CENSUS
Cybersecurity Engineering

Census Labs S.A.

Thinking Like an Adversary

Practical Introduction to Red Teaming

Ioannis Stais
Director of Organization Security Testing
(istais@census-labs.com)

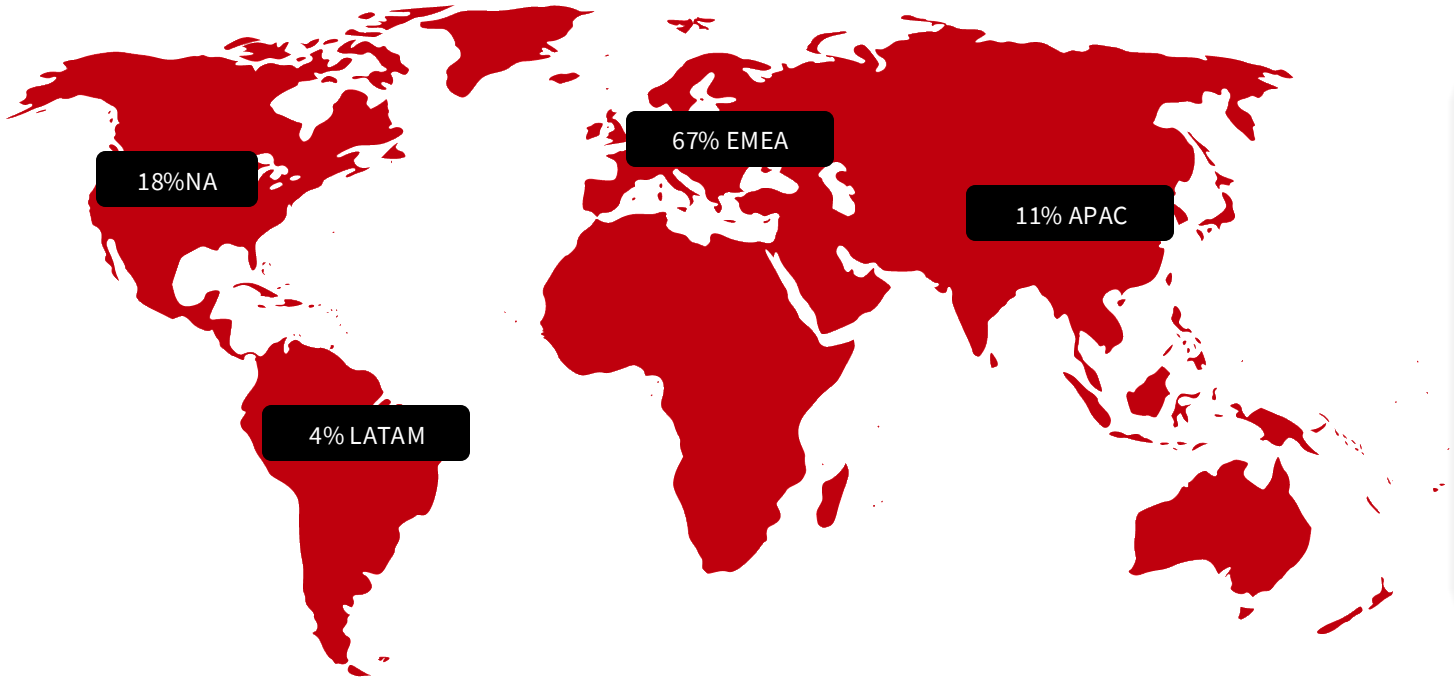
Classification Level: Intended Audience

CENSUS
Cybersecurity Engineering

CENSUS at a glance

Global presence

We help clients with their cybersecurity maturity journey by providing end to end state of the art assessment of their security posture to improve their cyber resilience and leverage the benefits of digital transformation.



19+
Countries

~400
Clients
80+ Fortune 500

In multiple market sectors

- Aerospace & Defence§
- Government
- Healthcare
- Maritime
- Transportation
- Banking, Finance & Insurance
- Industrial & Internet of Things
- Energy & Utilities
- Software Companies
- Application Developpers

CENSUS
Cybersecurity Engineering

CENSUS at a glance

- **CENSUS** is an **internationally acclaimed** Cybersecurity services provider, supporting the needs of **multiple industries**.
- We are offering state-of-the-art services to organizations **worldwide** to cover the complex needs of today's **IT & OT ecosystems**:
  - Security Assessments
  - Product Security
  - Secure Systems Development Lifecycle
  - Vulnerability Research
  - Information Security Consulting
- Services built upon the **company's leading research** to provide high quality InfoSec services.
- We are very proud of our **ethos**, as we care about **quality (in) systems**.

70+ Security engineers

12+ Years of innovation

Company certified for quality and security management systems

CENSUS
Cybersecurity Engineering

Census Labs

Thinking Like an Adversary: A Practical Introduction to Red Teaming

Agenda

- Red Teaming: Scope, Objectives, Goals, TTPs
- Threat Intelligence
- RT Methodology & Planning
- Reconnaissance
- Weaponization, Exploitation & Initial Access
- Privilege Escalation, Lateral Movement & Persistency
- Reporting & Debrief
- Ethical & Legal Consideration

Red Teaming: Scope, Objectives, Goals, TTPs

Red Teaming: Emulate real-world adversaries to test technology, people and processes

- Full-scope, intelligence-led, multi-layered attack simulation designed to measure how well a company's people and networks, applications processes and physical security controls can withstand an attack from a real-life adversary. The test will expose vulnerabilities and risks regarding:
  - Technology — Networks, applications, services, routers, switches, IoT appliances, access controls, etc.
  - People — Staff, independent contractors, interns, departments, business partners, etc.
  - Processes — IR playbooks, recovery, etc.
- Often operate over an extended time and combine multi-faceted testing approaches that are designed to not only seek to penetrate an organization but verify the detection, monitoring and incident response process and actions
- Aimed at improving resilience: It's a controlled simulation with rules and measurable objectives

CENSUS
Cybersecurity Engineering

Red Team vs Blue Team vs Purple Team vs …

Type	Main Goal	Focus Areas	Typical Activities	Outcome / Value
Red Team (RT)	Realistic simulation of Threat Actors	Offensive real TTPs, covert operations, broad scope, persistence, focused on critical assets	Recon, Phishing, lateral movement, C2	Tests detection & response, reveals true gaps
Blue Team (BT)	Defend, Detect, Recover	Monitoring, IR, forensics	Log analysis, EDR, SIEM tuning, hunts	Detects attacks, contains & recovers incidents
Purple Team (PT)	Collaborate & improve	Red + Blue integration	Replay attacks, evaluate and refine controls	Faster detection, knowledge sharing, tuned defences
Gold Team (GT)	Govern & align	Strategy, risk, policy	Table-Top exercises, Ransomware	Assurance, governance, continuous improvement
Penetration Testing (PT)	Finds technical flaws	Vulnerability identification & exploitation, limited actions	Mapping / Scan, exploiting, reporting	Lists and validates security weaknesses

CENSUS
Cybersecurity Engineering

Red Team vs Blue Team vs Purple Team vs …

Red Team
- You're the attacker!

Blue team
- You defend and escalate!

Purple Team
- You bridge both and coach!

Gold Team
- You oversee rules, playbooks and sign-offs!

Penetration Tester
- You conduct a focused technical assessment!

Goals & Objectives: Measure the organization's ability to detect, respond, and recover

- Identify security vulnerabilities across systems, processes and human behaviour
- Evaluate detection and response capability under realistic attack scenarios.
- Identify process and control failures (gaps in coverage, inefficient playbooks, errors in escalation, communication, etc).
- Test the organization's most critical assets and functions (crown jewels) under attack.
- Provide strategic insights: Deliver risk-based findings. Provide actionable intelligence about the organization's security posture.
- Drive blue team improvements


We should ensure that the simulation accurately reflects authentic cyber threat activity

The simulation should include real-world adversarial behaviours and TTPs

- Threat Actor: A person or a group of people that take part in malicious acts against systems, networks, or organizations
- Motivation: Can include financial gain, espionage, activism, political influence, or disruption.
- Archetypes / Categories: Nation-State Actors, Cybercriminals, Hacktivists, Insiders, Script Kiddies

Threat Actor TTPs:

Tactics	The attacker's high-level goals (e.g., Initial Access, Persistence, Exfiltration)
Techniques	The specific methods used to achieve a tactic (e.g., Phishing, RDP Brute-force, credential dumping)
Procedures	The concrete step-by-step actions and tools an actor uses (Emails and Common C2 Frameworks)

