Operation DarkCasino: In-Depth Analysis of Attacks by APT Group Evilnum (Part 2) - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks.

By NSFOCUS

Published: 2022-09-20 · Archived: 2026-04-05 16:29:06 UTC

Operation DarkCasino: In-Depth Analysis of Attacks by APT Group Evilnum (Part 1)

Components

Evilnum mainly used a new customized trojan in this operation. NSFOCUS Security Labs named it DarkMe based on the particular string in the trojan program.

NSFOCUS Security Labs also discovered another new trojan program that had a close connection to this operation and named it PikoloRAT, also based on the particular string in the program.

1. DarkMe

DarkMe is a VisualBasic spy trojan developed by Evilnum attackers and is used in various attack flows. The initial version of DarkMe appeared on September 25, 2021, and five iteration versions have been released so far.

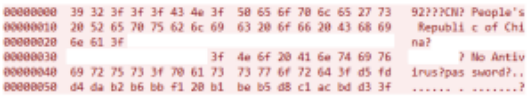
The communication ability of DarkMe is implemented through the public module WinSock32 (http://leandroascierto.com/blog/winsock32/). This module creates a window named SOCKET_WINDOW to implement socket communication with the server.

On the basis of this module, a significant number of functional codes are gradually added to DarkMe, allowing it to evolve from a downloader trojan into a stub spy trojan.

- Functions

Different versions of DarkMe have different functional codes. Here, we will describe the trojan program version 5, ShellRunDllVb.dll, that appeared in this operation.

After ShellRunDllVb.dll is executed, it will collect host information and send it to the C&C server. DarkMe collects the following host information, including the geolocation abbreviation, country name, computer name, user name, antivirus software list, trojan mark, and the title of the foreground window. These items are separated by a fixed separator 0x3F, and prepended with a fixed string “92”. The resulting register information is then sent to the C&C server.



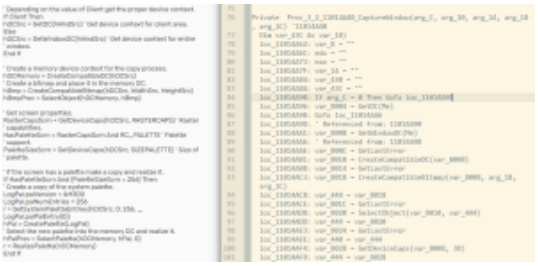
Register traffic of DarkMe

DarkMe has multiple modules to support different espionage functions. clsfile is a major module used to implement file operations under C&C control. The C&C instruction is contained in the first six bytes of the communication content. The function of each instruction is described as follows:

Instruction	Function
300100	Gets the disk volume information.
STRFLS	Traverses a specified directory to get the directory structure.
STRFL2	Traverses a specified directory to get the directory structure. Large-scale directories are supported.
SHLEXE	Executes the **cmd** command.
RNMFIL	Renames a specified file.
DELDEL	Deletes a specified file.
DIRMAP	Creates a specified directory.
DELMAP	Deletes a specified directory.
SEITUS	Writes to a specified file.
SEITUD	Reads a specified file.
ZIPALO	Writes to a compressed file.
FRIKAT	Writes to a registry startup key.
ZIPALO	Copies a specified file.
COPALO	Pastes a specified file.

Description of DarkMe instructions

In addition, DarkMe has been integrated with a set of public codes to achieve the screenshot function.

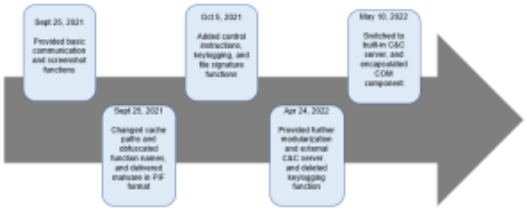


Screenshot function implemented by DarkMe (right) and public code (left)

DarkMe also provides persistence and self-updating functions as well as the keylogging function in some versions.

- Versions

With a deeper look at samples in the wild, NSFOCUS Security Labs found DarkMe had a history of more than half a year, and was already available in multiple versions. The version iteration timeline of DarkMe is as follows:



Version iteration of DarkMe

It can be seen that during its lifecycle, DarkMe has evolved from a loader trojan to a spy trojan, and then to a stub payload integrated into complex attack flows. DarkMe version 4 and DarkMe version 5 both have complete code functions and can be used as a primary stealing tool or as a loader for other tools, so they were widely adopted by Evilnum attackers in recent attacks.

