Detailed Analysis of DarkGate; Investigating new top-trend backdoor malware

medium.com/s2wblog/detailed-analysis-of-darkgate-investigating-new-top-trend-backdoor-malware-0545ecf5f606

S2W January 16, 2024

--

Author: Minyeop Choi | BLKSMTH

> *: Jan 16, 2024*

Photo by on

Executive Summary

- DarkGate is a malware that has been developed since 2017 and sold as Malware-as-a-Service.
- DarkGate was not widely used until 2021, but continued feature additions and modifications were made, and it is now found to be used in various attacks.
- DarkGate supports attackers able to do malicious acts to victims listed below.

— Remote Code Execution by Reverse Shell or Remote Desktop such as VNC and AnyDesk.

— Data Exfiltration on saved files, browser cookies, or cached passwords.

— Cryptocurrency Mining using XMRig

— Privilege Escalation using CVE-2021–1733 or Process Hollowing

— Persistence Management for DarkGate itself

Darkgate needs to be kept track as features are continuously added and detection bypasses occur.

Introduction

Recently, cybercriminals had a new interest in loader/botnet malware called DarkGate. DarkGate has been developed since 2017 and is being sold as MaaS (Malware-as-a-Service) by a user named *RastaFarEye,* who is active in underground forums such as Exploit.in and XSS.is.

Figure 1. Advertisement of DarkGate (XSS.is)

DarkGate was not widely used until 2021, although it was first released in 2018. However, DarkGate has gained demand by updating new features such as Loader, Miner, Remote Control, and Info-stealer. Also, they keep applying anti-analysis or bypass detection by monitoring the analysis report of DarkGate.

Figure 2. Patch note of DarkGate related to anti-analysis (Exploit. in)

DarkGate is sold as Malware-as-a-Service at XSS.is and Exploit.in, priced at $1,000 per day, $15,000 per month, and $100,000 per year. They set a limit of 10 clients per month to keep their project secret but recently increased to 30 due to demand increases.

Figure 3. Notice of increase in sales limit (Exploit.in)

Various threat actors such as TA577, Ducktail, UNC2975, and UNC5085 buy and utilize Darkgate in their attacks, which makes DarkGate distribute in various forms. Not only the well-known methods such as torrent or phishing mail but recently, some abuse the search engine's AD system to make their phishing site appear on top of the results to make victims access it and download DarkGate. DarkGate's various functions and detection bypass methods are continuously updated due to the active activities of creators and purchase attack groups, so periodic tracking of function updates is necessary.

Information of RastaFarEye

The contact information revealed by RastaFarEye is as follows,

- E-mail: coding_guru@exploit.im
- Tox: 09B950550CAD95899AC17C0B1384CD55C9BD81396B19EFFE2E80839D641D3221860ADEA89733
- Telegram: https://t[.]me/evtokens

Figure 4. Banned RastaFarEye account profile (Exploit.in)

Currently, on the Exploit.in, *RastaFarEye* has been banned after receiving a report from a user for not notifying that Packing (also called Crypto) is not applied by default when selling DarkGate. Nevertheless, since RastaFarEye has an account on XSS.is, we are expecting that they will continue their action in XSS.is.

Detailed Analysis

In this section, we describe the structure of DarkGate and detailed analysis of its features. First, we will explain the process of how DarkGate is distributed and installed, and then we will explain the functions that DarkGate has.

The analysis mentioned in our report is based on the analysis of the files below. Based on the configuration settings previously published by Trellix, this sample is identified as V5.

SHA256: 1fb6b8bed3a67ee4225f852c3d90fd2b629f2541ab431b4bd4d9d9f5bbd2c4b7

1. Distribution Type

DarkGate is mostly distributed in two forms; VBScript or Windows Installer Package(MSI). In the recent version of DarkGate, actors prefer MSI form since Windows deprecated VBScript.

