CYBER THREAT INTELLIGENCE

CRITICAL**START**® **Security Advisory**

TLP AMBER // [CS-SA-26-0304] HTML Smuggling Campaign

Executive Summary

The Critical Start Security Operations Center (SOC) was alerted to a phishing campaign targeting several customers across diverse critical industries. The campaign primarily used HTML smuggling delivered through Spearphishing as the initial access vector. The malicious HTML files were crafted to dynamically incorporate each recipient's email address in the naming, demonstrating automation, as well as the threat actor's sophistication. Evidence indicates the use of a Phishing-as-a-Service (PhaaS) platform. The timing and distribution of alerts across multiple customer environments suggest a coordinated effort. Critical Start's Cyber Research Unit (CRU) assesses with medium confidence that the threat actor(s) leveraged a PhaaS platform or other automation capability to:

- Deliver emails to a wide range of targets efficiently
- Customize HTML file names and content for each recipient to bypass hash-based detections

This advisory summarizes the findings and provides recommended actions.

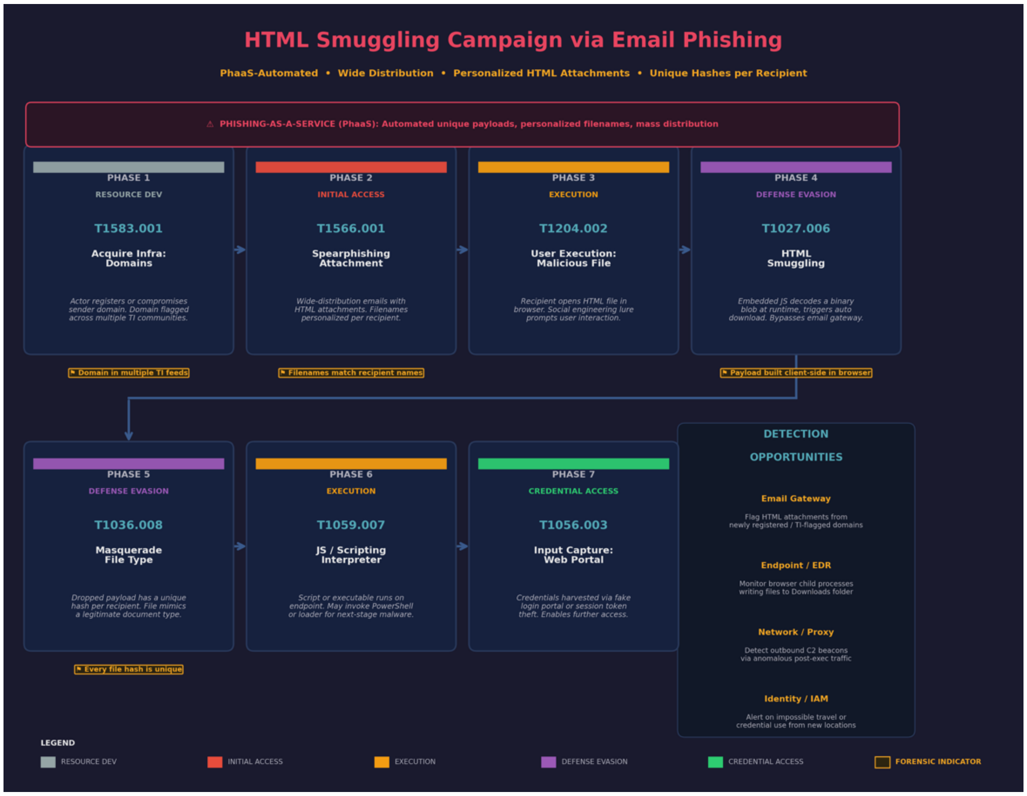
HTML Smuggling Campaign via Email Phishing
PhaaS-Automated • Wide Distribution • Personalized HTML Attachments • Unique Hashes per Recipient
⚠ PHISHING-AS-A-SERVICE (PhaaS): Automated unique payloads, personalized filenames, mass distribution
PHASE 1
RESOURCE DEV
T1583.001
Acquire Infra: Domains
Actor registers or compromises sender domain. Domain flagged across multiple TI communities.
⚑ Domain in multiple TI feeds
PHASE 2
INITIAL ACCESS
T1566.001
Spearphishing Attachment
Wide-distribution emails with HTML attachments. Filenames personalized per recipient.
⚑ Filenames match recipient names
PHASE 3
EXECUTION
T1204.002
User Execution: Malicious File
Recipient opens HTML file in browser. Social engineering lure prompts user interaction.
PHASE 4
DEFENSE EVASION
T1027.006
HTML Smuggling
Embedded JS decodes a binary blob at runtime, triggers auto download. Bypasses email gateway.
⚑ Payload built client-side in browser
PHASE 5
DEFENSE EVASION
T1036.008
Masquerade File Type
Dropped payload has a unique hash per recipient. File mimics a legitimate document type.
⚑ Every file hash is unique
PHASE 6
EXECUTION
T1059.007
JS / Scripting Interpreter
Script or executable runs on endpoint. May invoke PowerShell or loader for next-stage malware.
PHASE 7
CREDENTIAL ACCESS
T1056.003
Input Capture: Web Portal
Credentials harvested via fake login portal or session token theft. Enables further access.
DETECTION OPPORTUNITIES
Email Gateway
Flag HTML attachments from newly registered / TI-flagged domains
Endpoint / EDR
Monitor browser child processes writing files to Downloads folder
Network / Proxy
Detect outbound C2 beacons via anomalous post-exec traffic
Identity / IAM
Alert on impossible travel or credential use from new locations
LEGEND
RESOURCE DEV
INITIAL ACCESS
EXECUTION
DEFENSE EVASION
CREDENTIAL ACCESS
FORENSIC INDICATOR

