

WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group

23 June 2020

By [Stefano Antenucci](#)



- Research
- Research
- Threat Intelligence
- Fox-IT and European Research
- Fox-IT
- Managed Detection & Response

Authors: Nikolaos Pantazis

About the Research and Intelligence RIFT leverages our strategic insights ranging from IOCs and threat intelligence to a race where both attack and defense managed services remain at the core. This multidisciplinary approach

1. Introduction

WastedLocker is a new ransomware variant that has been in development for a number of months. It is attributed to the Evil Corp group, the latter came to prominence after its operations further described against Igor Olegovich Turchakov. These legal events set in motion specific indicted individuals

2. Attribution

We have tracked the activity of the group since 2011, we have been

2.1 Actor Tracking

Business associations are fairly fluid in organised cybercrime groups, Partnerships and affiliations are formed and dissolved much more frequently than in nation state sponsored groups, for example. Nation state backed groups often remain operational in similar form over longer periods of time. For this reason, *cyber threat intelligence reporting can be misleading*, given the difficulty of maintaining assessments of the capabilities of cybercriminal groups which are accurate and current.

As an example, the Anunak group (also known as FIN7 and Carbanak) has changed composition quite frequently. As a result, the public reporting on FIN7 and Carbanak and their various associations in various open and closed source threat feeds can distort the current reality. The *Anunak or FIN7 group has worked closely with Evil Corp, and also with the group publicly referred to as TA505*. Hence, TA505 activity is sometimes still reported as Evil Corp activity, even though these groups have not worked together since the second half of 2017.

It can also be difficult to accurately attribute responsibility for a piece of malware or a wave of infection because commodity malware is typically sold to interested parties for mass distribution, or supplied to associates who have experience in monetising access to a specific type of business, such as financial institutions. Similarly, it is easy for confusion to arise around the many financially oriented organised crime groups which are tracked publicly. *Access to victim organisations is traded as a commodity between criminal actors* and so business links often exist which are not necessarily related to the day to day operations of a group.

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Accept all cookies

Reject all cookies

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage

Off

2.2 Evil Corp

Nevertheless, despite these difficulties, we feel that we can assert the following with high confidence, due to our in depth tracking of this group as it posed a significant threat to our clients. Evil Corp has been operating the *Dridex malware* since July 2014 and provided access to several groups and individual threat actors. However, towards the end of 2017 Evil Corp became smaller and used Dridex infections almost exclusively for targeted ransomware campaigns by *deploying BitPaymer*. The majority of victims were in *North America* (mainly USA) with a smaller number in *Western Europe* and instances outside of these regions being just scattered, individual cases. During 2018, Evil Corp had a short lived *partnership with TheTrick* group; specifically, leasing out access to BitPaymer for a while, prior to their use of Ryuk.

In 2019 a fork of BitPaymer usually referred to as *DoppelPaymer* appeared, although this was ransomware as a service and thus was not the same business model. We have observed some cooperation between the two groups, but as yet can draw no definitive conclusions as to the current relationship between these two threat actor groups.

After the unsealing of indictments by the US Department of Justice and actions against Evil Corp as group by the US Treasury Department, we detected a short period of inactivity from Evil Corp until January 2020. However, since January 2020 activity has resumed as usual, with victims appearing in the same regions as before. It is possible, however, that this was primarily a strategic move to suggest to the public that Evil Corp was still active as, from around the middle of March 2020, we failed to observe much activity from the group. Of course, this may be related to the lockdowns due to the COVID19 pandemic.

The development of new techniques and malware variants such as Gozi ISFB 2 variant. It is also possible that the components on a targeted system are intended as a replacement for the original components.

The group has access to multiple levels. The group seems to be able to continue after a failure and able to continue after a failure happens. That is, detection has not been defeated.

The lengths Evil Corp go to to obtain a victim's email so they can use a protection product that is not a ransomware.

It appears the group relies on their practical experience gained from compromising a target system, by, for example, ensuring the ransomware.

