# TA571 Threat Actor Delivers IcedID Malware | Proofpoint US

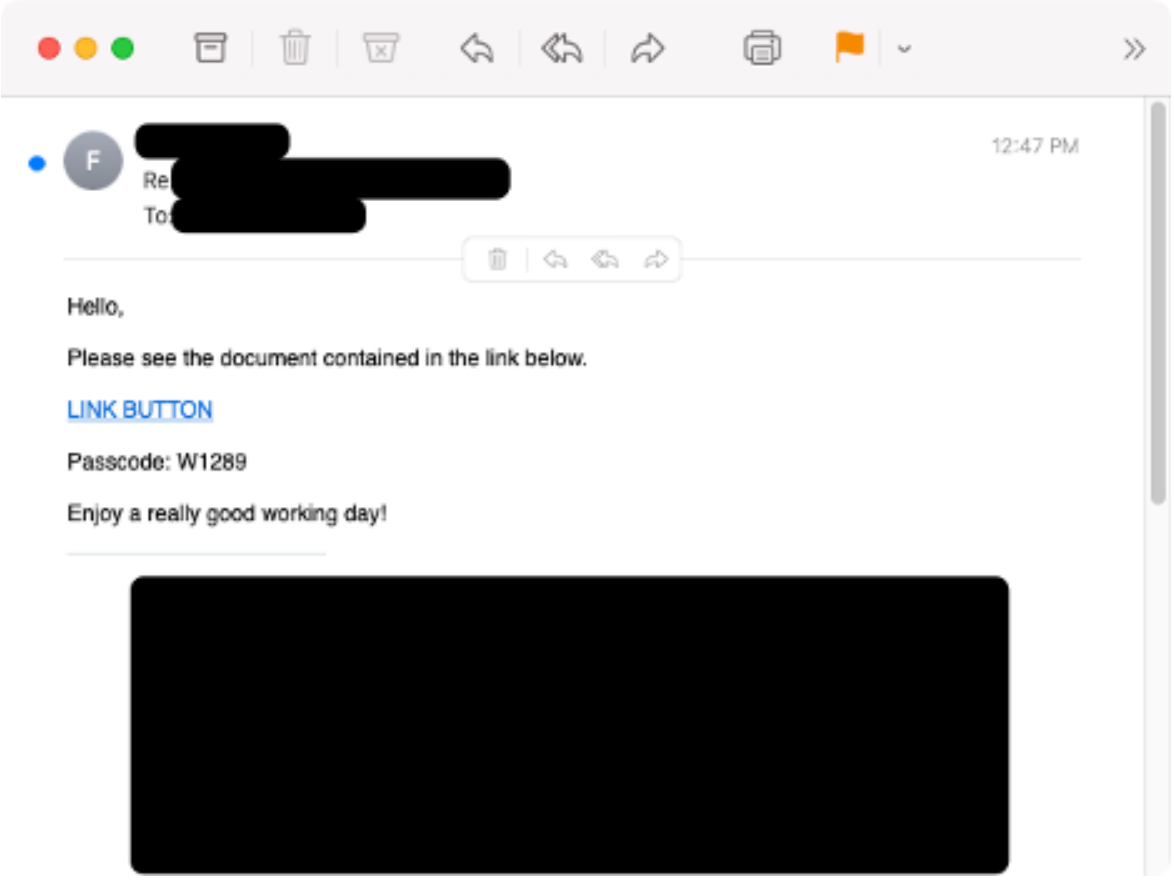
By October 30, 2023 Axel F and Selena Larson

Published: 2023-10-30 · Archived: 2026-04-05 18:57:25 UTC

## What happened

Proofpoint researchers identified TA571 delivering the Forked variant of IcedID in two campaigns on 11 and 18 October 2023. Both campaigns included over 6,000 messages, each impacting over 1,200 customers in a variety of industries globally.

Emails in the campaigns purported to be replies to existing threads. This is known as thread hijacking. The emails contained 404 TDS URLs linking to the download of a password-protected zip archive with the password listed in the email. The attack chain included a series of checks to validate the recipient before delivering the zip archive.




*TA571 lure used in an IcedID campaign on 11 October 2023.*

The zip file contained a VBS script and a benign text file. The VBS script, if double clicked by the user, ran an embedded IcedID Forked loader with regsvr32. The loader in turn downloaded the IcedID bot.

The use of the Forked IcedID variant is unusual, as it has only been observed in a small number of campaigns. Proofpoint first identified this variant in February 2023. A key difference between the original IcedID variant and the Forked variant was the removal of banking functionality. At the time, Proofpoint assessed actors were using the modified

variants to pivot the malware away from typical banking trojan and banking fraud activity to focus on payload delivery, which likely includes prioritizing ransomware delivery.

