BLACKFOG™

The 7 Most Common Social Engineering Attacks

AND HOW TO MITIGATE THEM



Contents

Overview 3
What Is Social Engineering? 4
The 7 Common Types of Social Engineering 6
1. Phishing 7
2. Spear Phishing 9
3. Vishing 11
4. Smishing 13
5. Pretexting 15
6. Baiting 17
7. Whaling 19
Take Your Next Steps With BlackFog 21

Social engineering attacks are on the rise. Learn how to protect your organization with this comprehensive guide, covering the seven most common types of attacks. This guide covers vishing, smishing, pretexting, baiting, and whaling, and provides expert tips on how to prevent data breaches, ransomware attacks, and other cyberthreats.

What Is Social Engineering?

Attackers use social engineering as a manipulation technique to gain unauthorized access to systems or sensitive information by exploiting human psychology and behavior. Unlike methods that target technical vulnerabilities, social engineering exploits human weaknesses to compromise security. A cybersecurity report revealed that 98% of all cyberattacks use social engineering tactics, demonstrating the techniques' effectiveness.

A notable real-world example of a social engineering attack occurred in 2016 when hackers targeted the Democratic National Committee (DNC) during the U.S. presidential election. The attackers crafted a convincing spear-phishing email that appeared to come from Google, prompting the recipient to change their password due to suspicious activity. The email directed the user to a fake Google login page, which captured their credentials when entered. Using this method, the attackers gained access to the DNC's network, leading to a significant data breach and leaked sensitive information.

Generally speaking, social engineering attacks follow three different phases:

1

Discovery and Investigation

In this phase, the attacker conducts extensive research and gathers as much information as possible about the target organization, its employees, roles, interests, online presence, and security posture. Techniques utilized include open-source intelligence gathering (OSINT), social media analysis, dumpster diving, and physical surveillance. The goal is to identify potential entry points, vulnerabilities, and individuals to target.

2

Deception and the Hook

Here, the attacker creates a believable pretext or scenario to gain the target's trust and interest. This often involves impersonating legitimate entities, such as colleagues, IT support, or trusted organizations - a technique known as pretexting. Baiting is another tactic, where the attacker leaves physical media like malicious USB drives or sets up websites with malicious code to entice the target.

3

The Actual Attack

Once trust is established, the attacker executes the actual exploit. Common methods include phishing (sending fraudulent emails/messages to trick recipients into revealing information or installing malware), vishing (voice phishing using fake calls/messages), tailgating (following authorized personnel through secure entrances), and shoulder surfing (directly observing targets entering credentials or sensitive data).

THE 7 COMMON TYPES OF SOCIAL ENGINEERING

These seven types of social engineering attacks – phishing, spear phishing, vishing, smishing, pretexting, baiting, and whaling – are among the most frequently employed tactics used by cybercriminals to deceive and manipulate victims.

While each type of attack has its distinct characteristics and methods, they all share the common objective of exploiting human trust and tricking individuals into divulging sensitive information or granting unauthorized access.

