III ENCUENTRO ENS

Ransomware: lecciones desde las trincheras

- **Speaker: Jess Garcia**
  - **Founder and CEO of One eSecurity**
  - **Twitter: @j3ssgarcia**

www.one-esecurity.com | www.ds4n6.io

En colaboración con:

Jess Garcia - Who am I?

Jess Garcia

@j3ssgarcia

- **Founder and CEO of One eSecurity, a global Digital Forensics and Incident Response (DFIR) company (~15 years).**
- **Leader of the DS4N6 project.**
  Visit: www.ds4n6.io
- **Senior Instructor at the SANS Institute (~20 years).**

Index

1. Who am I?
2. Statistics
3. Lessons from the trenches
4. Who is the enemy?
5. Demo: How ransomware is deployed in organizations and how to defend against it
6. Recovery and post – battle
7. Things to do when I'm back to office

Statistics

3/4 of ransom attacks end up in devices encryption.

26% of victims pay ransom.

311% increase in 2020.

94% gets data back (56% backups vs 26% payment).

8.7% of organizations receive a disclosure threat.

Statistics

- **1.5M** — phishing sites created every month.
- **2019** — Rise of 235% in 2019.
- **2020** — Rise of 150% in 2020.
- **$$ $$ $$** — Overall paying costs double than not paying (732k vs 1448k).
- **RaaS** — RaaS cost: 960$/year or 1200$ in 6 months.
- **50%** — out of 582 organizations admit not be ready.
- **287 days** — average days to fully recover from an attack.

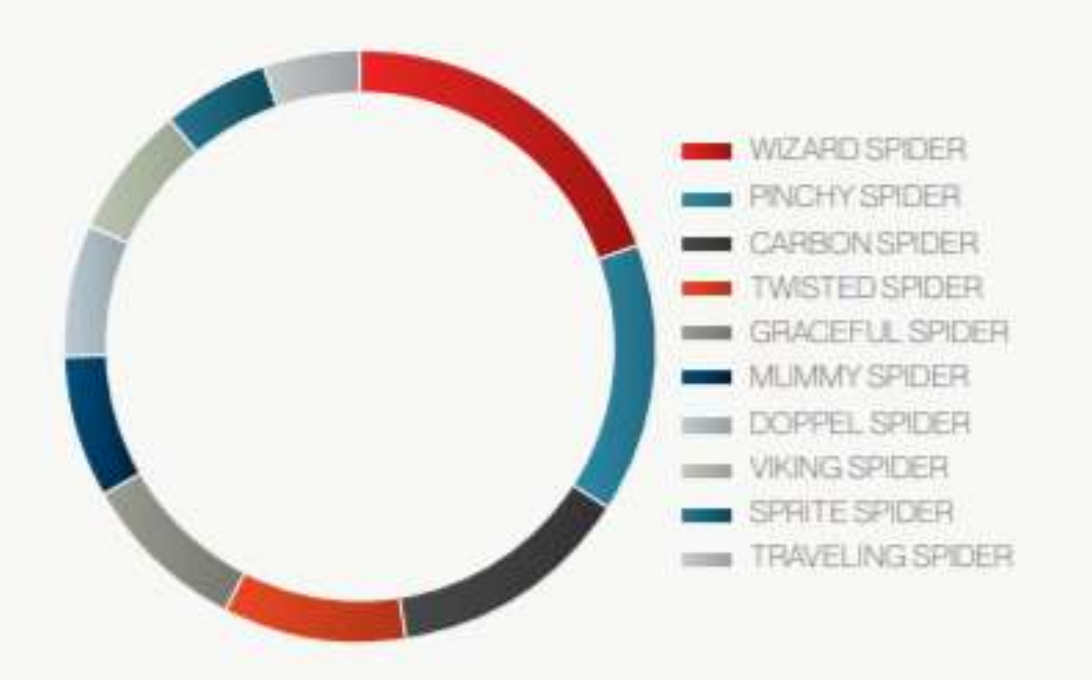
Lessons from the trenches

- Ransomware is the last step of the attack (**Big Game Hunting – BGH**)
- Actor has arrived 13 days before in average
- They want to get backups → If encrypted → Rise of probability of payment
- What can we do? Don't get paralyzed → Call your elite unit DFIR / Retainer
- In order to respond, we need to know the enemy…

Who Is the Enemy?

