ThreatMon

The Rise of Dark Power:

A Close Look at the Group and their Ransomware

@threatmon

@MonThreat

Used Methods:

In this report, which we prepared as ThreatMon Cyber Threat Intelligence company, we present this report to you with methods such as malware analysis and threat hunting, as well as proactive cyber threat intelligence, analysis and reporting techniques.

Used Resources

In this report prepared by the ThreatMon Cyber Threat Intelligence team, the threat intelligence and Malware Research Team that prepared the report benefited from platforms such as Ransomware Monitoring and Threat Hunting provided by ThreatMon.

Ransomware Attacks

What is Ransomware Attack?

Ransomware is a type of malicious software that is designed to block access to a computer system, data, or files until a ransom is paid. It is a form of cyber attack where cybercriminals use encryption to lock the victim's files and demand payment in exchange for a decryption key.

Ransomware has become increasingly prevalent in recent years, with cybercriminals targeting individuals and organizations alike. The attacks can cause significant financial and reputational damage, as well as disrupt normal business operations. In some cases, the attacks have even resulted in the loss of critical data, which can be devastating for individuals and businesses.

There are various ways that ransomware can be spread, including through phishing emails, software vulnerabilities, or by visiting infected websites. One of the most common methods of spreading ransomware is through phishing emails. These emails appear to be from a legitimate source, but they contain a malicious attachment or link that, once opened, infects the user's computer with ransomware.

Once the ransomware infects a system, it can quickly spread throughout the network and encrypt all the files, making them inaccessible to the user. The attackers then demand payment in exchange for a decryption key that will unlock the files. The ransom demanded by the cybercriminals can vary from a few hundred dollars to thousands of dollars, and the payment is often demanded in cryptocurrency to make it difficult to trace.

It's essential to note that paying the ransom doesn't guarantee that the files will be decrypted, and it may encourage cybercriminals to continue their criminal activities. In some cases, the attackers may even demand a second ransom payment after the first payment is made.

Types of Ransomware Attack

There are several types of ransomware that attackers can use to target victims, each with their own methods of infection and encryption. Some of the most common types of ransomware include:

Encrypting ransomware: This type of ransomware is designed to encrypt files on a victim's computer or network and demand payment for the decryption key.

Locker ransomware: This type of ransomware locks the victim out of their computer or network, making it impossible to access files or use the computer until a ransom is paid.

Scareware: This type of ransomware displays fake pop-ups or messages that appear to be from law enforcement or other authorities, demanding payment for alleged legal violations or security threats.

How to Avoid Ransomware Attacks?

To protect against ransomware attacks, it's crucial to have good cybersecurity practices in place. These include keeping software up-to-date, using strong passwords, and regularly backing up all data. Additionally, employees should receive training on how to identify and avoid phishing emails and suspicious websites.

Organizations should also consider implementing network segmentation, which separates different parts of the network to prevent the spread of ransomware in case of an attack. They should also have an incident response plan in place that outlines the steps to take in case of an attack.

Furthermore, it's essential to have an effective antivirus program installed on all devices, which can detect and remove ransomware threats. Some antivirus programs also offer ransomware-specific features, such as behavioral analysis and machine learning, which can help detect and block ransomware attacks.

Another crucial step in protecting against ransomware is to ensure that all software is up-to-date with the latest security patches. Ransomware often exploits vulnerabilities in outdated software, which can be prevented by keeping all software up-to-date.

It's also crucial to have a robust backup solution in place that regularly backs up all data. This can help in case of a ransomware attack, as the victim can restore their files from the backup without having to pay the ransom.

In conclusion, ransomware is a severe threat to individuals and organizations alike. It's crucial to be vigilant and take necessary precautions to prevent ransomware attacks. By implementing good cybersecurity practices, having an incident response plan in place, and using effective antivirus software, organizations can reduce the risk of falling victim to a ransomware attack.

Dark Power Ransomware Group

Definition of Dark Power

The Dark Power ransomware group emerged with a swift attack, infiltrating more than 10 organizations across industries in less than a month. The Dark Power ransomware group uses the Nim programming language to create ransomware. Their use of the Nim language places them in a different position compared to other groups. The biggest reason for this is that the Nim programming language is not used very much. Businesses therefore need to have policies and procedures in place to detect Nim binary files to protect themselves. While the Nim programming language was initially a bit obscure, it is now more widely used to create ransomware. The Tor site belonging to the Dark Power ransomware group was observed to be offline during the last inspection.

History of Dark Power

The Dark Power ransomware group was first observed to have started its attacks in January 2023.

Dark Power's Attacks

The Dark Power ransomware group operates on a global scale, with alleged victims in Algeria, the Czech Republic, Egypt, France, Israel, Peru, the US and Turkey. According to the group's website, they have successfully targeted 10 sector-independent systems.

Dark Power's Goals

When the targeted systems were analyzed, it was observed that there was no country and sectoral connection. When the sector and country information of the target systems are analyzed as a result of the related attacks,

In March 2023, the Dark Power ransomware group attacked On** Pha***, an Algerian-based pharmaceutical company in the pharmaceutical industry that provides pharmaceuticals, medical supplies and equipment, compromising data and demanding ransom payments, resulting in damage to the website and disruption to the company's operations.

In March 2023, the Dark Power ransomware group attacked Imt****, an Egypt-based food producer, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group attacked Aga***, a Czech Republic-based trailer manufacturer, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group attacked Turkey-based software company Eva**, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group attacked Ari****, an Israel-based company that manufactures cardiovascular imaging systems using advanced image processing and imaging technologies in the medical sector, and compromised data and demanded ransom payments.

In March 2023, the Dark Power ransomware group attacked Reg****** de* Mer**** d* Val****, a Peruvian company that oversees securities and stock exchange transactions managed by the central bank, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group attacked Gol*****, a Turkey-based industrial yarn manufacturer based in Turkey, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group attacked MDC****, an Israel-based company that provides a platform for processing and analyzing large-scale health data in the Israeli health technology sector, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group attacked Bet******, a France-based software company that provides customized software for the automotive and aerospace industries, compromising data and demanding ransom payments.

In March 2023, the Dark Power ransomware group was observed to have compromised data and demanded ransom payments as a result of an attack on the Nort***** S* organization, which manages several elementary and middle schools in Northern California, a United States-based education sector.

