

# Fake Zoom and Google Meet scams install Teramind: A technical deep dive

 malwarebytes.com/blog/threat-intel/2026/02/fake-zoom-and-google-meet-scams-install-teramind-a-technical-deep-dive

Stefan Dasic

February 26, 2026



**UPDATE (February 27, 2026):** We have added more clarity around the abuse of legitimate commercial products, and of Teramind's stealth mode.

Important note: Teramind, the software vendor referenced in this article, has stated they are not affiliated with the threat actors described, did not deploy the software referenced, and condemn any unauthorized misuse of commercial monitoring technologies. Teramind is a legitimate commercial product with lawful enterprise use cases.

February 24, 2026, we published an article about how a [fake Zoom meeting “update” silently installs monitoring software](#), documenting a campaign that used a convincing fake Zoom waiting room to push a legitimate Teramind installer abused for unauthorized surveillance onto Windows machines.

Following publication of our findings, the malicious domain was reported to its domain name registrar, Namecheap, which confirmed it suspended the service. Despite the takedown, our continued monitoring shows the campaign is not only still active but growing: we have now identified a parallel operation impersonating Google Meet, running from a different domain and infrastructure.

In this article, we'll provide the deeper technical analysis behind both variants, cataloguing the use of Teramind instance IDs by scammers that we have directly observed or collected from sandbox repositories, document our hands-on detonation of the installer in a controlled environment, and answer a question that emerged during our research: How can a single, identical Windows installer package serve several different attacker accounts?

## The campaign expands to Google Meet

While the original Zoom-themed site at [uswebzoomus\[.\]com](#) was taken down by Namecheap following community reporting, a second site at [googlemeetinterview\[.\]click](#) is actively deploying the same payload using an identical playbook adapted for Google Meet.

The Google Meet variant presents a fake Microsoft Store page branded as “Google Meet for Meetings” published by “Google Meet Video Communications, Inc,” which is a fabricated entity. A “Starting download...” button is displayed while the MSI file is silently delivered via the path [/Windows/download.php](#). The referring page is [/Windows/microsoft-store.php](#), confirming the fake Microsoft Store screen is served by the attacker's infrastructure, not by Microsoft.

Our Fiddler traffic capture of the Google Meet variant shows the response header:

```
Content-Disposition: attachment; filename="teramind_agent_x64_s-
i(__06a23f815bc471c82aed60b60910b8ec1162844d).msi".
```

Unlike the Zoom variant, where the filename was disguised as a Zoom component, this variant does not even attempt to hide the scammer's abuse of Teramind in the filename. We verified both files are byte-for-byte identical (MD5: AD0A22E393E9289DEAC0D8D95D8118B5), confirming a single binary is being served across both campaigns with only the filename changed.

## Infrastructure differences between variants

---

Despite using the same payload, the two variants are hosted on different infrastructure. The Zoom variant at [uswebzoomus\[.\]com](#) ran on Apache/2.4.58 (Ubuntu) and was registered through Namecheap on 2026-02-16. The Google Meet variant at [googlemeetinterview\[.\]click](#) runs on a LiteSpeed server.

Both serve the download via PHP scripts and use the same fake Microsoft Store redirect pattern, but the switch in web server and domain registrar suggests the operator anticipated takedowns and pre-positioned fallback infrastructure.

## One binary, many identities. How the installer reads its own filename

---

During our investigation, we identified 14 distinct MSI filenames sharing the same SHA-256 hash. Of these, two were directly captured from malicious infrastructure through our malware domain analysis: the Zoom variant from [uswebzoomus\[.\]com](#) and the Google Meet variant from [googlemeetinterview\[.\]click](#). The remaining filenames were sourced from sandbox repositories.

It is important to note that some of these sandbox-sourced filenames may represent legitimate corporate Teramind deployments rather than malicious activity. Teramind is a commercial product with lawful enterprise use cases, and files submitted to sandbox services do not necessarily indicate abuse. Nevertheless, they all share the same binary and demonstrate the same filename-based configuration mechanism.

Every file shares the same SHA-256 hash: `644ef9f5eea1d6a2bc39a62627ee3c7114a14e7050bafab8a76b9aa8069425fa`. This raised an immediate question: if the Teramind instance ID changes with every filename, but the binary is byte-for-byte identical, where is the ID actually stored?

The answer lies in a .NET custom action embedded inside the MSI. Our behavioral analysis reveals the following sequence:

```
Calling custom action Teramind.Setup.Actions!Teramind.Setup.Actions.CustomActions.ReadPropertiesFromMsiName
```

```
PROPERTY CHANGE: Modifying TMINSTANCE property. Its current value is 'onsite'. Its new value:
'__941afee582cc71135202939296679e229dd7cced'.
```

```
PROPERTY CHANGE: Adding TMROUTER property. Its value is 'rt.teramind.co'.
```

The MSI ships with a default `TMINSTANCE` value of `onsite`. This is the standard Teramind on-premise default. At install time, the `ReadPropertiesFromMsiName` custom action parses the installer's own filename, extracts the 40-character hex string from the `s-i(__)` portion, and overwrites the default with the attacker-specific instance ID.

