

How Secure Is Your Environment? Hacker Perspectives...



Who We Are



an atos company

whoami

Contact Details

Yves Pellaton

Senior Security Consultant | Team Lead

SEC Consult (Schweiz) AG

Freilagerstrasse 28 | 8047 Zurich | Switzerland

P +41 44 271 77 70

y.pellaton@sec-consult.com | www.sec-consult.com

SEC DEFENCE 24/7 EMERGENCY HOTLINE: +41 44 545 10 85
ADVISOR FOR YOUR INFORMATION SECURITY.

[website](#) | [blog](#) | [twitter](#) | [xing](#) | [linkedin](#)



an atos company

an atos company

Berlin | DE
Bochum | DE
Munich | DE
Nürnberg | DE

Luxembourg | LX
Zurich | CH

Vienna | AT | HQ EMEA
St. Pölten | AT
Linz | AT
Wiener Neustadt | AT

Bangkok | TH

Kuala Lumpur | MY

Singapore | SG | HQ APAC

- SEC Consult branches
- SEC Consult customers

8 countries | 3 continents

SEC Consult Service Portfolio



TECHNICAL SECURITY ASSESSEMENTS

(Web) Application Security
Mobile Security
IT Infrastructure Security
Security for SAP Services
IoT and Embedded System Security
Security Code Review



SEC Defence



CONTINUOUS SECURITY TESTING



RED TEAMING



PROZESS MANAGEMENT FOR INFORMATION SECURITY

Information Security Management
Data Protection Management



SEC Trainings



SECURE SOFTWARE DEVELOPMENT CONSULTING



an atos company

SEC Consult Vulnerability Lab



The Attackers



an atos company

The Hackers

Profiles of attackers

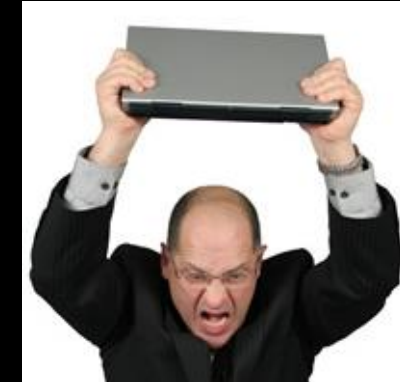
Script Kiddies



Hacktivists



Internal Threats



Cyber-Crime-as-a-Service Organized Criminal Gangs



Competitors



Nation States



The Hackers

Attacker vs. Defender

The Attacker...

- can choose the weakest point(s)
- can probe for unknown vulnerabilities
- can strike at will
- can play dirty
- many free software/tools available

The Defender...

- must defend all points
- can defend only against known attacks
- must be constantly vigilant
- must play by the rules
- mainly expensive software available



an atos company

The Process



an atos company

Steps to hack a large organization

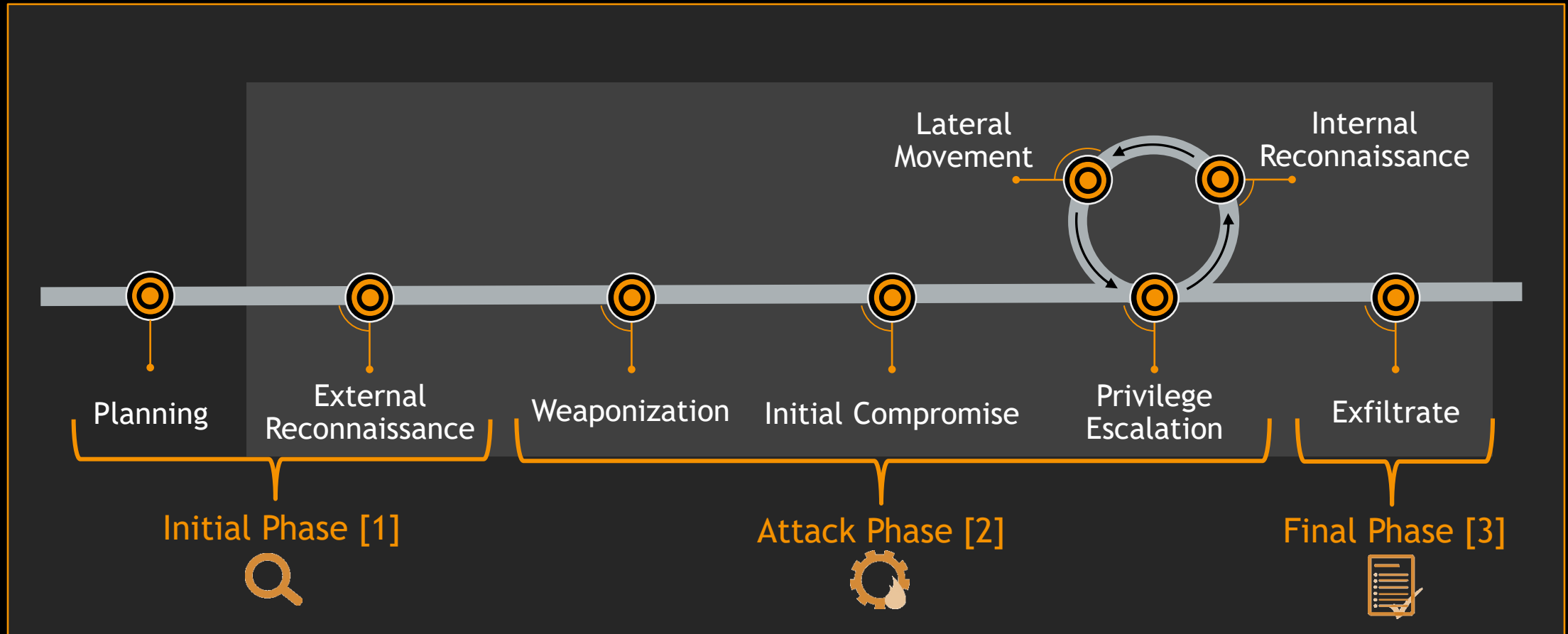
The Process

What are the typical steps involved in hacking a large organization?



