AtomSilo Ransomware Enters the League of Double Extortion

zscaler.com/blogs/security-research/atomsilo-ransomware-enters-league-double-extortion

Ransomware is used widely in cyberattacks to disrupt the victim's organization. Over the last two years, many attackers have evolved their ransomware tactics to include data exfiltration. This tactic is known as "double-extortion": attackers demand ransom for the data decryption in addition to the ransom to prevent public release of the stolen data. ThreatLabz monitors these threat actors and analyzes the attack sequences of double extortion attacks. AtomSilo is a new player on the scene, and in this blog, we'll break down the details of their attacks.

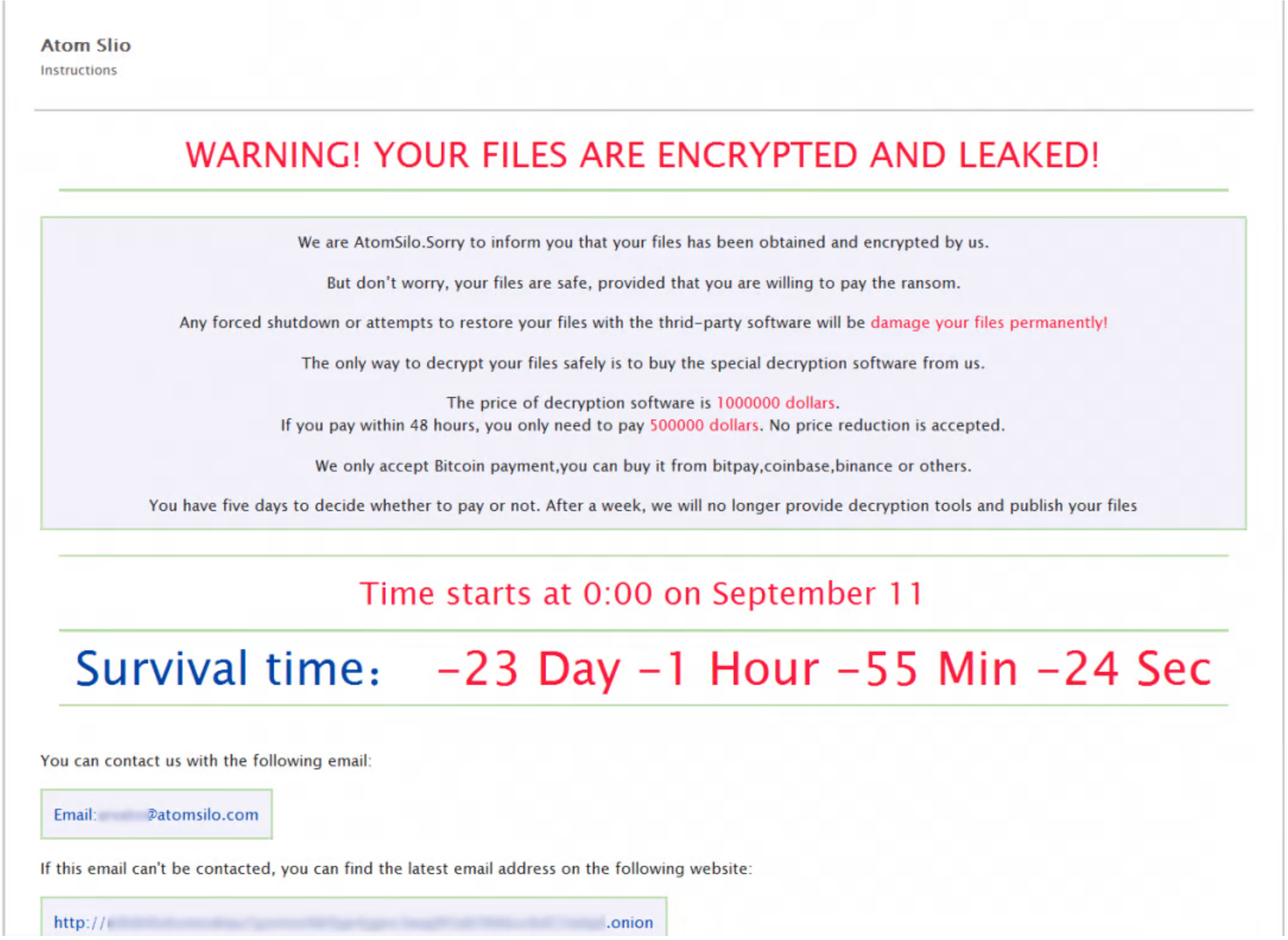
Introduction

AtomSilo ransomware emerged around September 2021, with their tactics including exfiltrating and publishing their first victim's data.

