TIR-20250506 SOCGholish and FakeCaptcha - What They Are, What They Look Like, and What Not to Do

5/6/2025

Prepared for:

Aspire Technology Partners
25 James Way
Eatontown, NJ 07724

NOTICE:

This document is marked TLP: CLEAR, allowing recipients to share this information globally without any disclosure limitations.

This report is governed by the terms outlined in the Master Services Agreement (MSA) or any other master agreement between Aspire Technology Partners and the client receiving this report, along with the Statement of Work (SOW) or Order detailing the services that led to its creation.

Contributor(s)

Portia S. Cole
CTI Threat Researcher
Aspire Technology Partners
pcole@aspiretransforms.com

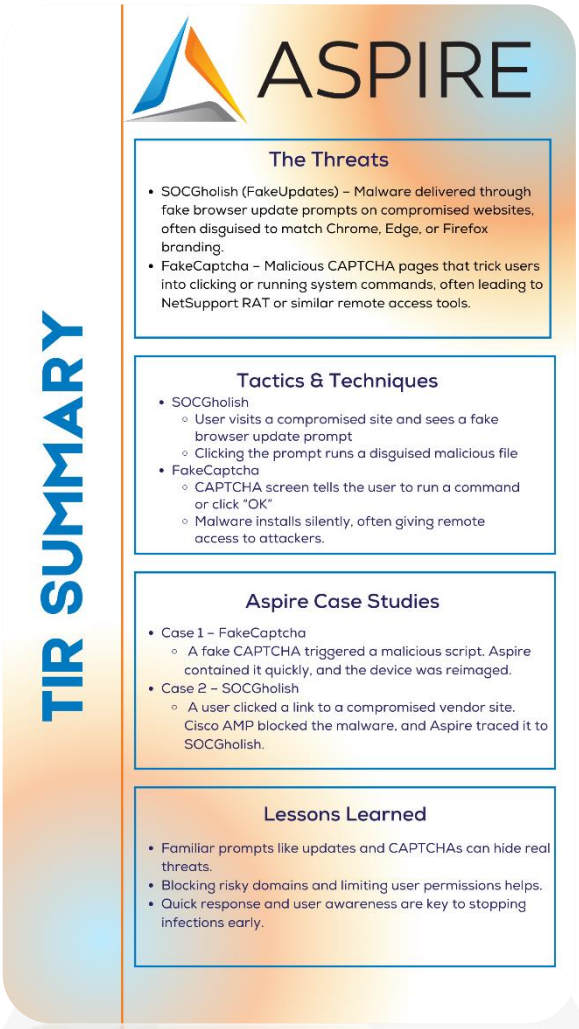
TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the past several months, Aspire's SOC has seen a clear pattern of infections tied to two familiar but dangerous threats - **SOCGholish** (FakeUpdates) and **FakeCaptcha**. Both rely on fake browser updates and fake CAPTCHA screens to trick users into infecting their own machines through seemingly harmless web interactions.

Once a user falls for it, attackers don't need to break into the network; they're let in through the front door. From there, attackers can drop remote access tools, steal credentials, or set the stage for ransomware.

This report outlines the tactics behind these attacks, how they have played out in real-world customer environments, and what steps organizations should take to reduce user-driven infections. It also provides clear examples companies can use to help employees recognize these attacks before a single click turns into a breach.



SOCGHOLISH

SOCGholish is an interesting name, and if you're wondering what it is and what it actually does, you're not alone. It is a JavaScript-based malware loader and has been active since at least 2018. It remains successful because it doesn't rely on software vulnerabilities, it relies on user trust.

The operators behind SOCGholish compromise legitimate websites and inject malicious JavaScript that silently runs in the background. When a user visits one of these sites, the code checks their system and browser settings to tailor a fake update prompt that matches what they're using, making it appear authentic. See the examples below - the images prompt the user to update their browsers.

