GOLDEN CHICKENS: Evolution of the MaaS

By Allison Ebel

Published: 2020-07-20 · Archived: 2026-04-05 16:36:27 UTC

Latest Golden Chickens MaaS Tools Updates and Observed Attacks

Executive Summary

- Throughout March and April, QuoIntelligence observed four attacks utilizing various tools from the Golden Chickens (GC) Malware-as-a-Service (MaaS) portfolio. We are now declassifying our findings for the general public.
- Overall, we attribute the separately conducted campaigns with confidence varying from low to moderate to GC05, GC06.tmp, and **FIN6**.
- During our analysis of the attacks, we uncovered the GC MaaS Operator, **Badbullzvenom**, created new variants of three existing tools in the service portfolio with notable code updates to TerraLoader, VenomLNK, and more_eggs.
- TerraLoader. A multipurpose loader written in PureBasic.
    - Updates – the new variant uses different string de/obfuscation, brute-forcing implementation, and anti-analysis techniques.
- VenomLNK. A Windows shortcut file likely generated by a newer version of the VenomKit building kit.
    - Updates – the new variant uses a new volume serial number, an evolved execution scheme, and only the local path to the Windows command prompt.
- more_eggs. A backdoor malware written in JavaScript (JS)
    - Updates – the new variant includes a minimum delay before executing or retrying an action, and cleans up memory after using it.
- In April, we detected two new attacks sharing similar characteristics of previously observed attack activity attributed to FIN6 – a financially-motivated threat actor group. Based on our analysis of the new campaigns, we assess attribution to FIN6 with low to moderate confidence.
- The uncovered campaigns highlight that Badbullzvenom is still highly active in the business of its MaaS, and that FIN6 is still one of Badbullzvenom's recurrent customers.

Introduction

Throughout March and April, QuoIntelligence observed four attacks (i.e. *sightings*) utilizing various tools from the Golden Chickens (GC) Malware-as-a-Service (MaaS) portfolio – we are now declassifying our findings, after first notifying clients on 22 May . Further, during our analysis of the sightings, we confirmed the GC MaaS Operator, Badbullzvenom, released improved variants with code updates to three tools in the service portfolio:

- **TerraLoader.** A multipurpose loader written in PureBasic. TerraLoader is a flagship product of GC MaaS service portfolio.

- **more_eggs.** A backdoor malware capable of beaconing to a fixed command and control (C2) server and executing additional payloads downloaded from an external Web resource. The backdoor is written in JavaScript (JS).
- **VenomLNK.** A Windows shortcut file likely generated by a newer version of the VenomKit building kit.

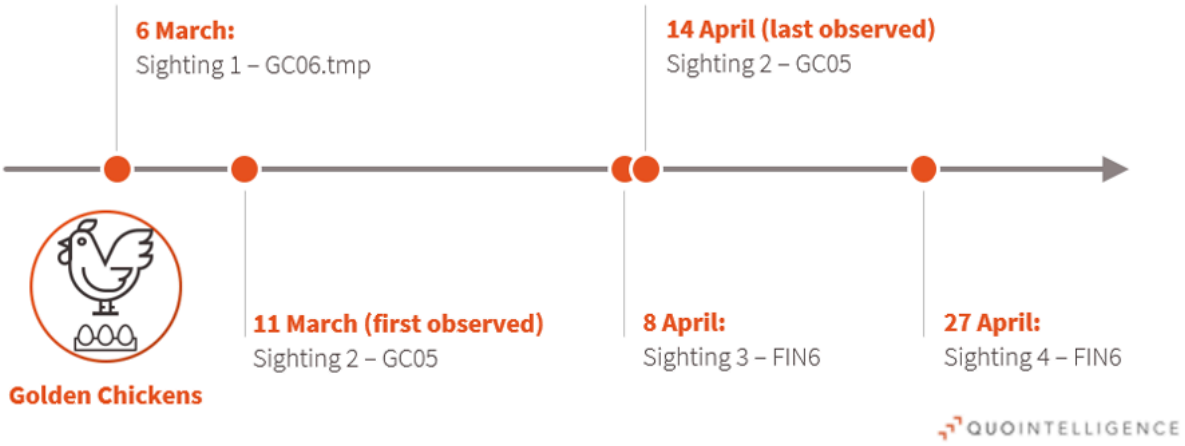

Figure 1: Timeline of sightings using various GC MaaS Tools during March & April 2020