Groups

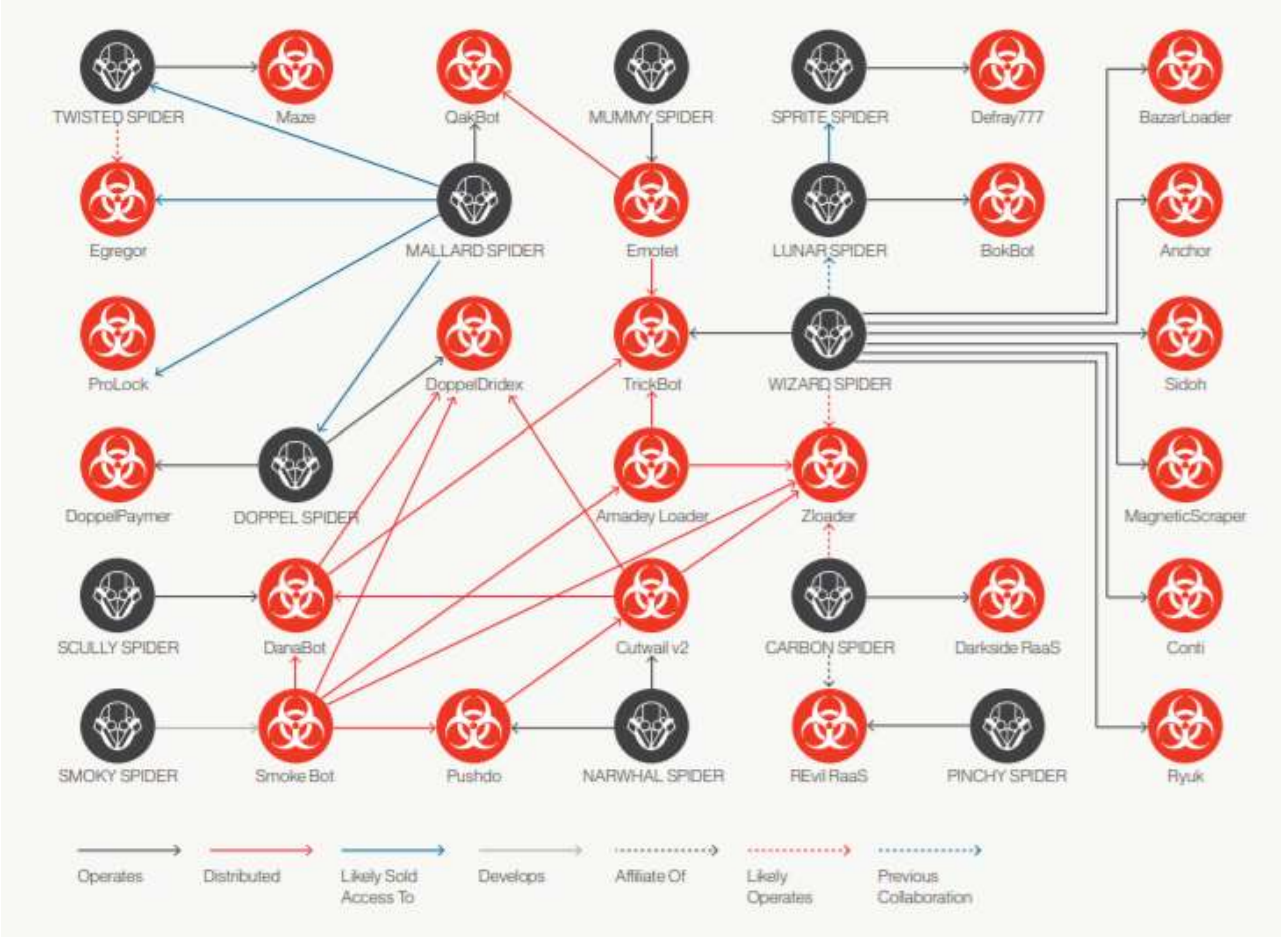
Wizard Spider (Ryuk / Conti)	Pinchy Spider (REvil/Sodinokibi)	Doppel Spider (DoppelPaymer ← BitPaymer fork)	Indrik Spider (BitPaymer)