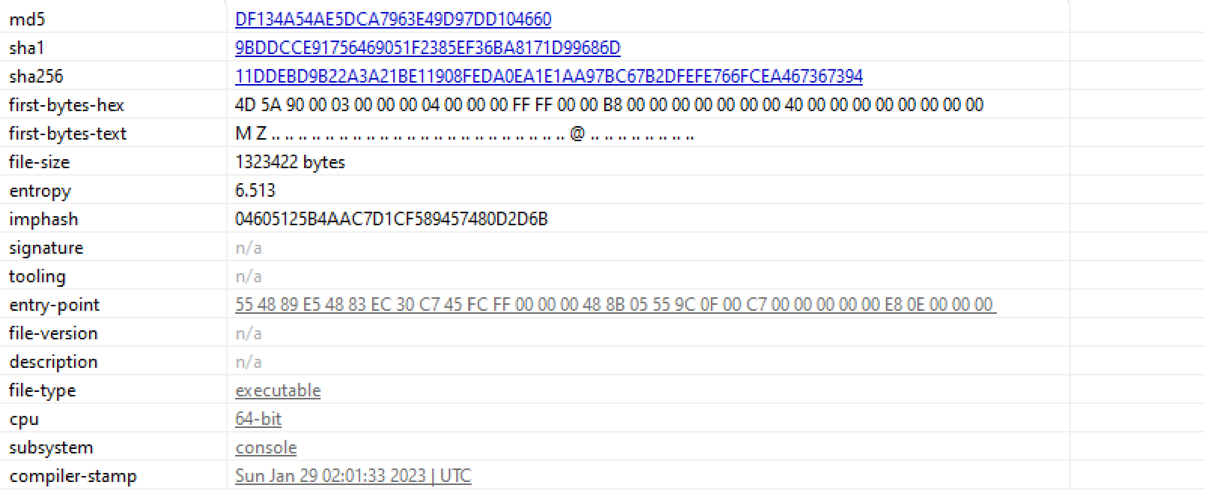
It has been observed that such attacks have been carried out.

Dark Power's Spread Methods

Like many other types of ransomware, the Dark Power ransomware group is generally thought to spread via phishing emails or by exploiting vulnerabilities in software or operating systems. Once the target system computer is infected, the ransomware begins encrypting files on the system, making them inaccessible to the user. The ransomware then displays a message demanding payment in exchange for the decryption key. One of the notable features of Dark Power is that it uses a "double extortion" technique, where attackers not only encrypt the victim's files, but also threaten to release sensitive data stolen from the victim's system if the ransom is not paid. This adds an extra layer of pressure for the victim to pay the ransom, as they may not want their confidential information to be made public.

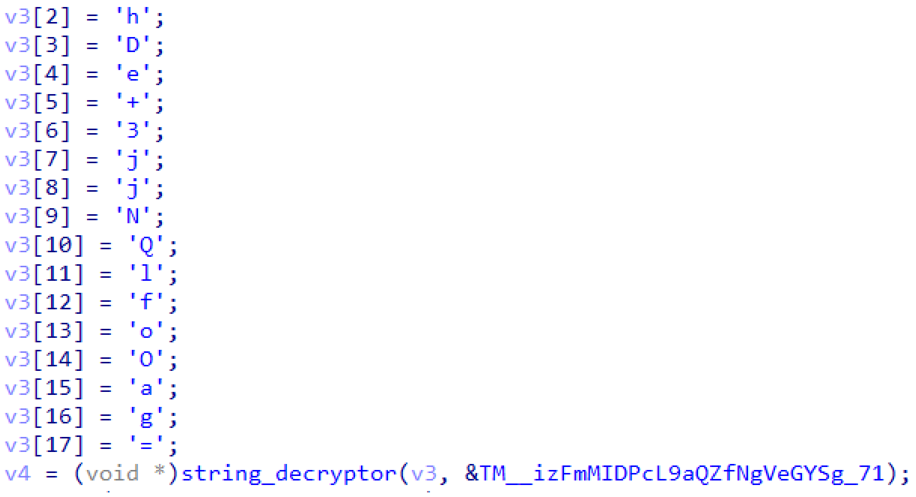
Dark Power Ransomware Malware Analysis

The binary file was written in C++ and compiled on January 29, 2023 using the Nim MinGW compiler. It is in Portable Executable format.



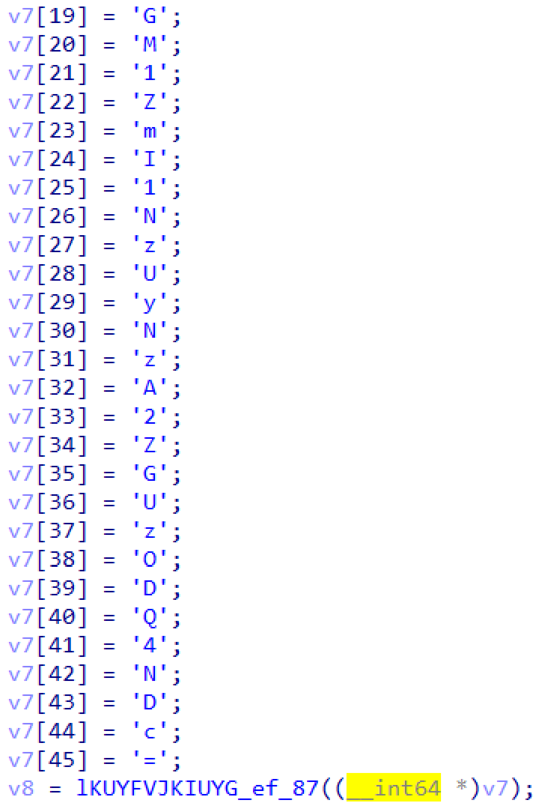
md5	DF134A54AE5DCA7963E49D97DD104660
sha1	9BDDCCE91756469051F2385EF36BA8171D99686D
sha256	11DDEBD9B22A3A21BE11908FEDA0EA1E1AA97BC67B2DFEFE766FCEA467367394
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	1323422 bytes
entropy	6.513
imphash	04605125B4AAC7D1CF589457480D2D6B
signature	n/a
tooling	n/a
entry-point	55 48 89 E5 48 83 EC 30 C7 45 FC FF 00 00 00 48 8B 05 55 9C 0F 00 C7 00 00 00 00 00 E8 0E 00 00 00
file-version	n/a
description	n/a
file-type	executable
cpu	64-bit
subsystem	console
compiler-stamp	Sun Jan 29 02:01:33 2023 | UTC

Strings are obfuscated so before it uses the strings, it has to implement a decryption routine. First it initializes chars one by one to avoid detection of hardcoded strings (through YARA etc.). In this example it is “*hDe+3jJNQlfoOag=*”. BASE64 decoded form is “*72MBW9*”.



```
v3[2] = 'h';
v3[3] = 'D';
v3[4] = 'e';
v3[5] = '+';
v3[6] = '3';
v3[7] = 'j';
v3[8] = 'j';
v3[9] = 'N';
v3[10] = 'Q';
v3[11] = 'l';
v3[12] = 'f';
v3[13] = 'o';
v3[14] = 'O';
v3[15] = 'a';
v3[16] = 'g';
v3[17] = '=';
v4 = (void *)string_decryptor(v3, &TM__izFmMIDPcL9aQZfNgVeGYSg_71);
```