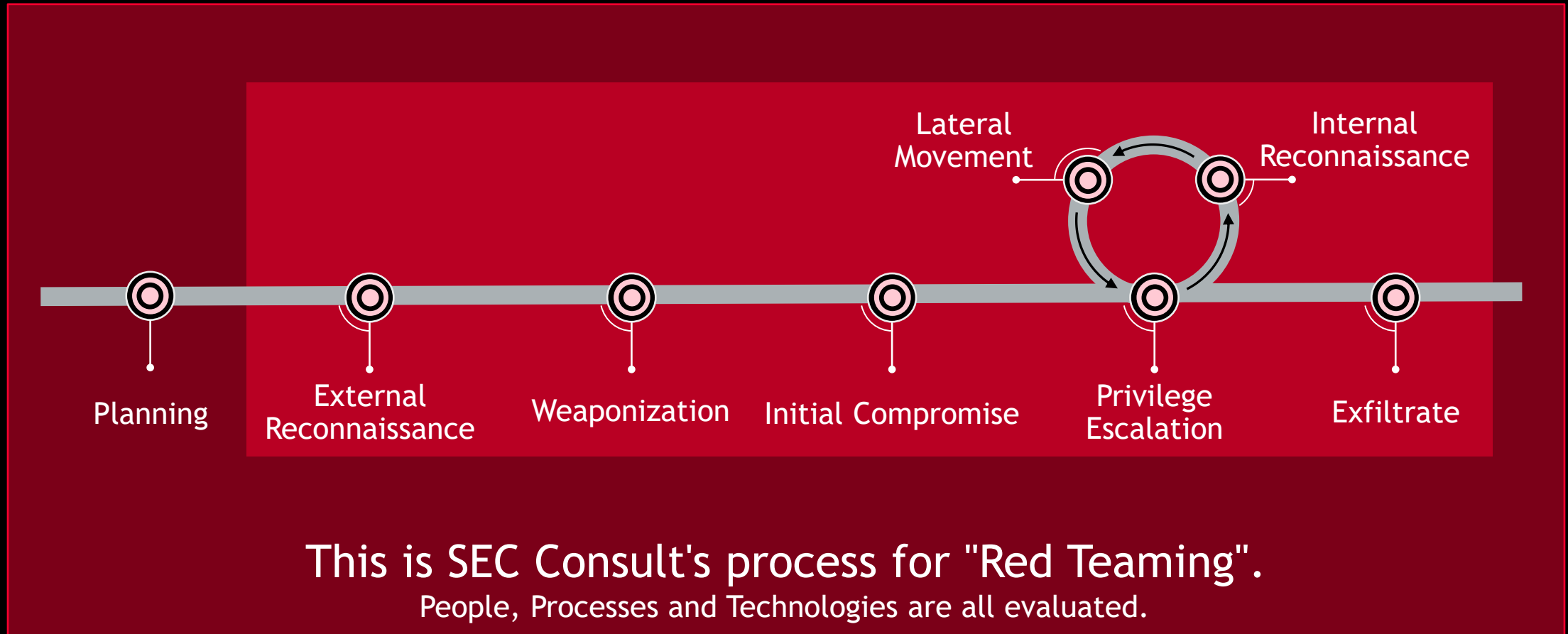
The Process

Anatomy of a targeted attack



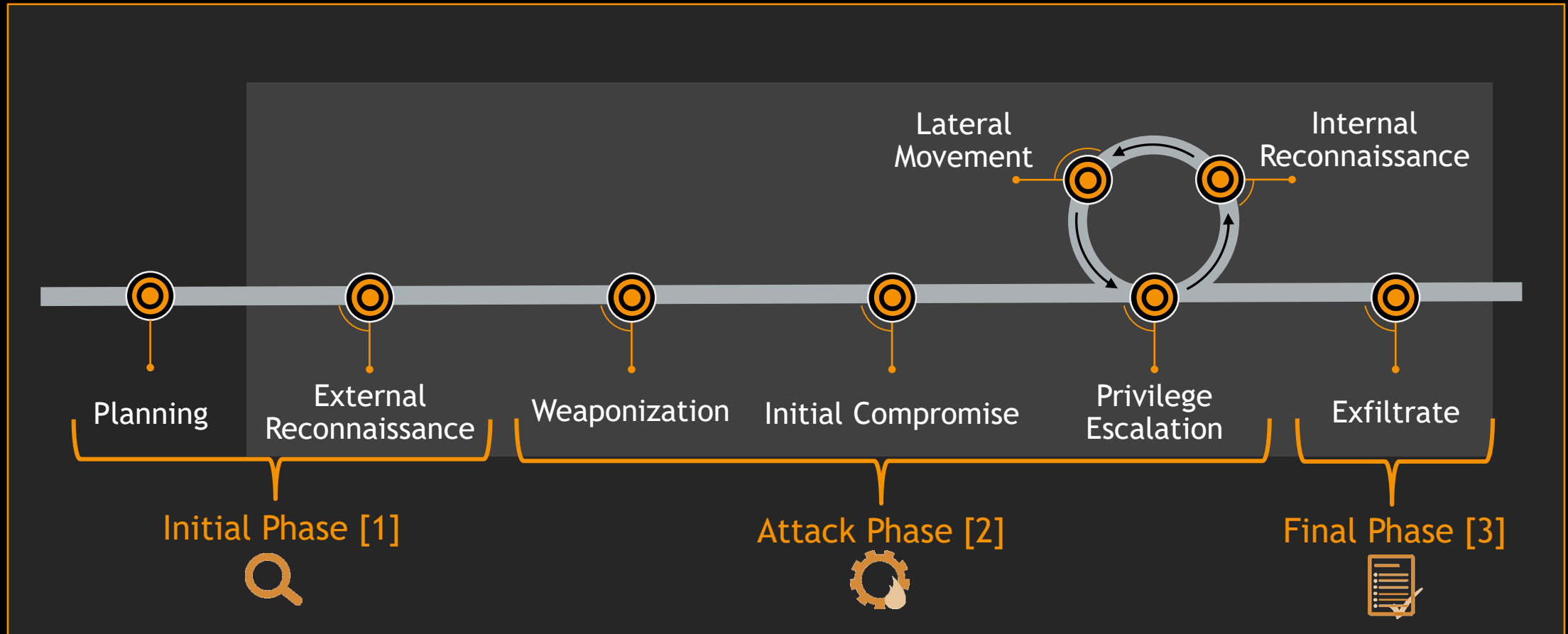
The Process

Anatomy of a targeted attack



The Process

Anatomy of a targeted attack



Hacker Perspectives Phishing Campaign



Hacker Perspectives

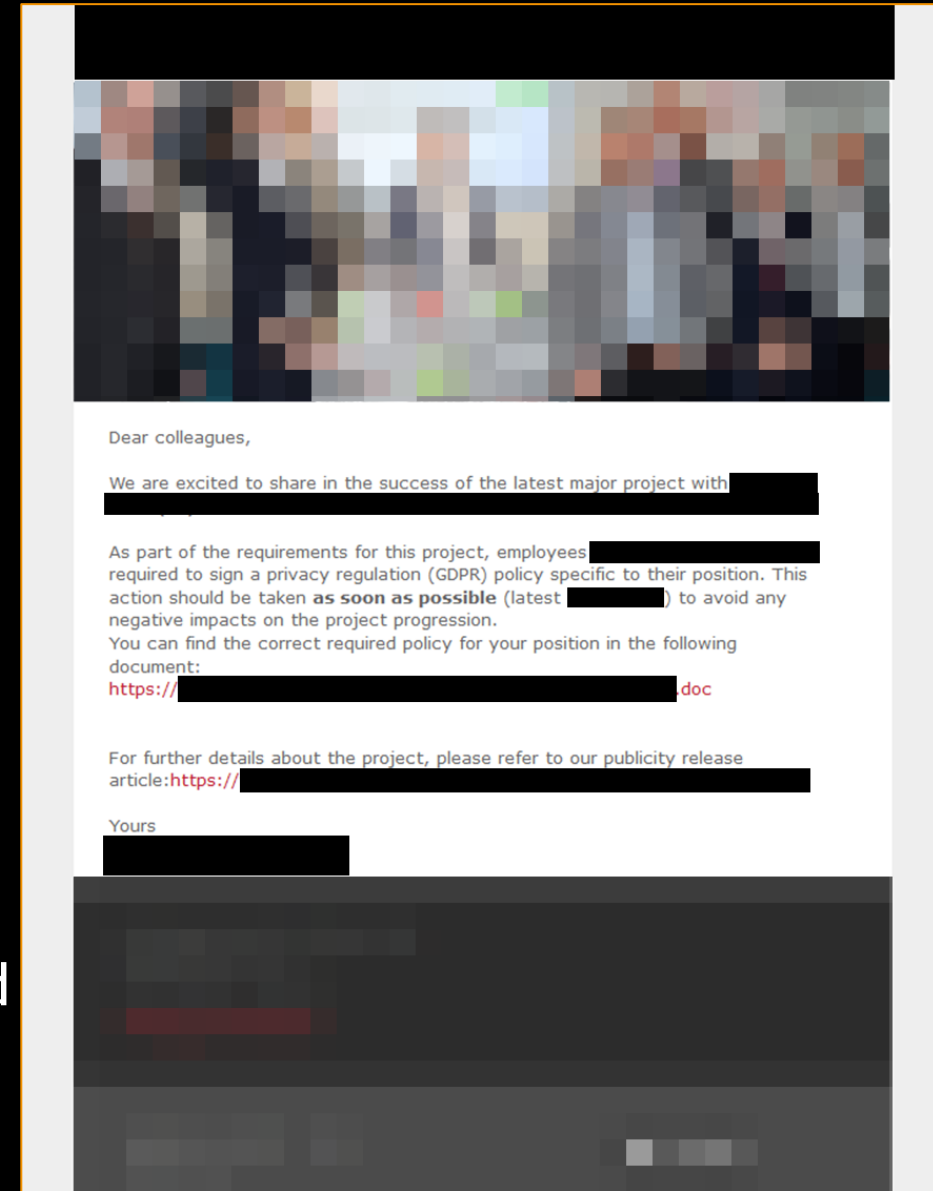
Phishing Campaigns

Phishing Emails remains a **widely used attack vector**.

Spear-Phishing Emails become more and more difficult to spot on the first look.

Combining actual public announcements (new managers, new contract wins, new processes, new awards) along with time pressure on the email, recipients **remain an efficient recipe for success**.

The trap can be a **malicious document or file** to download or a **login page** where the user has to provide their name, password and potentially also MFA information.



Hacker Perspectives

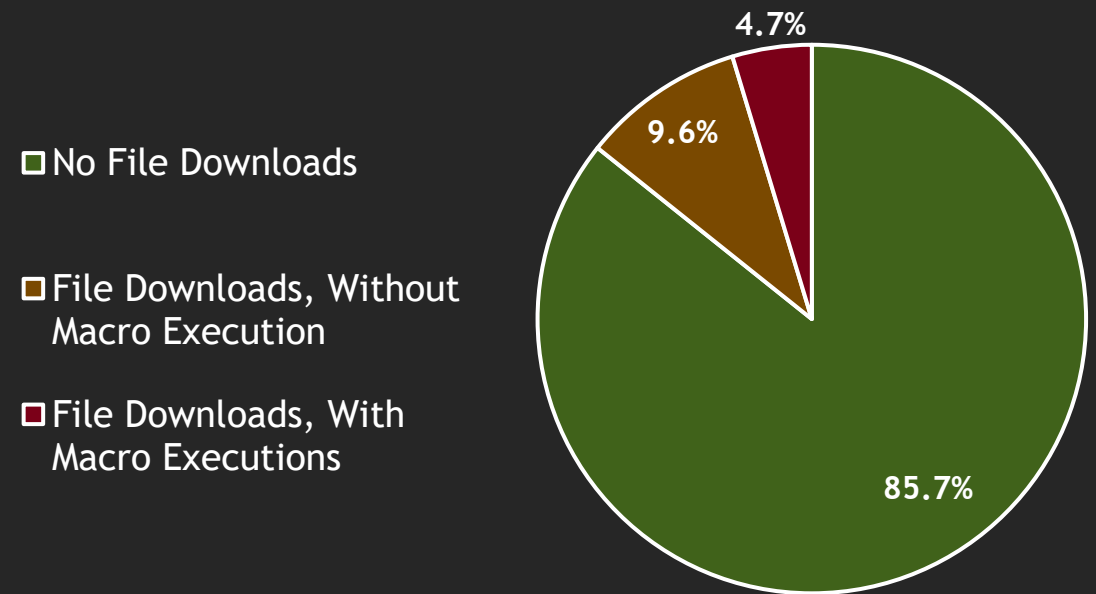
Phishing Campaign

A Phishing Campaign is an efficient **method to measure the awareness** within a team or a company.

