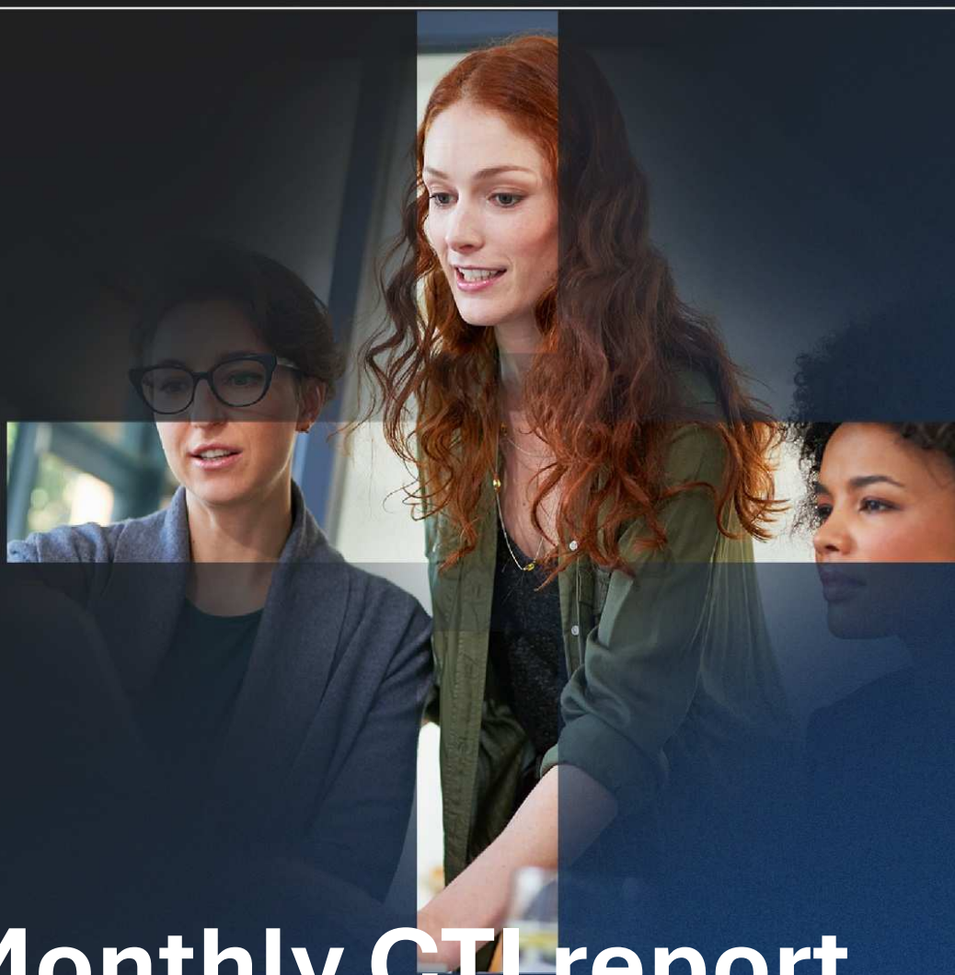
aDvens

For cyber, people & planet



Monthly CTI report

April 2026

CERT aDvens - CTI
Advens - 38 rue des Jeuneurs - 75002 Paris

TABLE OF CONTENT

1. EXECUTIVE SUMMARY

This month, CERT aDvens brings you an overview of emerging threats and recently identified vulnerabilities:

- Three new security vulnerabilities have been detected, all of which have a public *proof of concept* (PoC). These add to the vulnerabilities previously identified.
- An analysis of a recent and massive campaign targeting Microsoft 365 environments.

These topics aim to help you anticipate risks and strengthen your cybersecurity posture.

2. VULNERABILITIES

This month, the CERT aDvens highlights **three** vulnerabilities affecting commonly used technologies within companies.

They are sorted by severity (proofs of concept available, exploitation...). Applying their patches or workarounds is highly recommended.

2.1. CVE-2026-41070

An authentication flaw in OpenVPN has been discovered. When openvpn-auth-oauth2 is deployed in experimental plugin mode, a remote attacker can exploit the vulnerability to connect to the VPN.

The vulnerability can only be exploited if openvpn-auth-oauth2 is deployed in experimental plugin mode. The default management-interface mode is not affected because it does not use the OpenVPN plugin return-code mechanism.

2.1.1. Risk

- Security policy bypass

2.1.2. Type of vulnerability

- **CWE-287**: Improper Authentication

2.1.3. Severity

Attack vector	Network	Scope	Changed
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	None

2.1.4. Affected products

- OpenVPN- (openvpn-auth-oauth2), from versions 1.26.3 before 1.27.3

2.1.5. Recommendation

- Update OpenVPN (openvpn-auth-oauth2) to version 1.27.3 or later

2.1.6. Workarounds

- Switch to standalone management client mode (the default, non-plugin deployment). This mode is not affected by the vulnerability because authentication decisions are communicated entirely through the management interface protocol, not through the plugin return code.

- Restrict VPN access at the network level to only clients known to support WebAuth/SSO (e.g., OpenVPN Connect 3+).

2.1.7. Proof of concept

A proof of concept is available in open source.

2.2. CVE-2026-41676

An incorrect calculation of buffer size in OpenSSL allows a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service.