Figure 1: Attack Flow Showing a HTML Smuggling Attack Through Spearphishing as Initial Access Vector

What Was Observed

The Critical Start SOC investigated incidents where the consistent sender is “sinarsuburlogamindo.com”. Further OSINT investigations into this IOC revealed other relations with IP addresses, domains, etc. Additionally, static analysis of the HTML file revealed domains such as: “ytccomputer.com”, “anaksakti.online”, and “automedsos.com”. The table below shows a summary of associated indicators:

S/N	Indicator	Description	Notes
	sinarsuburlogamindo.com	Primary sender domain across all alerts	Business name and domain belong to manufacturer in Indonesia
	146.20.65.91	Initial IP correlation with sender domain	
	anaksakti77.org	Domain associated with - 146.20.65.91	
	ytccomputer.com	Constant domain in malicious HTML file	
	anaksakti.online	Constant domain in malicious HTML file	
	automedsos.com	Constant domain in malicious HTML file	
	104.21.18.91	IP enriched from OSINT	
	104.21.48.1	IP enriched from OSINT	
	104.21.112.1	IP enriched from OSINT	
	104.21.32.1	IP enriched from OSINT	
	104.21.80.1	IP enriched from OSINT	
	104.21.16.1	IP enriched from OSINT	
	104.21.16.1	IP enriched from OSINT	
	104.21.64.1	IP enriched from OSINT	This IP was involved in 1113 events across 1 distinct attack types. Attacks: dns-query
	104.21.96.1	IP enriched from OSINT	
	172.67.181.135	IP enriched from OSINT	
	162.255.119.236	IP enriched from OSINT	
	2a01:111:f403:c408::1	Sender IP	
	2a01:111:f403:c408::3	Sender IP	
	2a01:111:f403:c409::1	Sender IP	
	[Alert] Failed Renewal for [Company Name]	Subject composition convention consistent across several emails	
	Hash Values	N/A	All files had unique hash values

Note: To minimize volume, pivoting was done with no more than 2 layers down to maximize relevance to threat actor, especially considering the volatility of the observed indicators.

Industry Targeting

Alerts triggered were distributed across a wide range of industries, indicating broad targeting; however, the concentration is highest in a small set of sectors. Manufacturing led at 16.1%, followed by Banking and Finance at 14.3% and Construction at 12.5%. Business Services and Consulting each accounted for 7.1%, rounding out the top five most impacted industries. Retail and Transportation also showed notable activity at 7.1% each, while the remaining industries, including Energy and Utilities, Real Estate, Government, Healthcare, and Technology related sectors, were impacted at lower levels.

These sectors are targeted for specific operational reasons. Manufacturing is attractive due to its complex supply chains, reliance on multiple vendors and logistics partners, and operational urgency, which create realistic contexts for attackers to deliver content that appears trustworthy. Banking and Finance are exposed because frequent financial transactions, invoicing, and client communications provide opportunities for Spearphishing and HTML-smuggling attacks. Construction faces similar risks through project management, vendor coordination, and contract communications. Business Services and Consulting are often targeted because extensive client interactions and document-driven workflows increase the likelihood that recipients will open attachments or click on links.