The log also shows the message `Failed to get router from msi name`. The installer attempted to extract a C2 server address from the filename but could not. In this case, it falls back to the default value `rt.teramind.co`, which is preconfigured inside the MSI. However, `TMROUTER` is an exposed MSI property, so it could potentially be overridden at install time or changed in a different build. The filename in this campaign carries only the instance ID; the C2 destination is determined by the MSI's default configuration.

## Live detonation: what the installer actually does on a real system

---

To go beyond sandbox-based behavioral analysis, we detonated the MSI installer in an isolated Windows 10 virtual machine with verbose MSI logging enabled, ApateDNS for DNS interception, and Fiddler for network monitoring. This hands-on analysis revealed several critical behaviors not visible in automated sandbox reports.

## Installation chain and the CheckHosts gate

---

The MSI installer progresses through four .NET custom actions in sequence, all executed via the WiX Toolset's `zzzzInvokeManagedCustomActionOutOfProc` mechanism:

- **ReadPropertiesFromMsiName:** Parses the MSI's own filename to extract the Teramind instance ID and overwrites the default `onsite` value
- **CheckAgent:** Determines whether a Teramind agent is already installed on the machine
- **ValidateParams:** Validates the extracted configuration parameters
- **CheckHosts:** Performs a pre-flight connectivity check against the C2 server `rt.teramind.co`

The `CheckHosts` action is a hard gate: if the installer cannot reach the Teramind server, installation aborts with error code 1603. Our initial detonation attempt in a network-isolated VM failed at exactly this point:

```
TM: TMINSTANCE = __941afee582cc71135202939296679e229dd7cced
```

```
TM: TMROUTER = rt.teramind.co
```

```
CustomAction CheckHosts returned actual error code 1603
```

This behavior is significant for two reasons. First, it reveals the C2 server address: `rt.teramind.co`. Second, it means that victims on corporate networks with restrictive DNS or outbound filtering may be inadvertently protected. The installer will silently fail if it cannot phone home during installation. However, the MSI does support a `TMSKIPSRVCHECK` property that can bypass this check, and its default value is `no`.

To complete our analysis, we added `rt.teramind.co` to the Windows hosts file pointing to localhost, allowing the DNS resolution to succeed and the `CheckHosts` action to pass. The installation then completed successfully.

## Stealth mode confirmed

The successful installation log confirms what the original article suspected: Teramind's stealth mode (called Hidden Agent, a deployment option that runs silently in the background) is enabled by default in this build. Hidden or stealth deployment modes are standard features in legitimate enterprise endpoint monitoring products, typically used for insider threat detection or compliance monitoring with appropriate employee notice and consent. In this campaign, however, threat actors can abuse this feature to deploy the agent without victim knowledge. The MSI property dump shows:

```
Property(S): TMSTEALTH = 1
```

This confirms the agent installs with no taskbar icon, no system tray entry, and no visible entry in the Windows Programs list. The victim has no visual indication that monitoring software is running.

## Two services, not one

The install log reveals the campaign deploys two persistent services, not just the one documented in our original article:

| Service Name | Display Name        | Binary            | Start Type       |
|--------------|---------------------|-------------------|------------------|
| tsvchst      | Service Host        | svc.exe --service | Automatic (boot) |
| pmon         | Performance Monitor | pmon.exe          | Manual (demand)  |

Both service names are chosen to blend in: `tsvchst` mimics the legitimate Windows `svchost.exe` naming pattern, while `pmon` with the display name "Performance Monitor" mimics the built-in Windows Performance Monitor. Both run as `LocalSystem`, the highest privilege level on a Windows machine.

Both services are configured with aggressive failure recovery: restart on first failure, restart on second failure, and restart on subsequent failures, with delays of 160 seconds (`tsvchst`) and 130 seconds (`pmon`). This means even if a user or security tool terminates the service, it automatically restarts within minutes.

## Live C2 callback observed

Immediately after installation, ApateDNS captured the agent phoning home. DNS queries for `rt.teramind.co` appeared within seconds of the service starting, confirming the agent begins its callback cycle immediately. The queries repeated at approximately 11-second intervals, showing a persistent polling pattern.

In a real-world scenario where the victim has internet connectivity, these would resolve to Teramind's infrastructure and the agent would begin transmitting captured data.

## Full MSI configuration surface

---

The verbose installation log exposes every configurable parameter the MSI supports through its `SecureCustomProperties` list. This reveals the installer's full configuration surface:

- `TMSTEALTH` — Stealth mode (set to 1 in this build)
- `TMINSTANCE` — Account identifier (extracted from filename)
- `TMROUTER` — C2 server address (hardcoded to `rt.teramind.co`)
- `TMENCRYPTION` — C2 communication encryption toggle
- `TMSOCKSHOST` / `TMSOCKSPORT` / `TMSOCKSUSER` / `TMSOCKSPASSWORD` — Built-in SOCKS5 proxy support for tunneling C2 traffic through proxies
- `TMHTTPPROXY` — HTTP proxy support
- `TMSKIPSRVCHECK` — Skip the C2 connectivity pre-flight check
- `TMNODRV` / `TMNOFSDRV` — Disable kernel filter drivers
- `TMNOIPCCLIPBOARD` — Clipboard monitoring toggle
- `TMNOREMOTETS` — Remote terminal services monitoring toggle
- `TMHASHUSERNAMES` — Anonymize/hash captured usernames
- `TMDISABLESCREEN` — Disable screenshot capture
- `TMADDENTRYTOARP` — Add/remove entry from Add/Remove Programs (off in stealth)
- `TMCRASHUPLOADURL` — Crash telemetry upload endpoint
- `TMREVEALEDPASSWORDLESS` — Toggle for passwordless reveal functionality