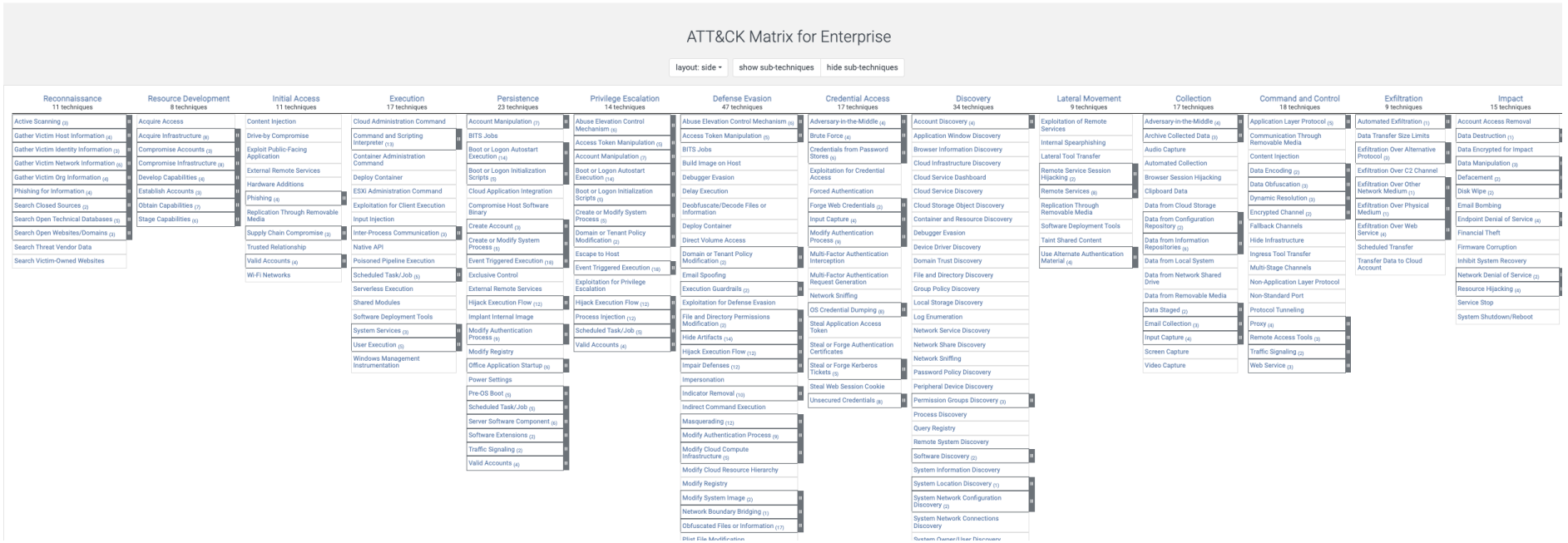
INTEL TAL: A standardized Threat Agent archetypes knowledge base

	Intent	NON-HOSTILE			HOSTILE																	
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Civil Activist	Competitor	Corrupt Government Official	Data Miner	Employee Disgruntled	Government Cyberwarrior	Government Spy	Internal Spy	Irrational Individual	Legal Adversary	Mobster	Radical Activist	Sensationalist	Terrorist	Thief	Vandal	Vendor
Access (1)	Internal	■	■	■						■		■	■							■		■
	External				■	■	■	■	■		■			■	■	■	■	■	■		■	
Outcome (1-2)	Acquisition/Theft												■	■		■				■		
	Business Advantage						■	■	■			■			■							■
	Damage	■	■	■	■					■	■			■			■	■	■		■	
	Embarrassment	■	■	■		■				■	■			■	■		■	■				
	Tech Advantage						■	■	■			■	■									■
Limits (max)	Code of Conduct		■	■																		
	Legal	■													■							■
	Extra-legal, minor					■	■	■	■				■				■	■		■	■	
	Extra-legal, major				■					■	■	■		■		■			■			
Resources (max)	Individual	■	■	■						■				■						■		
	Club				■													■				
	Contest																				■	
	Team								■													■
	Organization					■	■						■		■	■	■		■			
	Government							■			■	■										
Skills (max)	None				■									■						■		
	Minimal		■															■				
	Operational			■						■											■	■
	Adept	■				■	■	■	■		■	■	■		■	■	■		■			
Objective (1 or more)	Copy					■	■		■			■	■		■							■
	Deny							■			■											
	Destroy				■					■	■								■			
	Damage									■	■								■			
	Take														■	■			■	■		
	All of the Above/ Don't Care	■	■	■										■			■	■			■	
Visibility (min)	Overt		■		■			■							■		■	■				
	Covert	■				■										■			■		■	
	Clandestine			■			■		■			■	■							■		■
	Multiple/Don't Care									■	■			■								

Source: Intel IT Threat Assessment Group, 2007

URL: https://https://www.researchgate.net/publication/324091298_Threat_Agent_Library_Helps_Identify_Information_Security_Risks

MITRE ATT&CK®: A TTP knowledge base based on real-world observations.



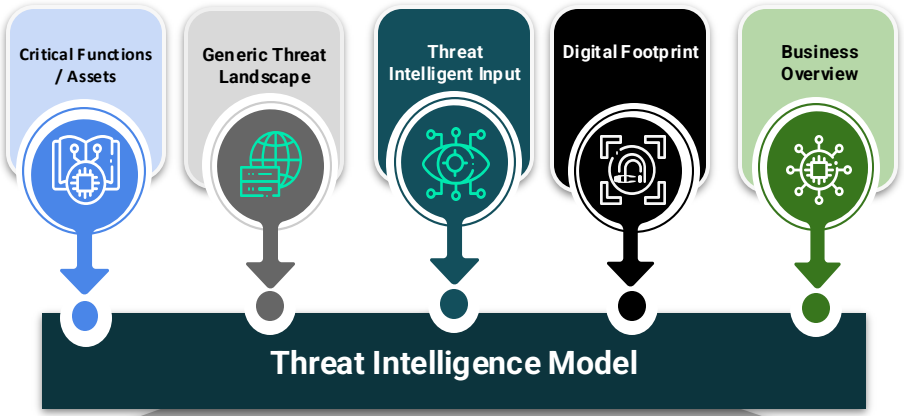
URL: https://attack.mitre.org

We must take into account industry-specific threat levels

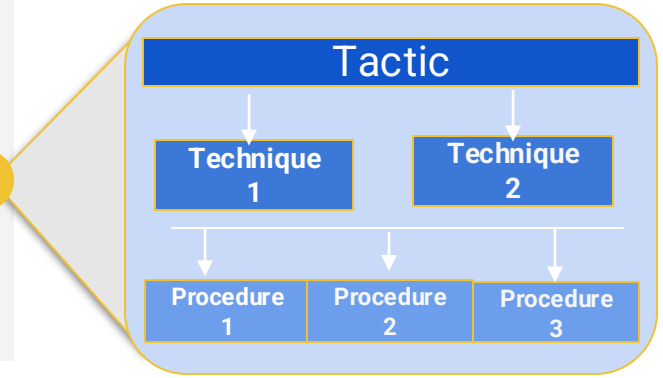
Tailored to a security organization's unique attack surface