2020 Maze stopped activity

2020 Takedowns:

- Egregor
- Netwalker
- Emotet



https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

Modus Operandi

Double extorsion after commitment

Don't give decryption key after ransom deployment

Wall of Shame: publish exfiltrated data

Intrusion - ransom deployment Time:
I. Depends on victim's size and attacker's skills.
II. Grim Spider is getting times between **2-5 hrs**

Attackers give between 24-72 hrs for payment

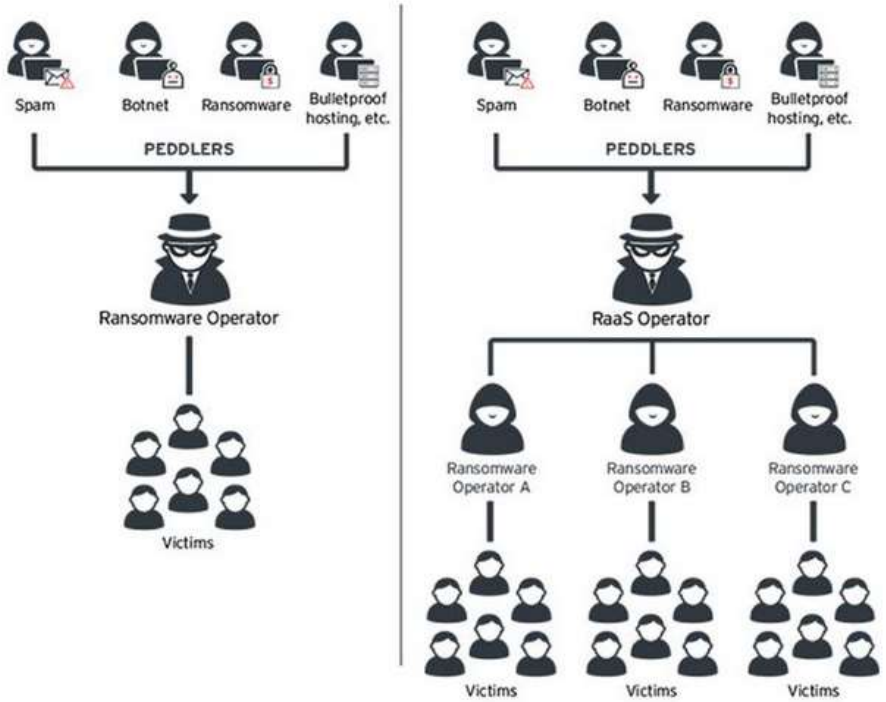
RaaS

Affiliates cooperate and share ransom payments

Developers get commisions around 30-40% of campaign payments

Affiliates get access to ransom and infraestructure.

