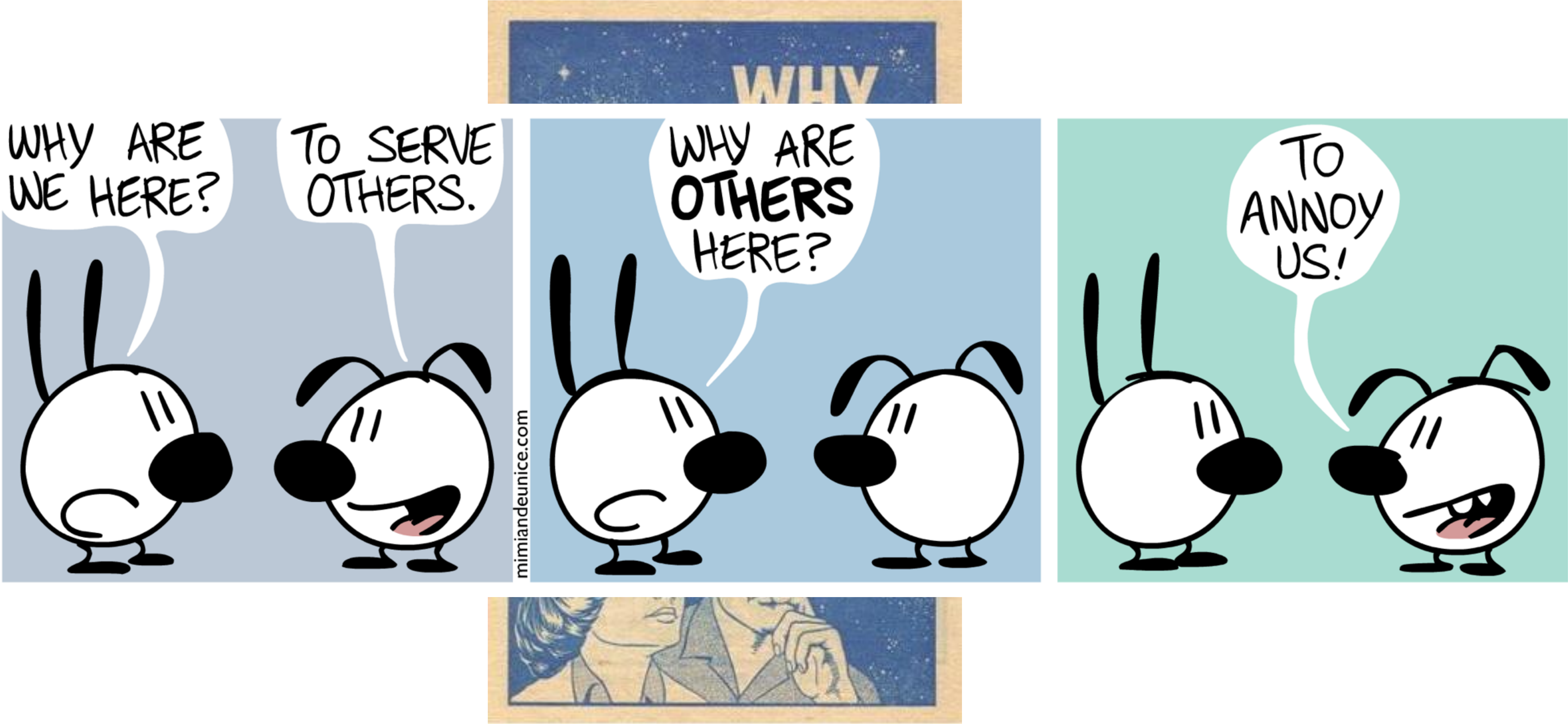
I chose cyber security because of the potential I see in the Internet, and I got hacked.

ixia | A Keysight Business

BENEFITS

1. We have a lab with every major network security product in the world
2. We build product that tests just about every security product in the world
3. Very brilliant and nice people
4. It provides me with an opportunity to accomplish my primary business goal
5. Most importantly to me, I enjoy the work we do

I AM AN AMATEUR PHILOSOPHER



THE INTERNET IS FLAWED

HUMAN DRIVE TO MAKE MONEY LEADS DECISIONS

CYBER SECURITY ECONOMY

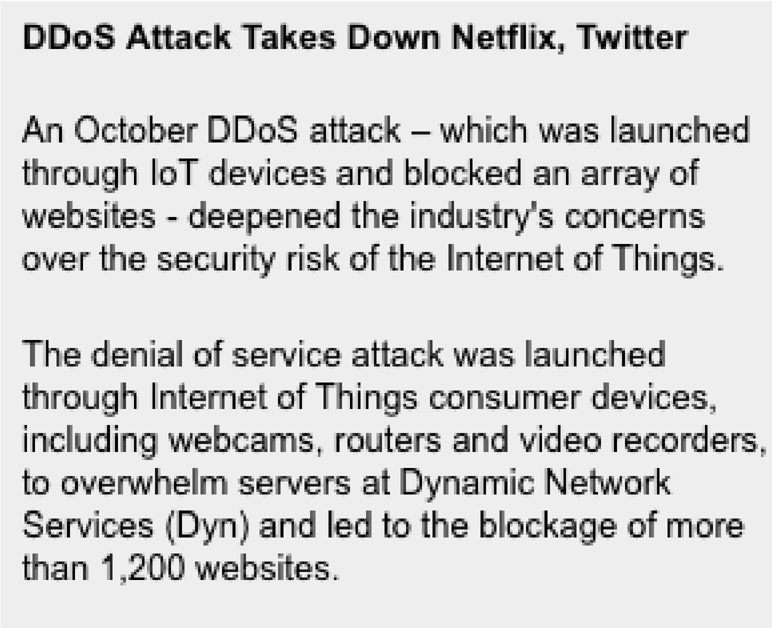
WHAT IF?

Internet was

Software and Devices

THAT'S A FAIRY TALE

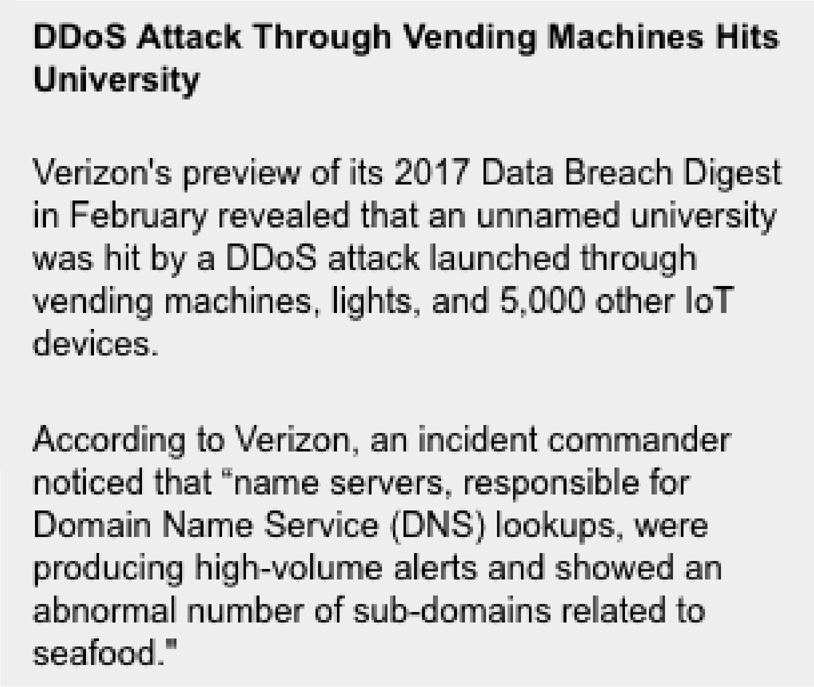
BACK TO REALITY



DDoS Attack Takes Down Netflix, Twitter

An October DDoS attack – which was launched through IoT devices and blocked an array of websites - deepened the industry's concerns over the security risk of the Internet of Things.

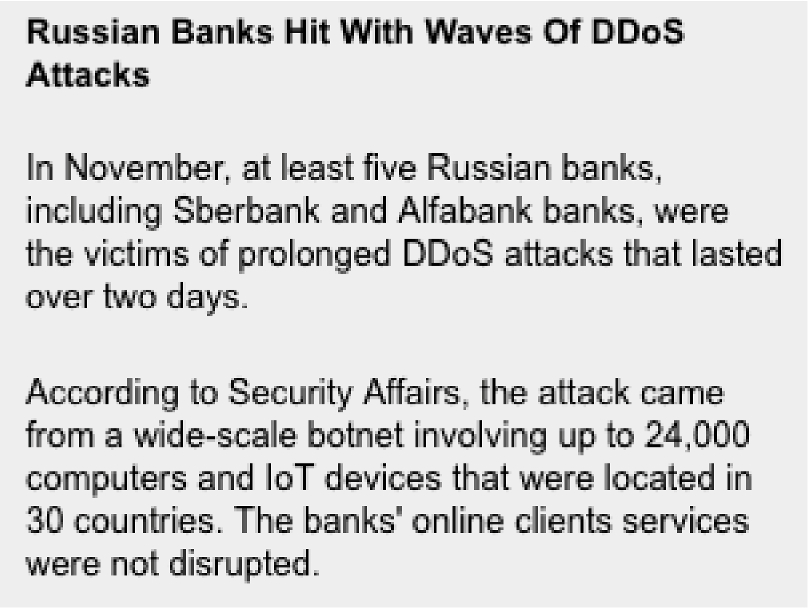
The denial of service attack was launched through Internet of Things consumer devices, including webcams, routers and video recorders, to overwhelm servers at Dynamic Network Services (Dyn) and led to the blockage of more than 1,200 websites.



DDoS Attack Through Vending Machines Hits University

Verizon's preview of its 2017 Data Breach Digest in February revealed that an unnamed university was hit by a DDoS attack launched through vending machines, lights, and 5,000 other IoT devices.

According to Verizon, an incident commander noticed that "name servers, responsible for Domain Name Service (DNS) lookups, were producing high-volume alerts and showed an abnormal number of sub-domains related to seafood."