Threat Intelligence

Phases of Threat Intelligence

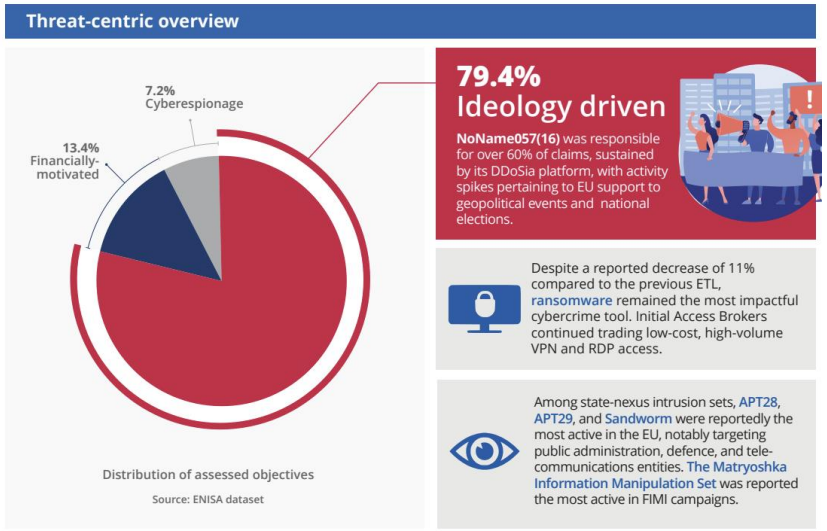


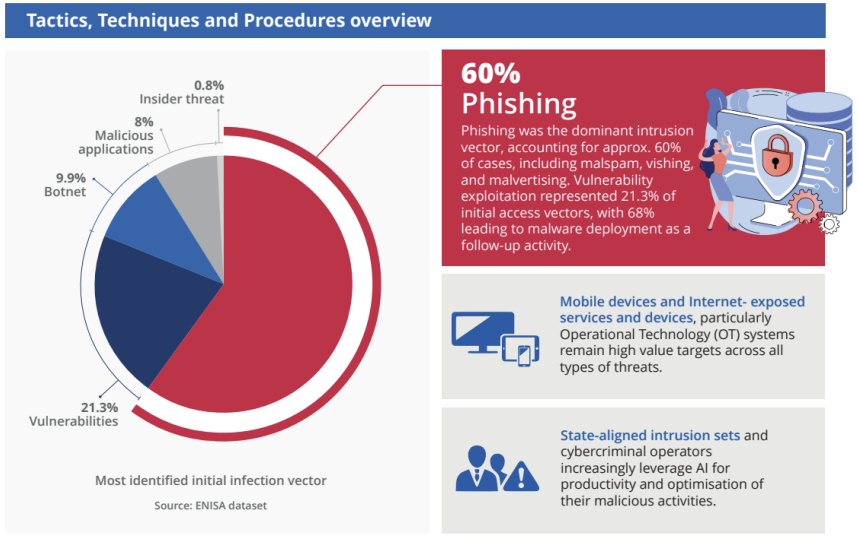
1. Contextualize critical functions / assets
2. Contextualize flags
3. Identify threat actors
4. Understand motivation and intent
5. Determine modus operandi
6. Create threat scenarios
7. Re-validate scope
8. Finalize flags



ENISA Generic Threat Landscape 2025

- ENISA Threat Landscape analyses 4875 incidents over a period spanning from 1 July 2024 to 30 June 2025.
- This report provides an overview of the most prominent cybersecurity threats and trends the EU faces



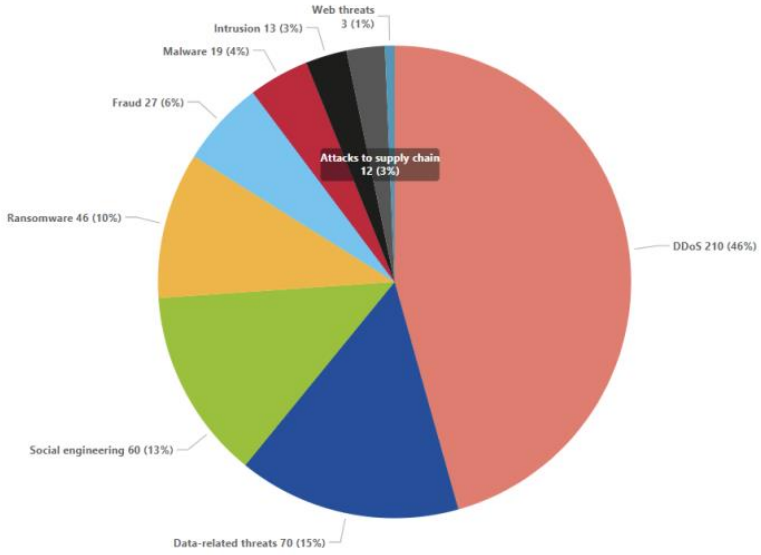


URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

ENISA Threat Landscape – Financial Sector

- From January 2023 to June 2024, the European financial sector faced significant cybersecurity challenges, highlighting threats and vulnerabilities across the sector.

Figure 5: Threats observed in the European finance sector (January 2023 to June 2024)



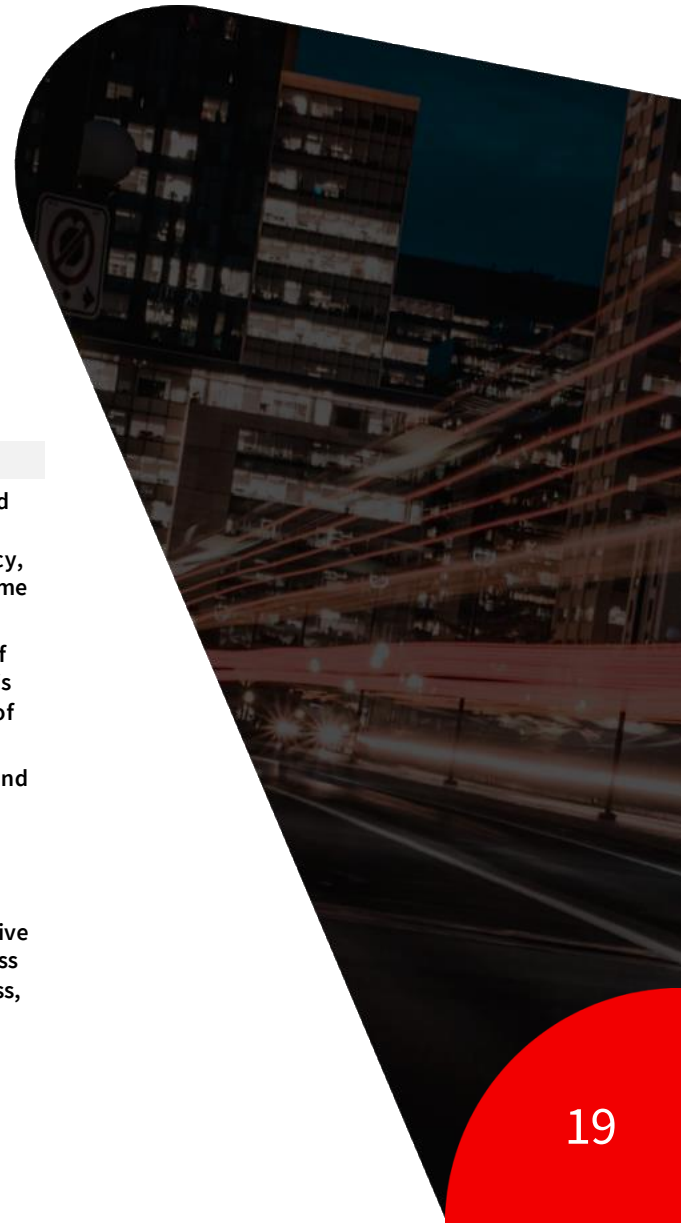
URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector

MITRE ATT&CK Groups / Threat Actor Catalog

- Groups are activity clusters that are tracked by a common name in the security community. MITRE ATT&CK tracks more than 160 such groups

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 targeted organizations involved in financial, economic, and trade policy, typically using publicly available RATs such as PoisonIvy, as well as some non-public backdoors.
G1030	Agrius	Pink Sandstorm, AMERICIUM, Agonizing Serpens, BlackShadow	Agrius is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East, with an emphasis on Israeli targets. Public reporting has linked Agrius to Iran's Ministry of Intelligence and Security (MOIS).
G0130	Ajax Security Team	Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, Operation Saffron Rose	Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax Security Team transitioned from website defacement operations to malware-based cyber espionage campaigns targeting the US defense industrial base and Iranian users of anti-censorship technologies.
G1024	Akira	GOLD SAHARA, PUNK SPIDER, Howling Scorpius	Akira is a ransomware variant and ransomware deployment entity active since at least March 2023. Akira uses compromised credentials to access single-factor external access mechanisms such as VPNs for initial access, then various publicly-available tools and techniques for lateral movement....

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



Collecting Information From Multiple Sources

- Open-source (OSINT), commercial feeds, dark web, sensors, telegram and internal logs.

```
root@kali:~# theHarvester -d kali.org -l 500 -b duckduckgo
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.4.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: kali.org

[*] Searching Duckduckgo.

[*] No IPs found.

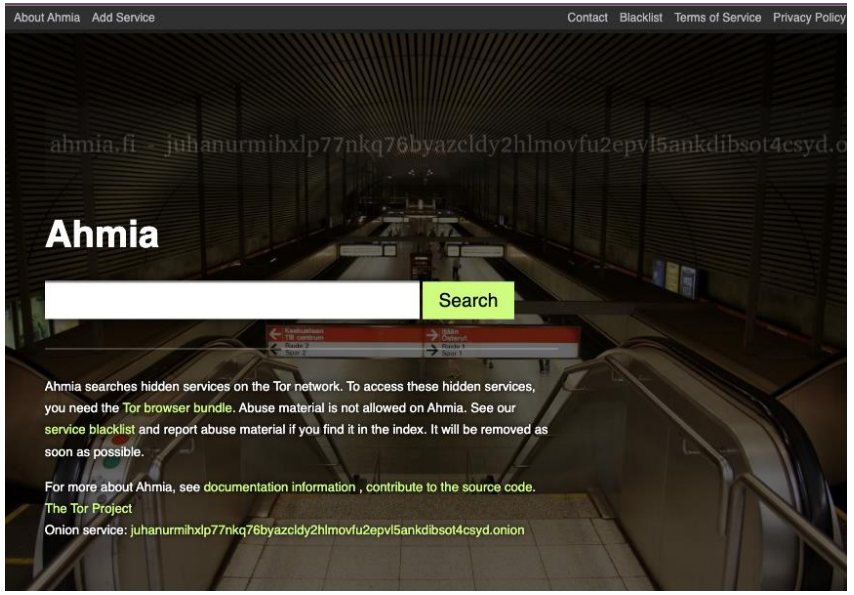
[*] No emails found.

[*] Hosts found: 14
---------------------
[...]