Top RaaS: Ryuk, Lockbit, REvil, Maze



Typical ransomware operation versus RaaS

https://pbs.twimg.com/media/E15eRXGXoAI4fnU

TTPs

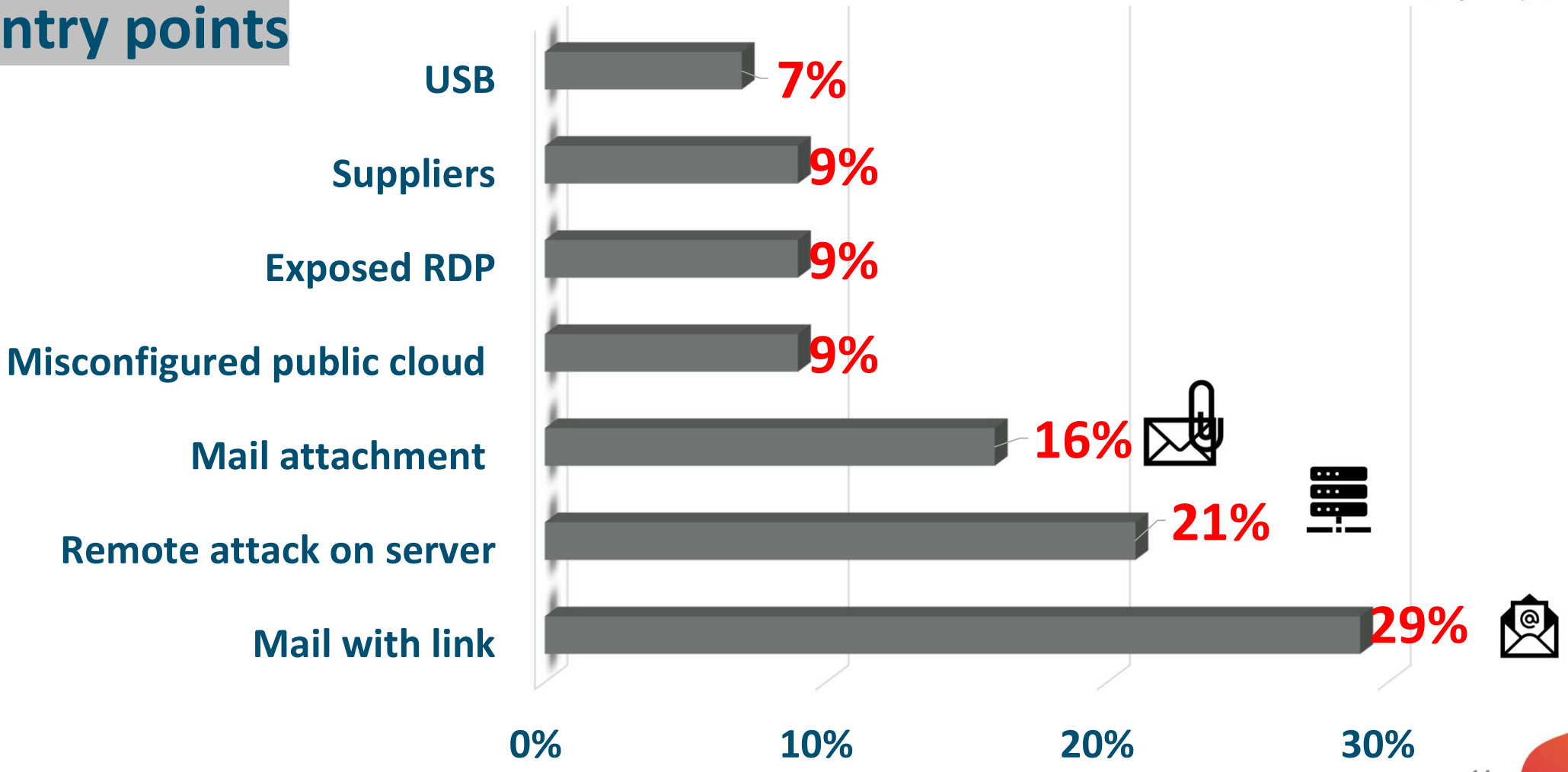
Identify TTP → Know possible actors

Password-Spraying RDP/SMB (vector de entrada más común)	Ofimatic document with macros (common entry point)	Dump credentials	Lateral movements
Disable backups / Shadow Copies	CVE-2020-1472 (Zerologon) ← Ryuk	CVE-2019-11510 (Pulse Secure Pulse Connect Secure) ← Sodinokibi	Information Exfiltration

Most commonly used tools

- **Colbalt Strike:** Pentest toolkit.
- **LaZagne**: Gathers credentials in a computer
- **PsExec:** Lolbin. Remote admin though SMB
- **ADfind:** CLI tool for AD querying
- **Bloodhound:** Find compromise paths & weaknesses in AD
- **CrackMapExec:** Automate asessing AD security
- **KeeThief:** Gets Keepass passwords from memory
- **Rubeus**: Tool for Kerberos interaction and abuse
- **Powerview:** powershell recon tool

