GOLDEN CHICKENS: Evolution of the MaaS

quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/

July 20, 2020

Latest Golden Chickens MaaS Tools Updates and Observed Attacks

Executive Summary

- Throughout March and April, QuoIntelligence (QuoINT) 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 A Windows shortcut file likely generated by a newer version of the VenomKit building kit.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 (QuoINT) 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.

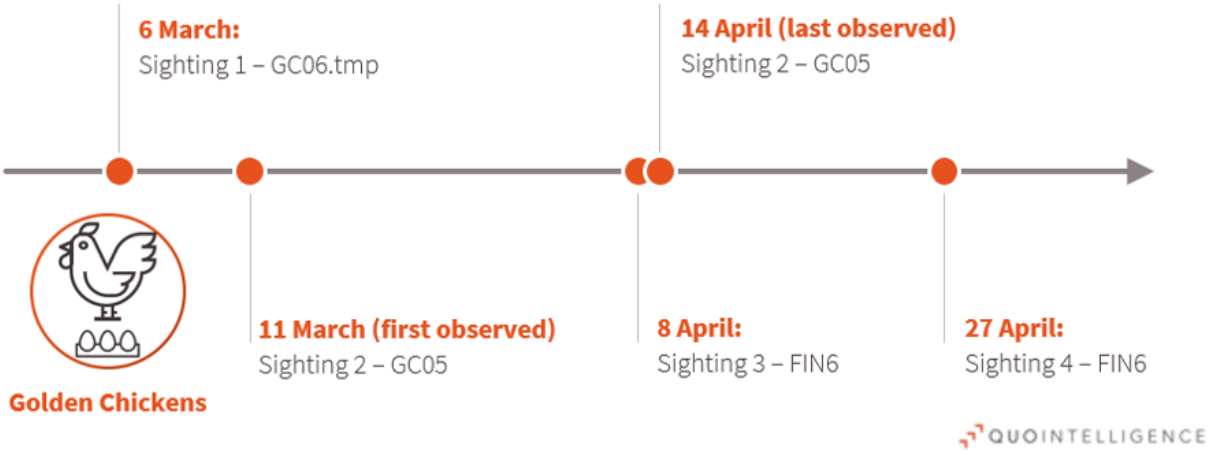


Figure 1: Timeline of sightings using various GC MaaS Tools during March & April 2020

The Golden Chickens

Since 2018, QuoINT 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, QuoINT 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, QuoINT 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.

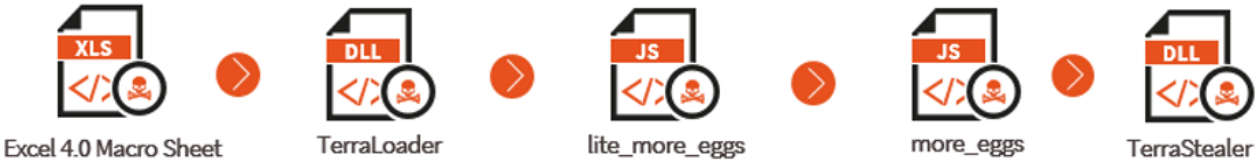


Figure 3 – Kill-Chain of Sighting 1

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".