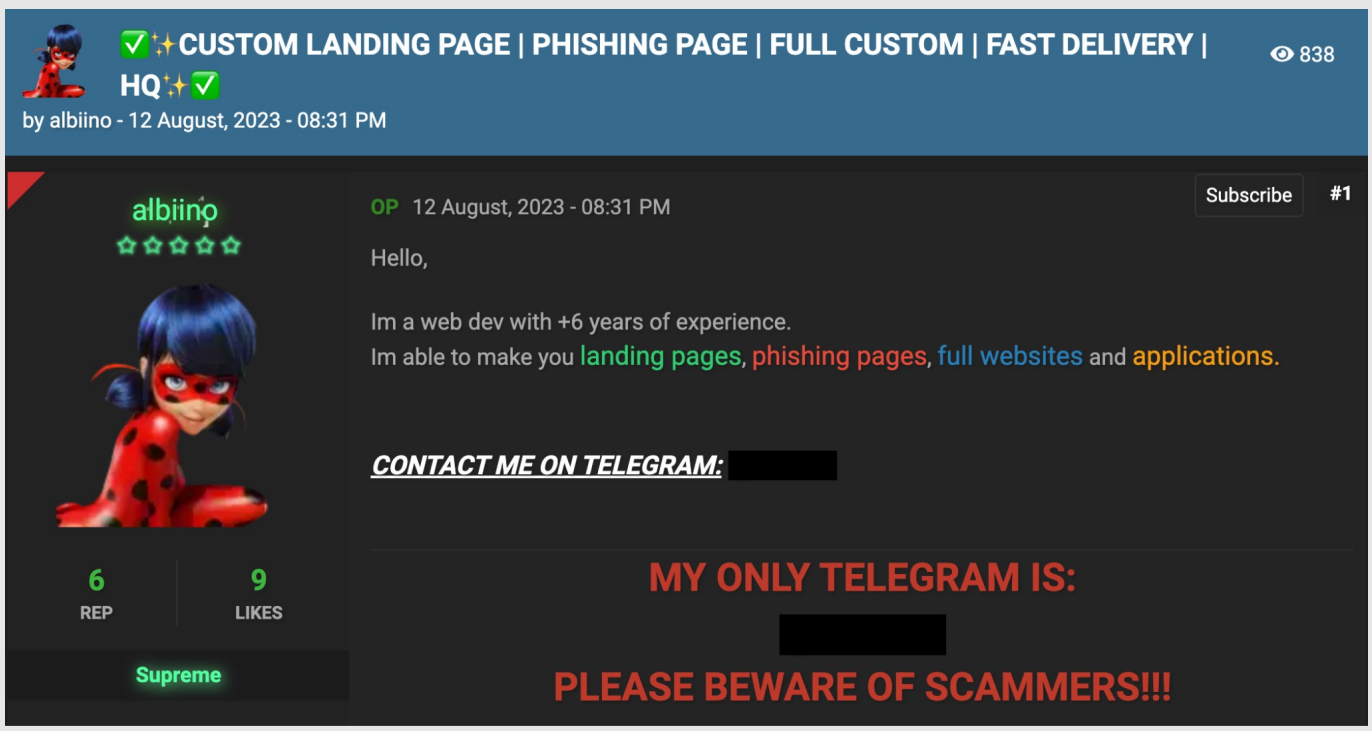
1

Phishing

Phishing is a type of social engineering attack where an attacker sends a fraudulent email, text message, or instant message that appears to come from a legitimate source, such as a bank or online retailer. The message typically asks the victim to provide sensitive information, such as login credentials or financial information.

For instance, an employee may receive an email appearing to be from their bank, asking them to click a link and verify their account information due to “suspicious activity.” However, the link actually leads to a fake website designed to steal login credentials. The message typically asks the victim to provide sensitive information in this deceptive manner.

To facilitate their phishing campaigns, cybercriminals



An example of the phishing pages that are sold and traded

often purchase or trade pre-made templates that closely mimic legitimate brands and organizations. These templates utilize email/website spoofing and lookalike domains, or mimic trusted brand logos to appear authentic.

Cybercriminals also purchase or gain access to phishing kits and email lists on underground markets to aid their campaigns. To protect against phishing attacks, use email authentication protocols such as SPF, DKIM, and DMARC to verify sender authenticity.

Additionally, deploy advanced email filtering solutions that employ machine learning algorithms to detect and block suspicious emails before they reach users' inboxes. Employees who receive regular security awareness training can also identify and report phishing attempts more quickly.