2.2.1. Risks

- Remote code execution
- Denial of service

2.2.2. Types of vulnerability

- **CWE-131**: Incorrect Calculation of Buffer Size
- **CWE-787**: Out-of-bounds Write

2.2.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Affected products

- OpenSSL (RUST), from versions 0.9.27 before 0.10.78

2.2.5. Recommendation

- Update OpenSSL (RUST) to version 0.10.78 or later.

2.2.6. Proof of concept

A proof of concept is available in open source.

2.3. CVE-2026-41176

A missing authentication in Rclone was discovered. Successful exploitation of this vulnerability allows an unauthenticated attacker to disable security controls, thereby granting them access to sensitive administrative functions, such as service configuration and management.

2.3.1. Risk

- Security policy bypass

2.3.2. Type of vulnerability

- **CWE-306**: Missing Authentication for Critical Function

2.3.3. Severity

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Affected products

- Rclone, from versions 1.45 to 1.73.4

2.3.5. Recommendation

- Update Rclone to version 1.73.5 or later.

2.3.6. Proof of concept

A proof of concept is available in open source.

3. LARGE-SCALE PHISHING CAMPAIGN TARGETING MICROSOFT O365 ENVIRONMENTS

3.1. Introduction

During the month of March, Advens's CERT observed a recurring phishing campaign relying on the use of a single compromised email account. The primary objective of this campaign was the theft of Microsoft credentials belonging to the targeted victims.

The attackers consistently used the same compromised account as the sender, while dynamically adapting both the email subject and the attached file in order to increase the credibility of the message and maximise the compromise rate. This level of customisation was intended to foster trust and encourage recipients to interact with the malicious content.

Phishing remains one of the most widely used initial access vectors, due to its effectiveness and its direct exploitation of the human factor, which continues to be a recurrent weak point in security controls. Attackers primarily rely on psychological triggers such as urgency, fear or pressure to prompt victims into unknowingly disclosing sensitive information, including their credentials.

Once these credentials have been harvested, they can be leveraged to conduct subsequent attacks against the targeted organisation's information system or alternatively be resold on underground forumso on the Darkweb.

This report aims to present the analysis of this phishing campaign, detail the techniques employed and provide operational recommendations designed to reduce the attack surface and limit the impact of this type of threat.

3.2. Analysis of the phishing email

3.2.1. Sender

Throughout the observed campaign, the email sender remains consistently the same: info@sinarsuburlogamindo[.]com.

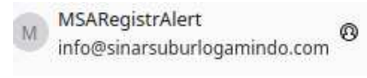


Figure 1. Source: Email sender

Open-source intelligence research also indicates that the address info@sinarsuburlogamindo[.]com has been associated with analyses of malicious emails in sandbox environments, notably Joe Sandbox, where it appears as the sender of messages classified as phishing.

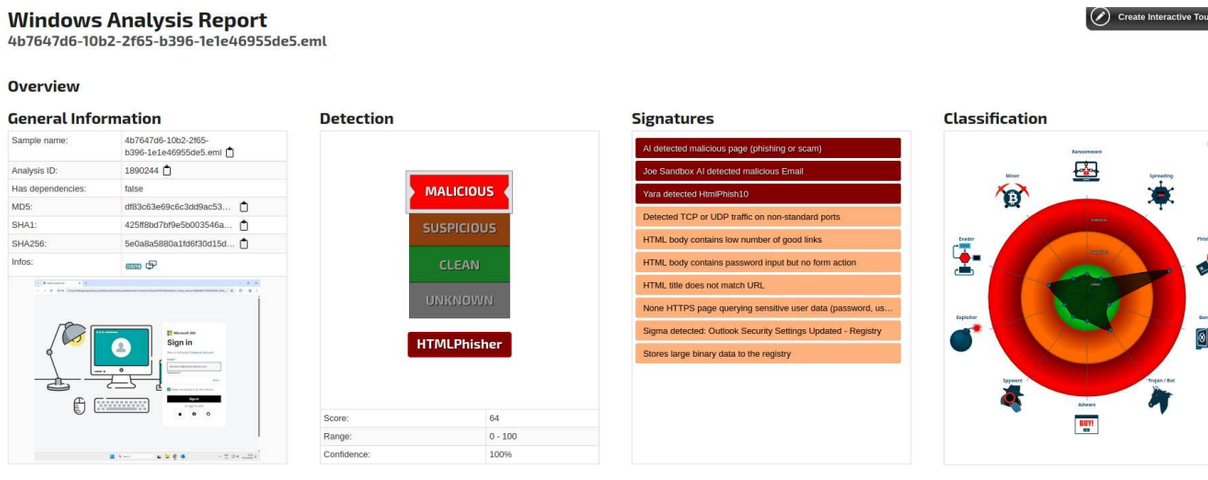


Figure 2. Source: Joe Sandbox – Analysis of the malicious email sent by info@sinarsuburlogamindo[.]com

The domain sinarsuburlogamindo[.]com corresponds to a legitimate company, PT. Sinar Subur Logamindo, founded in 2014 in Indonesia. The company operates in the recycling of aluminium waste and the production of aluminium ingots for the industrial and automotive sectors. Publicly available information (official website, legal registrations and company profiles) confirms the company's existence and business activity over several years, thereby reinforcing the apparent legitimacy of the domain.