Entry points



Entry points

90 seconds

time a new RDP port is discovered after first connecting to the Internet

4.7 million

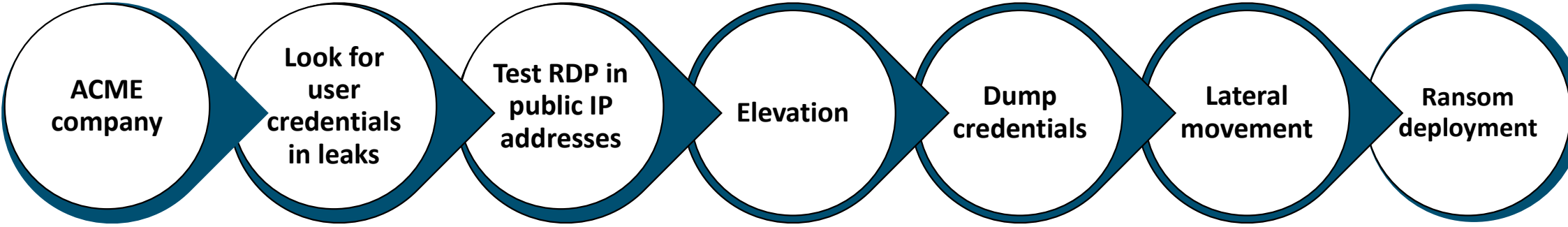
misconfigured RDP ports

1 in 3000

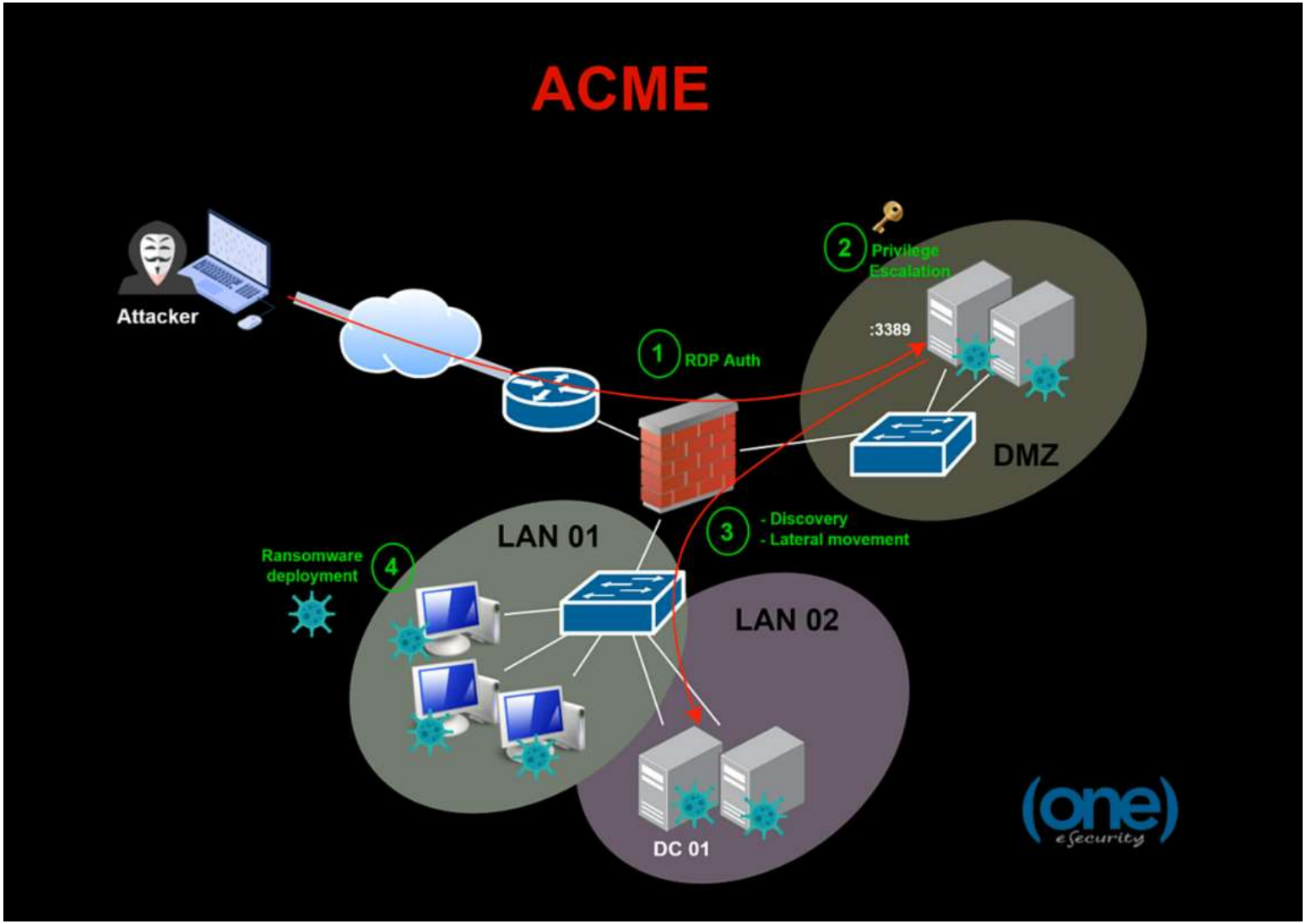
mail messages contains malware.