However, even when the results are better than average, **just one compromised employee/machine is enough** for APTs and skilled attackers to start compromising the whole infrastructure.

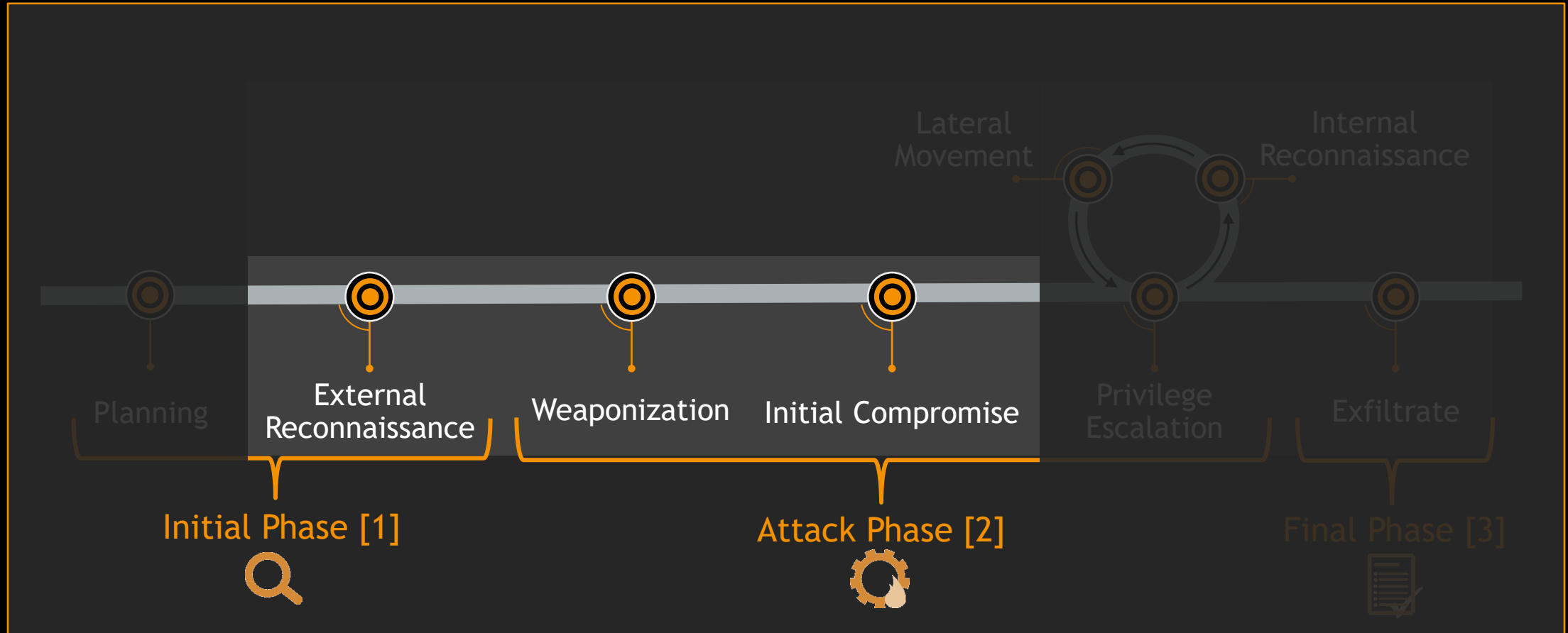
Everyone can fall for a properly prepared spear-phishing email. Unfortunately, conventional **MFA cannot protect the users** in case a **transparent reverse proxy** is used, for example like with "Modlishka", "Muraena / Necrobrowser" and "Evilginx2".

Phishing Campaign Statistics



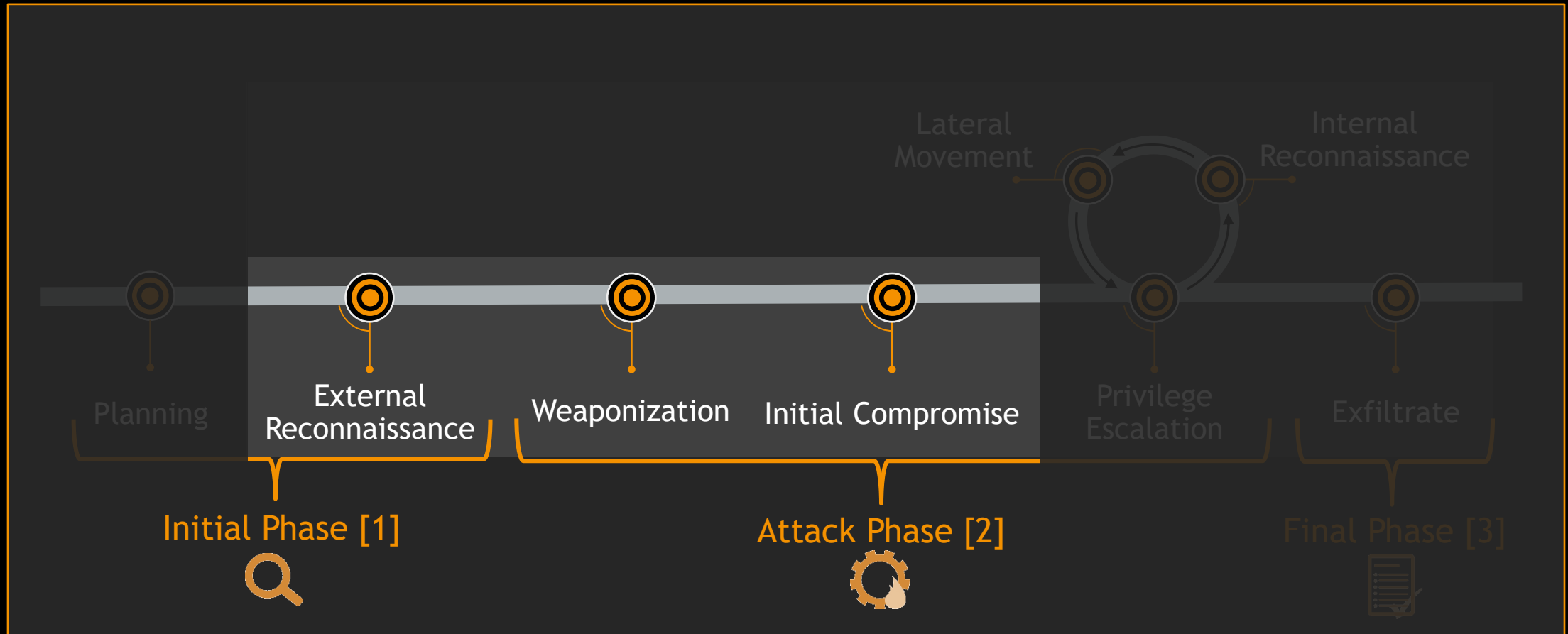
Hacker Perspectives

Phishing Campaign



Hacker Perspectives

Physical Intrusion



Hacker Perspectives Applications



Hacker Perspectives

Applications

Companies are using different **standard and dedicated software** to offer various internal and external services.

Those **applications are abused by attackers to gain an initial foothold** in the company network or to collect confidential information.

For example, web applications count for approximately **25%** of the attack paths involving data breaches¹.

As another example, SAP is used within more than **91%** of all Forbes 2000 companies for activities like HR, Finance, Controlling, Sales, Product Planning and Quality Management, therefore collecting critical information.