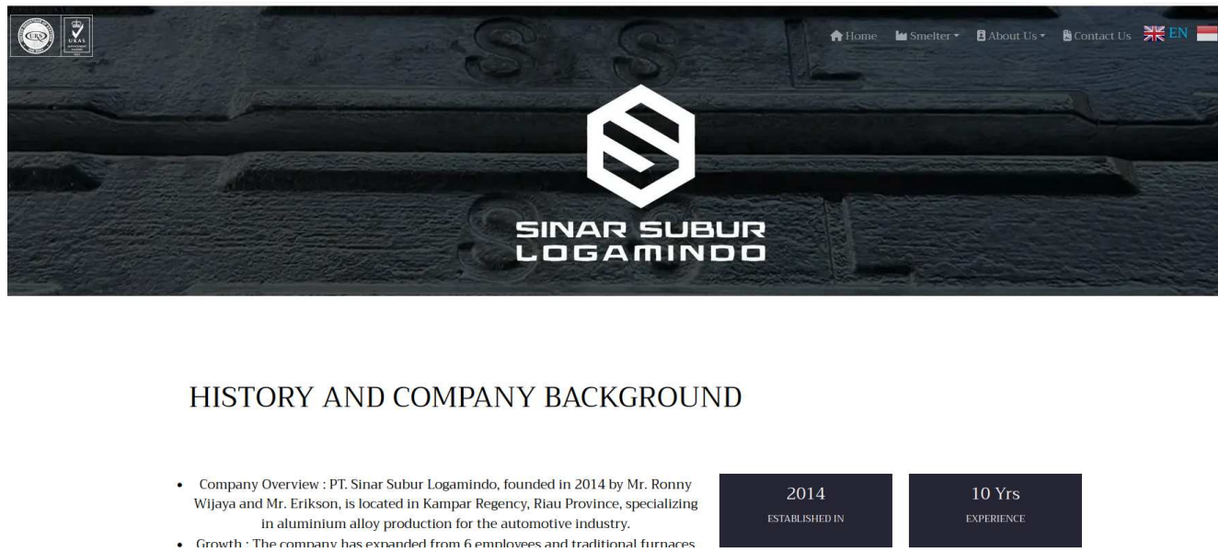


Figure 3. Source: sinarsuburlogamindo[.]com

Analysis of the domain sinarsuburlogamindo[.]com on VirusTotal shows that it is not considered malicious by security vendors at the time of analysis.

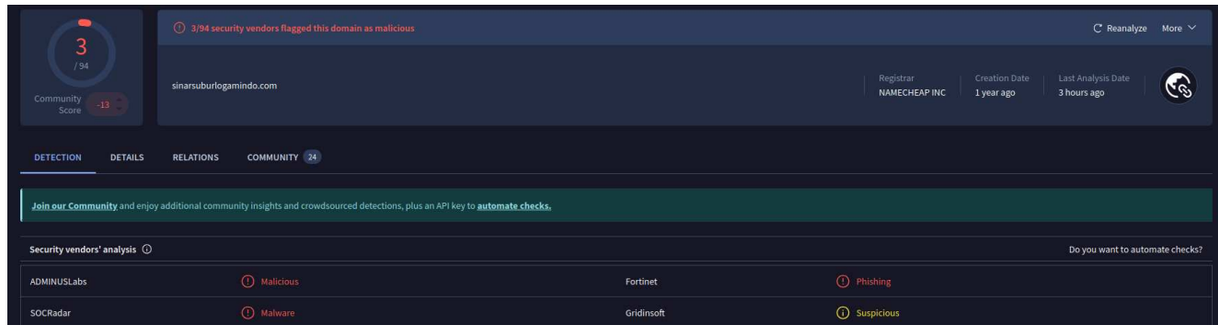


Figure 4. Source: VirusTotal – Analysis of the domain sinarsuburlogamindo[.]com

However, the domain exhibits a strongly negative community reputation, with numerous user reports classifying it as being associated with phishing activities.