2.3 WastedLocker

The new WastedLocker ransomware appeared in May 2020 (a technical description is included below). The ransomware name is derived from the filename it creates which includes an abbreviation of the victim's name and the string '*wasted*'. The abbreviation of the victim's name was also seen in BitPaymer, although a larger portion of the organisation name was used in BitPaymer and individual letters were sometimes replaced by similar looking numbers.

Technically, WastedLocker does not have much in common with BitPaymer, apart from the fact that it appears that victim specific elements are added using a specific builder rather than at compile time, which is similar to BitPaymer. Some similarities were also noted in the ransom note generated by the two pieces of malware. The first WastedLocker example we found contained the victim name as in BitPaymer ransom notes and also included both a protonmail.com and tutanota.com email address. Later versions also contained other Protonmail and Tutanota email domains, as well as Eclipso and Airmail email addresses. Interestingly the user parts of the email addresses listed in the ransom messages are numeric (usually 5 digit numbers) which is similar to the 6 to 12 digit numbers seen used by BitPaymer in 2018.

Evil Corp are selective in terms of the infrastructure they target when deploying their ransomware. Typically, they hit *file servers, database services, virtual machines and cloud environments*. Of course, these choices will also be heavily influenced by what we may term their 'business model' – which also means they should be able to disable or disrupt backup applications and related infrastructure. This increases the time for recovery for the victim, or in some cases due to unavailability of offline or offsite backups, prevents the ability to recover at all.

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy [↗](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

It is interesting that the group has *not appeared to have engaged in extensive information stealing* or threatened to publish information about victims in the way that the DoppelPaymer and many other targeted ransomware operations have. We assess that the probable reason for not leaking victim information is the unwanted attention this would draw from law enforcement and the public.

3. Distribution

While many things have changed in the TTPs of Evil Corp recently, one very notable element has not changed, the distribution via the *SocGholish* fake update framework. This framework is still in use although it is now used to directly distribute a custom *CobaltStrike* loader, described in 4.1, rather than Dridex as in the past years. One of the more notable features of this framework is the evaluation of whether a compromised victim system is part of a larger network, as a sole enduser system is of no use to the attackers. The SocGholish JavaScript bot has access to information from the system itself as it runs under the privileges of the browser user. The bot collects a large set of information and sends that to the SocGholish server side which, in turn, returns a payload to the victim system. Other methods of distribution also appear to still be in use, but we have not been able to independently verify this at the time of writing.

4. Technical Analysis

4.1 CobaltStrike payloads

The CobaltStrike payload (only) decodes a base64 string, computing the SHA256 hash of the decoded string (derived from the first 16 bytes of the decoded string) to byte

The second type is related to the CobaltStrike payload. It

An interesting behaviour is observed in the scripts. In these, the loader searches for the FilesCrowdStrike directory. Otherwise, the ‘FreeCrowdStrike’ directory is used to bypass CrowdStrike’s endpoint protection.

```
CS_found_flag = 0;
if ( GetFileAttributesA(
    FreeConsole();
else
    CS_found_flag = 1;
malware_load_Cobalt();
while ( 1 )
{
    Sleep(0x270Eu);
    if ( CS_found_flag )
        FreeConsole();
    CS_found_flag = 0;
}
```

4.2 The Crypter

WastedLocker is protected with a custom crypter, referred to as ***CryptOne*** by Fox-IT InTELL. On examination, the code turned out to be very basic and used also by other malware families such as: *Netwalker*, *Gozi ISFB v3*, *ZLoader* and *Smokeloader*.

The crypter mainly contains junk code to increase entropy of the sample and hide the actual code. We have found 2 crypter variants with some code differences, but mostly with the same logic applied.

The first action performed by the crypter code is to check some specific registry key. In the variants analysed the registry key is either: `interface{b196b287-bab4-101a-b69c-00aa00341d07}` or `interface{aa5b6a80-b834-11d0-932f-00a0c90dcaa9}`. These keys relate to the *UCOMIEnumConnections* Interface and the *IActiveScriptParseProcedure32* interface respectively. If the key is not detected, the crypter will enter an infinite loop or exit, thus it is used as an anti-analysis technique.