We'll break down one of their attacks, which started with initial access through exploiting a vulnerability in Atlassian’s Confluence collaboration software. The ransomware operators planted a back door using legitimate software via a dll side loading technique. The backdoor allowed remote code execution of Windows Shell commands through WMI (Windows Management Interface), which operators exploited using compromised administrative accounts before dropping AtomSilo.

Technical Analysis

The AtomSilo payload is 64-bit and packed with a modified UPX packer. Once executed, it enumerates each drive and drops a ransom note in each folder except the few listed in *Table1*. The ransom note is named “README-FILE-{COMPUTER_Name}-{DateTime}.hta”.



Atom Slio
Instructions

WARNING! YOUR FILES ARE ENCRYPTED AND LEAKED!

We are AtomSilo.Sorry to inform you that your files has been obtained and encrypted by us.

But don't worry, your files are safe, provided that you are willing to pay the ransom.

Any forced shutdown or attempts to restore your files with the thrid-party software will be damage your files permanently!

The only way to decrypt your files safely is to buy the special decryption software from us.

The price of decryption software is 1000000 dollars.
If you pay within 48 hours, you only need to pay 500000 dollars. No price reduction is accepted.

We only accept Bitcoin payment,you can buy it from bitpay,coinbase,binance or others.

You have five days to decide whether to pay or not. After a week, we will no longer provide decryption tools and publish your files

Time starts at 0:00 on September 11

Survival time: -23 Day -1 Hour -55 Min -24 Sec

You can contact us with the following email:

Email:[redacted]@atomsilo.com

If this email can't be contacted, you can find the latest email address on the following website:

http://[redacted].onion

Figure 1: AtomSilo ransom note

It enumerates each file and encrypts all folders and files EXCEPT those that contain the below names:

Folder name	File name
Boot	autorun.inf
Windows	index.html
Windows.old	boot.ini
Tor Browser	bootfont.bin
Internet Explorer	bootsect.bak
Google	bootmgr

Folder name	File name
Opera	bootmgr.efi
Opera Software	bootmgfw.efi
Mozilla	desktop.ini
Mozilla Firefox	iconcache.db
$recycle.Bin	ntldr
ProgramData	ntuser.dat
All Users	ntuser.dat.log
	#recycle
	thumbs.db
	ntuser.ini