Image 1: Fake Microsoft Edge Browser Update Example

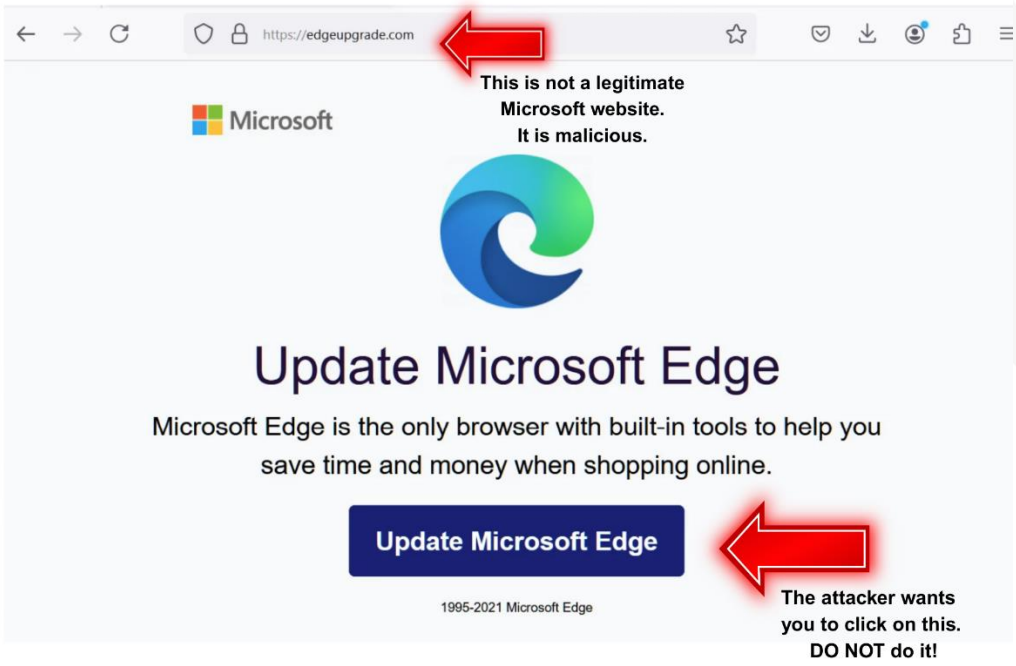
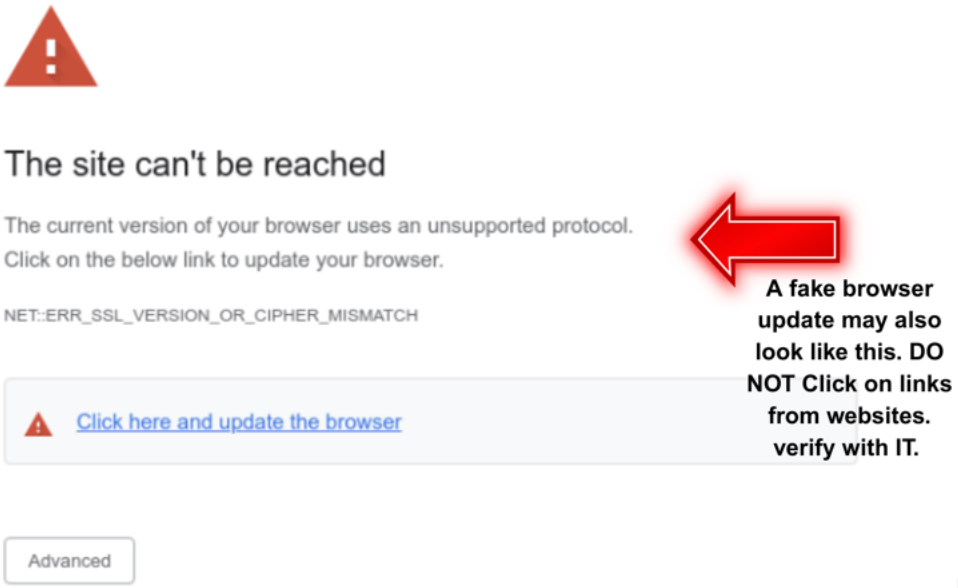


