Advisory

xHunt Campaign

aeCERT
One of Telecommunications Regulatory Authority (TRA) Initiatives
P O Box 116688, Dubai, United Arab Emirates (UAE)
www.aecert.ae | www.tra.gov.ae

Version: 1.0
Ref: ADV-19-052
Document Date: 24/09/2019

Document Details

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained within this report, aeCERT and the TRA bear no liability or responsibility for any recommendations issued or inadvertent damages that could be caused by the recipient of this information.

Accessing third-party links in this advisory will direct you to an external website. Please note that aeCERT bears no responsibility for third-party website traffic. aeCERT will have no liability to the entities for the content or use of the content available through the hyperlinks that are referenced.

Contents

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a campaign that utilizes previously unknown tools in the targeting of Kuwait-based transportation and shipping organizations. After installing a backdoor, the attacker downloads several different, custom-developed tools to carry out post-exploitation activities. The tools use HTTP for their command-and-control (C2) channels, with certain variants also using DNS tunneling, or emails, to communicate with their C2 channels; in particular, through the use of Exchange Web Servers (EWS) and stolen credentials to create email "drafts" to allow for communication between the attacker and the tool.

Details

The first instance of the campaign activity was observed on May 19, 2019, where a malicious binary called `insetinfo.sys` was detected to have been installed on a system in an organization within the transportation and shipping sector in Kuwait. This file is a variant of a backdoor called Hisoka.

The attacker, having gotten access to the system via Hisoka, deployed two additional tools: Gon – based on `Gon.sys` – and EYE – based on `EYE.exe`. Gon provides the actor with the capability to scan for ports on open remote systems, take screenshots, upload and download files, search for systems in the network, run commands on remotes systems, and establish a Remote Desktop Protocol (RDP) session. The following figure shows the Gon tool being used as a Graphical User Interface (GUI):

The EYE tool, on the other hand, acts like a failsafe for the actor while they are logged into the compromised system via RDP, as it will kill any and all processes established by the attacker and hide identifying artifacts should a legitimate user log in.

On July, 2019, similar activity was monitored in another organization within the same industry. The attacker installed Hisoka version 0.9 – an upgrade from the previous month's version 0.8 – which contained a `netiso.sys` file. This file was observed being moved to another system via the Server Message Block (SMB) protocol.

Another file, called otc.dll, was also moved shortly after, in the same manner. This file is a tool named Killua, which is a backdoor – possibly an enhanced version of the Hisoka backdoor tool – that provides the actor with the capability to issue commands from a C2 server. The commands are run on the infected system by communication with the C2 server via DNS tunneling.

Hisoka Email-Based C2

As stated previously, two versions of Hisoka have been identified – versions 0.8 and 0.9 – that have been installed onto the network of the two Kuwaiti organizations. Both versions had certain command sets incorporated within that enable the actor to control a compromised system. In addition, both versions allow an actor to communicate via a C2 channel through HTTP or DNS tunneling. Version 0.9, however, added the ability for an email-based C2.

The email-based communication capability utilizes Exchange Web Services (EWS) to allow the attacker to communicate with Hisoka. This is done through the use of a legitimate account on an Exchange server. To do this, the malware tries to log into an Exchange server using provided credentials, and uses EWS to send and receive emails to establish communication between the target and the attacker.

Rather than sending and receiving emails like other email-based C2 channels, however, the channel depends on creating email drafts that will be processed by Hisoka and the attacker for data exchange. Using email drafts avoids having emails being received inbound or detected outbound.

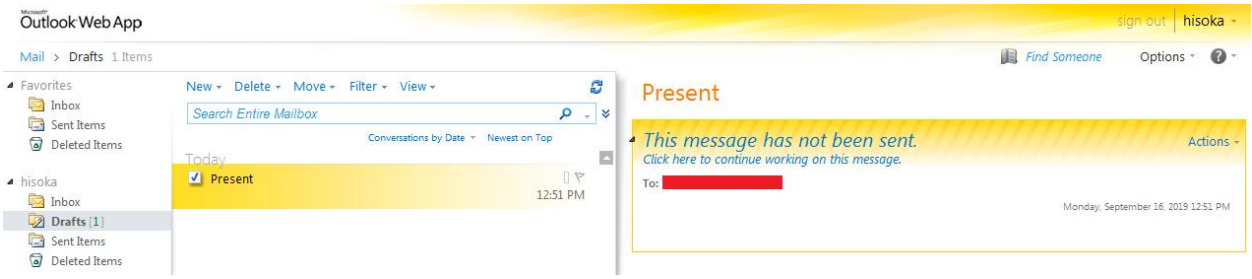
Communication between the legitimate account and the C2 channel that leverages EWS is done over an encrypted channel, as requests to the EWS application programming interface (API) utilizes HTTPS. To enable this email-based C2 channel, the actor provides -E EWS <data> on the command line followed by data, as exemplified below:

```
<username>;<password>;<domain for Exchange server>;<Exchange version
(2010|2013)>
```

