

Threat Activity Report: APT32 Using Asia-Europe Meeting as Lure to Conduct Intelligence Collection with METALJACK

Fusion (FS)

Cyber Espionage (CE)

July 03, 2020 10:47:00 AM, 20-00012668, Version: 1

Executive Summary

- **Delivery Method:** Probably spear-phishing email
- **Exploitation:** CVE-2017-11882
- **Malware Family:** METALJACK
- **Suspected Targets:** Cambodia and Asia-Europe Meeting (ASEM) Attendees
- **Suspected Attribution:** APT32

Threat Detail

On June 11, 2020, Mandiant Threat Intelligence identified an exploit document titled "Report_4th National Commission Meeting for ASEM preparation.doc" (MD5: dba71108565e663979a0442ba046ad51). Asia-Europe Meeting (ASEM) is an intergovernmental summit aimed at fostering dialogue and cooperation between Asian and European countries. We believe the lure was used in relation to the ASEM meeting taking place in Cambodia in November 2020. As a result, we suspect the meeting attendees and Cambodia to be the targets of this operation.

The sample ultimately infects its hosts with [METALJACK](#), a malware we attributed to the Vietnam-nexus group [APT32](#) (for further details see [18-00009067](#)). Unlike previous APT32 operations, which can have complex execution flows, this attack is comparably simple, with no other artifacts to create the instance of METALJACK.

Lure

Despite the title being likely of interest to the victim, the document is blank.