Figure 5. Execution Flow of DarkGate in VBScript Form (downloaded via PAPERTEAR)

DarkGate, distributed in VBScript form, was delivered through messengers such as E-mail or Skype. Those cases try to trick victims by making the dropper/downloader look like a document file such as using an LNK file, or adding spaces like “filename.pdf<spaces>www.skype.vbs". When the victim executes it, it downloads the Autoit script file and Autoit launcher from the server. Autoit script contains the XOR encrypted bytecode, which will be decrypted and injected into other processes. The VBS file that uses this method is named PAPERTAR, which is used by UNC2975.

Not much different from VBScript, recent DarkGate has an additional stage to execute Autoit script using DLL Side-loading to bypass the anti-virus detection.

Figure 6. Execution Flow of DarkGate in MSI Form

In the DLL Side-loading stage, pure EXE files in the wild and malicious DLL file pairs such as windbg.exe and malicious dbgeng.dll or KeyScrambler.exe and KeyScrambler.dll are used. Malicious DLL reads `data.bin`, which is extracted from MSI, and gets an additional payload to decrypt `data2.bin`, which contains AutoIt launcher and Autoit script. The rest of the process is the same as VBScript.

AutoIT script executes bytecode by callback of EnumWindows to execute DarkGate. The structure of the bytecode is shown below.

```
    90   nop
    E9 B9 03 00 00 jmp MZ_HEADER

MZ_HEADER:    4D   dec ebp  ; ‘M’ - DOS header magic 1    5A   pop edx  ; ‘Z’ - DOS header magic
2    45   inc ebp  ; Restore stack status    52   push edx  ;    E8 00 00 00 00 call $  ; push
eip    58   pop eax  ; eax = MZ_HEADER + 0x9    83 E8 09  sub eax, 0x9 ; eax = MZ_HEADER    50
push eax  ; function call argument set    05 00 B0 00 00 add eax, 0xb000 ; eax = PE_LOADER =
MZ_HEADER + 0xb000    FF D0  call eax  ; PE_LOADER(MZ_HEADER);    C3   ret…PE_LOADER:    … ; Load
and Execute the PE data
```

Executed code extracts and decrypts the encrypted DarkGate in the script.au3 file and execute it.

2. Characteristics of DarkGate

In this section, we describe the characteristics of DarkGate.

Custom BASE64

DarkGate encodes important constant strings in binary or data in C2 communication with Base64. However, DarkGate uses Base64 different table shown below.

```
zLAxuU0kQKf3sWE7ePRO2imyg9GSpVoYC6rhlX48ZHnvjJDBNFtMd1I5acwbqT+=
```

Configuration

DarkGate loads configuration saved in binary. In the case of the C2 server address, it is encoded in custom Base64. Other DarkGate settings are stored as plain text in the binary or encoded through Custom Base64. Plain DarkGate settings are formed as follows,

```
0=23511=Yes2=Yes3=No5=No4=100...
```

In each line, based on the equal sign, the setting key value is on the left, and the value assigned to the setting key is on the right. The meaning of the values stored in each setting key value is as shown in the table below, and there are a total of 30 values.

Table 1. DarkGate Configurations

Note that some of the settings can be changed or deprecated by updates of DartGate. In the case of “Unknown”, in DarkGate v4 and v5 versions, the purpose of the use is not found or the type of storage and use are different.

Vaccine Detection

DarkGate detects installed anti-virus into ten types listed below.

Table 2. Targeted vaccine list

In addition to the vaccines included in the above 10 categories, DartGate detects additional vaccines as shown below, but the actual malicious actions performed do not change.

- Avira, Trend Micro, McAfee, SUPER AntiSpyware, Comodo, ByteFence, Search & Destroy, 360 Total Security, Total AV, IObit Malware Fighter, Emsisoft, QuickHeal, F-Secure, G Data
- In the case of IObit Malware Fighter, DarkGate kills monitor.exe and smBootTime.exe repeatedly.

Initialize

If *option 1* in DarkGate configuration is Yes, to maintain continuity, perform one of the following actions depending on the type of installed vaccine.

1. Register the LNK file that runs the malicious AU3 script as AutoIt3.exe in the startup program.
2. Register the LNK file to Run the Register.