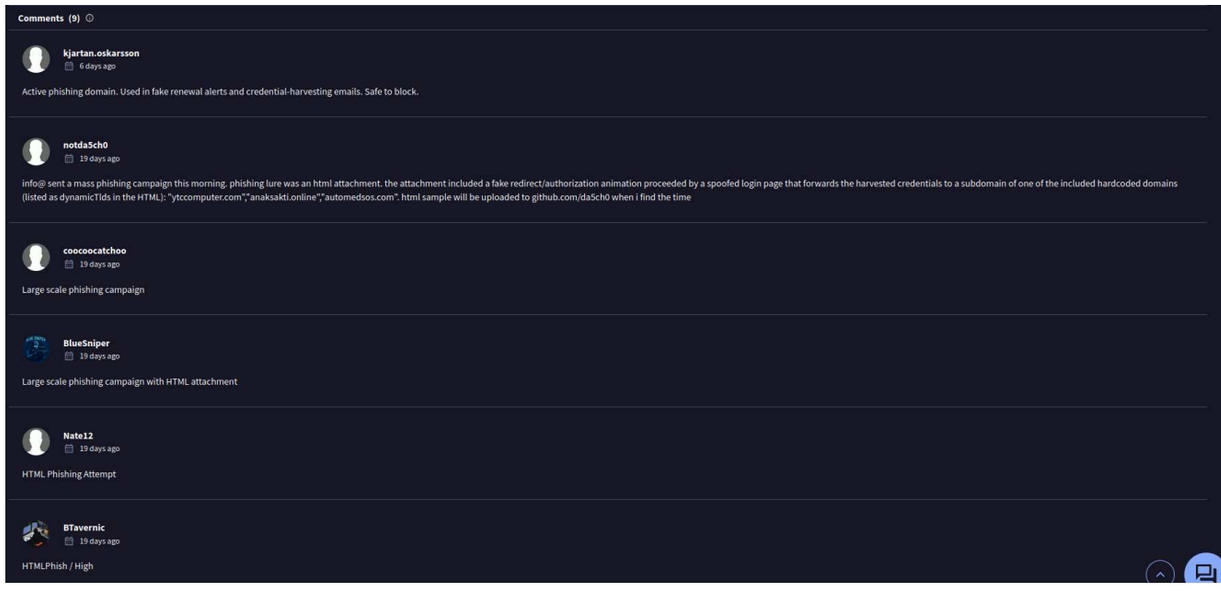


Figure 5. Source: VirusTotal – Analysis of the domain sinarsuburlogamindo[.]com

A more detailed review of the comments indicates that the earliest reports temporally coincide with the onset of the campaign, first observed in March. Several analysts describe a large-scale phishing campaign leveraging HTML attachments, sharing the same modus operandi as the one analysed in this report.

3.2.2. Subject of the email

The subject line observed in this campaign is as follows:

[ALERT]: Failed Renewal for [**victim_domain**] - Fri, 27 Mar 2026 08: **xx** : **xx** -0700 - ID: **XXXXXX**

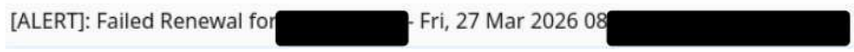


Figure 6. Source : Subject of the email

This subject line combines several elements designed to immediately capture the recipient's attention:

- The use of the term "ALERT" in uppercase letters,
- The explicit mention of a renewal failure,
- The inclusion of the victim's domain name,
- The addition of a precise timestamp and an arbitrary identifier, intended to reinforce the appearance of legitimacy and automation.

This type of wording is frequently observed in phishing campaigns targeting professional environments, as it closely mimics notifications generated by service management systems or cloud platforms.

Further open-source research shows that additional emails analysed as part of this campaign were also sent on the same date and at the same time. However, a discrepancy can be observed between the timestamp included in the email subject line and the actual time of receipt. Specifically, a difference of eight hours was identified, indicating that the timestamp embedded in the subject line is not configured in UTC+1.

Similar timezone discrepancies have been observed in other open-source samples related to this campaign. In these cases, the attackers appear to have used the timezone UTC-7 associated with North America within the subject line, further suggesting the use of standardised or automated infrastructure rather than a reflection of the attackers' actual location.

3.2.3. Message content

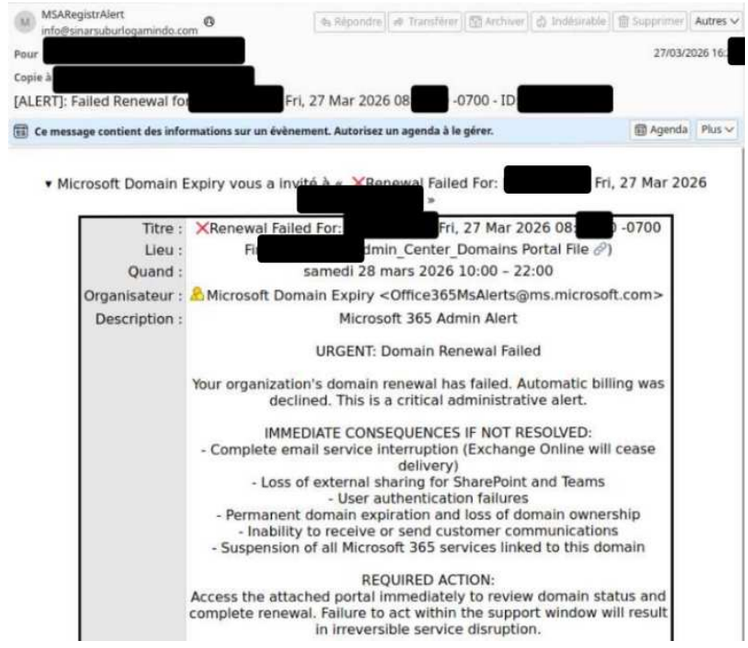


Figure 7. Analysed email

The message content is presented as a meeting invitation, with the organiser displayed as: Office365MsAlerts[@]ms[.]microsoft[.]com.

The meeting is scheduled for Saturday, 28 March 2026, over a particularly wide time window (from 10:00 to 22:00).

Although the address uses the legitimate microsoft[.]com domain, it does not correspond to an address officially used by Microsoft to send alerts related to Office 365 services or domain name renewals. This technique is intended to exploit the trust placed in major software vendors, while remaining sufficiently credible to bypass a superficial user verification.