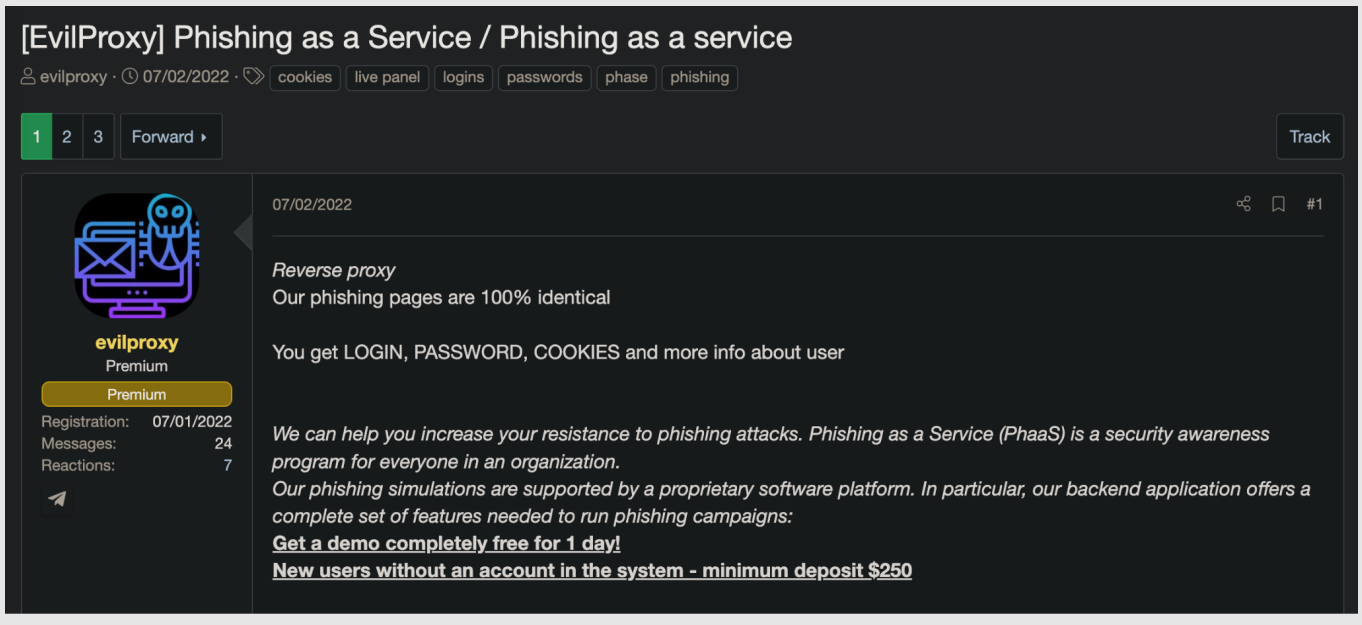
2

Spear Phishing

Spear phishing is a targeted form of phishing where an attacker gathers information about a specific individual or organization to create a highly convincing and personalized message. The emails or messages contain precise details about the victim's role, interests, and activities to increase credibility.

An example of this is an attacker researching details about a company's CEO and their upcoming business trip. They then send a personalized email mentioning specifics about the travel arrangements but claiming there is an issue with the hotel booking, to lure the CEO to enter credit card details on a malicious site.

In recent years, thriving phishing-as-a-service criminal infrastructure has emerged, with entire operations offering various



An example of phishing-as-a-service infrastructure

components needed for spear phishing campaigns. These include curated email data, automated phishing tools, and personalized email templates to enable sophisticated, targeted attacks.

You can combat spear phishing by adopting two-factor authentication (2FA) or multi-factor authentication (MFA) mechanisms to add an extra layer of security to user accounts. Encourage employees to verify unexpected or unusual requests, especially those involving sensitive information or financial transactions, through a secondary communication channel. Conduct regular security audits to identify and address vulnerabilities in your organization's digital footprint that attackers might exploit for reconnaissance.

