The Operations of Winnti group

Threat Detection NTT Ltd.

TLP: WHITE

29 April 2021

1. Overview

Threat actor **Winnti Group** tracked by **NTT Security Threat Intelligence analysts** as **Entity-1 (ENT-1)** is a highly active group with many parallel operations mainly targeted towards entities in Asia. The definition and classification of activity originating from the Winnti group diverge between various security companies, what we label as ENT-1 in this report overlaps activity classified by ESET and Dr Web as Winnti group in recent reporting [1][2][5].

The aim of this report is to offer a glimpse into the continuous Threat Intelligence efforts NTT Security are committed to on behalf of our clients, while also reporting on previously unreported aspects of the ENT-1 group in contribution to the security-communities effort of laying the puzzle of ENT-1 activity.

This research has been possible by harnessing NTT's owned and operated global tier-1 IP backbones, together with correlation of data from targeted customers, internal research and open source intelligence (OSINT).

The timespan of this research is from December 2020 to April 2021 where the following countries and regions has been observed as targets:

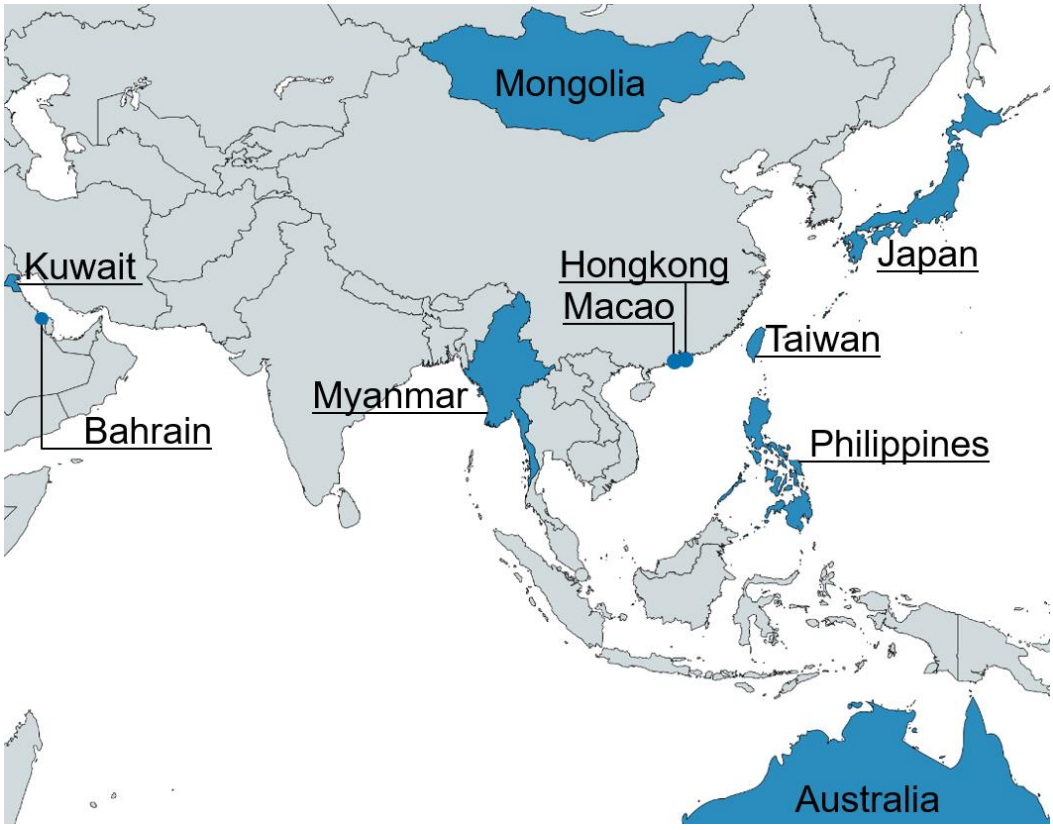

Figure 1 Targeted countries and regions December 2020 to April 2021

2. Daily operations

Analysis of traffic towards ENT-1 infrastructure shows that the group is active during office-hours in time zone UTC+6. Weekends normally lack any activity implying that the group is truly a full-time funded APT group.

