Mapping and Exploiting Social Networks as Cybersecurity Attack Surfaces

Explore the evolving landscape of social engineering attacks and the tactics used by threat actors to compromise organizations. organizations.

Presented By:
Mustafa Mohammad Majdi

Introduction

- **Stage 1 (Information Gathering)**
  - Collect publicly available data about targets (people, organizations, infrastructure) from OSINT sources — social media, social media, public records, DNS/WWHOIS, search engines, and leaked databases..
- **Stage 2 (Attack Strategy Development)**
  - Analyze gathered intelligence to identify weaknesses, prioritize high-value targets, and design a tailored attack plan (goals, attack plan (goals, attack vectors, timing, and required resources).
- **Stage 3 (Weaponization & Delivery Methods)**
  - Prepare the attack tools and content (malicious files, phishing pages, payloads, social-engineering scripts) and select and select delivery channels (email, social media, messaging, or exploit kits).
- **Stage 4 (Execution and impact)**
  - Deliver the crafted attack to the target and attempt to compromise it — e.g., send phishing messages, launch spoofed communications, or exploit technical vulnerabilities to gain access..
- **Stage 5 (Mitigations & Useful tools)**
  - After compromise, attackers may deploy malware to maintain access and exfiltrate data; defenders respond by detecting, containing, eradicating threats, and restoring systems — focusing on incident response and prevention.

Stage 1 (Information Gathering)

Understanding the OSINT Framework

Leveraging a comprehensive set of open-source data sources to gather information about the target, such as email addresses, phone numbers, social media profiles, and online infrastructure.

Analyzing Data Breaches

Examining how attackers can exploit data breaches to obtain valuable information, such as personal details and credentials, to launch targeted attacks.

Utilizing OSINT Tools

Employing tools like Maltego and SpiderFoot to automate the data collection process and transform the gathered information into a visual map of relationships.

Uncovering Attack Surfaces

Identifying potential vulnerabilities and attack vectors within the target's online presence, including social media accounts and web infrastructure.

By understanding the information gathering stage, organizations can better anticipate and defend against the tactics used by attackers to initiate social engineering attacks.

Maltego

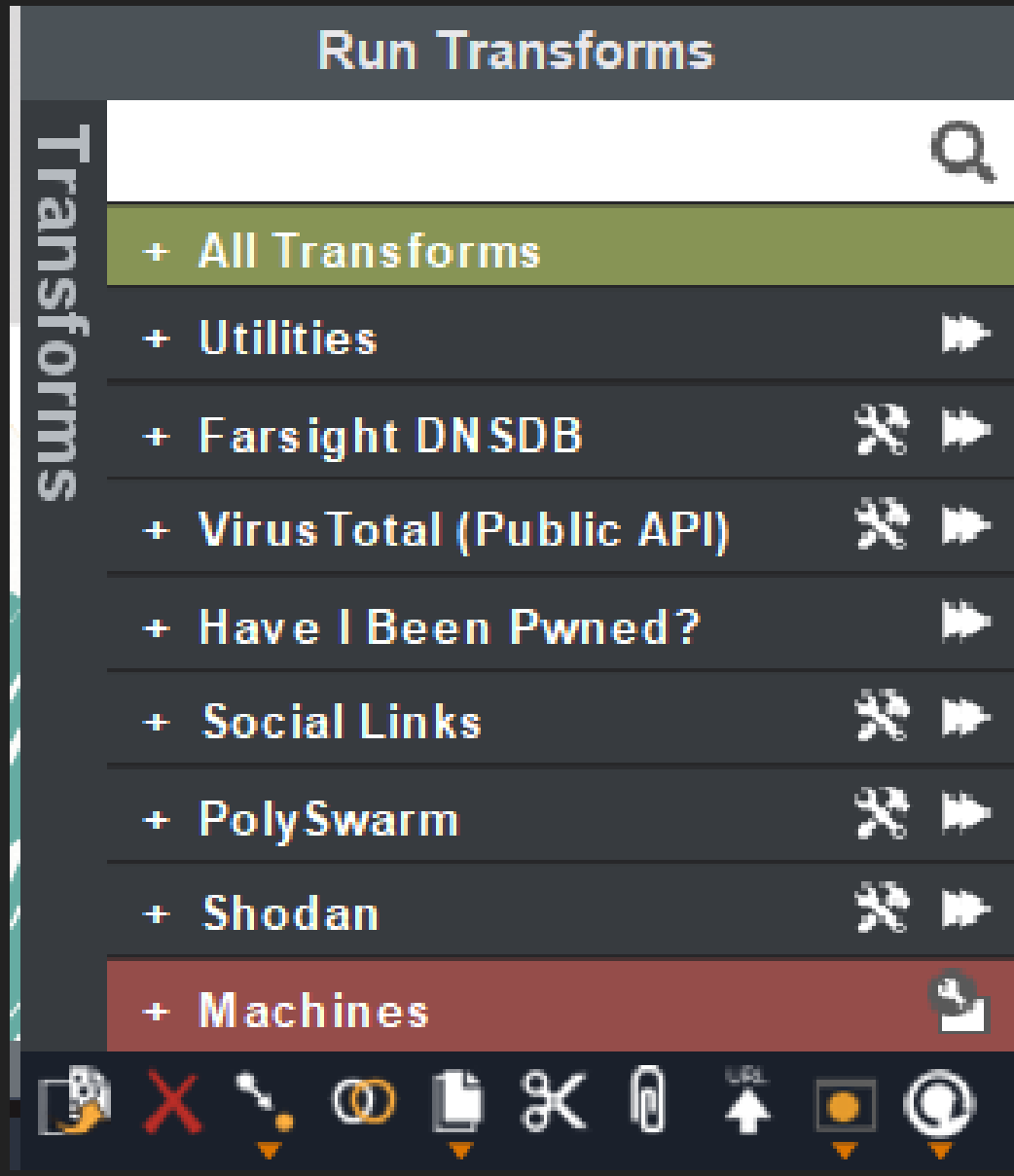
- **Maltego** is an open-source intelligence (OSINT) and graphical link analysis tool. It excels at taking disparate pieces of information from open sources and transforming them into a visual map of relationships.