Table1: List of files and folders

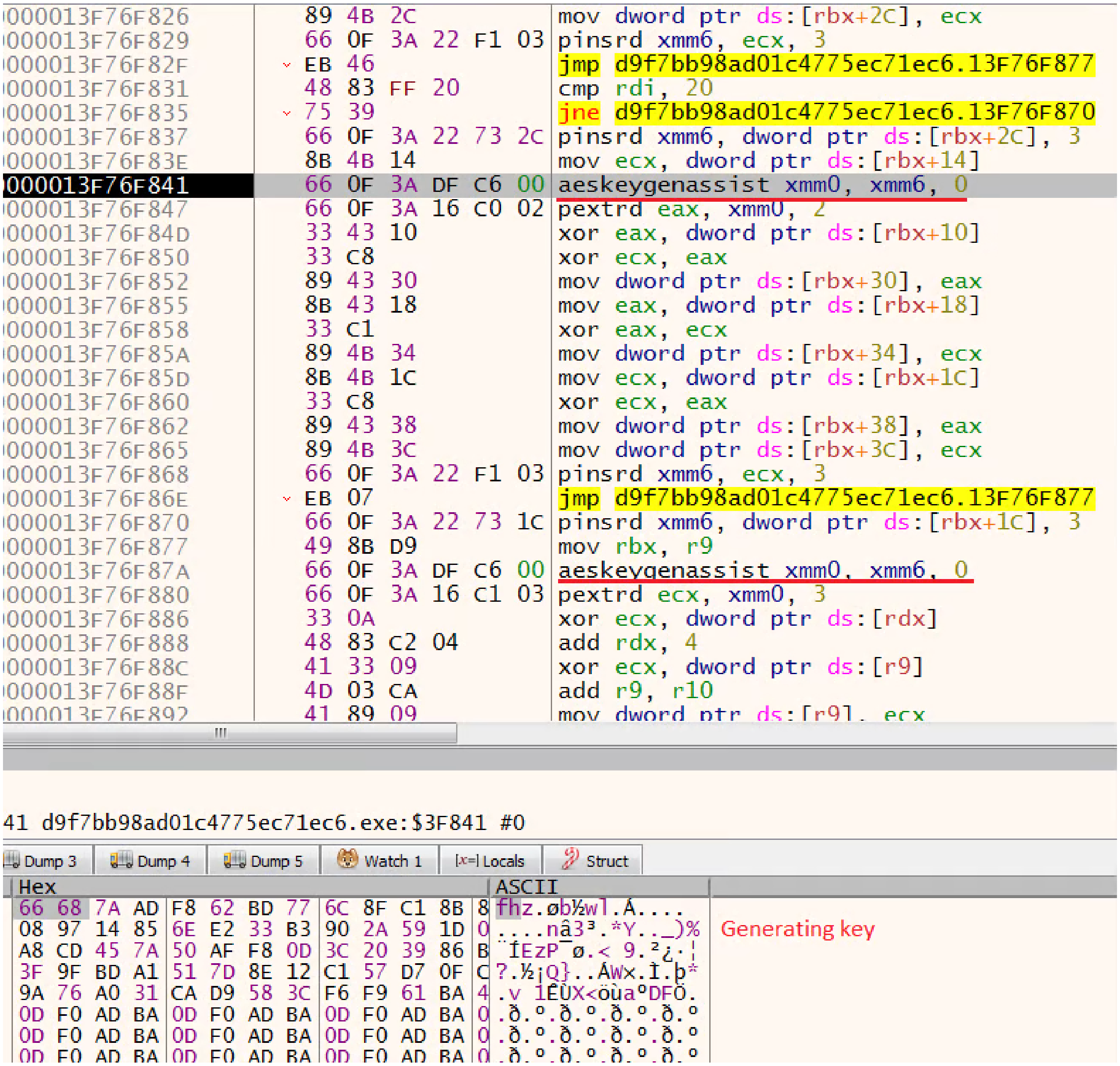
It also does not encrypt files with the following extensions:

.hta	.idx
.hlp	.ini
.html	.sys
.icl	.cab
.exe	.spl
.icns	.cur
.dll	.ocx
.ico	.cpl
.cpl	.drv

Table2: List of extensions

File Encryption

Ransomware appends ".atomsilo" extensions to files after encryption. Ransomware uses "CreateFileMappingA" and "MapViewOfFile" APIs to map the file in memory and moves the pointer to the start of the mapped file. AtomSilo uses XOR and AES Encryption algorithms to encrypt files. It generates AES round keys using the "AESKEYGENASSIST" instruction as shown in the below figure.



