Analysis on Sidewinder APT Group - COVID-19 - Rewterz

Published: 2020-06-22 · Archived: 2026-04-06 15:48:18 UTC

Introduction

Hardcore Nationalist group SideWinder is a threat group active since 2012 according to Kaspersky. This group mainly targets Pakistanis and Chinese military & government entities' windows machines. They also target mobile phone devices. This is the second time this group is using COVID-19 theme to lure victims, thereby capitalizing on the fear of global pandemic. Sidewinder aka HN2 is believed to be an Indian state sponsored group. A detailed analysis of SideWinder attacks on Pakistani military officials was also published in April.

MITRE ATT&CK Table

Figure 1: SidWinder Mapping Attack Categories with MITRE ATT&CK

Analysis of SideWinder APT Group

File Identity

Property	Value
File Name	OnlinePolicyGuide.pdf
File Type	PDF
File Info	PDF document, version 1.5
File Size	102.70 KB (105160 bytes)
MD5	8ae9cc797c2f3ec3eca3b54a2e70edf1
SHA-1	6c878840bd899936974a0364a2297b658beaeda9
SHA-256	65c42fef3df4a2b4974e9a1c907fa79b6c2cd96406c309b0963f358fc4a7c23a
Virus Total Score	0/61
Hybrid Analysis Score	More than 10% Risk Factor

Property	Value
File Name	file.hta
File Type	HTML executable file
File Info	HTML document ASCII text
File Size	322.46 KB (330200 bytes)
MD5	30398787041EFA25E1632A29D4F7730B

SHA-1	6B0B86897990A254F2FE4C6DF869A1276F10B407
SHA-256	36b653ede8d68fbb9a9343507aa437125e5915655fe12763dbb109c97bed617b
Virus Total Score	3/60
Hybrid Analysis Score	More than 16% Risk Factor

Property	Value
File Name	rekeywiz.exe
File Type	Win32 EXE
File Info	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File Size	322.46 KB (330200 bytes)
MD5	082ed4a73761682f897ea1d7f4529f69
SHA-1	4f77bda9714d009b16e6a13f88b3e12caf0a779d
SHA-256	fa86b5bc5343ca92c235304b8dcbcf4188c6be7d4621c625564bebd5326ed850
Virus Total Score	0/70
Hybrid Analysis Score	More than 10% Risk Factor

Summary of Analysis

As per the analysis of the file received by the Air University Online Teaching Intimation, the artifacts found belong to a well-known Indian SideWinder APT group. This APT group has been working in the interest of Indian government, targeting Pakistani government officials through their latest campaign with a decoy document related to online teaching during COVID-19 pandemic.

Figure 2: Dependency Flow of Malware File

Figure 3: Malware File Basic Properties

Characteristics

The following characteristics were found during the analysis:

1. When the victim opened the PDF file, it was observed that the PDF downloaded another decoyed document over HTTP (.hta file) in the background from the URL below.

”http://www.au-edu.km01s.net/cgi/8ee4d36866/16914/11662/eeef4361/file[.]hta.

After reviewing the PCAP file as shown below:

2. Once an HTA file is downloaded in the victim system, it then drops another payload from the URL to encrypt certain files and folders mentioned below.

a) As per the source code review of .HTA file, it was found that the file contains JavaScript obfuscated code with the encoding of base 64. In order to de-obfuscate the source code, we have to decode the encoded parameters first.

i) First, we decoded the key value, to decode the completely obfuscated code parameters.

b) After decoding the key value, we get the ASCII String “3110648411” in strings from the following line:

c) Now we can use the main key to decode the whole parameters of this JavaScript code. After using the key, we move towards the decoding of Var X Function encoded parameters.

We have found the URL http://www.au-edu.km01s.net/plugins/16914/11662/true/true[/] which means this hta file is also trying to communicate on the suspicious link and the line in the encoded format is defined below:

d) On further decoding from the code we have found that this file is intended to create another process instance in line mentioned below

e) After observing the above characteristics, we have searched for the exact file parameters. We found that the source file tried to create another file in the directory of “temp” with an anonymous name having the extension of .hta with the usage of mshta.exe process. As you can see in the hex view of decoded parameter taken from the line of Var SO:

f) The same hex value is found with another process i.e. intended to drop in the directory after its creation as shown in the image below:

g) In addition, after some other lines we have found that there is another process “csc.exe” is called in the parameter, which is used to perform CLI based compilation.

h) It also uses “ActiveXObject” utility to help in its execution through Microsoft products and internet browsers. The ActiveXObject object is used to create instances of OLE Automation objects in Internet Explorer on Windows operating systems. Several applications (Microsoft Office Word, Microsoft Office Excel, Windows Media Player, etc) provide OLE Automation objects to allow communication with them.