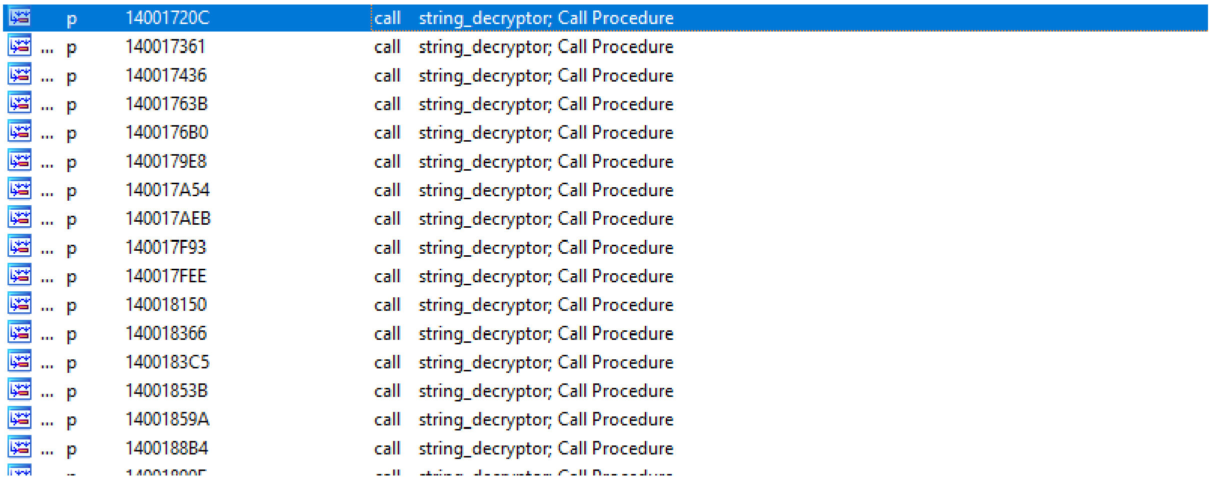
In String Decryptor we see a BASE64 encoded (“*YzU3MWUzZmE4NzIzNGM1ZmI1NzUyNzA2ZGUzODQ4NDcgIAo=*”) MD5 HASH “*c571e3fa87234c5fb5752706de384847*”.



```
v7[19] = 'G';
v7[20] = 'M';
v7[21] = '1';
v7[22] = 'Z';
v7[23] = 'm';
v7[24] = 'I';
v7[25] = '1';
v7[26] = 'N';
v7[27] = 'z';
v7[28] = 'U';
v7[29] = 'y';
v7[30] = 'N';
v7[31] = 'z';
v7[32] = 'A';
v7[33] = '2';
v7[34] = 'Z';
v7[35] = 'G';
v7[36] = 'U';
v7[37] = 'z';
v7[38] = 'O';
v7[39] = 'D';
v7[40] = 'Q';
v7[41] = '4';
v7[42] = 'N';
v7[43] = 'D';
v7[44] = 'c';
v7[45] = '=';
v8 = lKUYFVJKIUYG_ef_87((__int64 *)v7);
```

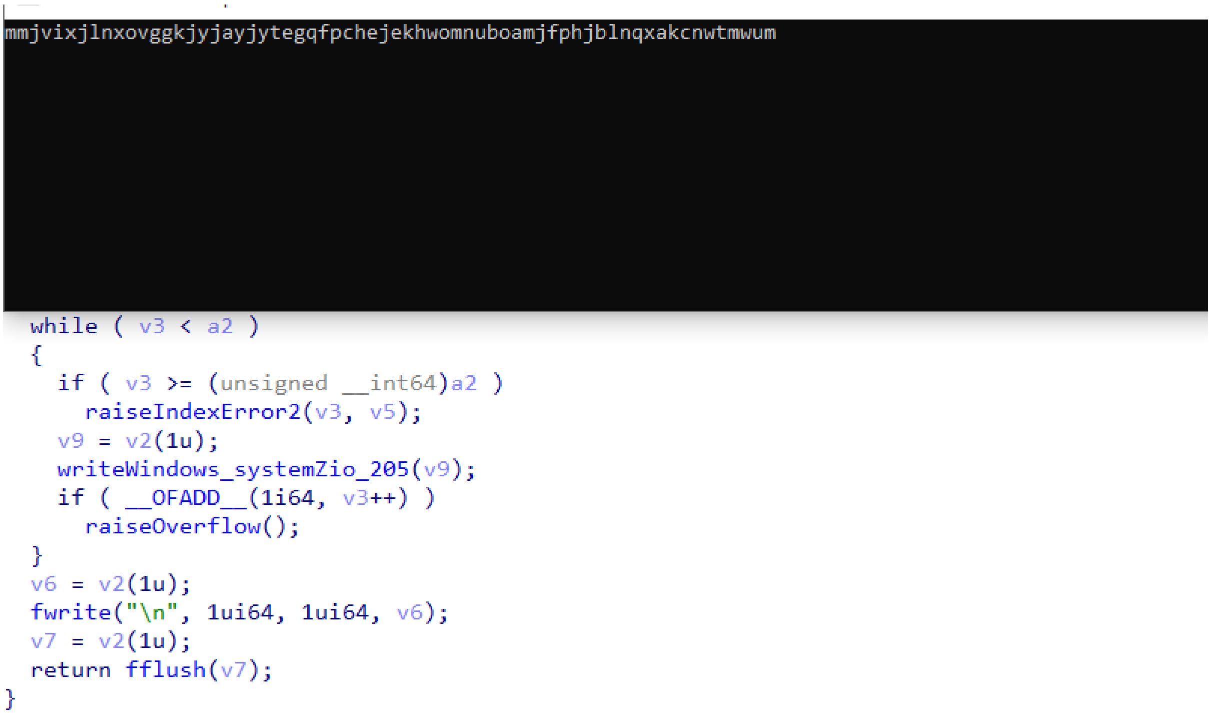
Using this MD5 hash, it does some string operations then taking the SHA256 form of it. Then use this hash as key for decryption. So the decrypted form of “*hDe+3jJNQlfoOag=*” *is “.dark_power”.*

Instead of decrypting all the strings at once, it uses this routine every time before it uses the string.



```
p      14001720C   call  string_decryptor; Call Procedure
... p  140017361   call  string_decryptor; Call Procedure
... p  140017436   call  string_decryptor; Call Procedure
... p  14001763B   call  string_decryptor; Call Procedure
... p  1400176B0   call  string_decryptor; Call Procedure
... p  1400179E8   call  string_decryptor; Call Procedure
... p  140017A54   call  string_decryptor; Call Procedure
... p  140017AEB   call  string_decryptor; Call Procedure
... p  140017F93   call  string_decryptor; Call Procedure
... p  140017FEE   call  string_decryptor; Call Procedure
... p  140018150   call  string_decryptor; Call Procedure
... p  140018366   call  string_decryptor; Call Procedure
... p  1400183C5   call  string_decryptor; Call Procedure
... p  14001853B   call  string_decryptor; Call Procedure
... p  14001859A   call  string_decryptor; Call Procedure
... p  1400188B4   call  string_decryptor; Call Procedure
```

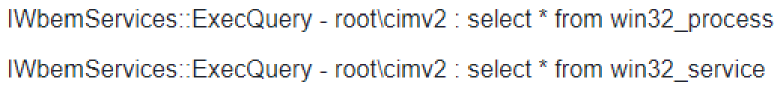
After some string decryption routines passed, it prints 64-chars long ASCII string to console using WriteWindowsSystem. This will be used for encryption later.