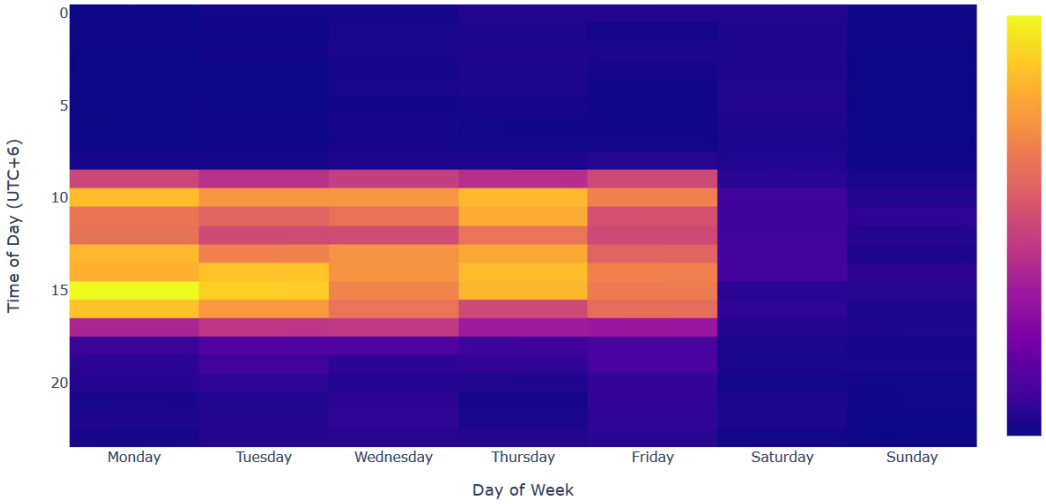

Figure 2 Intensity of ENT-1 activity in UTC+6

The groups daily operations include the exploitation of servers running the GlassFish Server software version 3.1.2 and below as means for easy infrastructure expansion. The exploited servers are then utilized during their operations:

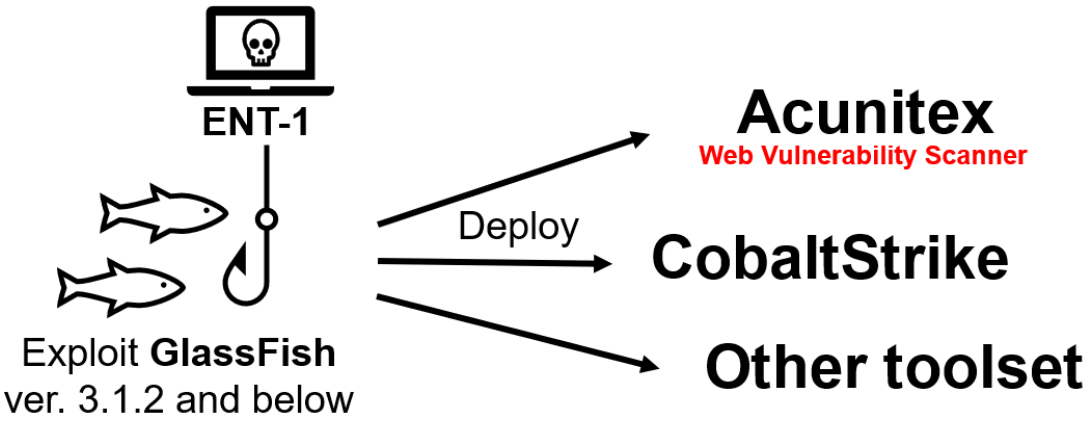

Figure 1 ENT-1 GlassFish Workflow

Commonly deployed software includes the Web Vulnerability Scanner Acunitex and the command-and-control product CobaltStrike.