The Golden Chickens

Since 2018, QuoItelligence has tracked the evolution of the GC MaaS, the activities of its Operator *Badbullzvenom*, as well as the different threat actors using the MaaS – including top-tier, financially-motivated threat actors such as FIN6 and the Cobalt Group. The GC MaaS remains as a preferred service provider for top-tier e-crime threat actor groups due to Badbullzvenom/the Operator's consistent updates and improvements of tools and its ability to maintain underlying network infrastructure. Although GC tools have primarily been used to compromise organizations in the retail and financial sector, one notable outlier includes a potentially targeted attack against a chemical company.

Technical Analysis

Latest Sightings Related to GC MaaS

Throughout March and April, QuoIntelligence has observed four sightings utilizing various tools from the GC MaaS portfolio. Overall, we attribute the separately conducted campaigns with confidence varying from low to moderate to GC05, GC06.tmp, and FIN6. To clarify GC05 and GC06.tmp, we categorize the multiple GC MaaS clients as GCxx based on their overall motives, means, and opportunities. Additionally, we append .tmp to the GC categorization to represent that we are investigating their exact singular attribution.

Sighting 1 GC06.tmp: Excel 4.0 Macro Sheet Used to Deliver GC MaaS Infection Chain

On 6 March, QuoIntelligence detected a new malicious Microsoft Excel document leading to the download of GC MaaS tools. Following our preliminary analysis, we confirmed the malicious document (maldoc) leads to an

attack kill-chain which entirely relies on GC MaaS tools. Based on our telemetry, we assess with moderate to high confidence this targeted attack was against a large German chemical company.

Upon further analysis, we do not attribute the maldoc to the GC MaaS toolset as it is clear the employed technique is a well-documented abuse of a legacy functionality in Microsoft Office known as Excel 4.0 Macro Sheet. The Macro Sheet was obviously adapted to use the downloaded *.ocx* file – the typical file extension of TerraLoader.

```
3:     43586 'Workbook'
            Plugin: BIFF plugin
              0085     21 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, very hidden
```

Figure 2: Output of tools to parse Microsoft document OLE objects

The Macro Sheet contains formulas in cells to perform actions, including *Run on open* (Auto_Open) and execute shell commands and web requests. Once the document is opened, the Macro Sheet's code is triggered, and it initiates the infection routine to download and execute the next stage payload which is a TerraLoader variant.

The attack chain consists of multiple known GC tools which are:

- **TerraLoader**. A multipurpose loader, written in PureBasic. TerraLoader is essentially a flagship product of GC MaaS service portfolio.
- **lite_more_eggs**. A lite version of more_eggs used as a loader, written in JavaScript.
- **more_eggs.** A backdoor malware capable of beaconing to a fixed command and control (C2) server and executing additional payloads downloaded from an external Web resource. The backdoor is written in JavaScript.
- **TerraStealer**. An information stealer (also known as SONE, StealerOne) written in PureBasic.

Figure 3 – Kill-Chain of Sighting 1

Consistent with our earlier observation, attacks relying on lite_more_eggs result in a variant of more_eggs dropped on the victim's the system. In this case, neither TerraLoader nor more_eggs were digitally signed, and the observed more_eggs variant version is the older "2.0b".

```
var BV = "2.0b";
var Gate = "https://origin.cdn77.kz/api/json";
var js_gate = "https://origin.cdn77.kz/api/json.txt";
var hit_each = 10;
var error_retry = 2;
var restart_h = 4;
var rcon_max = hit_each * (restart_h * 60) / (hit_each * hit_each);
var Rkey = "qNHGjfkQ1Fuq7vrH";
var rcon_now = 0;
var User = "";
var Build = "";
var gtfo = false;
```

Figure 4 – configuration of more_eggs delivered by the lite_more_eggs sample

We have observed three occurrences involving the same highlighted attack kill-chain of GC attributed tools, resulting specifically in the older "2.0b" variant of more_eggs. Although this activity is not distinct enough, we are temporally attributing these sightings to GC06.tmp.

Sighting 2 – GC05: A New Campaign with Familiar Tactics, Techniques, and Procedures (TTPs)

On 10 April, QuoIntelligence detected a new VenomLNK variant. The VenomLNK file is contained within a Zip archive; both themed as a financial document, and likely delivered to a targeted user as an email attachment or link. While the observed filenames indicate the exploitation of a financial theme, we cannot confirm the victimology at this time.