The message aims to alert the recipient to a critical issue involving the renewal of their organisation's domain name. According to the email content, an automatic payment is claimed to have failed and immediate action is required to avoid serious consequences. Specifically, it is stated that, without intervention, the domain name would be cancelled and that no rollback or recovery would be possible.

The email deliberately employs anxiety-inducing language, using terms such as "alert", "urgent", "required action" and "immediate consequences". These elements are designed to create a sense of urgency and panic, thereby reducing the victim's ability to rationally assess the situation.

Finally, the timing of the email, sent on a Friday for a meeting supposedly scheduled on Saturday, represents a key element of the attack scenario. This choice reinforces the urgency associated with the potential service disruption and is intended to push the recipient to act quickly, without internal validation or in-depth analysis.

3.2.4. Analysis of the attachment

An HTM attachment named Admin_Center_[victim_name]@[numeric_string]MSA.htm is embedded within the message. The recipient is explicitly encouraged to open it in order to access a supposedly official administration portal, allegedly allowing them to renew the affected domain name.

Figure 8. Attached file

The use of an HTM file as an attachment enables redirection to a phishing interface without any visible URL, thereby complicating detection by certain security solutions while simultaneously creating the impression of an internal or official portal.

The file was uploaded to the GLIMPS analysis platform and was classified as malicious.

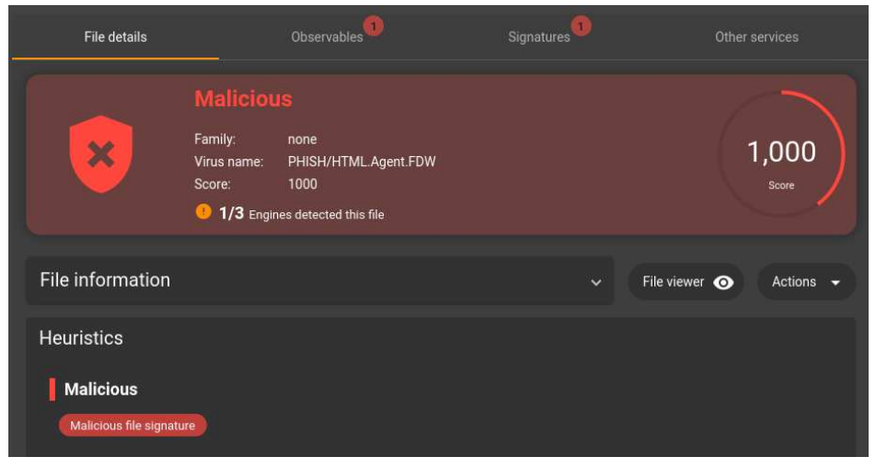


Figure 9. Source: GLIMPS – Attachment analysis

It was categorised as PHISH/HTML.Agent.FDW, indicating a phishing artefact delivered through an HTML page, with the designation “Agent”, which is consistent with the observations already made throughout the analysis.

Further open-source research on the PHISH/HTML.Agent.FDW detection name revealed multiple analyses published on the Hybrid Analysis platform dating back to early April 2026. This once again highlights the scale and persistence of this phishing campaign during the same time period.

The HTML file simulates a Single Sign-On (SSO) “Admin Center” login page designed to mimic Microsoft services. It includes several credibility-enhancing elements, such as: a fake but convincing loading screen, an animated progress Indicator and technical-sounding status messages (e.g. “SSO handshake”, “Authenticating...”).

These visual and textual elements are deliberately used to reinforce the legitimacy of the page and to encourage the victim to enter their credentials without suspicion.