If *Bitdefender (1), Quick Heal (6), Kaspersky (9)*, or *KES (10)* mentioned above are installed and the LNK file or registry that runs DarkGate does not exist, DarkGate shuts down the infected computer. If the *Bitdefender (1)* exists, it uses NtRaiseHardError with the STATUS_HOST_DOWN error code to cause a

BSOD on the infected computer. According to the author's post, it appears to have been implemented to copy to a safe path and shut down the device when it is recognized as being detected by an antivirus.

Figure 7. Patch note of DarkGate persistence (Exploit.in)

C2 Communication

DarkGate uses HTTP POST requests to communicate with the C2 server. At this time, a custom Base64 table different from the one mentioned above is used for the data. The process of how DarkGate creates the final body data for C2 is as follows.

1. Calculate `MD5(<Username> + <Computer Name> + <Product ID> + <Processor Name>)`
2. HEX encodes and applies substitute cipher to hash value (Substitute cipher table: 0123456789ABCDEF -> abcdefKhABCDEFGH)
3. Add every byte in step 2's result.
4. Set the random seed with step 3's result, and mix Custom Base64 table based on the random seed.

Here, the data to be sent is encoded using the newly created Base64 table, and the string calculated in step 2 is attached to the encoded data and sent together.

Request & Response

After all initial processes are completed, DarkGate periodically requests commands from the C2 server. DarkGate transmits data in the following format. Note that the entire data is encrypted using the newly created Base64 table.

```
1000|<Elapsed time since execution(sec)>|<Version of DarkGate>|<Permission>|22|
```

Then C2 identifies the client through the data and sends and controls the data as follows.

```
<4 digits command id><encrypted data>
```

The command is executed according to the received 4-digit number, and if data is required according to the command, it is encrypted and transmitted through a newly created Base64 table.

3. DarkGate Commands

We now talk about the malicious actions that DarkGate can do. Because there are too many commands that C2 can send, we categorized those commands for better explanation. Note that each command's availability or command ID can be different between versions of DarkGate.

Keylogging

Keylogging executes immediately after initial setup, regardless of the C2 command. The results are saved in a file in DD-MM-YYYY.log format, and the storage path varies depending on the version. C2 can retrieve or delete stored keylogs as needed.

Table 3. Commands of Keylogging

Collect Information

Table 4. Commands of collecting information

Manage Files

Table 5. Commands related to file managing

Steal Credentials

We can see that software created by NirSoft is used to steal various types of information. The existence of lol.exe used in the 1011 and 1012 commands could not be confirmed in the sample, but usage of /shtml and /stext argument in command among the software made by NirSoft and the skype.txt file name. It can be assumed that it is SkypeLogView that steals Skype information.

Table 6. Commands related to stealing credentials

Remove Data/Backups

DarkGate performs various malicious actions by utilizing programs or processes related to the browser. Here, the above function appears to exist to delete APPDATA related to the browser used and left behind by the malicious code. It is also believed that there is a function to delete restore points to prevent restoration to the time before infection.

Table 7. Commands related to removing data/backups

Privilege Escalation

DarkGate attempts to escalate privileges in two ways. One method is using PsExec to obtain SYSTEM privileges(CVE-2021–1733), and the other method is the Process Hollowing method.

Table 8. Commands related to privilege escalation

Crypto Mining

Analysis of related binary was not possible because additional downloaded data could not be received. Besides, we could get a clue by analyzing through information existing in DarkGate. Cryptocurrency mining supported by DarkGate uses XMRig to support mining using CPU and GPU and to mine Monero.

Table 9. Commands related to mining

Inspect Network

These functions trigger proxies to steal internet communication by setting up these registers.

Software\Microsoft\Windows\CurrentVersion\Internet Settings

— Key: ProxyEnable

— Key: ProxyServer

Table 10. Commands related to an Internet proxy

GUI Control

DarkGate supports remote control through the display. Attackers can use virtual display via Hidden VNC or Hidden AnyDesk, or use the originally installed display. It also can hide the process by running on top of the browser process.

Table 11. Commands related to remote display

Reverse Shell

DarkGate also supports the use of traditional reverse shells. However, interaction with the reverse shell must be done through DarkGate and can be transmitted through command 1467. The shell executed here uses the shell written in the environment variable COMSPEC.