The SOCKS5 proxy support is particularly noteworthy from a threat perspective. While proxy configuration is a standard enterprise feature—allowing organizations to route agent traffic through corporate infrastructure—in this context it means the agent could be configured to route captured data through an attacker-controlled proxy, making network-level detection significantly harder by disguising C2 traffic as legitimate proxy traffic.

## Observed Teramind instance IDs

---

The following table lists every MSI filename and corresponding Teramind instance ID we have collected. Of these, two were directly observed in the wild through our own malware domain analysis: the Zoom variant (`941afee...7cced`, captured from `uswebzoomus[.]com`) and the Google Meet variant (`06a23f8...2844d`, captured from `googlemeetinterview[.]click`). The remaining filenames were sourced from sandbox repositories.

As noted above, some of these may represent legitimate enterprise deployments rather than malicious use. All files share the same SHA-256 hash. Two filenames share the same instance ID `c0cea71...0a6d7`, indicating the same attacker account was used across multiple filename variations.

| MSI Filename                                                                    | Instance ID                               |
|---------------------------------------------------------------------------------|-------------------------------------------|
| zoom_agent_x64_s-i(__941afee582cc71135202939296679e229dd7cced).msi              | 941afee582cc71135202939296679e229dd7cced  |
| ZoomApp_agent_x64_s-i(__fca21db2bb0230ee251a503b021fe02d2114d1f0).msi           | fca21db2bb0230ee251a503b021fe02d2114d1f0  |
| 945bd48ad7552716f4583_s-i(__d72c88943945bd48ad7552716f4583ada0b7c2a6).msi       | d72c88943945bd48ad7552716f4583ada0b7c2a6  |
| teramind_agent_x64_s-i(__572d85bb94f4f59ef947c3faf42677f9adb223c3).msi          | 572d85bb94f4f59ef947c3faf42677f9adb223c3  |
| file_agent_x64_s-i(__f76fee1df21e19d93d5842f50c375286477b3f6c).msi              | f76fee1df21e19d93d5842f50c375286477b3f6c  |
| teramind_agent_x64_s-i(__653d105a51cc886dede8101d1b0cd02e20329546).msi          | 653d105a51cc886dede8101d1b0cd02e20329546  |
| e411293f92e8730f717_s-i(__c0cea713de411293f92e8730f71759aa1890a6d7).msi         | c0cea713de411293f92e8730f71759aa1890a6d7  |
| 0154299765aa7b198bce97d8361_s-i(__c0cea713de411293f92e8730f71759aa1890a6d7).msi | c0cea713de411293f92e8730f71759aa1890a6d7  |
| GoogleMeet_agent_x64_s-i(__ab28818c0806ce7996c10c59b0e4e5d102783461).msi        | ab28818c0806ce7996c10c59b0e4e5d102783461  |
| teramind_agent_x64_s-i(__5ca3d9dd35249200363946b1f007b59f88dbde39).msi          | 5ca3d9dd35249200363946b1f007b59f88dbde39  |
| file_agent_x64_s-i(__81c39bed817fc9989834c81352cb7f69b94342da).msi              | 81c39bed817fc9989834c81352cb7f69b94342da  |
| GoogleMeet_agent_x64_s-i_94120be3942474019852c62041d2f373fdb11a0e.msi           | 94120be3942474019852c62041d2f373fdb11a0e  |
| AdobeReader_agent_x64_s-i(__d57d34e76cc8c2c883cbdcdb42a14c47d00be03c0).msi      | d57d34e76cc8c2c883cbdcdb42a14c47d00be03c0 |
| teramind_agent_x64_s-i(__06a23f815bc471c82aed60b60910b8ec1162844d).msi          | 06a23f815bc471c82aed60b60910b8ec1162844d  |

The variety of filename prefixes is notable: `zoom_agent`, `ZoomApp_agent`, `GoogleMeet_agent`, `AdobeReader_agent`, `teramind_agent`, and `file_agent`. This suggests the campaign extends beyond video conferencing impersonation.

However, the AdobeReader-branded variant was found only in sandbox repositories and may represent testing or planned expansion rather than an active deployment. The filenames with generic prefixes like `teramind_agent` and `file_agent` similarly appear to be sandbox submissions that retained the default naming rather than a brand-specific social engineering lure.