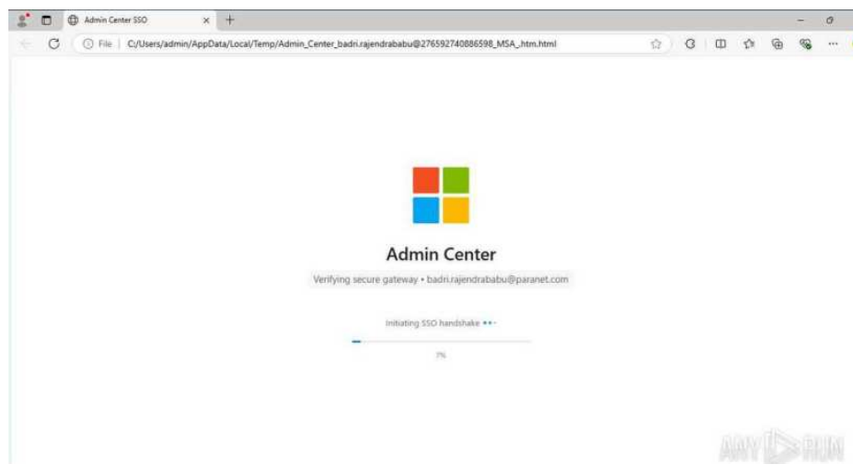


Figure 10. Source : AnyRun - Loading page

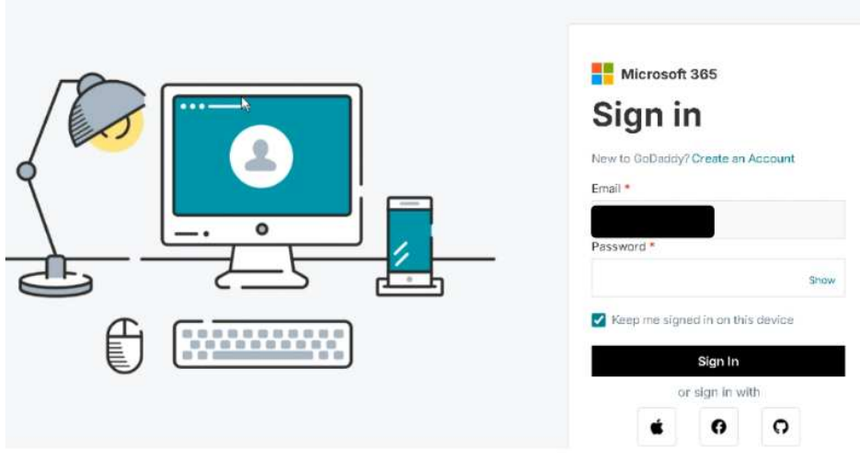


Figure 11. Source : AnyRun - Login page

The objective is to establish trust with the victim, who is led to believe they are interacting with a legitimate SSO portal. As a result, the victim enters their credentials, allowing the attacker to harvest these authentication details. At the same time, additional functions are executed in the background, without the user's awareness.

```
function buildUrl() {
const domain = getRandomDomain();
const randomParam = getRandomString(8);
return `hxxps://${*domain*}:2083/impact?${randomParam}=*victime[@]adresse[.]com*`;
}
```

```
const dynamicTlds = [ "ytccomputer[.]com", "anaksakti[.]online", "automedsos[.]com" ];
```

Figure 12. Source : Glimps - Code

The script implements a dynamic URL construction function designed to obfuscate the true destination of the traffic and to complicate detection efforts.

The code generates a pseudo-random domain name upon each execution by combining randomly generated strings with a predefined list of domains. This technique enables the attackers to vary the endpoints dynamically, thereby reducing the effectiveness of detection and blocking mechanisms based on static signatures or blacklists.

The constructed URL explicitly includes port 2083, which is commonly associated with web administration interfaces, particularly cPanel over HTTPS. The use of this port may indicate an attempt to leverage compromised or poorly secured hosting infrastructures, which are frequently abused in malicious campaigns to host fraudulent content.

Finally, the victim's email address is injected directly into the URL. This mechanism may allow the attackers to uniquely identify or track individual victims, dynamically customise the content displayed or correlate access attempts on the server side.

3.2.5. Analysis of the domains "ytccomputer[.]com", "anaksakti[.]online" and "automedsos[.]com"

During the analysis of the campaign, the domains ytccomputer[.]com, anaksakti[.]online and automedsos[.]com were identified as malicious infrastructure associated with phishing activities. On the VirusTotal platform, these domains are flagged as malicious by multiple security vendors and classified as being linked to phishing campaigns.