In the next step the crypter allocates a memory buffer calling the *VirtualAlloc* API. A while loop is used to join a series of data blobs into the allocated buffer, and the contents of this buffer are then decrypted with an XOR based algorithm. Once decrypted, the crypter jumps into the data blob which turns out to be a shellcode responsible for decrypting the actual payload. The shellcode copies the encrypted payload into another buffer allocated by calling the *VirtualAlloc* API, and then decrypts this with an XOR based algorithm in a similar way to that described above. To execute the payload, the shellcode replaces the crypter’s code in memory with the code of the payload just decrypted, and jumps to its entry point.

As noted above, we have observed this crypter being used by other malware families as well. Related information and IOCs can be found in the Appendix.

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

4.3 WastedLocker Ransomware

WastedLocker aims to encrypt the files of the infected host. However before the encryption procedure runs, WastedLocker performs a few other tasks to ensure the ransomware will run properly.

First, Wastedlocker decrypts the strings which are stored in the .bss section and then calculates a *DWORD* value that is used later for locating decrypted strings that are related to the encryption process. This is described in more detail in the *String encryption* section. In addition, the ransomware creates a log file *lck.log* and then sets an exception handler that creates a crash dump file in the *Windows temporary folder* with the filename being the ransomware’s binary filename.

If the ransomware is not executed with administrator rights or if the infected host runs Windows Vista or later, it will attempt to elevate its privileges. In short, WastedLocker uses a well-documented *UAC bypass method* [1] [2]. It chooses a random file (EXE/DLL) from the Windows system32 folder and copies it to the %APPDATA% location under a different hidden filename. Next, it creates an alternate data stream (ADS) into the file named bin and copies the ransomware into it. WastedLocker then copies winsat.exe and winmm.dll into a newly created folder located in the Windows temporary folder. Once loaded, the hijacked DLL (*winmm.dll*) is patched to execute the aforementioned ADS.

The ransomware supports the following command line parameters (*Table 1*):

Parameter	Purpose
-r	takeown.exe /F
-s	completed.
-p directory_path	on the drive
-f directory_path	

It is also worth noting that the ransomware does not encrypt the system files but applies the encryption to the files in the Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap

Name	Method
ProxyBypass	D
IntranetName	D
UNCAsIntranet	S
AutoDetect	S

The above modifications apply to both 32-bit and 64-bit systems and is possibly done to ensure that the ransomware can access remote drives. However, a bug is included in the architecture identification code. The ransomware authors use a well-known method to identify the operating system architecture. The ransomware reads the memory address **0x7FFE0300** (*KUSER_SHARED_DATA*) and checks if the pointer is zero. If it is then the 32-bit process of the ransomware is running in a Windows 64-bit host (*Figure 2*). The issue is that this does not work on *Windows 10* systems.

```
v9 = (&unk_100B2F8 + dword_100A644); // Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
malware_change_reg_zonemap(0, (&unk_100B2F8 + dword_100A644));
if ( !MEMORY[0x7FFE0300] )
    malware_change_reg_zonemap(0x100, v9); // same but for 64bit
```

Figure 2: Decompilation showing method used to identify operating system architecture

Additionally, WastedLocker chooses a random name from a generated name list in order to generate filename or service names. The ransomware creates this list by reading the registry keys stored in HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControl and then separates their names whenever a capital letter is found. For example, the registry key AppReadiness will be separated to two words, App and Readiness.

4.4 Strings Encryption

The strings pertaining to the ransomware are encrypted and stored in the .bss section of the binary file. This includes the ransom note along with other important information necessary for the ransomware’s tasks. The strings are decrypted using a key that combined the size and raw address of the .bss section, as well as the ransomware’s compilation timestamp.