## Indicators of Compromise

### File hashes

SHA-256: 644ef9f5eea1d6a2bc39a62627ee3c7114a14e7050bafab8a76b9aa8069425fa

MD5: AD0A22E393E9289DEAC0D8D95D8118B5

### Domains

uswebzoomus[.]com (Zoom variant: taken down by Namecheap)

googlemeetinterview[.]click (Google Meet variant: active as of 2026-02-26)

## Detection and defense recommendations

- **Alert on the ProgramData GUID directory** `{4CEC2908-5CE4-48F0-A717-8FC833D8017A}`. This GUID is fixed across all observed variants.
- **Query for both services:** `sc query tsvchst` and `sc query pmon`. Either running on a non-corporate machine confirms active surveillance.

- **Watch for kernel driver loads:** `tm_filter.sys` and `tmfsdrv2.sys` loading on personal machines should trigger high-severity alerts.
- **Block MSI execution from browser download directories.** Both variants rely on the user running an MSI from their Downloads folder. Application control policies that prevent MSI execution from user-writable paths would stop this attack chain.
- **Educate employees:** Never update applications by clicking links in messages. Use the application's built-in update mechanism or navigate to the vendor's official website manually.
- **Deploy browser policies** that warn on or block automatic file downloads from unrecognized domains.

## Removal

---

To uninstall the agent, run the following command as Administrator: `msiexec /x {4600BEDB-F484-411C-9861-1B4DD6070A23} /qb`. This removes the services, kernel drivers, and most installed files. However, our testing confirmed the uninstaller fails to fully delete the ProgramData directory due to runtime-generated files. After uninstalling, manually remove any remnants with `rmdir /s /q "C:\ProgramData\{4CEC2908-5CE4-48F0-A717-8FC833D8017A}"` and reboot to fully unload the kernel drivers from memory.

## Conclusion

---

This campaign demonstrates a growing trend: the abuse of legitimate commercial software for malicious purposes. The attackers did not write custom malware. Instead, they took an off-the-shelf monitoring product—one designed for lawful enterprise use—and abused its built-in stealth mode and filename-based configuration system, wrapping it in social engineering designed to exploit trust in brands like Zoom and Google Meet. This type of abuse can affect any legitimate software vendor and underscores the importance of user education about social engineering tactics.

The expansion to Google Meet, plus additional sandbox-sourced variants including an AdobeReader-branded filename, suggests this is an evolving operation that may expand to impersonate other applications.

Our hands-on detonation revealed details invisible to automated sandboxes: the `CheckHosts` C2 pre-flight gate, the `rt.teramind.co` router address, the second `pmon` service masquerading as Performance Monitor, the confirmed `TMSTEALTH = 1` flag, and the full SOCKS5 proxy capability for C2 evasion. The fact that a single binary serves unlimited attacker accounts through nothing more than a filename rename makes this campaign easily scalable.

## Acknowledgments

---

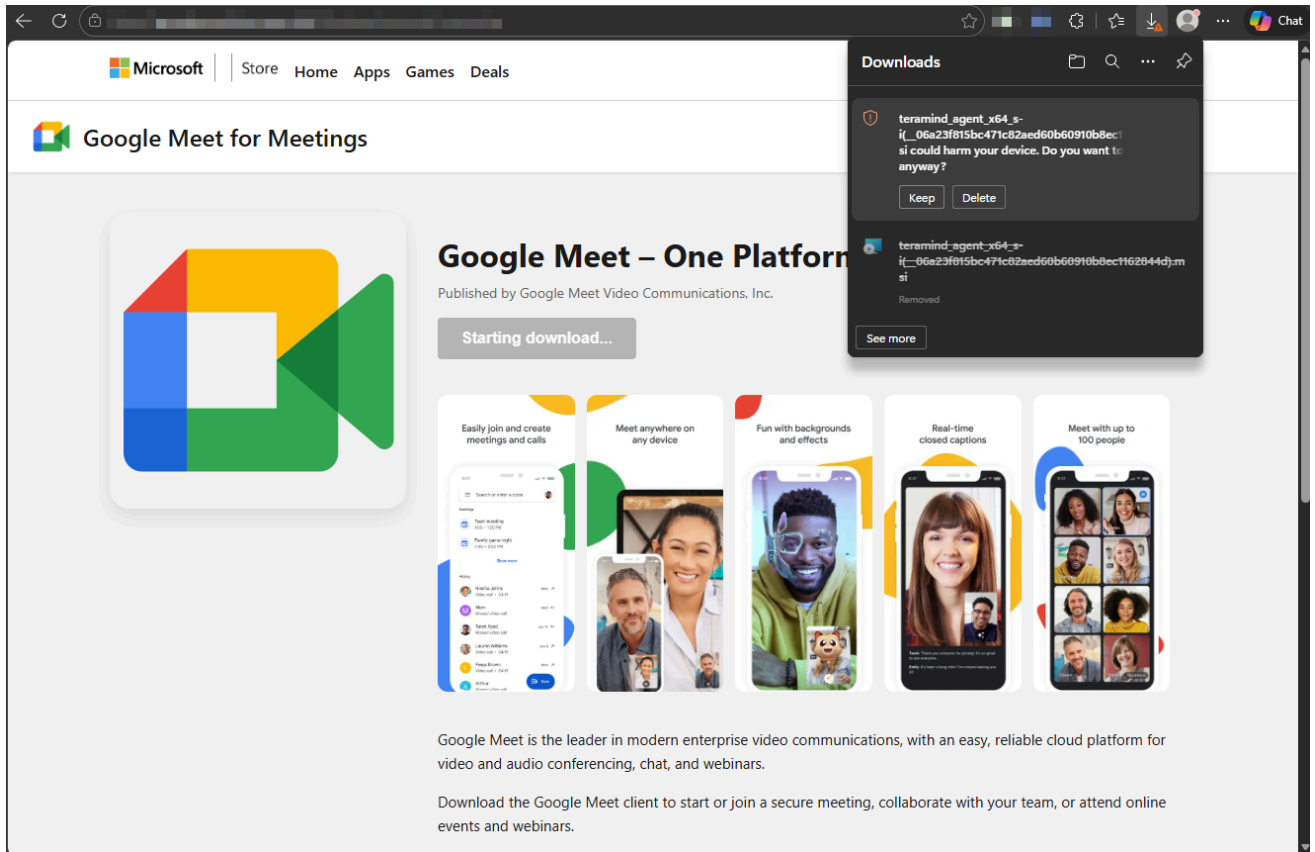
We would like to thank security researcher [@JAMESWT\\_WT](#) for promptly reporting the original malicious domain to Namecheap, leading to the takedown of [uswebzoomus\[.\]com](#).