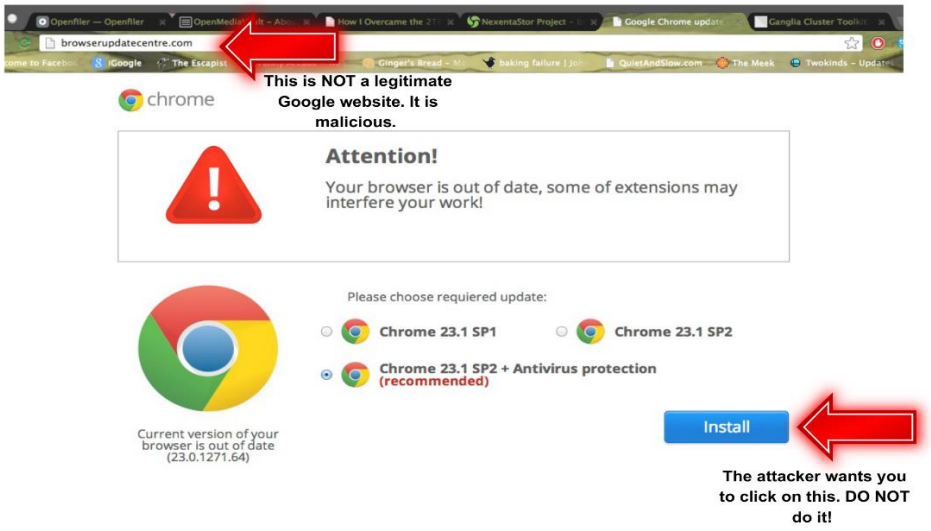
Image 2: Fake Generic Browser Update Example



The user is told that their browser is outdated and that they must install an urgent update. The message is styled to mirror genuine alerts from Chrome, Firefox, or Edge. If the user clicks the prompt, they're served a ZIP archive or JavaScript file disguised with names like "**AutoUpdater.js**." Running this file begins the infection process. The malware may launch through Windows scripting engines, such as **wscript.exe**, and often includes obfuscated PowerShell commands to fetch additional payloads from attacker-controlled infrastructure.

SOCGholish is typically used as a first stage downloader. Once it gains a foothold, it pulls down other types of malware based on the attacker's goals. This may include remote access trojans (RATs) to maintain long-term control, info stealers that scrape credentials and browser data, or ransomware loaders designed to encrypt files and demand a ransom payment.

Image 3: Fake Google Chrome Browser Update



The infrastructure behind SOCGholish shifts often. To evade detection, attackers use domain shadowing, hiding malicious activity behind subdomains of legitimate websites. They also rotate their payloads regularly and often obscure their code to make analysis difficult.

What makes SOCGholish so persistent is its ability to blend into normal user behavior. It doesn't break in through brute force or software bugs, it simply **asks the user** to install something that looks routine. That small mistake is all it takes to open the door to broader compromise.

Threat Actors Utilizing SOCGholish

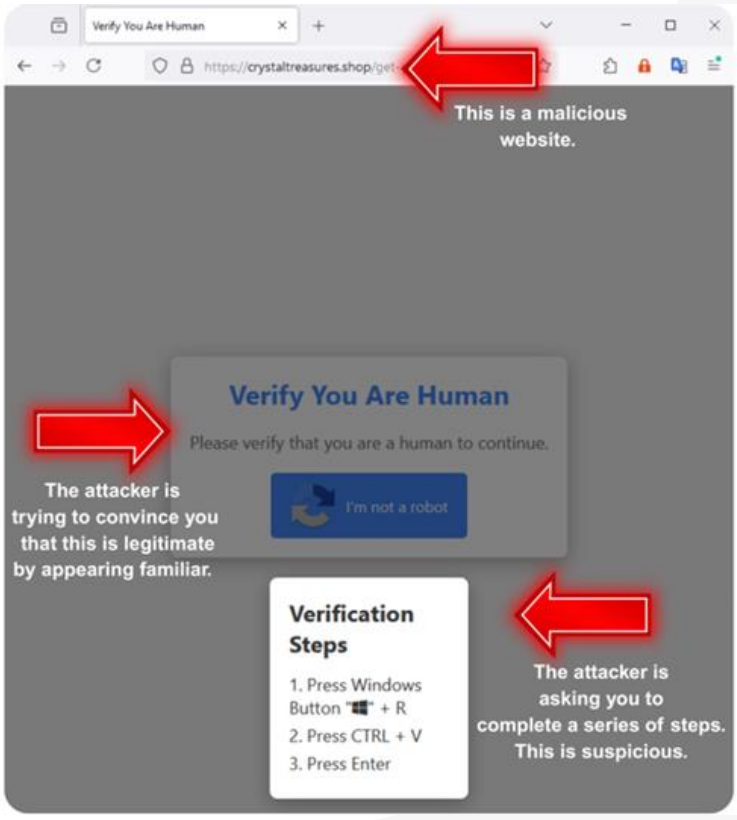
- Evil Corp (also known as UNC2165, Indrik Spider, Gold Drake)
  - Country of Origin – Russia
  - Industries Targeted – Finance, Government, Healthcare, Media, Transportation, Manufacturing, Non-profits, Technology, Education
- RansomHub

- Country of Origin – Strong possibility this is a threat actor from Russia.