- Investigators use it to uncover connections between people, groups, websites, domains, and various online infrastructure. By visualizing these links as a graph, Maltego makes it easier to spot patterns, identify key connections, and understand complex networks that might be hidden in raw data.

Maltego

Maltego Transform Engine

1. **Definition**: Maltego's core engine, called Transforms, powers its intelligence-gathering and data-linking process.
2. **Function**: Each transform is a query that takes one piece of information (like an email, domain, or IP) and discovers related data from various sources.
3. **Automation**: Transforms automate the process of connecting data across multiple OSINT and commercial APIs.
4. **Customization**: Users can create custom transforms to integrate internal data sources or APIs using Maltego TRX (Python framework).
5. **Integration Hub**: Access hundreds of pre-built transforms through the Transform Hub, integrating platforms like: Shodan, VirusTotal Have I Been Pwned, Whois, XMLRecorded Future, Social media and DNS databases
6. **Outcome**: Enables investigators to move from a single data point to a full intelligence map with just a few clicks.



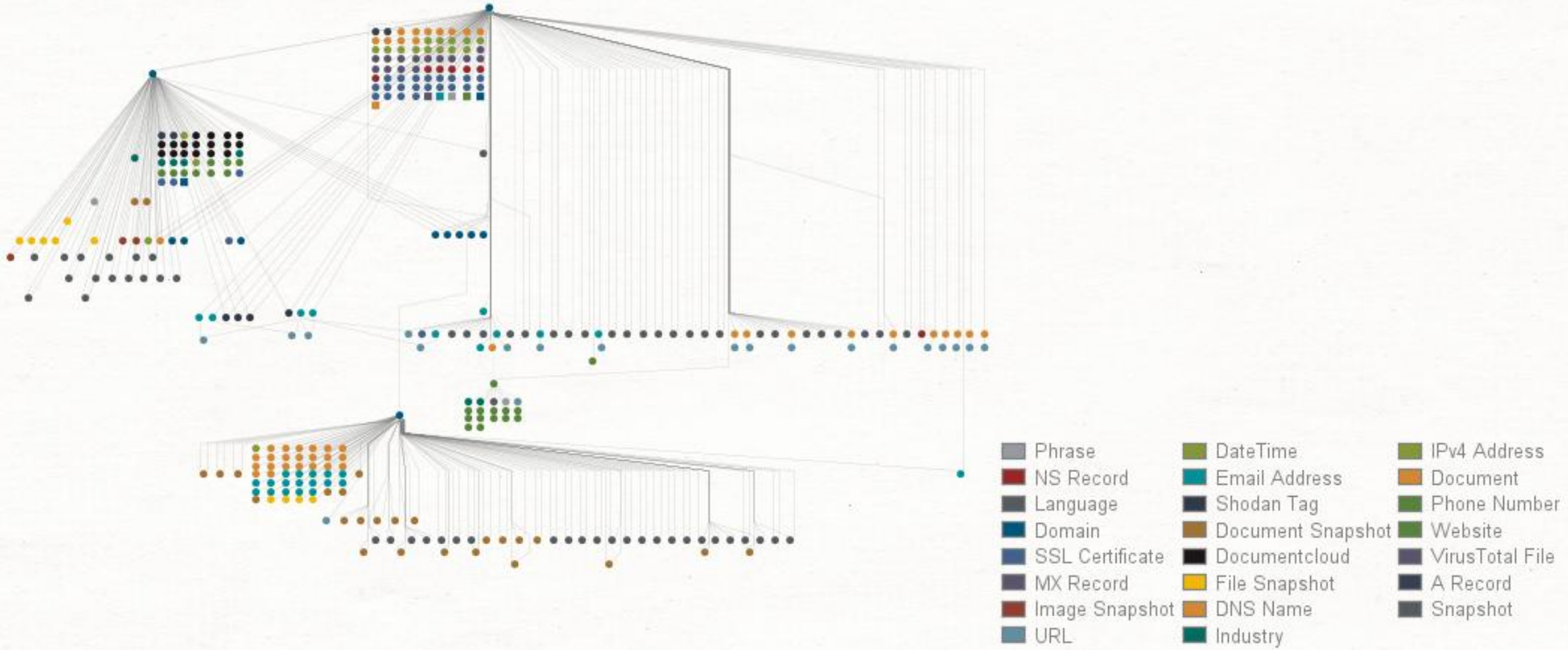


Image Shows Maltego OSINT Framework Info Gathering Results

Spider-foot

- **SpiderFoot** is an automated OSINT reconnaissance tool. Its main purpose is to automate the process of gathering intelligence about a specific target, which could be an IP address, domain name, email address, or username.