Teramind has confirmed that the company was not involved in this campaign and had no knowledge of or affiliation with the threat actors. Like many legitimate commercial software products, Teramind can be abused by malicious actors—a risk that exists across the enterprise software ecosystem. Because Teramind is a legitimate commercial product, it is not inherently flagged by security software, meaning we have no visibility into whether this campaign has resulted in real-world infections. What we can confirm is that the infrastructure we documented—including purpose-built phishing domains impersonating Zoom and Google Meet, fake Microsoft Store pages, and a Teramind agent configured in stealth mode—is consistent with a campaign designed to deploy monitoring software onto targets' machines without their knowledge or consent.

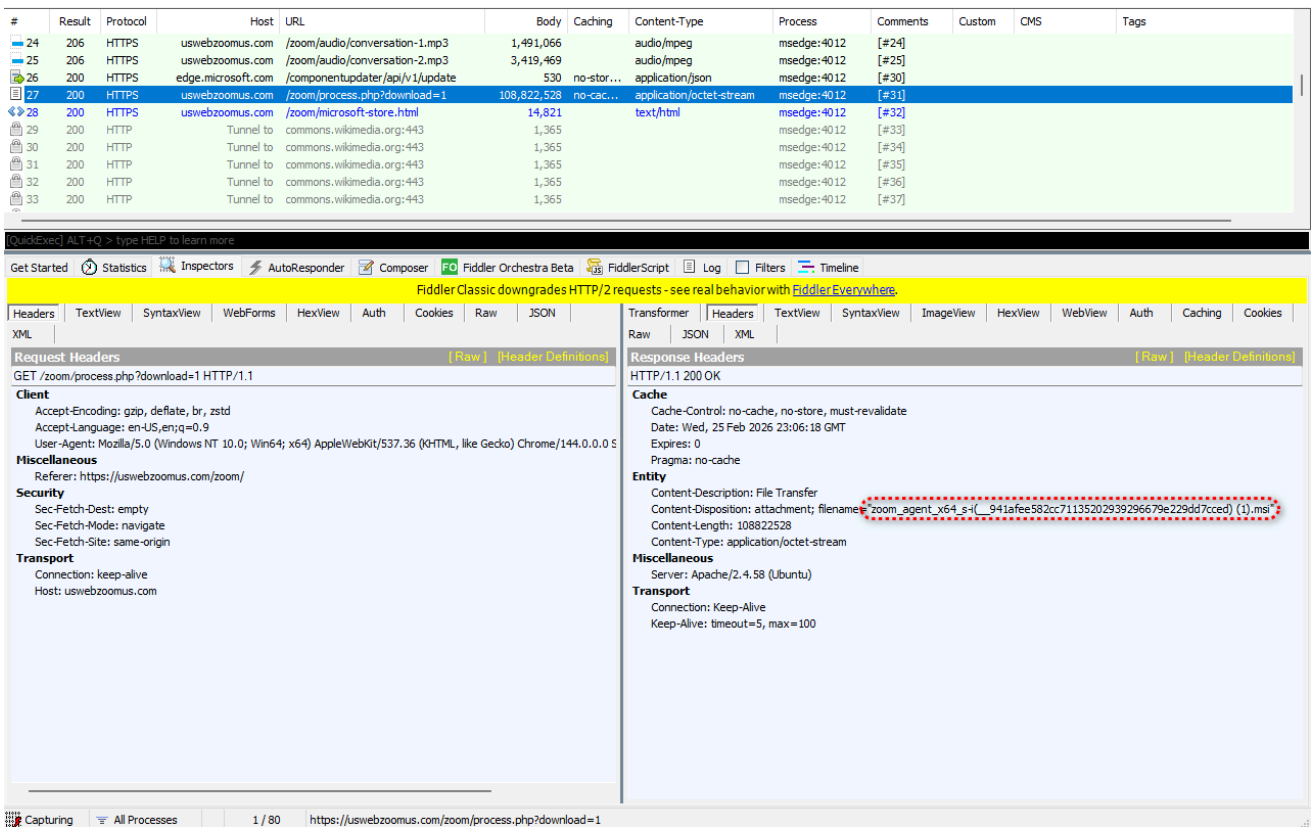
## Videos and screenshots

---

Fake Zoom update clickthrough.