```console
```

URL: https://github.com/laramies/theHarvester

URL: https://github.com/DedSecInside/TorBot



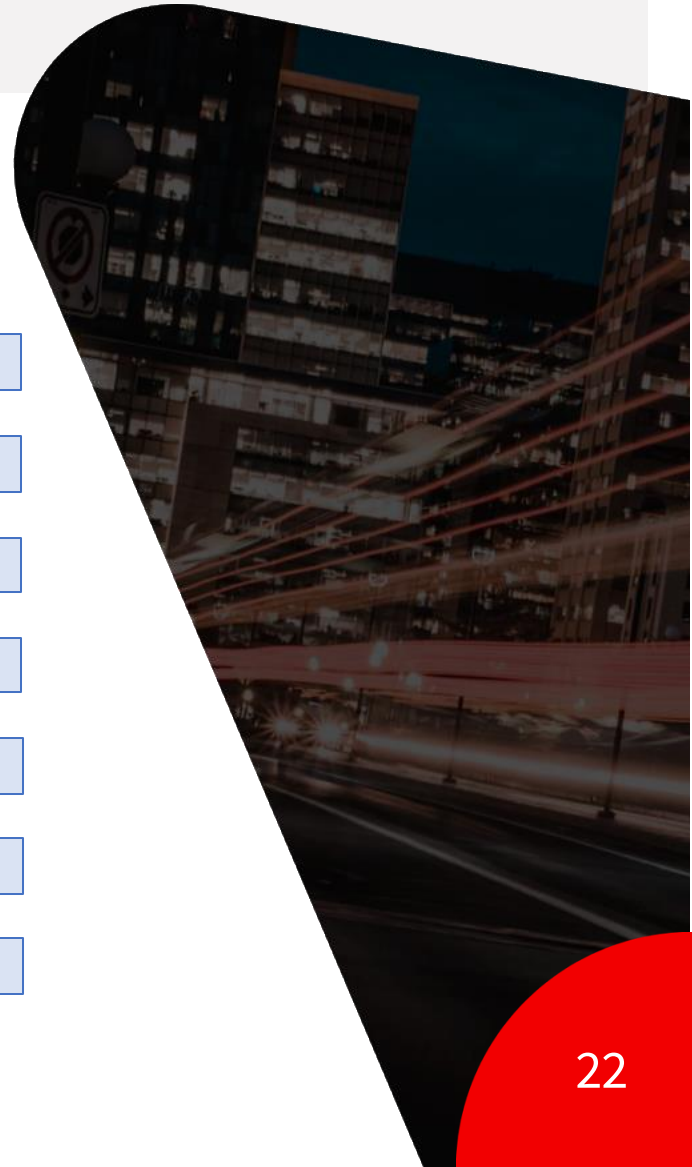
URL: https://ahmia.fi/
```

Methodology

Testing phase | Red Team Testing Methodology

- The testing methodology is primarily based on the Cyber Kill Chain (CKC) of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity, developed by Lockheed Martin

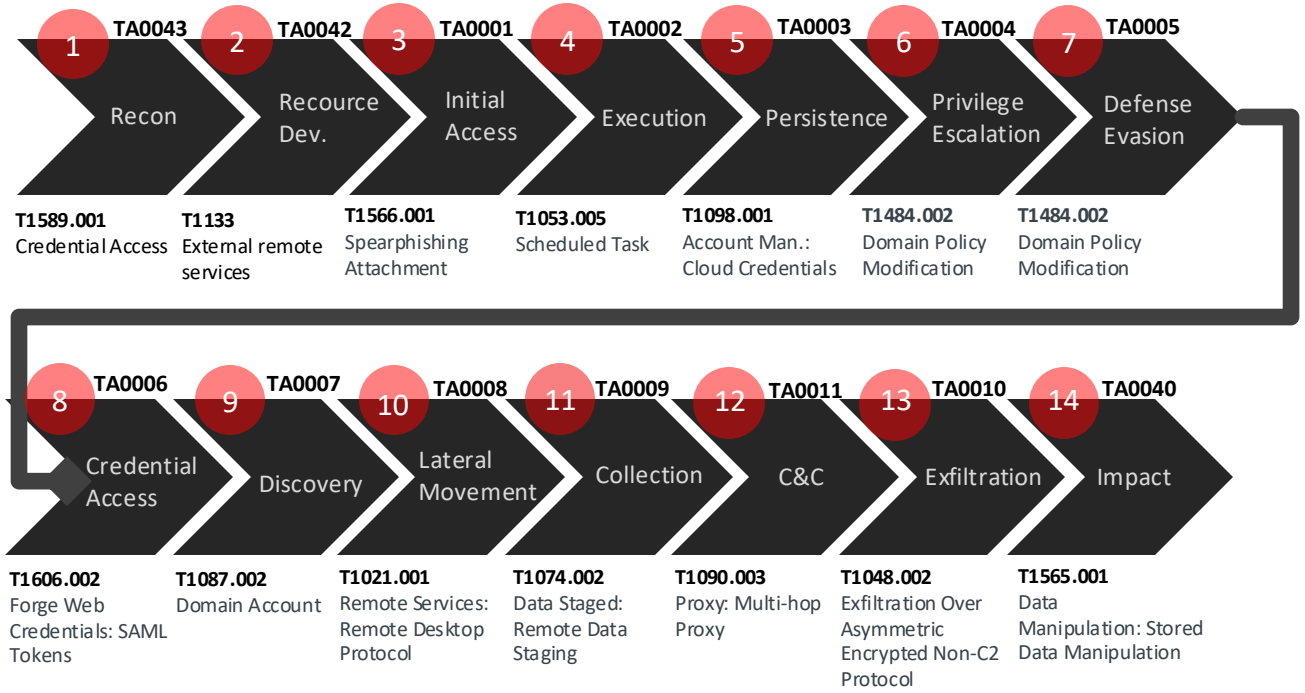
1	**Reconnaissance**	Collecting as much information as possible about the target.
2	**Weaponization**	Analysing the information gathered in previous phase.
3	**Delivery**	Carrying out the actions on the target(s) intended to reach the target flags.
4	**Exploitation**	Compromising servers/apps/networks and exploit target staff.
5	**Installation**	Installing persistent backdoors or implants in the environment.
6	**Command and Control**	Opening two way communications channel to C2 infrastructure
7	**Actions on objectives**	Accomplishing the mission's goal.



Testing phase | Red Team Testing Methodology

MITRE ATT&CK Enterprise tactics

- ATT&CK is used as a lower level of definition to map the actions as an adversary.
- Example of mapping TTPs of **APT29** to the ATT&CK.