Name	Type	Size
M&T_Bank_08_04_2020	Shortcut	4 KB
M&T_Bank_08_04_2020	Compressed (zipped) Folder	2 KB

Figure 5 –Financial themed Zip archive and extracted VenomLNK variant

The attack's kill-chain involves an obfuscated JS scriptlet dropping a TerraLoader variant and decoy Microsoft Word document. While the decoy document appears in the screen on the user's system, the TerraLoader is running and dropping a more_eggs variant. Finally, the more_eggs delivers a final payload of the information-stealer tracked by QuoItelligence as TerraStealer, two tools already attributed to the GC MaaS.

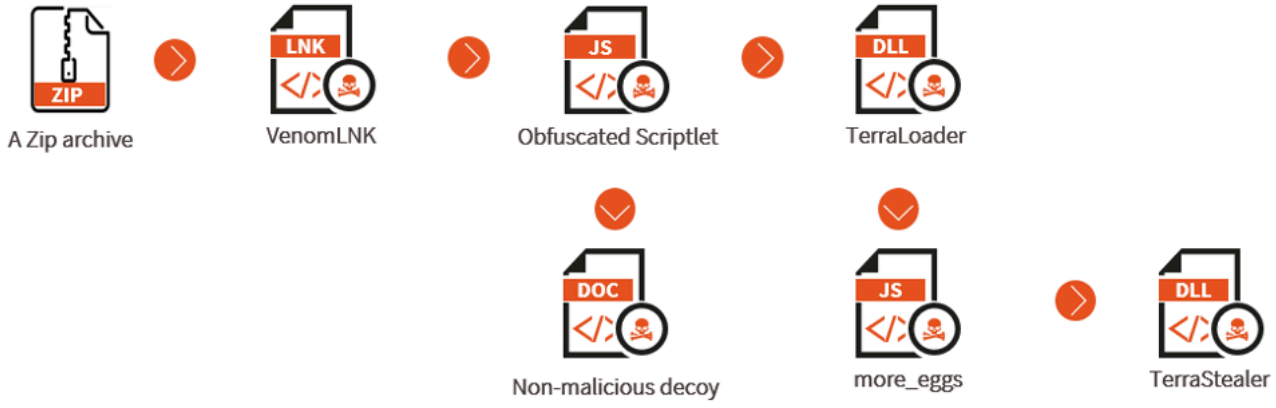

Figure 6 –Sighting 2 – Kill-Chain

Pivoting on our initial sample, we obtained additional VenomLNK files which are all similar except for the C2 URLs and contain slight modifications from earlier known variants. Further, we determined that our initial sighting was part of a campaign which likely began on 11 March through 14 April. Based on our observations, the campaign aligns with activities and TTPs we previously attributed to GC05; a threat actor we have tracked since September 2019 who leverages the GC MaaS extensively, especially VenomLNK, more_eggs, and TerraStealer.

FIN6: A Familiar and Returning GC MaaS Customer

In April, we processed two sightings of attacks sharing similar characteristics of previously observed activity attributed to the financially-motivated threat actor group known as FIN6. Since 2018, QuoIntelligence was able to attribute with high confidence the use of GC MaaS tools such as more_eggs, TerraLoader, and TerraTV to FIN6 campaigns. Based on our analysis of the new campaigns, it is evident that FIN6 remains a customer of the GC MaaS. Although FIN6 is known to primarily target the financial and retail sectors, we cannot confirm the victimology of these campaigns at this time.

Sighting 3 – ‘Fake Job’ Spearphishing Delivering VenomLNK

On 8 April, we became aware of a new variant of VenomLNK and its original Zip archive. Both filenames aligned with the theme for the known fake job campaign attributed to FIN6, by both researchers at IBM-X Force and Proofpoint, conducted since at least the middle of 2018. The original Zip archive, named *assistant_buyer.zip*, contained the VenomLNK variant named *Job Offering.lnk*. During analysis, the C2 URL was not serving the next stage payload of the kill-chain. Based on our telemtry, the first alleged execution of the attack occurred on 7 and 8 April, suggesting the sighting was likely part of new activity. However, due to lack of further pieces of evidence on the kill-chain, we currently attribute the sighting to FIN6 with low confidence.