Fake Google Meet site.



Traffic to the fake Zoom site.

| #   | Result | Protocol | Host                      | URL                                    | Body        | Caching          | Content-Type                | Process     | Comments | Custom | CMS | Tags |
|-----|--------|----------|---------------------------|----------------------------------------|-------------|------------------|-----------------------------|-------------|----------|--------|-----|------|
| 103 | 200    | HTTPS    | googlemeetinterview.click | /Windows/img/sc3.webp                  | 15,194      |                  | image/webp                  | msedge:4012 | [#23]    |        |     |      |
| 104 | 400    | HTTPS    | fonts.googleapis.com      | /css2?family=Segoe+UI:wght@400;...     | 6,441       | no-cache, no-... | text/html; charset=utf-8    | msedge:4012 | [#24]    |        |     |      |
| 105 | 200    | HTTPS    | googlemeetinterview.click | /Windows/img/sc4.webp                  | 14,226      |                  | image/webp                  | msedge:4012 | [#25]    |        |     |      |
| 106 | 200    | HTTP     | Tunnel to                 | edge.microsoft.com:443                 | 747         |                  |                             | msedge:4012 | [#26]    |        |     |      |
| 107 | 200    | HTTPS    | googlemeetinterview.click | /Windows/img/sc5.webp                  | 18,012      |                  | image/webp                  | msedge:4012 | [#27]    |        |     |      |
| 108 | 200    | HTTPS    | edge.microsoft.com        | /autofillservice/core/page/-1905757... | 20          | max-age=69...    | application/json; charse... | msedge:4012 | [#28]    |        |     |      |
| 109 | 200    | HTTPS    | googlemeetinterview.click | /Windows/download.php                  | 108,837,488 | must-revalida... | application/octet-stream    | msedge:4012 | [#29]    |        |     |      |
| 110 | 200    | HTTPS    | googlemeetinterview.click | /Windows/microsoft-store.php           | 7,392       |                  | text/html; charset=UTF-8    | msedge:4012 | [#30]    |        |     |      |
| 111 | 200    | HTTP     | Tunnel to                 | fonts.googleapis.com:443               | 1,040       |                  |                             | msedge:4012 | [#31]    |        |     |      |
| 112 | 400    | HTTPS    | fonts.googleapis.com      | /css2?family=Segoe+UI:wght@400;...     | 6,441       | no-cache, no-... | text/html; charset=utf-8    | msedge:4012 | [#32]    |        |     |      |

[QuickExec] ALT+Q > type HELP to learn more

Get Started Statistics Inspectors AutoResponder Composer Fiddler Orchestra Beta FiddlerScript Log Filters Timeline

Fiddler Classic downgrades HTTP/2 requests - see real behavior with Fiddler Everywhere

| Headers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | TextView | SyntaxView | WebForms | HexView | Auth | Cookies | Raw | JSON | Transformer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Headers | TextView | SyntaxView | ImageView | HexView | WebView | Auth | Caching | Cookies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|------------|----------|---------|------|---------|-----|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|----------|------------|-----------|---------|---------|------|---------|---------|
| XML                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |          |            |          |         |      |         |     |      | Raw                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | JSON    | XML      |            |           |         |         |      |         |         |
| <b>Request Headers</b> [Row] [Header Definitions]<br>GET /Windows/download.php HTTP/1.1<br><b>Client</b><br>Accept-Encoding: gzip, deflate, br, zstd<br>Accept-Language: en-US,en;q=0.9<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 S<br><b>Miscellaneous</b><br>Referer: https://googlemeetinterview.click/Windows/microsoft-store.php<br><b>Security</b><br>Sec-Fetch-Dest: empty<br>Sec-Fetch-Mode: navigate<br>Sec-Fetch-Site: same-origin<br><b>Transport</b><br>Connection: keep-alive<br>Host: googlemeetinterview.click |          |            |          |         |      |         |     |      | <b>Response Headers</b> [Row] [Header Definitions]<br>HTTP/1.1 200 OK<br><b>Cache</b><br>Cache-Control: must-revalidate<br>Date: Thu, 26 Feb 2026 13:00:02 GMT<br>Expires: 0<br>Pragma: public<br><b>Entity</b><br>Content-Description: File Transfer<br>Content-Disposition: attachment; filename="teramind_agent_x64_s-(_06a23f815bc471c82aed60b60910b8ec1162844d).msi"<br>Content-Length: 108822528<br>Content-Transfer-Encoding: binary<br>Content-Type: application/octet-stream<br><b>Miscellaneous</b><br>Server: LiteSpeed<br><b>Transport</b><br>Connection: Keep-Alive<br>Keep-Alive: timeout=5, max=100 |         |          |            |           |         |         |      |         |         |

Capturing All Processes 1 / 112 https://googlemeetinterview.click/Windows/download.php

Google Meet interview traffic.

