Cyber Security ▸ Research Blog

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 Pantazopoulos*, *Stefano Antenucci* (@Antelox), *Michael Sandee* and *in close collaboration with NCC's RIFT.*

About the Research and Intelligence Fusion Team (RIFT):
RIFT leverages our strategic analysis, data science, and threat hunting capabilities to create actionable threat intelligence, ranging from IOCs and detection capabilities to strategic reports on tomorrow's threat landscape. Cyber security is an arms race where both attackers and defenders continually update and improve their tools and ways of working. To ensure that our managed services remain effective against the latest threats, NCC Group operates a Global Fusion Center with Fox-IT at its core. This multidisciplinary team converts our leading cyber threat intelligence into powerful detection strategies.

1. Introduction

WastedLocker is a new ransomware locker we've detected being used since *May 2020*. We believe it has been in development for a number of months prior to this and was started in conjunction with a number of other changes we have seen originate from the *Evil Corp* group in 2020. Evil Corp were previously associated to the *Dridex* malware and *BitPaymer* ransomware, the latter came to prominence in the first half of 2017. Recently Evil Corp has changed a number of TTPs related to their operations further described in this article. We believe those changes were ultimately caused by the unsealing of indictments against *Igor Olegovich Turashev* and *Maksim Viktorovich Yakubets*, and the financial sanctions against Evil Corp in December 2019. These legal events set in motion a chain of events to disconnect the association of the current Evil Corp group an

2. At

We have e group
has chan activities
under th

2.1 A

Business
affiliation ed
groups, f n over
longer pe given
the diffic h are
accurate

As an exa osition
quite fre ;
associati ty. The
Anunak o *d to as*
TA505. He these
groups h

It can als ve of
infection
distributi applied 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.

2.2 Evil Corp

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 Off

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

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 i dividual
cases. Du leasing
out acces

In 2019 a was
ransomw some
cooperat the
current r

After the vil Corp
as group vil Corp
until Janu ns
appearin
strategic middle
of March yments.
Of course

The deve rted the
developn way
included his
variant is ponents
on a targ
observed viously
used.

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

The group has access to *highly skilled exploit and software developers* capable of bypassing network defences on all different levels. The group seems to put a lot of effort into bypassing endpoint protection products; this observation is based on the fact that when a certain version of their malware is detected on victim networks the group is back with an undetected version and able to continue after just a short time. This shows the importance of victims fully understanding each incident that happens. That is, detection or blocking of a single element from the more advanced criminal actors does not mean they have been defeated.

The lengths Evil Corp goes through in order to *bypass endpoint protection tools* is demonstrated by the fact that they abused a victim's email so they could pose as a legitimate potential client to a vendor and request a trial license for a popular endpoint protection product that is not commonly available.

It appears the group regularly finds *innovative but practical approaches to bypass detection* in victim networks based on their practical experience gained throughout the years. They also *demonstrate patience c* ths after

their initi

example, r to

deploying

2.3 W

The new luded

below). T

abbrevia name

was also d in

BitPayme

Technica ne fact

that it ap n at

compile t som note

generate ained the

victim na d

tutanota ta email

domains, ne email

addresse similar

to the 6 t

Evil Corp

ransomw

environm n their

'business

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.

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

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.

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 altho in 4.1,
rather th ork is the
evaluatio enduser
system is ation
from the s a large
set of inf payload
to the vic have not
been abl

4. Te

4.1 Co

The Coba type
(which ta using
the AES a f the
hard-cod s
derived f the
decrypte cuting it.

The seco ads, an
injector a he
loader ar

An intere rom the
second ty se of
detecting exists,
then the wise, the
'FreeConsole' function is called before loading the CobaltStrike beacon. It is assumed that this is an attempt to bypass CrowdStrike's endpoint solution, although it still unclear if this is the case.

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.