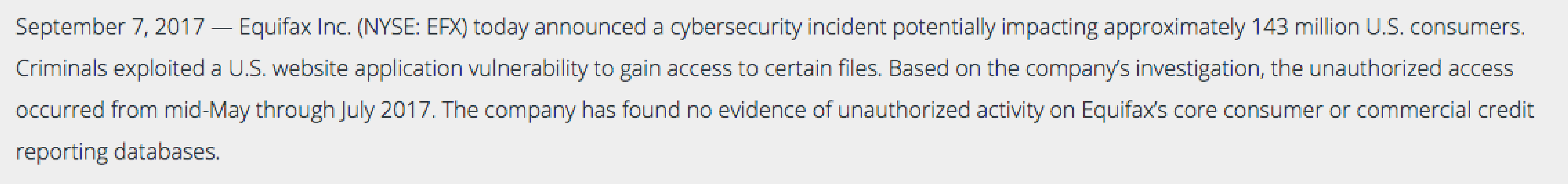


Russian Banks Hit With Waves Of DDoS Attacks

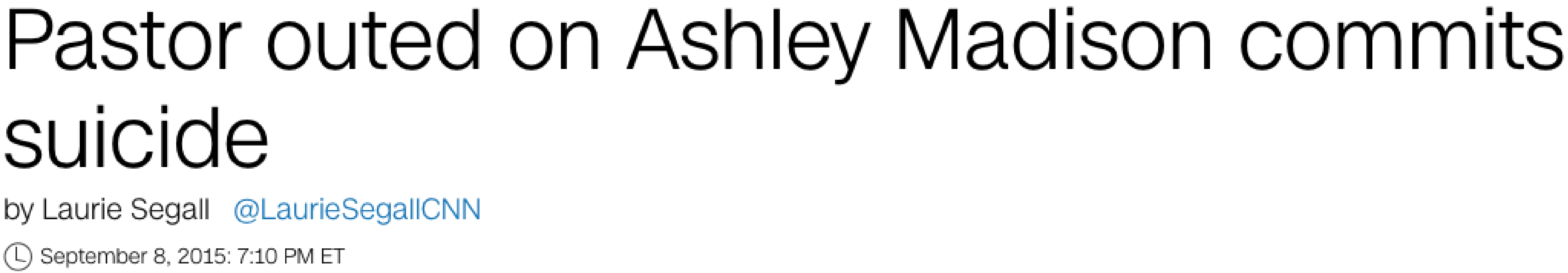
In November, at least five Russian banks, including Sberbank and Alfabank banks, were the victims of prolonged DDoS attacks that lasted over two days.

According to Security Affairs, the attack came from a wide-scale botnet involving up to 24,000 computers and IoT devices that were located in 30 countries. The banks' online clients services were not disrupted.

MORE REALITY



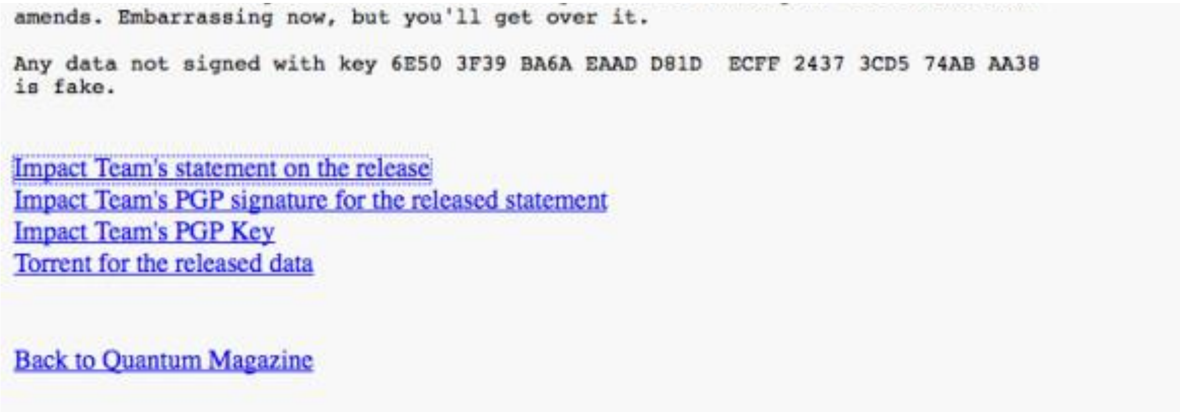
September 7, 2017 — Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.



Pastor outed on Ashley Madison commits suicide

by Laurie Segall @LaurieSegallCNN

September 8, 2015: 7:10 PM ET



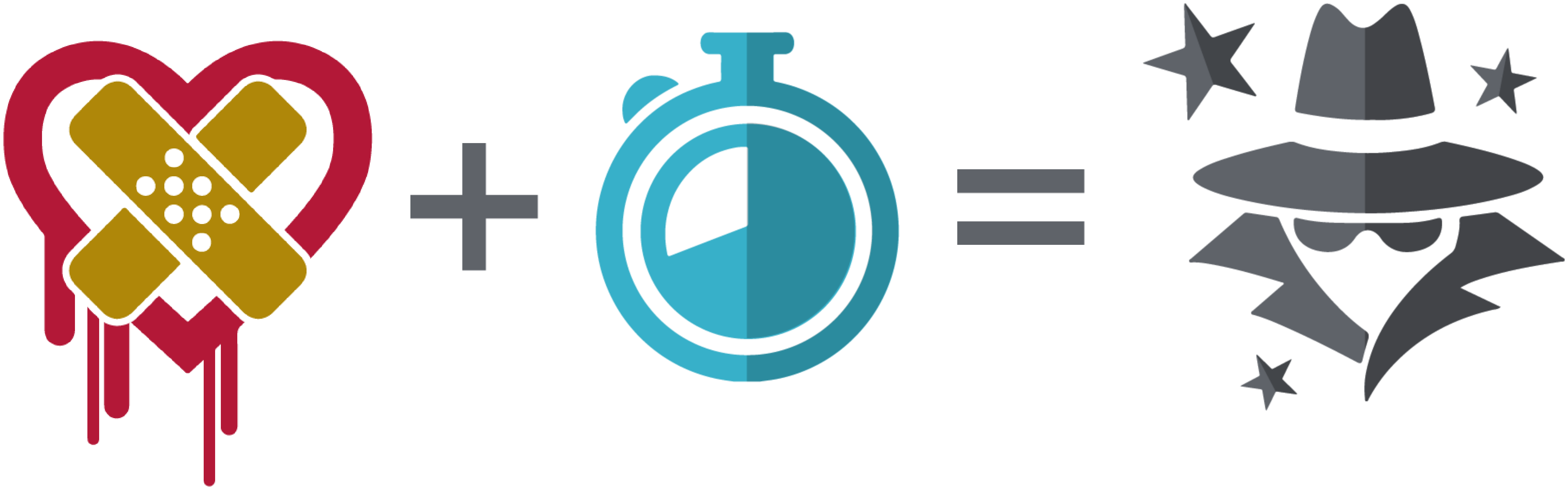
```
amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D  ECFF 2437 3CD5 74AB AA38
is fake.
```

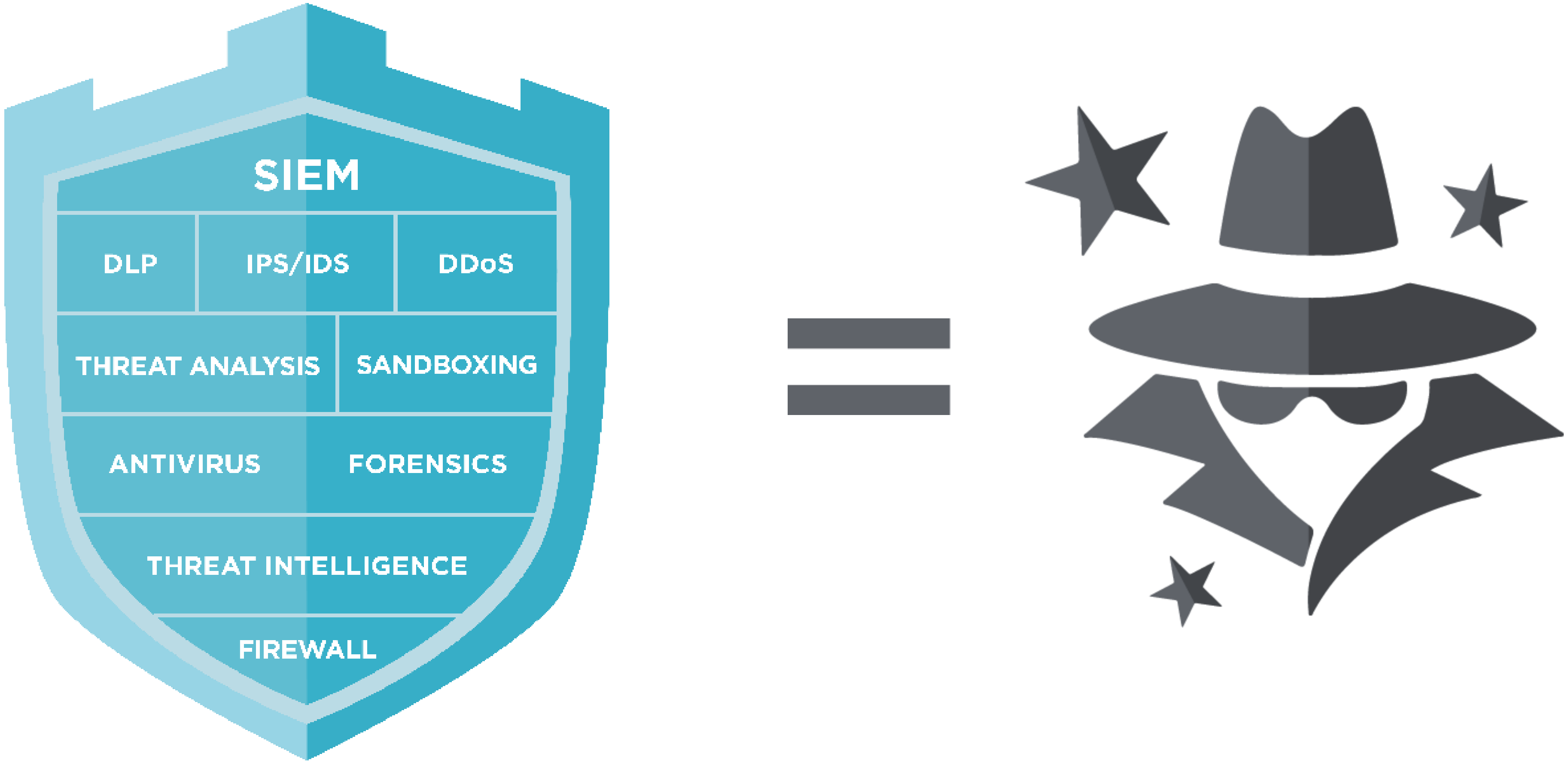
Impact Team's statement on the release
Impact Team's PGP signature for the released statement
Impact Team's PGP Key
Torrent for the released data