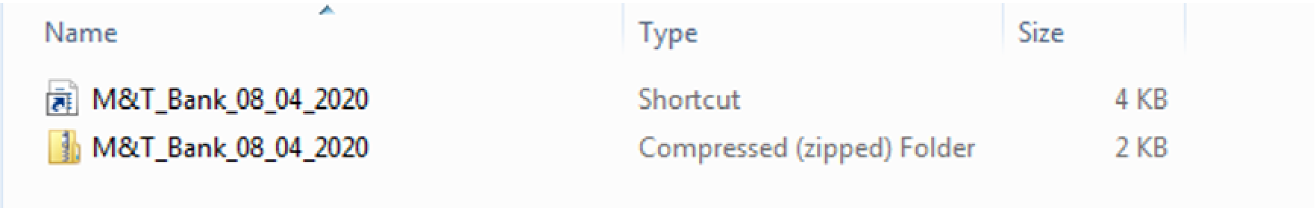
```
var BV = "2.0b";
var Gate = "https://origin.cdn77.kz/api/json";
var js_gate = "https://origin.cdn77.kz/api/json.txt";
var hit_each = 10;
var error_retry = 2;
var restart_h = 4;
var rcon_max = hit_each * (restart_h * 60) / (hit_each * hit_each);
var Rkey = "qNHGjfkQ1Fuq7vrH";
var rcon_now = 0;
var 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, QuoINT 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 QuoINT as TerraStealer, two tools already attributed to the GC MaaS.

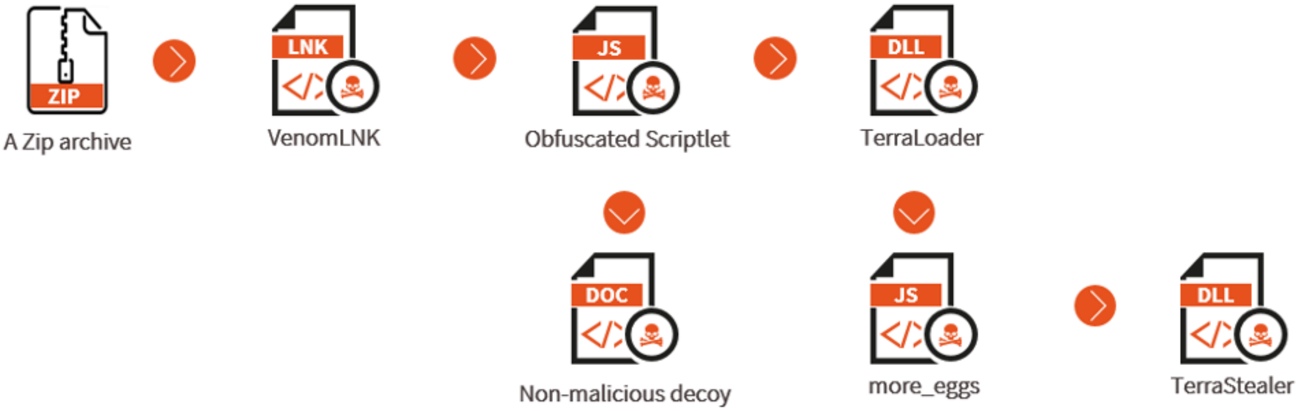


Figure 6 –Sighting 2 – Kill-Chain

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, QuoINT 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, QuoINT 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 which 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.

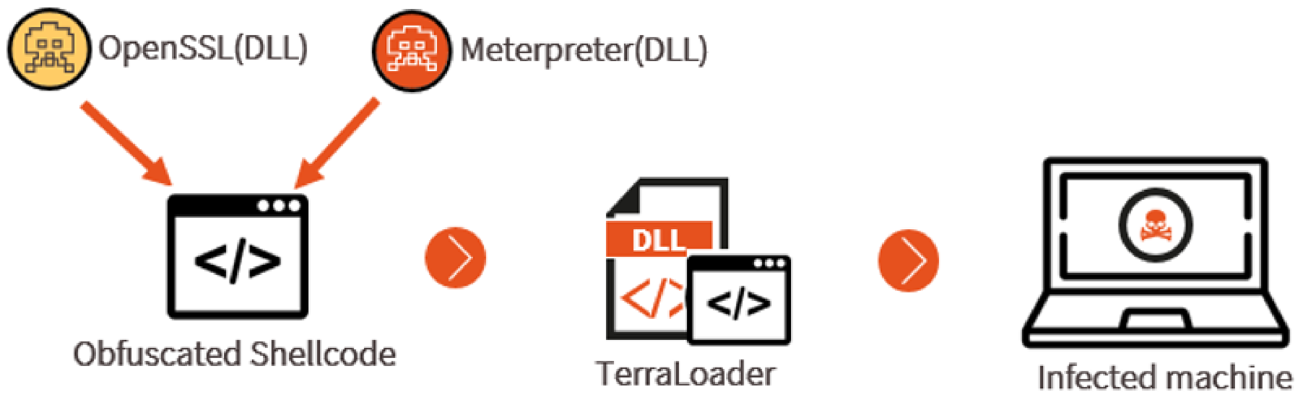


Figure 7 –Sighting 4 – TerraLoader direct memory injection

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.

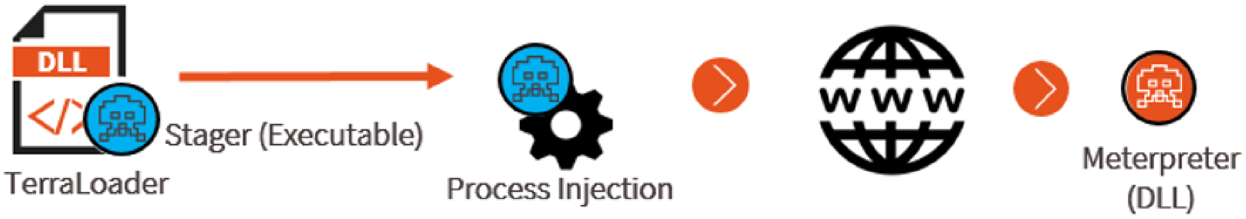


Figure 8 – April 2019 & 2020 – TerraLoader process injection

> **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

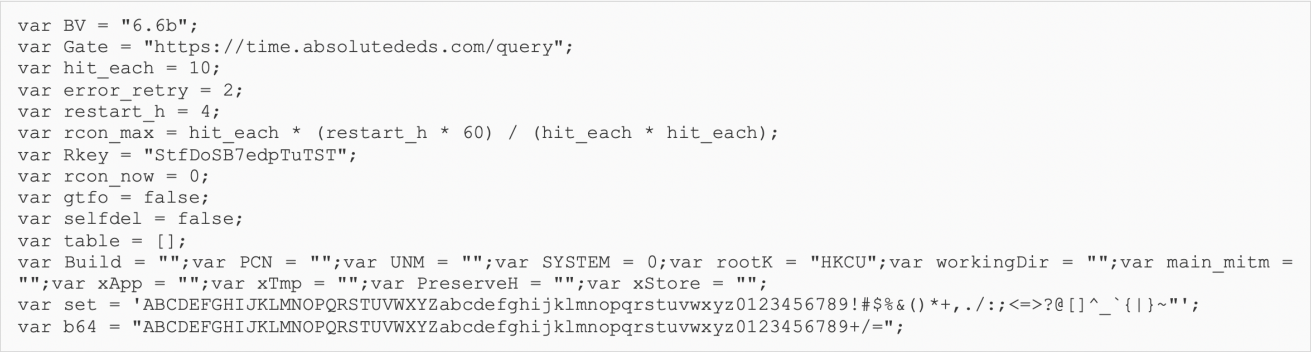
- In new variants, only the first half of the string encryption key is stored in the malware. The second half of the string encryption key is brute-forced – calculated at runtime by counting up from zero until it is found. As soon as the bruteforcing is able to decrypt a specific ciphertext to a specific 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.

Do you want to know more about Golden Chickens MaaS through exclusive and unpublished intelligence? Have information to share about about our findings?

Get in touch!

Join Our Newsletter!

Subscribe to our newsletter to receive Weekly Intelligence Summaries, cyber news, and exciting updates!

Only valid business emails will be approved.

Appendix I

Indicators of Compromise

Sighting 1