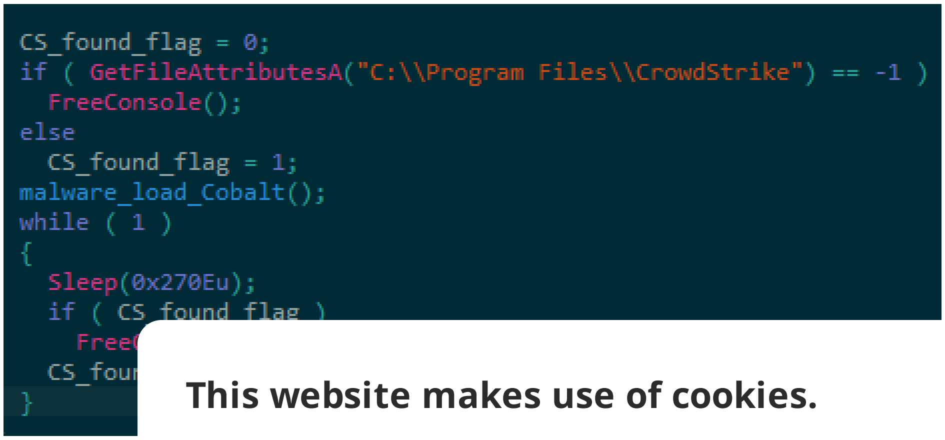
Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

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



```
CS_found_flag = 0;
if ( GetFileAttributesA("C:\\Program Files\\CrowdStrike") == -1 )
  FreeConsole();
else
  CS_found_flag = 1;
malware_load_Cobalt();
while ( 1 )
{
  Sleep(0x270Eu);
  if ( CS_found_flag )
    Free(
  CS_fou
}
```

4.2 Th

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.

WastedLo .. On
examinat es such
as: *Netwo*

The crypt tual
code. We same
logic app

The first ne
variants **41d07}**
or **interfa**
UCOMIEn tively. If
the key is anti-
analysis t

In the ne oop is
used to j er are
then dec e data
blob whic e
shellcode *lAlloc*
API, and d above.
To execu de 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.

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 ransomw … rash dump file … y filename.

If the ran … Vindows Vista or l… documer … ows system32 … ime. Next, it cr … ransomw … eated folder loc … *ll*) is patched …

The rans…

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.

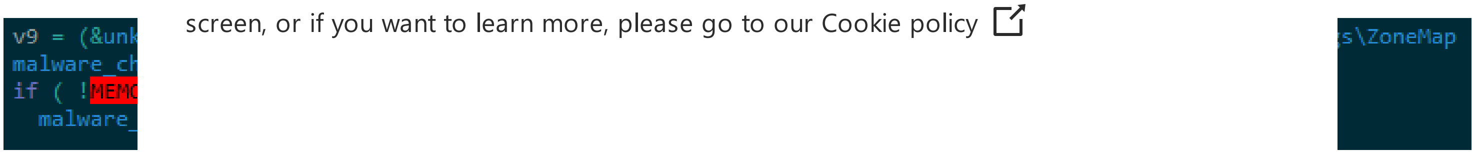
Param…	
-r	… *ns* … on
-s	
-p directo…	… st of
-f directory_path	Encrypt files in a specified directory

Table 1 – WastedLocker command line parameters

It is also worth noting that in case of any failure from the first two parameters (*-r* and –*s*), the ransomware proceeds with the encryption but applies the following registry modifications in the registry key SoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMap:

Name	Modification
ProxyBypass	Deletes this key
IntranetName	Deletes this key
UNCAsIntranet	Sets this key to 0
AutoD	

The abov ensure
that the r ecture
identifica erating
system a
(*KUSER_SH* ne
ransomw work on
Windows



```
v9 = (&unk                                s\ZoneMap
malware_ch
if ( !MEMO
  malware_
```

I e

Additiona to
generate istry
keys stor tes their
names w l be
separate

4.4 Str

The strin f the
binary fil sary for
the ranso d raw
address

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

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 En

The encr rive
types:

- Removab
- Fixed
- Shared
- Remote

Instead c and
extensior also
ignored a

Once a d is
encrypte node) for
each file. he RSA
encrypte n note.

For each omware
note. The along
with the
test.txt.o te). The
ransomw ppendix.
Finally, o e log file
with the

- Number
- Number
- Number of files which were not encrypted due to access rights issues

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

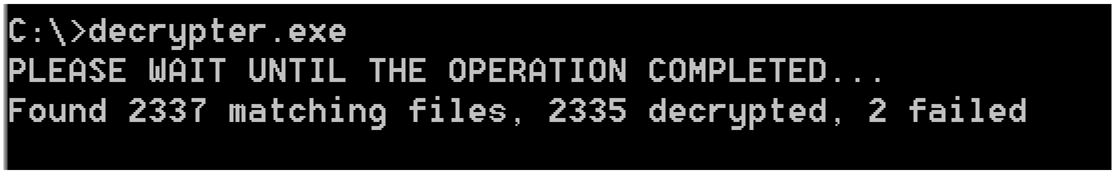
Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