Back to Quantum Magazine

THEY KNOW EVERYTHING ABOUT US



THEY KNOW EVERYTHING ABOUT US



SIEM

DLP

IPS/IDS

DDoS

THREAT ANALYSIS

SANDBOXING

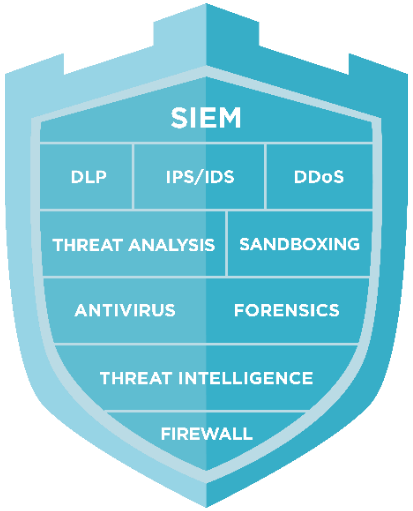
ANTIVIRUS

FORENSICS

THREAT INTELLIGENCE

FIREWALL

THE DECK IS STACKED AGAINST US



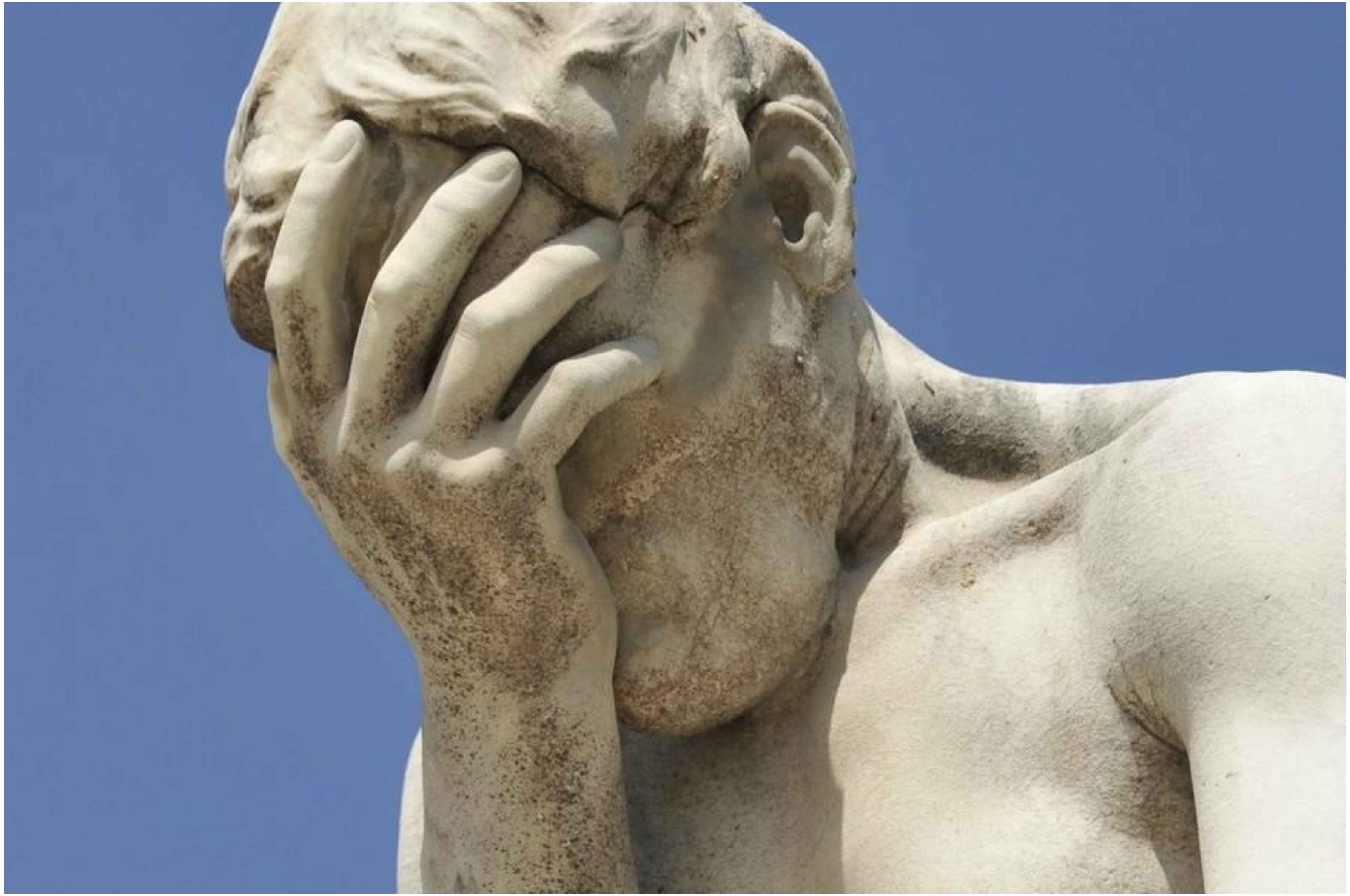
We know this!

Cybercriminals know this!

Who doesn’t know this?