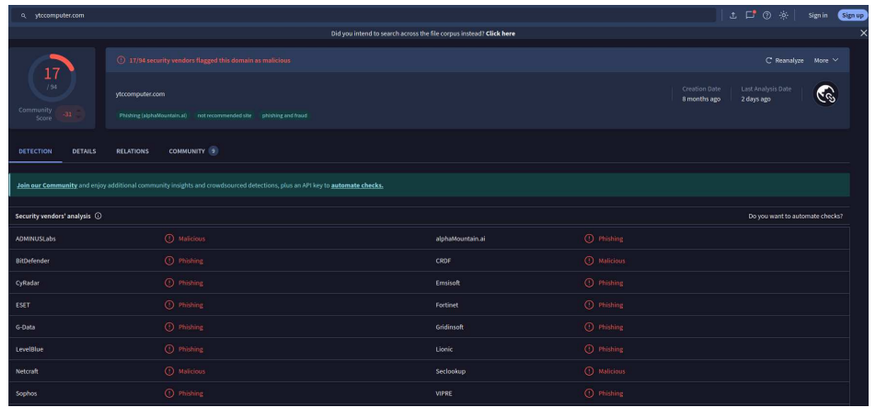


Figure 13. Source: VirusTotal - Analysis of the domain ytccomputer[.]com

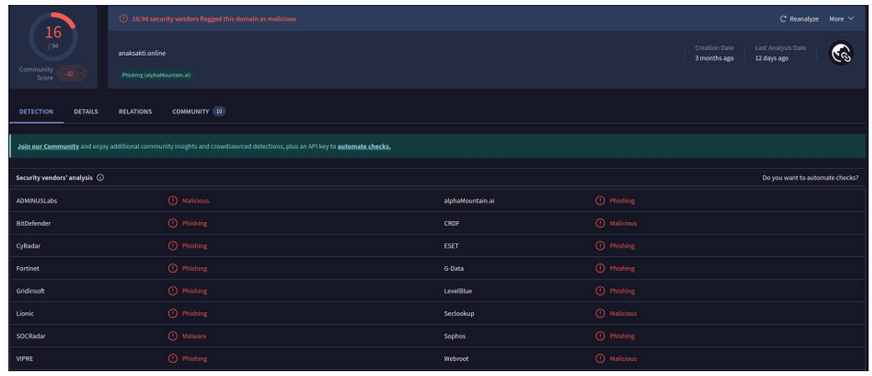


Figure 14. Source : VirusTotal - Analysis of the domain anaksakti[.]online

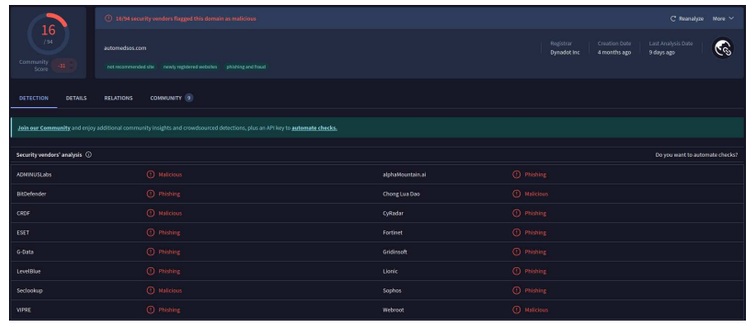


Figure 15. Source : VirusTotal - Analysis of the domain automedsos[.]com

Beyond automated detections, feedback from the analyst community highlights a phishing campaign exhibiting strong similarities with the one analysed by Advens's CERT. These similarities notably include an activity period corresponding to the same timeframe (March 2026), the use of HTML attachments and URLs constructed using random character strings placed before the primary domain.

Figure 16. Source : VirusTotal - Analysis of the domain ytccomputer[.]com

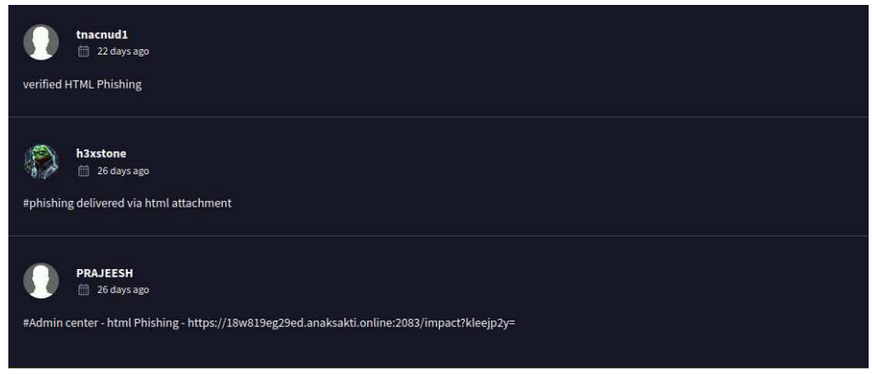


Figure 17. Source : VirusTotal - Analysis of the domain anaksakti[.]online

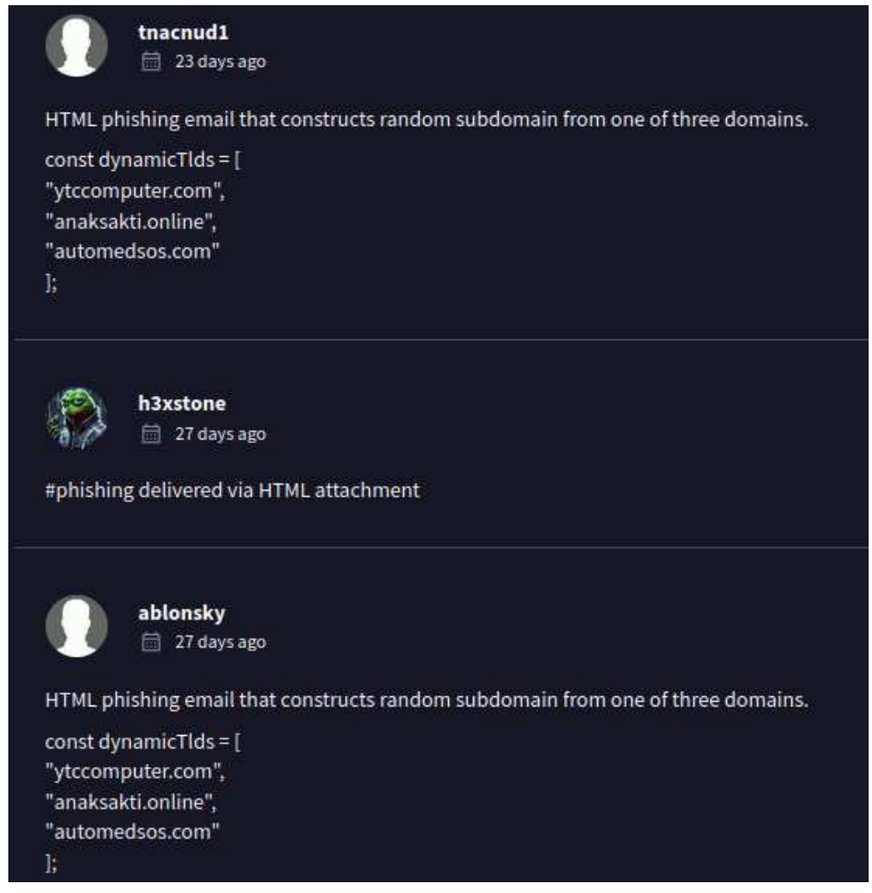


Figure 18. Source : VirusTotal - Analysis of the domain automedsos[.]com

This modus operandi suggests the use of a shared infrastructure across multiple campaigns or the exploitation of a Phishing-as-a-Service (PhaaS) platform, enabling advanced automation in the generation of phishing pages and links.