It is pertinent to note that the username and password have to be those of a valid account on the Exchange server. By creating a test account called “hisoka” with the password “pass123!”, and considering a hypothetical “mail.test.com” email server, the C2 channel was enabled with the following command:

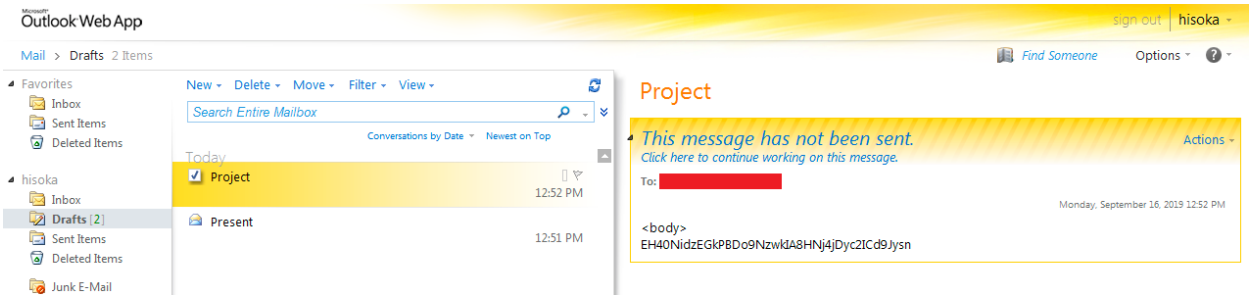
```
hisoka;pass123!;mail.test.com;2019
```

The Hisoka tool then notifies the actor that communication can be established by creating an email draft. This draft acts as a beacon similar to beacon in other C2 channels. A test initial draft can be seen below – note the subject, which is "Present"; the "To" email address; and the empty email body:

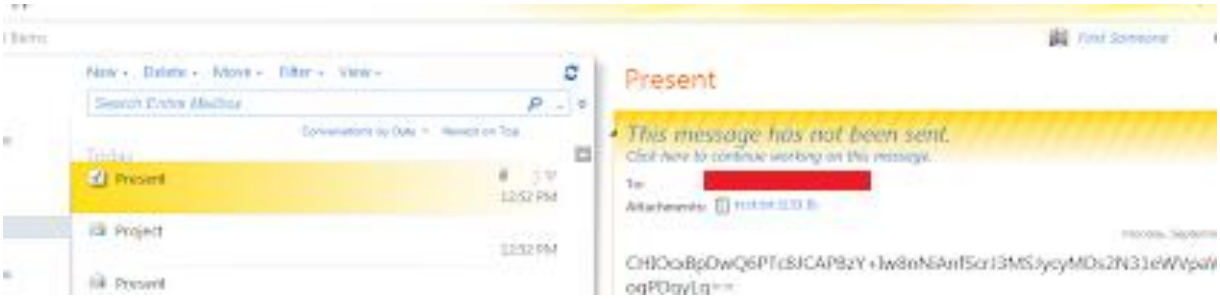


To issue commands, the attacker logs on to the same account and creates another draft: the subject being "Project"; and the message body being specially crafted to contain the command to run as an encrypted string. By analyzing the code, it was seen that the email must contain a base64 encoded ciphertext `<body>` tag. Hisoka then checks for three lines that contain the carriage return character `\r`. It is speculated that the three lines are for the ciphertext, closing the `</body>` tag, and closing the `</html>` tag.

The actor then encrypts the desired command by using the XOR operation on each character with the value 83 (0x53) and base64-encoding the ciphertext. The following screenshot shows a test email created that Hisoka will use to receive a command from:



Once the commands have been parsed and run, Hisoka will create another email draft – with the subject "Present" – that will contain the results of the command, and send it back to the attacker, as shown below:



Further malware analysis has shown similarities between Hisoka and other tools: one tool called Sakabota was identified – which was used in a campaign in mid-to-late 2018. Comparing the two tools and analyzing the two campaigns has shown that Sakabota may be a predecessor to Hisoka, and is very possibly the foundation used to develop the other tools utilized in these campaigns.