FAKE CAPTCHA

FakeCaptcha is another threat that depends on deceiving users, but instead of pretending to be an update, it disguises itself as a security feature. Attackers use websites, either fully malicious or compromised legitimate domains, to display what appears to be a CAPTCHA screen, the kind users see every day when verifying they're not a robot. The familiarity of this step is exactly what makes the attack effective.

Image 4: Fake CAPTCHA



Unlike SOCGholish, which typically involves a visible download, FakeCaptcha attacks exploit human behavior at a deeper level. Users don't expect a CAPTCHA to ask for downloads or system level actions, and that misplaced trust is what makes this technique effective. Take a look at the CAPTCHA above. It is asking the user to complete a series of steps via a malicious website.

A CAPTCHA is often seen as proof that a site is legitimate. FakeCaptcha turns that assumption against the user. At first glance, the CAPTCHA looks normal. But instead of allowing the user to check a box or select images, the page gives instructions. In many cases, users are told to press ***Windows + R***, which opens the Run dialog box, and then paste a pre-filled command. This command, often masked as part of the verification process, uses built-in Windows utilities to download and run malware in the background. Some variants of this attack rely on JavaScript tricks that pre-load the clipboard with malicious commands, so that all the user has to do is paste and press ***Enter***.

One of the most common payloads delivered through FakeCaptcha is NetSupport RAT, a remote access tool originally designed for legitimate IT support but widely abused by threat actors. Once installed, the RAT allows attackers to monitor the user, run scripts, and maintain access indefinitely. Other observed payloads include data stealing malware such as Lumma or Vidar, which exfiltrate saved passwords, cookies, and stored cryptocurrency wallet data.

FakeCaptcha campaigns evolve quickly. Attackers regularly refresh the visual design of the fake CAPTCHA screens, update their hosting infrastructure, and tweak delivery methods to avoid triggering web filters or endpoint detection tools. Because there’s no traditional exploit involved (just user action) these attacks often slip past technical defenses.

The real danger is how easily users can be manipulated. People trust CAPTCHA screens because they’ve come to associate them with added security. FakeCaptcha abuses that trust by inserting malware at the exact moment users think they’re doing something safe. That misalignment is what makes this tactic so effective.

Another variant of the fake CAPTCHA scam involves presenting users with a seemingly standard CAPTCHA prompt, asking them to type specific letters or words into a text box. In an example reported by Help Net Security, scammers lured Facebook users with

sensational headlines, prompting them to "verify" their identity by entering characters into a CAPTCHA field.

Image 5: FakeCaptcha

Instead of improving security, it posted the scam to the user's Facebook feed, spreading the link to their friends. This method capitalizes on users' familiarity with CAPTCHA challenges, exploiting their trust to facilitate the spread of deceptive content and potentially harvest personal information.

These attacks succeed because they exploit habits, not software. Most users see a CAPTCHA and immediately assume it is legitimate. FakeCaptcha takes advantage of that trust to slip past defenses without raising suspicion.

Internal investigations confirmed that NetSupport RAT infections from FakeCaptcha pages gave attackers persistent access. From there, they were able to run scripts and potentially prepare for further compromise if not contained quickly.

Another version of this tactic, sometimes referred to as **ClickFix**, takes the same social engineering concept a step further. Instead of executing the malware automatically in the background, ClickFix prompts the user to run it themselves, usually by opening the Run dialog and pasting in a preloaded command.

It's part of the same larger pattern - attackers aren't forcing their way in, they're guiding users through the door. There's no obvious pop-up, no alert, just a few steps that feel like routine instructions.