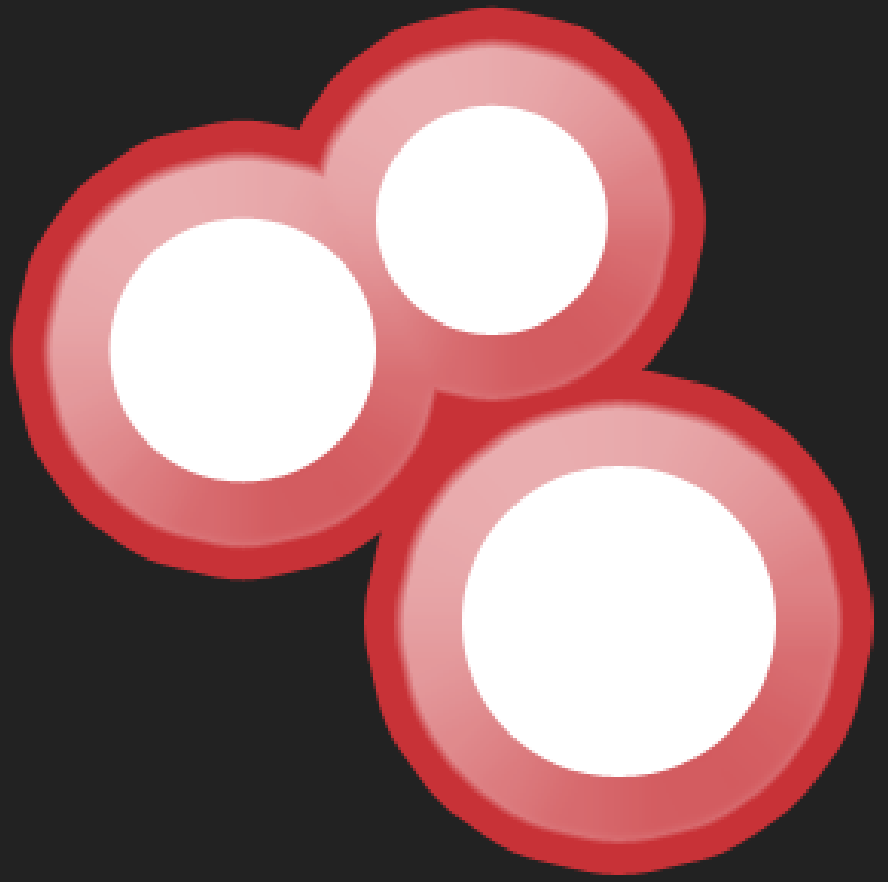
- **SpiderFoot** queries over 200 open-source data sources to collect a wide range of information, such as associated emails, subdomains, social media accounts, and potential vulnerabilities.

- By automating this data collection, SpiderFoot saves significant time and helps to quickly build a comprehensive profile of the target

Image Shows Spider-foot framework Info Gathering Results

Shodan

- **What is Shodan?**
  A specialized search engine that indexes devices and services connected to the internet, rather than websites.
- **Asset Discovery**
  Identifies a target organization's internet-facing assets, including servers, webcams, routers, traffic lights, and Industrial Control Systems (ICS).
- **Technology Profiling**
  Reveals the specific software versions, operating systems, and hardware models in use. For example, it can find all servers running a specific version of Apache in Mosul.
- **Vulnerability Identification**
  Allows searching for devices with default credentials, missing security patches, or known vulnerabilities (CVEs).
- **Creating Realistic Pretexts**
  An attacker can use Shodan to find a real, verifiable technical issue and then contact an employee posing as an IT support technician, referencing the specific server and its vulnerability, making their request to 'apply a patch' (click a malicious link) seem legitimate.
- **Physical Intelligence**
  Unsecured webcams discovered through Shodan can provide live views inside offices, revealing employee routines, what software is on their screens, or even passwords written on sticky notes.



Country	[redacted]
City	[redacted]
Organization	**Verizon Business**
ISP	**Verizon Business**
ASN	**AS701**