MAJORITY OF HUMANITY OUTSIDE OF THIS ROOM

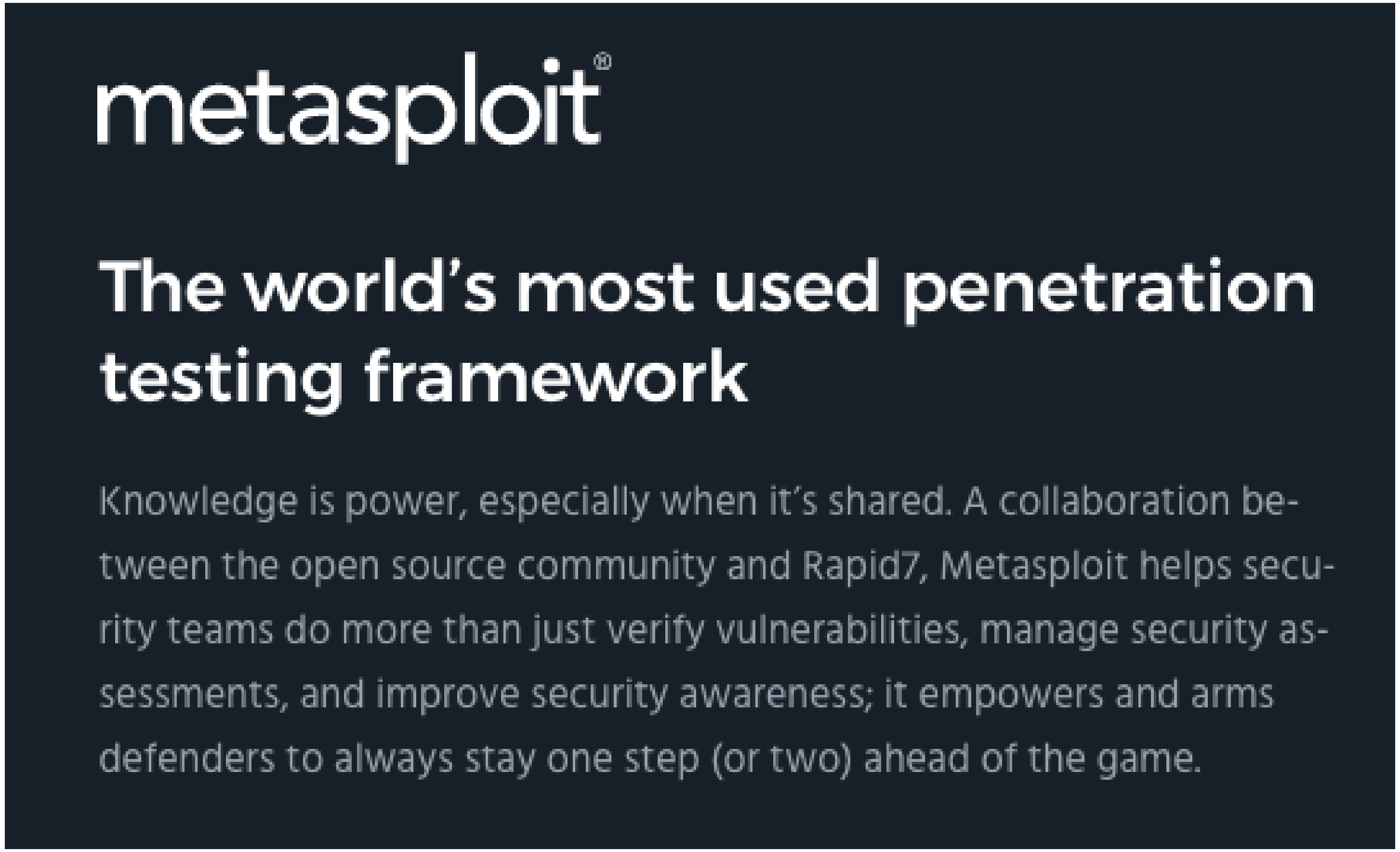
EVERYDAY…



CYBER SECURITY WOES

GENERAL POPULATION HAVE NO CLUE ABOUT THIS

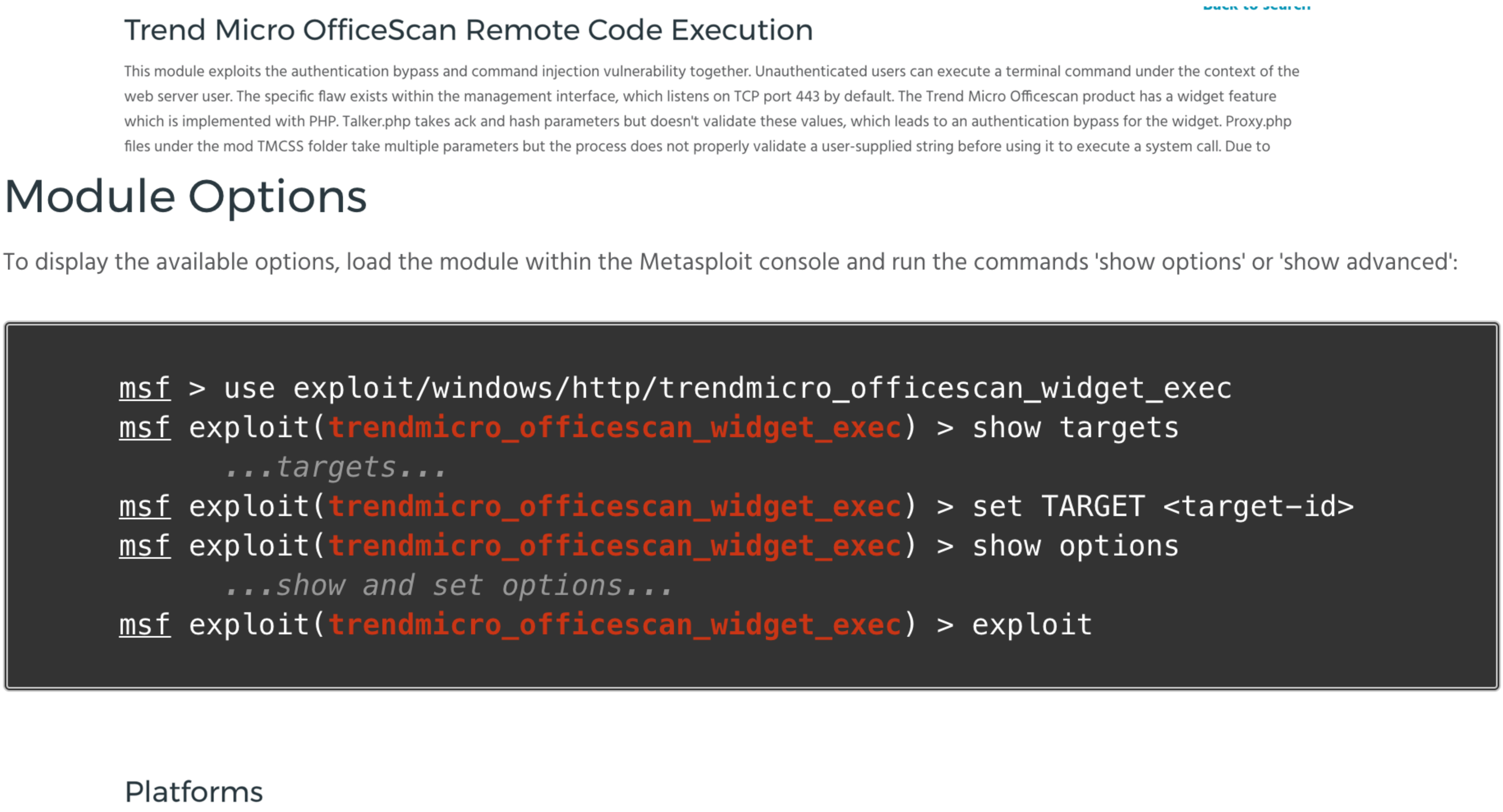
SHARING IS CARING, RIGHT?



metasploit®

The world’s most used penetration testing framework

Knowledge is power, especially when it’s shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.



Back to Search

Trend Micro OfficeScan Remote Code Execution

This module exploits the authentication bypass and command injection vulnerability together. Unauthenticated users can execute a terminal command under the context of the web server user. The specific flaw exists within the management interface, which listens on TCP port 443 by default. The Trend Micro Officescan product has a widget feature which is implemented with PHP. Talker.php takes ack and hash parameters but doesn't validate these values, which leads to an authentication bypass for the widget. Proxy.php files under the mod TMCSS folder take multiple parameters but the process does not properly validate a user-supplied string before using it to execute a system call. Due to

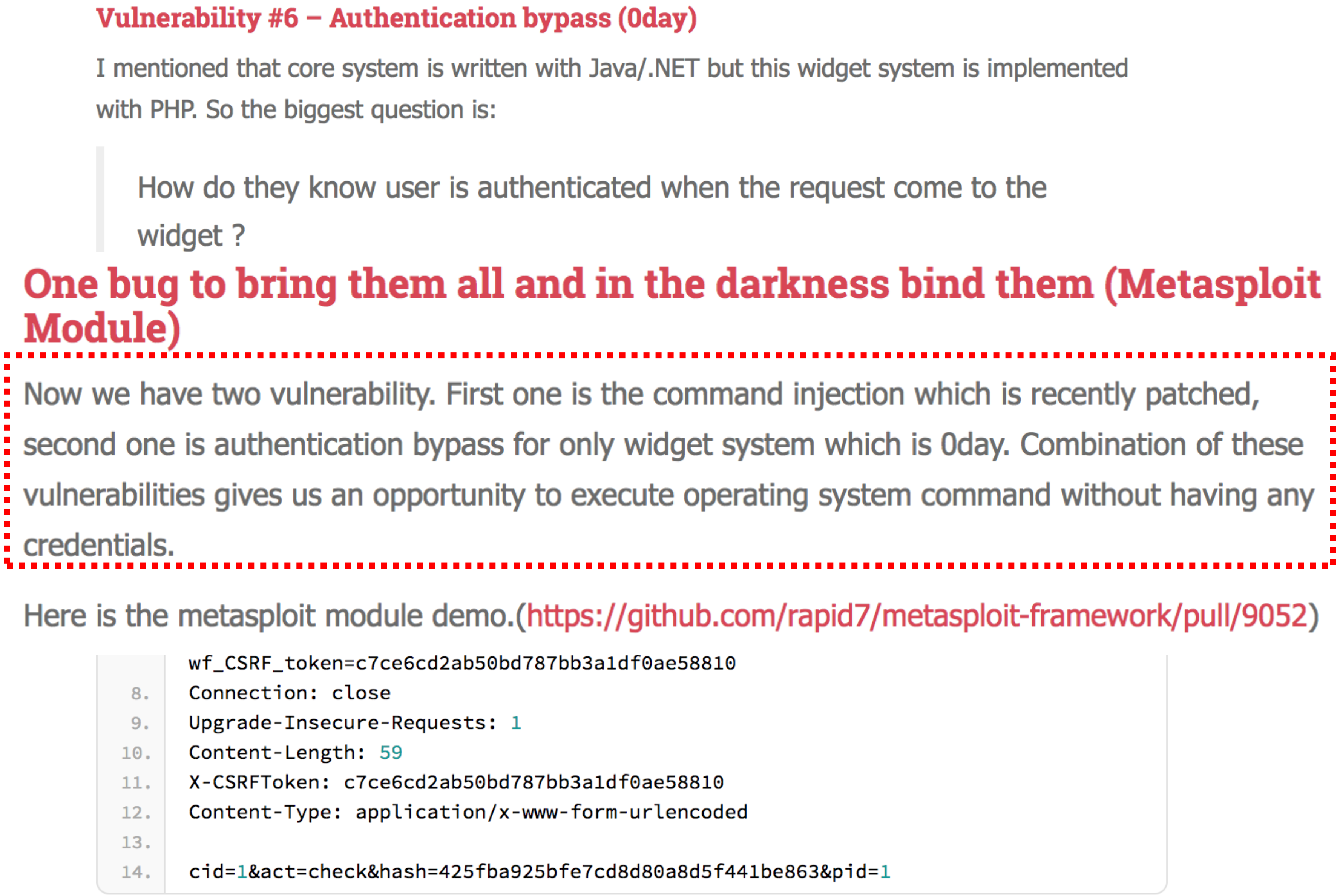
Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/http/trendmicro_officescan_widget_exec
msf exploit(trendmicro_officescan_widget_exec) > show targets
      ...targets...
msf exploit(trendmicro_officescan_widget_exec) > set TARGET <target-id>
msf exploit(trendmicro_officescan_widget_exec) > show options
      ...show and set options...
msf exploit(trendmicro_officescan_widget_exec) > exploit
```

Platforms

LET’S LOOK AT THE BLOG



Vulnerability #6 – Authentication bypass (0day)

I mentioned that core system is written with Java/.NET but this widget system is implemented with PHP. So the biggest question is:

> How do they know user is authenticated when the request come to the widget ?

One bug to bring them all and in the darkness bind them (Metasploit Module)

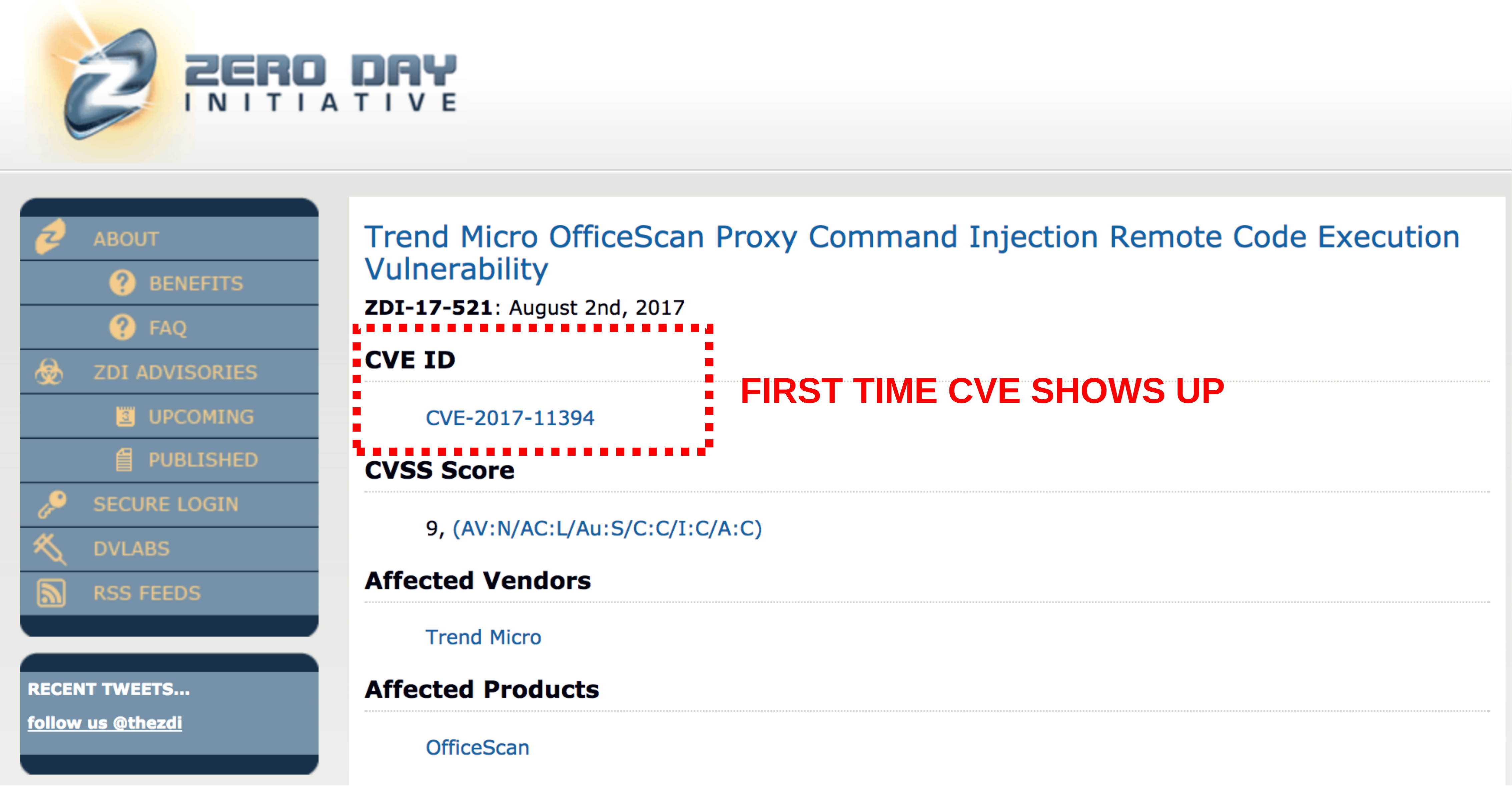
Now we have two vulnerability. First one is the command injection which is recently patched, second one is authentication bypass for only widget system which is 0day. Combination of these vulnerabilities gives us an opportunity to execute operating system command without having any credentials.

Here is the metasploit module demo.(https://github.com/rapid7/metasploit-framework/pull/9052)