Threat Actors Utilizing FakeCaptcha

- Various threat actors - The threat actors behind Fake CAPTCHA campaigns are not always clearly identified, but several have been associated with these tactics:
    - Lumma Stealer Operators - These actors distribute the Lumma information stealer malware through fake CAPTCHA pages.
    - ClearFake Campaign - This group uses fake reCAPTCHA or Cloudflare Turnstile verifications to trick users into downloading malware like Lumma Stealer and Vidar Stealer.
    - ClickFix Campaign - This campaign uses fake CAPTCHA pages to deceive users into executing malicious PowerShell commands, leading to malware infections.
    - OBSCURE#BAT Malware Operators - This group utilizes fake CAPTCHA screens to deploy stealthy rootkits, leveraging social engineering tactics.
- Country of Origin - These campaigns often originate from Russian-speaking cybercriminal communities; therefore, it is likely that their country of origin is Russia or Eastern Europe.

How Does This Happen?

How users end up in a SOCGholish or FakeCaptcha situation:

- **Compromised legitimate websites** – A user might visit a trusted site (like a news site, small business page, or community forum) that has been silently compromised. Attackers inject malicious code into the site, which then triggers the fake update (SOCGholish) or fake CAPTCHA (FakeCaptcha) when users visit.

- **Malicious ads (Malvertising)** – Sometimes users are served bad ads even on reputable websites. These ads can redirect users to malicious pages that immediately show the fake browser update or CAPTCHA screen.

- **Links in phishing emails** – Some campaigns use phishing emails that link to legitimate websites which have been compromised, or they link directly to attacker controlled pages set up to deliver SOCGholish or FakeCaptcha.

- **Search engine poisoning** – Attackers sometimes create malicious websites that are optimized to show up in search results. A user looking for free downloads, updates, or technical support might land on one of these fake pages without realizing it.

Aspire Case Studies

1. How Aspire's SOC Contained a Fake CAPTCHA Threat Before It Spread

In April 2025, Aspire's SOC was alerted of suspicious behavior on a customer's workstation after a command prompt was observed launching a batch file tied to a fake CAPTCHA interaction. The user had been browsing travel and hobby-related websites when they encountered what appeared to be a CAPTCHA screen asking them to click "OK" to confirm. That simple click silently triggered a script in the background, launching

a malicious process that installed NetSupport RAT, the legitimate remote access tool commonly abused by threat actors.

The SOC responded immediately by reviewing logs across CrowdStrike and DNS tools to confirm the activity. Within one hour, the device was fully contained from the network to prevent any further movement or communication with external domains. Known malicious domains seen during the session were added to the organization's block list as a precaution.

Further investigation revealed that the same device had previously been flagged for unrelated malware activity. This history, along with signs of persistence attempts and malicious scripts running from the user profile, made it clear that a full reimage was the safest next step. Aspire's SOC reached out to the client's technical contact, who coordinated a pickup and reimaging of the device.

During this time, additional suspicious domains linked to the browsing session were reviewed and blocked. Although not all were conclusively malicious, several carried high threat scores or signs of compromise, and were treated as part of the infection chain.

The SOC worked closely with endpoint protection and threat intelligence tools to ensure there were no lingering threats, and Falcon Complete assisted with cleanup. The case was resolved once the device was reimaged, and no signs of further compromise were observed.

This case reflects the same patterns described earlier in the FakeCaptcha section of this report. The infection didn't begin with a download or a malicious email, it began with a user doing something they've likely done hundreds of times - interacting with a CAPTCHA screen during casual web browsing. That routine action launched a script that installed NetSupport RAT in the background without raising obvious alarms. Just as outlined in the threat overview, the attacker didn't exploit a vulnerability in software, they exploited behavior.

2. SOC Blocks SOCGholish Threat Delivered Through a Compromised Vendor Website

In February 2025, Aspire's SOC investigated a detection involving a user who clicked a link in an email that appeared to come from a trusted business contact. The email included an encrypted link that redirected the user to a familiar vendor website. On the surface, nothing looked unusual, but seconds after the link was clicked, Cisco Secure Endpoint flagged and quarantined a malicious JavaScript file from the user's browser cache.

The SOC reviewed telemetry and determined that the file had been launched from the vendor's website, which had likely been compromised with malicious scripts. Threat Grid analysis of the quarantined file revealed behavior associated with SOCGholish malware, including excessive JavaScript functions, suspicious file paths, and redirection behavior commonly used in drive-by campaigns. Further sandbox analysis tied the file to JavaScript paths on the vendor's domain, including file names previously linked to SOCGholish droppers.