Web Technologies

JavaScript Frameworks

MooTools

webcamXP 5

webcamXP 5

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7486
Cache-control: no-cache, must revalidate
Date: Sat, 18 Oct 2025 18:06:27 GMT
Expires: Sat, 18 Oct 2025 18:06:27 GMT
Pragma: no-cache
Server: webcamXP 5
```

Image Shows Shodan Discovery of open webcam to the World

TwinSanity-Recon: An Automated Reconnaissance Framework

- **Automated Reconnaissance**
  TwinSanity-Recon is an open-source intelligence (OSINT) framework that automates the process of gathering information about a target.
- **Subdomain Enumeration**
  Discovers a wide range of subdomains associated with a primary domain, which often have weaker security than the main website.
- **Automated Vulnerability Scanning**
  Actively scans discovered assets for Common Vulnerabilities and Exposures (CVEs), providing the attacker with a list of exploitable weaknesses.
- **Information Aggregation**
  Integrates with other tools and services (including Shodan) to consolidate data and create a detailed map of the target's attack surface.
- **Targeted Attacks (Spear Phishing)**
  Knowledge of specific technologies and vulnerabilities allows an attacker to craft highly convincing spear-phishing emails.
- **Exploiting Internal Trust**
  Knowledge of non-public subdomains allows an attacker to create emails that appear to originate from an internal system, increasing the likelihood that the target will trust the message.

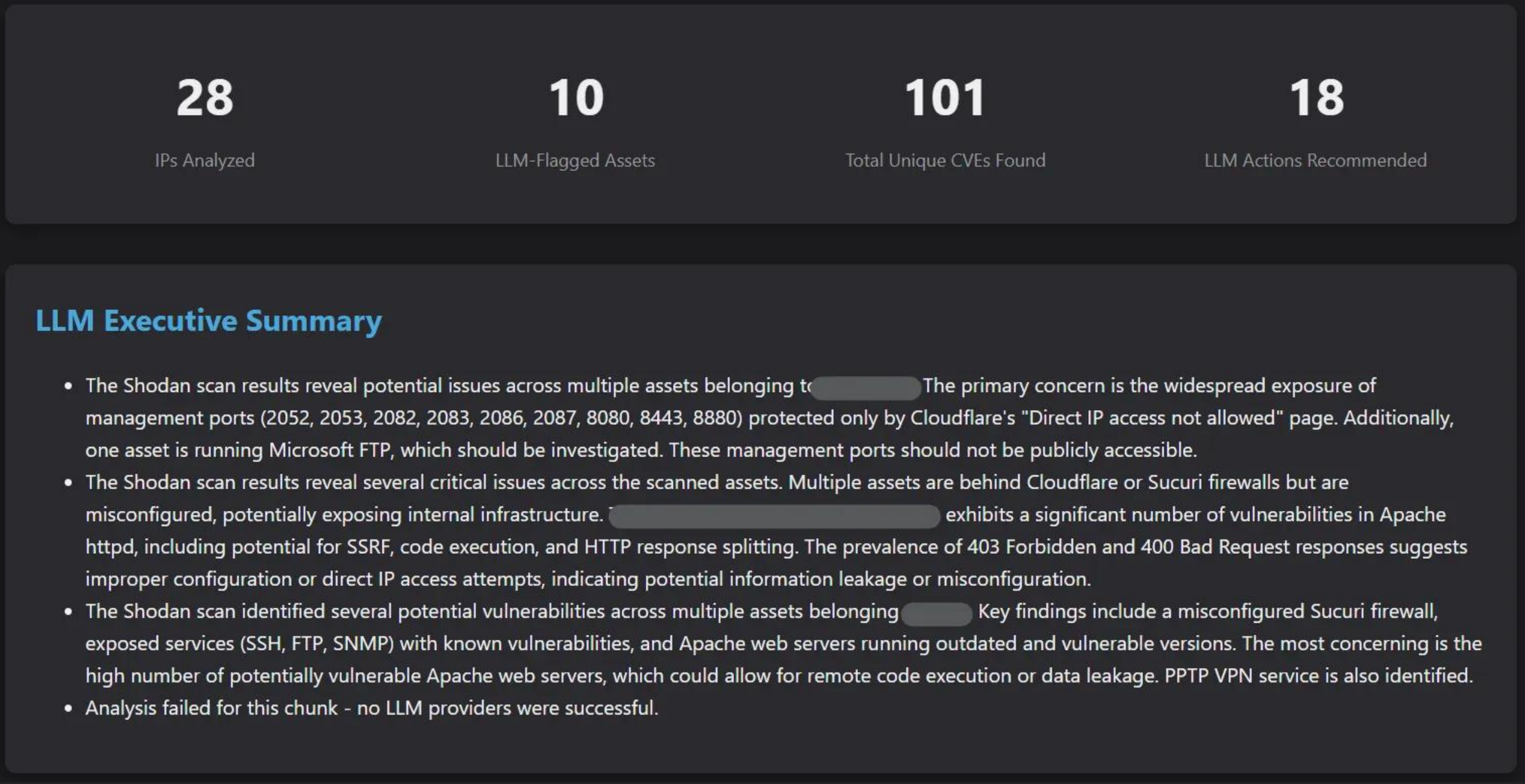


Figure 1 (Results of TwinSanity-Recon)

CVE-2024-38476	9.8	7	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
CVE-2024-38474	9.8	7	Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.
CVE-2022-23943	9.8	3	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

Figure 2 (Results of TwinSanity-Recon)

Comprehensive Vulnerability Listing (101 found)

This is a complete list of all vulnerabilities found across all scanned IPs. Use the search box to filter and click headers to sort.

CVE-2024-38476

CVE ID	CVSS	# Hosts	Summary	Affected IPs
CVE-2024-38476	9.8	7	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.	[redacted]

Figure 3 (Results of TwinSanity-Recon)

LLM Recommended Actions

Priority	Action	Justification
Critical	Restrict access to management ports (2052, 2053, 2082, 2083, 2086, 2087, 8080, 8443, 8880) to authorized IP addresses only, using firewall rules.	These ports are typically used for administrative purposes and should not be publicly accessible.
High	Investigate and secure the Microsoft FTP server on [redacted] Consider disabling it if not required or ensure it's using the latest security patches and strong authentication methods.	FTP is inherently insecure, and STARTTLS does not fully mitigate the risks. Unnecessary services should be disabled, and necessary ones must be hardened.
Medium	Review the Cloudflare configuration for the domain [redacted] to ensure it is correctly configured and that the website is only accessible via the domain name and not via direct IP access.	The 'Direct IP access not allowed' message indicates that direct access to the IP is blocked, but it would be better to redirect to the domain name to improve user experience and avoid exposing the underlying infrastructure.
Medium	Review the Plesk configuration for the domain [redacted] and ensure the default page is removed.	The presence of the default Plesk page reveals software version information and indicates that the site might be misconfigured.

Figure 4 (Results of TwinSanity-Recon)

Data Breaches and Their Impact

Data breaches have become a significant threat in the cybersecurity landscape, exposing organizations and individuals to a wide range of risks. Attackers can leverage the information obtained from these breaches to craft sophisticated strategies, including social engineering attacks, that aim to compromise systems, steal sensitive data, and disrupt operations. Understanding the impact of data breaches and how they can be exploited is crucial for developing effective cybersecurity measures.

Images Shows Data Breach via Exploiting vulnerability in organization System System