Table 12. Commands related to reverse shell

Run & Manage Processes

DarkGate supports various ways to execute code or programs. Not only just launching them, but also DarkGate supports Code Injection, Process Hollowing, and PPID spoofing to avoid detection.

Table 13. Commands related to processes

Managing DarkGate

Attackers can enable the test mode of some functions or debug messages to check DarkGate status. Also, it is possible to update or remove DarkGate remotely.

Table 14. Commands related to the DarkGate setting

ETC

Depending on the system situation, there are functions supported by DarkGate to interrupt the user or maintain operation. To terminate the monitor, it uses the SC_MONITORPOWER message in SendMessageA. Disabling sleep mode uses SetThreadExecutionState to prevent sleep mode.

Table 15. ETC commands

Conclusion

- DarkGate is a malware that, when installed on a target computer, allows attackers to perform various commands such as information theft, cryptocurrency mining, and execution of arbitrary programs.
- Darkgate first appeared in 2017 and is sold only to a small number of attack groups in the form of Malware-as-a-Service through underground forums.
- DarkGate continues to update it by adding features and fixing bugs based on analysis results from security researchers and vendors.
- On the fact that the structure and function of malware are continuously changing, it is expected that tracking these changes will be necessary to prevent damage.

Reference

Appendix A. IoCs

File hash (VBS)

- a448c4abbb2f1844a8fa0c929cd84c2f6f57a4af0442a6a4b5307af89c35cef6
- bc80b13b639ee4b4a6a79555cb4daf3ec360682322ffae68c1272b5aed8b1593
- e2a8a53e117f1dda2c09e5b83a13c99b848873a75b14d20823318840e84de243

File hash (MSI)

- 5b608a6729343cf8b6752d5bb201f906920fcb472f5949e04173b907f65ceff1
- 6e068b9dcd8df03fd6456faeb4293c036b91a130a18f86a945c8964a576c1c70
- 394ee7c88a0925698ce1a2e0268ca49404591eb5cdd961d657d785993212cd86
- aa92f9692dfa98ba9ee991156612f2015c10a5ecf02b605b0b6d528827430601
- de2064d4363a3ccbda5518c619f1c803393b0876e349530583a72b1d1643c16a
- 54f52ef506f6649c09838b9935aed223f0f320798e13fdb9541ffd1db3e08816
- 9f48b63528a24a1241f0bc793e960d420314d595c9927e2294f4475c4be143cd
- 9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3
- 23885818c2a665d5a57ba16acfe46db68258da619a8db3df8f069c0205ac648e
- 9b9514d5af8a9c92e7596dc15aadba0defaedd9f08ec50a588279aa6f6b8ea80
- 0e01bad874c61d09d09ce06f76f5e46f6648a1fc943644874c8e1a53a93af9a7
- c9b3e70c459be9643f764afd535976f9d308d098e1476013de431e7aea22b3e9
- bb37b05a34b2547941efdceee54ec8745e2ce7a7d5d0968c3b5c10274dc81880
- 5be83d13f20b4a044a8c8281d13723a808555cdd73a7ddcec37422a4e44fbd4e
- 4e48d4c355ceb58267a29fd3337b101722c805a7e53662816b73ce9b756ae321
- bde8e0c4bc687ea485fd4a00c86bd25ab14a04edf9b2bbc03808e9b86074717b
- cde0f0b6a29a11aa8a5a4ee543fd632cb460bc11927c7153c1f5f8664e474d23
- 01e578a65a143c884f054c96574f2f9e203b49f47ebf74a0749ff484866b2eb7
- 3a5e7ce24fc5a18843e4f877f5c704bf95eb90c039bc8d791273c191e4ca3242
- 4325d78175a803fb6a1d235e8255816a07283501087e1b115f28c38b6b542856

File hash (CAB)