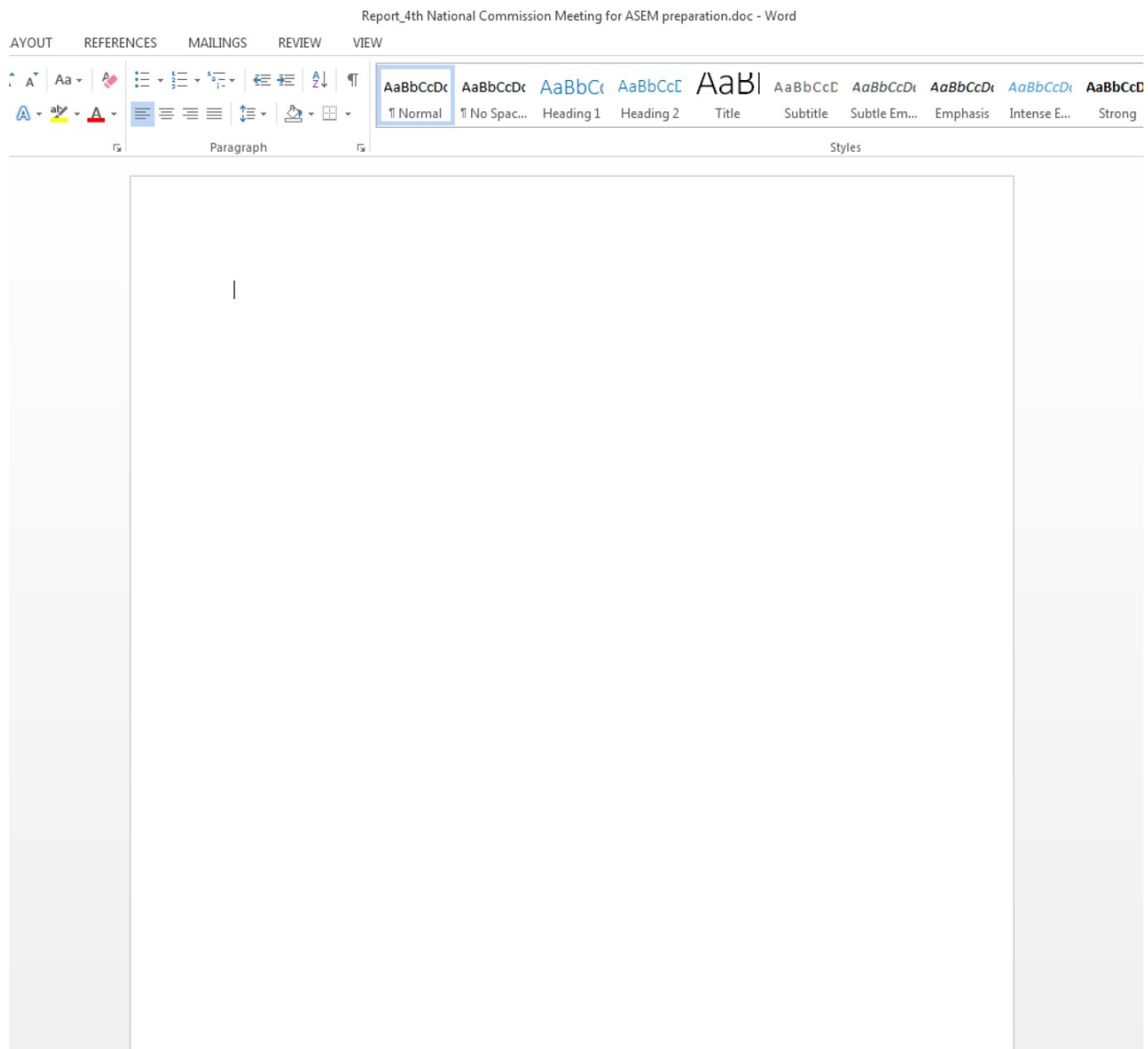


Figure 1: Blank lure document

Attribution

METALJACK is a malware proprietary to the Vietnam-nexus group APT32 ([18-00009067](#)). We previously observed APT32 targeting Vietnam's neighboring countries, including Cambodia ([19-00008978](#) and [18-00012896](#)). Furthermore, this METALJACK sample supports multiple networking protocols, a feature that has been observed in APT32's arsenal at least since 2018. Given these reasons, we attribute this operation to APT32 with high confidence.

Notably, this attack might not only show APT32's interest in Cambodia, but potentially in other ASEM members. Compromising Cambodia, the host country of the summit, would allow the threat actors to easily collect ASEM-related intelligence or even use the compromised target as a steppingstone to attack other participating countries.

Technical Annex

File Information

- **Filename:** Report_4th National Commission Meeting for ASEM preparation.doc
 - **MD5:** dba71108565e663979a0442ba046ad51
 - **Creation time:** 2020:06:17 13:39:16
 - **Description:** The CVE-2017-11882 exploit document
 - **C&C:** qwertyu.mentosfontcmb.com

Execution

Once the Equation editor exploit is triggered, the shellcode terminates the Word process running the initial exploit document, deletes the exploit document, and replaces it with a clean one (MD5: 0071f41c46662e20b1264f09bba40d8e).

Instead of making new artifacts, the shellcode directly injects the loader inside the Equation editor process "EQNEDT32.EXE" and creates an instance of METALJACK inside the same process in memory. This METALJACK sample reports to the C&C server "qwertyu.mentosfontcmb.com," which resolved to the IP address "139[.]162[.]111[.]226" at the time of analysis.

Network Communication

After successful execution, the malware makes the following callback to the C&C server "qwertyu.mentosfontcmb.com" via port TCP/46405 using a custom protocol.

<<VICTIM to C&C>>

```
00000000 19 00 00 00      ....
00000004 fa 10 9f b2 4a 55 a9 58 54 33 58 08 df 81 c4 19 ....JU.X T3X....
00000014 55 85 d7 9d 1b 75 fb a5 f0      U....u.. .
```

<<C&C to VICTIM>>

```
00000000 3f 00 00 00 80 02 00 00 a3 59 f2 6e f4 d5 3a fb ?..... .Y.n... 00000010 f9 e4 fa ab
b0 2e d7 b5 2c d7 91 c6 22 41 10 49 ..... ,..."A.I
00000020 11 fa f2 cb 33 73 eb 81 a2 ee ac 9e 94 59 f5 62 ....3s.. ....Y.b
00000030 ac 54 01 04 39 4f a8 b4 ee 9c 2f e3 ad 13 9d fd .T..9O.. ..../.....
00000040 f8 95 c4      ...
```

The malware can switch to other protocols when a port is not available. For example, we observed it supporting DNS tunneling.