The code’s authors use an interesting method to locate the encrypted strings related to the encryption process. To locate one of them, the ransomware calculates a checksum that is looked up in the encrypted strings table. The checksum is derived from both a constant value that is unique to each string and a fixed value, which are bitwise XORed. The encrypted strings table consists of a struct like shown below for each string.

```
struct ransomware_string
{
WORD total_size; // string_length + checksum + ransom_string
WORD string_length;
DWORD Checksum;
BYTE[string_length] ransom_string;
};
```

4.5 Encryption Process

The encryption process is quite straightforward. The ransomware targets the following drive types:

- Removable
- Fixed
- Shared
- Remote

Instead of including a list of extension targets, WastedLocker includes a list of directories and extensions to exclude from the encryption process. File names are encrypted in blocks of *64MB* and the ransomware encrypts

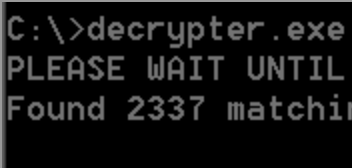
Once a drive is found, the ransomware generates a new key with a newly generated *public RSA key (4096 bits)* and stores it in a note.

For each encrypted file, the ransomware sets the file extension (this ransomware). For each file, the ransomware generates a note. The ransomware note contains the file name and the encryption of each file block.

- Number of targeted file
- Number of files which v
- Number of files which v

4.6 WastedLocker

During our analysis, we found a command prompt and similarl to the encr



References

- <https://medium.com/tenable-techblog/uac-bypass-by-mocking-trusted-directories-24a96675f66e>
- <https://github.com/hfiref0x/UACME>
- <https://github.com/TheWover/donut/>

Appendix

Ransom note

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

☐ Off

ORGANIZATION_NAME

YOUR NETWORK IS ENCRYPTED NOW

USE *EMAIL1* | *EMAIL2* TO GET THE PRICE FOR YOUR DATA

DO NOT GIVE THIS EMAIL TO 3RD PARTIES

DO NOT RENAME OR MOVE THE FILE

THE FILE IS ENCRYPTED WITH THE FOLLOWING KEY:

[begin_key]*[end_key]

KEEP IT

Excluded extensions (in addition to *orgnamewasted* and *orgnamewasted_info*)

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy [↗](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

*ntldr
*.386
*.adv
*.ani
*.bak
*.bat
*.bin
*.cab
*.cmd
*.com
*.cpl
*.cur
*.dat
*.diagcab
*.diagcfg
*.dll
*.drv
*.exe
*.hlp
*.hta
*.icl
*.icns
*.ics
*.idx
*.ini
*.key
*.lnk
*.mod
*.msc
*.msi
*.msp
*.msstyles
*.msu
*.nls
*.nomedia
*.ocx
*.ps1
*.rom
*.rtp
*.scr
*.sdi
*.shs
*.sys
*.theme
*.themepack
*.wim
*.wpx
*bootmgr
*grldr

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy [↗](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Excluded directories



```
adsmarketart.com
advancedanalysis.be
advertsttv.com
amazingdonutco.com
cofeedback.com
consultane.com
dns.proactiveads.be
mwebsoft.com
rostraffic.com
traffichi.com
typiconsult.com
websitelistbuilder.com
```