¹ <https://www.verizon.com/business/resources/reports/dbir/interactive/>

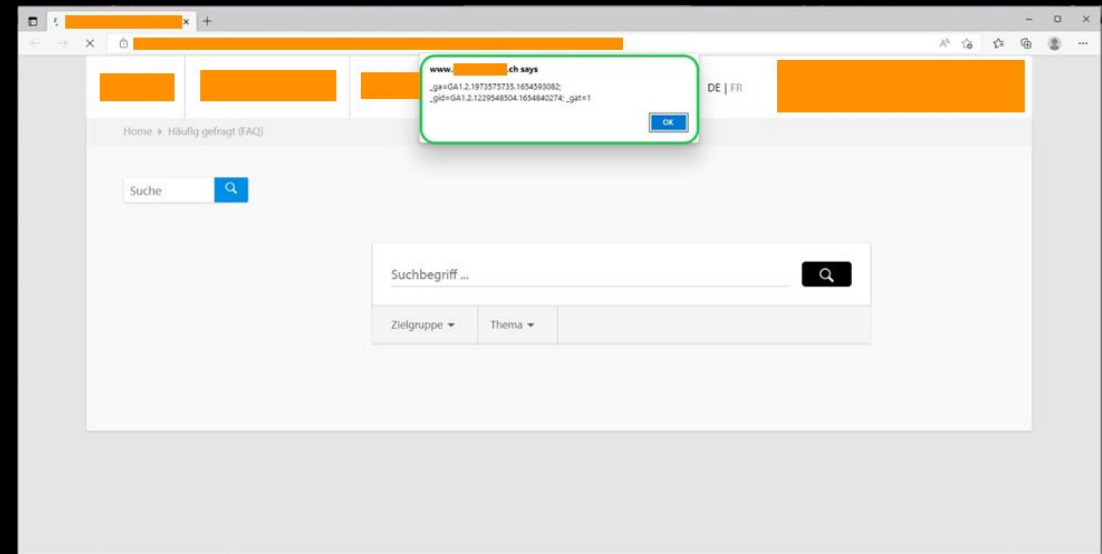
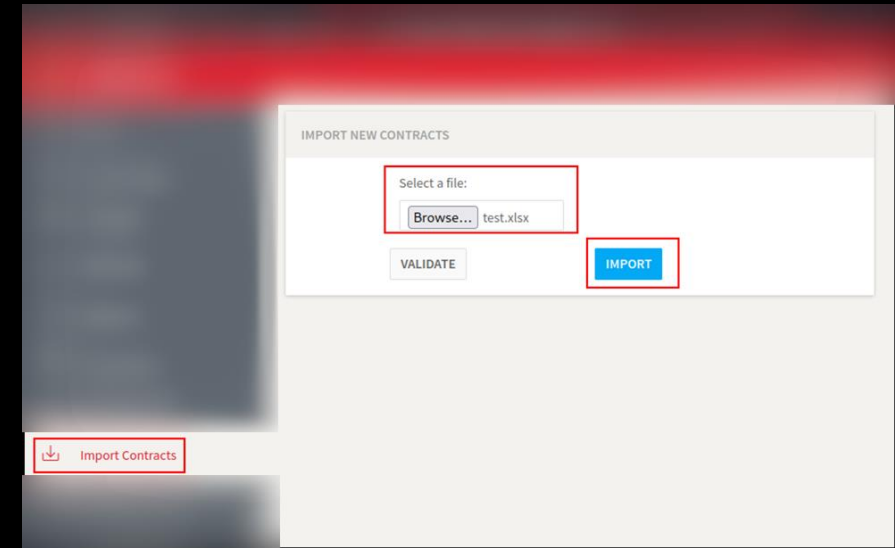
Hacker Perspectives

Applications

Web Applications

Attackers will try to compromise **internet-facing computers or services**. The weakness can be a bug or a design vulnerability. These applications are often websites, and depending on the flaw being exploited, this **can lead to data leakage or even full server compromise**, providing the attackers with a foothold within the company network.

Front-end, back-end, APIs and so on all have their advantages and disadvantages regarding their security aspects.



Hacker Perspectives

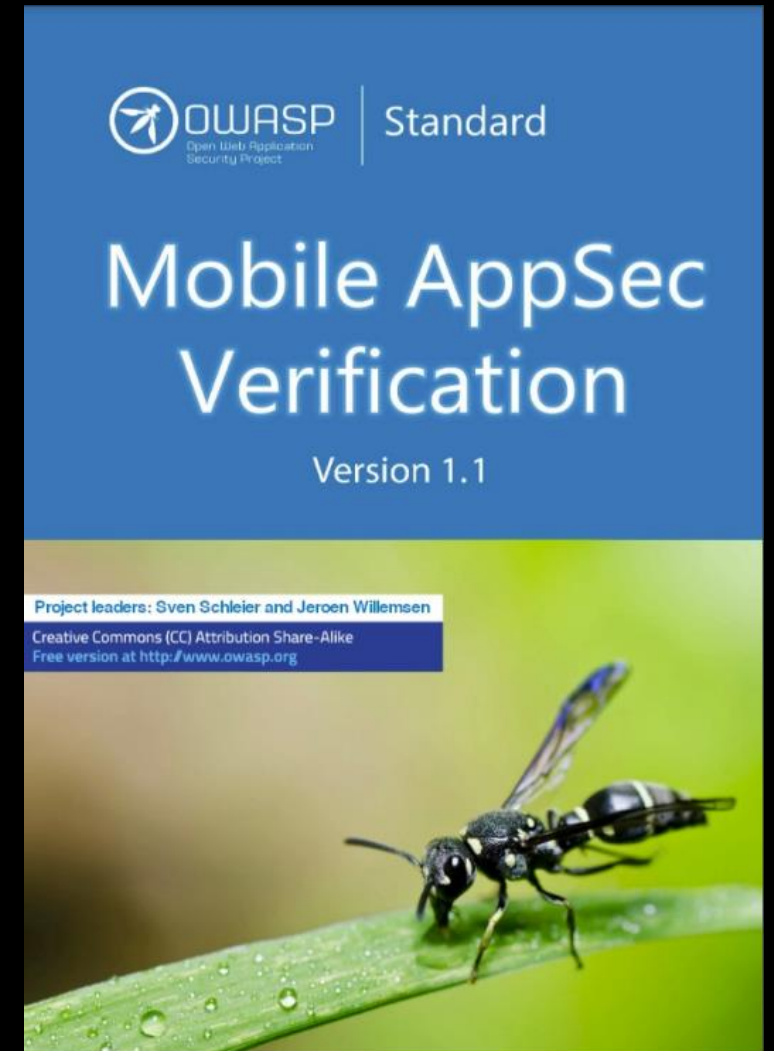
Applications

Mobile Security

Nowadays, over 50 percent of **business PCs are mobile**, and the increase in Internet of Things (IoT) devices poses new **challenges to network security**. Consequently, IT must adapt its approach to security.

A network security plan must account for all of the different locations and uses that employees demand of the company network, but some simple steps can be taken to improve mobile devices security.

Securing mobile devices requires a **unified and multilayered approach**. While there are core components to mobile device security, every approach will be slightly different.



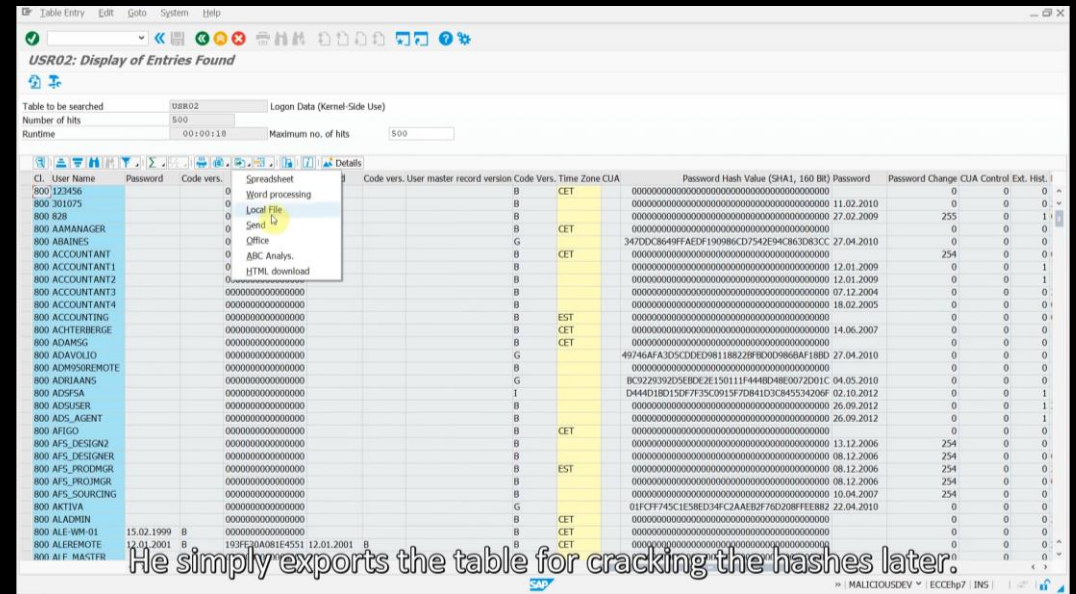
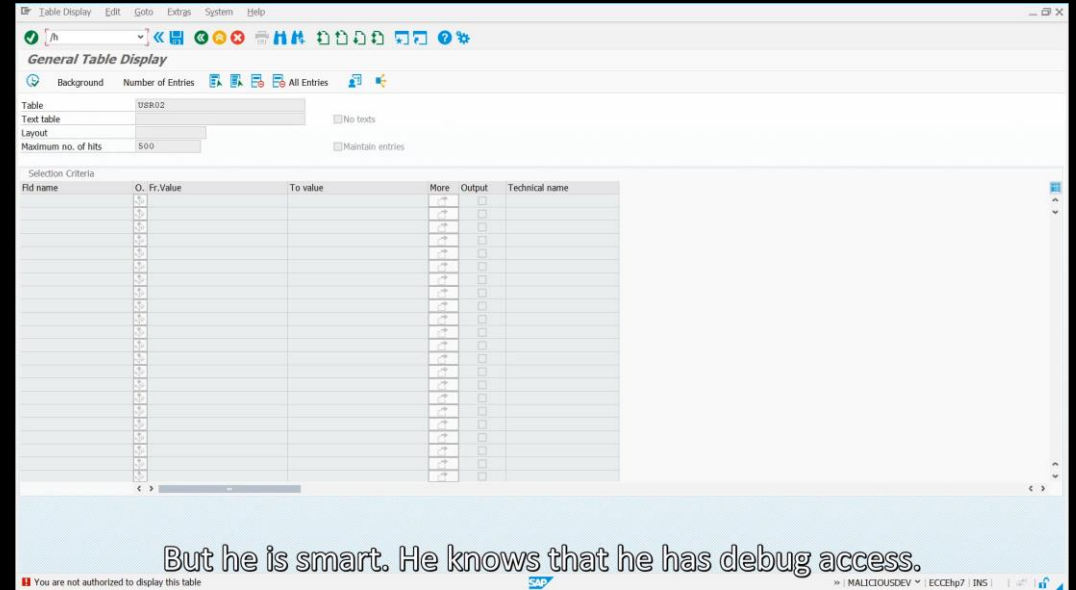
Hacker Perspectives

Applications

SAP Services

SAP is a highly complex system and there are countless possible vulnerabilities. If a vulnerability is identified, it is most likely a critical one. This is linked to the fact that these systems often contain transaction data, salary data and much more. The confidentiality, integrity and availability of these systems are very substantial for companies.

When testing happens in a production environment, it is important to understand the effect of every step performed, avoiding data corruption and data loss, except if it is the goal.



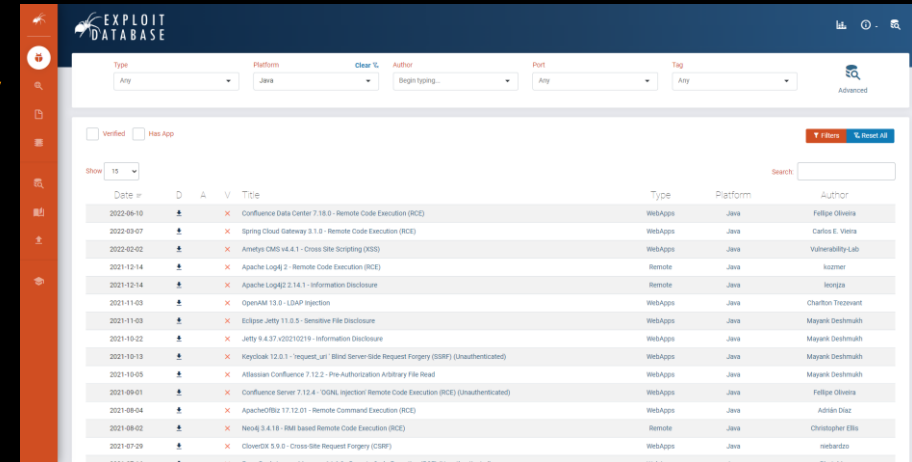
Hacker Perspectives

Applications

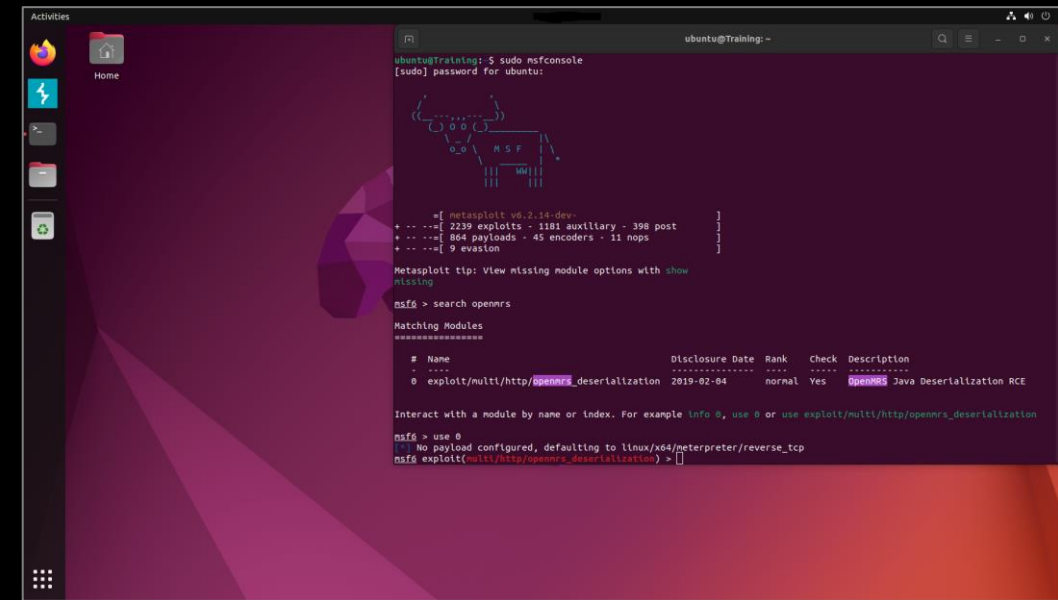
Application Security assessments allow to identify security issues related to data collected or distributed by the application. In the worst case, the application host, and therefore the internal infrastructure of a company, can be compromised.

The hackers will preliminarily look for known and unpatched vulnerabilities based on the available information. They will also aim to bypass any authentication and/or authorization mechanism.

Application security is an important aspect of every company and certainly the most used attack vector beside social engineering¹.



Date	D	A	V	Title	Type	Platform	Author
2022-09-10				Confurence Data Center 7.18.0 - Remote Code Execution (RCE)	WebApps	Java	Felix Oliveira
2022-09-07				Spring Cloud Gateway 3.1.0 - Remote Code Execution (RCE)	WebApps	Java	Carlos E. Viana
2022-02-02				Ameyra CMS v4.1.1 - Cross Site Scripting (CSS)	WebApps	Java	Vulnerability-Lab
2021-12-14				Apache Log4j 2 - Remote Code Execution (RCE)	Remote	Java	Wagner
2021-12-14				Apache Log4j 2 14.1 - Information Disclosure	Remote	Java	Vongsa
2021-11-03				OpenAM 13.0 - LDAP Injection	WebApps	Java	Charlton Trezvant
2021-11-03				Eclipse Jetty 11.0.5 - Sensitive File Disclosure	WebApps	Java	Mayank Deshmah
2021-10-22				Jetty 9.4.37-v20210219 - Information Disclosure	WebApps	Java	Mayank Deshmah
2021-10-13				Keycloak 12.0.1 - Inquest_Lat - Blind Server-Side Request Forgery (SSRF) (Unauthenticated)	WebApps	Java	Mayank Deshmah
2021-10-05				Alfresco Confluence 7.12.2 - Pre-Authentication Arbitrary File Read	WebApps	Java	Mayank Deshmah
2021-09-01				Confurence Server 7.12.4 - 'OGNL' Injection Remote Code Execution (RCE) (Unauthenticated)	WebApps	Java	Felix Oliveira
2021-08-04				ApacheORBit 17.12.01 - Remote Command Execution (RCE)	WebApps	Java	Adrian Diaz
2021-08-02				Neo4j 3.6.18 - RMI based Remote Code Execution (RCE)	Remote	Java	Christopher Ellis
2021-07-29				CloverDK 5.0.0 - Cross Site Request Forgery (CSRF)	WebApps	Java	nebrando



```
msf6 > search openrns
Matching Modules
=====
# Name                                     Disclosure Date  Rank  Check  Description
- - - - -
0 exploit/multi/http/openrns_deserialization 2019-02-04      normal Yes    openrns Java Deserialization RCE

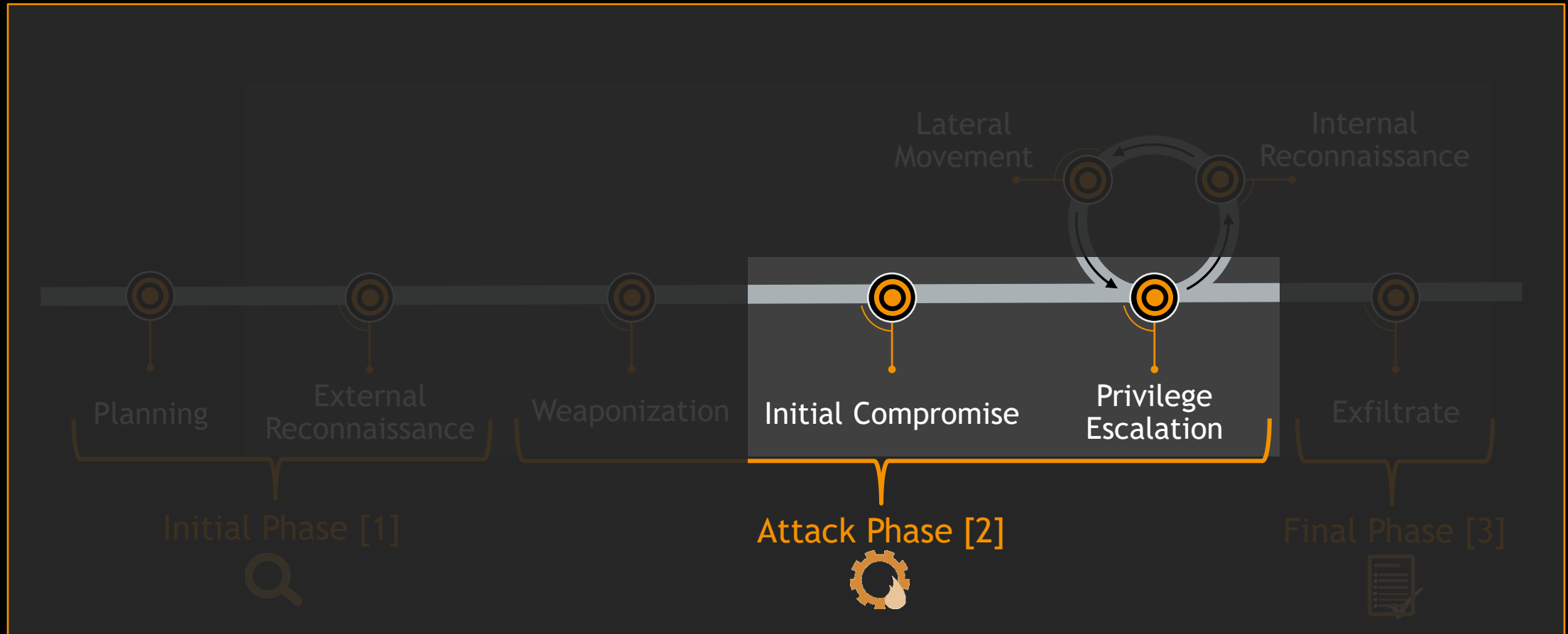
Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/openrns_deserialization

msf6 > use 0
[*] No payload configured, defaulting to linux/x64/peterpreter/reverse_tcp
msf6 exploit(multi/http/openrns_deserialization) > []
```