- 22933b3ae7d125f312b6d1fe6356092cdcd1def6dca3ad128de65ba7986266ae
- f8fcf37ab1e391d1809c4b5baf00d669c4263682d99230432c5199bde5914a60
- a3fc0ef279b5717d0b0dcbe25f8e543efee252cc116336a744968279ce9d3c29
- 1776dcbc4a3f430dd5ace833aac80b0954a050e5a7dec164b53b62fbe72feab3
- 59c026ed7f98aff21521b7a76845821aa5f1ce1a978d1c90404c073bd6310a1d
- acad12dd611551ee4cdfd9fba7dd06c1f6a7c4d8cd8619cbbafa3d8f88bde910
- 659733a584c52078ac6b568dfb34a089bef2b3835a5ea737d32c1623a468b743
- 7c6fa5cec54bc8afa51376db19c9c83d7c17f6e21ce761bfb1daeb7ad31d898d
- 6610e152e07225c91a723f3b65e33af4b0df0d816dd69fe73f9d25dc0fc975d4
- b7874a778f21b2d21a2a2ab2c2ec4a7ae5042443e1d3f20a070424d628079056
- 00dbb5f6bbb9c230fc0c7f7526b46d697850587b30d0b4f4d54106eb3a3d5410
- fa0a47360f68f211413d582d2c73035594a9191c2399c52612c940b45402065f

- 2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003
- 2bf6b1dcb11e7e32b353e0c135aca9c979177d14aa9834119cd8e4c1a5b08562
- 2d08809875f2cfcbe4538d11ee5537768beba0b7740e1785ac35fd90d32e5c25
- 6bc0a512fa3d69c724c2a0aaea8f915795f9c0ef68617dbd32d3b78ee5cddc06
- 70e79ddbcc5bb1f9d40133e4f3dbcea6362794854d47b6a2081f1439ff795dcd
- 37ea8a57e3d3964448238aff31125381c7063b98e1fe0d83a20b315b70546c94
- 6a81b3d6606bd5c4f9d3484719ec35fc6d2dedb902a85553705a71a6e1273104
- b2db96bae6065dbea52711c6f732a29bd39cbb4e81dde9e7d854d52cfb1970f0

File hash (AutoIt)

- 8458a43245c6ff9e3d688a8393f692d3088bf5338ae810ff78b8b3a1d751a87e
- 09bf1b88716c49a62cb4ff708f7ff4f09cb7c3ff42e58661802cd66f1a2a0311
- 7999c9ba66c57b8f2932f54db723feeef411295f8ed6a6d403376278153745c6
- 2ffb2a102df381c9688cc78c2cba4faa6a561d5aa78a9163888ebf7c73bdc8d0
- 453e7fabfa2d6fca1f9a5b9edc456e46417d8fb76332d397a39fcc8e76ccf54f
- 96c84918db77c8bc7d5080aca1b618f7ea7c824d27f67b2346364756f04b3226
- 20cd543224dc3229dece35f018678a52fc98e533596e4995a5534bde0e7e161f
- f02928ec21ad8c600eef3e3a006581a3af858975cbc2ad29ba3dfdd1a78d3cb9
- c6bce64cf86ff6f6b52b9ffa8b8dc2283645b9f0cea7391117d5dd80c2092ce6
- b7c6b567eab740efa575826c94f4c9c552ed5894b8b3ef57e77959b740d8bec8
- 1af981d9c5128b3657cdb5506d61563e0d1908b957e5dd6842059d6d3cfdc622
- b68736ce13dd44a60e7c462b4f451a4132187a0b76adf9cc201a1468379e7601
- b6b2b1773fbd354cc7fcf409f4b4208e570be077658c2a92ea59319c250d9f8c
- bd8fc787abfebba8d167e9979c2ec692f861ab21ea138c3381daa852a58677be
- fffa5abebf578cfc2200b4856889e397e412e56c5bff0032d2d7565d9286685f
- 22d5fdd23ff4302517d5652375ee5ec3bfb28cb964015b3e9902d2398c908fd9
- 684b3445349d8e08e2f2d33f3b30d509a3fde82cb798ccbad2726105301a9470
- da27475894815900fefb9d383de0d255bfa3b7a22927b2912a2d614742b3109c
- 2b49ceb658da03b30d38ee2dc46bcf2bb85af728cece29f8c30d7c1a92c1ad09
- af85ace1fd89e4c76efdda065cc2fc44de987bfd75f9f6850610327526c97d4b
- 063ea8cd25e166182ef68ab1b1157e6448caccaa89cf0f0166c08c21501bf273
- 9a19aa451bb9974c05e616bf02762ee001cc02669aca15150199415e5e190f01
- 3c520028ad9dbf10e5a94023fbbd5ca7134802a6def3fae427f70620c12f8988
- bd9426beaee1c5908b0f71b31539ae4fe3ffed155ab00041b543d48fda3f1654
- 6345b02dc1606522232ac853a0e2599d166aef91ae1d7f4d4104d184273dc1e8
- feeddfb2a7cc4945eaedd8f75907c42ff097252c3e38d7ef2006bd7a191f09ae
- b15e4b4fcd9f0d23d902d91af9cc4e01417c426e55f6e0b4ad7256f72ac0231a
- 7d2c98c8d667891c33119d314d1945c285e2a28701970532f6272cad91f59028
- f1fa42c3d50d4468b9ac3f7e5cdb1160c8f7ed7bbb6e4017859b837dac7e8d93
- a2be457dc7fc5d5662e5db1b51b77094898449fedab7b1a9f837c093c249c5ba
- cb93d34f34e5e999705fd5d17d6725b452c57bc799fc835899e4af9330f4169f
- d2b24a51e7e12fded160344bbac9ee1a9082b690d0c6f326170ea8a224038215
- aa5cb7f6ccb5470ff643cfcba9254263c9db9e7a84984d30166cc14945e219f2
- 3b271f7f34255146366ab7c7d916fa5ab3b1accfc4b0f3d727e16690cfb7ad3a
- 2f342c83cc564e0110f2c0a32a3259f0ef624cd47c50d82000b308411a402c17
- 8ff356af97443bd2b028eb57f160a92c2a1ecab2d227977a87a221ae6409c4be