2. PikoloRAT

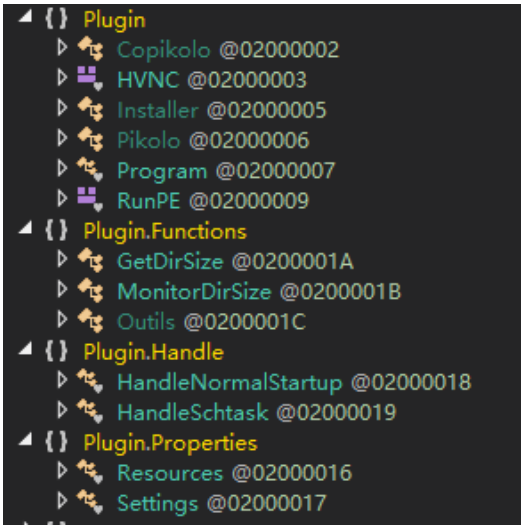
NSFOCUS discovered another new remote control trojan, PikoloRAT, during the in-depth analysis of the relevant information of this operation. PikoloRAT comes with typical remote control functions and can use built-in components to implement more complex control operations.

Since the built-in C&C addresses of PikoloRAT were found to coincide with the addresses used in this operation and PikoloRAT could complement the above-mentioned DarkMe, NSFOCUS Security Labs believed that PikoloRAT was used as an extension component by Evilnum attackers in the later stage of this operation.

The discovered cases demonstrated that PikoloRAT was delivered via a downloader trojan or packaged as a compressed file.

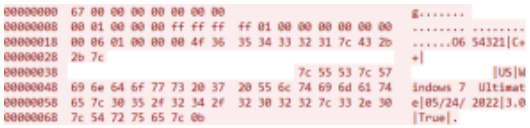
- Functions

PikoloRAT is a typical RAT trojan program written in C#.



Main frame of PikoloRAT

After PikoloRAT runs, it first collects and uploads the host information. The collected contents include the trojan mark, user name, computer name, geolocation, operating system version, trojan running time, trojan version, and antivirus software information. PikoloRAT uses a “|” to separate the preceding items, prepends them with a fixed string “654321”, and then sends it to the C&C server.



Online traffic of PikoloRAT

It can be seen that the content and format of the online traffic of PikoloRAT are similar to those of the above-mentioned DarkMe.

Then PikoloRAT enters the controlled state to control host behaviors by obtaining instructions from C&C servers. The supported remote control instructions are as follows:

Instruction Code	Operation
1	Exits the instruction loop.
2	Presses the left mouse button.
3	Presses the right mouse button.
4	Releases the left mouse button.
5	Releases the right mouse button.
6	Double-clicks the left mouse button.
7	Presses the corresponding keyboard key.
8	Moves the mouse to a specified location.
9	Gets the contents in the clipper board.
17	Sets the screenshot interval.
18	Sets the screenshot quality.
19	Sets the screenshot zoom size.
24	Terminates the process.
55	Sets the temporary file path.
4875	Executes the **cmd** command.
4876	Executes the **powershell** command.
8888	Uploads and runs PEGASUS HVNC.
8889	Downloads the trojan.
8890	Implements persistence, including adding autostart items and scheduled tasks.
8891	Deletes persistence contents.

Description of PikoloRAT instructions

In addition to basic remote control functions, PikoloRAT can perform more sophisticated remote control by dropping the built-in PEGASUS HVNC module, a recently leaked hVNC tool.

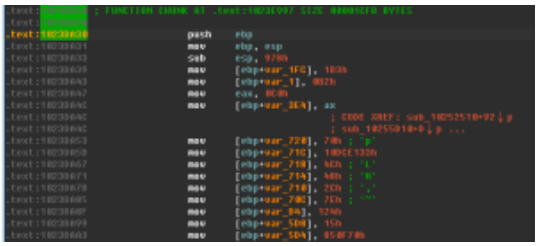
Techniques and Tactics

Overwriting Files While Sideloading

In attack flow A, Evilnum attackers delivered a malicious file **python39.dll** and sideloaded it through a legitimate file **python.exe**. Different from common sideloading build logics, **python39.dll** was obtained by directly overwriting the original **python39.dll**. Evilnum attackers directly wrote a piece of shellcode to the location of the function PyImport_AddModuleObject of the original **python39.dll** so that the shellcode was started when **python39.dll** was loaded.