Sighting 4 – TerraLoader Directly Injecting Metasploit’s Meterpreter

On 27 April, QuoIntelligence detected a new variant of TerraLoader having a modified payload delivery mechanism which decrypts the included payload (shellcode) and loads it directly into memory. During analysis, we identified two DLLs in memory – one very likely OpenSSL and the other highly likely Meterpreter, which is a full-featured backdoor. The Meterpreter uses HTTPS to callback to an attacker-controlled asset. Further aligning with the detection timeframe, the TerraLoader variant included a kill-switch of year 2020 – a feature that disallows the execution of a malware sample beyond a hardcoded date, time, or year value. As we have already noted, the kill-switch is a common feature of the Operator’s arsenal aimed at enforcing his own *licensing* with his customers.

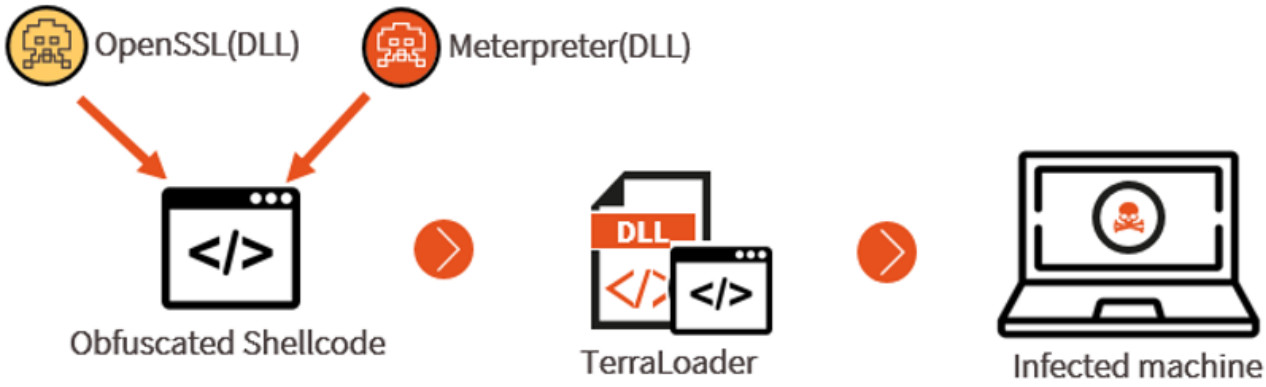

Figure 7 –Sighting 4 – TerraLoader direct memory injection

Previously in April 2019, we identified FIN6 as the only GC MaaS customer using a variation of the approach described above. Further to the attribution of the April 2019 case, the involved C2 domain, registered in January 2019, is also a domain we observed in attack activity we already attributed earlier, with high confidence to FIN6. In April 2020, we detected another attack with the same approach from 2019. The activity of all three cases are described as follows:

- **April 2019:** Involves initially generating an apparent stager executable, likely with Metasploit tools, for use by TerraLoader to inject into another process and download Meterpreter.
- **April 2020:** Similarly, this activity involves a generated stager executable used by TerraLoader to inject into another process (wermgr.exe) and download the next stage payload, which is a Meterpreter.

Figure 8 – April 2019 & 2020 – TerraLoader process injection

- **April 2020:** Differently, this activity involves TerraLoader loading obfuscated shellcode directly into the memory of itself, already including the Meterpreter payload, and executing it. Both TerraLoader variants detected in April included a kill-switch of year 2020, indicating recent or ongoing activity.

A reasonable hypothesis for the new approach of using obfuscated shellcode, instead of injecting into another process, could likely be to increase stealth and evade detection by security solutions such as Anti-Virus. As such, TerraLoader is known to be fully undetectable, so decrypting and executing code within the same memory space will increase the likelihood of being undetected by most Anti-Virus solutions.

GC MaaS Toolset Updates

TerraLoader

The TerraLoader variant observed in Sighting 2, spanning from 11 March to 14 April, contains some notable feature changes, which we previously observed only twice in December 2019. The new variant uses a different string de/obfuscation, brute-forcing implementation, and anti-analysis techniques.

String de/obfuscation

- The latest variants store strings RC4 (a stream cipher) encrypted as raw bytes and seems to entirely use the same stream cipher for decryption. In early variants, deobfuscation was achieved through XOR-decryption on strings stored as hex streams.

