Pulse Report:
New APT32 Malware Campaign Targets Cambodian Government

Recorded Future's Insikt Group has discovered a new malware campaign targeting the Cambodian government using an Association of Southeast Asian Nations (ASEAN)-themed spearphish. Using Recorded Future RAT controller detections and Network Traffic Analysis, Insikt Group identified new operational infrastructure that we attribute to the Vietnamese state-sponsored threat activity group APT32, also known as OceanLotus. This assessment is also supported by the identification of several Cambodian victim organizations communicating with this infrastructure, and aligns with previous campaigns targeting these organizations.

History

Vietnam and Cambodia have a long history of conflict, dating back to the Sino-Vietnamese War of the 1970's, when Vietnam began retaliatory attacks on China's "little brother," Cambodia. In 2017, Vietnam started strengthening its cyber warfare capabilities with the formation of APT32, which targeted ASEAN's website during the 2017 annual summit, as well as targeting websites of ministries or government agencies in Cambodia, Lao PDR, and the Philippines.

In recent years, the relationship between Vietnam and Cambodia has deteriorated in part because of China's Belt and Road Initiatives (BRI) in the region. As Cambodian Prime Minister Hun Sen has grown closer to Chinese President Xi Jinping, the two have strengthened the partnerships between the two countries, pushing Vietnam out of critical regional cooperatives. Chinese investments in Cambodia include critical infrastructure, joint military exercises in the South China Sea, and a new property development just North of Ream Naval Base, strategically located on the Gulf of Thailand between Vietnam and Cambodia.

New APT32 Infrastructure

In June 2020, Insikt Group reported on new APT32 operational infrastructure identified through a proprietary method of tracking malware activity associated with APT32, such as METALJACK and DenisRAT. Using this same methodology, Insikt Group has continued to identify new, active APT32 IP addresses and associated domains.

Insikt researchers discovered several samples that are a part of this campaign:

Sample 1: The first sample is delivered via a malicious document titled, "បញ្ជីឈ្មោះនាមអនុព័ន្ធយោធាបរទេសនិងការិយាល័យសហប្រតិបត្តិការយោធាប្រចាំកម្ពុជា.docx~[.]exe", which translates to "List of Foreign Military Attachments and Office of Military Cooperation in Cambodia.docx~[.]exe". This sample, likely delivered via spearphishing, is a self-extracting archive (SFX) containing four files:

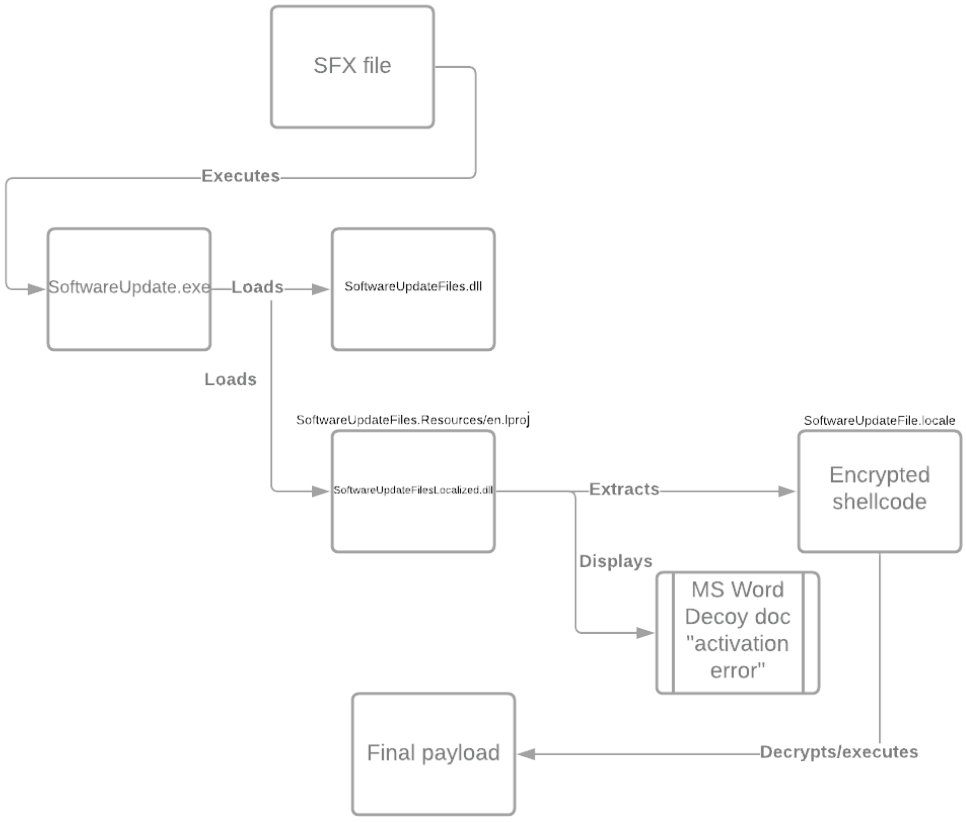
1. A legitimate executable signed by Apple (SoftwareUpdate.exe).