Although antivirus had stopped the file before it could execute, Aspire's SOC took several steps to reduce further risk. The team initiated a full system scan, reviewed file trajectory logs in Cisco AMP, and submitted associated domains to Cisco Threat Grid for deeper analysis. Based on the returned threat scores (some reaching as high as 95/100) the SOC placed the vendor's domain on the Umbrella global block list to prevent any other users from being exposed to the same compromised site.

The client was notified and Aspire recommended reviewing the user's inbox for similar emails, resetting the user's password as a precaution, and conducting security awareness training. Aspire also advised reaching out to the vendor to inform them that their website was hosting malicious code. At first, the site appeared to be safe because it belonged to a known business partner. But after a closer look, it became clear the site had been compromised and was hosting malware.

This case shows how SOCGholish often slips in through the back door - a trusted website that's been quietly compromised. The user doesn't think they're doing anything risky. They just click a familiar link and end up triggering something malicious without realizing it. That's all it takes. Aspire acted quickly, using alerting tools and threat analysis to block the threat before it had a chance to spread.

CONCLUSION

These weren't just one-off detections, they were warning signs of larger, repeatable attack patterns. Aspire's SOC didn't just respond. We recognized what was happening early and linked the activity to a broader campaign. That's the role of real threat intel - catching the behavior behind the malware, not just the file.

Aspire's analysts don't just look at what happened, we look at what nearly happened, what could have happened, and what's likely to happen next. That kind of insight helps us shut down threats early and protect clients before damage is done.

FROM THE CTI DESK

In the final quarter of 2024, SOCGholish stood out as the most prevalent malware, responsible for [1]53% of observed infections, as reported by the Center for Internet Security. As previously stated, this JavaScript based malware typically infiltrates systems through compromised legitimate websites, presenting users with fake browser update prompts that deliver malicious JavaScript payloads.

Attacks like this show how quickly things can escalate when users trust the wrong prompt, and why ongoing awareness matters just as much as technical defenses. Let's do a quick recap, so you are clear on what to look for and what not to do.

What are the threats?

- FakeUpdates (SOCGholish) – A fake browser update prompt that appears on a legitimate website after it's been compromised. Clicking it can launch malware.
- FakeCaptcha – A phony CAPTCHA screen that asks users to click buttons or run commands, often leading to remote access tools like NetSupport RAT.

[1] Top 10 Malware Q4 2024

What do they look like?

- A pop-up that says “Your browser is out of date - click to update”
- A CAPTCHA that looks normal but asks you to press Windows + R, paste something in, or run code.

What should users avoid?

- Don’t install browser updates from pop-ups or websites. Always go through IT or official update channels
- Never press keys, run commands, or download anything from a CAPTCHA prompt.
- Don’t blindly trust update prompts on unfamiliar websites, even if the site looks legitimate. If you are unsure, contact IT.