Hence, It was identified that the attacker used multiple obfuscation techniques, which are techniques used by attackers to hide the attack, to avoid detection and to make it difficult to decode the key string and actual payload and command instruction.

3. Static analysis of rekeywiz.exe revealed that it uses built-in function “ShellExecuteW” in which the document name is passed in lpfile parameters for which the execution will be performed as shown below.

4. Further analysis concluded that the rekeywiz.exe was also using another function which is used for the encryption of file system, named as “SetUserFileEncryptionKeyEx”. The purpose of this function is to encrypt the files and folders:

Dependencies:

Following are the dependencies observed in the malware code and required user interaction for execution.

1. It was observed that this malware didn’t provide Auto Run/Auto Execute functionality. However, the victim needs to manually open the pdf to execute and download the other .hta and payload.
2. This malware was designed and is compatible with the Windows environment only. Otherwise, it is useless.
3. Hta file is also dependent on the Microsoft .Net Framework v2.0.50727 / v4.0.30319.
4. Reykeywiz.exe dropper file needs to create its entity in the registry entries of Remote access service address.

Following is the complete process-working graph for this attack.

Behavioral Findings through Analysis

Following are the behavior of the malicious files,

- When the victim opens the pdf document, it shows all the information about the notification related to policy guidelines, which are for the online classes going to be held in Air University. The display below further clarifies it.

In the background, it makes a connection with a suspicious IP Address “185.163.45.199” to download .hta & Payload.

- After fetching the .hta file, it needs to be opened and once it accidentally runs it will first look for the windows environment, and after that it will look for the Microsoft .NET framework v2.0.50727 and v4.0.30319.

- After checking the perfect environment it will drop the executable file with the name of rekeywiz.exe in the directory “C:\ProgramData\font2Files” created by the hta file itself for the dropper as shown below:

- Once the dropper drops, it will also be responsible for some registry changes in the directory of “Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing” which is used to allow the process to establish remote access network connection (RAS). Entries are defined below:

Registry	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASAPI32	%windir%\traci
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASMANCS	0

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASMANCS	0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASMANCS	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASMANCS	1048576
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASMANCS	%windir%\tracı
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASAPI32	1048576
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASAPI32	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASAPI32	4294901760
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rekeywiz_RASAPI32	0

As already shown in the above screenshot, registry changes will surely occur when rekeywiz.exe drops in the system and executes itself for intentional damage.

By reviewing the logs, in the directory “C:\WINDOWS\tracing” and the log file name as “rekerywiz_RASAPI32.log” and “rekeywiz_RASMANC.log”, we find that the first log file is generated and as the malware was not properly executed in the sandbox environment created for analysis so it does not show plenty of information. Furthermore, you can also get information from these log files defined below:

- After every step, finally the dropper itself uses shell execution technique and encryption for which it is designed.

Remediation

In order to remediate following points are defined below:

1. Block subjected URL http://www.au-edu.km01s.net.
2. Remove the registry changes defined in the behavioral findings.
3. Search for the reykeywiz.exe in the directory of “C:\Program Data\font2Files” and remove the file.
4. Disable EFS encryption in windows.

Beware of social engineering techniques employed by cyber criminals—including strategies used in phishing emails, impersonated calls, and fraudulent businesses and domains— to identify and respond to a suspected compromise.

The above analysis is performed in a controlled environment in Rewterz Threat Intelligence Labs. In case you have any malware samples/binaries that need to be analyzed, Rewterz is here to help.

Conclusion

It is concluded after in-depth analysis that a malicious pdf file attempts to connect to a random public IP address to download other supporting components of malware in the form of .hta extension file. This file .hta is actually playing the dropper role in this infection cycle, which generates calls to download malicious executable (rekeywiz.exe). The core components of this malware are file.hta and rekeywiz.exe. Rekeywiz.exe encrypts the system files if the .net framework existence fulfills the dependency of file.hta

---