BIG GAME HUNTING DEMO

How ransomware is deployed in organizations and how to defend against it



Demo: Scenario



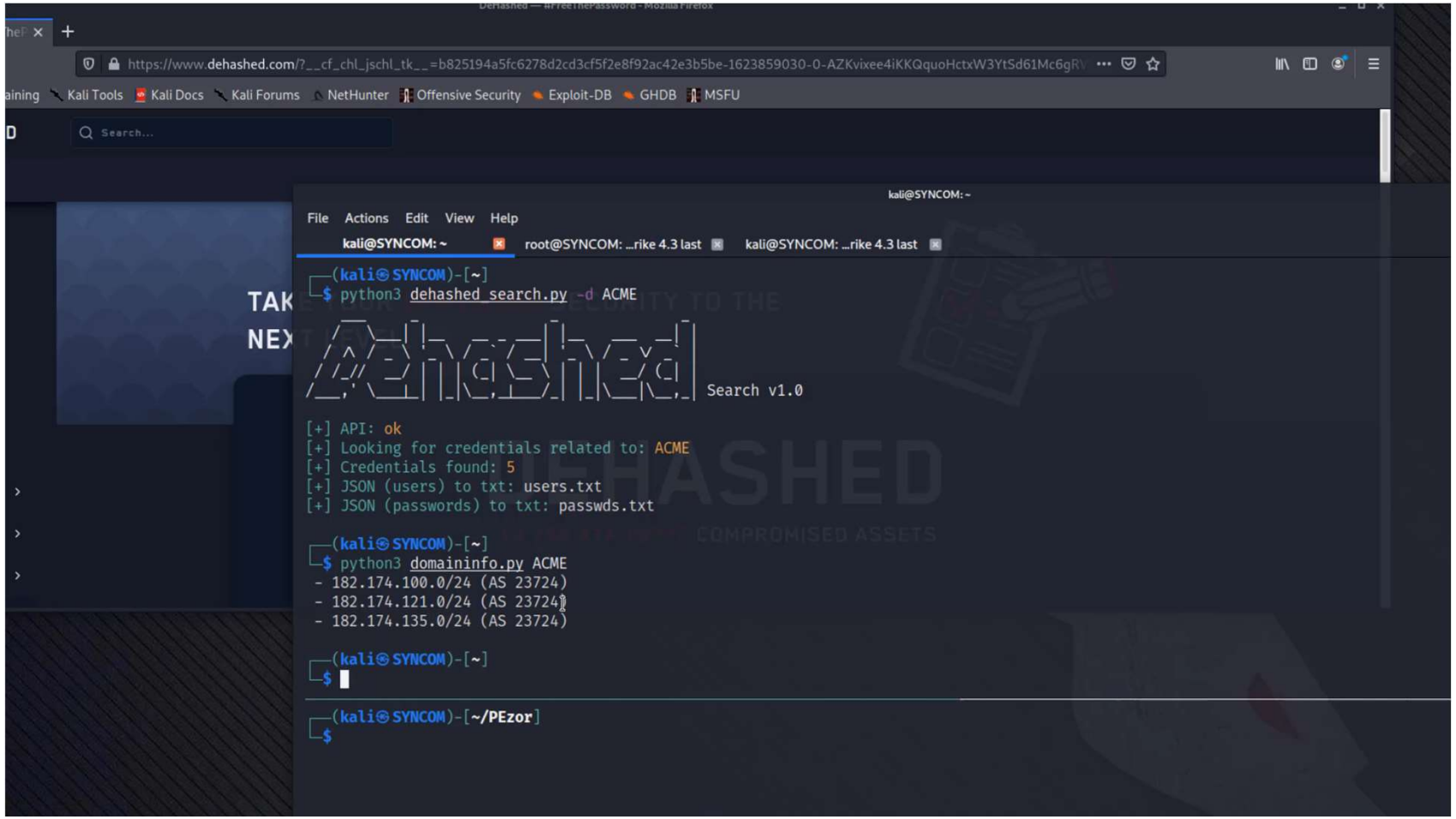
Exploration

- ✓ Exposed actives
- ✓ Public breaches
- ✓ Accidental leaks

Exploration

Lessons from the trenches

- ✓ Vigilance in Shodan/Censys/GitHub
- ✓ Automate notifications
- ✓ Raise user awareness
- ✓ Poison information


https://www.dehashed.com/?__cf_chl_jschl_tk__=b825194a5fc6278d2cd3cf5f2e8f92ac42e3b5be-1623859030-0-AZKvixee4iKKQquoHctxW3YtSd61Mc6gR
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
kali@SYNCOM: ~
File Actions Edit View Help
kali@SYNCOM: ~
root@SYNCOM: ...rike 4.3 last
kali@SYNCOM: ...rike 4.3 last
(kali㉿SYNCOM)-[~]
$ python3 dehashed_search.py -d ACME
Search v1.0
[+] API: ok
[+] Looking for credentials related to: ACME
[+] Credentials found: 5
[+] JSON (users) to txt: users.txt