CENSUS
Cybersecurity Engineering

Testing phase | Red Team Testing Methodology

Other widely accepted methodologies

- OWASP Testing Guide
- OWASP Application Security Verification Standard,
- NIST Technical Guide to Information Security Testing and Assessment
- PTES standard
- Open-Source Security Testing Methodology Manual

OWASP®

CWE Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org

PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines

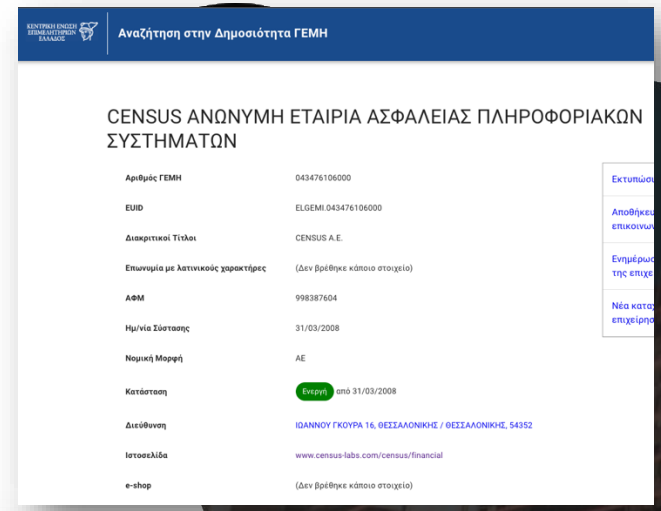
Planning & Scoping

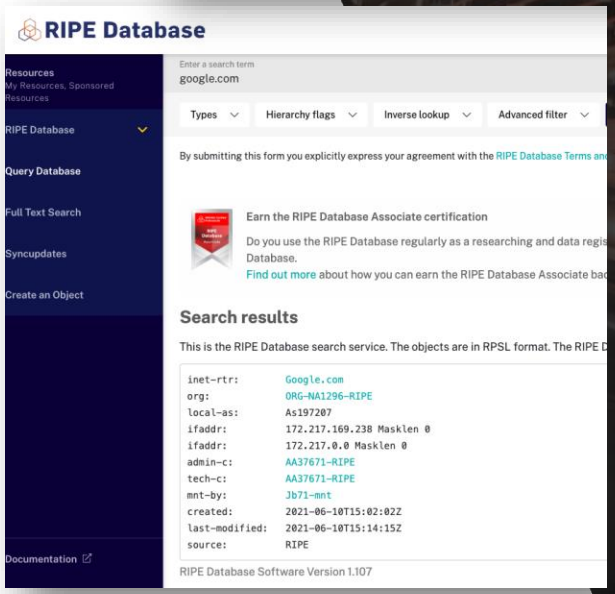
- Define allowed targets, prohibited techniques, and data handling rules.
- Set success criteria and acceptable business impact (e.g., no production outages).
- Decide communication cadence, emergency kill-switch, and escalation contacts.
- Capture legal approvals and executive sponsorship in writing.
- Build a controlled test plan with risk mitigations (backups, rollback).

Reconnaissance

Reconnaissance

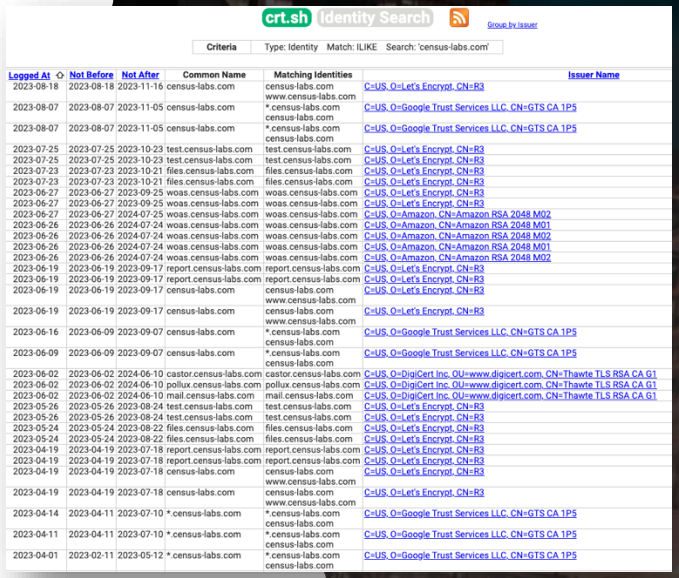
- **Internet Fingerprinting & Passive Reconnaissance involves:**
  - **Web Search**: A comprehensive search approach to gather a diverse range of data, including important contact details, addresses, up-to-date news, articles, social media content, leaked credentials, exploration of an organization's digital footprint on websites, blogs, social media profiles, online discussions, and other relevant online presence indicators.
  - **Business Registry Search:** Reveals several details regarding a company's history, organization, and operations.
  - **Whois and RIRs:** Querying databases holding information of registered users or assignees of Internet.
  - **Autonomous System Number (ASN) Lookup**: Identification of the Autonomous System (AS) number associated with a specific IP address.

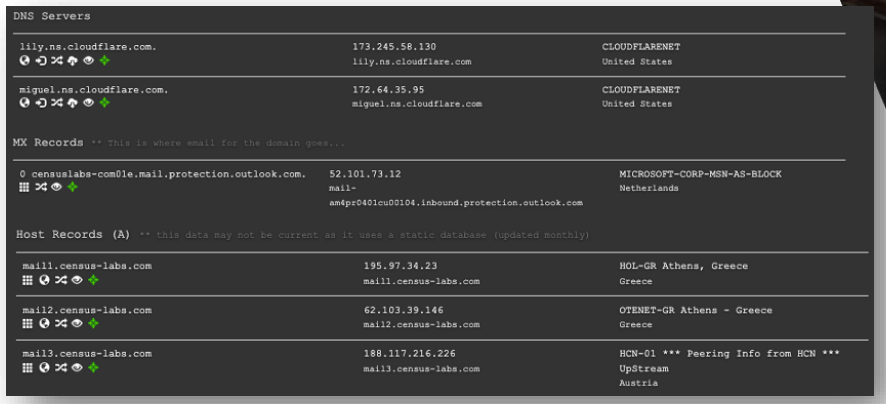




Reconnaissance

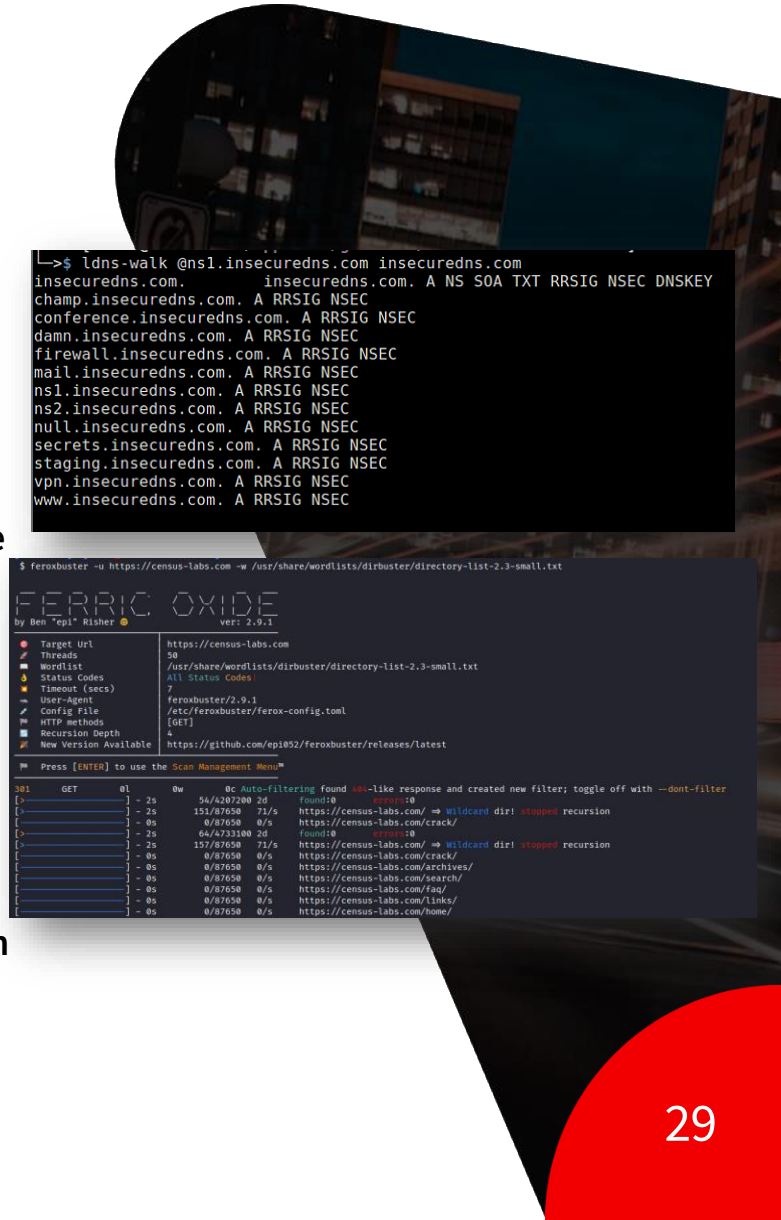
- **Internet Fingerprinting & Passive Reconnaissance involves:**
  - **Domain Name System Enumeration:** Gathering information about DNS servers, DNS records, and the types of servers in-use.
  - **Certificate Transparency:** Identification of subdomains using the publicly available CT Logs.
  - **Subdomain Automated Dictionary Attacks:** Trying systematically to identify valid subdomains using a dictionary or list of potential subdomain names.
  - **Email Gathering:** Collecting emails from target companies or individuals that are publicly available.