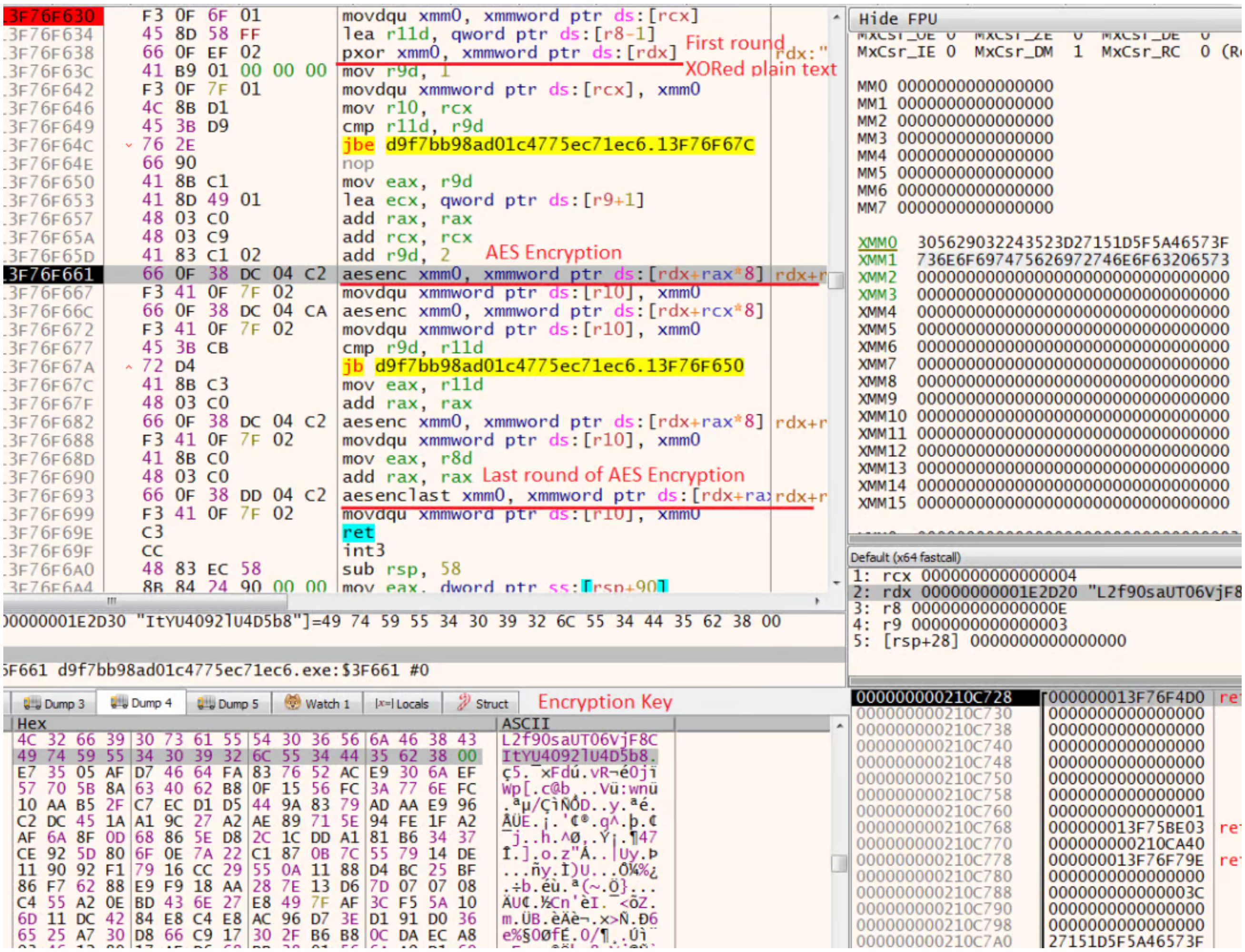
```
000013F76F826   89 4B 2C            mov dword ptr ds:[rbx+2C], ecx
000013F76F829   66 0F 3A 22 F1 03   pinsrd xmm6, ecx, 3
000013F76F82F   EB 46               jmp d9f7bb98ad01c4775ec71ec6.13F76F877
000013F76F831   48 83 FF 20         cmp rdi, 20
000013F76F835   75 39               jne d9f7bb98ad01c4775ec71ec6.13F76F870
000013F76F837   66 0F 3A 22 73 2C   pinsrd xmm6, dword ptr ds:[rbx+2C], 3
000013F76F83E   8B 4B 14            mov ecx, dword ptr ds:[rbx+14]
000013F76F841   66 0F 3A DF C6 00   aeskeygenassist xmm0, xmm6, 0
000013F76F847   66 0F 3A 16 C0 02   pextrd eax, xmm0, 2
000013F76F84D   33 43 10            xor eax, dword ptr ds:[rbx+10]
000013F76F850   33 C8               xor ecx, eax
000013F76F852   89 43 30            mov dword ptr ds:[rbx+30], eax
000013F76F855   8B 43 18            mov eax, dword ptr ds:[rbx+18]
000013F76F858   33 C1               xor eax, ecx
000013F76F85A   89 4B 34            mov dword ptr ds:[rbx+34], ecx
000013F76F85D   8B 4B 1C            mov ecx, dword ptr ds:[rbx+1C]
000013F76F860   33 C8               xor ecx, eax
000013F76F862   89 43 38            mov dword ptr ds:[rbx+38], eax
000013F76F865   89 4B 3C            mov dword ptr ds:[rbx+3C], ecx
000013F76F868   66 0F 3A 22 F1 03   pinsrd xmm6, ecx, 3
000013F76F86E   EB 07               jmp d9f7bb98ad01c4775ec71ec6.13F76F877
000013F76F870   66 0F 3A 22 73 1C   pinsrd xmm6, dword ptr ds:[rbx+1C], 3
000013F76F877   49 8B D9            mov rbx, r9
000013F76F87A   66 0F 3A DF C6 00   aeskeygenassist xmm0, xmm6, 0
000013F76F880   66 0F 3A 16 C1 03   pextrd ecx, xmm0, 3
000013F76F886   33 0A               xor ecx, dword ptr ds:[rdx]
000013F76F888   48 83 C2 04         add rdx, 4
000013F76F88C   41 33 09            xor ecx, dword ptr ds:[r9]
000013F76F88F   4D 03 CA            add r9, r10
000013F76F892   41 89 09            mov dword ptr ds:[r9], ecx

41 d9f7bb98ad01c4775ec71ec6.exe:$3F841 #0
```

```
Hex                                            ASCII
66 68 7A AD F8 62 BD 77 6C 8F C1 8B 8          fhz.øb½wl.Á....
08 97 14 85 6E E2 33 B3 90 2A 59 1D 0          ....nâ3³.*Y.._)%
A8 CD 45 7A 50 AF F8 0D 3C 20 39 86 B          ¨ÍEzP¯ø.< 9.²¿·¦
3F 9F BD A1 51 7D 8E 12 C1 57 D7 0F C          ?.½¡Q}..ÁWx.Ì.þ*
9A 76 A0 31 CA D9 58 3C F6 F9 61 BA 4          .v 1ÊÙX<öùaºDFÖ.
0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0          .ð.º.ð.º.ð.º.ð.º
0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0          .ð.º.ð.º.ð.º.ð.º
0D F0 AD BA 0D F0 AD BA 0D F0 AD BA 0          .ð.º.ð.º.ð.º.ð.º
```