CobaltStrike Beacon config

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

```
SETTING_PROTOCOL: short: 8 (DNS: 0, SSL: 1)
SETTING_PORT: short: 443
SETTING_SLEEPTIME: int: 45000
SETTING_MAXGET: int: 1403644
SETTING_JITTER: short: 37
SETTING_MAXDNS: short: 255
SETTING_PUBKEY: ''
SETTING_PUBKEY_SHA256: 14f2890a18656e4e766aded0a2267ad1c08a9db11e0e5df34054f6d8de749fe7
ptr SETTING_DOMAINS: websitelistbuilder.com,/jquery-3.3.1.min.js
ptr SETTING_USERAGENT: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
ptr SETTING_SUBMITURI: /jquery-3.3.2.min.js
SETTINGS_C2_RECOVER:
    print: True
    append: 1522
    prepend: 84
    prepend: 3931
    base64url: True
    mask: True
SETTING_C2_REQUEST (tr
    _HEADER: Accept: te
    _HEADER: Referer: h
    _HEADER: Accept-Enc
BUILD: metadata
BASE64URL: True
PREPEND: __cfduid=
HEADER: Cookie
SETTING_C2_POSTTREQ (t
    _HEADER: Accept: te
    _HEADER: Referer: h
    _HEADER: Accept-Enc
BUILD: metadata
MASK: True
BASE64URL: True
PARAMETER: __cfduid=
BUILD: output
MASK: True
BASE64URL: True
PRINT: True
ptr DEPRECATED_SETTING
ptr SETTING_SPAWNT0_X8
ptr SETTING_SPAWNT0_X6
ptr SETTING_PIPENAME:
SETTING_CRYPT0_SCHEME:
SETTING_DNS_IDLE: int: 1249756273
SETTING_DNS_SLEEP: int: 0
ptr SETTING_C2_VERB_GET: GET
ptr SETTING_C2_VERB_POST: POST
SETTING_C2_CHUNK_POST: int: 0
SETTING_WATERMARK: int: 305419896 (0x12345678)
SETTING_CLEANUP: short: 1
SETTING_CFG_CAUTION: short: 0
ptr SETTING_HOST_HEADER:
SETTING_HTTP_NO_COOKIES: short: 1
SETTING_PROXY_BEHAVIOR: short: 2
SETTING_EXIT_FUNK: short: 0
SETTING_KILLDATE: int: 0
SETTING_GARGLE_NOOK: int: 154122
ptr SETTING_GARGLE_SECTIONS: '`x02x00Qxfdx02x00x00x00x03x00xc0xa0x03x00x00xb0x03x000xcex03'
SETTING_PROCINJ_PERMS_I: short: 4
SETTING_PROCINJ_PERMS: short: 32
SETTING_PROCINJ_MINALLOC: int: 17500
ptr SETTING_PROCINJ_TRANSFORM_X86: 'x02x90x90'
ptr SETTING_PROCINJ_TRANSFORM_X64: 'x02x00x00'
```

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

```
ptr SETTING_PROCIJN_TRANSFORM_X64:  x02x90x90
ptr SETTING_PROCIJN_STUB:  *p?'??7???]
ptr SETTING_PROCIJN_EXECUTE:  Bntd1lRtlUserThreadStart
SETTING_PROCIJN_ALLOCATOR:  short: 1
Deduced metadata:
  WANTDNS:  False
  SSL:  True
  MAX_ENUM:  55
  Version:  CobaltStrike v4.0 (Dec 5, 2019)
```

Custom *CobaltStrike* loader samples (sha256 hashes):

```
2f72550c99a297558235caa97d025054f70a276283998d9686c282612ebdbea0
389f2000a22e839ddafb28d9cf522b0b71e303e0ae89e5fc2cd5b53ae9256848
3dfb4e7ca12b7176a0cf12edce288b26a970339e6529a0b2dad7114bba0e16c3
714e0ed61b0ae779af573dce32cbc4d70d23ca6cfe117b63f53ed3627d121feb
810576224c148d673f47409a34bd8c7f743295d536f6d8e95f22ac278852a45f
83710bbb9d8d1cf68b425f52f2fb20d5ebbbd05052b605b2f00ac600dfc5f1076c
91e18e5e048b39dfc8d250e0000000000000000000000000000000000000000
adabf8c1798432b766260a0000000000000000000000000000000000000000
b0354649de6183d455a45400000000000000000000000000000000000000000
bc1c5fecadc752001826b70000000000000000000000000000000000000000
c781c56d8c8daedbed9a150000000000000000000000000000000000000000
c7cde31daa7f5d0923f9c70000000000000000000000000000000000000000
f093b0006ef5ac52aa1d5100000000000000000000000000000000000000000
```

.NET injector (*Donut*) (sha256 hashes):

```
6088e7131b1b146a8e573c0000000000000000000000000000000000000000
```

Gozi ISFB v2

This particular set contains 2 Gozi variants used for persistence in victims.