3. Acunitex activity

The web vulnerability scanning activity covers geographical sectors and industries typically associated with the ENT-1 interest sphere. Our observation is a strong focus on the Media sector located in Hong Kong, Taiwan, and Japan. Travel and

Transportation companies operating out of Hong Kong. Government infrastructure in Australia, Mongolia, Myanmar, Vietnam, Japan and Macao. Universities and telecom operators in Bahrain and Kuwait have also been targeted.

Figure 3 Targeted industries

While the scanning is targeted in respect to sector and geographical location it also appears to be opportunistic. Organisations which have been scanned by any of the Acunitex IPs listed in the IOC section should expect and protect from further intrusion attempts performed by ENT-1 and/or related APT groups which possibly have been provided with the same target list.

4. CobaltStrike infrastructure

The CobaltStrike infrastructure shows different variations of customization where publicly available (malleable) or default profiles are sometimes used but also more advanced methods are observed. Typosquat domains and certificates are commonly utilized to make the traffic blend in. For example, a self-signed certificate imitating Microsoft on 141.164.62.81 over port 443:

```
Issuer: C=USA, ST=Ags, L=Ags, O=Micorsoft Corp, OU=Mic, CN=Micorsoft Corp
Validity
    Not Before: Dec 25 03:28:47 2020 GMT
    Not After : Dec  1 03:28:47 2120 GMT
Subject: C=USA, ST=Ags, L=Ags, O=Micorsoft Corp, OU=Mic, CN=Micorsoft Corp
```

Figure 4 Self signed certificate on C2

The CobaltStrike Command and Control (C2s) are often observed on compromised Glassfish servers. This could be due to CobaltStrike being utilized as the first layer backdoor during campaigns where the more well-known ENT-1 utilized backdoors such as Shadowpad, Spyder and the Winnti backdoor are deployed as a second stage payload on interesting victims. This behaviour indicates that the Glassfish servers are seen as use-and-throw away C2s.

More ambitious efforts of CobaltStrike usage is a custom stager called **Fishmaster** according to the embedded PDB path:

C:\Users\test\Desktop\fishmaster\x64\Release\fishmaster.pdb

Figure 5 PDB path for Browser_Plugin.exe

Avast classifies the sample as “Win64:BidenHappy-A [Apt]”, likely due to the embedded string:

Address	String
0x1400257e8	Bidenhappyhappyhappy

Figure 6 Embedded string in Fishmaster sample

The sample were hosted at hxxps://jquery-code[.]ml/Download/Browser_Plugin.exe and at the index page of the domain the html loads an iframe of code.jquery.com in order to appear legitimate:

view-source:https://jquery-code.ml/

```
</html>
<head>
<title>jQuery CDN</title>
</head>
<body>
<iframe src="https://code.jquery.com/index.php" frameborder="0"
</body>
</html>
```

Figure 7 Observed iframe usage

The stager will request a pdf from a Cobalt Strike C2 on the URL path hxxp://37.61.205[.]212:8880/dow/Aili.pdf and store it to “C:\Users\Public\Aili.pdf”. The pdf holds a job-application in Mandarin for a Vietnamese individual:

申请职位 Position:

一、个人基本情况 Personal Particulars								
姓名 Name	艾丽	性别 Sex	女	民族 Race	越南	年龄 Age	28	
身份证号 ID No.	272160266			婚姻状况 Marital Status		单身		
身高 Height	158cm	体重 Weight	47 公斤	出生日期 Date Of Birth		1993/07/29		
最高学历 Educational Level		大学本科		外语程度 Foreign language		英语基本交流		
联系电话 Contact Phone				QQ NO. :				

Figure 8 Job application

Secondly the stager will request the CobaltStrike related destination hxxp://micsoftin[.]us:2086/dow/83.dmp, part of the response is XOR encoded with the key “misgat_mg” which the stager will decode and executed as shellcode. We have been unable to download the 83.dmp payload but explain the payload structure below:

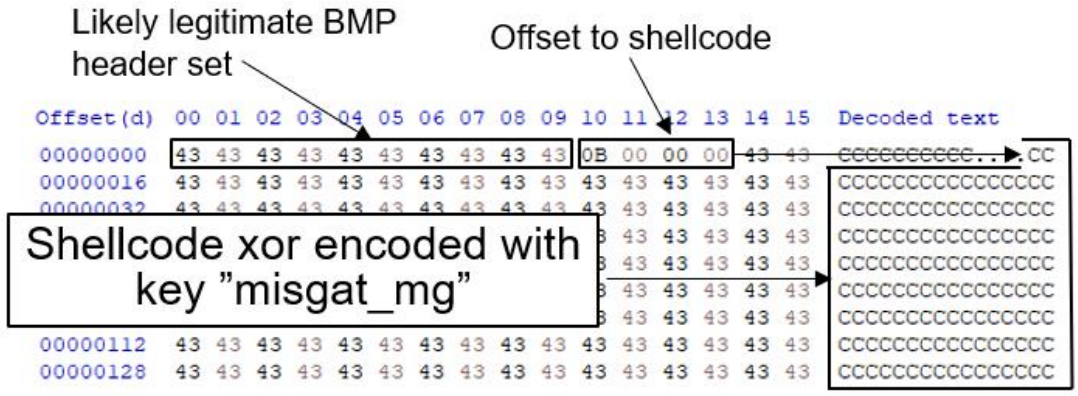

Figure 9 Format of likely CobaltStrike beacon payload

The use-case behind the downloaded pdf is unknown and we encourage fellow researchers to explore it in depth for the possibility of it holding command and control traffic. The adoption of Fishmaster still appears relatively low and it remains to be seen if it will become an integral of the groups toolset.

5. Shadowpad, Spyder and Winnti backdoor utilization

ENT-1 extensively use Shadowpad, Spyder and the Winnti backdoor for long-running operations. It is not unseen that the group keep on using domains and IPs even after they have publicly been reported, for example the following domains are still actively used even though they are publicly reported:

- livehost[.]live (Reported by ESET 31th Jan 2020 [1], still utilized Apr 2021)
- symantecupd[.]com (Reported by PTSecurity Jan 2021 [3], still used Apr 2021)

ENT-1 has also utilized snoc.hostingupdate[.]club which is reported by Dr Web as a Spyder C2, Spyder is a backdoor reported to be utilized by Winnti Group [5].

Given the large infrastructure overlaps and shared toolset utilization NTT Threat Detection assess ENT-1 to be part of Winnti Group.

6. Breadcrumbs from other payloads

The likely GlassFish exploited server 168.138.137.235 appears to have been utilized as hosting-grounds for ENT-1 payloads. On Virustotal some samples are uploaded, among them a malicious lnk shortcut named *“Business Registration_JHUAN SHUN MOTOR CO., LTD.pdf.lnk”* targeted towards a Taiwanese entity.

Another clue towards Taiwanese targeting is a previously hosted self-extracting archive with “TW” in the filename:

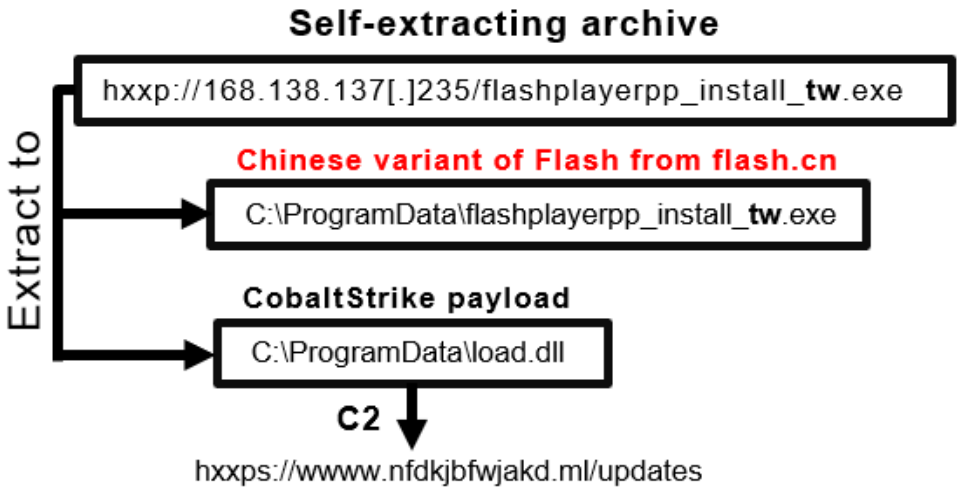

Figure 10 flashplayerpp_install_tw.exe execution flow

7. Conclusion

ENT-1 shows signs of being a full-time funded APT group with a continuously diversified toolset and a growing network infrastructure to support their operations.

8. How NTT Can help

NTT Security Threat Intelligence researchers are monitoring **telemetry of suspicious traffic** traversing our Global IP Network Service global tier-1 IPv4/IPv6 backbone network for threat indications. Correlating such findings with the insights of our global Advanced Threat Detection (ATD) and Managed Detection and Response (MDR) services enable a truly unique and global perspective of the continuously evolving cyber security threat landscape.

Research findings on threat actors and campaigns, such as **ENT-1,** are continuously being feed from our Threat Intelligence analyst back into our services as Machine-Learning capabilities, Behaviour models, Indicators-of-Compromise(IOC)’s and Threat Intelligence. Enhancing the services ability to efficiently Monitor, Detect, Triage and Respond to these threats on behalf of our clients. Often without depending on an initial compromise.

For further information on NTT Security Services please contact your local account manager or visit our website here.

References

[1] https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/

[2] https://news.drweb.com/show/?i=14154&lng=en

[3] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/higaisa-or-winnti-apt-41-backdoors-old-and-new/

[4] https://news.drweb.com/show/?i=14048&lng=en

[5] https://st.drweb.com/static/new-www/news/2021/march/BackDoor.Spyder.1_en.pdf

Indicators of compromise for Entity 1:

Acunitex scanners, most of which are compromised Glassfish servers:

101.53.136.36
116.203.104.216
202.73.97.91
186.250.242.178
186.250.242.178
107.170.109.82
67.205.143.19
107.161.183.116
45.33.100.13
206.189.69.127
95.111.245.74
192.99.169.235
64.227.20.224

169.61.11.68

CobaltStrike C2s:

198.98.62.191
83.169.3.55
141.164.62.81
160.16.208.58
37.61.205.212
93.180.156.77

Shadowpad C2s:

45.76.100.224
207.148.72.133
45.77.107.26

Winnti backdoor C2s:

139.180.141.227
154.212.129.30

Related domains

micsoftin.us
google-images.ml
lmgur.me
nfdkjbfwjakd.ml
jquery-code.ml

hostingupdate.club
symantecupd.com
livehost.live

Related files

Business Registration_JHUAN SHUN MOTOR CO., LTD.pdf.lnk	550425bd3474f729c0cf1b1c131fb011
flashplayerpp_install_tw.exe	5dfb7f863cd291544b9dfdb3de25162f
Browser_Plugin.exe	738f46546f6d4a79e2d917b26bf8a93a
download.dat	0fab8fa2ef340a93f0b062d575ade5b7
Aili.pdf	a465f18c7e50500c6b6f94741ef56b2f

About Security and NTT Ltd.

Security is a division of NTT Ltd., a global technology services company. The Security division helps clients create a digital business that is secure by design. With unsurpassed threat intelligence, we help you to predict, detect, and respond to cyberthreats, while supporting business innovation and managing risk. Security has a global network of SOCs, seven R&D centers, over 2,000 security experts and handles hundreds of thousands of security incidents annually across six continents. Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology.

NTT Ltd. partners with organizations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital, and secure. As a global ICT provider, we employ more than 40,000 people in a diverse and dynamic workplace, and deliver services in over 200 countries and regions. Together we enable the connected future. Visit us at our new website hello.global.ntt