Generating key

Figure 2: AtomSilo generates encryption keys using AESKEYGENASSIST

The encryption key is 240 bytes. The first 32 bytes are randomly generated by the payload, and other 208 bytes are generated using the "AESKEYGENASSIST" instruction. In the file , it takes 16 bytes of plain text and does XOR as a first stage encryption. Then, it encrypts it with 14 rounds of AES encryption. It uses "AESENC" instruction for the first 13 rounds and the last round uses "AESENCLAST" instruction.



```
.3F76F630   F3 0F 6F 01         movdqu xmm0, xmmword ptr ds:[rcx]
.3F76F634   45 8D 58 FF         lea r11d, qword ptr ds:[r8-1]
.3F76F638   66 0F EF 02         pxor xmm0, xmmword ptr ds:[rdx]      rdx:"
.3F76F63C   41 B9 01 00 00 00   mov r9d, 1
.3F76F642   F3 0F 7F 01         movdqu xmmword ptr ds:[rcx], xmm0
.3F76F646   4C 8B D1            mov r10, rcx
.3F76F649   45 3B D9            cmp r11d, r9d
.3F76F64C   76 2E               jbe d9f7bb98ad01c4775ec71ec6.13F76F67C
.3F76F64E   66 90               nop
.3F76F650   41 8B C1            mov eax, r9d
.3F76F653   41 8D 49 01         lea ecx, qword ptr ds:[r9+1]
.3F76F657   48 03 C0            add rax, rax
.3F76F65A   48 03 C9            add rcx, rcx
.3F76F65D   41 83 C1 02         add r9d, 2
.3F76F661   66 0F 38 DC 04 C2   aesenc xmm0, xmmword ptr ds:[rdx+rax*8]  rdx+r
.3F76F667   F3 41 0F 7F 02      movdqu xmmword ptr ds:[r10], xmm0
.3F76F66C   66 0F 38 DC 04 CA   aesenc xmm0, xmmword ptr ds:[rdx+rcx*8]
.3F76F672   F3 41 0F 7F 02      movdqu xmmword ptr ds:[r10], xmm0
.3F76F677   45 3B CB            cmp r9d, r11d
.3F76F67A   72 D4               jb d9f7bb98ad01c4775ec71ec6.13F76F650
.3F76F67C   41 8B C3            mov eax, r11d
.3F76F67F   48 03 C0            add rax, rax
.3F76F682   66 0F 38 DC 04 C2   aesenc xmm0, xmmword ptr ds:[rdx+rax*8]  rdx+r
.3F76F688   F3 41 0F 7F 02      movdqu xmmword ptr ds:[r10], xmm0
.3F76F68D   41 8B C0            mov eax, r8d
.3F76F690   48 03 C0            add rax, rax
.3F76F693   66 0F 38 DD 04 C2   aesenclast xmm0, xmmword ptr ds:[rdx+ra  rdx+r
.3F76F699   F3 41 0F 7F 02      movdqu xmmword ptr ds:[r10], xmm0
.3F76F69E   C3                  ret
.3F76F69F   CC                  int3
.3F76F6A0   48 83 EC 58         sub rsp, 58
.3F76F6A4   8B 84 24 90 00 00   mov eax, dword ptr ss:[rsp+90]

)0000001E2D30 "ItYU4092lU4D5b8"]=49 74 59 55 34 30 39 32 6C 55 34 44 35 62 38 00

5F661 d9f7bb98ad01c4775ec71ec6.exe:$3F661 #0
```