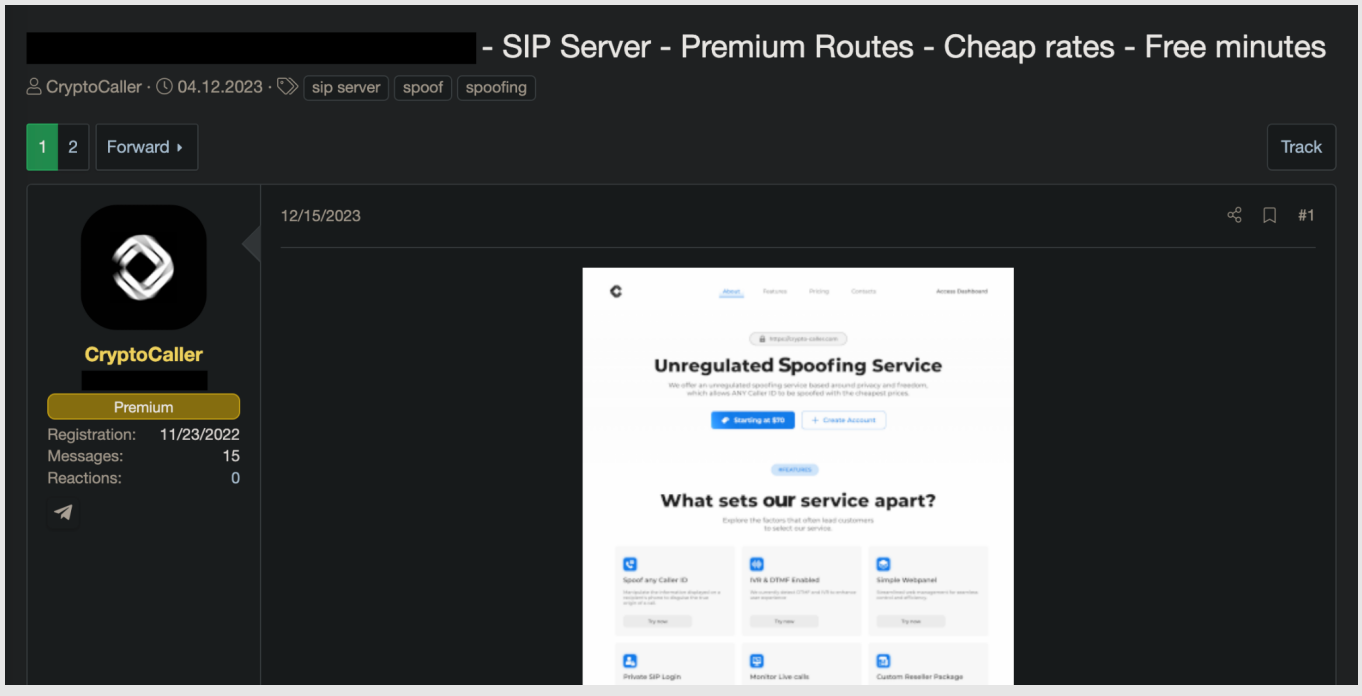
3

Vishing

With vishing, also known as voice phishing, an attacker uses a phone call to trick victims into divulging sensitive information. Attackers impersonate legitimate entities like customer support and utilize caller ID spoofing, voice-changing technology, and social engineering pretexts to appear credible.

An example of this is an attacker calling an employee while spoofing the number of the company's IT helpdesk, and claiming there is a critical system update required, to trick the employee into revealing their login credentials over the phone.

To enhance the deception, cybercriminals often rent or abuse caller ID spoofing services that allow them to display a legitimate-



An example of a caller ID spoofing service

looking phone number when making vishing calls. This makes it easier to convince victims to comply with requests for sensitive data over the phone.

Mitigate vishing attacks by educating employees about the risks of disclosing sensitive information over the phone and establishing strict verification procedures for any requests made via phone calls. Implement call authentication solutions that analyze call metadata and voice characteristics to identify spoofed calls. Maintain up-to-date records of authorized personnel and their contact information to detect and block unauthorized callers effectively.