Gozi C C Domains

```
bettyware.xyz
celebratering.xyz
fakeframes.xyz
gadgetops.xyz
hotphonecall.xyz
justbesarnia.xyz
kordelservers.xyz
tritravlife.xyz
veisllc.xyz
wineguroo.xyz
```

Gozi versions

```
217119
217123
```

Gozi Group ID

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

	vuARb2EPotEtfAX2 Z6fiC4XCvQmfkgua
C Cs	hxxps://devicelease.xyz hxxps://guiapocos.xyz hxxps://ludwoodgroup.xyz hxxps://respondcritique.xyz hxxps://triomigratio.xyz hxxps://uplandcaraudio.xyz hxxps://woofwoofacademy.xyz

ZLoader (MD5: fb95561e8ed7289d015e945ad470e6db)

RC4 key	das32hfkAN3R2TCS
Botnet name	pref
Nonce	0x7
Static config RC4 key	kyqvkjlpclbcnagbhiwo
Version	1.0.0.0
C Cs	

Binary Distribution

Netwalker ransomware (MD5: 21424242424242424242424242424242)

SmokeLoader (MD5: 21424242424242424242424242424242)

RC4 send
RC4 recv
C Cs
Binary Distribution

SecTool checker (MD5: b21424242424242424242424242424242)

We have found a sample of the **SecTool checker** tool, which is a tool used for detecting/disabling a list of security software. We have found that it was used by Evil Corp, however in the past we have seen execution of commands listed in the tool to disable Microsoft Windows Defender.

List of Registry Keys checked	SoftwareESET SYSTEMControlSet001ServicesMBAMService
List of Mutex checked	00082fbb-a419-43f4-bd80-e3631ebbf4c8 069e4409-bd54-4a1f-8e37-49da2cf6a537 0ca9a8d3-01bf-4f9e-bfc7-7eb51e67e0c4 12a2c0fc-00d2-4614-b4ae-c18eb500a088 138be83c-2a52-4c31-9ee8-bfd4eac53d72 15417794-7485-46f6-9965-d34730ea0f48 168cb052-69eb-45be-be07-d4f323dc67d6 16ed8dab-ee6b-44ea-8cea-31c66d6864b9 172821eb-729d-4307-a56f-63063b2677de 17689d7a-89bf-4e2a-a49c-9e4e5a51a9d7 197a1689-8bb1-4fcd-80e9-32b86e3751f5 1a379834-6135-41e7-9cf7-e79a9f705fbc 1cce886d-1841-4e18-963b-15f2e90a3c44 1e8e5806-2e99-4002-b62c-7a78a6641874

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on

Off

1f1769de-42fa-4883-b37c-f0de488de557
240187f4-b097-4a3c-a6fa-2ca5b1e0b373
25f07256-3b46-4531-aa3e-e1729d9aa7cb
274f61dd-3fed-4bfe-9aa6-8a012339a41f
27a0f05f-41fa-43f1-86b9-7e48bde3d716
2a942be2-9252-4d60-9483-3651a92192a5
2c0c5f0d-6ad7-4c97-b1a8-2c706d03a4f8
39309b80-cef5-4ce1-b215-0719723c4c30
3c159c86-0e90-47d1-ad37-788c00ba2948
3f78ca48-011c-4ffb-abfa-c9f659e4a820
3ffd4715-4991-4bc8-9c51-2e3aeb6e737e
3G1S91V5ZA5fB56W
48353b4f-51f9-4961-bcc1-c8d5163a8978
4d6a57e9-e692-4da2-8ba8-adb25645e4b8
4e1ac580-d3cf-4961-81eb-072dff249c17
4e5e7d5e-a1fe-4de7-ad53-5f4aaecd7402
55731fe5-97ad-47dc-953f-37a8aca1451b
5962654a-a395-4714-96f2-2419ab2172bf
5e76294a-2787-4ae2-9ddc-b792b0c45ec2
60f8896b-a437-4e79-9e29-96522ca88c4c