```
wf_CSRF_token=c7ce6cd2ab50bd787bb3a1df0ae58810
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 59
X-CSRFToken: c7ce6cd2ab50bd787bb3a1df0ae58810
Content-Type: application/x-www-form-urlencoded

cid=1&act=check&hash=425fba925bfe7cd8d80a8d5f441be863&pid=1
```

LET’S LOOK AT ZDI PAGE



Trend Micro OfficeScan Proxy Command Injection Remote Code Execution Vulnerability

ZDI-17-521: August 2nd, 2017

CVE ID

CVE-2017-11394

FIRST TIME CVE SHOWS UP

CVSS Score

9, (AV:N/AC:L/Au:S/C:C/I:C/A:C)

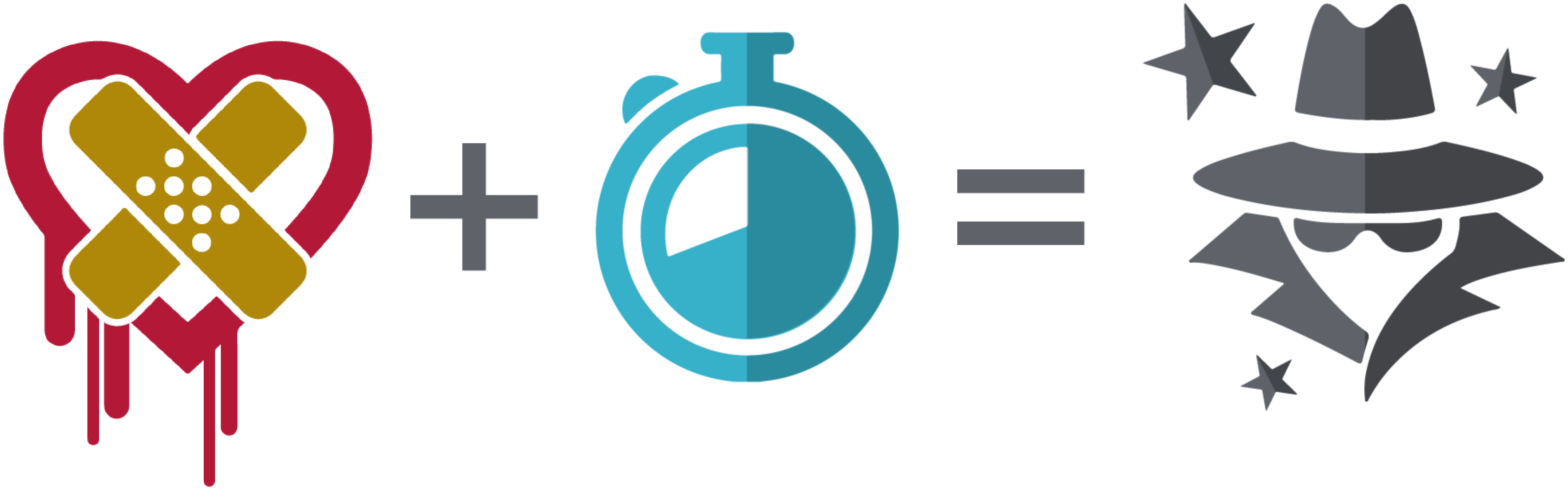
Affected Vendors

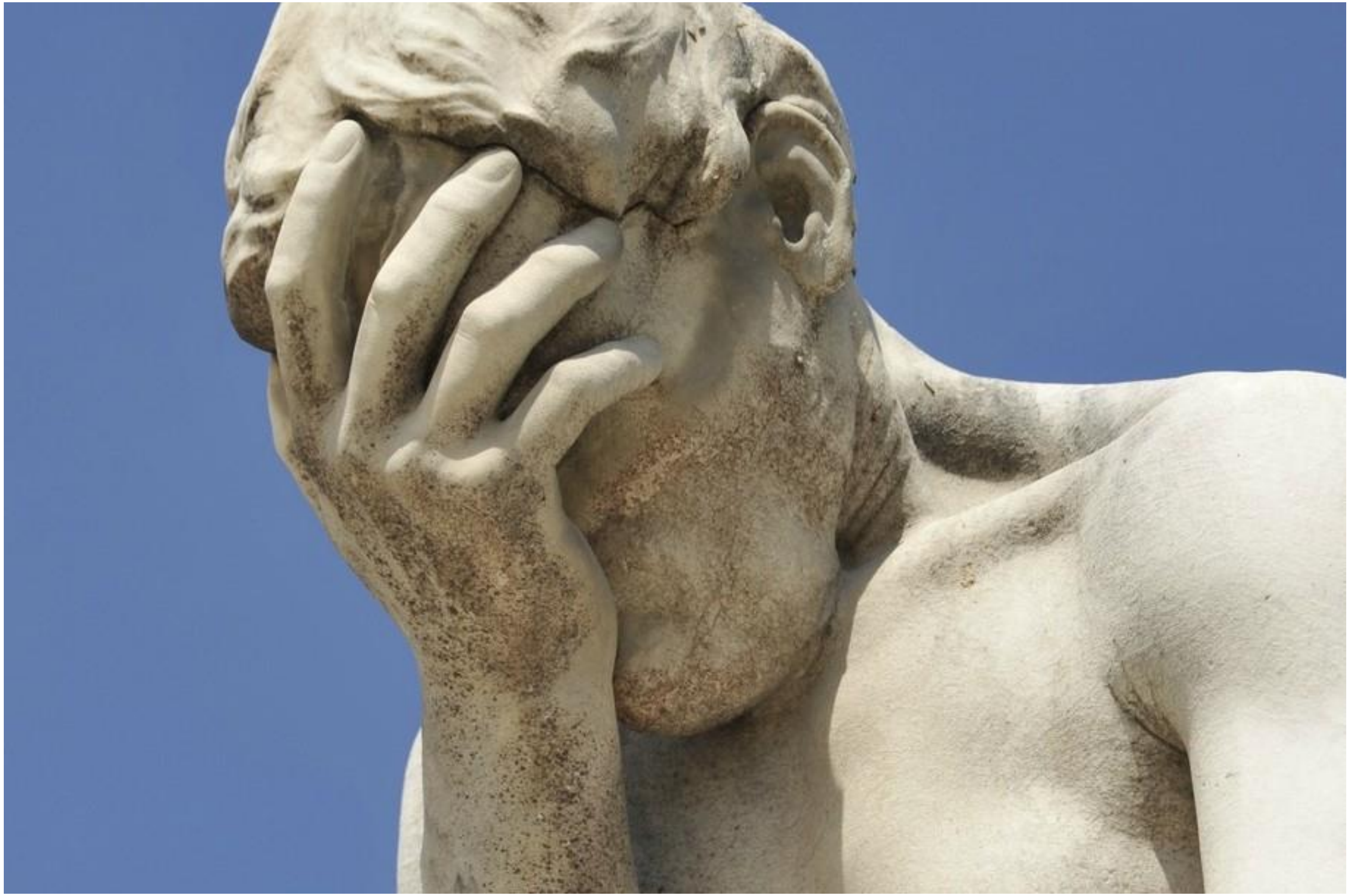
Trend Micro