Attackers further improve success across these industries by using domains tied to legitimate organizations or registered businesses with verifiable details, such as Google listings and reviews, which enhance trust and increase engagement. This is the case with the Indonesian manufacturer “PT. Sinar Subur Logamindo”, which domain is the observed malicious domain. The targeting across many sectors reinforces a broad, scalable targeting approach designed to maximize reach rather than focus on a single vertical.

Tactics, Techniques, and Procedures (TTPs)

CRU observed this campaign touches on several TTPs including HTML Smuggling, Spearphishing, and BEC. However, due to the uniqueness of the observed incidents, and to assist with narrowing down investigations, this section details HTML Smuggling.

BEC note: BEC is mentioned due to the observed compromise of the website and domain of a legitimate manufacturer in Indonesia namely, “Sinar Subur Logamindo”. At the time of writing this report, the website is down.

Technique Name: Obfuscated Files or Information: HTML Smuggling

MITRE ID: TA0005.T1027.006

HTML smuggling is a technique in which attackers deliver malicious payloads inside seemingly benign HTML files, often sent as phishing email attachments. Instead of transmitting a detectable binary over the network, the payload is embedded within the HTML using JavaScript and HTML5 features such as Data URLs, the Blob API, and the anchor tag download attribute.

These features allow HTML documents to store large amounts of encoded data. Malicious content can be obfuscated and hidden within Data URLs or JavaScript Blobs, which represent raw byte data. Because this content is packaged as harmless MIME types like text/html or text/plain, it can bypass perimeter defenses such as secure email gateways and web content filters that rely on inspecting files in transit.

When the victim opens the HTML file in a browser, embedded JavaScript executes and reconstructs the payload locally. This includes decoding or deobfuscating the hidden data and converting it into a usable file. JavaScript Blobs can be used to dynamically generate file like objects in the browser, which are then written to disk using features such as the HTML5 download attribute or functions like msSaveBlob.

By shifting payload reconstruction to the endpoint, HTML smuggling avoids detection during delivery. The malicious file is never transmitted in its final form over the network, making traditional signature-based detection ineffective and allowing attackers to evade security controls while successfully delivering their payload.

Threat Actor Profiling

The HTML attachment technique spans state actors and prolific cybercriminal operators alike. Several Threat Actors known to Use HTML Smuggling in Email Phishing include:

- NOBELIUM (APT29 / Cozy Bear) is a Russian state-sponsored espionage group linked to the Russian Foreign Intelligence Service (SVR) and widely known as the actor behind the 2020 SolarWinds supply chain compromise. They primarily target government agencies, NGOs, think tanks, and diplomatic organizations across NATO-aligned nations. In their most documented HTML smuggling incident, starting in March 2021 and escalating in May 2021, NOBELIUM distributed spear-phishing emails containing an HTML attachment called EnvyScout. When opened in a browser, the HTML used JavaScript to write an ISO file directly to the target's disk. The ISO contained a shortcut file (LNK) that, when executed, loaded a DLL delivering a custom Cobalt Strike Beacon loader Microsoft dubbed NativeZone, enabling persistent remote access to compromised systems. At its peak the campaign impersonated USAID via the legitimate Constant Contact mailing service and targeted roughly 3,000 accounts across more than 150 organizations.
- APT41 (also known as Wicked Panda, BARIUM, or Brass Typhoon) is a Chinese state-sponsored threat group active since at least 2012, uniquely operating both espionage and financially motivated campaigns simultaneously. They target organizations in healthcare, telecommunications, high-tech, gaming, and government sectors across at least 14 countries. APT41 often relies on spear-phishing emails with attachments such as compiled HTML (.CHM) files as their initial compromise method, and in one campaign running nearly a year, the group compromised hundreds of systems and deployed close to 150 unique pieces of malware including backdoors, credential stealers, keyloggers, and rootkits.
- DEV-0193 is a financially motivated cybercriminal group tracked by Microsoft, believed to overlap with the operators behind TrickBot. The group primarily targets organizations in the healthcare and education sectors and functions as an access broker, selling footholds to ransomware operators including those behind the Ryuk ransomware. In September 2021, Microsoft attributed an HTML smuggling campaign to DEV-0193 in which phishing emails carried a specially crafted HTML attachment disguised as a business report. When the recipient opened the attachment, a password-protected JavaScript file was constructed locally on the victim's device. Once the victim entered the password from the HTML attachment, the JavaScript executed a Base64-encoded PowerShell command that contacted attacker-controlled infrastructure to download TrickBot, paving the way for follow-on ransomware deployment.
- TA571 is a high-volume initial access broker tracked by Proofpoint, active since at least 2019. The group operates large-scale spam distribution campaigns delivering malware on behalf of downstream cybercriminal customers, with infections frequently serving as precursors to ransomware. They are known for rapidly iterating their delivery techniques to stay ahead of detection. In March 2024, Proofpoint observed TA571 launch a campaign exceeding 100,000 messages targeting thousands of organizations globally. Emails contained HTML attachments that displayed a page impersonating Microsoft Word, presenting a fake error message claiming the "Word Online" extension was not installed.