First round XORed plain text

AES Encryption

Last round of AES Encryption

```
Hide FPU
MxCsr_IE 0   MxCsr_DM  1   MxCsr_RC  0 (R

MM0 0000000000000000
MM1 0000000000000000
MM2 0000000000000000
MM3 0000000000000000
MM4 0000000000000000
MM5 0000000000000000
MM6 0000000000000000
MM7 0000000000000000

XMM0   305629032243523D27151D5F5A46573F
XMM1   736E6F697475626972746E6F63206573
XMM2   00000000000000000000000000000000
XMM3   00000000000000000000000000000000
XMM4   00000000000000000000000000000000
XMM5   00000000000000000000000000000000
XMM6   00000000000000000000000000000000
XMM7   00000000000000000000000000000000
XMM8   00000000000000000000000000000000
XMM9   00000000000000000000000000000000
XMM10  00000000000000000000000000000000
XMM11  00000000000000000000000000000000
XMM12  00000000000000000000000000000000
XMM13  00000000000000000000000000000000
XMM14  00000000000000000000000000000000
XMM15  00000000000000000000000000000000

Default (x64 fastcall)
1: rcx 0000000000000004
2: rdx 00000000001E2D20 "L2f90saUT06VjF8
3: r8 000000000000000E
4: r9 0000000000000003
5: [rsp+28] 0000000000000000
```