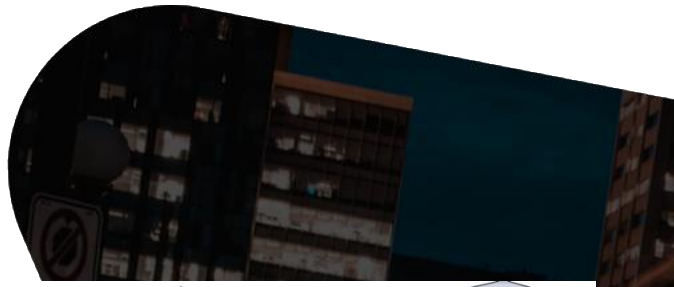
Reconnaissance

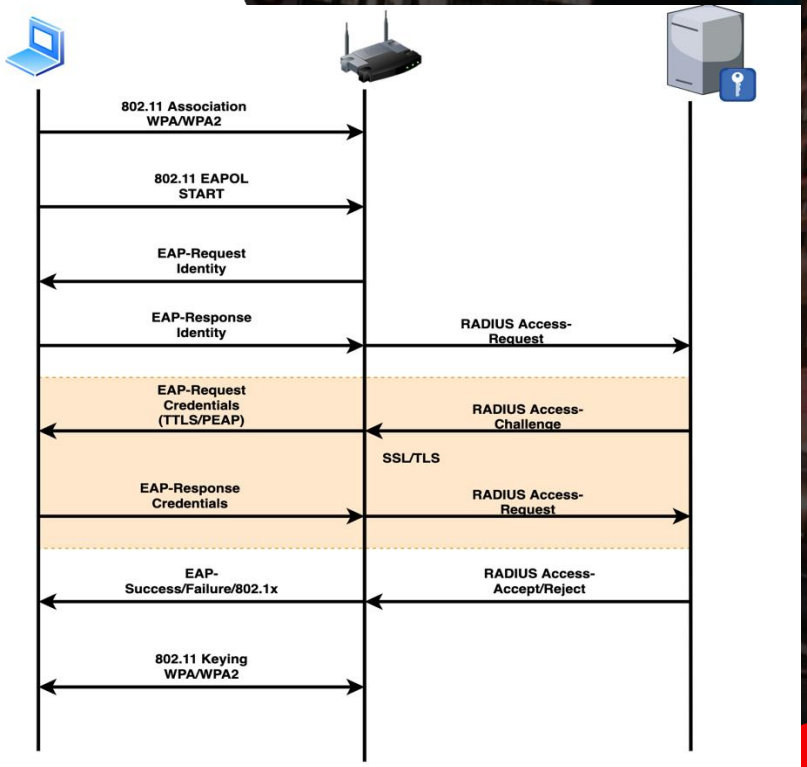
- **Active Reconnaissance involves:**
  - DNS Zone Walking: walking in DNSSEC zones to enumerate all content. DNSSEC's NSEC/NSEC3 records provide information about the range of existing domain names, even if some of these names are not published or visible through normal DNS queries.
  - Network Port Scanning: Sending network requests to different ports on a target system to determine which ports are open and listening for connections (TCP Connect, SYN/Stealth, UDP)
  - Service Version Identification: Determine software versions to identify known vulnerabilities
  - Web Folders Enumeration Attack: Known as directory or path enumeration attack, involves systematically attempting to identify and access hidden or sensitive directories and folders on a web server.
  - Vulnerability Scanning: An industry-standard automated vulnerability scanning tool is used to search for publicly reported security issues in third-party software and services' configurations.
  - Manual Inspection of Accessible Network Services: The services are analyzed by the team.



Reconnaissance

- **Wireless Reconnaissance**
  - Passive Wi-Fi discovery: collect SSIDs, BSSIDs, channels, beacon frames, and signal strength.
  - BT Client & device enumeration: observe probe requests, Bluetooth/LE advertisements, and device vendors
  - Infrastructure inventory: map authorized APs, guest networks, IoT endpoints, and weak encryption settings.
  - RF footprint mapping: wardrive or site sweep to record coverage gaps, signal bleed, and physical exposure.





Reconnaissance

- **Physical Premises Reconnaissance**
  - Perimeter & entry points: gates, doors, loading docks, delivery entrances, shift change windows.
  - Access control checks: badge readers, interlocks, visitor flows, tailgating opportunities, and signage.
  - Points-of-Sale & kiosks: POS placement, unattended terminals, exposed USB/network ports
  - Cameras & CCTV posture: camera locations, blind spots, camera cables
  - Environmental & human factors: lighting, landscaping (hiding spots), employee routines, vendor deliveries, and contractor access.

Reconnaissance

- **Sample Basic Tooling**
  - dirb - directory buster (wordlist-based web content discovery): https://github.com/v0re/dirb
  - gobuster - fast directory/file, DNS and vhost brute-forcer (Go): https://github.com/OJ/gobuster
  - theHarvester - OSINT collector for emails, subdomains, names: https://github.com/laramies/theHarvester
  - BBOT - OSINT / subdomain enumeration: https://github.com/blacklanternsecurity/bbot
  - dnsrecon - DNS enumeration: https://github.com/darkoperator/dnsrecon
  - Gitleaks - find secrets in github repos: https://github.com/gitleaks/gitleaks
  - Trufflehog – find secrets in github, s3, Jenkins, postman, elasticsearch, huggungface: https://github.com/trufflesecurity/trufflehog
  - nmap - network mapper: https://github.com/nmap/nmap
  - Aircrack-ng - suite for Wi-Fi monitoring and auditing (includes airodump-ng): https://github.com/aircrack-ng/aircrack-ng
  - bettercap - wireless monitoring (Wi-Fi, BLE, HID, more): https://github.com/bettercap/bettercap
  - Kismet - wardriving: https://www.kismetwireless.net

Weaponization, Exploitation, Initial Access

Weaponization, Exploitation, Initial Access

- **Weaponization and Delivery involves:**
  - **Attack Planning:** Classification of the riskiest attack paths which have the easiest exploitation. The above classification helps in the understanding of the risks and also simulates the worst-case scenarios with respect to the vulnerabilities found. **TTPs that are requested for simulation are also taken into account.**
  - **Vulnerability Research / Creating Custom Exploits:** The exploit could be a zero-day or a known vulnerability that the attacker expects will not have been patched.
  - **Combining the payload with custom agent:** This can be anything that performs malicious actions, such as data exfiltration, system damage, or establishing a persistent presence for further exploitation.
  - **Testing evasion techniques / IDS Bypass**: Ensuring that the weaponized content can bypass security measures like firewalls, intrusion detection systems, and antivirus software.
  - **Transmission to the Target**: Sending the payload to the target directly over a network, such as through a vulnerable public-facing server.

Weaponization, Exploitation, Initial Access

- **Exploitation involves:**
  - **Known vulnerability exploitation:** Exploiting known vulnerabilities in software and systems using tools like Metasploit. Attempting to exploit zero-day vulnerabilities or unpatched systems.
  - **Password-based / Credential attacks**: Brute force attacks to guess passwords, Dictionary attacks with lists of commonly used passwords, Credential stuffing attacks
  - **Web Services Attacks:** Abusing common OWASP Top-10 vulnerabilities (SQL injection, XSS, XSRF, LFI, etc.).
  - **DNS Hijacking and Subdomain Takeover**: Redirecting traffic from a legitimate domain to a malicious one, Taking over unclaimed or improperly configured subdomains.
  - **Memory-related Attacks**: Exploiting applications by overrunning a buffer's boundary
  - **Exploiting Misconfigurations**: Taking advantage of insecure configurations in systems and applications, such as default credentials or open shares.
  - **Session Hijacking, Token Manipulation Attacks**: Intercepting and using valid session tokens
  - **Cloud Infrastructure Attacks:** Taking advantage of insecure configurations in cloud buckets