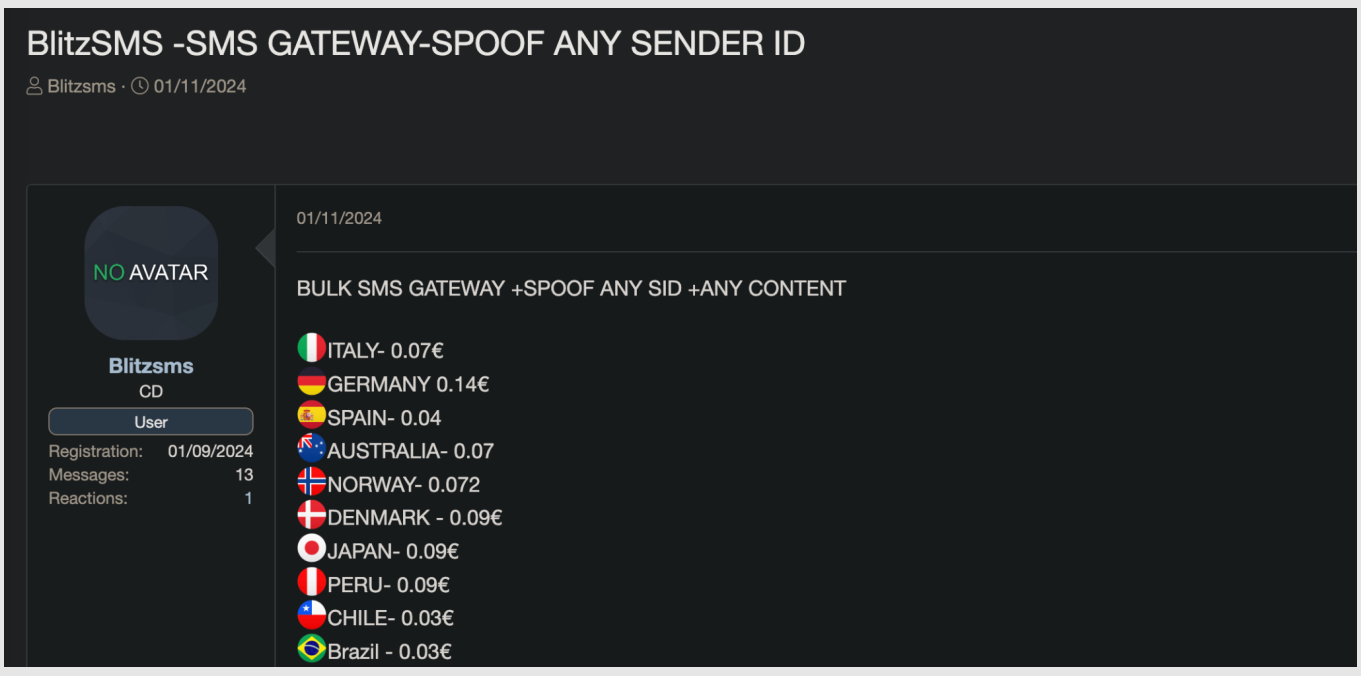
4

Smishing

Smishing, a type of social engineering attack that uses SMS or text messages, is similar to phishing but conducted over mobile channels. The lures mimic common SMS communications from banks, delivery services, etc., and contain malicious links.

An example scenario might be an employee receiving a text message impersonating a popular delivery service about a missed package delivery, with the message containing a malicious link that, if clicked, installs malware on the employee's mobile device.

To facilitate their smishing campaigns, cybercriminals frequently purchase or gain access to SIP trunking services, which allow them to send large volumes of text messages from a variety of spoofed



An example of a SMS spoofing service

numbers. This makes it harder for security systems to detect and block the smishing attacks.

To mitigate smishing attacks, deploy mobile device management (MDM) solutions that allow administrators to enforce security policies and restrict the installation of apps from unknown sources. Encourage employees to avoid clicking on links or downloading attachments from unsolicited text messages and to verify the authenticity of SMS communications through official channels whenever possible.