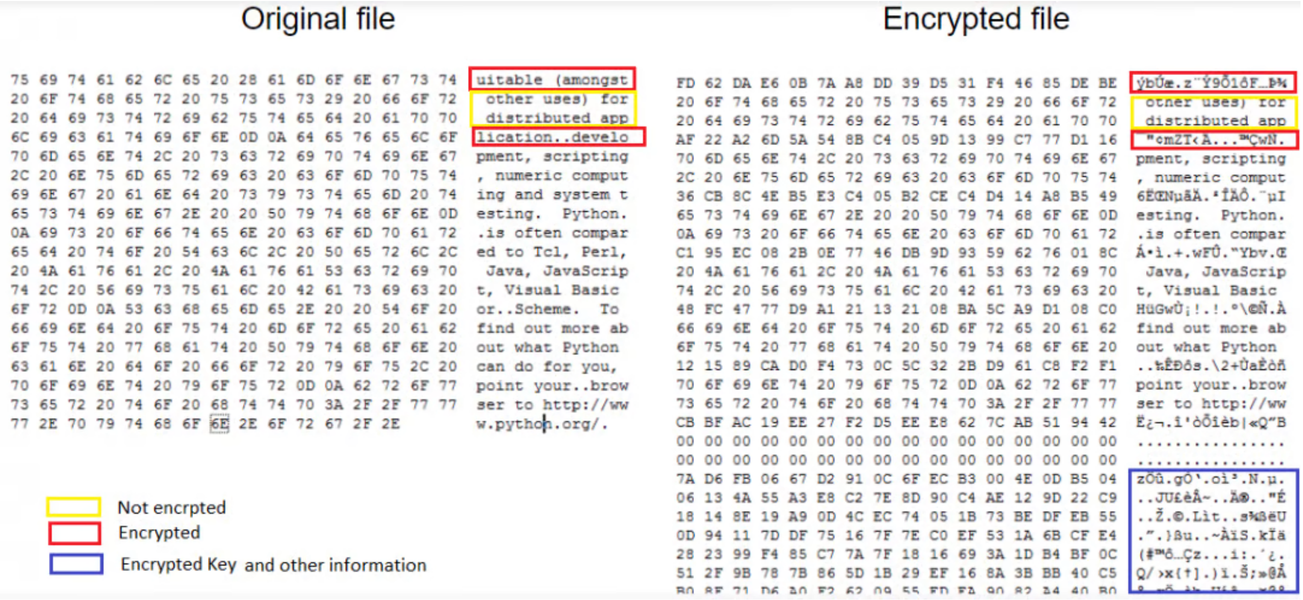
Encryption Key

```
Hex                                               ASCII
4C 32 66 39 30 73 61 55 54 30 36 56 6A 46 38 43   L2f90saUT06VjF8C
49 74 59 55 34 30 39 32 6C 55 34 44 35 62 38 00   ItYU4092lU4D5b8.
E7 35 05 AF D7 46 64 FA 83 76 52 AC E9 30 6A EF   ç5.¯×Fdú.vR¬é0jï
57 70 5B 8A 63 40 62 B8 0F 15 56 FC 3A 77 6E FC   Wp[.c@b¸..Vü:wnü
10 AA B5 2F C7 EC D1 D5 44 9A 83 79 AD AA E9 96   .ªµ/ÇìÑÕD..y.ªé.
C2 DC 45 1A A1 9C 27 A2 AE 89 71 5E 94 FE 1F A2   ÂÜE.¡.'¢®.q^.þ.¢
AF 6A 8F 0D 68 86 5E D8 2C 1C DD A1 81 B6 34 37   ¯j..h.^Ø,.Ý¡.¶47
CE 92 5D 80 6F 0E 7A 22 C1 87 0B 7C 55 79 14 DE   Î.].o.z"Á..|Uy.Þ
11 90 92 F1 79 16 CC 29 55 0A 11 88 D4 BC 25 BF   ...ñy.Ì)U...Ô¼%¿
86 F7 62 88 E9 F9 18 AA 28 7E 13 D6 7D 07 07 08   .÷b.éù.ª(~.Ö}...
C4 55 A2 0E BD 43 6E 27 E8 49 7F AF 3C F5 5A 10   ÄU¢.½Cn'èI.¯<õZ.
6D 11 DC 42 84 E8 C4 E8 AC 96 D7 3E D1 91 D0 36   m.ÜB.èÄè¬.×>Ñ.Ð6
65 25 A7 30 D8 66 C9 17 30 2F B6 B8 0C DA EC A8   e%§0ØfÉ.0/¶¸.Úì¨
```

```
000000000210C728   000000013F76F4D0   re
000000000210C730   0000000000000000
000000000210C738   0000000000000000
000000000210C740   0000000000000000
000000000210C748   0000000000000000
000000000210C750   0000000000000000
000000000210C758   0000000000000000
000000000210C760   0000000000000001
000000000210C768   000000013F75BE03   re
000000000210C770   000000000210CA40
000000000210C778   000000013F76F79E   re
000000000210C780   0000000000000000
000000000210C788   000000000000003C
000000000210C790   0000000000000000
000000000210C798   0000000000000000
000000000210C7A0   27151D5F5A46573F
```

Figure 3: Encrypting data using AES algorithm

It encrypts chunks of the file, not the complete file. It encrypts the first 16 bytes, leaves the next 32 bytes as-is, encrypts the next 16 bytes, and so on. The below screenshot shows the comparison of the normal file and encrypted file, where we can see that chunks of files are not encrypted. The encryption key and other information are encrypted and appended at the end of the encrypted file.