Initial Access

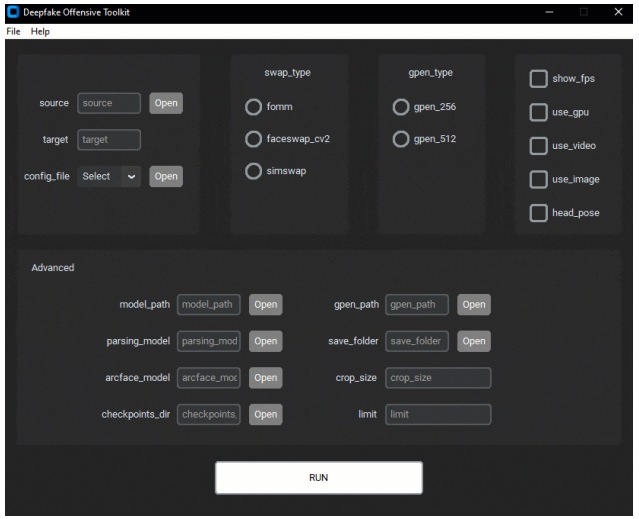
- **Social Engineering attacks**
  - Collection of open-source intelligence information about employees (Victims identification, including high-profile targets - whaling)
  - **Social engineering attacks such as Spear phishing, Baiting, Scareware, Pretexting & Client-side attacks.**
  - **Typosquatting**
  - **AI-driven social engineering attacks (e.g. Deepfake vishing, AI-generated spear phishing)**
  - **Build customized payloads (malwares / trojans) that circumvent EDRs**
  - **Pack initial access vectors for luring victims to execute the payloads (e.g. ISO, MSC, HTA)**
  - **Social networks & Third Party Services Abuse for payload delivery**

URL: https://shop.hak5.org/products/omg-cable

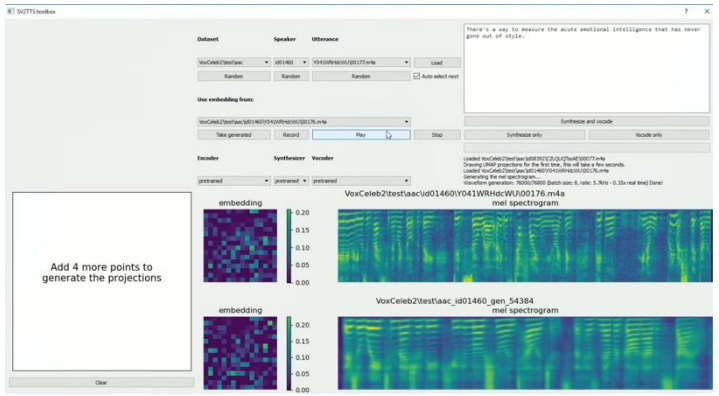
URL: https://shop.hak5.org/products/usb-rubber-ducky

Initial Access

- **Deepfake attacks**



URL: https://github.com/redteam-re/dot

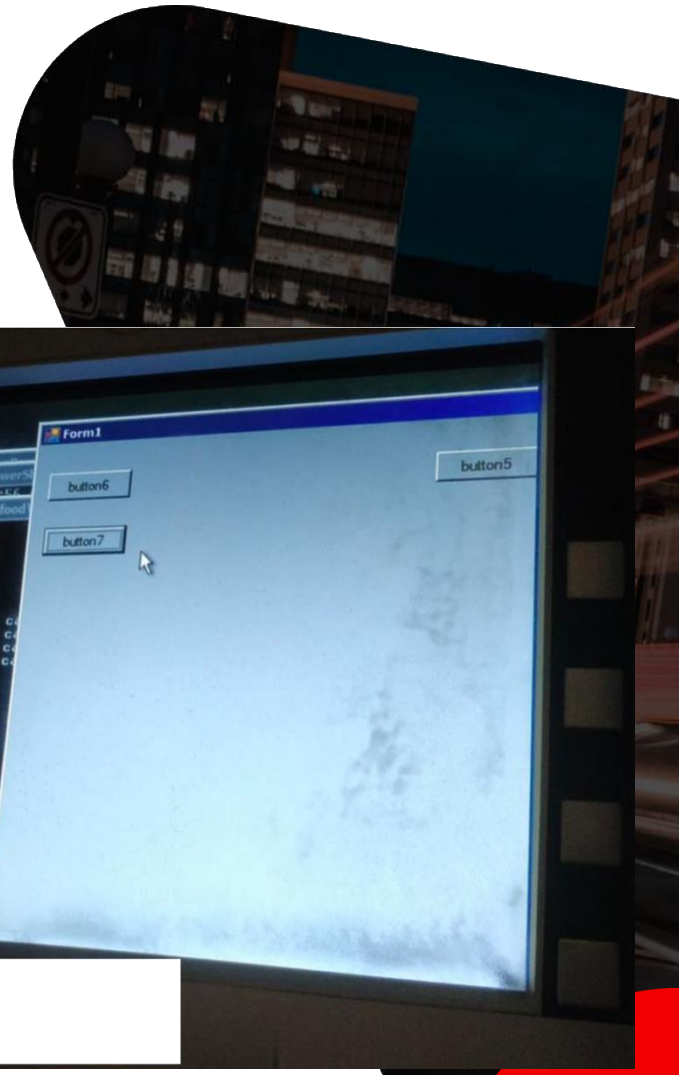


URL: https://github.com/CorentinJ/Real-Time-Voice-Cloning

Initial Access

- **Physical Attacks**

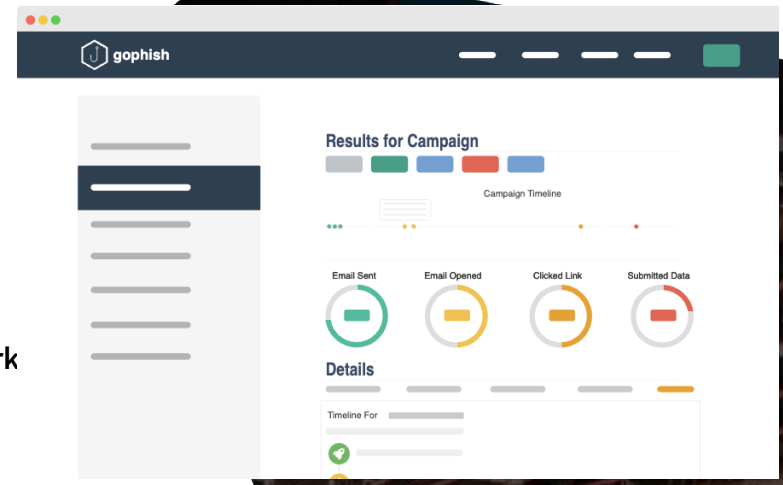
- Gaining physical access in premises: tailgating, stolen/unattended badges, insecure vendor access,
- Tampering with devices: unattended terminals / USB ports / PoS devices / IoT devices.
- Implanting devices (Evil Maid Attack): Gaining remote access in the network

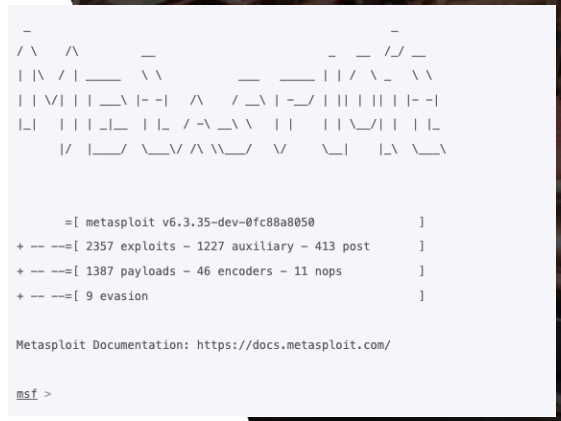


Weaponization, Exploitation, Initial Access

Sample Basic Tooling

- sqlmap - automated SQL injection discovery and exploitation: https://github.com/sqlmapproject/sqlmap
- Metasploit Framework - exploitation framework & payload generation: https://github.com/rapid7/metasploit-framework
- Havoc - post-exploitation / C2 agent framework: https://github.com/HavocFramework/Havoc
- Sliver - post-exploitation / C2 agent framework: https://github.com/BishopFox/sliver
- Gophish - phishing campaign platform: https://github.com/gophish/gophish
- Phishing Frenzy - phishing campaign platform: https://github.com/pentestgeek/phishing-frenzy
- Evilginx - browser man-in-the-middle attack: https://github.com/kgretzky/evilginx2
- dnstwist - typosquatting software: https://github.com/elceef/dnstwist
- Social-Engineer Toolkit (SET) - scenario builder (email templates, USB baiting simulations): https://github.com/trustedsec/social-engineer-toolkit
- Red Baron – Red Team Infrastructure Automation: https://github.com/byt3bl33d3r/Red-Baron