- 1239ab2c5b8f4445353eacba276938c9cce9711a643851db8979728defc5a3ee
- a63bce69103155accf3c836e7bedf155bee789276624def8713a4431d6562883
- 1d256c2fd442e69120cdf8d12d7bd865f058ec667e2119a66259fc9052dbaa36
- 9e398fb049ae1cf95976ba1c80280cb3f78833569fe7fc5c1ba93c7e57c00fac
- 284458ee75b1d1c2f07ad9fe3a811589360c23092852b2b80a67d2e25e06b269
- 2d8f91bb2359c13abf0ff31af101fc6ecb39849350fbfde015b549e97c8877d5
- 7837e71f9bf00f48ab5336ed8647b116471561181069b79d29dbaee0e951ded7
- 6a9e7b47bec075225861d61cf20555c38a17b7b9ff46ff85de7f6791c548cc2e
- cefc06b2bec8d175eaa9bf3f91c8246731811a8ad7b52af336478655dbc70039
- 4aea930309b590d34488187a8c9cb31b83ff1faa2ff4d27606e50fac3a0db742
- 975d1510380171076b122cd556a1a05bd1eca33b98a9fd003fb3662cb8c83571
- 2f5af97b13b077a00218c60305b4eee5d88d14a9bd042beed286434c3fc6e084

File hash (DarkGate)