Affected Products

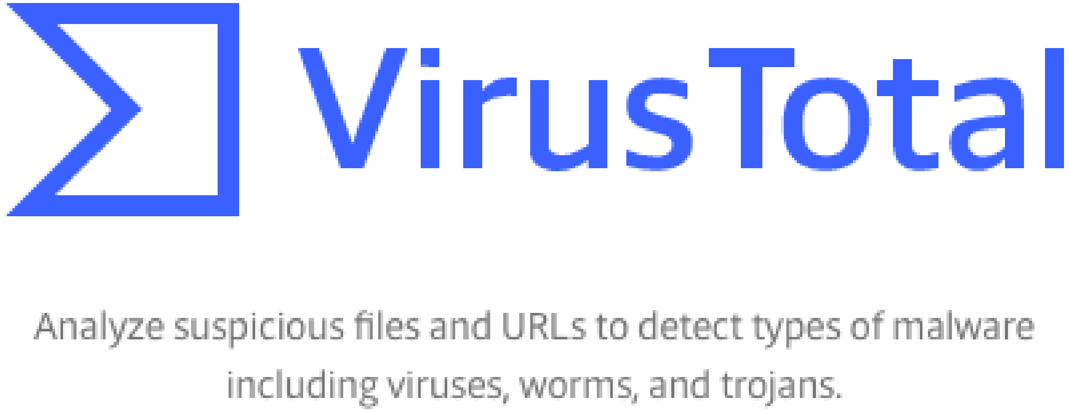
OfficeScan

THEY KNOW EVERYTHING ABOUT US



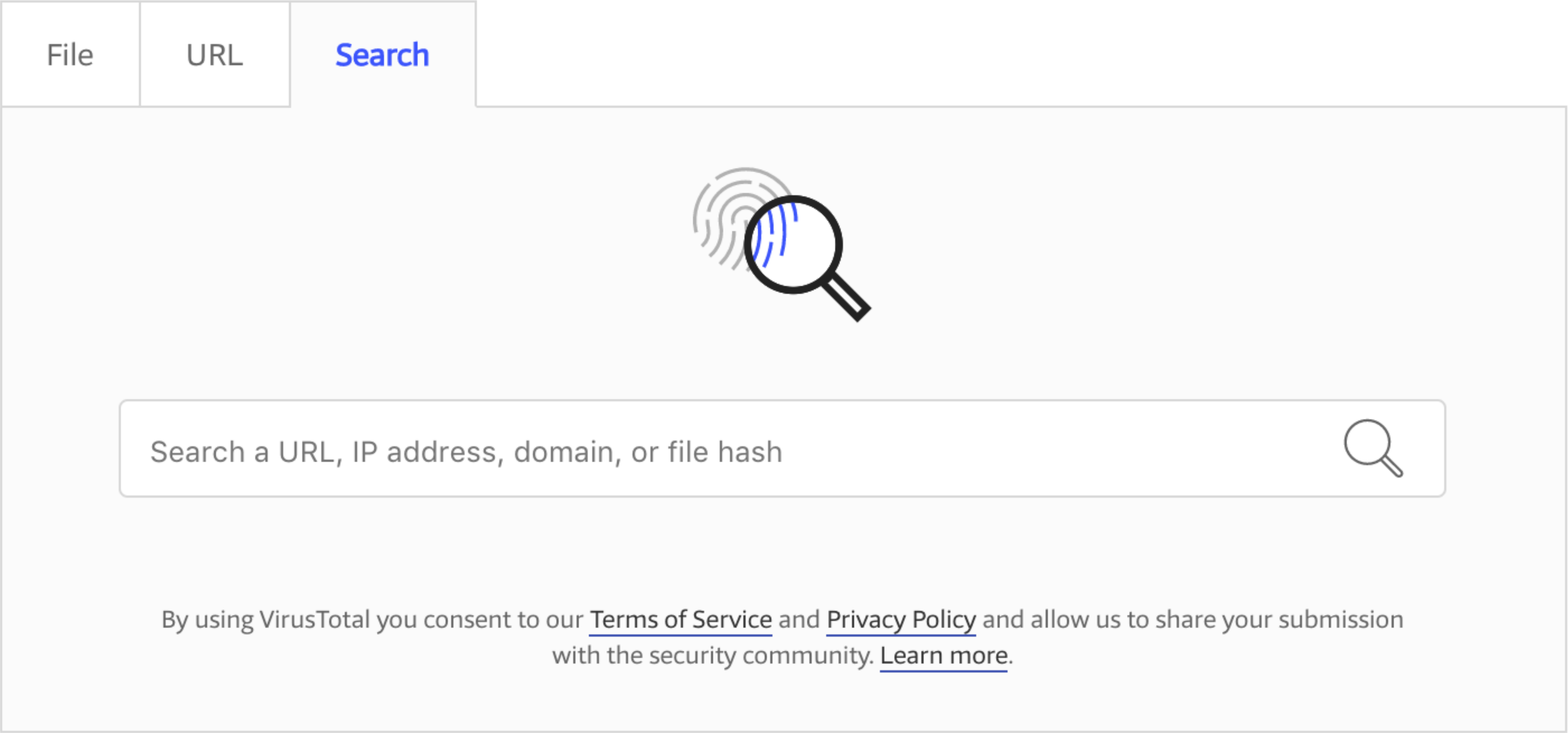


SHARING IS CARING, RIGHT?



Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

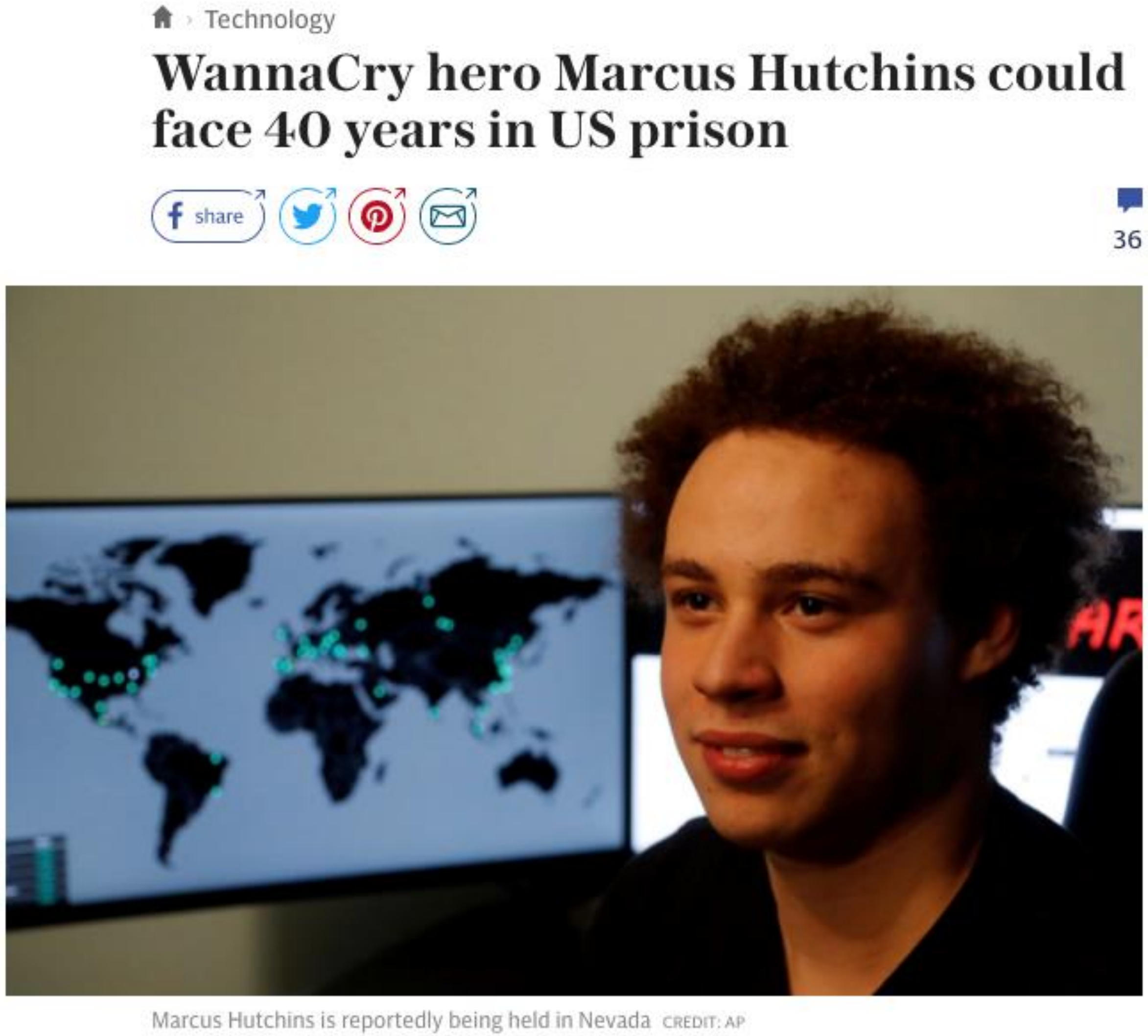
MALWARE DEVELOPER MONITOR



Search a URL, IP address, domain, or file hash

By using VirusTotal you consent to our Terms of Service and Privacy Policy and allow us to share your submission with the security community. Learn more.

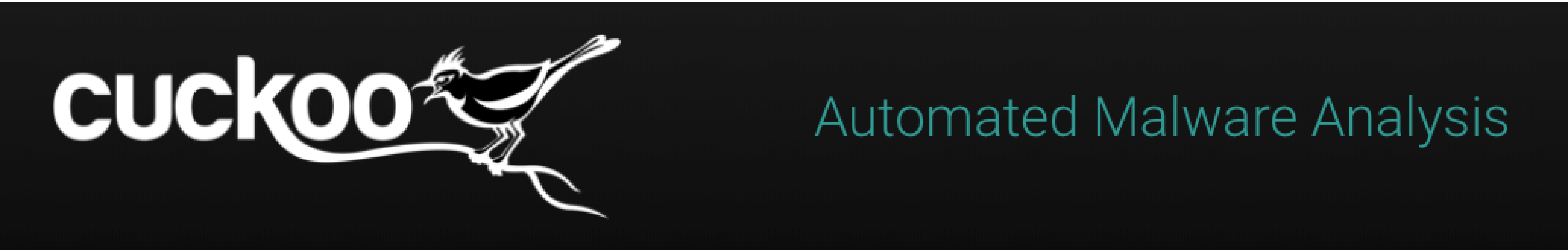
BE CAREFUL WITH THAT EXPLOIT POC

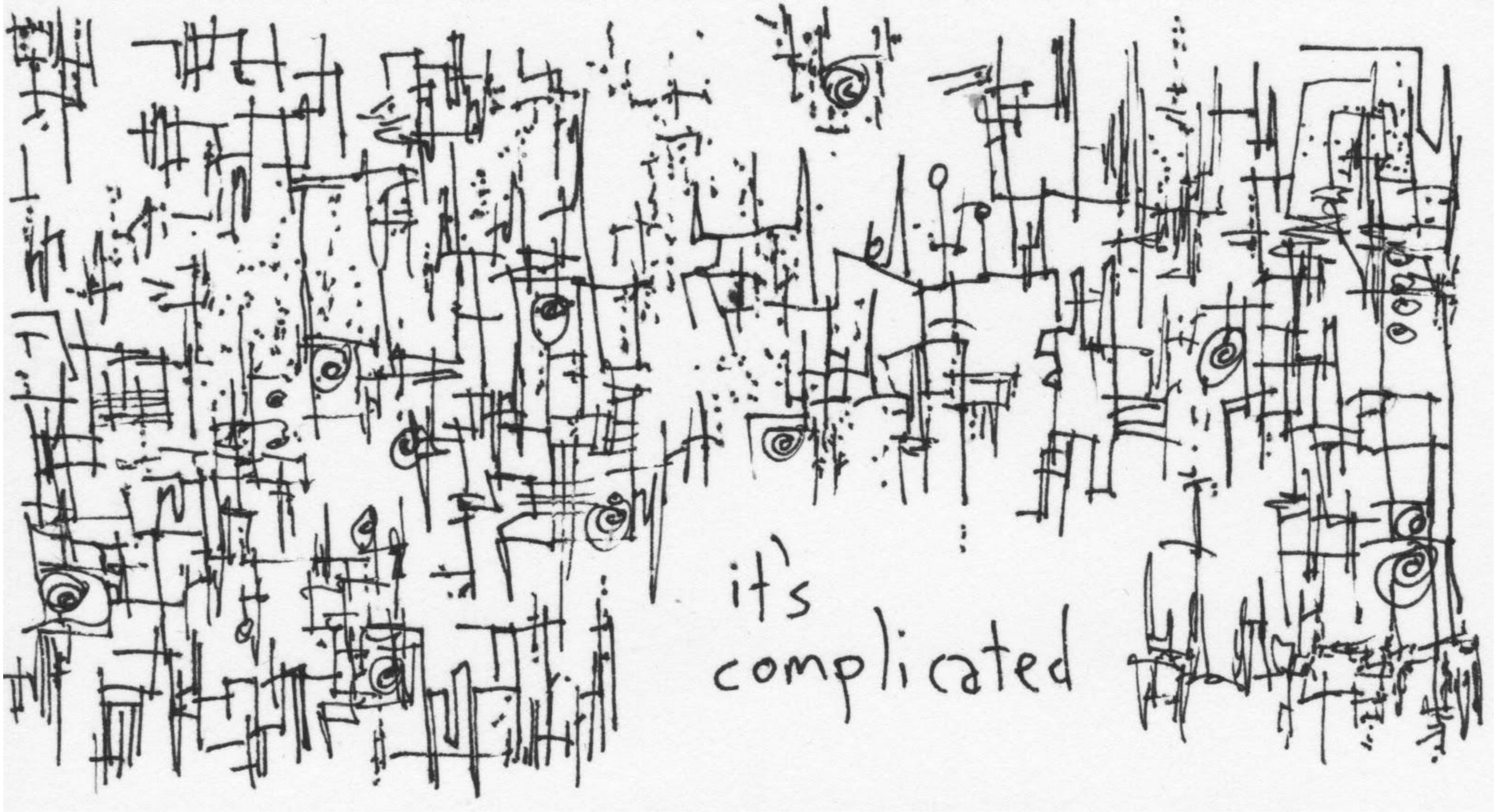