```
black@Black:[redacted]$ head -n 20 DATA1_fixed.json
{"lang": "en_US", "tz": "Asia/Baghdad", "uid": 1667, "allowed_company_ids": [1], "params": {"cids": 1, "menu_id": 162, "action
": 538, "model": "g2p.group.membership", "view_type": "list"}, "bin_size": true}
{"id": 892255, "group": [1077321, "6540149141"], "individual": [1077306, "نسح زاندع لالد"], "kind": [], "head_member": [107730
9, "زيسح دبع لوسر"], "relation_to_head": [9, "2 - Wife"], "start_date": "2023-01-28 17:02:01"}
{"id": 892254, "group": [1077322, "6450013756"], "individual": [1077308, "نسحلادبع دمحم هللادبع"], "kind": [], "head_member":
[1077305, "نوسح دمحم نسحلادبع"], "relation_to_head": [13, "6 - Other"], "start_date": "2023-01-28 17:02:01"}
{"id": 892253, "group": [1077317, "6510210786"], "individual": [1077304, "يدامح وطم هفادرا"], "kind": [], "head_member": [1077
307, "ديبع مجاح ميك"], "relation_to_head": [9, "2 - Wife"], "start_date": "2023-01-28 17:02:01"}
{"id": 892252, "group": [1077321, "6540149141"], "individual": [1077302, "دبع لوسر ضترم"], "kind": [], "head_member": [107730
9, "زيسح دبع لوسر"], "relation_to_head": [14, "9 - Son/Daughter"], "start_date": "2023-01-28 17:02:01"}
{"id": 892251, "group": [1077322, "6450013756"], "individual": [1077305, "نوسح دمحم نسحلادبع"], "kind": [1], "head_member": [1
077305, "نوسح دمحم نسحلادبع"], "relation_to_head": false, "start_date": "2023-01-28 17:02:01"}
{"id": 892250, "group": [1077317, "6510210786"], "individual": [1077300, "مجاح ميك ضترم"], "kind": [], "head_member": [10773
07, "ديبع مجاح ميك"], "relation_to_head": [14, "9 - Son/Daughter"], "start_date": "2023-01-28 17:02:01"}
{"id": 892249, "group": [1077321, "6540149141"], "individual": [1077299, "دبع لوسر دمحم"], "kind": [], "head_member": [1077309
, "زيسح دبع لوسر"], "relation_to_head": [14, "9 - Son/Daughter"], "start_date": "2023-01-28 17:02:01"}
```

(Before Analysis)

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	record_id	record_type	group_id	group_ref	individual_id	individual_name	head_member_id	head_member_name	relation_code	relation_description	kind	start_date	group_name
2	892255	Household Membe	1077321	6540149141	1077306	[redacted]دلال	1077309	[redacted]رسول	9	2 - Wife		2023-01-28 17:02:01	
3	892254	Household Membe	1077322	6450013756	1077308	[redacted]عبدالله	1077305	[redacted]عبدالحسن	13	6 - Other		2023-01-28 17:02:01	
4	892253	Household Membe	1077317	6510210786	1077304	[redacted]اردافه	1077307	[redacted]كريم	9	2 - Wife		2023-01-28 17:02:01	
5	892252	Household Membe	1077321	6540149141	1077302	[redacted]مرتضى	1077309	[redacted]رسول	14	9 - Son/Daughter		2023-01-28 17:02:01	
6	892251	Household Membe	1077322	6450013756	1077305	[redacted]عبدالحسن	1077305	[redacted]عبدالحسن			1	2023-01-28 17:02:01	
7	892250	Household Membe	1077317	6510210786	1077300	[redacted]مرتضى	1077307	[redacted]كريم	14	9 - Son/Daughter		2023-01-28 17:02:01	
8	892249	Household Membe	1077321	6540149141	1077299	[redacted]محمد	1077309	[redacted]رسول	14	9 - Son/Daughter		2023-01-28 17:02:01	
9	892247	Household Membe	1077317	6510210786	1077290	[redacted]احمد	1077307	[redacted]كريم	14	9 - Son/Daughter		2023-01-28 17:02:01	

(After Analysis)

Stage 2 (Attack Strategy Development)

Leveraging Gathered Information from Social Media and Organization

Attackers can use the Gathered information from OSINT tools like like Maltego of target's interests, interests, activities, and connections connections within the organization. organization. This information can be can be used to start conversations conversations and open new communication channels, such as as through social media apps or the the organization's website.

Impersonation and Social Engineering

Attackers may impersonate people in higher positions, such as the CEO, to obtain sensitive information from the target that should not be disclosed. This technique is used by some companies to target other companies and gather information about their future plans or projects.

Building Rapport and Establishing Establishing Trust

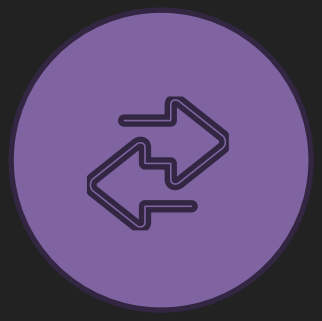