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on

China1839099
China4150039
CryptoMaxima
D1JozWrldD
d86a1229-2cb7-409b-a3de-5366eec3db90
d8ba5865-ac00-4df1-8437-eb144077e031
dad17f2e-5f30-4313-b1c3-5ae8c2149757
dec0f5aa-1fd1-458f-916c-693887610891
e3024a8f-3f2b-4e06-ac36-0997c1090d00
ed3a7d1d-ed6f-4c8f-86d4-44dcde3b32f8
f1e7974a-30e1-423c-9745-bbb7ff7dbf71
f378f238-6503-4544-8e43-cbe4bbf3615e
f967041f-20dd-4d31-a34a-f5e04bdfdf7b
FamilyWeekend
fbac80bd-ba6a-4cd5-92d9-3a31a87f7af6
fda765a3-b5a2-4417-9097-3b18dc6fe6fb
fe711d65-f31a-4c22-a12f-cec65d231941
FixLCD
FMPsDSCV0I

Page 14 of 16

	<div>FoloDrite</div> <div>Hk4kKLL0ZAF8a</div> <div>HTTPEBalancer_v2.15</div> <div>ION8129AZR1A</div> <div>ImageCreator_v4.2</div> <div>InRAMQueue</div> <div>IntelBIOSReader</div> <div>lwS01003993</div> <div>JerkPatrol</div> <div>JKLSXX1ZA1QRLER</div> <div>KDOWEtRVAB</div> <div>LenovoSuite</div> <div>MaverickMeerkat</div> <div>MDISequencer</div> <div>MK5Cheats</div> <div>MLIXNJ9AEGPSE</div> <div>MLIXNJAEGPSE</div> <div>MovieFinder</div> <div>N800HANOI</div> <div>NattyNarwhal</div> <div>N</div> <div>N</div> <div>N</div> <div>N</div> <div>N</div> <div>N</div> <div>N</div> <div>C</div> <div>C</div> <div>C</div> <div>P</div> <div>P</div> <div>P</div> <div>P</div> <div>P</div> <div>C</div> <div>C</div> <div>R</div> <div>R</div> <div>R</div> <div>R</div> <div>S</div> <div>S</div> <div>S</div> <div>S</div> <div>T</div> <div>U</div> <div>UtopicUnicorn</div> <div>VHO9AZB7HDK0WAZMM</div> <div>VideoBind</div> <div>VirginPoint</div> <div>VirtualDesktopKeeper</div> <div>VirtualPrinterDriver</div> <div>VividVervet</div> <div>VRK1AIIXBJDA5U3A</div> <div>WinDuplicity</div> <div>WireDefender</div> <div>wwallmutex</div>
Commands executed	<div>C:Windowssystem32WindowsPowershellv1.0powershell.exe Set-MpPreference -DisableBehaviorMonitoring \$true ; Set-MpPreference -MAPSReporting 0 ; Set-MpPreference -ExclusionProcess rundll32.exe ; Set-MpPreference -ExclusionExtension dll</div> <div>C:WindowsSystem32netsh.exe advfirewall firewall add rule name="Rundll32" dir=out action=allow protocol=any program="C:Windowssystem32rundll32.exe"</div>

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

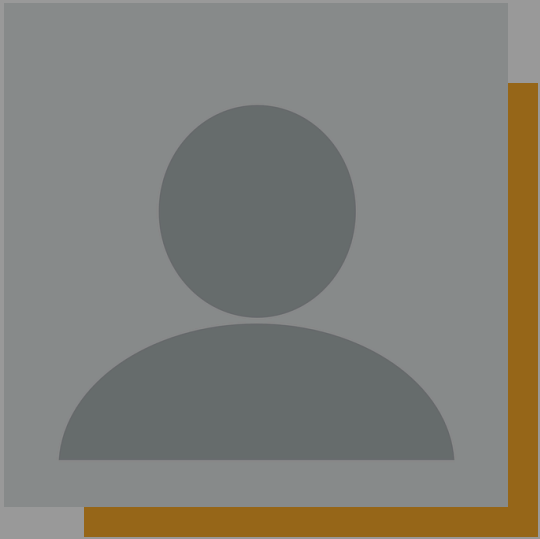
Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

Off

Analytical cookies help us to improve our website by collecting and reporting information on



Stefano Antenucci



[Terms and Conditions](#)

[Privacy Policy](#)

[Contact Us](#)




[Incident Response Hotline](#)
or cirt@nccgroup.com

© NCC Group 2024. All rights reserved.

This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#) 

Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies

☐ Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.