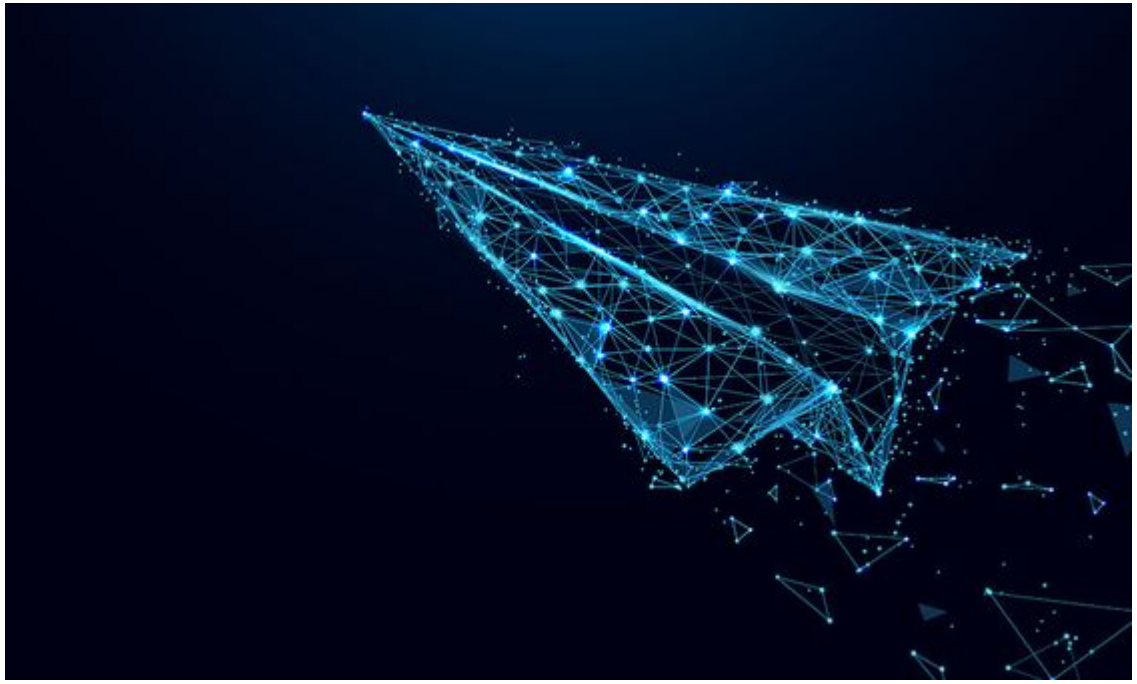
SugarGh0st RAT attacks Kazakhstan

sts.kz/2024/02/09/sugargh0st-rat-atakuet-kazahstan

9.02.2024

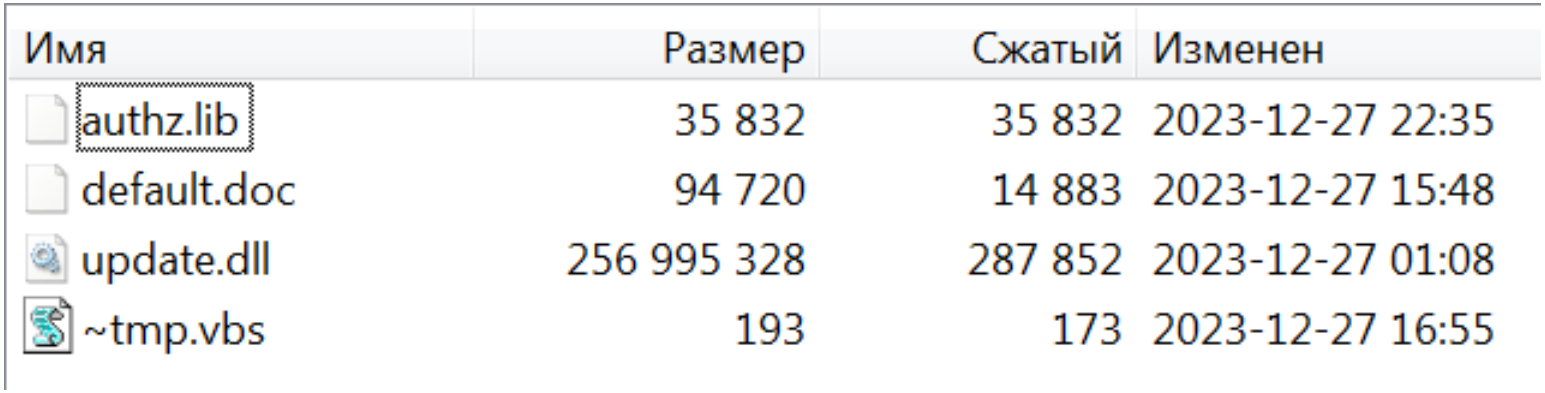


In November 2023, the Cisco Talos research group published a report in which it provided details of the SugarGh0st RAT malware cyberattack. Experts confirmed evidence that the infrastructure of a number of foreign countries was attacked using this malicious program. After analyzing the cyberattack, Cisco Talos came to the conclusion that the SugarGh0st RAT malware was allegedly created by a pro-government group in a third country.

At the end of December 2023, GTS JSC, using the funds of the NKCIB, recorded a mass phishing mailing to email addresses belonging to one of the government bodies of the Republic of Kazakhstan. The attackers created an address on the Yahoo mail service that imitated the email address of an employee of the press service of a government agency of the Republic of

Kazakhstan.

Attached to the letter was an RAR archive, which contained a self-extracting archive (SFX - self-extracting archive) with a Microsoft Word icon, which misleads the user. When SFX is launched, the contents are unpacked into the %TEMP% directory and using the “~tmp.vbs” script, the “update.dll” library is installed as a Logon Script. The user was also shown a decoy document containing a Happy New Year greeting.



Имя	Размер	Сжатый	Изменен
authz.lib	35 832	35 832	2023-12-27 22:35
default.doc	94 720	14 883	2023-12-27 15:48
update.dll	256 995 328	287 852	2023-12-27 01:08
~tmp.vbs	193	173	2023-12-27 16:55

When the “update.dll” library was launched, the “authz.lib” file was read and its contents were decrypted using a dynamic XOR key, after which control was transferred to the beginning of the shellcode section.

```