[+] JSON (passwords) to txt: passwds.txt
(kali㉿SYNCOM)-[~]
$ python3 domaininfo.py ACME
- 182.174.100.0/24 (AS 23724)
- 182.174.121.0/24 (AS 23724)
- 182.174.135.0/24 (AS 23724)
(kali㉿SYNCOM)-[~]
$
(kali㉿SYNCOM)-[~/PEzor]
$

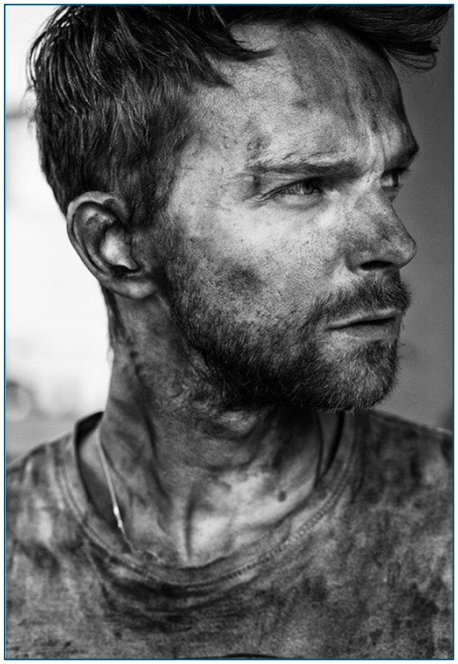
Landing: Point

- ✓ Phishing/maldoc, 29% in 2020
- ✓ Antispam platform have problems with (zip,7z..) and domain fronting
- RDP - 52% of attacks
- Citrix / External access: 17 % of attacks

Landing Point

Lessons from the trenches

- ✓ **PREVENT**: Limits in mail platform, admin rights in computers, awareness simulations
- ✓ **DETECT**: Anomalous Parent-children processes relationships / Proxy logs / Impossible trip / VPN Intelligence / Delivery threshold / Machine names
- ✓ **RESPONSE**: Bulk deletion, mail rules
- ✓ **PREVENT**: 2FA 2FA 2FA!
- ✓ **DETECT**: multiple IP one user, multiple users one IP, VPN