Victims who clicked the offered fix had a Base64-encoded PowerShell command silently copied to their clipboard, which when executed led to the installation of malware including DarkGate and Matanbuchus.

- QakBot operators ran one of the longest-running cybercriminal botnet operations, with QakBot active from at least 2007 until its infrastructure was dismantled by the FBI in August 2023. The group delivered banking trojans and provided initial access for ransomware groups including Black Basta and Conti. In a documented campaign, the QakBot operators distributed a new variant of the malware via HTML file attachments. The HTML contained a JavaScript payload that automatically executed upon being opened in a browser, decoding and downloading the QakBot loader module to the victim's device without requiring additional user interaction beyond opening the file.
- ClearFake is a threat cluster associated with fake browser update campaigns that compromise legitimate websites to inject malicious scripts. The cluster primarily pursues credential theft and initial access, delivering information stealers and remote access tools. Beginning in April 2024, Proofpoint observed ClearFake adopting the same HTML attachment technique used by TA571, using embedded fake error messages to trick victims into copying and pasting malicious PowerShell commands. ClearFake layered additional evasion by hosting the malicious scripts on blockchain infrastructure via Binance Smart Chain contracts, a method known as EtherHiding, making takedown significantly harder.
- SuperMailer Operators behind SuperMailer-generated credential phishing campaigns used the software's template features to automatically craft emails containing users' email addresses and organization names, generating unique per-recipient HTML attachments at high volume.

Threat Actor Summary Table

Actor	Type	HTML Attachment Use
NOBELIUM / APT29	Russian nation-state	HTML smuggling, ISO/payload delivery
APT41	Chinese nation-state	Compiled HTML (.CHM) spear-phishing
TA571	IAB / cybercrime	Fake Word/OneDrive HTML lures, ClickFix
QakBot operators	Cybercrime botnet	HTML → JS → QakBot loader
DEV-0238/0253/0193	Microsoft-tracked groups	HTML smuggling → keyloggers / TrickBot
TA542 (Emotet)	Cybercrime botnet	Email campaigns with various attachments incl. HTML
SuperMailer operators	PhaaS/commodity	Per-recipient personalized HTML credential phishing
ClearFake	Fake update cluster	HTML attachments with fake error + PowerShell lures

Understanding attacker tradecraft helps organizations define defenses, strengthen posture, and anticipate potential next steps. It does not confirm attribution to a specific actor. For threat groups that operate Malware-as-a-Service (MaaS), operators may change, associated indicators such as IP addresses or domains may vary, and they may leverage legitimate but compromised infrastructure to evade detection. As such, organizations should exercise caution when attributing activity to a particular threat actor.

Implications for Organization

HTML smuggling poses significant risks to organizations due to its ability to bypass traditional email and endpoint security controls. Compromised credentials can provide attackers with initial access, which may lead to lateral movement, data exfiltration, or deployment of ransomware and other malicious payloads. Organizations with complex supply chains, frequent external communications, or high-value intellectual property are particularly exposed.

Failure to address this threat can result in operational disruption, financial loss, reputational damage, and regulatory consequences. Even if no user interaction occurs, the presence of malicious attachments or links highlights potential gaps in email hygiene, endpoint configurations, and user awareness. Proactive measures, continuous monitoring, and integration of threat intelligence are essential to mitigate the impact of these attacks and maintain overall security resilience.

What Critical Start is Doing

The SOC is actively investigating and responding to the phishing campaign to limit exposure and prevent potential compromise. Investigative actions focus on identifying any interaction with the malicious attachments or links, while response actions aim to contain the threat, block malicious infrastructure, and remediate affected accounts where necessary. The following steps outline the current investigative and response measures being undertaken.