```
2ec3639c055d1951eb0149e3bc903bc127a4ae6f9e31cf6761c0df847f764cf7
7122cf59f8a59f9a44f20fd4c83451c5c4313e0021d3f1ba9c2b1a4f39801db1
0aee265a022ee84e9c8b653e960559c9761a7362e1c345019a552188114b7e80
hxxps://origin[.]cdn77[.]kz/api/json
hxxps://origin[.]cdn77[.]kz/api/json[.]txt
hxxp://download[.]sabaloo[.]com/css/libatk-1[.]0-0[.]dat
5[.]255[.]96[.]203
```

Sighting 2

```
19c2f16334fe30296299ca92f716c1e074c16e6a7b9ee6a74bedec7ccfdcd6f0
4e562916eb56c7a2c9336c82e49c3a1285ccd95a74a5d1ab881e1d3dd8fba8e9
60914099428861a8aeeb361359035e11feb464fa291772eb0b45805802d96d7d
686b279d282c9794dcecbd8b6164ec8b12f6b4617df0eb0fa72149cedd215ac8
831537fff141897aee0fea5f03f4ffa7fb7a3598568da58dc27ddd0aa8473809
b33ca728423df9873bff43fea7c02755a1efeac8e1d013653a6ab706d5d09af5
b479f1beb42a8784862381a38b023ce009acfac79770b3ad7cc2245a56320bb8
b7431497f682697968ddcbdafc510350aaf04697bda1e0bc638d89a972e9461d
b95637122a540083d7a5a7063a4b97ad7fdd0bb22ddb301ed3859a394b35b3a0
Citibank_statement_08_03_2020.lnk
Citibank_statement_08_03_2020.Zip
fbe753e22f80486e80dc764cfc60a87ed08548f76cefbfae0c38b19f36552fa0
fcffcc8511483f3dbeb8e2eaa3184a866cfadc11a98f05d5f97f800e970b4aba
ff50be3fe471cbda1d2ce980f82659efe3a07d8266b93474bd8b0aa3ae372988
hxxp://json[.]digebuy[.]com/demo[.]txt
hxxp://json[.]digebuy[.]com/english[.]txt
hxxp://web[.]rossnnam[.]com/readme[.]txt
doaglas[.]com
162[.]255[.]119[.]21
office[.]fielnnam[.]com
91[.]92[.]109[.]59
ScottBank_01_04_2020.lnk
ScottBank_01_04_2020.Zip
ScottBank_05_04_2020.lnk
ScottBank_05_04_2020.Zip
ScottBank_statem_23.04.2020.lnk
ScottBank_statem_23.04.2020.Zip
ScottBank_statem_23.04.2020.Zip
M&T_Bank_08_04_2020.Zip
28bdd1dbd4a15f6b5142bb3170de6e69320c3c96ba74a33198b0559a896d472a
a7d4402917a32299b74d707efd81d7e1f3692a3871f4491691a45fc5e69ef19d
M&T_Bank_08_04_2020.lnk
M&T_Bank_08_04_2020.Zip
931ff382b786e15b4bceaebd40ec61baa096a2f4ac873c28c50667ef2be6755a
af0e95119ad9a56415e77ae4b6bab2081dccb1516f6f2c5dfd357c29f2e3259d
ScottBank_05_04_2020.lnk
web[.]rossnnam[.]com/readme[.]txt
85[.]204[.]116[.]135
json[.]digebuy[.]com/english[.]txt
json[.]digebuy[.]com/demo[.]txt
192[.]64[.]119[.]132
hxxps://office[.]fielnnam[.]com/update/check
hxxps://maps[.]doaglas[.]com/update/check
```

Sighting 3