WannaCry hero Marcus Hutchins could face 40 years in US prison

Marcus Hutchins is reportedly being held in Nevada CREDIT: AP

DON’T LEAK SANDBOX TRAFFIC




it's
complicated

WE EXPECT TO TRAIN PEOPLE TO NOT BE PEOPLE?

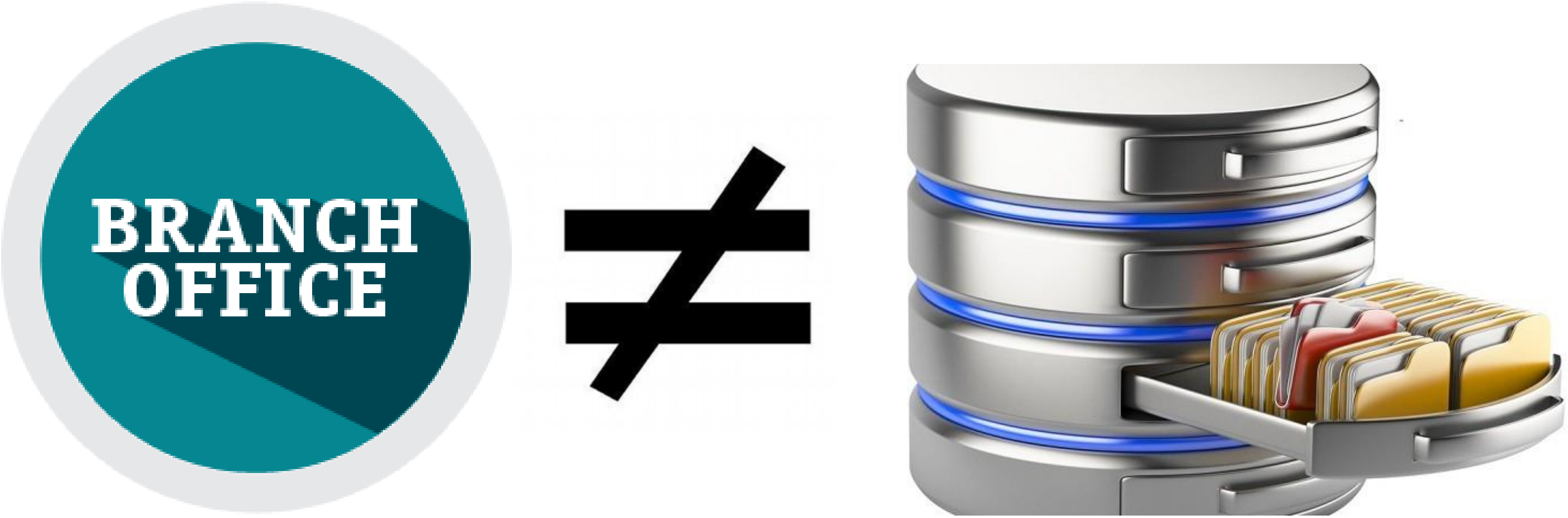
DO NOT PRESS
THIS BIG, SHINY
RED BUTTON

I HOPE WE ARE HERE TO ACCEPT AND ENCOURAGE CHANGE

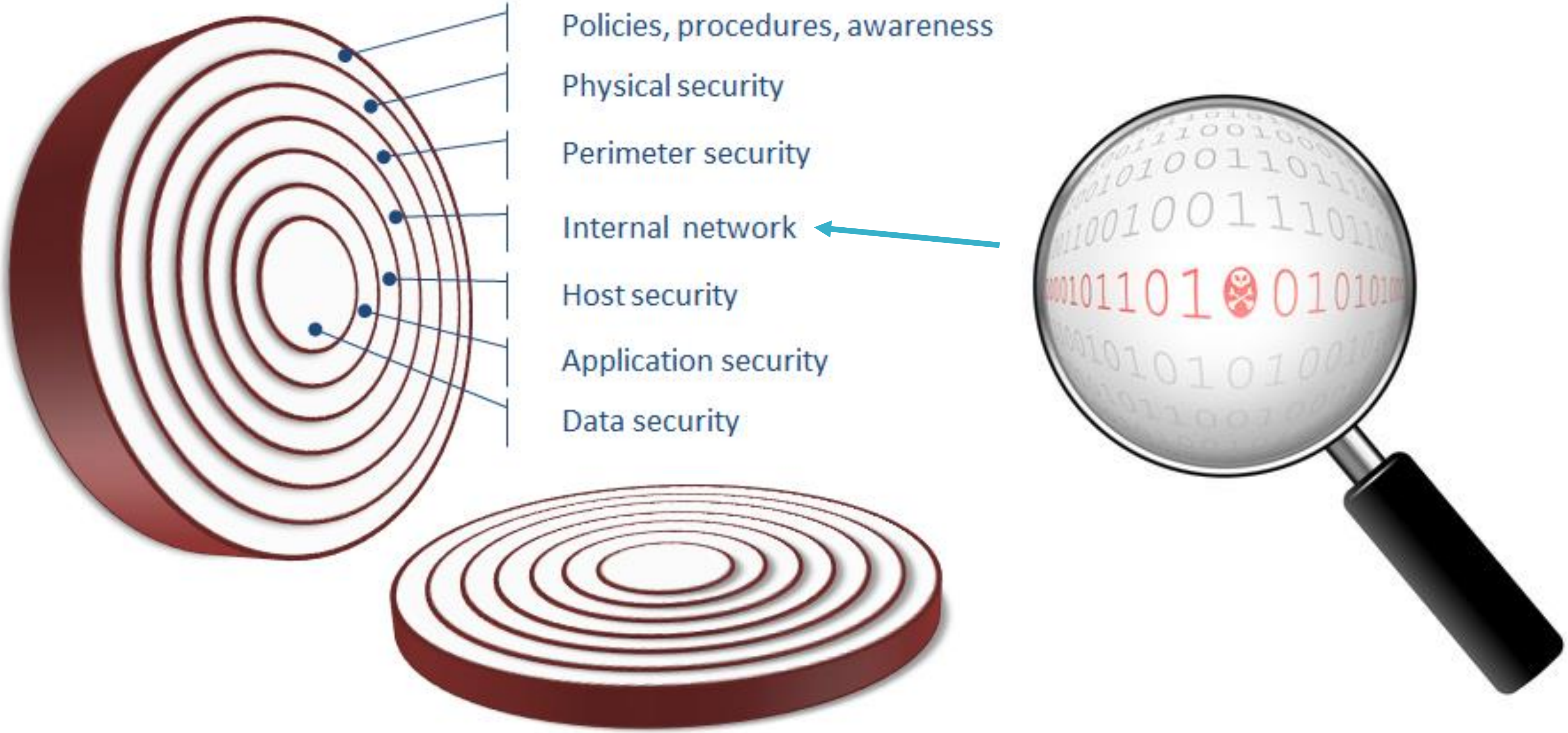
FIRST, LET'S TALK ABOUT RESOURCE SHORTAGE

What we have is a **shortage** in **companies investing in cyber security**

EVERYTHING IS NOT OF EQUAL VALUE



LAYERED SECURITY AND AT LEAST TWO CONTROLS AT EACH LAYER