Attackers can leverage the gathered information to build rapport and establish trust with the target, making them more likely to share sensitive information or fall for social engineering tactics.

By leveraging the information gathered during the reconnaissance stage, attackers can initiate conversations, build trust, and establish new communication channels with the target, ultimately making them more vulnerable to social engineering attacks.

Stage 3 (Weaponization and Delivery)

Email Delivery

Static Phishing



Dynamic Phishing

Malware Delivery

Attackers employ a variety of sophisticated techniques to exploit human vulnerabilities and gain unauthorized access to systems and data. Understanding these methods is crucial for developing effective countermeasures and strengthening organizational security posture.

Email Delivery

- **Free Webmail Providers**
  Using regular Google SMTP or similar free webmail is commonly seen in simulations, but less effective for real-world phishing.
- **Compromised Accounts**
  Attackers may leverage compromised email accounts to improve deliverability and evade detection.
- **Abused ESP Access**
  Attackers may gain unauthorized access to email service provider (ESP) accounts to send phishing emails.
- **Look-alike Domains**
  Attackers may use domains that closely resemble legitimate ones to increase the chances of successful phishing.
- **Botnets**
  Attackers may utilize botnets, networks of compromised devices, to send phishing emails and evade detection.
- **Underground SMTP Services**
  Attackers may utilize underground SMTP services, which are designed to maximize deliverability and evade detection, for their phishing campaigns.

Email delivery is the channel used to send phishing; real attackers Favor covert, high-deliverability methods that maximize trust.

Static Phishing Attacks

Gophish Email Campaign

- A fake email pretending to be from a bank asking the user to log in via a phishing link.
- The login page is static and does not interact with the real bank server.

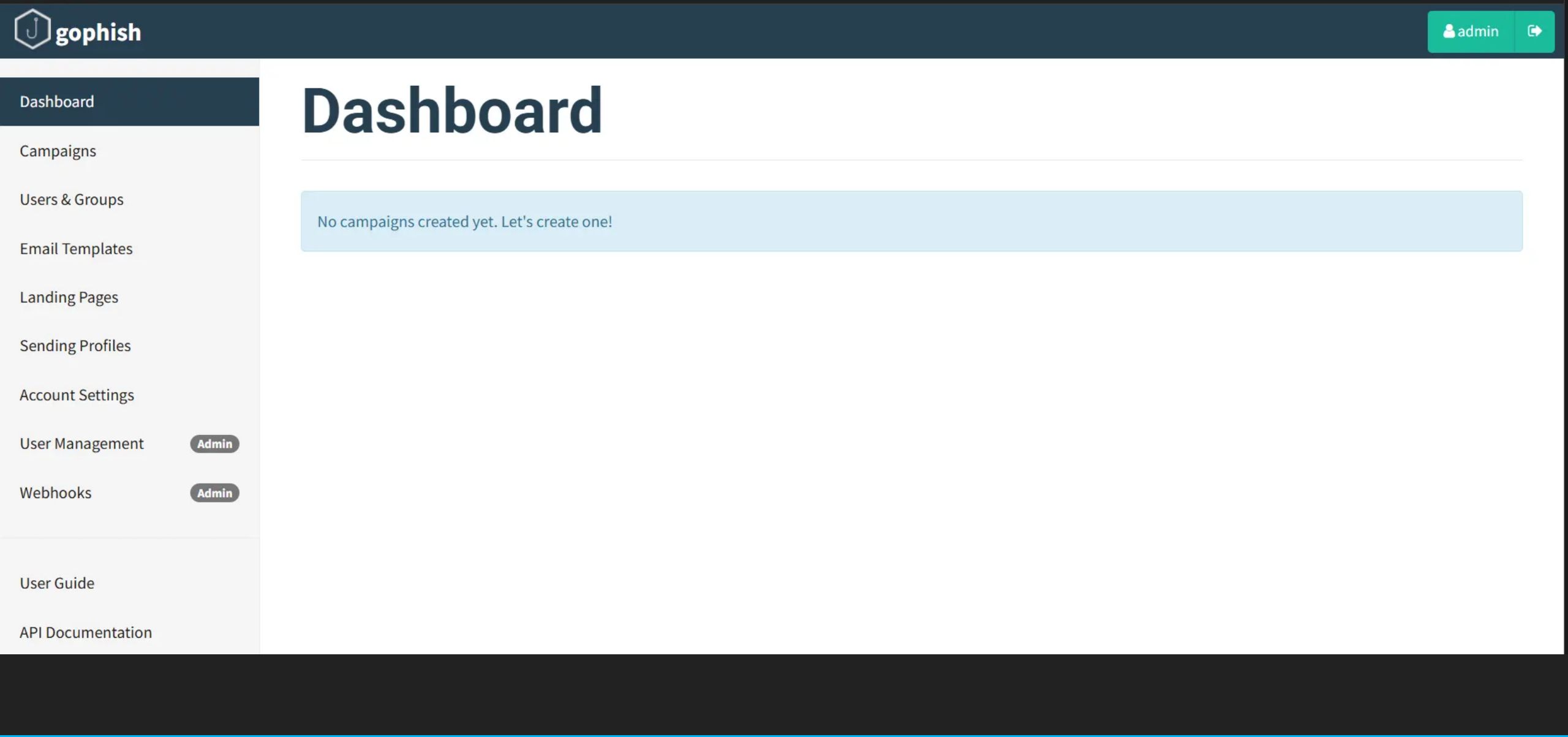
Fake Social Media Login Page

- A cloned Facebook or Instagram login page hosted on a different domain.
- User enters credentials, which are stored in the attacker's database.

Malicious PDF or Document Link

- A document with embedded phishing links that redirect to a static login page.

Attackers create fake websites or emails that mimic legitimate services to trick users into revealing credentials or sensitive information. These attacks do not adapt in real-time and rely on human error, making awareness, training, and technical defences' critical to prevent compromise.



A good Example of Static Phishing is Gophish landing pages.

Dynamic Phishing Attacks

Evilginx2 Attack

- The attacker proxies the real login page, capturing session cookies and credentials in real-time.
- Works even if MFA is enabled.

Modlishka Proxy

- A dynamic reverse proxy that that forwards users to the legitimate site while harvesting credentials and and session tokens.

Real-Time Banking Phishing

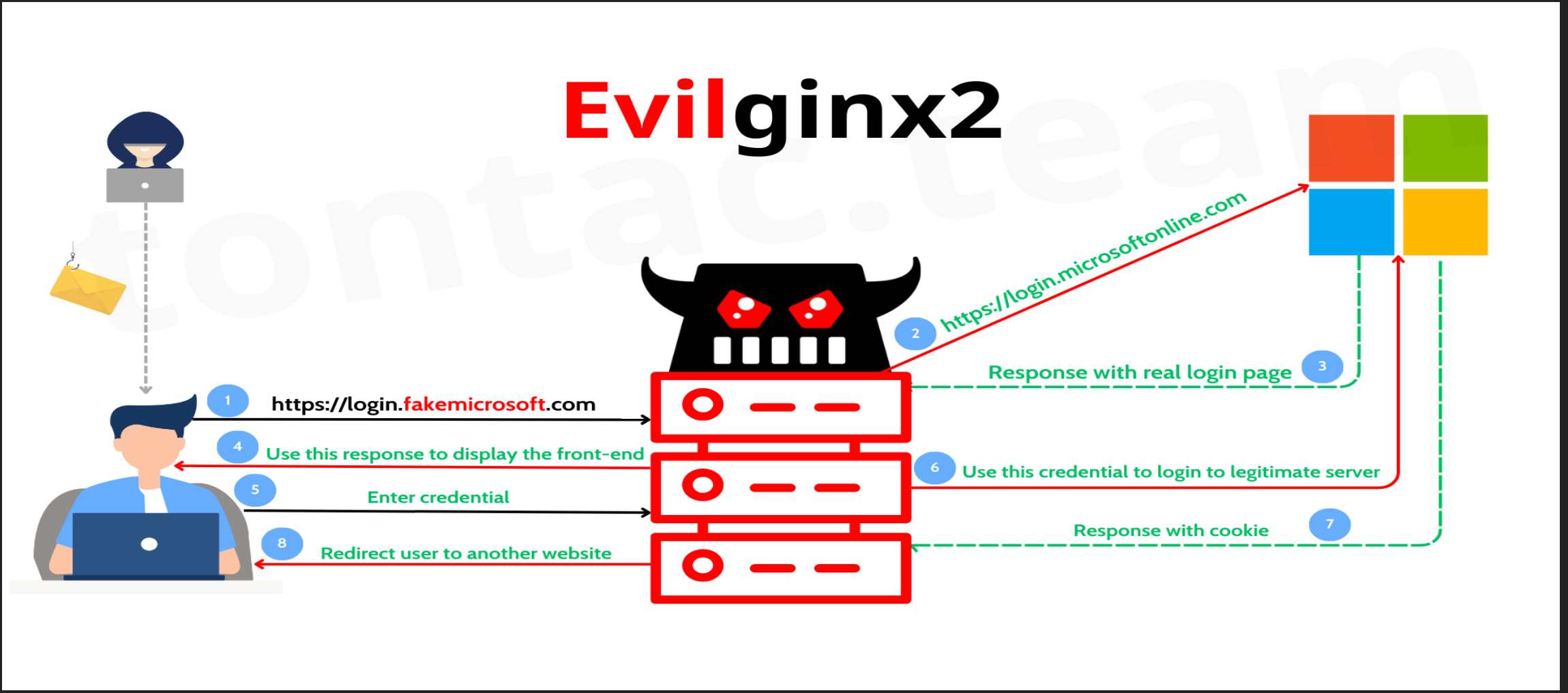
- The phishing page interacts with the bank's actual login server, generating real OTP codes and session tokens to bypass 2FA.

Dynamic phishing is a type of phishing attack that adapts in real-time to the target's environment, often bypassing security measures such as Multi-Factor Authentication (MFA) or security warnings. It usually uses a **live proxy or real-time interaction** with the legitimate site to steal credentials or session tokens.

Road to Advanced Phishing..

A server the attacker runs that sits between the victim and the real website, forwarding traffic both ways while the attacker inspects or modifies the traffic.

Adversary-in-the-Middle (AiTM) Attacks



Adversary-in-the-Middle (AiTM) attack is a targeted, real-time phishing technique where the attacker operates a proxy between the victim and the legitimate service to intercept and manipulate the live authentication flow — capturing credentials, session cookies, tokens, or one-time codes so the attacker can immediately take over the session (often bypassing MFA).