Analytical Cookies Off

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

4.6 WastedLocker Decrypter

During our analysis, we managed to identify a decrypter for WastedLocker. The decrypter requires administrator privileges and similarl to the encryption process, it reports the number of files which were successfully decrypted (*Figure 3*).



```
C:\>decrypter.exe
PLEASE WAIT UNTIL THE OPERATION COMPLETED...
Found 2337 matching files, 2335 decrypted, 2 failed
```

Figure 3: Command line output of the decrypter of WastedLocker

References

- hxxps://m 6675f6e
- hxxps://g
- hxxps://g

Appe

Ransom r

```
*ORGANI

YOUR NI

USE *EI

DO NOT

DO NOT

THE FII
[begin_
KEEP IT
```

Excluded

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
*.diag
*.diag
*.dll
*.drv
*.exe
*.hlp
*.hta
*.icl
*.icns
*.ics
*.idx
*.ini
*.key
*.lnk
*.mod
*.msc
*.msi
*.msp
*.msstyles
*.msu
*.nls
*.nomedia
*.ocx
*.ps1
*.rom
```

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.

```
*.rtp
*.scr
*.sdi
*.shs
*.sys
*.theme
*.themepack
*.wim
*.wpx
*bootmg
*grldr
```

Excluded

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

```
*$recycle.bin*
*appdata*
*bin*
*boot*
*caches*
*dev*
*etc*
*initd
*lib*
*progr
*run*
*sbin*
*sys*
*syste
*users
*var*
*vmlin
*webca
*windo
c:prog
c:prog
c:prog
c:reco
c:user
c:user
c:wind
```

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.

IoCs

IoCs relat he case of targeted ransomware. Each ransomware victim has a custom build configured or compiled for them and so the knowing the specific hashes used against historic victims does not provide any protection at all. Even if behavioural patterns of the ransomware or network related indicators of the ransomware stage are given (should they exist), it is arguable whether detection of the attack at that stage would allow prevention of the actual attack. We do include known ransomware hashes here; however, please note that these are for RESEARCH PURPOSES ONLY. Blocking files based on these file attributes in any endpoint protection product will not provide any value.

At Fox-IT we focus mainly on detection of the initial stages of such attacks (such as the initial stage of infection) by detecting the various methods of infection delivery as well as the lateral movement stage which typically involves scanning, exploitation and/or credential dumping. Providing these IoCs to the wider public would, however, be counterproductive as the threat actors would simply change these methods or work around the indicators. However, we have included some of them to provide historical as well as current protection or detection against this parti oped this infor :ular threat.

CobaltStr

This part ent activity, u ısing CobaltStr eing updated

CobaltStr

```
adsmar
advanc
advert
amazin
cofeed
consul
dns.pr
mwebso
rostra
traffi
typicon
websit
```

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

CobaltStrike Beacon config

```
SETTING_PROTOCOL: short: 8 (DNS: 0, SSL: 1)
SETTING_PORT: short: 443
SETTING_SLEEPTIME: int: 45000
SETTING_MAXGET: int: 1403644
SETTING_JITTER: short: 37
SETTIN
SETTIN
SETTIN
ptr SE
ptr SE
ptr SE
SETTIN
    pr
    ap
    pr
    pr
    ba
    ma
SETTIN
   _HE
   _HE
   _HE
   BUI
   BAS
   PRE
   HEA
SETTIN
   _HE
   _HE
   _HE
   BUI
   MASK: True
   BASE64URL: True
   PARAMETER: __cfduid
   BUILD: output
   MASK: True
   BASE64URL: True
   PRINT: True
```

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

```
ptr DEPRECATED_SETTING_SPAWNTO:
ptr SETTING_SPAWNTO_X86: %windir%syswow64rundll32.exe
ptr SETTING_SPAWNTO_X64: %windir%sysnativerundll32.exe
ptr SETTING_PIPENAME:
SETTING_CRYPTO_SCHEME: short: 0 (CRYPTO_LICENSED_PRODUCT)
SETTING_DNS_IDLE: int: 1249756273
SETTING_DNS_SLEEP: int: 0
ptr SE
ptr SE
SETTIN
SETTIN
SETTIN
SETTIN
ptr SE
SETTIN
SETTIN
SETTIN
SETTIN
SETTIN
ptr SE
SETTIN
SETTIN
SETTIN
ptr SE
ptr SE
ptr SE
ptr SE
SETTIN
Deduce
  WANTDI
  SSL:
  MAX EI
  Version: CobaltStrike v4.0 (Dec 5, 2019)
```

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.

*Custom **CobaltStrike** loader samples (sha256 hashes):*

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