¹ <https://www.verizon.com/business/resources/reports/dbir/interactive/>

Hacker Perspectives

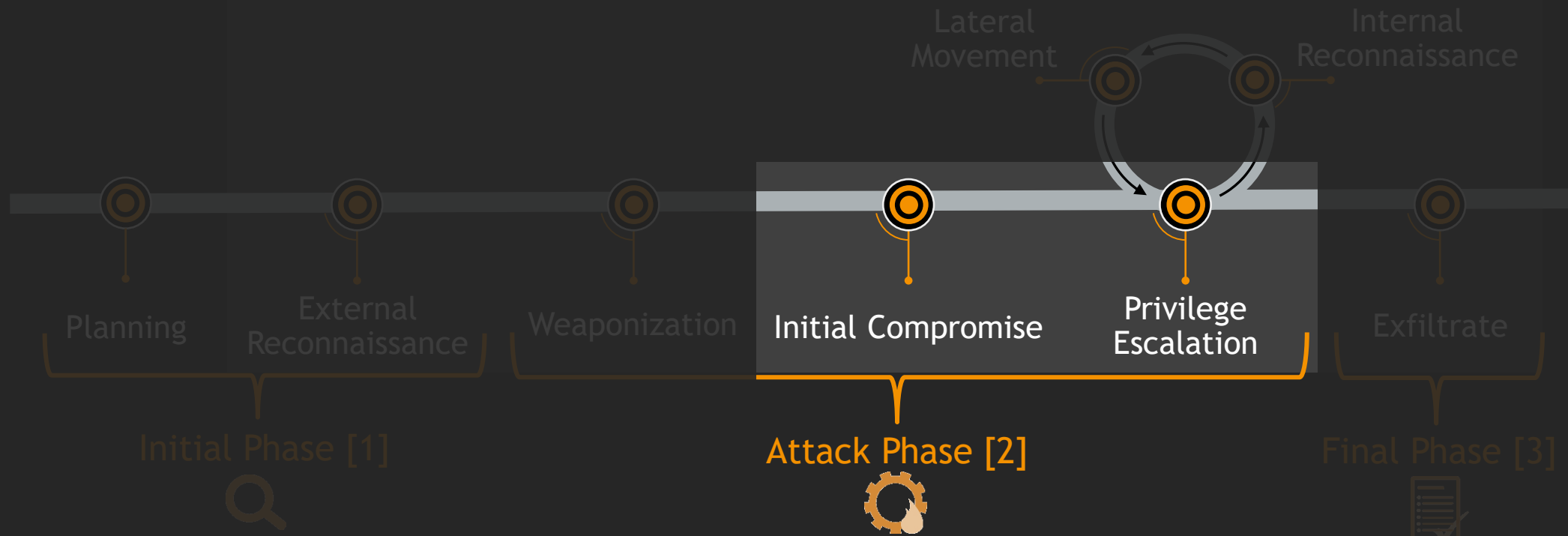
Applications



Hacker Perspectives

Applications

Those are also the scope of bug-bounty programs.



Hacker Perspectives Internal Infrastructure

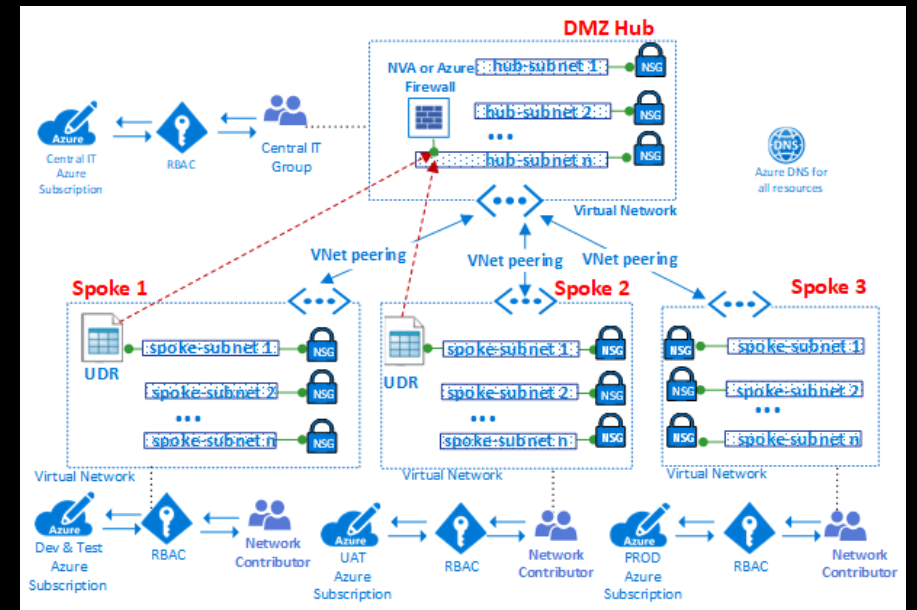


Hacker Perspectives

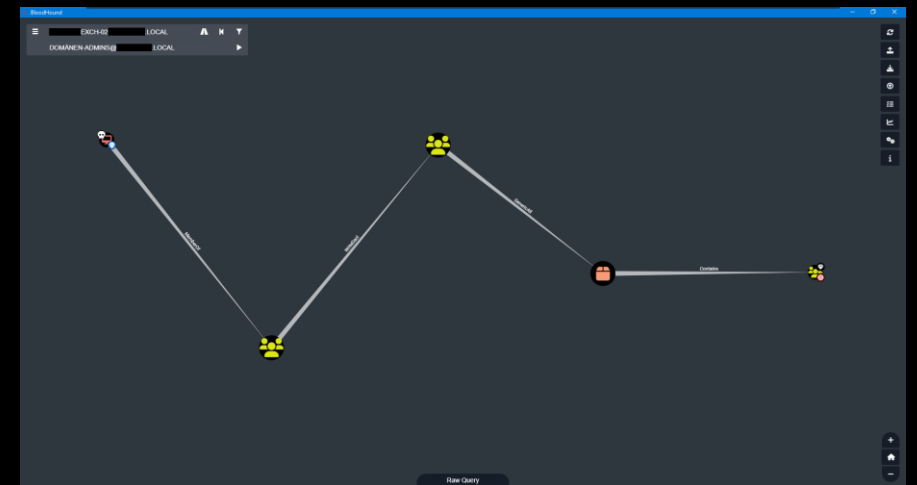
Internal Infrastructure

DMZ, Backup, Management or HR networks are part of **internal infrastructure**. Most companies use **Active Directory** in order to manage their **servers, computers, users and access controls**. From flat to micro-segmented networks, each solution has advantages and disadvantages regarding management, visibility and security.

Kerberoast, ADCS issues, readable Domain Controller backups, local administrator **password reuse** and **trust relationships** are all common paths used by **attackers** to **gain administrative privileges** within corporate environments, allowing them to **steal secrets**, compromise backups and **deploy ransomware**.