<<VICTIM to C&C>>

```
00000000 30 73 01 00 00 01 00 00 00 00 00 00 07 71 77 65 0s.....
.....qwe
00000010 72 74 79 75 0d 6d 65 6e 74 6f 73 66 6f 6e 74 63 rtyu.men tosfontc
```

00000020 6d 62 03 63 6f 6d 00 00 01 00 01	mb.com.. ...
---	--------------

Related Samples

- **Filename:** 36 ASEAN Summit 26-06-2020 Conference.doc.exe
 - **MD5:** 7579aede6a223c96231ad30472a060db
 - **Creation time:** 2019-02-24 19:03:32
 - **Description:** A malicious executable masquerading as an Office document delivering METALJACK, which shares the same parent domain and IP with the origin sample.
 - **C&C:** tripplekill.mentosfontcmb.com (resolves to 139[.]162[.]111[.]226)

Threat Activity Reports are a quick examination of activities observed within the cyber threat environment, typically to expand coverage on important topics, reinforce a trend, or support other intelligence products. If present, reliability (A-F) and credibility (1-6) scores are based on the NATO System and reflects source confidence based on prior history, not judgements about the veracity of any specific claims. We welcome feedback with questions, additional findings, or simply an indication of interest.

[Please rate this product by taking a short four question survey](#)

First Version Publish Date

July 03, 2020 10:47:00 AM

Threat Intelligence Tags

Source Geography

- Vietnam

Affected Industry

- Government - National
- Government - Subnational

Tactics, Techniques And Procedures(TTPs)

- Communications
- Exploit Development
- Malware Propagation and Deployment

Target Geography

- Cambodia

Actor

- APT32

Targeted Information

- Government Information

Malware Family

- METALJACK

Technical Indicators & Warnings

Domain:	tripplekill.mentosfontcmb.com
Actor:	APT32
Malware Family:	METALJACK
Network Type:	network
Identifier:	Attacker
Domain:	qwertyu.mentosfontcmb.com
Actor:	APT32
Malware Family:	METALJACK
Network Type:	network
Identifier:	Attacker
IP:	139[.]162[.]111[.]226
Identifier:	Related
Network Type:	network
SHA1:	4e78cc2ea55582926f6fc5b19ae1d6dc2c8fec1d
Identifier:	Attacker
Actor:	APT32
File Name:	report_4th national commission meeting for asem preparation.doc
Malware Family:	METALJACK
File Size:	1550103
SHA256:	1aebbaf54fb568cba07687704f91a718cfcf5bab6fb550542287134f893cc79d
Type:	text/rtf
MD5:	dba71108565e663979a0442ba046ad51
SHA1:	db336d7738e982b3b0a904329cb6da4f23d42858
Identifier:	Related
File Name:	Report_4th National Commission Meeting for ASEM preparation 2.doc
File Size:	13462
SHA256:	9c9575f866c33d324d3483c9adaa29247d1319ed0a760964af9964c422c784b6
Type:	application/x-docx
MD5:	0071f41c46662e20b1264f09bba40d8e
SHA1:	4a41bc81b27374b8a711794a7b27d51700403341
Identifier:	Attacker
Actor:	APT32
File Name:	36 asean summit 26-06-2020 conference.doc~.exe
File Size:	2143611
SHA256:	dbde2b710bee38eb3ff1a72b673f756c27faa45d5c38cbe0f8a5dfccb16c18ba
Type:	application/x-dosexec

MD5: 7579aede6a223c96231ad30472a060db

Common Vulnerabilities and Exposures

CVE ID: CVE-2017-11882([NVD Description](#))External Link

Version Information

Version:1.0, July 03, 2020 10:47:00 AM

Threat Activity Report: APT32 Using Asia-Europe Meeting as Lure to Conduct Intelligence

Collection with METALJACK



5950 Berkshire Lane, Suite 1600 Dallas, TX

75225

This message contains content and links to content which are the property of FireEye, Inc. and are protected by all applicable laws. This cyber threat intelligence and this message are solely intended for the use of the individual and organization to which it is addressed and is subject to the subscription Terms and Conditions to which your institution is a party. Onward distribution in part or in whole of any FireEye proprietary materials or intellectual property is restricted per the terms of agreement. By accessing and using this and related content and links, you agree to be bound by the subscription .

For more information please visit: https://intelligence.fireeye.com/reports/20-0001266_8

© 2020, FireEye, Inc. All rights reserved.