as-a-Service (MaaS) Provider and Two New Threat Actors Using It

QuoScient GmbH Follow
Nov 29 · 12 min read

Executive Summary

Over the last few years, QuoScient's Intelligence Operations Team (QuoINT) has tracked activities attributed to the Cobalt group, and observed their notable evolution and continuously improving Tactics, Techniques, and Procedures (TTPs).

Since September 2018, we have identified multiple attacks that share similar TTPs used by Cobalt during a specific timeframe but exhibit enough differences to attribute them to separate threat actors. This blog post provides an overview on a specific Malware-as-a-Service (MaaS) used within the e-Crime threat actor landscape. It also provides details on two different threat actors using the MaaS that fall under the umbrella of a family we dubbed *Golden Chickens*: GC01 and GC02. The success of GC operations heavily relies on a specific MaaS sold in underground forums, which provides customers with the malwares and the infrastructure they need for targeted attacks. The service owner provides the MaaS through the use of the following toolkits: Venom and Taurus building kits for crafting documents used to deliver the attack, and the more_eggs (aka Terra Loader, SpicyOmelette) backdoor for taking full control of the infected computer.

Between November 2017 and July 2018, we attributed to GC02 five spear phishing waves which indiscriminately targeted companies and organizations in at least India and the United States. As a result of using the same MaaS provider, GC02 and Cobalt group's TTPs and infrastructure strongly overlapped in May 2018, making it hard at first glance to differentiate the two threat actors.

Between August and October 2018, we attributed to GC01 nine spear phishing waves targeting multiple companies and organizations operating in the financial industry. Throughout the campaign, we observed the installation of multiple Remote Access Tool (RAT) variations as the result of a successfully compromised victim machine.

By highlighting the multi-layer infrastructure adopted by Cobalt and Golden Chickens, as well as the multi-client business model of the MaaS behind it, we emphasize the difficulty of performing reliable attribution for cyberattacks, and the high uncertainty that analysts are confronted with during the process. To note, other researchers reported the same Indicators of Compromise (IoC) and C2 infrastructure covered in this blog post. We hope that our attribution will clarify the current threat landscape and make the covered threat actor profiles more accurate.

The following blog post is a preview of the Intelligence Assessment we will disseminate to our clients, partners, and vetted requesters.

. . .

Introduction

Cyber attribution is becoming increasingly challenging as threat actors frequently use false flag techniques and shared infrastructure to increase the resiliency of their operations against takedowns and law enforcement investigations. Especially for e-Crime actors, it is a common practice to rent the same bulletproof infrastructure or botnet used by other e-Crime groups, resulting in the increased likelihood for an overlap of C2 servers. In the last years, we have noted a tendency of threat actors outsourcing even more parts of the kill-chain to third parties by using/offering MaaS solutions. Figure 1 shows an example of such a network where multiple stakeholders are involved.

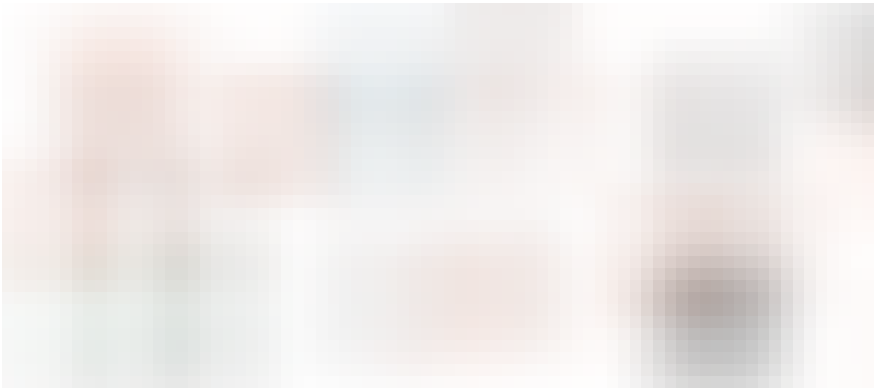

Figure 1—Example of attribution complexity

A threat actor can buy several malware from multiple developers, rent the C2 infrastructure from various providers, and deliver the attack vector to victims from yet another provider. This compartmentalized

business relationship guarantees the threat actor an elevated level of privacy and deniability since the involved stakeholders rarely know the full scale of the operation. On the other hand, those providers offering MaaS solutions simplify the entire process through *One Stop Shop* solutions, where one single entity sells and rents both the malware and the infrastructure needed for an attack.