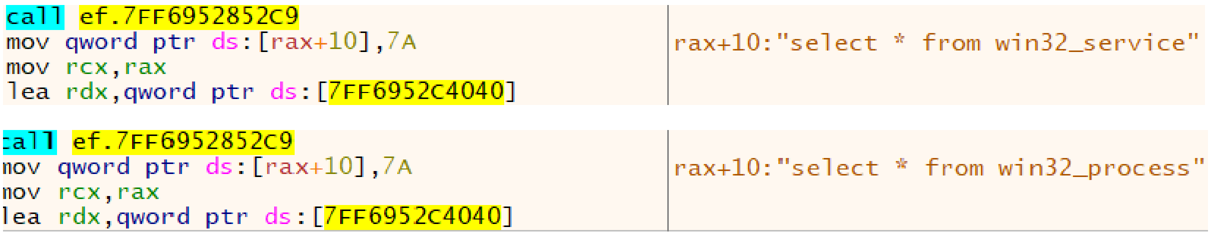
```
mmjvixjlnxovggkjyjayjytegqfpchejekhwomnuboamjfphjblnqxakcnwtmwum
```

```
  while ( v3 < a2 )
  {
    if ( v3 >= (unsigned __int64)a2 )
      raiseIndexError2(v3, v5);
    v9 = v2(1u);
    writeWindows_systemZio_205(v9);
    if ( __OFADD__(1i64, v3++) )
      raiseOverflow();
  }
  v6 = v2(1u);
  fwrite("\n", 1ui64, 1ui64, v6);
  v7 = v2(1u);
  return fflush(v7);
}
```

Then it queries all processes and services using WMI, “SELECT * FROM win32_process” and “SELECT * FROM win32_service”.



```
IWbemServices::ExecQuery - root\cimv2 : select * from win32_process

IWbemServices::ExecQuery - root\cimv2 : select * from win32_service
```



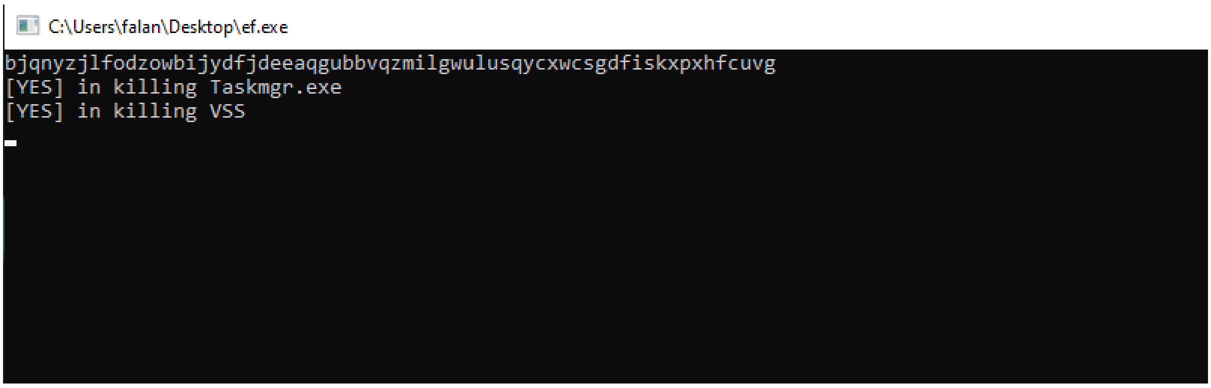
```
call ef.7FF6952852C9                           rax+10:"select * from win32_service"
mov qword ptr ds:[rax+10],7A
mov rcx,rax
lea rdx,qword ptr ds:[7FF6952C4040]

call ef.7FF6952852C9                           rax+10:"select * from win32_process"
mov qword ptr ds:[rax+10],7A
mov rcx,rax
lea rdx,qword ptr ds:[7FF6952C4040]
```

Searches for specific processes and services. Those are:

- taskmgr.exe
- agntsvc.exe
- synctime.exe
- encsvc.exe
- mspub.exe
- infopath.exe
- powerpnt.exe
- onenote.exe

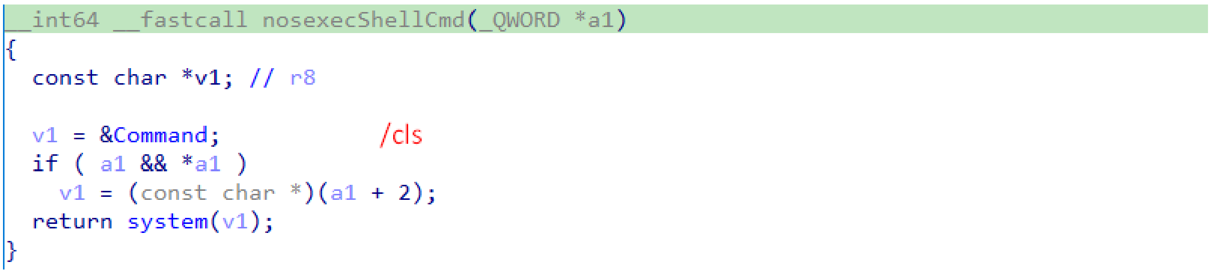
- mydesktopservice.exe
- ocssd.exe
- winword.exe
- firefox.exe
- steam.exe
- thebat.exe
- oracle.exe
- isqlplussvc.exe
- excel.exe
- sqbcoreservice.exe
- outlook.exe
- mydesktopqos.exe
- dbeng50.exe
- sql.exe
- ocautoupds.exe
- tbirdconfig.exe
- ocomm.exe
- thunderbird.exe
- msaccess.exe
- visio.exe
- dbsnmp.exe
- wordpad.exe
- xfssvccon.exe
- veeam.exe
- memta.exe
- vssvc.exe
- savservice.exe
- mepoc.exe

If it finds, terminates the process and print the screen in following syntax: *[YES] in killing XXXX.EXE*

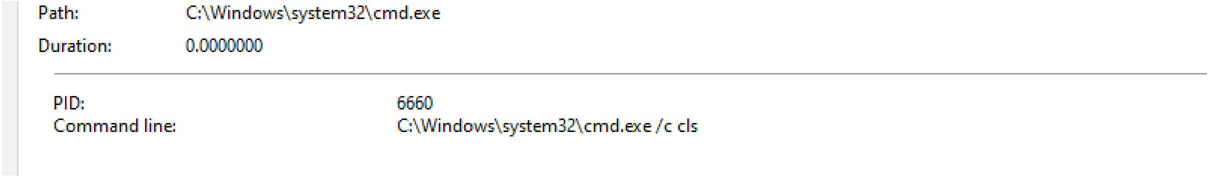


```
bjqnyzjlfodzowbijydfjdeeaqgubbvqzmilgwulusqycxwcsgdfiskxpxhfcuvg
[YES] in killing Taskmgr.exe
[YES] in killing VSS
```

Clears the console.