The benefits of this design are:

- Easy to operate. It is not required to compile a separate DLL program to implement the export.
- Wide applicability. In theory, any legitimate DLL file can be overwritten in a similar way to build a sideloading shellcode attack chain.
- Strong concealment. The new DLL file is so similar to the original DLL file that it is not easy to locate.



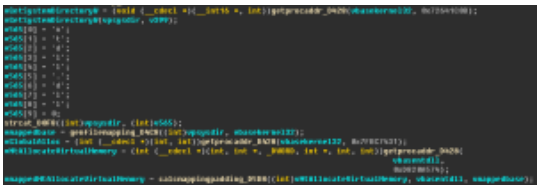
Overwritten PyImport_AddModuleObject function in python39.dll

Shellcode Framework

In attack flow A, Evilnum attackers used different shellcodes at different stages. Since these shellcodes had similar code implementation logic, NSFOCUS Security Labs believed that they originated from the same shellcode programming framework. The overall composition and code complexity in this operation were improved compared to previous Evilnum activities.

ntdll Mapping

In the shellcode used in this operation, Evilnum attackers still adopted two modules, kernel32 and ntdll, to build the main attack flow. To avoid API detection for such behaviors, the attackers used the following method to map the ntdll file and use the API of the mapped file.



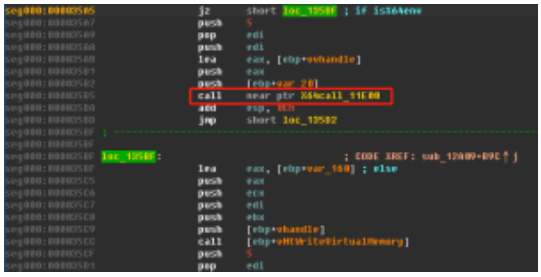
Mapping logic of the ntdll module in the shellcode

In the implementation, the attacker reloaded the ntdll module through file mapping, and obtained the API base address of the mapped API by calculating the offset of the base address of the API in the original ntdll file. Then the shellcode used the mapped API to implement corresponding behaviors, thus avoiding original API call behaviors and preventing key parameters from being monitored and recorded.

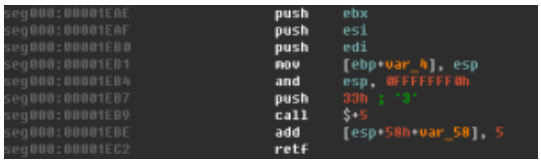
X64call

In attack flow A, Evilnum attackers used X64call to call key APIs while injecting cmd.exe.

The injected shellcode firstly detected the process environment and the host CPU model. If the requirements were satisfied, it would call their 64-bit implementations while using key injection APIs such as NtAllocateVirtualMemory and NtWriteVirtualMemory.



X64call calling logic in the shellcode injection code



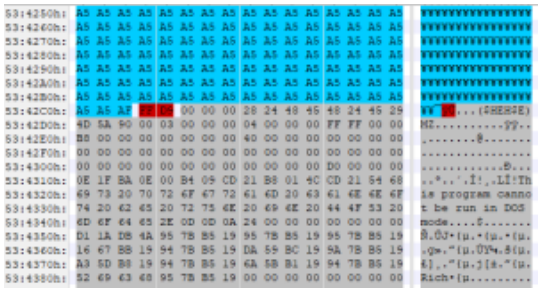
X64call calling code

This technique can also bypass API detection.

Image Steganography

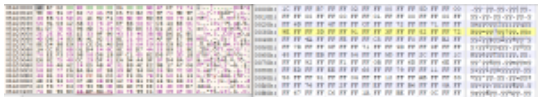
Evilnum attackers used two types of steganographic images in this operation.

In attack flow B, the image IMG.jpg used redundant steganography that deposited the malicious code at the end of the file and used a fixed string (HEHE) as the separator.



Steganographic information in IMG.jpg.

In attack flow A, the image carrying the payload used the RGB color image steganography scheme that deposited the malicious code in the R color pixel.



RGB values in the steganographic image sKr93I.png (right) and extracted compressed data content (left)

This construction could make blue-green dots show in white areas and red dots show in black areas in the steganographic image.