Policies, procedures, awareness

Physical security

Perimeter security

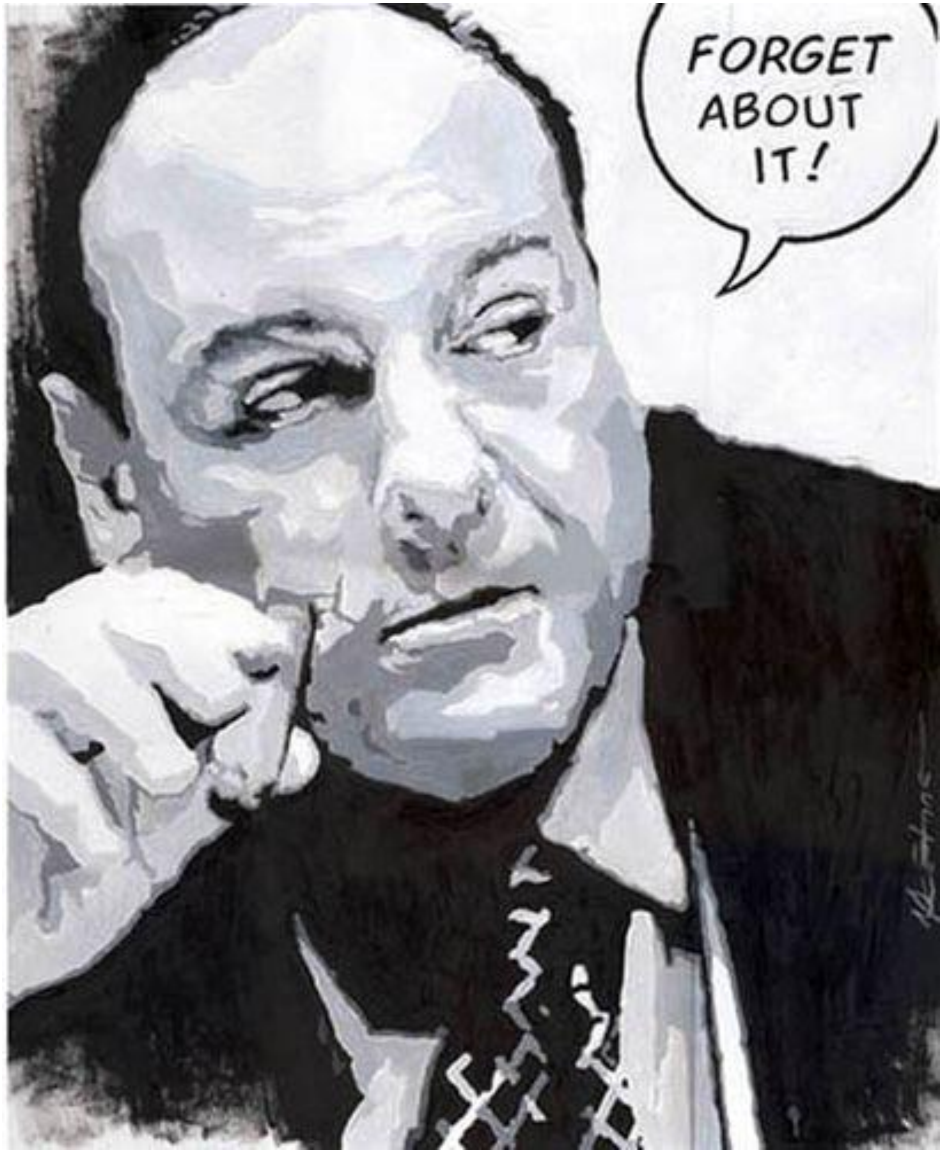
Internal network

Host security

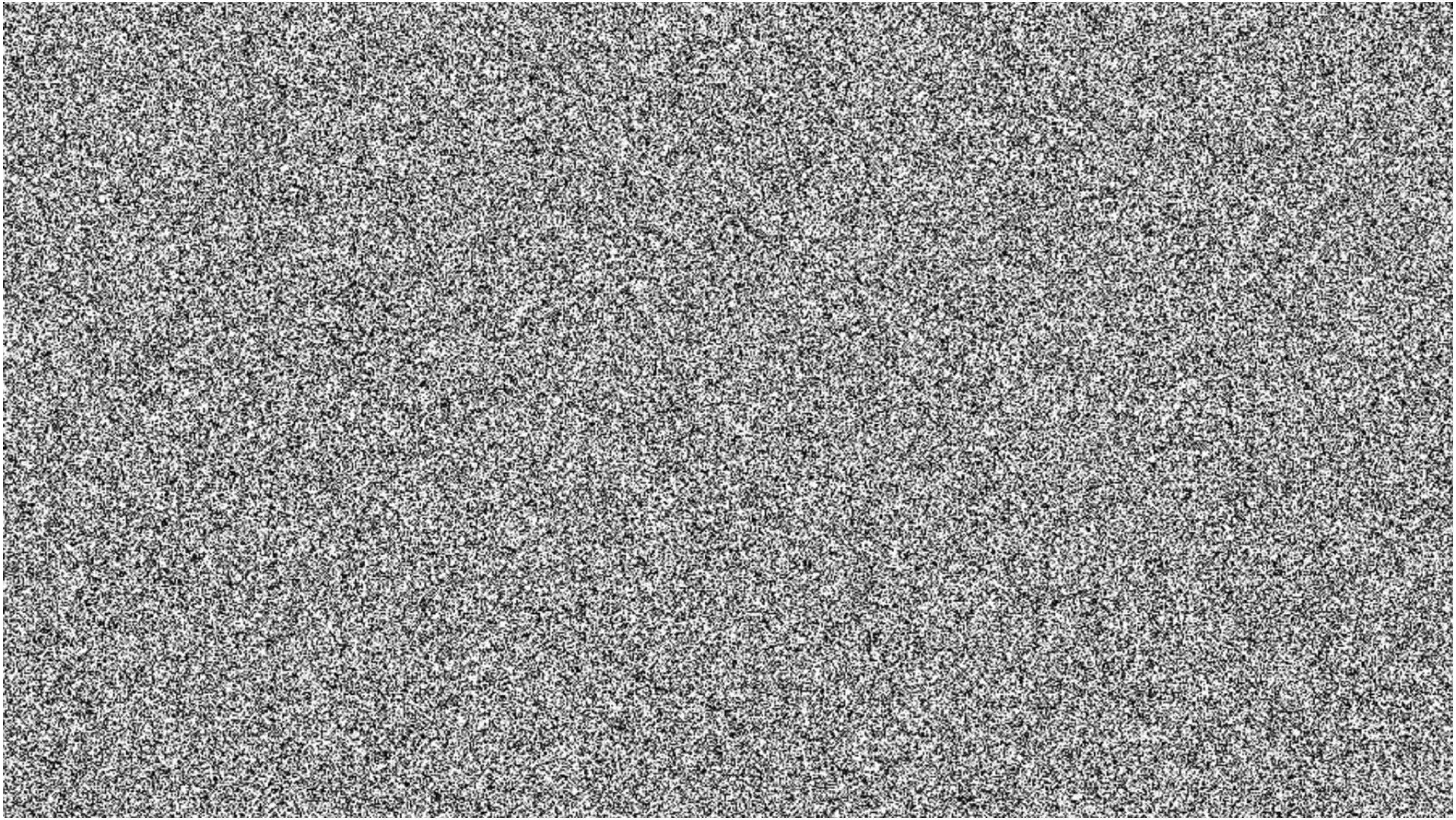
Application security

Data security

ATTRIBUTION IS USELESS

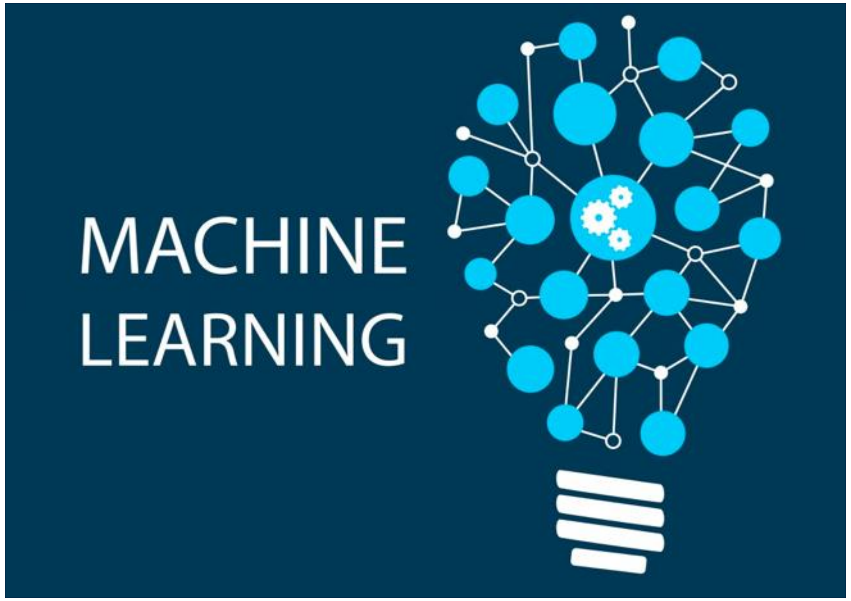


EVERYTHING IS COMPLEX, TOO NOISY

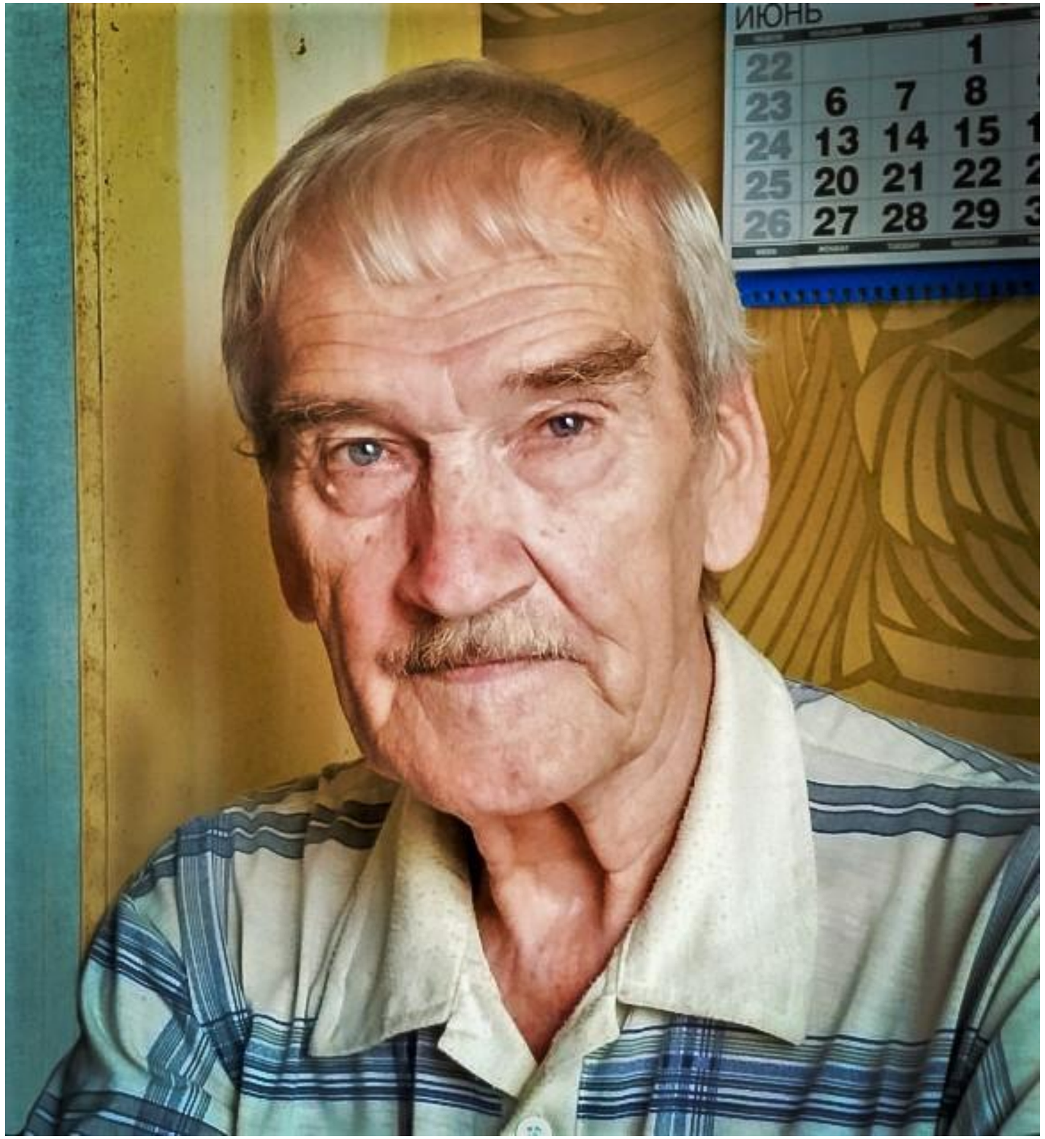


LET THE COMPUTERS TO THE PROCESSING

LET THE COMPUTERS TO THE PROCESSING



HOWEVER, YOU CAN'T BEAT HUMAN INTUITION



IN CLOSING

LET'S NOT PERPETUATE THE PROBLEMS

FOCUS, KNOW WHAT'S MOST IMPORTANT

ONE QUESTION FOR EVERY DECISION!

ixia

THANK YOU