```
2f72550c99a297558235caa97d025054f70a276283998d9686c282612ebdbea0
389f2000a22e839ddafb28d9cf522b0b71e303e0ae89e5fc2cd5b53ae9256848
3dfb4e7ca12b7176a0cf12edce288b26a970339e6529a0b2dad7114bba0e16c3
714e0ed61b0ae779af573dce32cbc4d70d23ca6cfe117b63f53ed3627d121feb
810576224c148d673f47409a34bd8c7f743295d536f6d8e95f22ac278852a45f
83710bb
91e18e5
adabf8
b03546
bc1c5f
c781c5
c7cde3
f093b0
```

.NET inje

```
6088e7
```

Gozi ISFB

This part ryption keys for 2

Gozi C C D

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

```
bettyware.xyz
celebratering.xyz
fakeframes.xyz
gadgetops.xyz
hotphonecall.xyz
justbe
kordel
tritra
veisll
winegu
```

Gozi versi

```
217119
217123
```

Gozi Grou

```
30000
```

Gozi RSA

```
000200                                                  276D7A
45A540                                                  000000
000000
```

Gozi serpent network encryption keys:

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

```
8EzkwaSgkg565AyQ
eptDZELKvZUseoAH
GbdG3H7PgSVEme2r
RQ5btM2UfoCHAMKN
```

Gozi samı

```
5706e1l
ba71dd
c20292
cf744b
```

WastedLc

```
5cd048
887aac
8897db
bcdac1
e3bf41
ed0632
```

The follo… to as CryptOne… t those related t…

List of me…

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

Bot version	3.00.854
RSA key	00040000C3DC07D4E1AC941077214371F45B5FDDDF389654D0851D66809BC989AB

Group IDs	202004081 202004091 202004141 202004231 202005041 80000
Serper keys	
C Cs	

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

ZLoader (

RC4 ke	
Botnet	
Nonce	
Static (	
Versio	
C Cs	hxxp://advokat-hodonin.info/gate.php hxxp://penaz.info/gate.php
Binary Distribution	hxxp://paiolets.com/install.exe

Netwalker ransomware (*MD5: 198b2443827f771f216cd8463c25c5d8*)

SmokeLoader (*MD5: 2143d279be8d1bb4110b7ebe8dc3afbc*)

RC4 send	0x69A84992
RC4 recv	0x5D7C6D5B
C Cs	hxxp://flablenitev.site/index.php hxxp://lendojekam.xyz/index.php hxxp://lgrarcosbann.club/index.php
Binary	

SecTool c

We have :h is
capable (d during
ransomw
However crosoft
Windows

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.

List of Registr Keys checke	
List of checke	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

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

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

ASUSNet20
ATYNKAJP30Z9AQ
b22d1dd8-e3ea-4764-ba9b-0ebf41fddee7
b3e32042-d969-43d1-b20c-bcf8da5ba436
beb41e13-5e33-450f-a9c5-3e5a382d224d
BiosChecksumChecker

bitcoreguard
BlueEye
c3c2a8b3-fc8a-4fe3-8f24-6f2a757a5012
ca1b68fd-56d5-4355-94b2-ed6ab0857890
CBKZiOPASRHKL
CDNetStreamer2.r05
cf3573d5-bf4f-4094-bbea-ced8efde2257

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.

JerkPatrol
JKLSXX1ZA1QRLER
KDOWEtRVAB
LenovoSuite
MaverickMeerkat
MDISequencer

MK5Cheats
MLIXNJ9AEGPSE
MLIXNJAEGPSE
MovieFinder
N800HANOI
NattyNarwhal
NeoNetPlasma

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

VHO9AZB7HDK0WAZMM
VideoBind
VirginPoint
VirtualDesktopKeeper
VirtualPrinterDriver
VividVervet

	VRK1AlIXBJDA5U3A WinDuplicity WireDefender wwallmutex
Commands executed	C:Windowssystem32WindowsPowershellv1.0powershell.exe Set-MpPreference -DisableBehaviorMonitoring $true ; Set-MpPreference - ; Set-

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.

Contact Us

Managed Services

Incident Response

Threat Intelligence

24/7 Incident Response Hotline
+1-(855)-684-1212
or cirt@nccgroup.com

© NCC Gr

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