Appearance of the steganographic image sKr93I.png

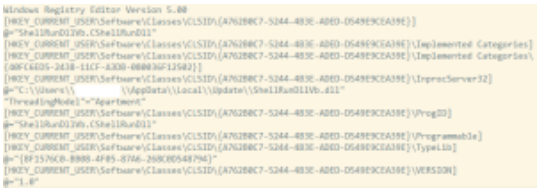
Appearance of the steganographic image Fruit.png

Socket Window

In this operation, the trojan DarkMe used SOCKET_WINDOW communication, an old VisualBasic socket programming technique that hooks winsock messages through a SOCKET_WINDOW window and handles event messages passed by WSAAsyncSelect in the window callback function. For the original framework, refer to here.

COM Component Execution

Some DarkMe trojans were delivered as COM components in this operation. Evilnum attackers wrote the registry operation logic to the preloaded trojan payload, allowing it to generate and execute the file Register.reg that contained the following contents.



Contents of Register.reg

Then the preloaded trojan payload started DarkMe via a **cmd** command in the form like rundll /sta [CLSID] 'Hello'. This could avoid direct calls to DarkMe, reducing exposure risks to a certain extent.

Conclusion

Operation DarkCasino is a series of ongoing APT attacks targeting cash flows in online trading. The Evilnum group adopted a variety of ever-improving attack techniques and tools, demonstrating its keen sense of confrontation.

The analysis showed that the attack scope of Operation DarkCasino was not limited to Europe. Under the operation of the Evilnum attackers, this attack was extended to some Asian countries, which may cause unexpected damage.

To effectively prevent this operation, online financial platform users should pay special attention to files of LNK, PIF, SCR, and COM types transmitted through various channels and be more vigilant of files with keywords such as offer, visa, and casino to avoid Evilnum attacks, which may cause direct economic losses.

Indicators of Compromise (IoCs)

Decoy files of attack flow A

`43eda4ff53eef4513716a5b773e6798653ee29544b44a9ae16aa7af160a996f2`	`offer deal visa 2022.lnk`

Decoy files of attack flow B

`5fb252474237a4ca96cc0433451c7d7a847732305d95ceeaeb10693ecef2eeee`	`Scatters Casino offers Daily Promotions.pif`
`8e4a4c5e04ff7ebacb5fe8ff6b27129c13e91a1acc829dbb3001110c84dc8633`	`new casino crypto.com`
`d0899cb4b94e66cb8623e823887d87aa7561db0e9cf4028ae3f46a7b599692b9`	`Promo CPL CPA Traffic.com`

Decoy files of attack flow C

`4ffa29dead7f6f7752f2f3b0a83f936f270826d2711a599233dc97e442dee85f`	`333TER.exe`
`9cf7f8a93c409dd61d019ca92d8bc43cc9949e244c9080feba5bfc7aac673ac3`	`d33v3TER.exe`
`259cebed2cd89da395df2a3588fadde82cd6542bc9ff456890f7ee2087dc43c9`	`d333TER.exe`
`0cdf27bb8c0c90fc1d60fb07bd30b7e97b16d15e3f58fb985350091ecad51ba6`	`ed333TER.exe`
`5ba84191a873d823ccf336adfa219cc191a004e22b56b99c6d0e1642144129b8`	`wed333TER.exe`
`15a076c7bb6a38425d96aa08b8a15e9a838c9697d57c835aaca92fd01607b07a`	`PayRedeemUpdateIntegration19052022.scr`
`3329f5e3a67d13bd602dca5bbe8e2d0b5d3b5cb7cb308965fb2599a66668c207`	`offer crypto casino.scr`
`8a49a7f6c95fade72ef86455794cdedfca9129aa0f5281e09929dfebfb3417c4`	`DOCUMENTATION AGREEMENTS S CONSULTING INTEGRATION.pif`