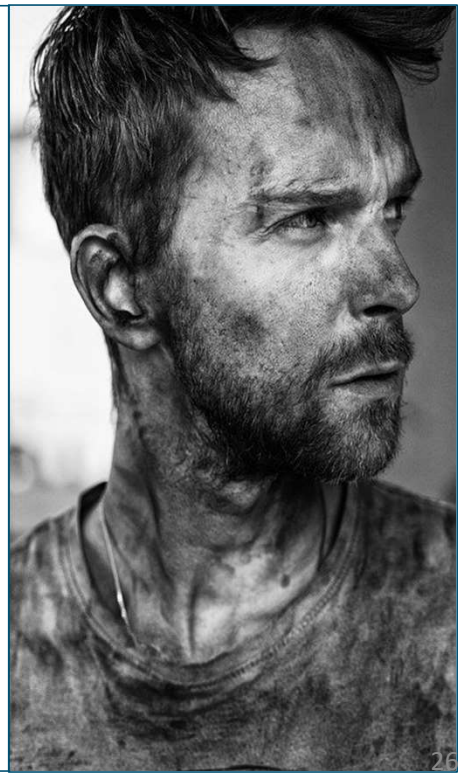
Infiltration behind enemy lines

- Lateral movement
- psexec / RDP
- We observed 50% of our cases psexec, 50% RDP
- Dump credentials > admin server > domain admin

Infiltration behind enemy lines

Lessons from the trenches

- ✓ **PREVENT:** Network Segmentation, Admin Rights Control, LAPS
- ✓ **DETECT:**
  - ✓ psexec from client
  - ✓ honey users
  - ✓ default tools config: root in windows
  - ✓ command line first actions
  - ✓ sysvol honeys
- ✓ **RESPONSE:**
  - ✓ Isolation
  - ✓ blocks& passwords changes



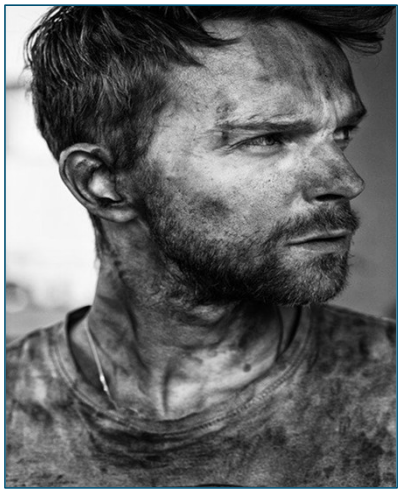
Espionage

- Data exfiltration
- Used for extorsion

Espionage

Lessons from the trenches

- ✓ **PREVENT:** Limit access to sensitive data
- ✓ **DETECT:** Anomalous traffic volume, 1×1 pixel honey doc
- ✓ **RESPONSE:** Restrict access to information, Request takedown, Invalidate credentials



Detonation

- Compromise a domain controller > deploy ransomware

Detonation

Lessons from the trenches

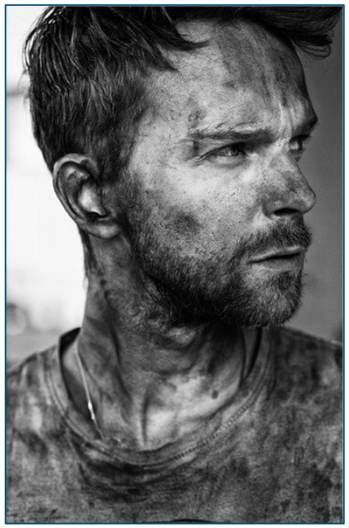
- Early contention:
  - Block even when you don't know were the enemy comes from
  - Protect the Backup Soldier!
- What if my sysadmin/DFIR team are at home?
- Do you have remote access domain independent?

- What do we tell users? Careful with the press!
- Am I legally forced to notify to the regulator?
- Is Business involved? **They** decide:
  - Tourniquets
  - Take down times
  - Crown jewels

Recovery and post-battle

Lessons from the trenches

- ✓ Backups: protect and isolate them. Before recovering, we must be sure of first compromise date.
- ✓ Rebuild DC –> change krbtgt password twice, Use dirty network → Clean network approach
- ✓ Report writing



When You Are Back in the Office:

1. Review VPN/Citrix users without 2FA
2. Search yourself in Shodan
3. Consider deploying LAPS
4. Identify abandoned domain admins
5. Auto AD assessments: Bloodhound / DPAT

   AND...

6. **BACKUP BACKUP BACKUP!!!** (and keep them safe!)

(one) eSecurity

Detection · Response

www.one-esecurity.com | www.ds4n6.io

Thank You!

En colaboración con:

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

FEMP 40 AÑOS Poder Local