Malware Delivery

Remote Access Trojans

Malware that provides backdoor access to the attacker, allowing them to control the infected system remotely.

Ransomware (TOP 1)

Malware that infiltrates devices and holds files hostage, compelling victims to pay a ransom to regain access to their encrypted data

Spyware

Malware that collects and sends sensitive data, such as browsing history, location, and other personal information, to the attacker.

Key loggers

Malware that records user keystrokes, including sensitive information like login credentials and credit card numbers.

Cryptocurrency Miners

Malware that hijacks the infected system's resources to mine cryptocurrency for the attacker's financial gain.

Malware is malicious software's delivered via phishing messages (links, attachments, or payloads) designed to steal credentials/data, gain persistent access, move laterally, or extort victims.

Stage 4 (Execution and Impact)

Phishing Attack Execution

In this stage, the attacker executes the phishing attack by sending the malicious email or message to the target user. This could involve impersonating a legitimate organization or individual to gain the user's trust and trick them into revealing sensitive information or performing an action that compromises their system.

Achieving the Goal

Once the user falls for the phishing attempt and takes the desired action, the attacker achieves their goal, which could be obtaining login credentials, installing malware, or gaining unauthorized access to the target's system or network.

Escalating the Attack

The attacker may then use the gained access or information to further their malicious activities, such as launching more sophisticated attacks like Advanced Persistent Threats (APTs) or deploying ransomware. These types of attacks can have far-reaching consequences, potentially causing significant financial and operational damage to the targeted organization.

Real-World Implications

Significant Financial Losses

Successful social engineering attacks can lead to substantial financial losses for organizations, from theft from theft of funds to costly data breaches and recovery recovery efforts.

Reputational Damage

High-profile social engineering attacks can severely severely damage an organization's reputation, eroding eroding trust with customers, partners, and the public, public, and leading to long-term consequences.

Operational Disruption

Attackers can leverage social engineering tactics to gain to gain access to critical infrastructure and systems, systems, causing widespread operational disruptions that disruptions that impact businesses and the public. public.

Regulatory Scrutiny

Successful social engineering attacks often lead to increased regulatory oversight and enforcement, as organizations are required to demonstrate robust security measures to protect sensitive data and systems.

Social engineering attacks can have far-reaching and devastating consequences, from financial losses to operational disruptions and reputational damage.
The sophisticated tactics employed by threat actors demand a proactive and comprehensive approach to cybersecurity.

Case Study's

2013

Target Data Breach: Credential Theft from Vendors Leads to Massive Customer Data Theft

2016

Bangladesh Bank SWIFT Heist: Targeted Malware and Spear-Phishing Used to Gain Access to Financial Systems

2020

Twitter Account Hijack: Coordinated Social Engineering Attacks Compromise High-Profile Accounts

2021

Colonial Pipeline Ransomware: Compromised VPN Account Without MFA Enables Ransomware Deployment

Bangladesh Bank SWIFT Heist (Feb–Mar 2016)

Unauthorized Access

Attackers entered Bangladesh Bank's systems using spear-phishing and custom malware to steal SWIFT credentials and monitor network activity.

Fraudulent SWIFT Transfers