Identifying the relationship between the two tools, and conducting more research, has shown that the two tools were configured to use the domain `pasta58[.]com` for the C2 server.

Recommendations

In order to avoid and mitigate the impact of the threat, we highly recommend the following:

- IOC hashes should be blocked
- Communication to the malicious Command-and-Control server should be blocked
- Any communication associated with the IOCs should be monitored and blocked
- Monitor Exchange servers for any suspicious/anomalous activity
- Monitor/Detect for DNS tunneling activity
- Implement more cybersecurity awareness workshops

Indicators of Compromise

The following is a list of the indicators of compromise:

SHA256	Filename	Tool Name	C2
892d5e8e763073648dfebcfd4c89526989d909d6189826a974f17e2311de8bc4	inetinfo.sys	Hisoka v0.8	microsofte-update.com
a5c1974cf23f5659cc588067ac80e56dee2cbd17a4190b719cb77c343935cd7b		Hisoka v0.8	microsofte-update.com
2fd6384af8a6120d7bbd9b6466d4067466e25f31da1951be19289fd0226599a9		Hisoka v0.8	microsofte-update.com
be02188eaa4fb68295508b42578807bdab5fc67c4ea8b08affadb251978ea08a		Hisoka v0.8	microsofte-update.com
2b2d8bdb5e18694810d70facd2b807cbb94f0f3b3b4d11ec998b674ead31456f		Hisoka v0.8	microsofte-update.com
3432ecb711f06deed786ae58ba88a167c15b34b4232cf924fc6a2f6cfc8ef3c9		Hisoka v0.8	microsofte-update.com
ec47f99e9fce7af06e8b11f877aca2351b15362efc0fc91dcc23630a54f3c116		Hisoka v0.8	microsofte-update.com
4fc4b7ae5da0aeb6285edf0ddd07055c1231e718c2fbfd402f0a17da2f1ba31a	netiso.sys	Hisoka v0.9	google-update.com
882b4e810489b61507eb3576e0228030dd12a0e03f0148a82055220412603e37	netiso.sys	Hisoka v0.9	
a78bfa251a01bf6f93b4b52b2ef0679e7f4cc8ac770bcc4fef5bb229e2e888b5	netiso.sys	Hisoka v0.9	learn-service.com
3996efe9a3cf471a1f816287368fa0f99d2cdb95786530b0b61c7b9024ff717b		Hisoka v0.9	
84122b55e5552af1752a00f1a268247feca7e7dbeb4c4cd7b3f5a3005a19fe16	EYE.exe	EYE	
8391c571bffb3ce538ace4d8a3388b28eb486cca5bdab08ab7b568b4e8fc0ec8	Gon.sys	Gon	
a391c5b80a729cc661614f3e64d65cb136eca9900a9025aee3af9a167b38f5c9	smsc.exe	Sakabota	pasta58.com
3314cc701f5c9030622de055879141f6e8c23408029995bd7a88374008aa4390	smscC.exe	Sakabota	pasta58.com
19e3b10056e33fa7559daf8d9a5104ebb313675a2b4daca37bab7da1a49c2e0f	taskhost.exe	Sakabota	pasta58.com
ff0bd8f8dee90ba71a491f17b9fda52c918ef9d3580d562029268a99b7410e19	taskhost.exe	Sakabota	pasta58.com
0ea5565c15303c56c69bbadee462e9c63dbd6ee52f00f187e435af224a48795b	taskhost.exe	Sakabota	pasta58.com
47ca763da840fdee68b97e8d53cbc56b3f90e4d6532f0b1501b90175b8fca24f	smsc.exe	Sakabota	pasta58.com
761635c23f3c98a8d18e48c767fff2b0ec321b58064b404ea1b2b4a555913296	smsc.exe	Sakabota	pasta58.com
b73facbf55053519b5da29397cfd3beea519e9f1bd41c50b6c2f3f1b4eca15a3	smsc.exe	Sakabota	pasta58.com
db1f460f624a4c13c3004899c5d0a4c3668ba99bb1e6be7f594e965c637b6917	smsc.exe	Sakabota	pasta58.com
9a431838f2613454c5630a5f186f0aee240dfc5723bd6e1b586bb4118cc3aab7	smsc.exe	Sakabota	pasta58.com
b9c56da9e911dc85b06f8dc9d1a486663af8f982511e1c3ad568e635e2323274	smsc.exe	Sakabota	pasta58.com
bf7a448ef2603cce5488d97474c913ba14c9550d03cc5e387fe31eb416dc0259	smsc.exe	Sakabota	pasta58.com
cc21bc11d9aed226e9c511480e54bb1305cea086ab0b5e310de68228debdc80e	smsc.exe	Sakabota	pasta58.com
d80aeb4fb326af0bf1179c4fcf2ad01cf98ddab81f709e690bbd728c027064e9	smsc.exe	Sakabota	pasta58.com
d0f57e566c6b457d6e97dc02266d67d81ef561fba50a86e9f9fc889dc5167068	smsc.exe	Sakabota	pasta58.com
df0f874219ffac8038290eb4a39ba6686edc35de8913563f8ddc9644ad4bde64	smsc.exe	Sakabota	pasta58.com
2d7ff8d3aee31cd2f384d74e6b0f07ecda2cea860fb3210c9afe66bc7cc6f90b	smsc.exe	Sakabota	pasta58.com
66e57d2909e37d39791bee91eb9e8121aa48ea89eae8a09275ae078e9dda2f50	smsc.exe	Sakabota	pasta58.com
ea31e5afec3b94635e98473183ec420e9c3e6fd13b618dadb5b34bf5c257a5aa	smsc.exe	Sakabota	pasta58.com
8e18b28dc7351b0e7928b0f5373a6e987ba6d084d84bfd0b29e7f458ca5401e5	smsc.exe	Sakabota	pasta58.com
40b18a1c06888f8e116b6de21f70359b9763b8066c764542ff3816c118b7d482	smsc.exe	Sakabota	pasta58.com