- 00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df
- 0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2
- 10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896
- 2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4
- 6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e
- 73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be
- 74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e
- 74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b
- bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1
- bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40
- e7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca
- 3340013b0f00fe0c9e99411f722f8f3f0baf9ae4f40ac78796a6d4d694b46d7b
- 0c3ef20ede53efbe5eebca50171a589731a17037147102838bdb4a41c33f94e5
- 52c47a529e4ddd0778dde84b7f54e1aea326d9f8eeb4ba4961a87835a3d29866
- b0542a719c6b2fc575915e9e4c58920cf999ba5c3f5345617818a9dc14a378b4
- dadd0ec8806d506137889d7f1595b3b5447c1ea30159432b1952fa9551ecfba5
- c88eab30fa03c44b567bcb4e659a60ee0fe5d98664816c70e3b6e8d79169cbea
- 2264c2f2c2d5a0d6d62c33cadb848305a8fff81cdd79c4d7560021cfb304a121
- 3c68facf01aede7bcd8c2aea853324a2e6a0ec8b026d95c7f50a46d77334c2d2
- a146f84a0179124d96a707f192f4c06c07690e745cffaef521fcda9633766a44
- abc35bb943462312437f0c4275b012e8ec03899ab86d353143d92cbefedd7f9d
- 908f2dfed6c122b46e946fe8839feb9218cb095f180f86c43659448e2f709fc7
- 3491bc6df27858257db26b913da8c35c83a0e48cf80de701a45a30a30544706d
- 1fb6b8bed3a67ee4225f852c3d90fd2b629f2541ab431b4bd4d9d9f5bbd2c4b7
- 567d828dab1022eda84f90592d6d95e331e0f2696e79ed7d86ddc095bb2efdc8
- 99f25de5cc5614f4efd967db0dae50f20e2acbae9e98920aff3d98638b9ca1f1
- de3f49e68c45db2f31d1cc1d10ff09f8cfce302b92a1f5361c8f34c3d78544e5
- 68952e8c311d1573b62d02c60a189e8c248530d4584eef1c7f0ff5ee20d730ab
- d4e766f81e567039c44ccca90ef192a7f063c1783224ee4be3e3d7786980e236
- 5e94aa172460e74293db106a98327778ae2d32c6ce6592857a1ec0c581543572

Network (C2 List)

- infocatalog.pics
- bikeontop.shop
- positivereview.cloud
- dreamteamup.shop
- whatup.cloud
- thebesttime.buzz
- msteamseyeappstore.com
- 107.181.161.200
- 80.66.88.145
- private-edinmarketing.com
- positivereview.cloud
- 167.114.199.65
- reactervnamnat.com
- 89.248.193.66
- xfirecovery.pro
- naserviceebaysmman.shop
- 185.8.106.231
- 149.248.0.82
- 45.89.65.198
- drkgatevservicceoffice.net
- 5.188.87.58
- 5.34.178.21
- 185.39.18.170
- 179.60.149.3
- sanibroadbandcommunicton.duckdns.org
- bikeontop.shop
- akamai.la
- hardwarenet.cc
- ec2–14–122–45–127.compute-1.amazonaws.cdnprivate.tel
- awsamazon.cc
- battlenet.la
- a40–77–229–13.deploy.static.akamaitechnologies.pw
- a-1bcdn.com
- 185.143.223.64
- avayacloud.com.global.prod.fastly.net
- intranet.mcasavaya.com
- onlysportsfitnessam.com
- marketisportsstumi.win
- coocooncookiedpo.com
- wmnwserviceadsmark.com
- 161.35.113.5

Appendix B. MITRE ATT&CK

Initial Access

Phishing: Spearphishing Attachment (T1566.001)

Execution

User Execution: Malicious File (T1204.002)

Persistence

Boot or Logon AutoStart Execution: Registry Run Keys / Startup Folder (T1547.001)

Privilege Escalation

- Exploitation for Privilege Escalation (T1068)
- Process Injection: Process Hollowing (T1055.012)

Defense Evasion

- Access Token Manipulation: Parent PID Spoofing (T1134.004)
- Hijack Execution Flow (1574.002)
- Indicator Removal (T1070.004)
- Process Injection: Process Hollowing (1055.012)

Credential Access

- Credentials from Password Stores (T1555)
- Credentials from Web Browsers (T1555.003)
- Steal Application Access Token (T1528)
- Steal Web Session Cookie (T1539)

Discovery

- Process Discovery (T1057)
- Browser Information Discovery (T1217)
- File and Directory Discovery (T1083)
- System Information Discovery (T1082)

Collection

- Archive Collected Data: Archive via Utility (T1560.001)
- Data from Local System (T1005)
- Input Capture: Keylogging (T1056.001)

Command and Control

- Application Layer Protocol: Web Protocols (T1071.001)
- Data Encoding: Non-Standard Encoding (T1132.002)
- Remote Access Software (T1219)

Exfiltration

Exfiltration Over C2 Channel (T1041)

Impact

System Shutdown/Reboot (T1529)