```
eaf88363657b4989ceb9c4d7cde824cf62e10c2d6d05bfd80277464d4282da82
f0bdf8e640ed3e5441675ab57e09f680ea41edd95c3cf87b82d742bead29ff36
hxxp://18[.]221[.]151[.]210/21[.]odt
```

Sighting 4

```
30cdbb1ff2e85502bd81bfe8547c95f735a120aa7547d42867f7bb5e8b91c405
xo[.]mikeplein[.]com
hxxps://xo[.]mikeplein[.]com:443/9XpHPVaMe23UyNXJim_0kwxeHtbpYrZo13FcMH30leL6Qcs0J
8h6tklBPDDnPY1x66UU9L0FPPcOUStSycnI1UvIV/
193[.]42[.]111[.]180
1142282962fd60d51a6ab75a83696d6121442ebed1b24590b95409d6cf98c7ba
255778a7f2ae8818b8a94eedb2eb1760843e6d2c9130a0a48d6995d1e66303ec
secure[.]jobscur[.]com
```

Updated Tools

TerraLoader

38f3a52e1ebd93db75f0fb6ce6172565cc0f27f0f86f32f470fa7a9c8de9f094
1142282962fd60d51a6ab75a83696d6121442ebed1b24590b95409d6cf98c7ba

more_eggs

3d9baa8ffd350fb9d8ad7c2591c321a402b8e8f2e083dc83c941e1c9bb022549

VenomLNK

19c2f16334fe30296299ca92f716c1e074c16e6a7b9ee6a74bedec7ccfdcd6f0

MITRE ATT&CK

Toolkit	Tactic & Technique	Recommended Course of Action
TerraLoader	**Execution** T1117 Regsvr32 **Defense Evasion** T1116 Code Signing T1027 Obfuscated Files or Information T1140 Deobfuscate/Decode Files or Information	• Anti-Virus software and advanced End-Point solution can significantly reduce the impact, and lessen the likelihood of successful execution, of TerraLoader. • Often, TerraLoader is digitally signed. Enforce signature validation via Domain Group Policy. • Log *cmd.exe* and *regsvr.exe* usage via Domain Group Policy.

More_eggs	**Execution** T1053 Scheduled Task **Defense Evasion** T1027 Obfuscated Files or Information T1140 Deobfuscate/Decode Files or Information **Discovery** T1082 System Information Discovery T1016 System Network Configuration Discovery T1033 System Owner/User Discovery **Lateral Movement** T1105 Remote File Copy **Command and Control** T1043 Commonly Used Port T1071 Standard Application Layer Protocol T1032 Standard Cryptographic Protocol T1041 Exfiltration Over Command and Control Channel	• Perform HTTPS traffic inspection. • Log *exe* and *regsvr.exe* usage via Domain Group Policy. • Endpoint solutions capable of, or configurable for, detecting the combined use of msxsl.exe and Windows Management Instrumentation (WMI).

VenomLNK	**Execution** T1204 User Execution T1059 Command-Line Interface T1191 CMSTP **Lateral Movement** T1105 Remote File Copy **Command and Control** T1043 Commonly Used Port T1071 Standard Application Layer Protocol	Log *exe* and *regsvr.exe* usage via Domain Group Policy.

Blog updated on 21 July to fix error in Sighting 2 and Sighting 3 IOC order.

Want to learn more?
Click here to listen to the Podcast “What came first, the Golden Chickens or more_eggs?” made in collaboration with The CyberWire.

Join Our Newsletter!

Subscribe to our newsletter to receive Weekly Intelligence Summaries, cyber news, and exciting updates!

Only valid business emails will be approved.