When profiling e-Crime threat actors, we always deal with the hypothesis that the malware and C2 infrastructure we are analyzing do not belong to the threat actor *per se*, but rather to the used MaaS provider. When we confirm the use of a MaaS, the attribution process focuses on *how* and *when* threat actors used it, and *who* they targeted. By using such an approach, we were able to differentiate past spear phishing campaigns mistakenly attributed to the Cobalt group and characterize two distinct threat actors—GC01 and GC02—and the MaaS used by them to carry out their attacks.

. . .

Golden Chickens' MaaS

From November 2017 to October 2018, we attributed 14 campaigns to the GC threat actors that used a specific MaaS provider (hereinafter "*the Provider*") offered by a known individual (hereinafter *"the Provider Operator"*). The following section explains the operational model of the Provider, and the toolkits used to deliver the requested service to paying customers.

Operational workflow

A typical business case between a threat actor and the Provider is shown in Figure 2 and detailed below.

Figure 2 –The Provider operational workflow

1. Threat actors buy the service offered and then give the Provider Operator the final payload to be executed on the infected machine. Since we have observed the same threat actor using the Provider to different extents, we assess that the Provider Operator's offering is modular.

2. The Provider Operator builds the malicious document (maldoc), the backdoor, and prepares the server infrastructure needed for the execution of the attack. Next, the backdoor is stored on a webserver and the full URL path of it is embedded into the maldoc. Lastly, the C2 panel that the backdoor will beacon to is set up.

3. The Provider returns the maldoc to the threat actor. Although not confirmed, the Provider Operator also likely delivers the access details for the backdoor's C2 web panel.

4. The threat actor disseminates (directly or through the use of a botnet) the maldoc via spear phishing.

5. Once the maldoc is executed on a victim's machine, it will retrieve and execute the backdoor from the hardcoded web location.

6. The backdoor beacons to the hardcoded C2 on a regular basis and executes the commands it receives.

7. Finally, the threat actor (or the Provider) will review the system details of the infected machine reported by the backdoor, and eventually deploy the final payload.

Building Kits Used

The Provider relies on the use of specific malicious artifacts advertised in the underground since 2017. Those artifacts are generated by three building kits and offered to paying customers with the supporting C2 infrastructure.

VenomKit. VenomKit is a tool that threat actors can use to craft malicious Rich Text File (RTF) documents that exploit multiple vulnerabilities, including CVE-2017–11882, CVE-2018–0802, and CVE-2018–8174. Successful exploitation leads to batch and scriptlet files being dropped and executed in order to download the second stage payload from a Web resource. The AV detection rate for RTF documents generated by VenomKit is *moderate* to *high* due to the exploitation of known vulnerabilities.

Taurus Builder Kit. The Taurus Builder Kit generates Microsoft Word documents weaponized with malicious Visual Basic for Application (VBA) macro code. Unlike the malicious RTFs created by VenomKit, the weaponized Word documents require user interaction in order to enable the contained malicious code. On the other hand, documents generated by this kit are more resilient to AV detection due to the use of multiple layers of obfuscation in the VBA code.

Once the VBA code is enabled by the user, documents created by Taurus Builder Kit will download and execute additional malware by using multiple legit Windows tools in order to bypass AppLocker.

More_Eggs Backdoor. More_eggs is a JavaScript (JS) backdoor capable of beaconing to a fixed C2 server and executing additional payloads downloaded from an external Web resource. The backdoor is delivered encrypted inside of another JavaScript, with changing function names, variable names, and encryption keys. Overall, the technique used allows the Provider Operator to guarantee its clients a low AV detection rate. The more_eggs building kit allows customization of its multiple variables, for values such as the C2 server, beaconing and sleeping time, and part of the cryptographic key used for ciphering the C2 communications. Figure 3 shows an example of more_eggs configuration that includes the version number *BV*, C2 address *Gate*, and part of the ciphering key used to encrypt C2 communications, *Rkey*.

Figure 3– Excerpt of more_eggs backdoor configured variables

Threat actors can ask for the customization of the backdoor by requesting the addition of specific variables or entire functionalities. For instance, more_eggs samples attributed to GC02 contained the extra variable *Researchers,* differently from the ones attributed to GC01 or Cobalt Group.

Although not confirmed, it is reasonable to assume that multiple more_eggs used by different threat actors cannot share the same *Gate* value due to the derived complication that would imply for the backend to understand which C2 communications belong to which threat actor using the infrastructure. However, the same C2 server can host multiple gates by using different web pages; hence, multiple threat actors might use distinct gates hosted on the same domain name. Additionally, the *Rkey* variable can be considered as something that is randomly generated every time a new sample is created for a customer (i.e. the relationship between the threat actor and RKey used is likely 1:1). Due to this consideration, we used the Rkey variable while clustering attacks together and attributing them to specific threat actor.

The Provider Operator demonstrates notable efforts in keeping the more_eggs backdoor updated by fixing bugs and adding new features: in the last year alone, we observed six different versions in use, from 2.0 to the most recent version 5.4. Notably, more_eggs backdoors are also capable of automatically updating themselves to the latest version, and even updating the configured *Gate* variable.

. . .

Threat Activity Analysis

The following section highlights the operations and TTPs of three distinct threat actors that have used the Provider in the last year: the Cobalt Group, GC01 and GC02.

Timeline analysis

Figure 4 represents the multiple spear phishing campaigns we have attributed to either Cobalt[1] or the GC family during the last year. While all GC campaigns used the Provider, only those attributed to Cobalt in May, June, and on 2 August used the Provider. QuoINT determines the level of confidence based on both the reliability of the information processed, and the extent of the analytic techniques adopted during the analysis.

Our analysis distinguished three different threat actors based on the following factors:

1. **Targeting.** Which types of companies the threat actors targeted.
2. **Use of the MaaS.** How the Provider was used, to what extent, and the configuration requested.
3. **Final Payload.** What final payload the MaaS delivered.
4. **Time of attack.** When the threat actor used the Provider

Figure 4—Timeline analysis of attacks conducted by GC family and Cobalt Group

In May 2018, Cobalt executed three different spear phishing campaigns in between two GC02 campaigns. The attacks leveraged the same Provider since they used maldocs generated by either VenomKit or Taurus Building Kit, more_eggs, and the Provider's C2 infrastructure. However, as also highlighted by researchers, the attacks presented key differences based on (a) the targeting; (b) the attack vector, and; (c) the more_eggs configuration.

Figure 4 also shows that the Cobalt group ceased to use the Provider after the campaign on 2 August, and then started to consistently use different malware and infrastructure.

Tactics, Techniques, and Procedures

Figure 5 details the TTPs we observed during all the attacks that leveraged the Provider.

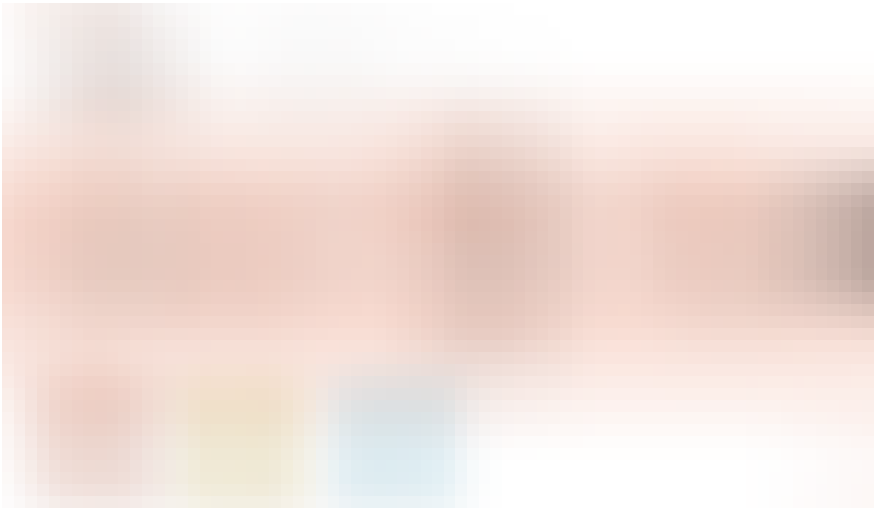

Figure 5 — Cobalt and GC campaigns using the Provider

1. Delivery. Each campaign began with a spear phishing email, but each presented differences depending on the threat actor behind the attack:

- GC threat actors used either compromised or spoofed email addresses. Furthermore, GC01 targeted companies and organizations operating in the financial industry mainly in Europe, Africa, and Asia. Differently, GC02 indiscriminately targeted companies and organizations in at least India and the United States.
- Cobalt also used compromised addresses but only in three attacks. The other 12 spear phishing emails were sent from domain names previously registered by them, imitating a specific organization. Registration of look-alike domains is a common technique used by Cobalt Group. Lastly, all Cobalt campaigns targeted financial institutions and organizations mainly in Europe, Asia and Middle East.

2. Exploitation I (Optional). Both threat actor groups used a non-malicious PDF, luring the user to click on the contained link in order to download the maldoc. The attackers used a technique known as *Google Redirector* which consists of appending the malicious URL at the end of a Google logout URL. By doing this, the user will first visit the legit Google logout page and then automatically be redirected to the final URL, triggering the download of the malicious document.

- GC01 always used this technique. GC02 used this technique in all but one campaign (10 July), which is one reason why we assessed such attribution with low confidence.
- Cobalt only used this technique two times, during the campaigns of 7 and 29 June.

It is not clear to us if the Provider Operator offers the non-malicious PDF (with Google Redirector technique) directly or recommends the use of a third-party kit. To note, we are aware of attacks in the wild using this technique, but without relying on the Provider altogether.

3. Exploitation II—Getting the Maldoc. The user downloads either a macro-weaponized Word document created by Taurus Builder Kit, or a malicious RTF created by VenomKit. Successful execution of the maldocs initiates the download of additional batch scripts and then the ultimate download of the more_eggs backdoor.

- GC01 and GC02 used newer more_eggs versions: 3.0, 4.2, 4.4, 5.2 and 5.4. GC02 used the variable *Researchers* assigned with the value "*We are not cobalt gang, stop associating us with such skids!*".
- Cobalt Group only used more_eggs versions 2.0, having a specific command named *via_x*. This command is used to execute additional executables via cmd.exe. For those campaigns that were not using the non-malicious PDF attack vector, the victims got the downloader through either browsing a link included in the email body, or directly through the email attachment.

4. C2 I—Getting the Backdoor. The maldoc retrieves more_eggs from a remote location and executes it. Next, the backdoor starts beaconing to the C2 defined in the *Gate* variable.

5. C2 II—Getting the Final Payload. Once the threat actor (or the Provider Operator) determines that the infected system is of interest, the final payload is eventually pushed and executed. To note, we were not always able to get the final payload because the more_eggs C2 normally has a short lifetime. However, we were able to observe the following different payloads being distributed by the different threat actors:

- Campaigns attributed to GC01 resulted in the download of three different RATs: Netwire, Remcos, and Revenge.
- Campaigns attributed to Cobalt Group resulted in the download of either the CobInt backdoor, or the Cobalt Strike beacon. So far,

> CobInt is a backdoor that was only observed in Cobalt Group campaigns, while Cobalt Strike is a notorious attack framework used to execute Red Team exercises. We consider the use of CobInt and Cobalt Strike as a final payload a strong indicator while attributing attacks to the Cobalt Group.

. . .

Conclusion

In general, the continued adoption of threat actors leveraging MaaS plays two roles in the cyber threat landscape: (a) it enables less sophisticated actors to execute attack campaigns against high value targets, which may otherwise be out of scope due to the potentially multi-layer perimeter defenses, and; (b) it creates a cluster of technical indicators from the same infrastructure that complicates attribution efforts. During our analysis, we identified three threat actors utilizing one particular MaaS which has operated for almost two years, proving its success and profitability. As a result, this scenario of multiple actors using the same MaaS further corroborates why attribution of campaigns incorporating aspects of MaaS becomes more complex to distinguish due to the presumable overlap in technical indicators.

QuoINT continues to track the activity of these threat actors to help our customers both identify and thwart potential attacks against their environments.

Our Intelligence Assessment will also cover the following points:

- *More information about the Provider, its Operator, and the services advertised:*
- *Assessment on current and prospected capabilities of the Provider*
- *In depth analysis of each spear phishing campaign covered*
- *Full IoC list per Kit, TA, and campaign*
- *Recommended Course of Actions*
- *MITRE ATT&CK mapping*

You can request it via this link.

[1] To note, we only included in the timeline those campaigns attributed to Cobalt group that used the Provider or occurred near or in

the same month of GC's activities. Hence, we excluded Cobalt's activities occurring in January, February, and March 2018. Additionally, this reporting only includes intelligence obtained until October 2018.

. . .

Indicators of Compromise

GC01

Email Subjects:

Payment Details REF # 18110486098

Payment Details REF # 18110486098

Re: Payment Ref 34981***** receive problem

Re: Bank query / S-170526–005399

Amendment/Cancellation

Fund Transfer 08-October-2018

Confirmations on October 16, 2018

confirmation-16003907

Email Attachments (Not-Malicious PDF with Google Redirector)

444c63bb794abe3d2b524e0cb2c8dcc174279b23b1bce949a7125df9fab25c1c

1c1a6bb0937c454eb397495eea034e00d1f7cf4e77481a04439afbc5b3503396

988d430ce0e9f19634cf7955eac6eb03e3b7774b788010c2a9742b38016d1ebf

1d0aae6cff1f7a772fac67b74a39904b8b9da46484b4ae8b621a6566f7761d16

57f65ecb239833e5a4b2441e3a2daf3513356d45e1d5c311baeb31f4d503703e

852f11e5131d3dab9812fd8ce3cd94c1333904f38713ff959f980a168ef0d4ce

Google Redirector links

hxxps://appengine[.]google[.]com/_ah/logout?continue=https%3A%2F%2Fsafesecurefiles[.]com%2Fdoc041791[.]pdf

hxxps://appengine[.]google[.]com/_ah/logout?continue=https%3A%2F%2Falotile[.]biz%2FDocument092018[.]doc

hxxps://appengine[.]google[.]com/_ah/logout?continue=https%3A%2F%2Ffundsxe[.]com%2FDocument09202018[.]doc

hxxps://appengine[.]google[.]com/_ah/logout?continue=https%3A%2F%2Ffundswp[.]com%2FDocument082018[.]doc

hxxps://appengine[.]google[.]com/_ah/logout?continue=https%3A%2F%2Ftransef[.]biz%2FDoc102018[.]doc

hxxps://appengine[.]google[.]com/_ah/logout?continue=https%3A%2F%2Ffundsxe[.]com%2FDocument0922018[.]doc

Landing Page

hxxps://safesecurefiles[.]com/doc041791[.]pdf

hxxps://alotile[.]biz/Document092018[.]doc

hxxps://fundsxe[.]com/Document09202018[.]doc

hxxps://fundswp[.]com/Document082018[.]doc

hxxps://transef[.]biz/Doc102018[.]doc

hxxps://fundsxe[.]com/Document0922018[.]doc

Maldocs

19dc9b93870ddc3beb7fdeea2980c95edc489040e39381d89d0dfe0a825a1570

020ba5a273c0992d62faa05144aed7f174af64c836bf82009ada46f1ce3b6eee

07a3355f81ff69a197c792847d0783bfc336181d66d3a36e6b548d0dbd9f5a9a

161ba501b4ea6f7c2c8d224e55e566fef95064e1ed059d8287bc07e790f740e8

19dc9b93870ddc3beb7fdeea2980c95edc489040e39381d89d0dfe0a825a1570

dc8425f8c966708b1a3c26f0545664ccbf853852af401b91ae7f29d351e2649c

dc8425f8c966708b1a3c26f0545664ccbf853852af401b91ae7f29d351e2649c

GC02

Email Subjects:

Contract April

Description of my complaint about your service

Email Attachments (Not-Malicious PDF with Google Redirector)

45310fcc9f9ef367f16bed4c4ba4c51d7eb72550082cd572f6a5636227514d70

df18e997a2f755159f0753c4e69a45764f746657b782f6d3c878afb8befe2b69

Google Redirector links

hxxps://appengine.googlecom/_ah/logout?continue=hxxps://cloud.pallets32[.]com/Doc00581691.pdf

hxxps://appenginegooglecom/_ah/logout?continue=hxxps://cloudpallets32[.]com/Doc00581951pdf

hxxps://appengine.google.com/_ah/logout?continue=hxxps://mail.halcyonih[.]com/uploads/doc004718538.pdf

Landing Page

hxxps://cloud.pallets32[.]com/Doc00581691.pdf

hxxps://cloudpallets32[.]com/Doc00581951.pdf

hxxps://mail.halcyonih[.]com/uploads/doc004718538.pdf

Maldocs

476c9d4383505429c10c31fb72f5218b3b42d985a2b46a0de62fd6ec5d08eebf

27ec680a57b658d0e63a2b209f407253b4d8904ea025b3ef7c544d98d5798356

a1f3388314c4abd7b1d3ad2aeb863c9c40a56bf438c7a2b71cbcff384d7e7ded

GC Maas C2 infrastructure

outlooklive.org[.]kz

mail.yahoo.org[.]kz

api.outlook[.]kz

nl.web-cdn[.]kz

api.toshiba.org[.]kz

api.outlook[.]kz

api.fujitsu.org[.]kz

api.asus.org[.]kz

api.miria[.]kz

ww3.cloudfront.org[.]kz

webmail.cloudfront.com[.]kz

mail.halcyonih[.]com

cloudpallets32[.]com

contents[.]bz

safesecurefiles[.]com

usasecurefiles[.]com

freecloud[.]biz

alotile[.]biz

fundswp[.]com

transef[.]biz

fundsxe[.]com

document[.]cdn-one[.]biz