2. A related benign dynamic link library (DLL) file (SoftwareUpdateFiles.dll).

3. A malicious DLL (SoftwareUpdateFilesLocalized.dll).

4. A file named “SoftwareUpdateFiles.locale” containing encrypted shellcode.

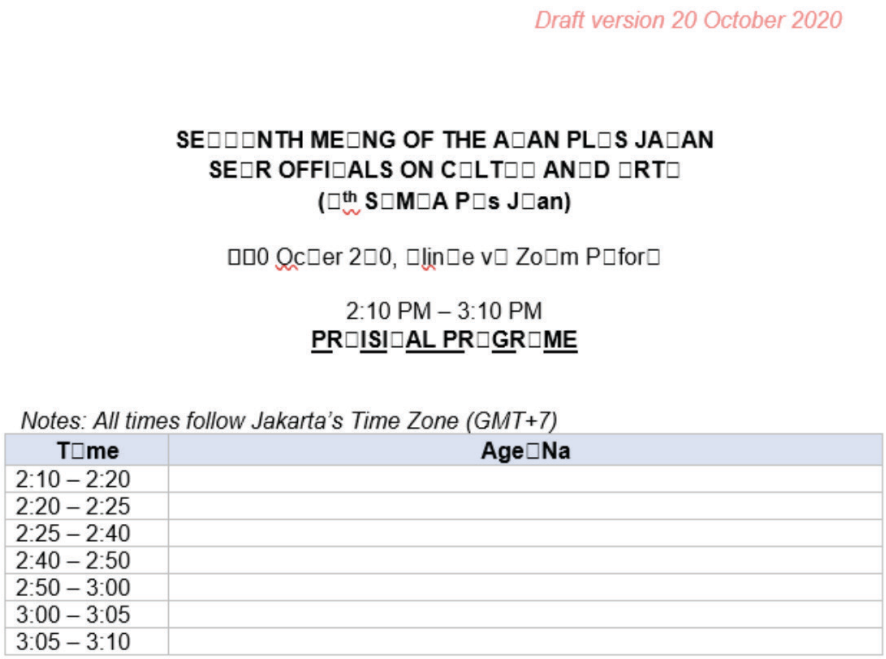
Upon execution of the SFX, the Apple executable loads the benign DLL before loading the malicious DLL, which is stored in the SoftwareUpdateFiles.Resources/en.lproj file path. The malicious DLL then extracts the encrypted shellcode from the SoftwareUpdateFile.locale file and decrypts and executes it, while displaying a decoy document to the user (an Microsoft Word document displaying an “activation error”), eventually loading the final payload.



This loading process matches APT32 activity previously reported by Insikt Group and Ahnlab in relation to an APT32 sample referencing the 2020 ASEAN Summit. Further analysis of these artifacts for identification of the malware family is ongoing within Insikt Group and updates will be posted as more samples are analyzed.

Sample 2: A second sample, uploaded to a malware repository on October 22, 2020, uses this same loading process and communicates with one of the identified C2 domains, cloud.bussinesappinstant[.]com.

In this sample, the SFX file is called "9_Programme_SOMCA-Japan_FINAL.docx~.exe", likely in reference to the ASEAN Senior Officials Meeting for Culture and Arts (SOMCA), indicating APT32's continued interest in the targeting of ASEAN and other member states.