Brute-forcing Implementation

- In new variants, only the first half of the string encryption key is stored in the malware. The second half of the string encryption key is brute-forced – calculated at runtime by counting up from zero until it is found. As soon as the bruteforcing is able to decrypt a specific ciphertext to a specific plaintext, which are both stored in the malware, the key is successfully found.
- From an analysis perspective, earlier variants used XOR obfuscation which can be bypassed quickly, however, the latest variants use RC4 so the same bruteforce search for the actual key needs to be performed to successfully decrypt all strings.

Anti-analysis Techniques

- Checks where in memory *ntdll.dll* (a Microsoft file that contains NT kernel functions) is loaded.
- Checks hash of executable (exe) name against a whitelist (pre-calculated hashes) including *regsvr32.exe*, using ZwQueryInformationProcess.
- Checks hash of loaded DLLs against a blacklist. (pre-calculated hashes)
- Compares hash of Dynamic-link library (DLL) extension, expects *.ocx*, and exe name (expects *regsvr32.exe*) against pre-calculated hash values. To do so, Process Environment Block (PEB) is used to know where a process exists in memory.
- Uses *NtQueryInformationProcess* to check if a debugger is present on the system.
- Dynamic function address resolution continues to perform lookup by hash (CRC32), but additionally uses an XOR value to make direct hash value comparison impractical.

more_eggs

On 29 April, we detected a new variant of TerraLoader which contains a msxml.exe (a Windows command line utility that invokes the Microsoft XML Parser for transformation) and new more_eggs version, “6.6b”, embedded in its *.data* section.

```
var BV = "6.6b";
var Gate = "https://time.absolutededs.com/query";
var hit_each = 10;
var error_retry = 2;
var restart_h = 4;
var rcon_max = hit_each * (restart_h * 60) / (hit_each * hit_each);
var Rkey = "StfDoSB7edpTuTST";
var rcon_now = 0;
var gtfo = false;
var selfdel = false;
var table = [];
var Build = "";var PCN = "";var UNM = "";var SYSTEM = 0;var rootK = "HKCU";var workingDir = "";var main_mitm =
"";var xApp = "";var xTmp = "";var PreserveH = "";var xStore = "";
var set = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!#$%&()*+,./:;<=>?@[]^_`{|}~"';
var b64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";
```

Figure 9 – more_eggs configuration of the latest variant

The latest variant of more_eggs is 6.6b, one iteration above the last known version “6.6a”, was observed during the campaign from 11 March through 14 April. Besides the typical customized more_eggs configuration variables (version number *BV*, C2 address *Gate*, and part of the ciphering key used to encrypt C2 communications, *Rkey*), the latest variant contains two notable main code changes:

- Introduces minimum delay before executing or retrying an action.
- Attempts to cleanup memory by assigning empty values to variables after using them. In general, it is not clear how effective this approach is in JavaScript; however, this does at least hinder a JavaScript debugger.

VenomLNK

Sighting 3 utilized an updated variant of VenomLNK as an initial attack vector in a targeted campaign. We have observed VenomLNK used in various campaigns involving different infection chains.

Metadata analysis of the LNK file allows key information to be extracted about the direct link to another file and the execution process. In general, LNK files have a small file size but contain valuable information such as shortcut target file, file location and name, and the program that opens the target file.

The VenomLNK files obtained from the campaign were all similar and contain slight modifications from earlier known samples which are:

- Uses a new volume serial number: 0xcae82342. The Serial Number is dependent of the hard drive the LNK file was created on.
- Evolution of the execution scheme: /v /c set “z1=times”. The command line input places the first variable in double quotes, which can often break detection-based security solutions.
- Only uses the Local Path (C:\Windows\System32\cmd.exe) to the Windows command prompt, dissimilar from earlier variant which also included the Relative Path (……..\Windows\System32\cmd.exe)

Conclusion

The GC MaaS continues to offer a versatile catalog of attack tools and underlying C2 infrastructure to fulfill the entire attack kill-chain. The Operator continues to regularly evolve and improve the toolset within his service portfolio, and adapt new techniques over time, such as in the campaign leveraging TerraLoader to directly inject a

payload into memory. We expect the MaaS will continue to prove its success and profitability, through at least its returning customers and the known top-tier e-crime threat actors who have utilized the available services.