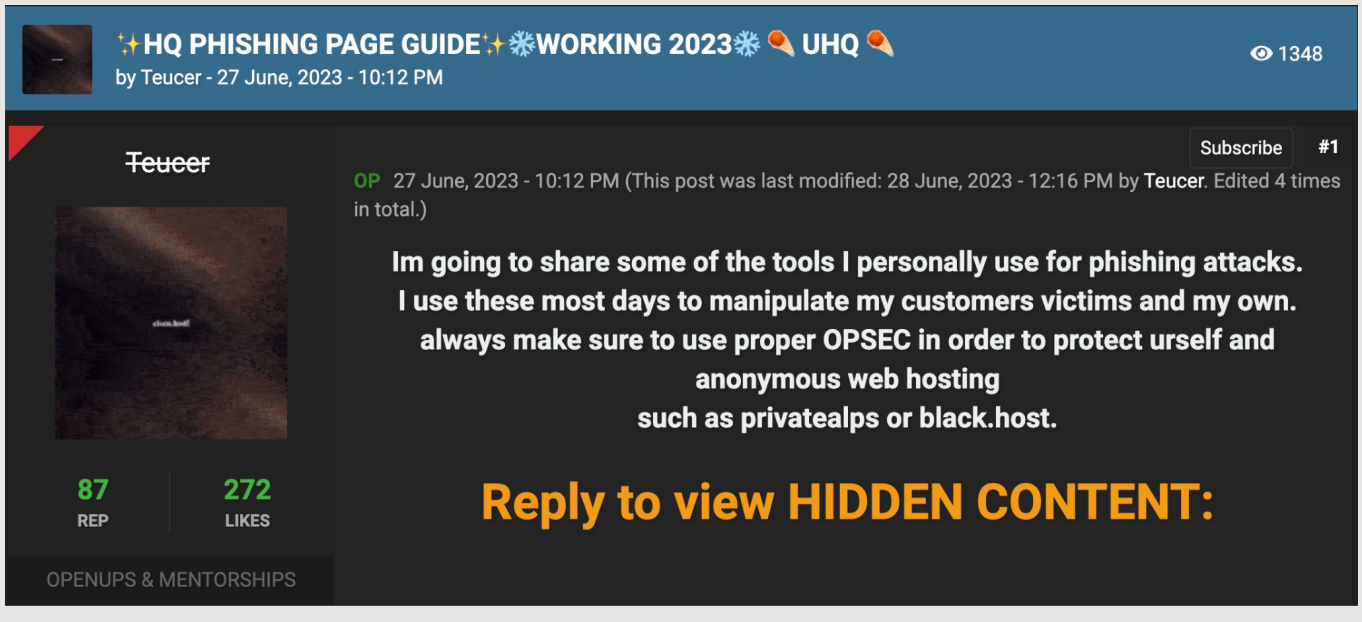
5

Pretexting

Pretexting is a type of social engineering attack where an attacker creates a fake scenario or story to gain the victim's trust. The attacker may impersonate roles like IT staff, auditors, or managers and utilize urgency or authority to convince victims to comply with requests for sensitive data under false pretenses.

For instance, an attacker could impersonate an auditor and call an accounting employee claiming to be conducting standard financial checks. Under this pretext, they could convince the employee to email them confidential financial records.

Cybercriminal forums serve as a hub for sharing tactics, improving deception skills, and exchanging guides on crafting convincing pretexts for these attacks. This allows attackers to continually refine and optimize their social engineering techniques.



An example of a cybercrime phishing guide

Combat pretexting by implementing strict access controls and authentication mechanisms to limit the exposure of sensitive information to unauthorized individuals. Establish clear policies and procedures for handling requests for confidential data, including verification steps for validating the legitimacy of the requestor's identity and authority. Conduct regular security awareness training sessions emphasizing the importance of skepticism and critical thinking when interacting with unfamiliar or unexpected requests.