← Post

 **JAMESWT**  
@JAMESWT\_WT



@Namecheap  
fake @Zoom Website spread malware

[https://uswebzoomus.\]com/zoom](https://uswebzoomus.]com/zoom)  
[https://uswebzoomus.\]com/zoom/process.php?download=1](https://uswebzoomus.]com/zoom/process.php?download=1)



[virustotal.com/gui/file/644ef...](https://virustotal.com/gui/file/644ef...)



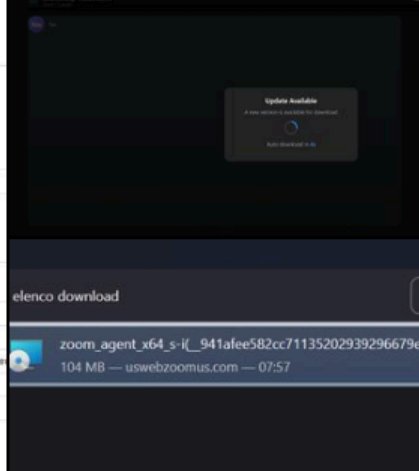
[bazaar.abuse.ch/sample/c73b756...](https://bazaar.abuse.ch/sample/c73b756...)



[app.any.run/tasks/88ca5549...](https://app.any.run/tasks/88ca5549...)

Record for Uswebzoomus.com

|              |                                                                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File         | NameCheap, Inc.<br>IANA ID: 1048<br>URL: <a href="http://www.namecheap.com">http://www.namecheap.com</a><br>Whois Server: whois.namecheap.com<br>abuse@namecheap.com<br>(p) +1.6613102107 |
| Usage        | clientTransferProhibited                                                                                                                                                                  |
| Age          | 9 days old<br>Created on 2026-02-16<br>Expires on 2027-02-16<br>Updated on 2026-02-17                                                                                                     |
| Hosts        | ARTEMIS.DNS-PARKING.COM (has 9,266,701 domains)<br>HERMES.DNS-PARKING.COM (has 9,266,701 domains)<br>76.13.126.51 is hosted on a dedicated server                                         |
| Registrar    | AS47583 AS-HOSTINGER Hostinger International Limited, CY (registered in New York - New York - Yahoo Holdings Inc.)                                                                        |
| Registration | Registered And No Website                                                                                                                                                                 |
| Changes      | 3 changes on 3 unique IP addresses over 0 years<br>2 changes on 3 unique name servers over 0 year                                                                                         |
| History      | (last updated on 2026-02-26)                                                                                                                                                              |



 Gianni Amato and 6 others

 **Malwarebytes** @Malwarebytes · Feb 24

A fake Zoom meeting site mimics a video call, then uses an “Update Available” countdown to automatically download a malicious installer onto Windows machines—no permission required.

[bit.ly/4qXyLp7](https://bit.ly/4qXyLp7)

8:08 AM · Feb 26, 2026 · 802 Views



1



1



11



1



Post your reply

Reply



**Namecheap.com** @Namecheap · 11h

Hello! We have suspended the abusive service. Thank you for reporting the issue!



2



50



Namecheap takedown.

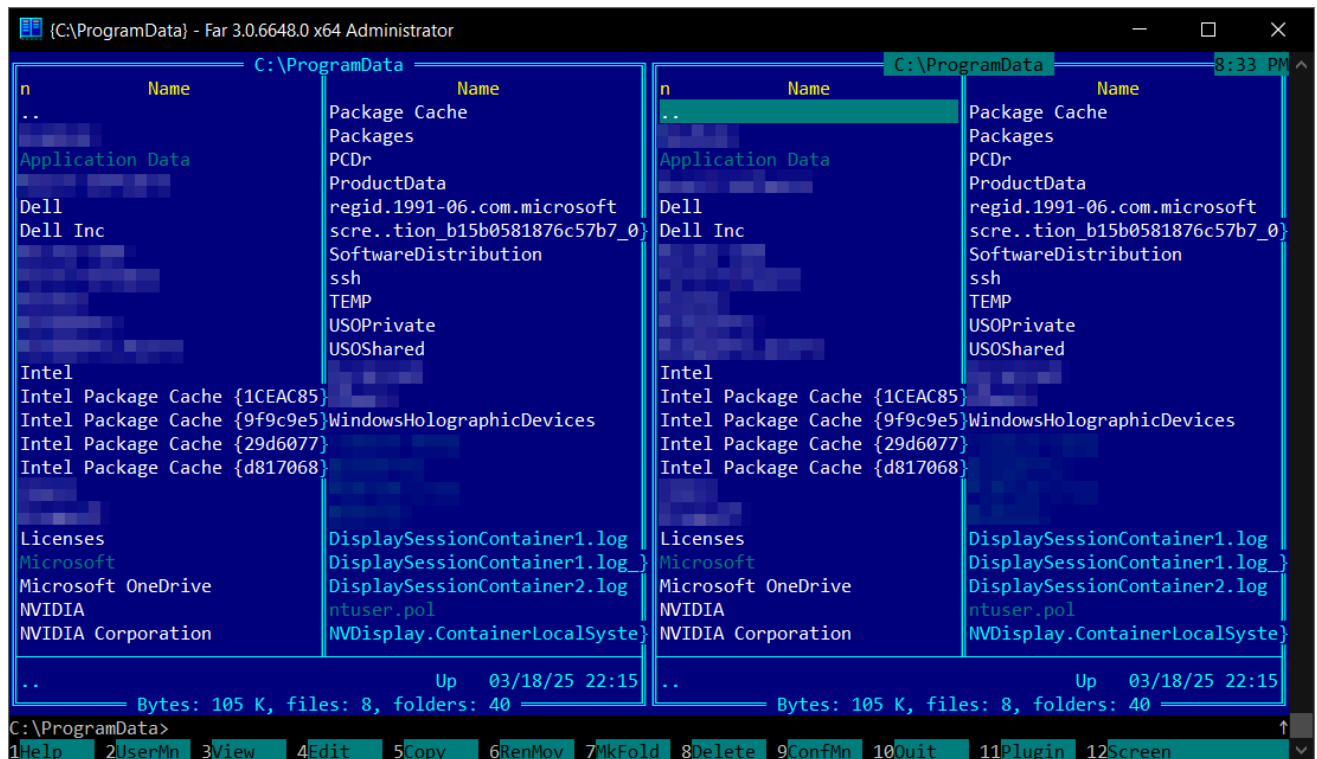
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.5679]
(c) Microsoft Corporation. All rights reserved.