- Investigative Actions:
    - A check is done for the malicious .htm file attachments being observed on an endpoint using data in the DeviceFileEvents table
    - A check is done for any UrlClickEvents corresponding to emails from the malicious domain

- Response Actions - Where permissions and ROE allow:
    - Attempting to delete emails associated with the alert using the Identify & Respond: Similar Emails (blast radius TAP). This identifies similar emails based on sender/subject characteristics and can respond to all matches in one go.
    - Adding a domain block indicator for sinarsuburlogamindo[.]com to block endpoint connections to URLs observed within the emails
    - Identity remediations if interaction is observed
        - Revoke sessions
        - If suspicious sign-ins observed:
            - Disable user
            - Force password reset

Additionally, the SOC has confirmed that no users have interacted with the malicious attachments. Escalations have been sent to all affected customers advising them to block the sender at the tenant level. The SOC is in the process of applying block indicators for all four domains involved. Detection Engineers have pushed detections for the observed indicators to ensure coverage and effectiveness. CRU continues to monitor the dark web and OSINT sources for additional indicators or activity.

Prioritized Mitigation Strategies

To limit the risk of HTML smuggling and other phishing-based attacks, we recommend the following:

Immediate

- Enforce Phishing-Resistant MFA: Replace push-based or OTP MFA with FIDO2 hardware keys or certificate-based authentication across all user accounts. HTML smuggling campaigns frequently terminate in credential harvesting and adversary-in-the-middle frameworks can bypass standard MFA. This is the single highest-impact control given that identity compromise is the most likely outcome of a successful HTML smuggling attack.

Short-Term

- Block HTML File Attachments at the Email Gateway: Implement a policy at the email gateway level to quarantine or reject inbound emails carrying HTML or HTM attachments, including those embedded inside ZIP or RAR archives. Since legitimate business workflows rarely involve HTML file attachments, this policy has minimal operational disruption while significantly reducing the attack surface before any SOC involvement is required.

- Restrict Script Execution in Enterprise Browsers: Push a managed browser configuration policy that prevents locally opened HTML files from executing JavaScript. HTML smuggling is entirely dependent on browser-side script execution to assemble and drop the payload. Disabling this execution path for untrusted local content neutralizes the technique at the point of delivery.

- Apply Least Privilege and Just-in-Time Access: Audit and reduce user permissions so that a compromised account has the minimum access necessary to perform its function. Since HTML smuggling is frequently used as a first-stage delivery mechanism for ransomware operators and access brokers, limiting what a compromised identity can reach significantly reduces post-compromise blast radius regardless of whether initial detection succeeds.

Medium-Term

- Conduct Regular Red Team Exercises Simulating HTML Smuggling Chains: Commission periodic adversary simulation exercises that specifically replicate HTML smuggling delivery chains, ClickFix-style lures, and credential harvesting pages. This surfaces gaps in existing detection coverage, user behavior, and control effectiveness that routine SOC operations may not expose until a real incident occurs.

Conclusion

HTML smuggling is a sophisticated and evolving threat that can compromise credentials and enable further attacks. While Critical Start's SOC actively monitors, investigates, and mitigates this campaign, organizations are advised to implement the recommended actions. Additionally, fostering a culture of vigilance is critical to reducing risk and ensuring organizational resilience against these HTML smuggling attacks.

For more threat reports, including H2 2025 detailing industry targeting visit Critical Start's Intel Hub. Should anything new surface, this advisory will be updated. This advisory was written using the best intelligence available at the time and is subject to change as additional information becomes available.

Further Reading

1. https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
2. https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation
3. https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
4. https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
5. https://www.fortinet.com/blog/threat-research/new-variant-of-qakbot-spread-by-phishing-emails
6. https://cofense.com/blog/html-attachments-used-in-malicious-phishing-campaigns/
7. https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
8. https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/
9. https://blog.sekoia.io/nobeliums-envyscout-infection-chain-goes-in-the-registry-targeting-embassies/
10. https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation
11. https://www.proofpoint.com/us/blog/threat-insight/clipboard-compromise-powershell-self-pwn
12. https://www.fortinet.com/blog/threat-research/new-variant-of-qakbot-spread-by-phishing-emails
13. https://www.levelblue.com/blogs/spiderlabs-blog/html-file-attachments-still-a-threat
14. https://blog.talosintelligence.com/hidden-between-the-tags-insights-into-evasion-techniques-in-html-smuggling/
15. https://attack.mitre.org/techniques/T1566/001/
16. https://www.kaspersky.com/resource-center/threats/malicious-html-attachments