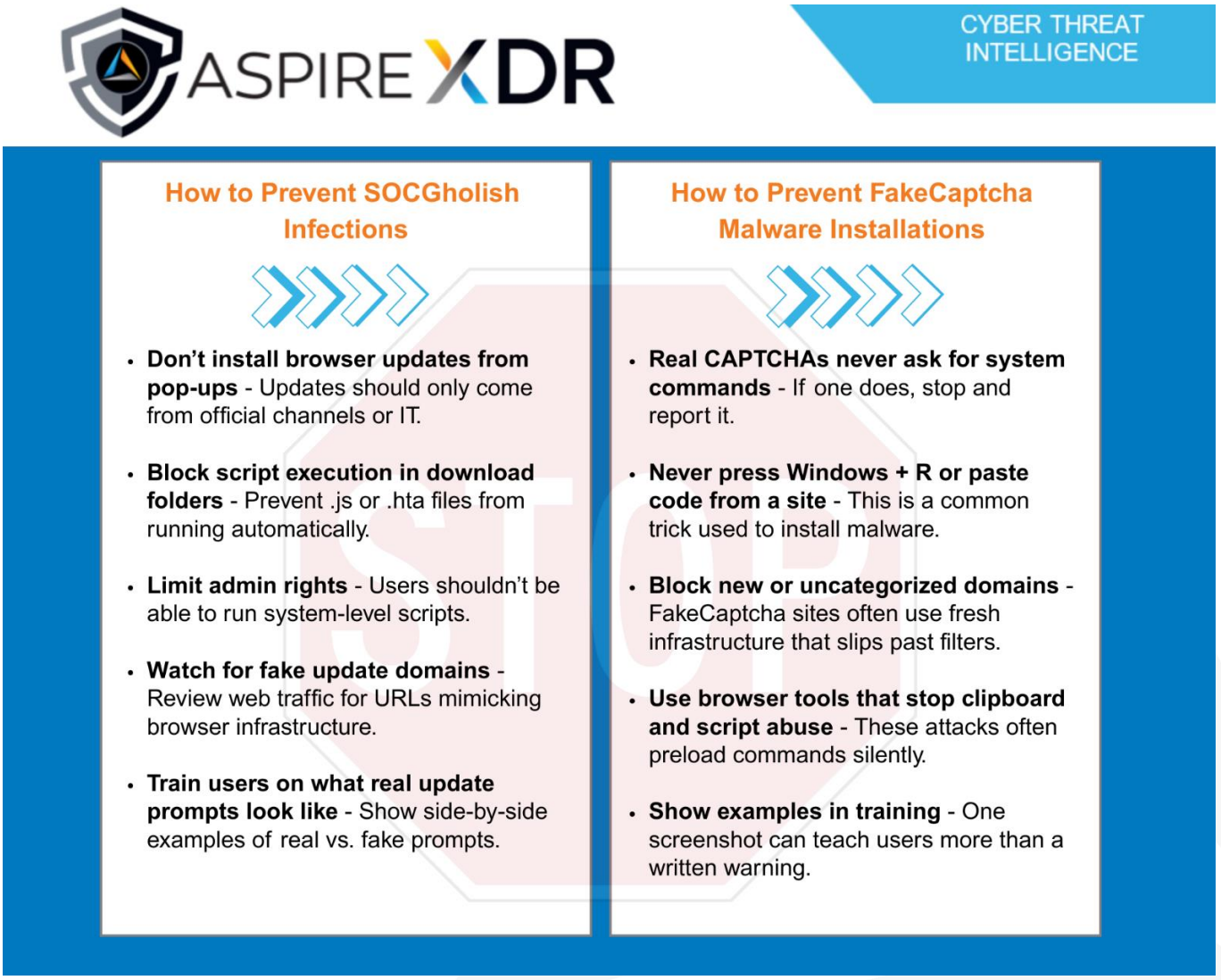
What should users do?

- Report suspicious pop-ups or CAPTCHAs to IT right away
- Close the page and avoid interacting if something feels off
- Stay alert, especially when browsing less familiar sites or clicking links in email.

Note!: *We value your feedback and want to make sure these reports are as helpful as possible. Take a minute to let us know what worked and what could be better by completing **this form**. Your input helps us improve what we deliver to your company.*

ASPIRE'S RECOMMENDATIONS

Threats like SOCGholish and FakeCaptcha don't break in. They blend into what looks routine and rely on user trust. The steps below are based on real incidents and can help prevent these attacks from slipping through.



MITRE MAP

SOCGholish

Initial Access (*How it Gets In*)	T1189 – Drive-by Website Compromise T1566.002 – Phishing: Spearphishing Link
Execution *(What it Tries to Do)*	T1204.002 – User Execution: Malicious File T1059.007 – Command and Scripting Interpreter: JavaScript
Defense Evasion *(How it Hides)*	T1027 – Obfuscated Files or Information T1218.005 – System Binary Proxy Execution: Mshta
Command and Control *(How it Talks Back)*	T1071.001 – Application Layer Protocol: Web Protocols

FakeCaptcha

Initial Access *(How it Gets In)*	T1189 – Malicious CAPTCHA on a Website T1566.002 – Phishing: Spearphishing Link
Execution *(What it Tries to Do)*	T1204.001 – User Execution: Malicious Link T1059.003 – Command and Scripting Interpreter: Windows Command Shell
Persistence & Evasion *(How it Tries to Stay in and Hide)*	T1547.001 – Boot Logon Autostart Execution: Registry Run Keys/Startup Folder T1036 – Masquerading T1140 – Deobfuscate/Decode Files or Information
Command and Control *(How it Talks Back)*	T1219 – Remote Access Tools T1071.001 – Application Layer Protocol: Web Protocols
Discovery *(What Else it Might Do)*	T1082 – System Information Discovery

ASPIRE PROTECTS

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.