for ( i = 0; i < FileSize; ++i )
  *((_BYTE *)ptr_authz + i) ^= FileSize ^ (i * i) ^ 0x11;
```

The shellcode performs the Reflective Loading procedure, loading a program in PE32 format, which is stored in its body in encrypted form. The specified program is a SugarGh0st RAT with the control center address “account.drive-google-com[.]tk”.

The functionality of the malware corresponds to the description given in the Cisco Talos publication and includes file system management, loading/uploading data (files) to the C&C server, managing services and processes, making changes to the registry, managing windows and transmitting keys/mouse clicks, and also has keylogger and screenlogger functions.

In addition, SugarGh0st RAT has the ability to download additional malicious modules. So, the program searches for files that are located in the %PROGRAM_FILES%\Common Files\DESIGNER directory. If the file has an .OLE extension, the program tries to load this file as a library and call the export function “O”.

Conclusion

Thus, evidence has been obtained that the hacker group behind the SugarGh0st RAT malware, in addition to other countries, also attacks users in Kazakhstan.

We will continue to monitor the activity of this group.

Indicators of compromise :

1. ***~tmp.vbs***

MD5: 56E231A9DB0F55E333C4F9EC99EEC086

SHA1: 834D0F8DE3F0A2C8C05F477DFB8E4F51D7932B15

2. ***update.dll***

MD5: DEDF98E7E085CED2D3266AFA9279E4C7

SHA1: 84CE02B980EE304A5B624F0DFC9400EC39BBABAE

3. ***authz.lib***

MD5: C2049C234BF2CA534668F8A10CE244D5

SHA1: 30755EA403E3509A2F835D18B9349D13A6FF10BA

C2: account[.]drive-google-com[.]tk

Mutex: account[.]drive-google-com[.]tk

File: %PROGRAM_FILES%\WinRAR\WinLog.txt

File: %PROGRAM_FILES%\WinRAR\~temp.dat

If indicators of compromise of this cyber attack are identified, we recommend contacting 1400 .