Source: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/_images/vdc/networking-infrastructure-high-level.png



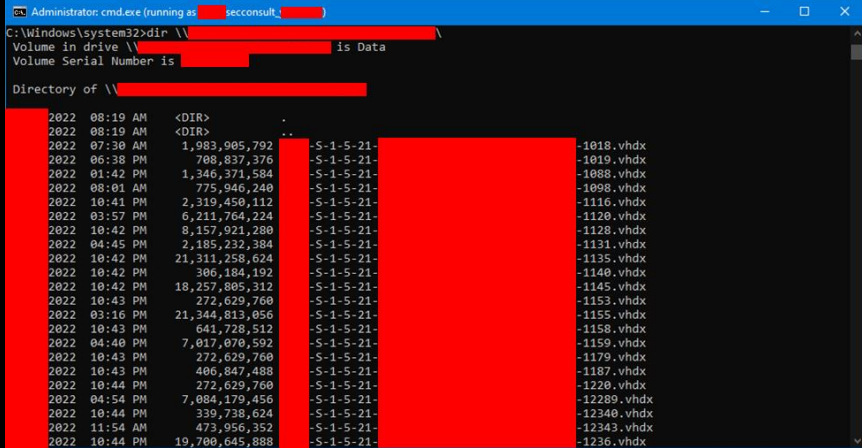
Hacker Perspectives

Internal Infrastructure

Internal Infrastructure assessments allow to evaluate the **security posture** of a company against **internal threats**, **misconfigurations** and **ransomware deployment**.

The hackers use **automated scanners** along with **manual spot-checks** and **analysis** to **identify vulnerable systems and services**. The goal is to gain access to confidential information, perform privilege escalation/lateral movement and potentially **deploy ransomware** and/or **destroy data**.

The attacker will try everything to **monetize their access** to the **infrastructure** of the company.



```
Administrator: cmd.exe (running as [redacted] seconconsult, [redacted])
C:\Windows\system32>dir \\[redacted]
Volume in drive \\[redacted] is Data
Volume Serial Number is [redacted]

Directory of \\[redacted]

2022 08:10 AM <DIR>
2022 08:10 AM <DIR>
2022 07:30 AM 1,983,905,792 [redacted] -S-1-5-21-[redacted]-1018.vhdx
2022 06:38 PM 708,837,376 [redacted] -S-1-5-21-[redacted]-1019.vhdx
2022 01:42 PM 1,346,371,584 [redacted] -S-1-5-21-[redacted]-1088.vhdx
2022 08:01 AM 775,946,240 [redacted] -S-1-5-21-[redacted]-1098.vhdx
2022 10:41 PM 2,319,450,112 [redacted] -S-1-5-21-[redacted]-1116.vhdx
2022 03:57 PM 6,211,764,224 [redacted] -S-1-5-21-[redacted]-1120.vhdx
2022 10:42 PM 9,157,921,280 [redacted] -S-1-5-21-[redacted]-1128.vhdx
2022 04:45 PM 2,185,232,384 [redacted] -S-1-5-21-[redacted]-1131.vhdx
2022 10:42 PM 21,311,258,624 [redacted] -S-1-5-21-[redacted]-1135.vhdx
2022 10:42 PM 306,184,192 [redacted] -S-1-5-21-[redacted]-1140.vhdx
2022 10:42 PM 18,257,805,312 [redacted] -S-1-5-21-[redacted]-1145.vhdx
2022 10:43 PM 272,629,760 [redacted] -S-1-5-21-[redacted]-1153.vhdx
2022 03:16 PM 21,344,813,056 [redacted] -S-1-5-21-[redacted]-1155.vhdx
2022 10:43 PM 641,728,512 [redacted] -S-1-5-21-[redacted]-1158.vhdx
2022 04:40 PM 7,817,070,592 [redacted] -S-1-5-21-[redacted]-1159.vhdx
2022 10:43 PM 272,629,760 [redacted] -S-1-5-21-[redacted]-1179.vhdx
2022 10:43 PM 406,847,488 [redacted] -S-1-5-21-[redacted]-1187.vhdx
2022 10:44 PM 272,629,760 [redacted] -S-1-5-21-[redacted]-1220.vhdx
2022 04:54 PM 7,084,179,456 [redacted] -S-1-5-21-[redacted]-12289.vhdx
2022 10:44 PM 339,738,624 [redacted] -S-1-5-21-[redacted]-12340.vhdx
2022 11:54 AM 473,956,352 [redacted] -S-1-5-21-[redacted]-12343.vhdx
2022 10:44 PM 19,708,645,888 [redacted] -S-1-5-21-[redacted]-1236.vhdx
```



```
@0 [redacted] 9: ~/volatility3-2.0.1
File Actions Edit View Help

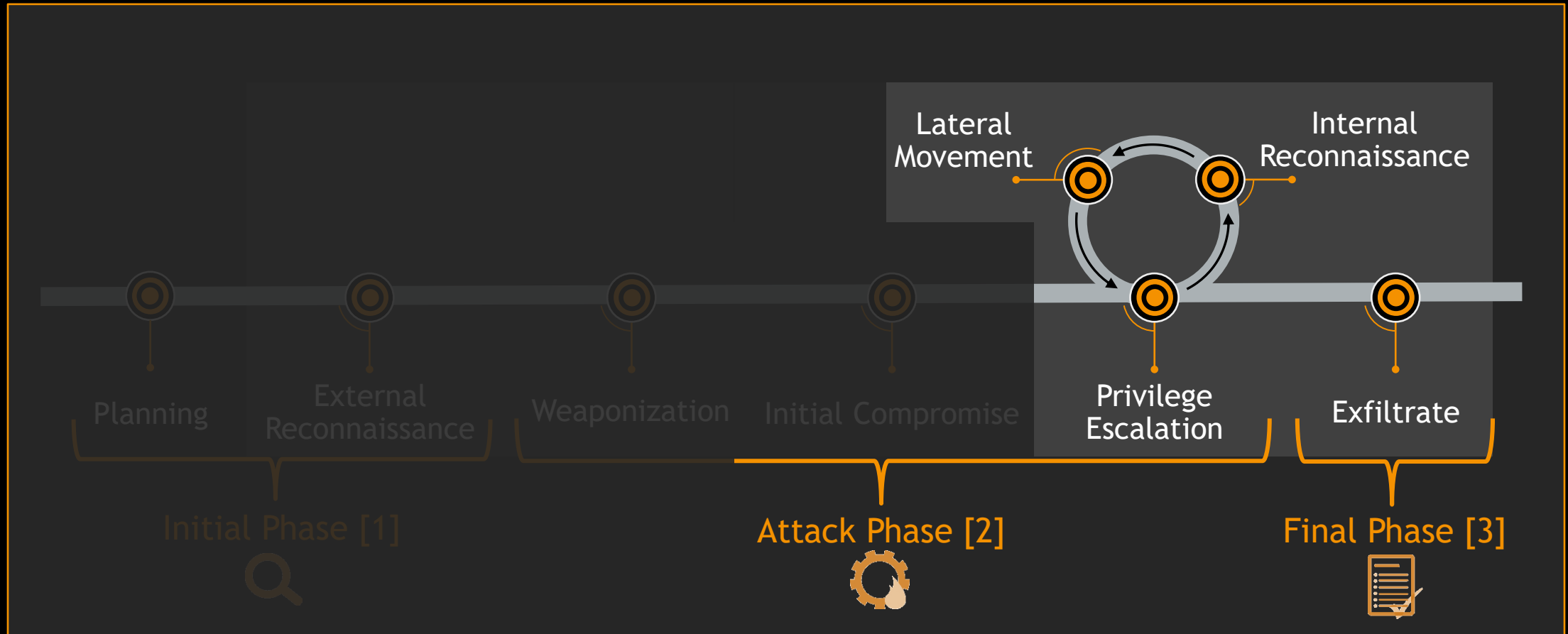
[redacted] [redacted] 9) -[~/volatility3-2.0.1]
$ python3 vol.py -f /home/[redacted]/Desktop/85_Kali_VW/10.[redacted].69.raw -r pretty windows.hashdump.Hashdump
Volatility 3 Framework 2.0.1
Formatting...0.00 PDB scanning finished

* | User | rid | lmhash | nthash
* | Administrator | 500 | aad3b435b51404eeaad3b435b51404ee | 44 | [redacted] | 9c
* | Guest | 501 | aad3b435b51404eeaad3b435b51404ee | 31 | [redacted] | c0
* | PCAdmin | 1001 | aad3b435b51404eeaad3b435b51404ee | 8e | [redacted] | 0d
* | CMS | 1008 | aad3b435b51404eeaad3b435b51404ee | 2a | [redacted] | 14
* | Sophos [redacted] | aaa | 11771 | aad3b435b51404eeaad3b435b51404ee | d8 | [redacted] | c7

[redacted] [redacted] 9) -[~/volatility3-2.0.1]
```

Hacker Perspectives

Internal Infrastructure



Hacker Perspectives

Digital Forensics & Incident Response [DFIR]