- **Aspire Managed Detection and Response (MDR)**
  - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire MDR delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

  - Our team of experts act as an extension of your IT operations to quickly identify and mitigate security threats before they impact your business.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

INDICATORS OF COMPROMISE (IOCS)

SOCGholish *(from Aspire's case study)*

Domains

- xxx[.]cadogantate[.]com
- link[.]zixcentral[.]com

File Hashes

- 6ca84b9443525b44c3badb80019768eafe291ae7ecfa56e4b8967c14e62ac589
- fd279330bdae563653ec2a1b4ff354eba7d53b67f4e3c928a9e8ffae71884268
- 69068df3e5859ef098ab2d84d575cede899d7d99d3ff408d9c6dc7dba9bffab8

URLs

- xxx[.]cadogantate[.]com/wp-content/themes/cadogantate-theme/public/~partytown/partytown[.]js
- xxx[.]cadogantate[.]com/wp-content/plugins/advanced-custom-fields-pro/assets/inc/datepicker/images/images[.]php

FakeCaptcha *(From Aspire's case study)*

Domains

- umpmfss[.]top
- pl26140969[.]effectiveratecpm[.]com
- settlementstandingdread[.]com
- githack[.]com
- postrelease[.]com
- fishingandfish[.]com
- ml314[.]com

File Hashes

- badf4752413cb0cbdc03fb95820ca167f0cdc63b597ccdb5ef43111180e088b0
- 312a0e4db34a40cb95ba1fac8bf87deb45d0c5f048d38ac65eb060273b07df67

Executable Paths

- C:\Users\Public\boom.bat
- C:\Users\827921\AppData\Roaming\MyApp23\client32.exe

SUPPORTING DOCUMENTATION

Information Security | Helping to secure the UChicago community

Facebook scam uses fake CAPTCHA to spread - Help Net Security

eSentire | NetSupport RAT Clickfix Distribution

Beware Fake Browser Updates: TA569, Rogueraticate & More | Proofpoint US

Fake browser updates spread updated WarmCookie malware

Fake CAPTCHA Initiates Malware - South Atlantic Bank

Browser Update Scams

Supply Chain Compromise or False Positive: The Intriguing Case of efile.com [updated - confirmed malicious code] - SANS Internet Storm Center

SocGholish: Risks & Mitigation | Sucuri

These aren't your grandmother's 'warm cookies'

Facebook scam uses fake CAPTCHA to spread - Help Net Security

eSentire | NetSupport RAT Clickfix Distribution

SocGholish Malware: A Real Threat from a Fake Update | Proofpoint US

SocGholish Malware in the Healthcare Sector | Proofpoint US

An Update on Fake Updates: Two New Actors, and New Mac Malware | Proofpoint US

SocGholish | Red Canary Threat Detection Report

Widespread Fake CAPTCHA Campaign Delivering Malware | Arctic Wolf

Lumma Stealer: Fake CAPTCHAs & New Techniques to Evade Detection - Netskope

New Evasive Campaign Delivers LegionLoader via Fake CAPTCHA & CloudFlare Turnstile - Netskope

Resurgence of a Fake Captcha Malware Campaign

Fake CAPTCHA websites hijack your clipboard to install information stealers | Malwarebytes

Beware: Fake CAPTCHA Campaign Spreads Lumma Stealer in Multi-Industry Attacks

Malware campaign expands its use of fake CAPTCHAs | The Record from Recorded Future News

Fake CAPTCHA Malware Campaigns | Latest Alerts and Advisories | NJCCIC

An ounce of prevention: Ensuring that updates to software, devices are legitimate

RansomHub using FakeUpdates scheme to attack government sector | Cybersecurity Dive

Malware campaign expands its use of fake CAPTCHAs | The Record from Recorded Future News

Fake CAPTCHA Malware Campaign: How Cybercriminals Use Deceptive Verifications to Distribute Malware - CYFIRMA

APPENDIX II: DISCLAIMER

This document and its contents are not intended to serve as legal advice and should not be used as a substitute for it. The results of a Security Risk Assessment are intended to guide the implementation of diligent measures to reduce the risk of potential vulnerabilities being exploited to compromise data.

While the Services and this report may offer information that the Client can use to support its compliance efforts, the responsibility for evaluating and fulfilling compliance obligations rests solely with the Client, not Aspire. This report does not guarantee or assure the Client's compliance with any law, regulation, or standard.