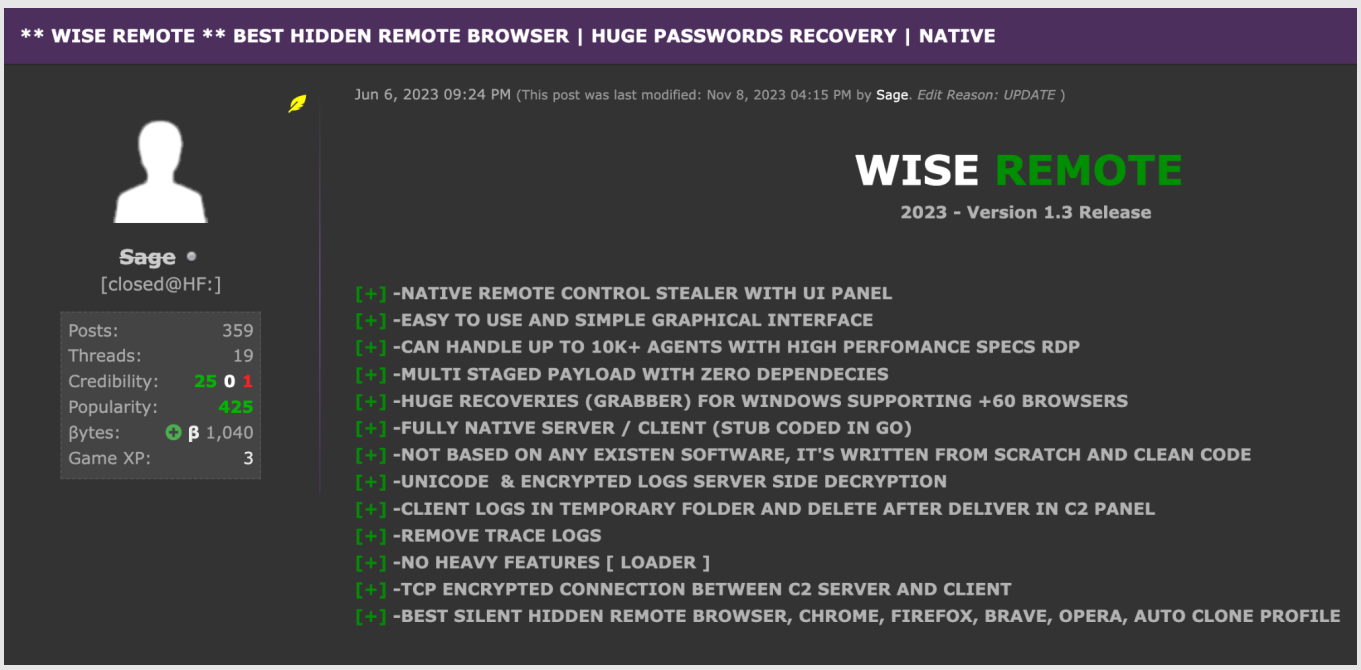
6

Baiting

Baiting is a type of social engineering attack where an attacker leaves a malware-infected device or storage media, such as a USB drive, in a public area or sends it directly to a victim. The malicious payloads used can vary, ranging from remote access tools (RATs) and keyloggers that grant unauthorized system access, to ransomware that encrypts the victim's data and demands payment.

An example of this is when an attacker leaves a USB drive labeled "Confidential Reports" in the common area of an office. When plugged into a PC by a curious employee, this unleashes malware on the company's network.

In baiting attacks, attackers exploit the natural human curiosity and interest in accessing data on abandoned or received physical media devices. They rely on victims being unable to resist plugging in or accessing the malicious USB



An example of malware that could be deployed through baiting

drives or other infected media.

Mitigate baiting attacks by implementing endpoint security solutions that automatically scan removable media devices for malware and block unauthorized file executions. Enforce strict physical security measures, such as surveillance cameras and access controls, to prevent unauthorized individuals from tampering with or accessing abandoned media devices. Educate employees about the risks of inserting unknown USB drives or other external media into company devices and encourage them to report suspicious findings to the IT security team immediately.