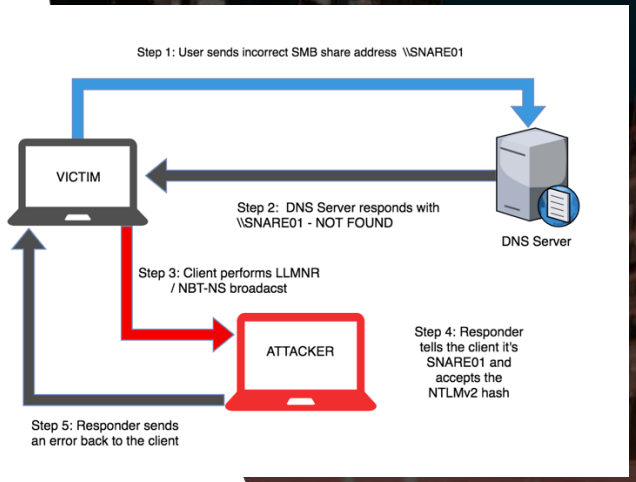


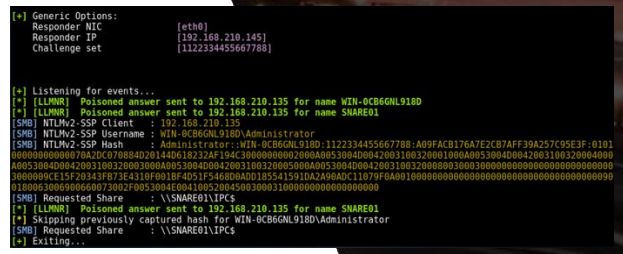


Privilege Escalation, Lateral Movement & Persistency

Privilege Escalation & Lateral Movement

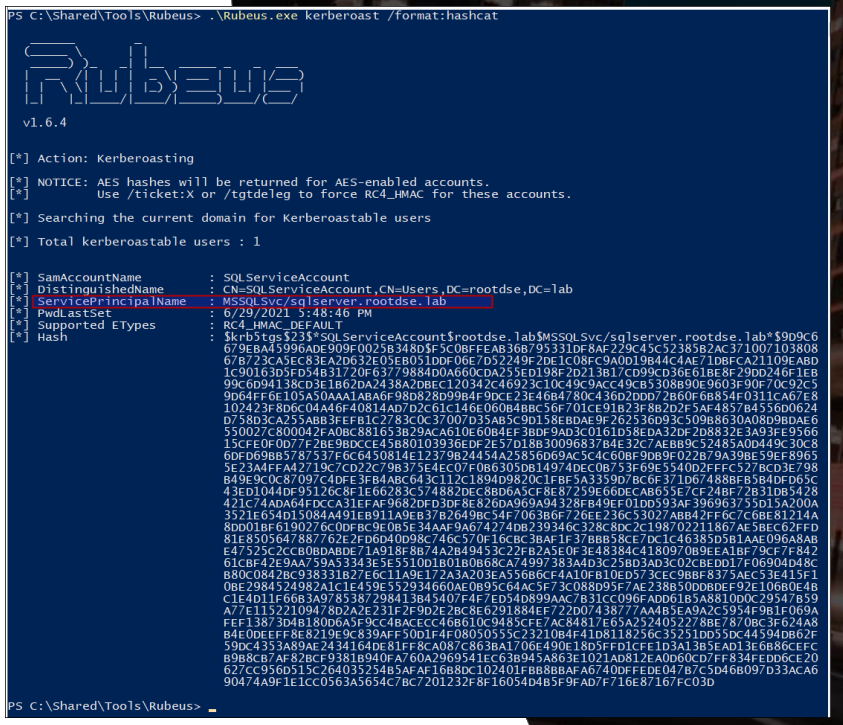
- **Internal Network Reconnaissance & Priv. Escalation and Lateral Movement:**
- Network Shares Scanning: If network shares are accessible, they may contain sensitive data
- Domain Mapping: The Active Directory is enumerated using tools such as Bloodhound.
- Network Port Scanning: Sending network requests to different ports on a target system to determine which ports are open and listening for connections (TCP Connect, SYN/Stealth, UDP)
- Name Resolution Protocols Spoofing: LLMNR/NBNS/mDNS - If such packets are travelling in the network, hijack them to obtain hashes for cracking.
- Null Authentication Testing: Attempting to authenticate against various services (like SMB, LDAP) for identification of open shares.
- Password-based / Credential attacks: Brute force attacks to guess passwords, Dictionary attacks with lists of commonly used passwords, Credential stuffing attacks using breached username and password pairs





Privilege Escalation & Lateral Movement

- **Active Directory specific attacks:**
  - **Kerberoasting:** Exploiting Kerberos TGS tickets for cracking.
  - **ASREP Roasting:** Attacking users with non-pre-authentication requirement.
  - **Insecure Delegation:** Abusing permissions forwarding within a domain.
  - **Coercion and relay:** force a workstation to perform a connection, intercept and reuse the authentication sessions.
  - **Cross-domain Trust Relationships:** Exploiting trust relationships between multiple domains.
  - **GPO attacks:** Targeting insecure Group Policy configuration for privilege escalation.
  - **Certificate Services:** Abusing insecure PKI services configuration for credentials theft/manipulation.



Establishing Persistency

- **Persistency involves:**
  - **Scheduled Tasks:** Setting up tasks to execute payloads periodically, ensuring continued access.
  - **Service Registry Modifications:** Adding or modifying registry keys to execute malicious software at system startup.
  - **GPO Modifications:** Adding or modifying Group Policy to execute malicious software on login at targeted machines.
  - **Account Manipulation:** Creating or modifying accounts to ensure they can be used to regain access.
  - **Golden Ticket**: With domain admin rights, attackers can create a ticket-granting ticket (TGT) that gives them authorization to any service in the domain.
  - **Silver Ticket**: Similar to the Golden Ticket attack, but it targets service tickets (ST) for specific services rather than creating a TGT.

Privilege Escalation, Lateral Movement & Persistency

- **Sample Basic Tooling**
  - Responder - LLMNR/NetBIOS/mDNS responder: https://github.com/SpiderLabs/Responder
  - Impacket - python implementation of network protocols (SMB, Kerberos, LDAP): https://github.com/fortra/impacket
  - BloodHound - map AD relationships/attack paths: https://github.com/SpecterOps/BloodHound
  - Mimikatz - memory extraction, Kerberos ticket manipulation (DCSync/DCShadow techniques): https://github.com/ParrotSec/mimikatz

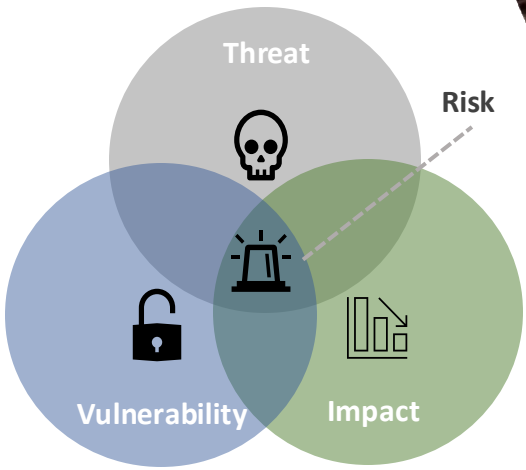
Reporting & Debrief

Closure phase | Reporting & Debrief

A story-drive report that contains the RT flow of progress, and its ability to execute or meet the predefined goals with the following additional sections:

- Executive Summary
- Attack path diagrams, specific attack-flow diagrams
- Map techniques to MITRE ATT&CK for defender alignment
- A separate section with findings discovered towards meeting the predefined goals.

Rating and Score	Impact	Likelihood
CRITICAL (5)	Extreme	Almost certain. Knowledge of the vulnerability and how to exploit it are in the public domain.
HIGH (4)	Major impact to entire organization / regulatory violation.	Relatively easy to detect and exploit by an attacker with little skill.
MEDIUM (3)	Noticeable impact to line of business if exploited.	A knowledgeable insider or expert attacker could exploit the vulnerability without much difficulty.
LOW (2)	Minor damage if exploited	Requires considerable expertise and resources.
INFO (1)	Does not represent an immediate risk on its own	Not likely to be exploited on its own



Reporting & Debrief

- Include prioritized remediation: quick wins, medium fixes, long-term projects.
- Run a debrief workshop with blue team and executives.
- Deliver a clear timeline: actions, timestamps, detected vs undetected events.
- Share reproducible detection recipes (SIEM queries, EDR rules).

Ethical & Legal Consideration

Ethical & Legal Consideration

- Always **work under explicit written authorization and scope.**
- **Adhere to privacy laws and data handling requirements**.
- **Avoid destructive or disruptive techniques** in production.
- **Maintain clear evidence chains** for post-engagement analysis.
- **Communicate transparently** with leadership and legal teams.

CENSUS
Cybersecurity Engineering

Thank you!

www.census-labs.com

Classification Level: Intended Audience