Downloader Trojan

`864dccbeda7d88cad91336b5ae9efd50972508d1d8044226e798d039a0bc1da2`	`AONNRJP.exe`

PikoloRAT Trojan

`eb5e42c726c7b125564455d56a02b9d42672ca061575ff911672b9165e8e309d`	`stub1.exe`

be544a1f9f642bb35a9bd0942ae16a7a6e58a323d298a408a00fa4c948e8ea17	Stub1.exe

DarkMe Trojan

a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569	Project1.exe
7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5	Project1.exe
e72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0	Project1.exe
414a11e8eabb64add97a866502edcd7e54108bd247f4ae12fe07feeae4e549f6	Projec3.exe
7913cdf40cc17a28487a71ab0d7724b8bf3646a2a53e3905798ce23a657061b8	Project1.exe
3a6694567e9d722357b8e92153d9c878bbcab55a2f65cd0f9a2e6579fbeb935a	Projec3.exe
a6a70c85b8c40932678c413fde202a55fcfc9d9cae23822708be5f28f9d5b6d2	Projec3.exe
c50ebe13972e6e378248d80d53478d8e01e754c5d87113d9b6f93bf3b84380b4	Project1.exe
1ac7715b1762788b5dc1f5f2fc35243a072fe77053df46101ce05413cca62666	Projec3.exe
4ecc2925cfb073323314611a3892d476a58ff2f6b510b434996686e2f0ac3af7	Projec3.exe
541b3011953a3ce1a3a4a22c8c4f58c6a01df786a7cc10858649f8f70ee0a2f3	Projec3.exe
f25cbc53d0cc14b715ee83e51946d5793e4e86e71e96f68e9b6c839b514e8cb8	Projec3.exe
4244f274a12f4672f2dda1190559d96c5a9631c9ee573b853c89e30701819b63	Projec24.pif
1f0d908c677fb3ec5b9422eb5f7d2a2b3ffa01659521afc07cc4dfaea27aa532	Nuovo.pif
028057e54a2e813787a14b7d33e6a2caa91485ed879ef1bbcb94df0e1cf91356	bvo.exe
0a9c183f0b5a225228da5e8589fac8b3affe2e51c790a08148ef72481de610c4	bvo.exe
3eb84676249cb26dd3d1962cfca2a9fde442d0feaa1b0351f6331313f3ac1138	bvo.exe
46fbfc263959084d03bd72c5b6ee643711f79f7d76b391d4a81f95b2d111b44e	bvofinal.pif
5e04dd49b82320eca63b483e87453d2a68a9f4873f47d37e5080d537bc811d0e	pppppesst.exe
dc8190279dcea4f9a36208ba48b14e6c8313ef061252027ef8110b2d0bd84640	pppppesst.exe
4959cdba7edee68b5116cc1b8ef5016978d3dff2016f027a4f76b080b7c3849a	faster.exe
24ace8fd73b2a5a13f3e5b459f0764dd4b5bda2cea2b0e13bbf88a88afe0cdac	fastest.exe
c66e6ee55e9799a8a32b7a2c836c26bb7ebea98d09c1535ad9ae59e9628835fb	fastest.exe
32ce8d0dcbfcc2517480d0e08f8896ab4f6ea13ccb0eefe7205cd352c7b359c3	h5a.exe
c192684d296ea587e93457d060cbef900143cf1a11301e6c2e34e264e3e55ef6	h5a.exe
1d01b143a56eba431387b9b973790d174deb48c2e3445d96b131a7d8e0a9d4ef	vvt1.exe
b8ba2c0478649dc099d0a869755a7e205173a9b0d15fad920317a89d07eaa930	vvt1.exe

`d95853e6e16d90c00fd72aaeaca9885b953dae14d7d6aa7fedcc6150fb788667`	`656.exe`
`7add6700c6e1aa1ac8782fdd26a11283d513302c672e3d62f787572d8ad97a21`	`ShellRunDllVb.dll`
`17fe047b9a3695d4fd8ad9d2f7f37486c0bc85db0f9770471442d31410ff26a1`	`ShellRunDllVb.dll`
`2665a09ec5b4ca913f9f3185df62495f13611831dba9073779a36df088db143b`	`ShellRunDllVb.dll`
`7c06a03d712be8c0df410bea5d1c2004c6247bcde5a46ce51746f18de9621ac1`	`ShellRunDllVb.dll`

URL

https[:]//puccino.altervista.org/wp-content/uploads/2022/05/6h.txt
https[:]//storangefilecloud.vip/IMG.jpg
https[:]//storangefilecloud.vip/PI.txt
https[:]//storangefilecloud.vip/PRGx.jpg
https[:]//bukjut11.com/FRIGO.JPG
https[:]//bukjut11.com:443/AEVC.JPG
https[:]//imagizer.imageshack.com/img922/1527/sKr93I.png
https[:]//imagizer.imageshack.com/img923/7651/jMwIGI.png
https[:]//i.imgur.com/fkNiY9Z.png
https[:]//laurentprotector.com/LRGBPFV.bin
https[:]//laurentprotector.com/NnQFqsOEUtkezvIEcLpfa.bin

Darkme C&C

aka7newmalp23.com
csmmmsp099q.com
muasaashishaj.com
cspapop110.com
938jss.com
8as1s2.com
kalpoipolpmi.net
pallomnareraebrazo.com
185.236.231.74

PikoloRAT C&C

51.195.57.232