TA571 regularly uses 404 TDS in campaigns to deliver malware, including AsyncRAT, NetSupport, and DarkGate. Proofpoint researchers have been tracking 404 TDS since at least September of 2022, and it is used by a number of threat actors. A traffic distribution system (TDS) is an application used to route web traffic through operator-controlled servers. They can be used by threat actors to redirect traffic to malware downloads and use IP filtering to determine whether to deliver a payload or redirect to a credential harvesting website. Proofpoint assesses 404 TDS is likely shared or sold to other actors due to its involvement in a variety of unrelated phishing and malware campaigns.

## Attribution

TA571 is a spam distributor, and this actor sends high volume spam email campaigns to deliver and install a variety malware for their cybercriminal customers, depending on the subsequent operator's objectives. Proofpoint assesses with high confidence that TA571 infections can lead to ransomware.

## Why it matters

TA571's delivery of the Forked IcedID variant is unique as Proofpoint does not often observe it in threat data. Additionally, Proofpoint considers TA571 to be a sophisticated cybercriminal threat actor. Its attack chain includes unique filtering using intermediary "gates" for traffic to pass through. These gates, which are intermediary URLs, will filter traffic based on IP and geo-fencing. TA571 may have as many as two gates per campaign. This is to ensure only specifically targeted users receive the malware, and to bypass automated sandboxing or researcher activity.

## Emerging Threats signatures

2853110 - ETPRO EXPLOIT_KIT 404 TDS Redirect

2032086 - ET TROJAN Win32/IcedID Request Cookie

2847335 - ETPRO TROJAN Win32/IcedID Stage2 Checkin

2032086 - ET TROJAN Win32/IcedID Request Cookie

## Indicators of compromise

| Indicator | Description | First Observed |
|---|---|---|
| 6c6a68da31204cfe93ee86cd85cf668a20259220ad44341b3915396e263e4f86 | SHA256 Payload Example<br><br>HLSV1249_5361051.zip | 11 October 2023 |
| 0a61d734db49fdf92f018532b2d5e512e90ae0b1657c277634aa06e7b71833c4 | SHA256 Payload Example | 11 October |

| | | |
|---|---|---|
| | OFFER[2023.10.11_08-07].vbs | 2023 |
| 57897b750473215a2ea6a15070ad5334465019ea4847a2c3c92dae8e5845b2c4 | SHA256 Payload Example<br><br>ReadMe[2023.10.11_08-07].txt | 11 October 2023 |
| a12045a6177dd32af8b39dea93fa92962ff1716381d0d137dede1fc75ecd2c0c | SHA256<br><br>IcedID Forked Loader<br><br>0050-1.dll | 11 October 2023 |
| 5d5bc4f497406b59369901b9a79e1e9d1e0a690c0b2e803f4fbfcb391bcfeef1 | SHA256<br><br>IcedID<br><br>Useqacaw.dll | 11 October 2023 |
| hxxps://gestionhqse[.]com/qd | 404 TDS Redirected to Gate #1 | 11 October 2023 |
| hxxps://gilaniultrasound[.]com/wfhfxtktx | Gate #1 redirected to Gates #2 (which then leads to download of a Zip) | 11 October 2023 |
| modalefastnow[.]com | IcedID Forked Loader C2 | 11 October 2023 |
| hxxps://jerryposter[.]com/news/1/255/0 | IcedID Bot C2 Communication Observed (Example) | 11 October 2023 |
| opuscards[.]ca | 404 TDS URL Domain | 11 October |

| | | |
|---|---|---|
| | | 2023 |
| cornerbakeryrestaurant.net | 404 TDS URL Domain | 11 October 2023 |
| karo[.]ca | 404 TDS URL Domain | 11 October 2023 |
| ekaraj[.]ir | 404 TDS URL Domain | 11 October 2023 |
| roatancruiseship[.]com | 404 TDS URL Domain | 11 October 2023 |
| jonanna[.]com | 404 TDS URL Domain | 11 October 2023 |
| liguys[.]com | 404 TDS URL Domain | 11 October 2023 |
| naughtycharlotte[.]com | 404 TDS URL Domain | 11 October 2023 |
| compacta[.]com | 404 TDS URL Domain | 11 October 2023 |

| | | |
|---|---|---|
| brandworks[.]com[.]au | 404 TDS URL Domain | 11 October 2023 |

## Subscribe to the Proofpoint Blog

---

Source: https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader