CryptoCore

A Threat Actor Targeting Cryptocurrency Exchanges

June 2020

Table of Contents

Cryptocurrency Exchanges Targeted by the CryptoCore Group

Background

In recent years, cryptocurrency exchanges have become targets for constant attacks, mainly from criminal groups and lone hackers. Threat actors of all kinds try to infiltrate corporate networks for reconnaissance, ransomware deployment, and plainly to steal money from those exchanges, specifically from their "hot" (i.e. active, connected) wallets. This kind of targets is somewhat unique, different from traditional financial institutions for two reasons:

- Banks in general, and the SWIFT system in particular, are perceived as highly secured targets in comparison to cryptocurrency exchanges. The lower security of those exchanges' networks rises their potential as a lucrative target for cybercriminals.
- While at first it seems easier to track the stolen money through blockchain, identifying and attributing wallets to entities and individuals is generally more difficult.

From the top 3 attacks against Coinbase, Upbit, and Binance (which was hacked at least twice and had its KYC[1] leaked), to smaller-scale but still sophisticated attacks, such as those carried out by the DPRK-attributed group "Lazarus" (aka HIDDEN COBRA), or the exploitation of vulnerabilities in the Ethereum platform in the (ultimately unsuccessful) attack on Uniswap and Lenf.me[2], attacks against crypto-exchanges had had a discernible place in the 2019-early 2020 landscape.

In this research we would like to present a hidden and persistent group, that has been targeting crypto-exchanges, mainly in the US and Japan since as early as 2018, stealing millions' worth of cryptocoins; we track it as "CryptoCore" (or "Crypto-gang"), aka "Dangerous Password"[3], "Leery Turtle"[4].

Unlike other reports about this threat actor, the CryptoCore report mainly focuses on the group's profile, modus operandi, and digital infrastructure. The "Dangerous Password" and "Leery Turtle" reports zoom in on different aspects of the operation (e.g. toolset, anti-software detection capabilities) and provide complementary findings to what is presented in this report.

We will briefly introduce the report with a general overview, and then proceed to discuss in detail its tactics, techniques, and procedures (TTPs), and also present one case study from our experience. We will conclude with a list of indicators of compromise (IoC).

To all future targeted cryptocurrency exchanges, we encourage your IR team to validate malicious activity with our findings to fingerprint and mitigate additional CryptoCore operations. For further help, please reach us out at info@clearskysec.com.

[1] "Know Your Customer" – a fairly common practice by crypto-exchanges to ask their customers to provide some identification documents and/or photos
[2] zdnet.com/google-amp/article/hackers-steal-25-million-worth-of-cryptocurrency-from-uniswap-and-lendf-me/
[3] https://www.secrss.com/articles/16505
https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/offshore%20APT%20organization/DangerousPassword/2020-04-02/Analysis.md
[4] https://cyberstruggle.org/delta/LeeryTurtleThreatReport_05_20.pdf

Introducing CryptoCore

CryptoCore is a group that targets, as mentioned above, almost exclusively cryptocurrency exchanges and companies working with them via supply-chain attack. Although we have seen singular infections in different countries, the group seems to focus on the United States, Japan, and other countries.

The CryptoCore group is known for having accumulated a sum of approximately 70mil USD from its heists on exchanges. We estimate that the group managed to rake in more than 200mil USD in two years.

This group is not extremely technically advanced, yet it seems to be swift, persistent, and effective, nevertheless. We assess it to be active at least since May 2018, judging from the timestamp of the first known relevant sample, and it maintained steady activity since then. Its activity has receded in the first half of 2020, one possible reason being the limitations induced by the COVID-19 pandemic, but it didn't stop completely.

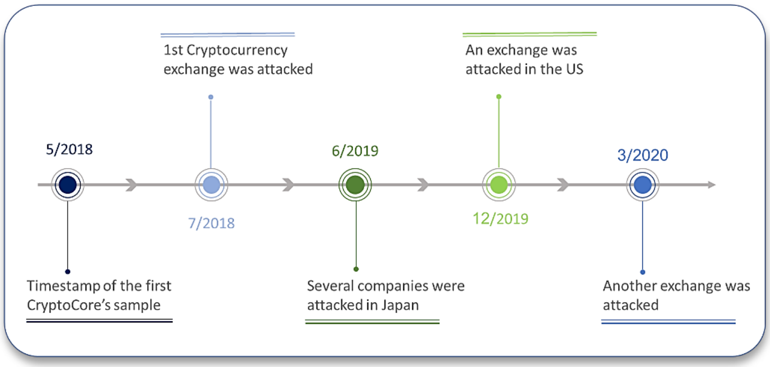

1st Cryptocurrency exchange was attacked
An exchange was attacked in the US
5/2018
6/2019
3/2020
7/2018
12/2019
Timestamp of the first CryptoCore's sample
Several companies were attacked in Japan
Another exchange was attacked

Figure 1: CryptoCore operations timeline

Attribution

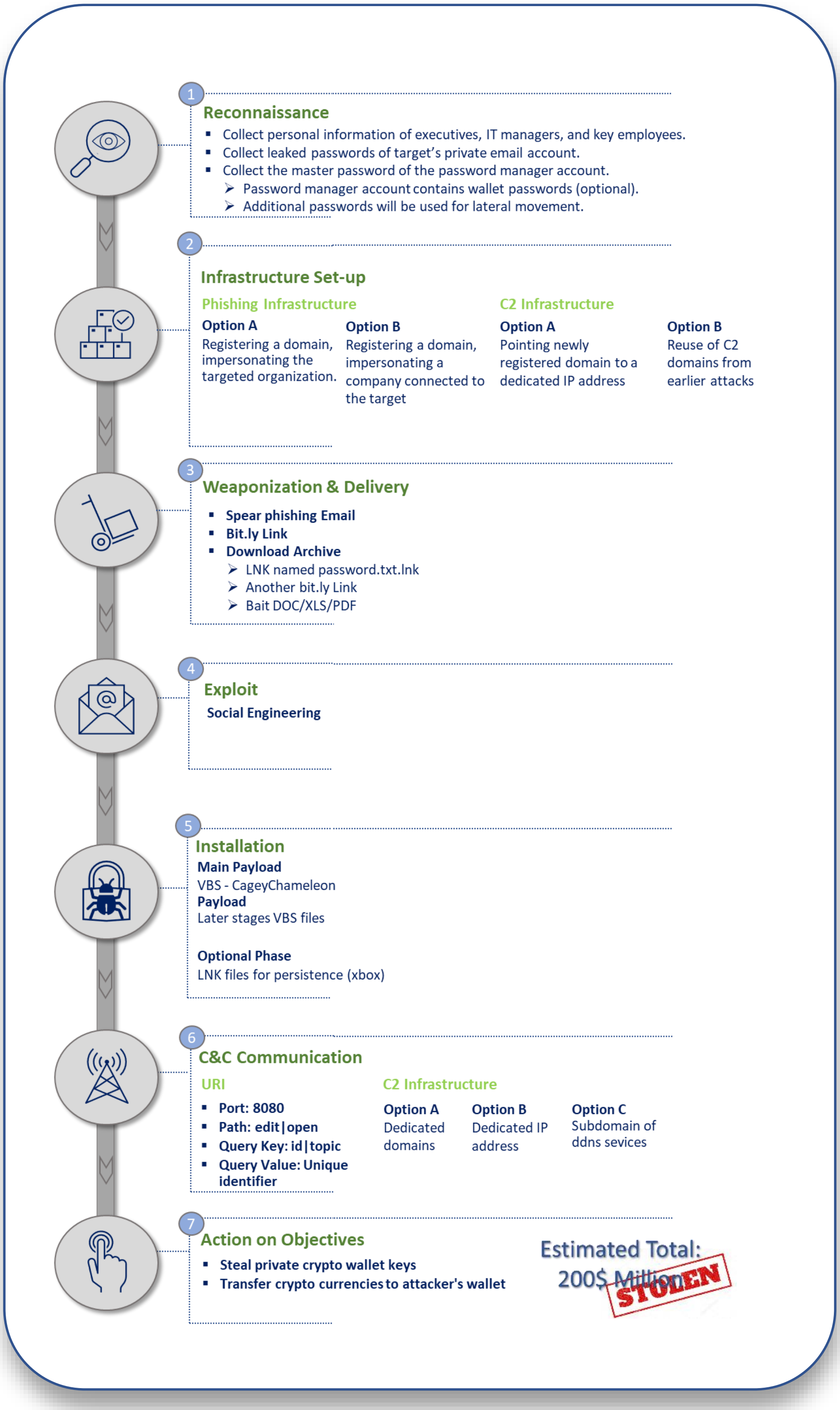
We have been tracking CryptoCore group campaigns for almost two years, with no conclusive understanding of the operators' origin; however, we assess with medium level of certainty that the threat actor has links to the East European region, Ukraine, Russia or Romania in particular.

Modus Operandi

The key goal of CryptoCore's heists is to gain access to cryptocurrency exchanges' wallets, be it general corporate wallets or wallets belonging to the exchange's employees. For this kind of operation, the group begins with an extensive reconnaissance phase against the company, its executives, officers and IT personnel. While the group's key infiltration vector to the exchange is usually through spear-phishing against the corporate network, the executives' personal email accounts are the first to be targeted. Infiltrating the personal email accounts is an optional phase; however, it's a matter of hours to weeks until the spear-phishing email is sent to a corporate email account of an exchange's executive.

The spear-phishing is typically carried out by impersonating a high-ranking employee either from the target organization or from another organization (e.g. advisory board) with connections to the targeted employee. After gaining initial foothold, the group's primary objective is obtaining access to the victim's password manager account. This is where the keys of crypto-wallets and other valuable assets – which will come handy in lateral movement stages – are stored. The group will remain undetected and maintain persistence until the multi-factor authentication of the exchange wallets will be removed, and then act immediately and responsively.

Cyber Kill Chain



1
Reconnaissance

- Collect personal information of executives, IT managers, and key employees.
- Collect leaked passwords of target's private email account.
- Collect the master password of the password manager account.
  - Password manager account contains wallet passwords (optional).
  - Additional passwords will be used for lateral movement.

2
Infrastructure Set-up

Phishing Infrastructure		C2 Infrastructure	
Option A	**Option B**	**Option A**	**Option B**
Registering a domain, impersonating the targeted organization.	Registering a domain, impersonating a company connected to the target	Pointing newly registered domain to a dedicated IP address	Reuse of C2 domains from earlier attacks

3
Weaponization & Delivery

- **Spear phishing Email**
- **Bit.ly Link**
- **Download Archive**
  - LNK named password.txt.lnk
  - Another bit.ly Link
  - Bait DOC/XLS/PDF

4
Exploit

Social Engineering

5
Installation

Main Payload
VBS - CageyChameleon
Payload
Later stages VBS files

Optional Phase
LNK files for persistence (xbox)

6
C&C Communication

URI

- **Port: 8080**
- **Path: edit|open**
- **Query Key: id|topic**
- **Query Value: Unique identifier**

C2 Infrastructure

Option A	Option B	Option C
Dedicated domains	Dedicated IP address	Subdomain of ddns sevices

7
Action on Objectives

- **Steal private crypto wallet keys**
- **Transfer crypto currencies to attacker's wallet**

Estimated Total:
200$ Million
STOLEN

CryptoCore Group's Main Characteristics

- Persistence and adherence to same general TTPs and targets – the group maintains the same general course of action regarding the infection and post-exploitation stages. While the bait document type, the services the phishing sites mimic, the exact tooling and others may vary, an overarching strategy remains the same. Also, the group seems to be reluctant to let go of a target: in some cases that we have investigated, the group keeps attacking the same company over and over. The group also appears to steadily use the same titles for its bait documents and even some payloads.
- Use of Cloud services, particularly – but not limited to – Google Drive – the group often uses Google Drive as the storage for its files, specifically the baits. Sometimes, the phishing emails contain links claiming to be from Drive, while actually directing to a copycat site, and sometimes it uses the actual Drive service. Again, Drive is not the only service they use, it's just common.
- Use of malicious cryptocurrency-themed domains such as btcprime[.]tk, krypitalvc[.]com, blockchaintransparency[.]institute and the like.
- Use of bit.ly URL shortening service – the group uses this service widely for its communications, specifically to deploy scripts and files for further infection. The service has two main advantages for the group's operators: first, it allows to mask a suspiciously looking link behind a neutral bit.ly link; second, it provides the attacker with click statistics, which allow them to track the number of potential infections and their geographical spread.
- Use of LNK shortcuts as downloaders – we have seen the attackers hide LNK shortcuts behind icons and titles of other file types, mostly text files. Sometimes it could be a password file needed to open the main document, sometimes it could be the main document that is actually a shortcut, but LNK files are a staple for this group. These files are used to connect to the command and control (C2) server and download next-stage files.
- Use of Visual Basic Script (VBS) files – one distinct characteristic of the group is a relatively heavy use of VBS files both as downloaders and as backdoors. What appears to be the main backdoor of the group is also a VBS file (tracked by Proofpoint Emerging Threats as CageyChameleon), rather than an executable or an in-memory payload. We are not sure why VBS, but we can assume that these files are deemed lighter and less prone to detections, as opposed to, say, EXE or DLL files. However, in singular cases we have seen the group downloading and using the Mimikatz password-dumping tool as well, so VBS files are not the only tools used in post-exploitation.
- Swiftness and responsiveness – the group's infrastructure is continuously and rapidly changing. While in some cases we have seen the same infrastructures being constantly reused, perhaps against multiple victims, the group is generally quick to register and employ new domains and links. In some cases, the freshly created bit.ly link is used immediately, on the same day; in one case, a new domain was registered, we have alerted the client, and within 30-40 minutes their systems identified an attack from that new domain.

CryptoCore Infrastructure Insights:

1) CryptoCore Working Time Zone

In attempt to better understand the origin of CryptoCore operators, we have collected the Whois registration dates of C&C domains. After data cleaning, a plot of the distribution of Whois registration records showed no distinct time zone. As shown in the chart below, as for UTC+0, the operators do not register their C&C domains in certain working hours.

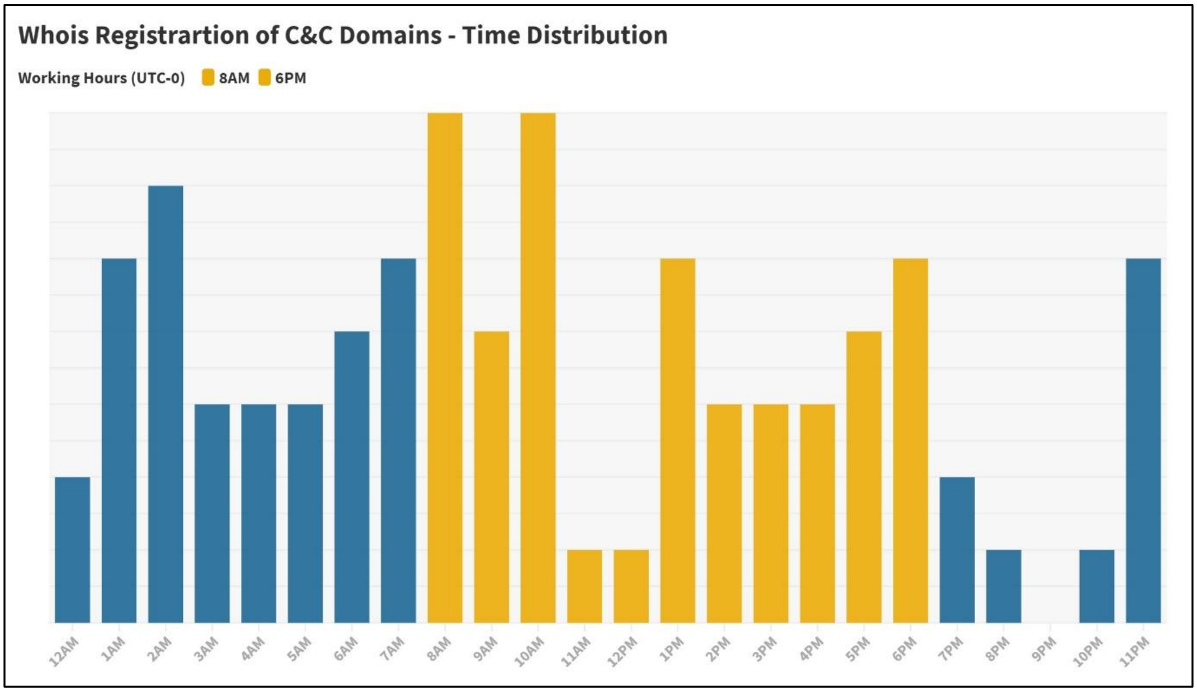


Figure 2: CryptoCore C&C Whois registration records by hour

2) CryptoCore operators use dedicated IP addresses where they host their C&C domains. These IPs are associated with AS networks located in multiple countries, mainly the United States, Taiwan, Brazil, Egypt, Mongolia, and Thailand (in descending order).

3) C&C TLD to Registrar & Nameserver Distribution
CryptoCore group mostly registers dedicated C&C domains, using the .xyz TLD via NameCheap registrar services. Moreover, the operators register all dedicated C&C domains that are associated with the .info TLD via NameSilo registrar services. The hostname usually contains keywords that resemble names of cloud services (also through typo-squatting). They frequently use the known TLD .com, alongside gTLDs containing meaningful words to mislead the victims, such as .email, .services, etc. In addition, it appears that the threat group prefers PublicDomainRegistry and NameSilo registrars; however, these are not the only registrars used.

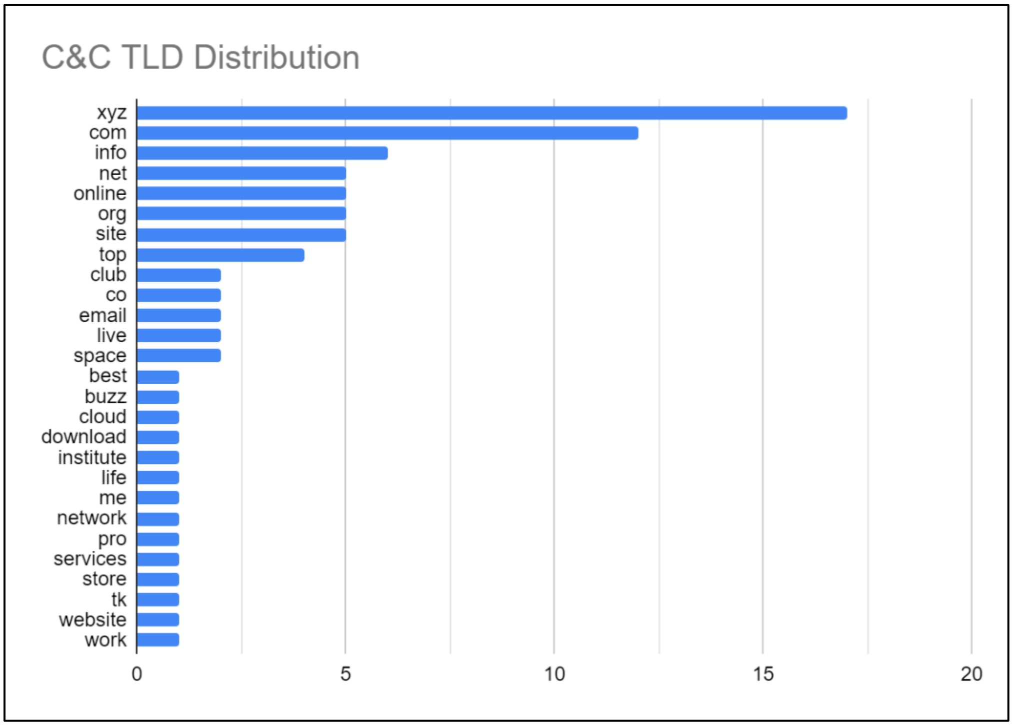


Figure 3: CryptoCore C&C TLD Distribution

4) Anomalous Registration of multiple C&C Domains in 3 Days

   Usually, CryptoCore operators do not register multiple C&C domains on the same day, except on special occasions. One company was targeted by CryptoCore in July 2018, two months before the group registered **10 domains within 3 days**. This may indicate that the group's operators were aware that their digital infrastructure has been discovered, so they have started quickly setting up new digital infrastructure in a few days.

   In addition, **they tend to register a new C&C domain once or twice a month until this day.**

5) CryptoCore operators re-register expired C&C domains

   This may suggest the attackers' intent to reuse the infrastructure for different ongoing campaigns, as well as future ones. In addition, it emphasizes that year-old domains are still in use, and hence should be blocked for long periods.

6) Use of DDNS services till 2019

   In 2018 and 2019, CryptoCore operators had heavily relied on DDNS services such as dynu (dynu.com, kozow.com, theworkpc.com), ChangeIP (onmypc.org, itemdb.com, itsaol.com) and DNSExit/Netdorm (linkpc.net, publicvm.com). However, in 2020 we have observed an uptick in registering new domains and pointing C&C domains to dedicated servers.

Infection Chain

The following diagram shows the general infection pattern of CryptoCore, as presented in a research published independently by the Japanese CERT and dealing with CryptoCore's activity in Japan[5].

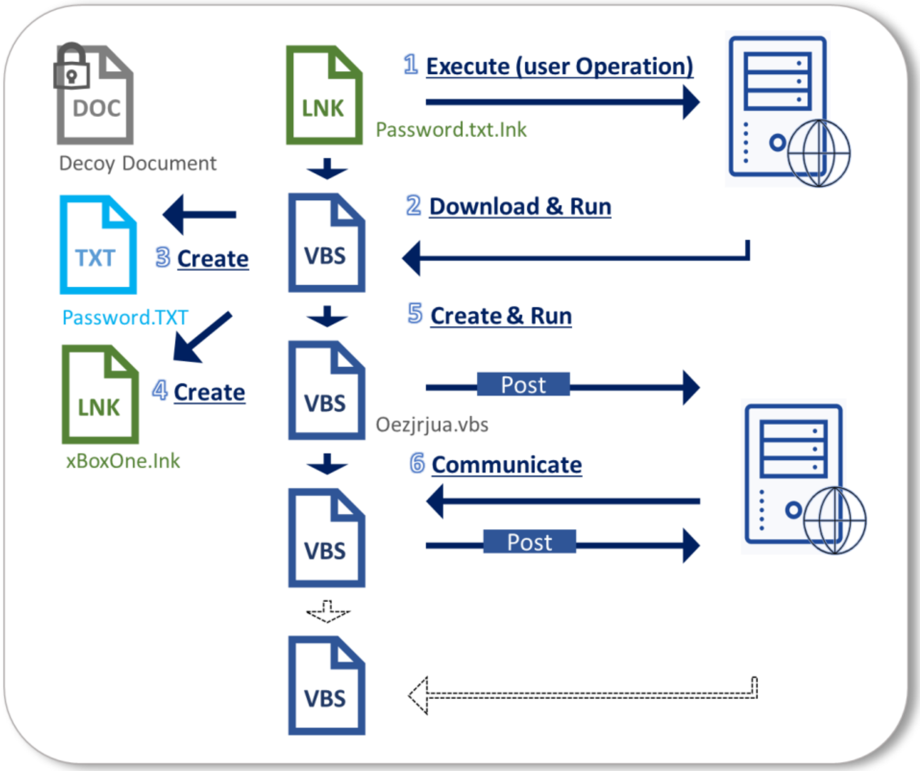
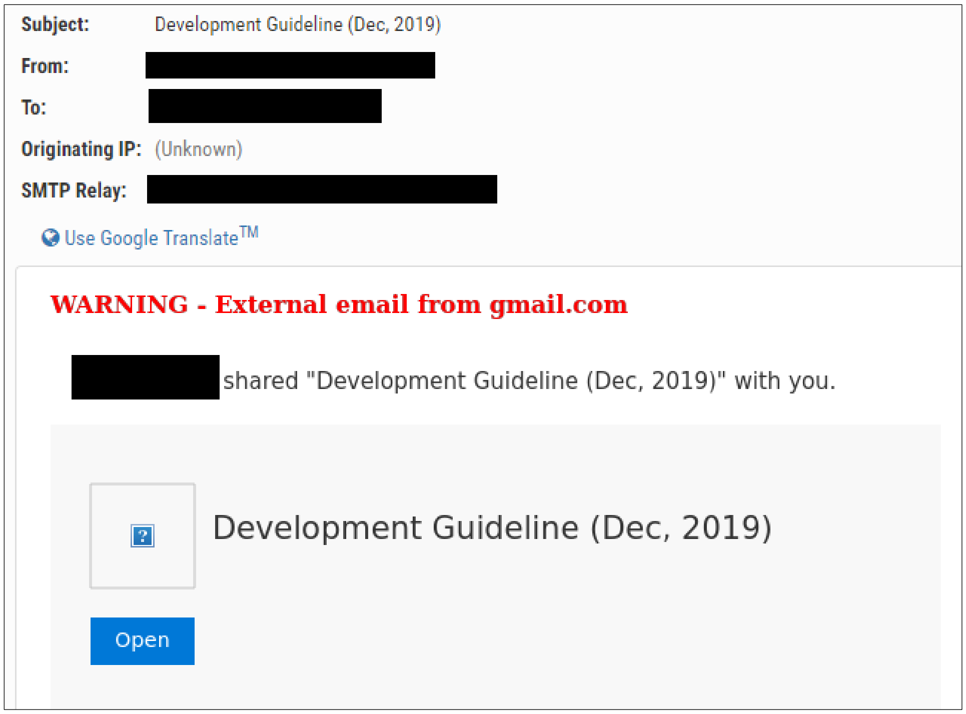


Figure 4: CryptoCore's TTP outline as presented in JPCERT's research

CryptoCore TTPs

As previously mentioned, the campaign begins with an extensive reconnaissance stage against the company, it's executives, IT managers and key employees. Optionally, the group operators gain access to private email accounts of executives in the targeted cryptocurrency exchange. The next stage would be spear-phishing, typically impersonating a high-ranking employee, either from the target company itself or from a company that deals with the target. The email's quality is not consistent and can vary from almost generic-looking phishing email with a shared link (see Figure 5), to a well-crafted email that is only slightly flawed (see Figure 6).

[5] blogs.jpcert.or.jp/en/2019/07/spear-phishing-against-cryptocurrency-businesses.html



Subject: Development Guideline (Dec, 2019)

From: [redacted]

To: [redacted]

Originating IP: (Unknown)

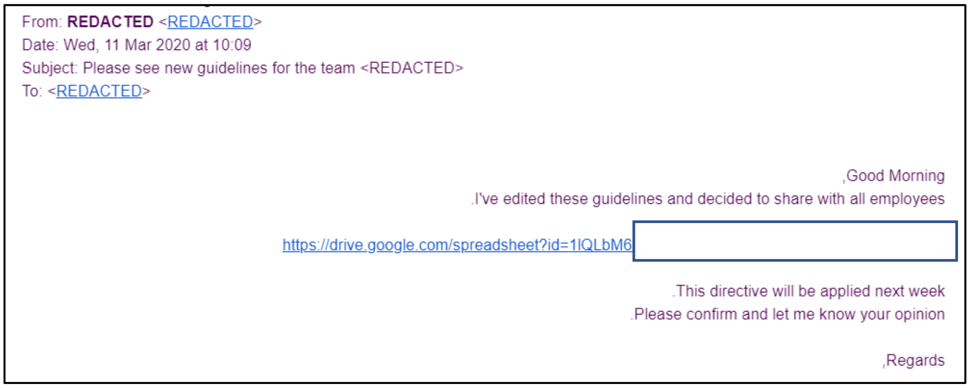
SMTP Relay: [redacted]

WARNING - External email from gmail.com

[redacted] shared "Development Guideline (Dec, 2019)" with you.

Development Guideline (Dec, 2019)

Figure 5: example of a simplistic phishing email by the group



From: **REDACTED** <REDACTED>
Date: Wed, 11 Mar 2020 at 10:09
Subject: Please see new guidelines for the team <REDACTED>
To: <REDACTED>

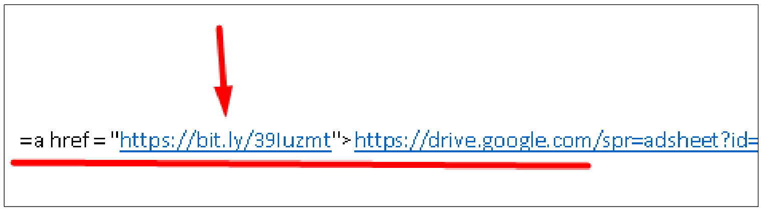
,Good Morning
.I've edited these guidelines and decided to share with all employees

https://drive.google.com/spreadsheet?id=1lQLbM6

.This directive will be applied next week
.Please confirm and let me know your opinion

,Regards

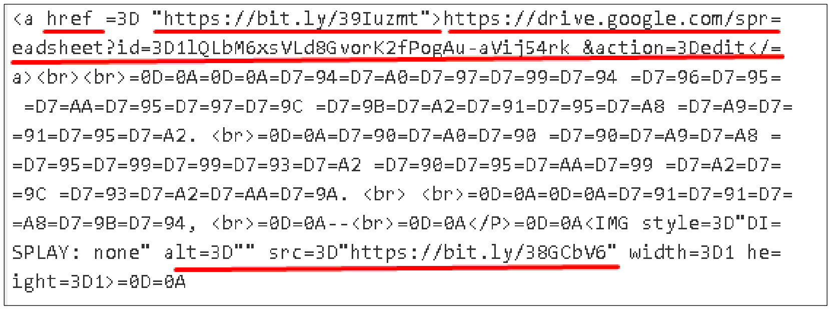
Figure 6: example of a spear-phishing email by the group, note the misplaced punctuation



```
=a href = "https://bit.ly/39luzmt"> https://drive.google.com/spr=adsheet?id=
```

Figure 7: An href attribute leads to a bit.ly link instead of Google Drive

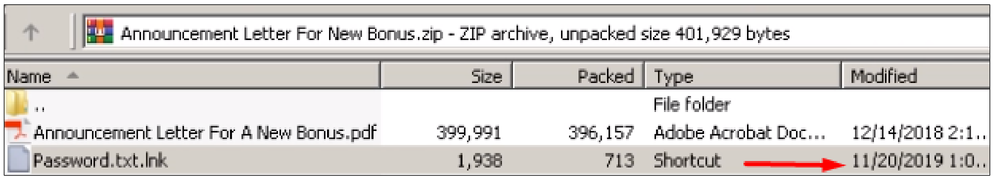
While the link in the email states that its destination is Google Drive, it really leads to malicious landing page with a similarly-sounding name. The true link is served via an HTML href attribute, shortened with bit.ly, probably for analysis obstruction and statistics' collection as bit.ly allows its users to track the shortened link's clicks. In parallel, another bit.ly connection will be established, using an <img> HTML tag probably containing the company's logo and the second bit.ly link. However, this tactic in not a consistent characteristic of Crypto Core, as it has only been observed once until now – in most cases the link will not hide behind another link but rather lead to the download.



```
<a href =3D "https://bit.ly/39Iuzmt">https://drive.google.com/spr=
eadsheet?id=3D1lQLbM6xsVLd8GvorK2fPogAu-aVij54rk &action=3Dedit</=
a><br><br>=0D=0A=0D=0A=D7=94=D7=A0=D7=97=D7=99=D7=94 =D7=96=D7=95=
 =D7=AA=D7=95=D7=97=D7=9C =D7=9B=D7=A2=D7=91=D7=95=D7=A8 =D7=A9=D7=
=91=D7=95=D7=A2. <br>=0D=0A=D7=90=D7=A0=D7=90 =D7=90=D7=A9=D7=A8 =
=D7=95=D7=99=D7=99=D7=93=D7=A2 =D7=90=D7=95=D7=AA=D7=99 =D7=A2=D7=
=9C =D7=93=D7=A2=D7=AA=D7=9A. <br> <br>=0D=0A=0D=0A=D7=91=D7=91=D7=
=A8=D7=9B=D7=94, <br>=0D=0A--<br>=0D=0A</P>=0D=0A<IMG style=3D"DI=
SPLAY: none" alt=3D"" src=3D"https://bit.ly/38GCbV6" width=3D1 he=
ight=3D1>=0D=0A
```

Figure 8: a code snippet with the link in the <img> tag

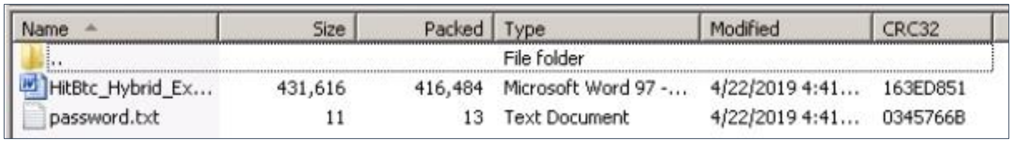
Clicking the link in the email will result in a compressed file being downloaded to the target computer. This file will typically contain two additional files – a bait document (DOC, PDF or XLS) that is password-protected, and an LNK file disguised as a text file with the password (see Figure 9). However, in singular cases we have seen the password file being a text file indeed, while the password-protected bait initiated the connection with the C2 server (see Figure 10)



Announcement Letter For New Bonus.zip - ZIP archive, unpacked size 401,929 bytes

Name	Size	Packed	Type	Modified
..			File folder	
Announcement Letter For A New Bonus.pdf	399,991	396,157	Adobe Acrobat Doc...	12/14/2018 2:1..
Password.txt.lnk	1,938	713	Shortcut	11/20/2019 1:0..

Figure 9: the LNK file



Name	Size	Packed	Type	Modified	CRC32
..			File folder		
HitBtc_Hybrid_Ex...	431,616	416,484	Microsoft Word 97 -...	4/22/2019 4:41...	163ED851
password.txt	11	13	Text Document	4/22/2019 4:41...	0345766B

Figure 10: the txt file

Usually, the LNK file will present the target with a text file containing the password and at the same time it will also download a malicious VBS script, also through a bit.ly-shortened URL. At this point, the campaigns slightly differ, specifically those presented in the JPCERT/CC report[6].

In the Japanese case, in addition to presenting the password, the LNK also creates and runs a VBS file in %TEMP%, and also lists the processes running on target computer, looking for specific strings: "hudongf" or "qhsafe", which are suspected to represent the "zhudongfangyu.exe" and "qhsafemain.exe" processes of the Quihoo360 security solutions suite. If those are absent, an LNK file, named "xBoxOne.lnk", will be added to the Startup folder, making it run every time a user logs into the infected computer; if one of those strings is present in the process list, no further action will be taken. The Japanese CERT was unable

[6] blogs.jpcert.or.jp/en/2019/07/spear-phishing-against-cryptocurrency-businesses.html

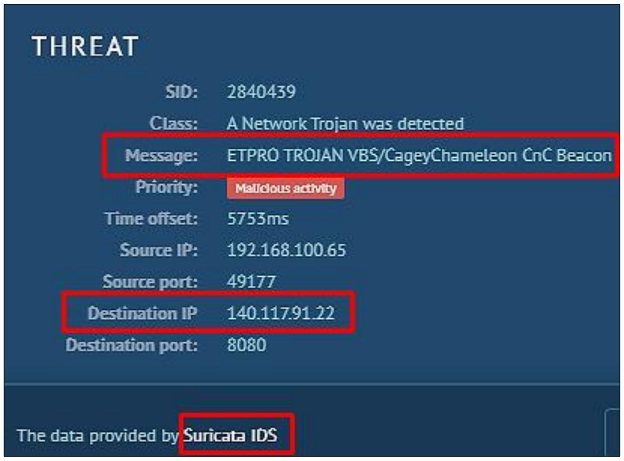
to confirm, as of June 2019, the LNK's ultimate purpose, however, given the fact that it sits in the Startup folder, we assume it to give the attackers persistence on the target.

As for the VBS created in %TEMP%, it acts as a downloader for another VBS. That VBS collects the following information:

- Username
- Host name
- OS version, install date and run time
- Time zone
- CPU name
- Execution path of the VBS in %TEMP%
- Network adapter information
- List of running processes

The information is sent to the C2 server every minute, and it expects additional VBS as a response. The JPCERT couldn't confirm the nature of this latter-stage payload.

In the cases observed by us, manual execution of the LNK file initiates the infection chain. While the user is presented with the password for the bait document, the compromised host performs a one-time communication with the C2 to download a VBS payload identified as VBS/CageyChameleon by Proofpoint's Emerging Threats service. This VBS collects the same information as the one mentioned in the Japanese case, i.e. username, OS, time zone etc. The cases differ, then, in the intermediate stages between the "password" file's opening and the activation of the stage 2 payload – in the Japanese case there are additional stages (e.g. the presence of oezjrjua.vbs), not seen by us.



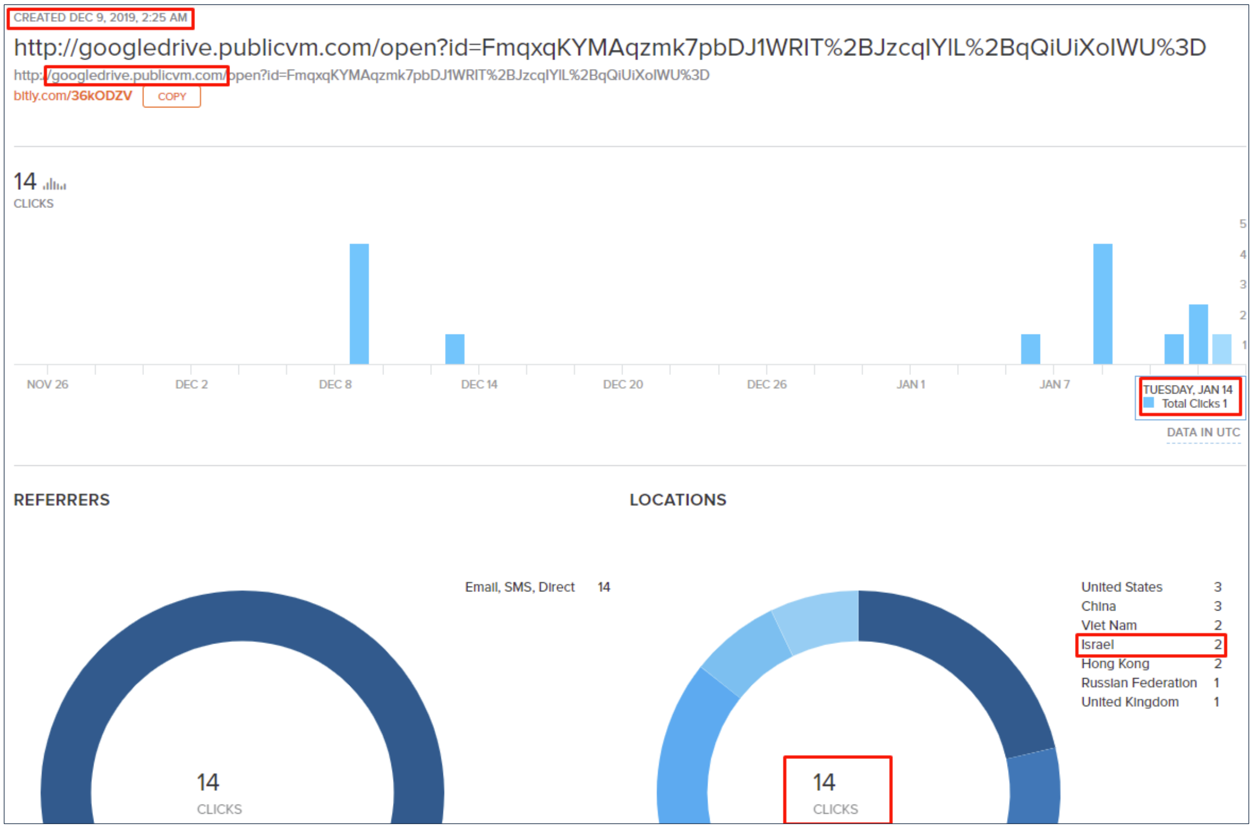
THREAT

SID:	2840439
Class:	A Network Trojan was detected
Message:	ETPRO TROJAN VBS/CageyChameleon CnC Beacon
Priority:	Malicious activity
Time offset:	5753ms
Source IP:	192.168.100.65
Source port:	49177
Destination IP	140.117.91.22
Destination port:	8080

The data provided by Suricata IDS

Figure 11: the second stage VBS payload identified as part of the campaign

As already mentioned, the group makes extensive use of the legitimate bit.ly shortening service in its communications. The service not only allows the attacker to hide their links behind innocuously looking shortcuts, but also provides them with click statistics. It's worth the mention that those statistics used to be publicly viewable, roughly until early 2020, but are currently open only to the links' creators.



CREATED DEC 9, 2019, 2:25 AM

http://googledrive.publicvm.com/open?id=FmqxqKYMAqzmk7pbDJ1WRIT%2BJzcqlYIL%2BqQiUiXolWU%3D

http://googledrive.publicvm.com/open?id=FmqxqKYMAqzmk7pbDJ1WRIT%2BJzcqlYIL%2BqQiUiXolWU%3D

bitly.com/36kODZV COPY

14 CLICKS

TUESDAY, JAN 14
Total Clicks 1

DATA IN UTC

REFERRERS

Email, SMS, Direct	14

14 CLICKS

LOCATIONS

United States	3
China	3
Viet Nam	2
Israel	2
Hong Kong	2
Russian Federation	1
United Kingdom	1

14 CLICKS

Figure 12: Statistics provided for the attacker through one of the links

As depicted in Figure 12, **CryptoCore operators tend to use their bit.ly links to a limited number of highly targeted victims originated in different countries. They reuse the same bit.ly links**, using them continuously for 3-7 days, as seen in December 2019 and January 2020 (Figure 12).

Another characteristic of the group is communicating with the C2 server through the 8080 port with the target's unique identifier appended usually to an "id" parameter, or, rarely, to a "topic" parameter:

a. <C2 domain>:8080/edit?(<id or topic>)=<unique_identifier>

b. <C2 domain>:8080/open?(<id or topic>)=<unique_identifier>

c. <DDNS C2 subdomain>:8080/search.php

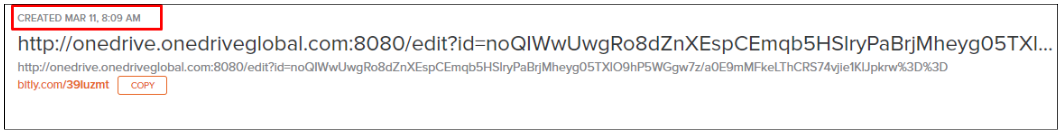
CryptoCore in action: Case Study

We have presented out main understandings about the group, now we would like to demonstrate it in action, through one case that we have investigated this March.

That morning, we've notified one of our clients about freshly discovered CryptoCore indicators. The client informed us, that **roughly 30-40 minutes after we've sent the notification their systems identified an attack through the new infrastructure**.

The attack began with a phishing email impersonating the client's CEO and supposedly containing some new instructions which should be distributed and acquainted with by the employees. The email was written in fairly good local language, but it was nevertheless imperfect and with odd punctuation. What's more is that communications inside the company are conducted mostly in English, so however good was the language used by the operators, it was still suspicious.

Analyzing the emails headers, we saw it being initially sent from a computer belonging to the Italian hosting company "Aruba". Moreover, the link written in the email was supposedly leading to Google Spreadsheets, while the <href> actually contained a bit.ly link and the Spreadsheets link was just a ruse. The true link led to a page mimicking Google Drive and registered that same morning.



CREATED MAR 11, 8:09 AM

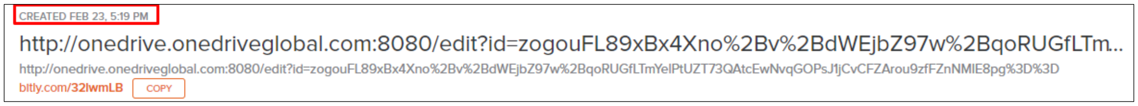
http://onedrive.onedriveglobal.com:8080/edit?id=noQIWwUwgRo8dZnXEspCEmqb5HSlryPaBrjMheyg05TXI...

http://onedrive.onedriveglobal.com:8080/edit?id=noQIWwUwgRo8dZnXEspCEmqb5HSlryPaBrjMheyg05TXIO9hP5WGgw7z/a0E9mMFkeLThCRS74vjie1KIJpkrw%3D%3D

bitly.com/39luzmt

Figure 13: The newly registered page being employed right away

For the second stage, another bit.ly link was used, leading to a page created in late February:



CREATED FEB 23, 5:19 PM

http://onedrive.onedriveglobal.com:8080/edit?id=zogouFL89xBx4Xno%2Bv%2BdWEjbZ97w%2BqoRUGfLTm...

http://onedrive.onedriveglobal.com:8080/edit?id=zogouFL89xBx4Xno%2Bv%2BdWEjbZ97w%2BqoRUGfLTmYelPtUZT73QAtcEwNvqGOPsJ1jCvCFZArou9zfFZnNMIE8pg%3D%3D

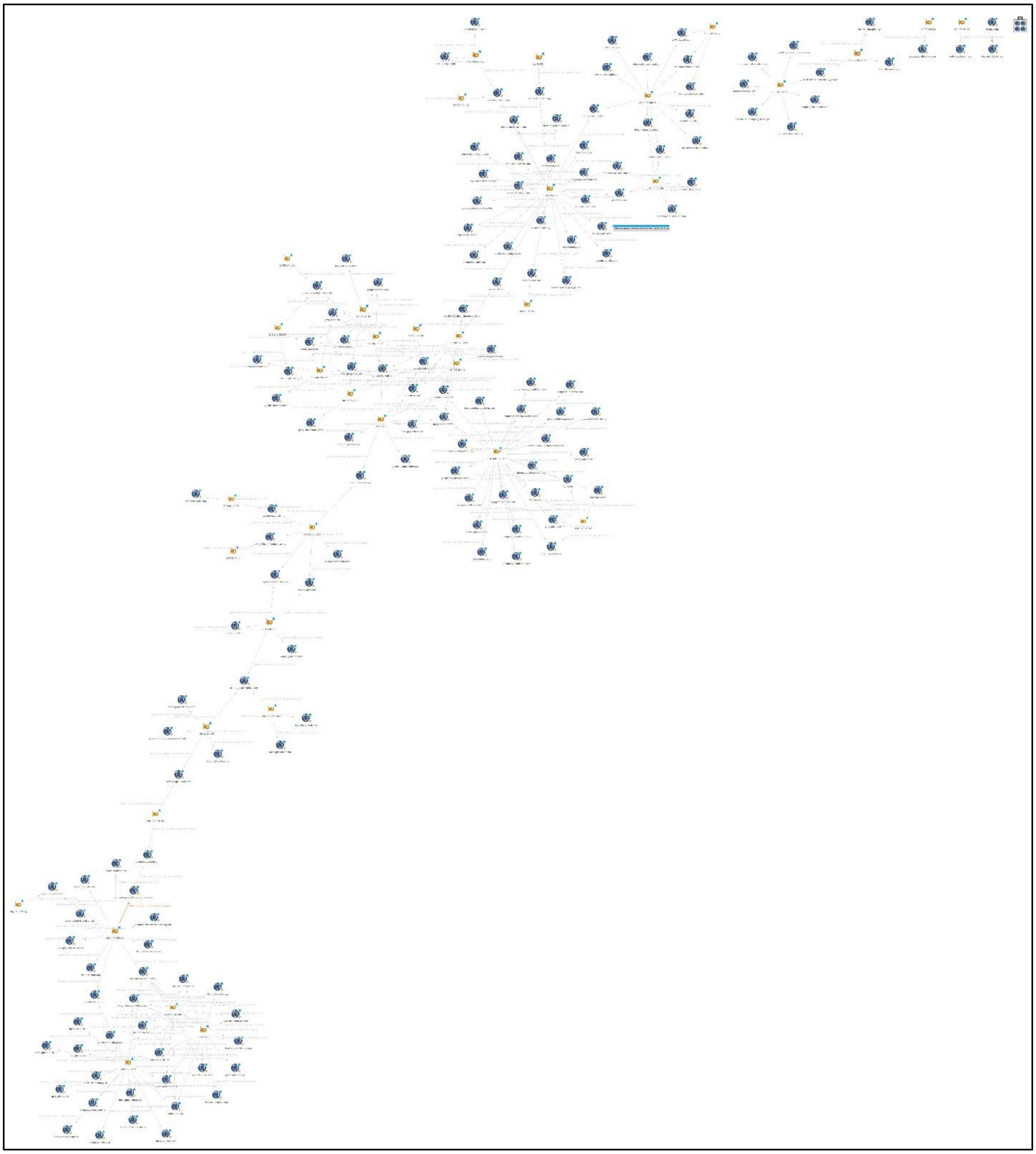
bitly.com/32lwmLB

Figure 14: Use of another bit.ly link that was created in late February

During the attack, we suspect the group also employing Mimikatz for credentials harvesting.

CryptoCore Digital Infrastructure - Graph

The following Maltego graph visualizes CryptoCore digital infrastructure, mainly dedicated IP addresses linked to C&C domains via passive DNS. The long, chain-like structure of the graph demonstrates a strong connection between network indicators, which in turn corroborates our findings.



IOCs

Domains:

gogleshare[.]xyz
googledrive[.]network
googledrive[.]email
gmaildrive[.]site
googldocs[.]org
gdriveupload[.]info
googleapis[.]online
gmaildriver[.]info
googleexplore[.]net
googledrv[.]com
googlefileshare[.]com
googledrive[.]online
goglesheet[.]com
gdriverfileshare[.]com
gdrvupload[.]xyz
filecloud[.]website
gdriveupload[.]site
googledrive[.]download
gdrvcheck[.]co
googldrive[.]xyz
gdrvup[.]xyz
fcloudshare[.]xyz
gmaildrive[.]info
gdrvauth[.]cloud
googledriver[.]xyz
showprice[.]xyz
sharesdown[.]xyz
wechart[.]org
googledriver[.]net
googledriver[.]info
googledriveshare[.]com
liveonedrvshare[.]xyz
krypitalvc[.]com
sendspace[.]buzz
secureshares[.]online
uploadsfiles[.]xyz
googleupload[.]info
googleshare[.]org
microsoftapp[.]life
onedrivecloud[.]store
navicheck[.]xyz
googlecloud[.]live
googlefiledrive[.]com
msupdatepms[.]xyz
onedrvfile[.]site
provemail[.]net
privacyshield[.]services
googleauth[.]pro
googlecstorage[.]com
googleclouddrive[.]com
ownemail[.]me
onedrivems[.]online
onedriveglobal[.]com
onedrvdn[.]co
onedrivrshares[.]xyz
sharegoogldrive[.]online
sharedrivegght[.]xyz
euprotect[.]net
dns-cloud[.]net
digifincx[.]com
gdrvshare[.]site
gdrives[.]best
drivegooglshare[.]xyz
amazonaws1[.]info
gdriveshareslink[.]xyz
financialmarketing[.]live
drivegmail[.]top
gdriveshare[.]top
gdrives[.]top
decurret[.]site
1drv[.]email
1driv[.]org
drivegoogle[.]org
cloudsecure[.]space
cloudocs[.]space
blockchaintransparency[.]institute
amzonnews[.]club
1drvmail[.]work
cloudfiles[.]club
bugscrowd[.]com

DDNS sub-domains

onedriveupdate[.]publicvm[.]com
msupdate[.]publicvm[.]com
twosigma[.]publicvm[.]com
drivegoogle[.]publicvm[.]com
googleupdate[.]publicvm[.]com
connsec[.]publicvm[.]com
drivegooogle[.]publicvm[.]com
chromeupdate[.]publicvm[.]com
mpksl[.]publicvm[.]com
mskpupdate[.]publicvm[.]com
googledrive[.]publicvm[.]com
googledrive[.]dynu[.]net
europegdprsec[.]onmypc[.]org
coinnews[.]onmypc[.]org
vpset[.]onmypc[.]org
armzon[.]onmypc[.]org
coindeck[.]onmypc[.]org
eusharesrv[.]onmypc[.]org
gdrive[.]onmypc[.]org
termsofservice[.]onmypc[.]org
esosv[.]itemdb[.]com
excinfo[.]itemdb[.]com
sevicebill[.]itemdb[.]com
coinomic[.]itsaol[.]com
ddsvr[.]itsaol[.]com
tokenomic[.]itsaol[.]com
btcprime[.]itsaol[.]com
ledgerservice[.]itsaol[.]com
vpsfree[.]linkpc[.]net
googledrive[.]linkpc[.]net
matrix-partners[.]theworkpc[.]com
blackwell[.]tekstar[.]us
windrvupdate[.]kozow[.]com

IP addresses

66[.]181[.]166[.]11
78[.]94[.]213[.]101
203[.]144[.]133[.]42
69[.]64[.]54[.]215
210[.]212[.]148[.]30
66[.]181[.]166[.]15
23[.]65[.]190[.]86
70[.]184[.]87[.]103
91[.]98[.]251[.]208
59[.]127[.]150[.]197
190[.]85[.]159[.]46
190[.]81[.]34[.]163
191[.]215[.]16[.]82
91[.]140[.]255[.]62
68[.]232[.]175[.]188
128[.]201[.]64[.]194
23[.]254[.]144[.]139
209[.]208[.]109[.]38
59[.]120[.]122[.]35
145[.]108[.]194[.]10
140[.]117[.]91[.]22
199[.]66[.]91[.]106
202[.]39[.]61[.]57
192[.]48[.]29[.]14
197[.]44[.]198[.]211
186[.]232[.]112[.]25
125[.]100[.]175[.]62
192[.]183[.]29[.]182
62[.]201[.]228[.]179
181[.]193[.]82[.]122
197[.]51[.]50[.]158
140[.]136[.]134[.]201
185[.]45[.]28[.]182
203[.]151[.]166[.]13
104[.]168[.]137[.]213
88[.]204[.]166[.]59

URLs (Hardcoded IP addresses)

140.136.134[.]201:8080/open?topic=
41.85.145[.]164:8080/open?topic=

Hashes (MD5)

097698566d9c88a520e0d5459566a6b1
8cc8bdc017b103f4dbd00e6336809594
d7b8c3c986495a814c9b8bd10d3f5eef
7d9d91748258e35176386497765dbc00
cd0a391331c1d4268bd622080ba68bce
15f1ae1fed1b2ea71fdb9661823663c6
e7d42e055708a6659661370b99f516d1
eab491a31d4f049695c0aa515a0d90b6
dbbe0311788f525b2163fb510ca8f22a
3078265f207fed66470436da07343732
f3b7eaf965e30bef2d5ef1ee1bb6634b
db3c54038e0b2db2c058a5e9761e4819
ff9ee83f13bd8167d9ba780b2a147668
0bc0ed48bb02e5d08d5549b59ff1105a
6af21f0bdefb55a4219fd4c25674ba67
3812cdc4225182326b1425c9f3c2d50b
a9c5355fce2bd42e5cb3cd1fe6c375f1
874ef600af0a8b88ca5c937d140ea8c5
034c0ad0de6464db26a54620d28382cb
ee15bec0e9ba39f186d721515efd6a00
5ebdfa1bf92d8075f53427531567fbf7
56fe283ca3e1c1667191cc7764c260b6
88349b3e7e2e61a8dc3d0fc02e461c7e
d7748383f7c1c8a198da473a5f5842fa
0eb71e4d2978547bd96221548548e9f0
fe9f9f690943047e1f877644cb6d4648
e91de2e139d6560f5a81016d46d03db3
4274e6dbc2b7aee4ef080d19fff47ce7
a0d98d01ed78fd66494138ac155c56c1
d3d32225bf893ccc62dee9d833fe04f2
d41f422a621b097b949e1540e48d5f58
797adc31b6370ca50318ae342d692ad6
09bca3ddbc55f22577d2f3a7fda22d1c
0e529999ed0a329c39a2fbdda3458b74
00ba843f8d6dcb8bbc5b22c3288e8a3e
0c9170a2584ceeddb89e4c0f0a2353ed
e9b4c4ec893a15f23524766764b696c6
36ad2e8ac0ec506fe582c14ba5713cd5
2ea2ceab1588810961d2fc545e2f957e
1a8282f73f393656996107b6ec038dd5
97e2ce9d86c1c99619a343b69e447d02
da6a366750e77d3e24126e0a69379c42
45123dac5e13cebe1dc7fc95afd9c63e
16fe7f469b46cd01f35dff21a5cdf5fd

```
3e9b52e3b90ac45ac5ddb9c91615c7ae
ebe8b4bdf1536a788afa6ab67ad9e53c
3b6a9b2cbb4874c551929c2b530412ab
b8406b91b0eb57267f192a1aee6d3ee0
da599b0cde613b5512c13f299fec739e
de762f4e393af735609cf2e08f56ee7b
b85879c0a463dddc3a98c91c9cd52934
ce9030dd0ce0c3872f5b59088e9a3362
0efd61f2ed379a5ae43c39333196d178
b33cade6a8c03e94a7d06306c7cfc36b
16be84684b3cbcde54b45315164bdd23
850751de7b8e158d86469d22ad1c3101
e6e64c511f935d31a8859e9f3147fe24
093eae51bd7566c40d646c1b37bce0ea
9b694c70494d968c319566f72f358fd3
feccea47b97e78f2d6c4271da3f565c4
0a512f11ab114c91dadcd5ca9cea63b8
7d5c259d422310218a8888ec1ce65e92
561f70411449b327e3f19d81bb2cea08
64272932a09b818a818e965aafc579ab
d73499bc6b500b4fc5648943e12ce9e2
7cd7604ddfa4eb0caf7c878c8fdf617f
146827291a77c6d85ec53f18e371a03c
220e32ff140ef5f0fdef71b5b82b3a48
170a96fd6fb606a56474e2fc716d91bb
786e61e00c33175cc9ed9b7b99d166d4
c869b0fe739d0626e4474eea980dd018
4668e0de731ea41243c5bce6ea506309
9b4df98a975b622c456c7f8e2001628f
83bac6075fe0d21eea6c9942b2738a1e
23949657ccb9913f746bd777017eca17
753959ab347cc43af439cb3eb36e8caa
c5d9a6478b9b68c213301cb81cbd3833
e2dd0bf4bdf8d51954c7c8a924571d3c
bd191dac5e16ec6db262b92b3f4f2556
cf1bc39380f40a514aa82e4db6215b11
318285813e4665c80be08db657c2bd4c
92b9808028e5d7019c29ea41df162db4
c509890d250d6e986e3c3654aa5cea26
f0a92e7d0a8eb7a85003a316704c9812
9aa464cc5f50b3db260a0d2ec9e74ead
8b7350ac6d069e77fb63b3cee3df31a8
a1c607fe90eecdb3dafea82bb7a089b4
0dc133b5b06b454d9777b552e84f1f4e
427bdfe4425e6c8e3ea41d89a2f55870
53b800066811b7668e59774bd4c763ca
8cb554127837a4002338c10a299289fb
244a23172af8720882ae0141292f5c47
ce09cdb7979fb9099f46dd33036b9001
8468a0bae15202a634ac48e56724edbe
5d662269739f1b81072e4c7e48972420
bd1cf2404e0d03d6256ce333e97af25a
2888f852a8a90e16aa72282fad6eb16e
5241c8bf6be44eea9c9c45ef2dcf3867
7a83be17f4628459e120a64fcab70bac
17d97dca939836fe4eeb61eac371960f
2d27e4aa3315c7b49ce5edd1a3fb5485
92aa224af7d71c9fc162fdb6ce53bc5b
1439d13eee4b43501bfadbe40da1e1f6
d0c500c37ae9f9e3657d26272722b997
a929b7eb37a7fa26dc59c1fee364ec65
629f6a17bea4c386aee3dfec2ed6ec2c
97fd02ae666988d853a68fdd7f7d2e7f
cc7d27698488a80f9fc35341d31ef872
5bb049c31f5fb8c4a076def3efb91177
059bde35d1f07a4af75a7e2cbdd73380
47c91edfe71fe31801a86ea97cf5a42c
```

ClearSky Cyber Intelligence Report

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY Cyber Security

Ahead of the Threat Curve

Photos by Dmitry Demidko on Unsplash

https://unsplash.com/photos/z4VuRg-ZOEg