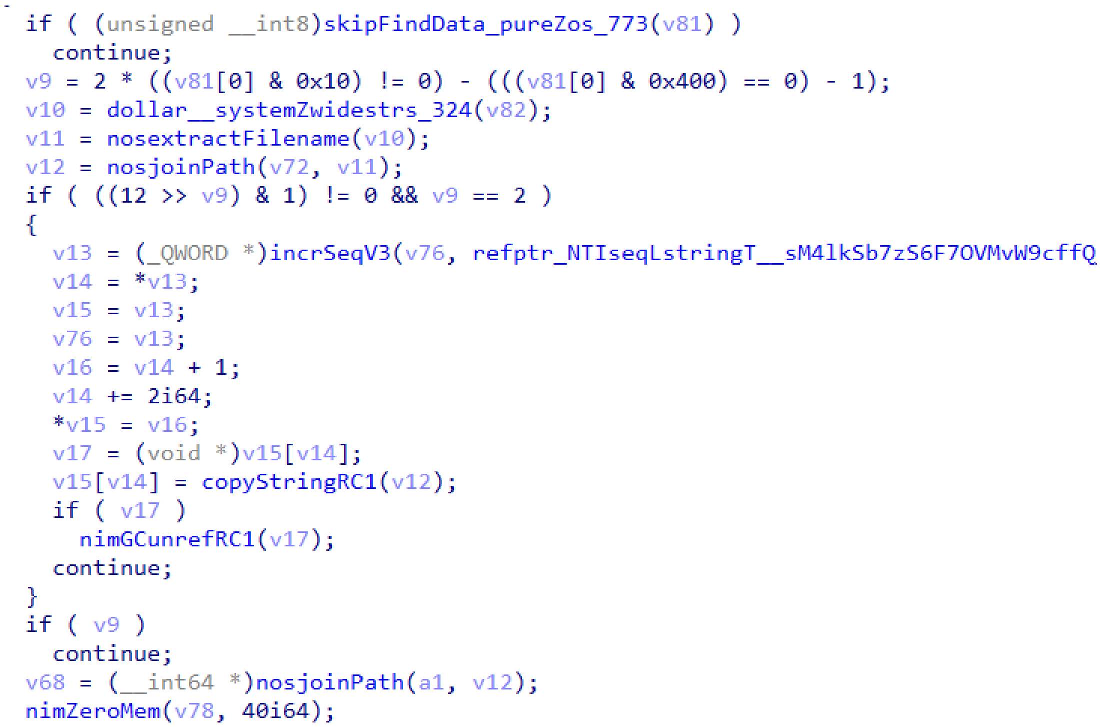
```
__int64 __fastcall nosexecShellCmd(_QWORD *a1)
{
  const char *v1; // r8

  v1 = &Command;              /cls
  if ( a1 && *a1 )
    v1 = (const char *)(a1 + 2);
  return system(v1);
}
```



Path: C:\Windows\system32\cmd.exe
Duration: 0.0000000

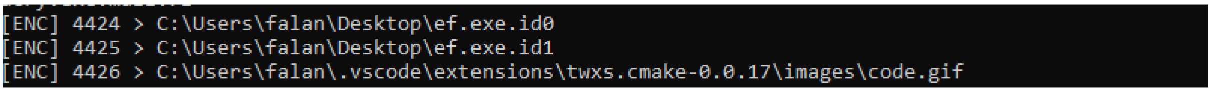
PID: 6660
Command line: C:\Windows\system32\cmd.exe /c cls

After all, it begins doing its main job: encrypting files. It iterates through all the system, encrypts files (some are excluded because they have a critical role in OS) and changes their extensions to ".dark_power".



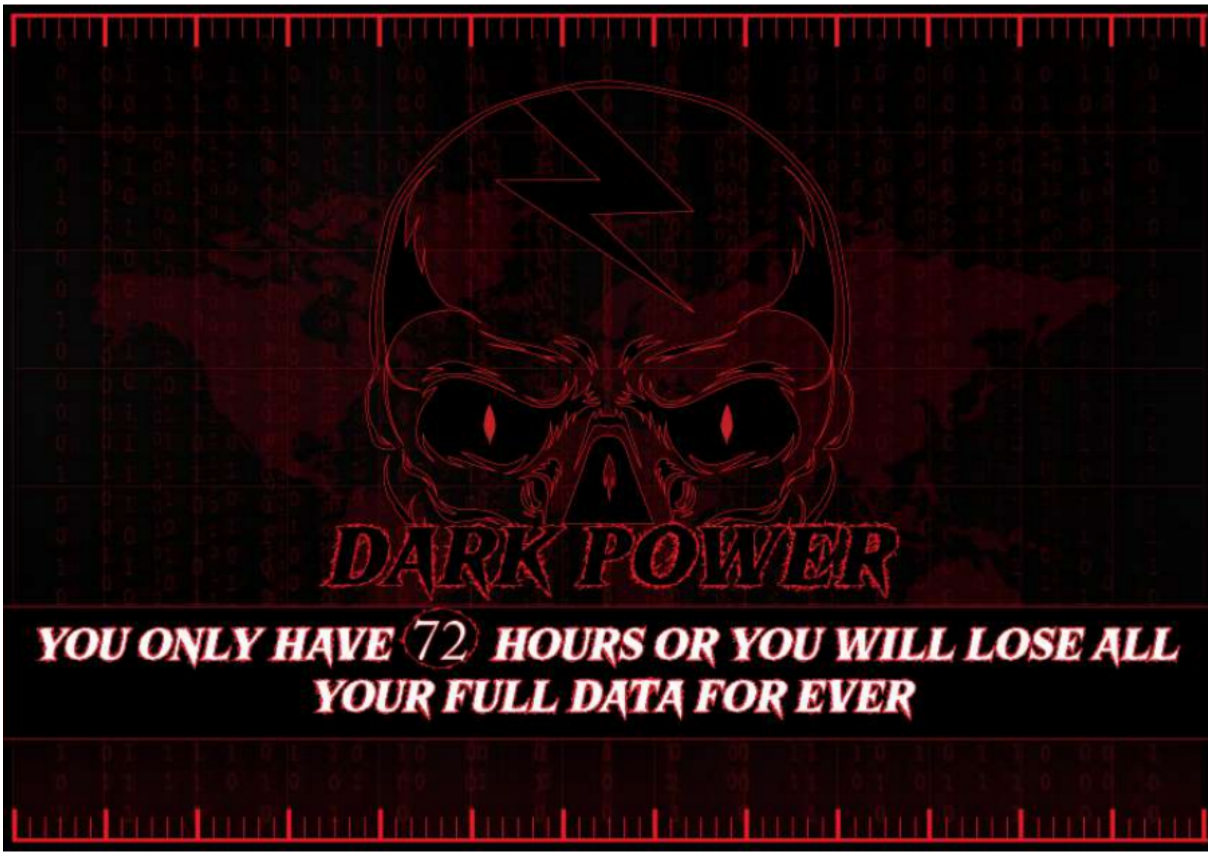
```
if ( (unsigned __int8)skipFindData_pureZos_773(v81) )
  continue;
v9 = 2 * ((v81[0] & 0x10) != 0) - (((v81[0] & 0x400) == 0) - 1);
v10 = dollar__systemZwidestrs_324(v82);
v11 = nosextractFilename(v10);
v12 = nosjoinPath(v72, v11);
if ( ((12 >> v9) & 1) != 0 && v9 == 2 )
{
  v13 = (_QWORD *)incrSeqV3(v76, refptr_NTIseqLstringT__sM4lkSb7zS6F7OVMvW9cffQ
  v14 = *v13;
  v15 = v13;
  v76 = v13;
  v16 = v14 + 1;
  v14 += 2i64;
  *v15 = v16;
  v17 = (void *)v15[v14];
  v15[v14] = copyStringRC1(v12);
  if ( v17 )
    nimGCunrefRC1(v17);
  continue;
}
if ( v9 )
  continue;
v68 = (__int64 *)nosjoinPath(a1, v12);
nimZeroMem(v78, 40i64);
```

Then writes to console in following syntax: "[ENC] -i- FILENAME"

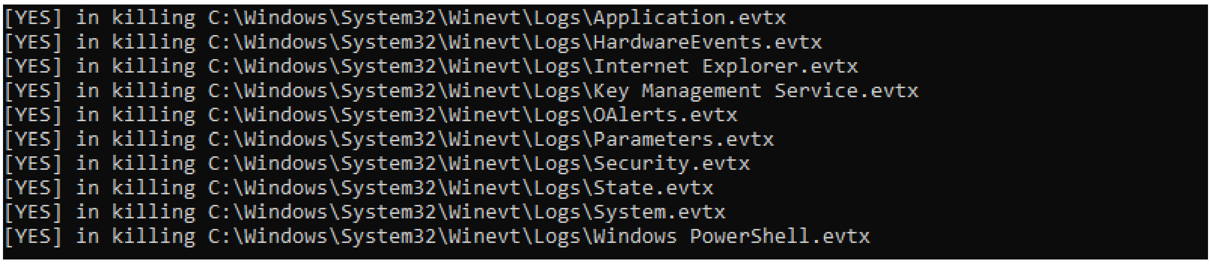


```
[ENC] 4424 > C:\Users\falan\Desktop\ef.exe.id0
[ENC] 4425 > C:\Users\falan\Desktop\ef.exe.id1
[ENC] 4426 > C:\Users\falan\.vscode\extensions\twxs.cmake-0.0.17\images\code.gif
```

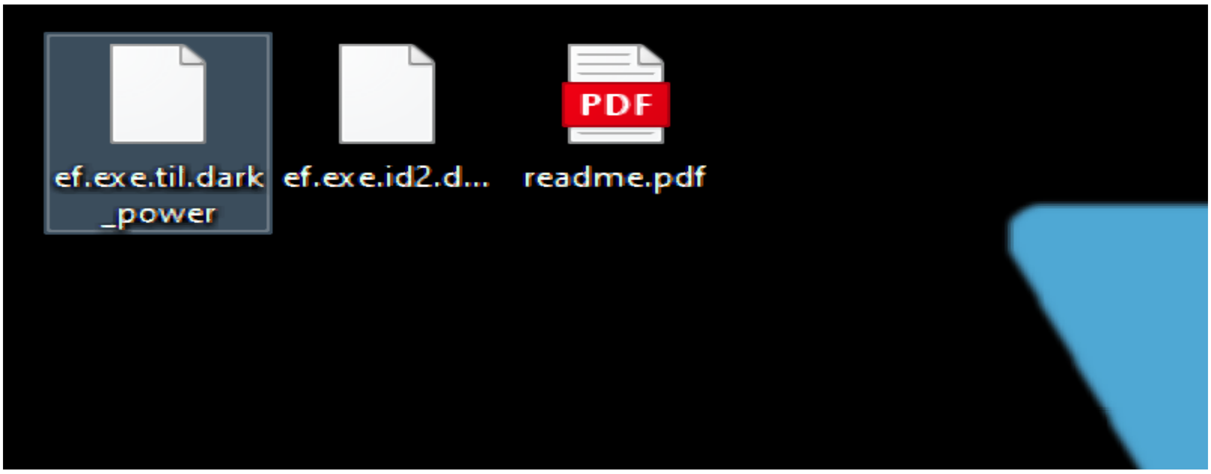
Leaves us a ransom note in pdf format.



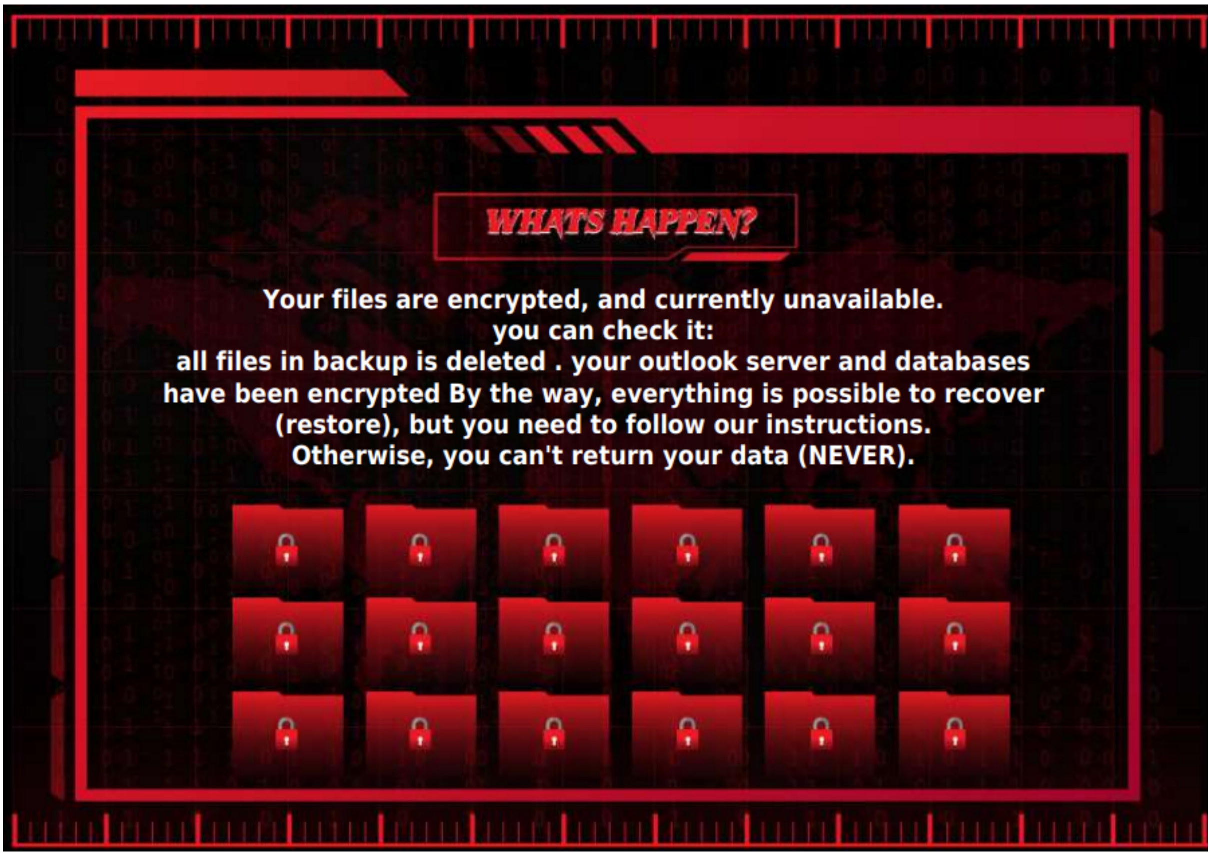
Lastly it clears all the event logs and exits.



```
[YES] in killing C:\Windows\System32\Winevt\Logs\Application.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\HardwareEvents.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\Internet Explorer.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\Key Management Service.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\OAlerts.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\Parameters.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\Security.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\State.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\System.evtx
[YES] in killing C:\Windows\System32\Winevt\Logs\Windows PowerShell.evtx
```

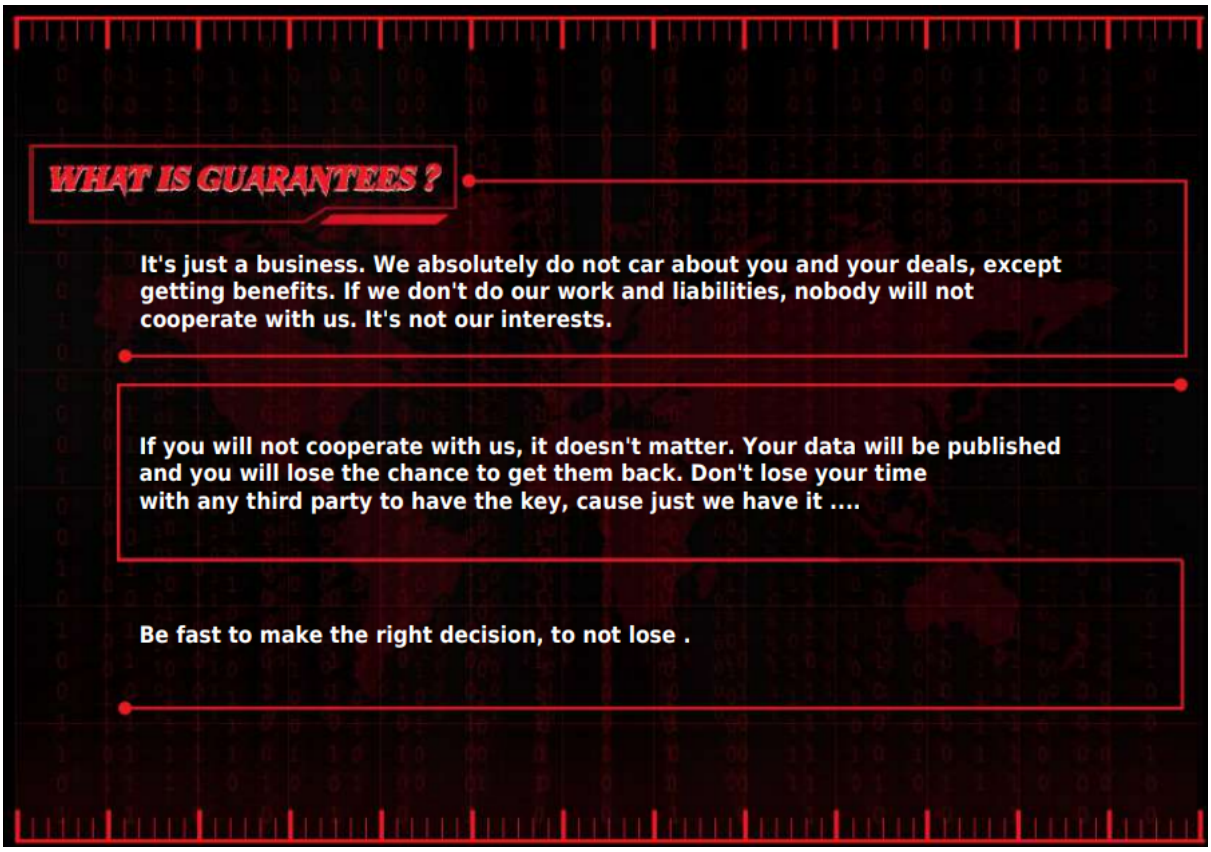


Here is all the ransom note.



WHATS HAPPEN?

Your files are encrypted, and currently unavailable.
you can check it:
all files in backup is deleted . your outlook server and databases have been encrypted By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you can't return your data (NEVER).

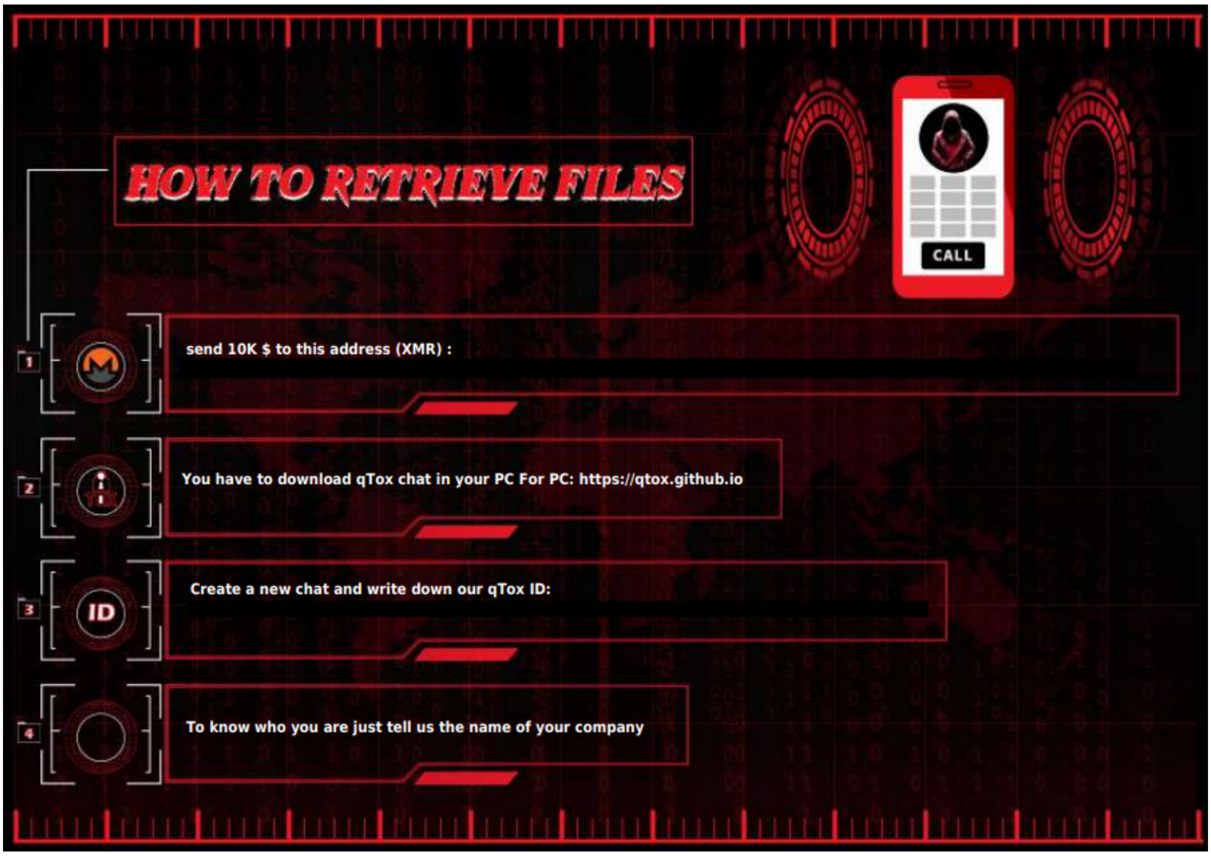


WHAT IS GUARANTEES ?

It's just a business. We absolutely do not car about you and your deals, except getting benefits. If we don't do our work and liabilities, nobody will not cooperate with us. It's not our interests.

If you will not cooperate with us, it doesn't matter. Your data will be published and you will lose the chance to get them back. Don't lose your time with any third party to have the key, cause just we have it ....

Be fast to make the right decision, to not lose .



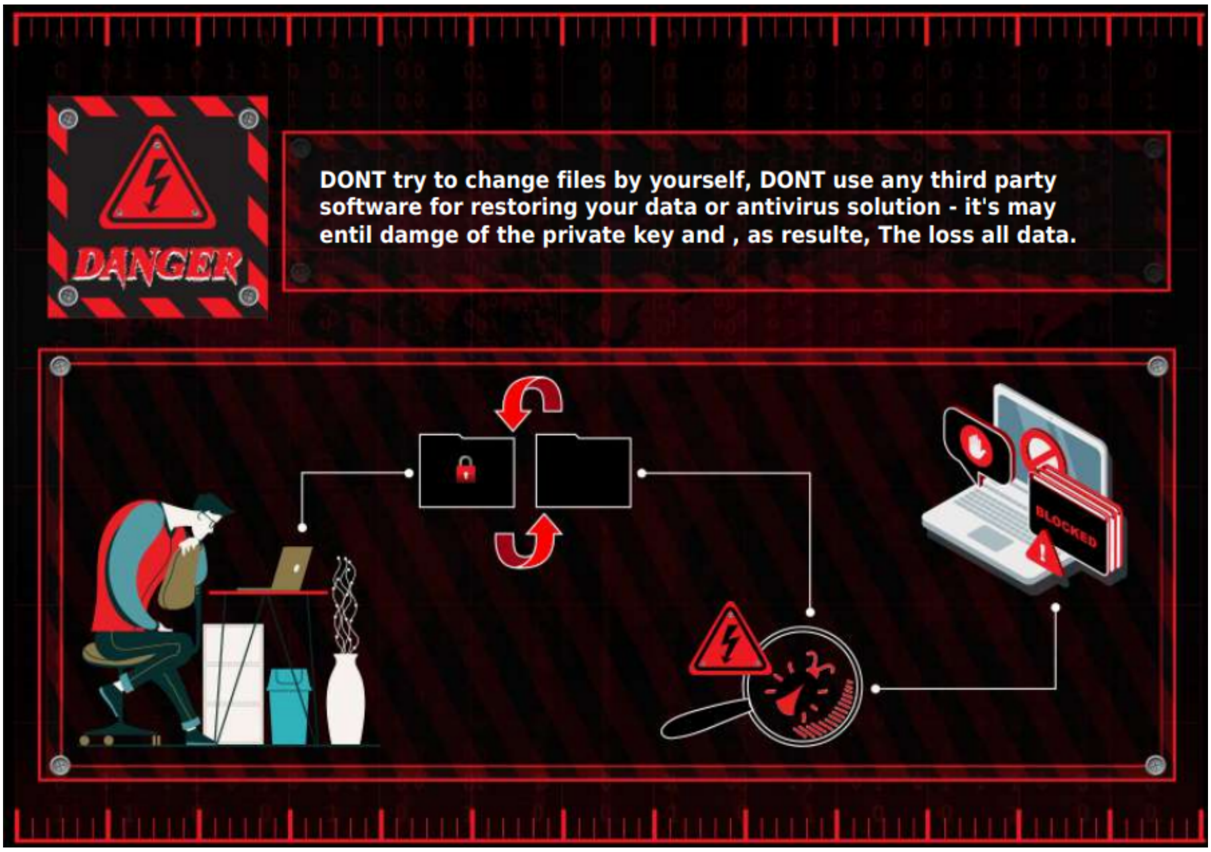
HOW TO RETRIEVE FILES

1 send 10K $ to this address (XMR) : [redacted]

2 You have to download qTox chat in your PC For PC: https://qtox.github.io

3 Create a new chat and write down our qTox ID: [redacted]

4 To know who you are just tell us the name of your company



DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solution - it's may entil damge of the private key and , as resulte, The loss all data.

YARA RULE

```
rule Dark_Power_Ransomware
{
    meta:

        author = "seyitsec"
        date = "2023-03-31"
        hash =
"11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394"

    strings:

        str1= ”GCC: (MinGW-W64 x86_64-posix-seh, built by Brecht
Sanders) 11.1.0”
        str2= ”<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><assembly xmlns="urn:schemas-microsoft-com:asm.v1"
manifestVersion="1.0"><assemblyIdentity version="1.0.0.0"
processorArchitecture="*" name="winim"
type="win32"/><dependency><dependentAssembly><assemblyIdentity
type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0"
processorArchitecture="*" publicKeyToken="6595b64144ccf1df"
language="*"/></dependentAssembly></dependency></assembly>\r\n”
        str3=
”_Z53del_OOZOOZOnimbleZpkgsZwinim4551O56O48ZwinimZcom_1049P57tyObject_v
ariantcolonObjectType___FBSF3pWyJz9clqwLRXzZTsA”
        str4=
”_Z58newTable_OOZOOZOnimbleZpkgsZwinim4551O56O48ZwinimZcom_1907x”



    condition:

        all of ($str*)

}
```

MITRE ATT&CK

ATT&CK NAME	ID
Windows Management Instrumentation	T1047
Shared Modules	T1129
Thread Execution Hijacking	T1055.003
Masquerading	T1036
File Deletion	T1070.004
Virtualization/Sandbox Evasion	T1497
Obfuscated Files or Information	T1027
System Checks	T1497.001
Reflective Code Loading	T1620
System Service Discovery	T1007
Virtualization/Sandbox Evasion	T1497
Query Registry	T1012
System Information Discovery	T1082
File and Directory Discovery	T1083
Data Encrypted For Impact	T1486

DarkPower Ransomware And Groups IOC’s

IOCs

TYPE	VALUE
SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
SHA1	9bddcce91756469051f2385ef36ba8171d99686d
MD5	df134a54ae5dca7963e49d97dd104660

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166