They issued ~36 fraudulent SWIFT instructions to the New York Fed, attempting to move nearly $951 million. Of these, $81 million was successfully transferred to accounts in the Philippines, while one $20 million request to Sri Lanka was blocked

Attempted Cover-up

Malware deleted or altered logs, intercepted printer outputs, and disabled alerts to mask the unauthorized transactions.

Strengthened Defenses

Afterwards, banks worldwide adopted stricter controls: network segmentation, hardened access policies, real-time anomaly monitoring, and SWIFT's Customer Security Program (CSP).

This attack demonstrates the significant impact that targeted malware and spear-phishing can have on financial systems, highlighting the importance of robust cybersecurity measures to protect critical infrastructure.

Attack Vector Breakdown

Attackers use OSINT tools and and techniques to collect data data from social media, websites, websites, data breaches, and other public sources to build a a comprehensive understanding understanding of the target.

With the gathered information, information, attackers craft social social engineering tactics, such as such as phishing emails and communication channels outside outside of email, to establish trust trust and gain access to the target.

Attackers exploit the established established communication channels to deliver malware, such such as information stealers, downloaders, or banking trojans, trojans, and use techniques like like adversary-in-the-middle (AiTM) attacks to bypass security security controls.

The final stage of the attack process, where the attacker achieves their goal, which can range from data theft and financial fraud to the deployment of more advanced malware like ransomware, causing severe consequences for the target.

Stage 5 (Mitigations)

1. Email Authentication

Enforce SPF, DKIM, and DMARC to stop email spoofing

2. Phishing-Resistant MFA

Use FIDO2/WebAuthn security keys for high-risk users

3. Email Gateway

Rewrite URLs and sandbox attachments to block malware

4. Endpoint Detection

Leverage EDR with memory/behavioral analysis to catch threats

5. Domain & Certificate Monitoring

Detect look-alike domains and unexpected certificates early

6. Secure Backups

Implement immutable, air-gapped backups to protect against ransomware

7. Phishing Simulation

Train users to identify and report phishing attempts

Stage 5 (Useful Tools)

#	Control	Primary Tool (recommended)	Free / Low-cost Alternative	Explain
1	Email Authentication (SPF / DKIM / DMARC)	**Valimail Authenticate**	**MXToolbox** (checks & reports)	Automates SPF/DKIM enforcement and centralizes DMARC reporting to stop spoofing.
2	Phishing-Resistant MFA (FIDO2 / WebAuthn)	**Secret Double Octopus**	**Windows Hello / WebAuthn** (built-in)	Provide phishing-resistant, passwordless login for high-risk users (FIDO2/push).
3	Email Gateway (URL rewrite & sandbox)	**SpamTitan**	**Proxmox Mail Gateway**	Rewrite URLs and detonate attachments in a sandbox before delivery.
4	Endpoint Detection & Response (EDR)	**CrowdStrike Falcon**	**Wazuh / Velociraptor**	Behavioral + memory analysis to detect, investigate and contain endpoint threats.
5	Domain & Certificate Monitoring	**CertPing**	**DNSTwist + crt.sh**	Detect look-alike domains and unexpected TLS certificates with real-time alerts.
6	Secure Backups (Immutable / Air-gapped)	**Veeam Data Platform**	**Restic + immutable object store**	Store immutable, air-gapped backups with safe restore options against ransomware.
7	Phishing Simulation & Training	**KnowBe4**	**GoPhish**	Run realistic phishing campaigns and push targeted awareness training to users.

Resources of Lecture

Telegram Resources Channel

Telegram Contact:

For navigate to links press: Ctrl + click

Maltego OSINT Framework

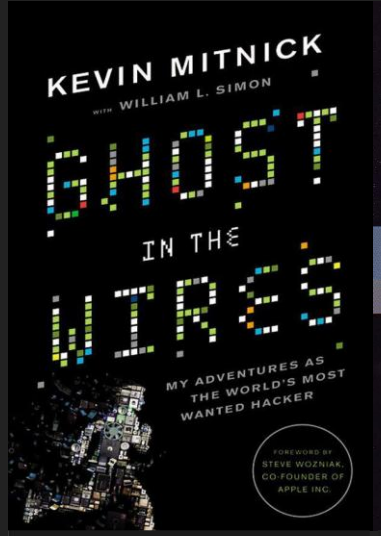
Spider-foot OSINT Framework

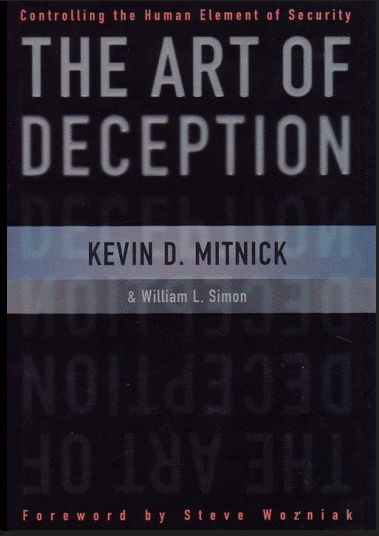
Shodan Search Engine

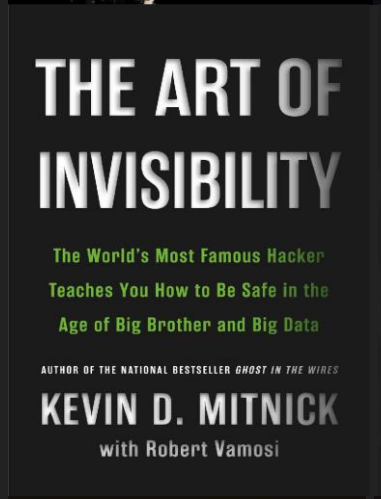
TwinSanity-Recon Framework

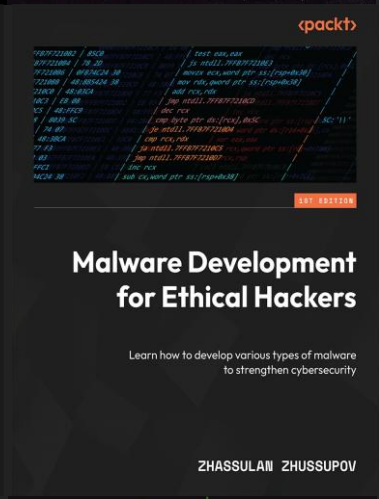
Gophish Phishing Toolkit

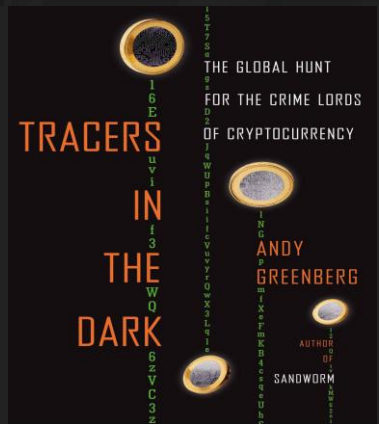
Evilginx Framework












Thank You