SEC Consult

an atos company

Hacker Perspectives

DFIR

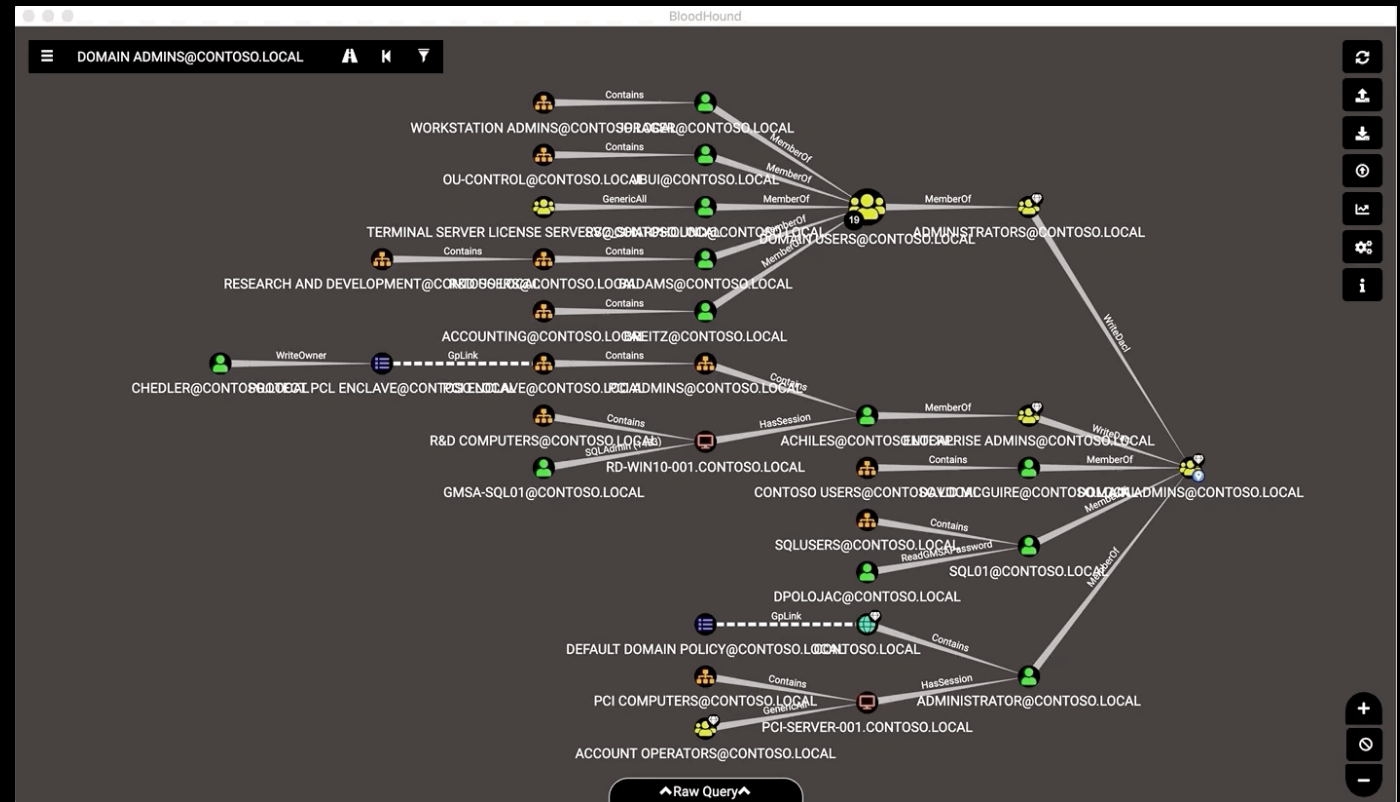


Companies are not left helpless in only being able to **respond** to attacks performed by threat actors, but can proactively engage with security (blue) teams to **hunt** out the potential threats facing their environment, even with the use of offensive tooling!

Using knowledge of “hacker tools”
to the advantage of the Blue Team 😊

AD Attack Path Mapping &
Configuration Remediation:
BloodHound (On Prem)
AzureHound (Hybrid/Cloud)

<https://bloodhound.readthedocs.io/en/latest/index.html>



https://bloodhound.readthedocs.io/en/latest/_images/right-click-edge-help.gif



Hacker Perspectives

DFIR

Command and Control (C2) technologies are no longer just an advantage for the adversaries or Red Teams anymore, the Blue Team can fight back with them too!

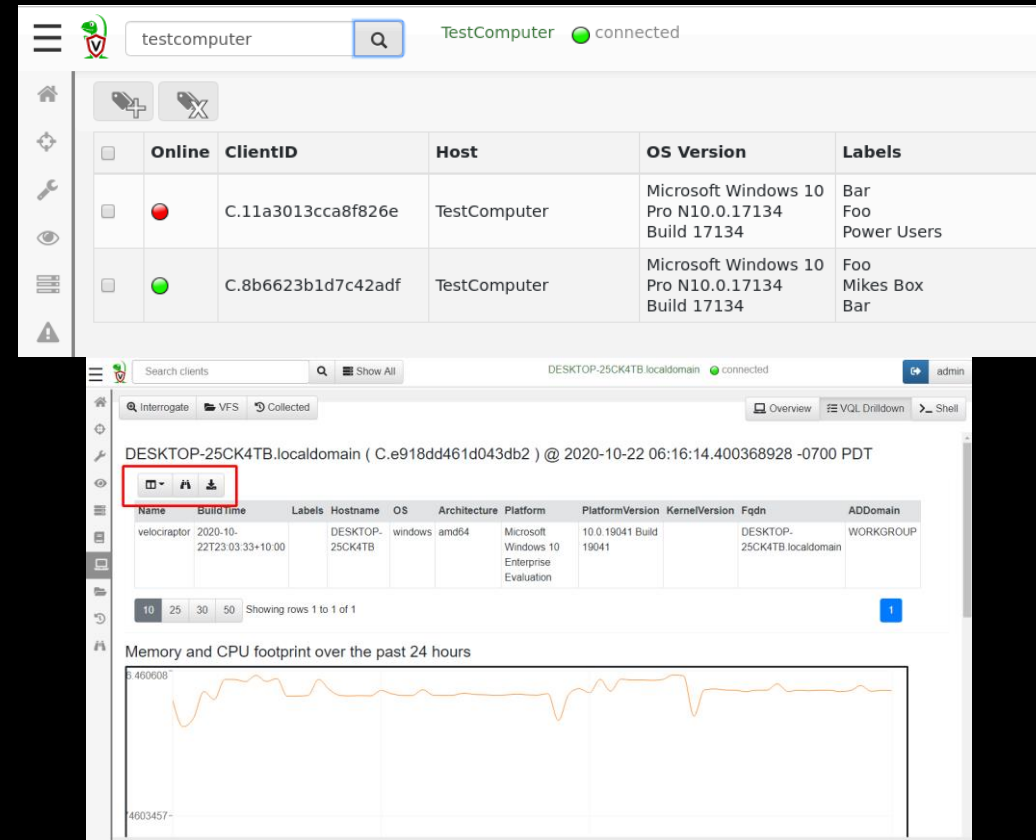
Using agile, scalable and quick to deploy (IR) C2 frameworks to enable:

- Immediate Asset Visibility Gains
- Real-Time Access To Asset Forensic/Log Artifacts
- Active Real-Time Threat Hunting
- Active Real-Time Alerting
- Real-Time Asset Quarantine

Enter stage....



<https://docs.velociraptor.app/>



The screenshot displays the Velociraptor web interface. The top section shows a client list with columns for Online status, ClientID, Host, OS Version, and Labels. Below this, a detailed view of a client (DESKTOP-25CK4TB.localdomain) is shown, including a table of system information and a graph of memory and CPU footprint over the past 24 hours.

Online	ClientID	Host	OS Version	Labels
●	C.11a3013cca8f826e	TestComputer	Microsoft Windows 10 Pro N10.0.17134 Build 17134	Bar Foo Power Users
●	C.8b6623b1d7c42adf	TestComputer	Microsoft Windows 10 Pro N10.0.17134 Build 17134	Foo Mikes Box Bar

Name	Build Time	Labels	Hostname	OS	Architecture	Platform	PlatformVersion	KernelVersion	Fqdn	ADDomain
velociraptor	2020-10-22T23:03:33+10:00		DESKTOP-25CK4TB	windows	amd64	Microsoft Windows 10 Enterprise Evaluation	10.0.19041 Build 19041		DESKTOP-25CK4TB.localdomain	WORKGROUP

<https://docs.velociraptor.app/docs/gui/clients/>

Outro



an atos company

Hacker Perspectives

Many Possibilities

Hacking is not a crime. Hacking is a lifestyle and mindset.

Hackers provide valuable information on the security posture of companies in many different aspects and **independently to compliance checks, products or brands.**

Being for phishing campaigns, applications, infrastructures, EDR/XDR bypasses, **hackers will find new ways/methods to reach their goal.**

Every individual **hacker cannot know everything in depth**, but the colleagues/friends/community will allow them to **get to the information in an efficient way.**

Hackers like to share the information to allow everyone to move forward and grow.

Hacker Perspectives

Think Different, Act Different

The hacker community provides many examples of **different ways to think** and share information.

What about sensibilizing to usage of password managers and MFA?

Video from Rachel Tobac

Source:

<https://twitter.com/RachelTobac/status/1352409636792492035>

Licensing:

This file is licensed under the [Creative Commons Attribution 4.0 International](#) license.



Hacker Perspectives

Hire a Hacker



Do you have any questions?

Don't hesitate to contact us: office-switzerland@sec-consult.com

CYBER INCIDENT? CALL +41 44 545 10 85

www.sec-consult.com

SEC Consult in Switzerland

SEC Consult (Schweiz) AG



SWITZERLAND

SEC Consult (Schweiz) AG

Freilagerstrasse 28

8047 Zurich

Tel +41 44 271 777 0

Email: office-switzerland@sec-consult.com