The use of Namecheap as a registrar is also a common characteristic of phishing campaigns. This provider offers rapid domain registration processes, low costs and the ability to conceal WHOIS information, making it attractive for malicious actors. In addition, the domain is associated with Cloudflare shared IP addresses, which hinders IP-based blocklists and contributes to infrastructure anonymisation.

3.3. Conclusion

The analysis of this phishing campaign highlights a threat that is both classic in its approach and effective in its execution, relying on the exploitation of the human factor, compromised legitimate infrastructure and well-established techniques commonly found in phishing kits.

The correlation of technical indicators, sandbox analyses and community feedback reveals a structured campaign conducted at

scale, rather than an isolated or opportunistic operation.

This campaign clearly illustrates the limitations of a defensive approach based solely on Indicators of Compromise (IOCs). The rapid rotation of domains, the use of shared IP addresses and the abuse of legitimate infrastructure significantly reduce the long-term effectiveness of static blocking mechanisms. In this context, the identification and understanding of the Tactics, Techniques and Procedures (TTPs) employed by attackers remain essential to achieving sustained improvements in detection and response capabilities.

3.4. Recommendations

To reduce the risks associated with phishing, several measures can be implemented to strengthen identity security:

- Deploy a robust multi-factor authentication (MFA) solution
- Implement context-based conditional access policies (location, device, sign-in risk)
- Monitor and restrict connections originating from unexpected countries, non-compliant devices or unknown browsers
- Enable advanced logging for authentication events and access to critical resources.

It is also recommended to enhance the detection of malicious emails:

- Complement reputation-based controls with behaviour-based detection mechanisms (subject line variations, abnormal sending frequency, recurring campaign patterns)
- Implement specific rules for high-risk attachments (HTML, ISO, IMG)
- Encourage the use of built-in reporting buttons within email clients to facilitate rapid incident reporting.

3.5. Tactics, Techniques and Procedures (MITRE ATT&CK)

INITIAL ACCESS

T1566.001 Phishing: Spearphishing Attachment. T1566.002 Phishing: Spearphishing Link.

EXECUTION

T1204.002 User Execution: Malicious File.

CREDENTIAL ACCESS

T1056.003 Input Capture: Web Portal Capture.

DEFENSE EVASION

T1656 Impersonation.

COMMAND AND CONTROL

T1071.001 Application Layer Protocol: Web Protocols.

EXFILTRATION

T1041 Exfiltration Over C2 Channel.

Figure 19. Mitre Att&ck matrix

3.6. Indicators of Compromise

TLP	TYPE	VALUE	DESCRIPTION
TLP:CLEAR	Domain	automedsos[.]com	Phishing infrastructure
TLP:CLEAR	Domain	ytccomputer[.]com	Phishing infrastructure
TLP:CLEAR	Domain	anaksakti[.]online	Phishing infrastructure
TLP:CLEAR	File	Admin_Center_[nom_de_victime]@*MSA*.htm	File included in the phishing email
TLP:CLEAR	Email adress	info@sinarsuburlogamindo[.]com	Legitimate email address used to send this phishing campaign

3.7. DECEPTION Matrix

The table below lists the psychological manipulation tactics and techniques identified in the campaign. This knowledge model (DECEPTION 5.0) is currently under development and aims to help analysts identify and understand the manipulation risks associated with certain cyberattacks.

REFERENCES	TACTICS	TECHNIQUES
T2.11.4	Ressource	Resource for manipulation: Text
T3.14	Initialisation	Emergency effect
T4.23	Intrusion	Exaggeration of problems or False breakdown

4. SOURCES

CVE-2026-41070

- https://www.tenable.com/cve/CVE-2026-41070
- https://advisories.gitlab.com/golang/github.com/jkroepke/openvpn-auth-oauth2/CVE-2026-41070/
- https://github.com/advisories/GHSA-246w-jgmq-88fg

CVE-2026-41676

- https://nvd.nist.gov/vuln/detail/CVE-2026-41676
- https://github.com/rust-openssl/rust-openssl/security/advisories/GHSA-pqf5-4pqq-29f5
- https://www.tenable.com/cve/CVE-2026-41676
- https://dailycve.com/rust-openssl-buffer-overflow-cve-2026-41676-high/

CVE-2026-41176

- https://www.tenable.com/cve/CVE-2026-41176
- https://github.com/rclone/rclone/security/advisories/GHSA-25qr-6mpr-f7qx
- https://security.snyk.io/vuln/SNYK-GOLANG-GITHUBCOMRCLONERCLONEFSRC-16191586

Article

- Virus Total
- Glimps
- https://learn.microsoft.com/en-us/answers/questions/5842804/(alert)-renewal-failed-for-(moderator-note-persona
- https://hybrid-analysis.com/sample/fca3cb967c525b4b3e440b6f4af347b15437b7f74b70678206d49e764e85f006
- https://app.any.run/tasks/e7dce1bd-ac99-4824-bc5a-a349df015879
- https://app.any.run/tasks/46236cd0-5b8e-46cf-a566-87bc0524a997
- https://www.joesandbox.com/analysis/1890244/0/html