C:\Users\>sc query tsvchst
[SC] EnumQueryServicesStatus:OpenService FAILED 1060:

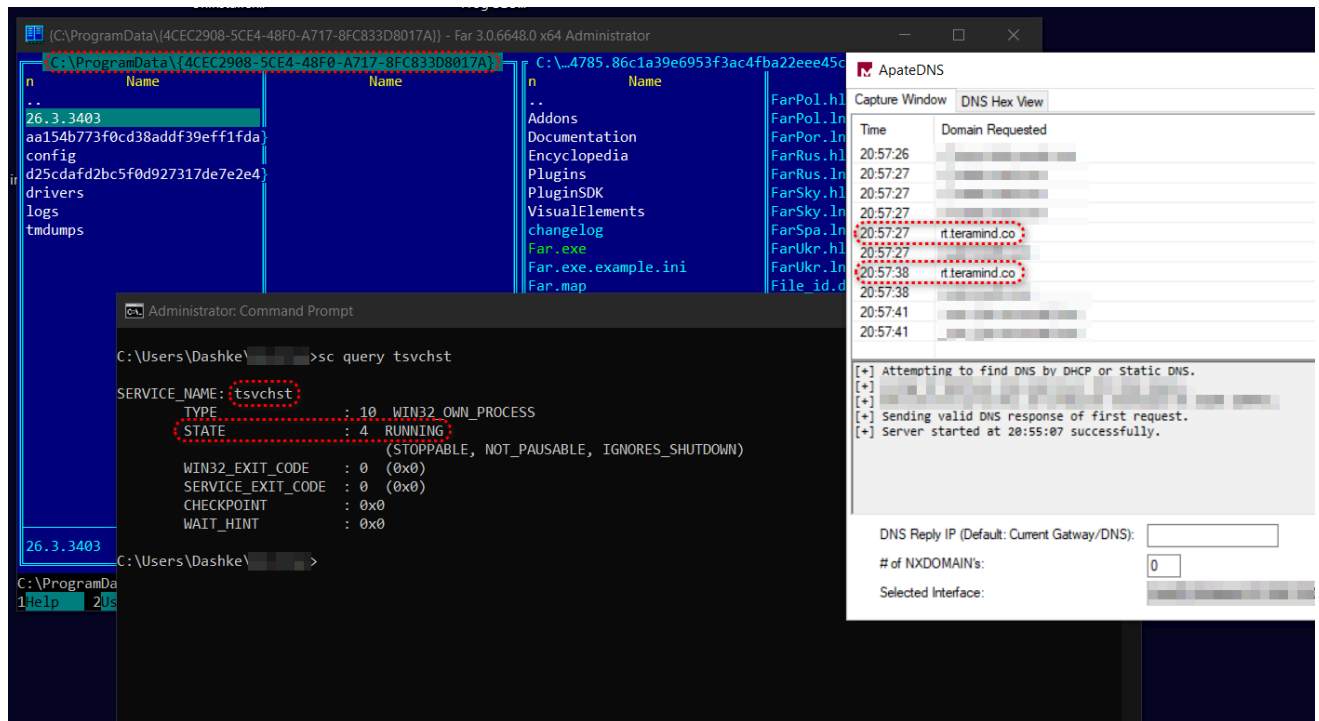
The specified service does not exist as an installed service.

C:\Users\>
```

Before install. No Teramind service.



Before install. No Teramind folder.



After install.