335e9eb0bb571ca81cc6829483f0b8d015627f8301373756d04d844cde04918d	smsc.exe	Sakabota	pasta58.com
5b5f6869d8e7e5746cc9bec58694e4e0049aef0dcac5dfd595322607ba10e1ae	smsc.exe	Sakabota	pasta58.com
7cfd75ab4822b489f74e83d3046536509c44b29b72b43125b0eca1fe449b5953	smsc.exe	Sakabota	pasta58.com
ead4efbc822d2f6351225b35e108100ebef0cdd4b4f3c4762e2ab766ea1ab873		Killua	
18117d1029bad681b1fc28b3bcf3e3dcb63c040d48e369976fb4968376d7195c		Killua	learn-service.com
a49ef5833ed5bf3938f535cf25876555fc0e85bcd278da7227593d9b25d8f65e		Killua	learn-service.com
b63cb7453a835d3af235b6424ffae9ce8b20716c4b35eec6d448d4c95121da69		Killua	
a78bfa251a01bf6f93b4b52b2ef0679e7f4cc8ac770bcc4fef5bb229e2e888b5		Killua	learn-service.com
970f656c3c41d09e674d8da94d66b81cbf7428754780f2a155d400d5e98ca5fa	otc.dll	Killua	
72eeac8fecf392ece7ba0a12ebe02e69dd8d1740ba82f017c87d8a08d71b890b	otc.dll	Killua	
206b735740abf36cd2c3515cfcb9016f65e51cbf4930ddff6abf2e75a07a23d4	msdtd.sys	Netero	
3996efe9a3cf471a1f816287368fa0f99d2cdb95786530b0b61c7b9024ff717b	msd	Netero	
			alforatsystem.com
			winx64-microsoft.com
			6google.com
			windows-updates.com
			windows64x.com
			microsoft-check.com
			firewallsupports.com
			check-updates.com
			sakabota.com
			antivirus-update.top
			traveleasy-kw.com

In addition, the following IP addresses were hardcoded in the file:

- 245.10.10[.]11
- 244.10.10[.]10
- 66.92.110[.]

The last octet of the third IP address mentioned above is used to tell the Hisoka tool how many IP addresses should be treated as data.

Artifacts:

`Z:\TOOLS\Sakabota_Tools\Utility\Micosoft_Visual_Studio_2010_Experss\PRJT\Sync\Sakabota\EYE\EYE\obj\Release\EYE.pdb`

Registry Keys:

```
HKCU\Control Panel\International\_ID: <unique identifier>

HKCU\Control Panel\International\_EndPoint: "learn-service[.]com"

HKCU\Control Panel\International\_Resolver_Server: " "

HKCU\Control Panel\International\_Response: "180"

HKCU\Control Panel\International\_Step: "3"
```

References

Unit 42 | paloalto Networks

---

aeCERT Contact Info

P.O. Box 116688

Dubai, United Arab Emirates

Tel (+971) 4 777 4003

Fax (+971) 4 777 4100

Email incident[at]aeCERT.ae

Instagram @TheUAETRA

Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to incident[at]aeCERT.ae