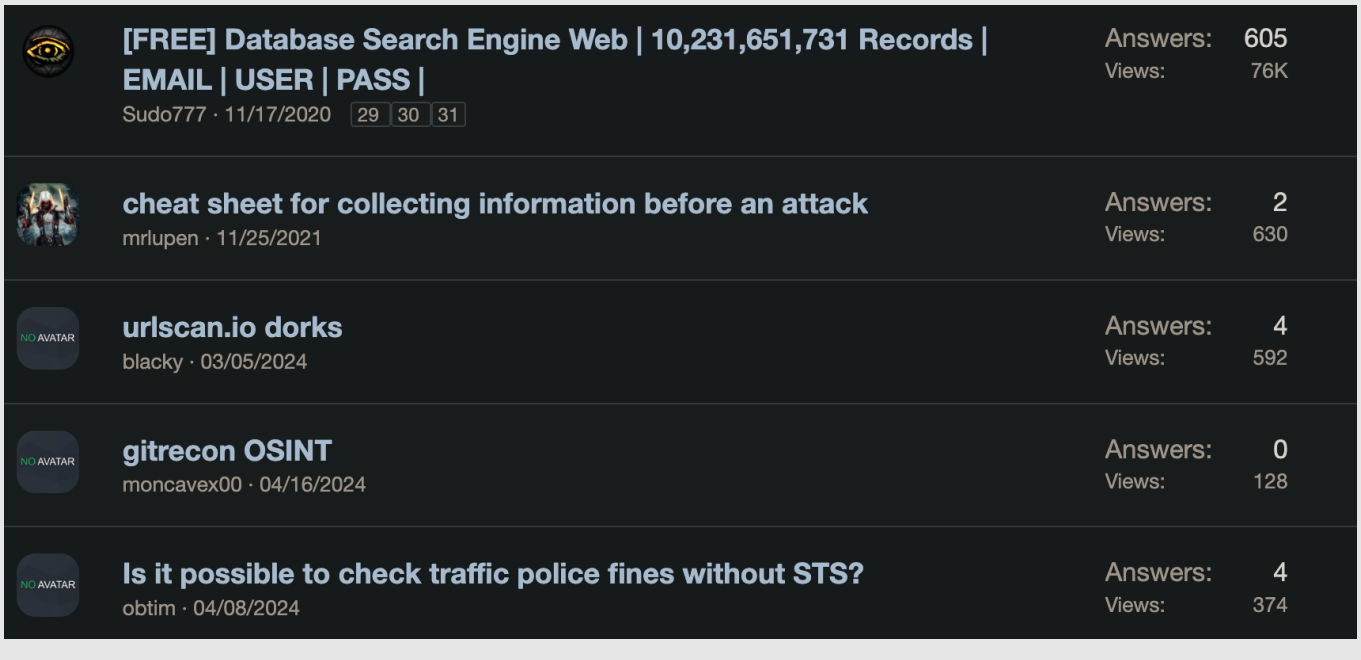
7

Whaling

Whaling is a type of social engineering attack that targets high-level executives or officials, such as CEOs or CFOs. Attackers leverage sophisticated, personalized lures crafted with detailed information gathered through OSINT techniques on the targeted victims from public sources like social media.

An example scenario might be extensive research conducted on a company's CFO using publicly available information, allowing the attacker to craft an extremely convincing email requesting an urgent wire transfer, impersonating a trusted business partner or legal authority known to the CFO.

The potential payoff is high, as compromising privileged executive accounts can lead to major security breaches, financial fraud, and unauthorized fund transfers.



An example of OSINT resources on a cybercrime forum

Whaling preys on the sensitive data and access that high-value targets have within an organization.

To mitigate whaling attacks, implement email filtering rules that flag emails containing financial requests or sensitive information from high-level executives for additional scrutiny. Establish hierarchical approval processes for significant financial transactions or data disclosures involving privileged accounts. Conduct regular security assessments to identify and address gaps in executive-level security awareness and ensure that top executives receive specialized training on recognizing and responding to whaling attempts effectively.

Take Your Next Steps With BlackFog

Don’t let social engineering attacks compromise your organization’s security and put your valuable data at risk.

BlackFog’s anti data exfiltration solution (ADX) has been designed to help you prevent global security threats such as ransomware, spyware, malware, phishing, unauthorized data collection and profiling.

Our experts can work closely with your team to strengthen your defenses against sophisticated social engineering tactics and prevent unauthorized data exfiltration using our ADX technology.

Contact us today **to schedule a demo and learn how we can safeguard your organization from emerging cyberthreats.**

BLACKFOG™

ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

All contents copyright © 2024 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.