Draft version 20 October 2020

SE□□□NTH ME□NG OF THE A□AN PL□S JA□AN
SE□R OFFI□ALS ON C□LT□□ AN□D □RT□
(□th S□M□A P□s J□an)

□□0 Qc□er 2□0, □lin□e v□ Zo□m P□for□

2:10 PM – 3:10 PM
PR□ISI□AL PR□GR□ME

Notes: All times follow Jakarta's Time Zone (GMT+7)

T□me	Age□Na
2:10 – 2:20	
2:20 – 2:25	
2:25 – 2:40	
2:40 – 2:50	
2:50 – 3:00	
3:00 – 3:05	
3:05 – 3:10	

Decoy document utilized in this campaign shows a blank agenda for the "Seventh Meeting of the ASEAN Plus Japan Senior Officials on Culture and Arts. (Source: Recorded Future)

This archive file drops the same "SoftwareUpdateFilesLocalized.dll" file seen in the previous sample. In addition to the TTP (tactics, techniques, procedures) and infrastructure overlaps, the malicious DLLs linked to this latest sample share an identical rich header and import hash seen in historical APT32 samples.

Insikt Group identified further evidence of targeting of Cambodia through several IP addresses assigned to a Cambodian government organization regularly communicating with the APT32 C2 IP address 43.254.132[.]212.

Recorded Future recommends using the following indicators of compromise from this campaign for detection and defense against this malware. Additionally, Insikt Group has provided a YARA rule for detection, below.

For more insight into state-sponsored cyber threats, visit www.recordedfuture.com/category/research/

Appendix A: Indicators of Compromise

IP Address	Domain
43.254.132[.]117	bussinesappinstant[.]com, cloud.bussinesappinstant[.]com, query.bussinesappinstant[.]com
43.254.132[.]212	insappstaticanalyze[.]com, dns.insappstaticanalyze[.]com

Malware Hash	Malware Description
a030435018a67c07747751766132eb30a9a6bb6af161df225a27c0ec57156b61	Sample 1 parent SFX file
d873bdb08c45378650761bad71df7418c7b542adb13ccd4a87df2001801f4808	SoftwareUpdateFilesLocalized.dll
625f5253e306cce30da4dbff2a6ade608ca295b10d086b9eaaec4743e53b0c82	File named “SoftwareUpdateFiles.locale” containing encrypted shellcode
Dbde2b710bee38eb3ff1a72b673f756c27faa45d5c38cbe0f8a5dfccb16c18ba	APT32 sample referencing the 2020 ASEAN Summit
47ba92dc8c9302b2f70db70a0d46fef0ee2972edc3e1c4b637d5c76b4141c7a0	Sample 2 parent SFX file
75c61d9d8da4a87882ccdd37b664953c10a186b5545c5152fd1b6bf788a1a846	Historical Related APT32 Sample
cfbacb8a1ca087810d17d86fcf94d9c660cf3331ccb0b015709bb48a9adb1cc7	Historical Related APT32 Sample

Appendix B: YARA Detection

```
import “pe”
rule APT_VN_APT32_DLLSideloading_Oct2020
{

        meta:
            description = “Track DLL Sideloading Technique Used by APT32/OceanLotus in October 2020”
            author = “Insikt Group, Recorded Future”
            hash1 = “d873bdb08c45378650761bad71df7418c7b542adb13ccd4a87df2001801f4808”
            hash2 = “75c61d9d8da4a87882ccdd37b664953c10a186b5545c5152fd1b6bf788a1a846”
    date = “2020-10-22”

        strings:
            $s1 = “SoftwareUpdateFilesLocalized.dll”
            $s2 = “SoftwareUpdateFiles.locale” wide
            $s3 = “This indicates a bug in your application.”

        condition:
            uint16(0) == 0×5a4d and filesize < 60KB
            and ((all of them and pe.timestamp == 4294967295000)
            or pe.imphash() == “3937374c70baa93e1fd75d8e894faf94”
            or pe.rich_signature.key == 0×6597ead6)
}
```