Original file

```
75 69 74 61 62 6C 65 20 28 61 6D 6F 6E 67 73 74  uitable (amongst
20 6F 74 68 65 72 20 75 73 65 73 29 20 66 6F 72   other uses) for
20 64 69 73 74 72 69 62 75 74 65 64 20 61 70 70   distributed app
6C 69 63 61 74 69 6F 6E 0D 0A 64 65 76 65 6C 6F  lication..develo
70 6D 65 6E 74 2C 20 73 63 72 69 70 74 69 6E 67  pment, scripting
2C 20 6E 75 6D 65 72 69 63 20 63 6F 6D 70 75 74  , numeric comput
69 6E 67 20 61 6E 64 20 73 79 73 74 65 6D 20 74  ing and system t
65 73 74 69 6E 67 2E 20 20 50 79 74 68 6F 6E 0D  esting.  Python.
0A 69 73 20 6F 66 74 65 6E 20 63 6F 6D 70 61 72  .is often compar
65 64 20 74 6F 20 54 63 6C 2C 20 50 65 72 6C 2C  ed to Tcl, Perl,
20 4A 61 76 61 2C 20 4A 61 76 61 53 63 72 69 70   Java, JavaScrip
74 2C 20 56 69 73 75 61 6C 20 42 61 73 69 63 20  t, Visual Basic
6F 72 0D 0A 53 63 68 65 6D 65 2E 20 20 54 6F 20  or..Scheme.  To
66 69 6E 64 20 6F 75 74 20 6D 6F 72 65 20 61 62  find out more ab
6F 75 74 20 77 68 61 74 20 50 79 74 68 6F 6E 20  out what Python
63 61 6E 20 64 6F 20 66 6F 72 20 79 6F 75 2C 20  can do for you,
70 6F 69 6E 74 20 79 6F 75 72 0D 0A 62 72 6F 77  point your..brow
73 65 72 20 74 6F 20 68 74 74 70 3A 2F 2F 77 77  ser to http://ww
77 2E 70 79 74 68 6F 6E 2E 6F 72 67 2F 2E        w.python.org/.
```

Encrypted file

```
FD 62 DA E6 0B 7A A8 DD 39 D5 31 F4 46 85 DE BE  ýbÚæ.z¨Ý9Õ1ôF…Þ¾
20 6F 74 68 65 72 20 75 73 65 73 29 20 66 6F 72   other uses) for
20 64 69 73 74 72 69 62 75 74 65 64 20 61 70 70   distributed app
AF 22 A2 6D 5A 54 8B C4 05 9D 13 99 C7 77 D1 16  ¯"¢mZT‹Ä...™ÇwÑ.
70 6D 65 6E 74 2C 20 73 63 72 69 70 74 69 6E 67  pment, scripting
2C 20 6E 75 6D 65 72 69 63 20 63 6F 6D 70 75 74  , numeric comput
36 CB 8C 4E B5 E3 C4 05 B2 CE C4 D4 14 A8 B5 49  6ËŒNµãÄ.²ÎÄÔ.¨µI
65 73 74 69 6E 67 2E 20 20 50 79 74 68 6F 6E 0D  esting.  Python.
0A 69 73 20 6F 66 74 65 6E 20 63 6F 6D 70 61 72  .is often compar
C1 95 EC 08 2B 0E 77 46 DB 9D 93 59 62 76 01 8C  Á•ì.+.wFÛ."Ybv.Œ
20 4A 61 76 61 2C 20 4A 61 76 61 53 63 72 69 70   Java, JavaScrip
74 2C 20 56 69 73 75 61 6C 20 42 61 73 69 63 20  t, Visual Basic
48 FC 47 77 D9 A1 21 13 21 08 BA 5C A9 D1 08 C0  HüGwÙ¡!.!.º\©Ñ.À
66 69 6E 64 20 6F 75 74 20 6D 6F 72 65 20 61 62  find out more ab
6F 75 74 20 77 68 61 74 20 50 79 74 68 6F 6E 20  out what Python
12 15 89 CA D0 F4 73 0C 5C 32 2B D9 61 C8 F2 F1  ..‰ÊÐôs.\2+ÙaÈòñ
70 6F 69 6E 74 20 79 6F 75 72 0D 0A 62 72 6F 77  point your..brow
73 65 72 20 74 6F 20 68 74 74 70 3A 2F 2F 77 77  ser to http://ww
CB BF AC 19 EE 27 F2 D5 EE E8 62 7C AB 51 94 42  Ë¿¬.î'òÕîèb|«Q"B
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
7A D6 FB 06 67 D2 91 0C 6F EC B3 00 4E 0D B5 04  zÖû.gÒ'.oì³.N.µ.
06 13 4A 55 A3 E8 C2 7E 8D 90 C4 AE 12 9D 22 C9  ..JU£èÂ~..Ä®.."É
18 14 8E 19 A9 0D 4C EC 74 05 1B 73 BE DF EB 55  ..Ž.©.Lìt..s¾ßëU
0D 94 11 7D DF 75 16 7F 7E C0 EF 53 1A 6B CF E4  .".}ßu..~ÀïS.kÏä
28 23 99 F4 85 C7 7A 7F 18 16 69 3A 1D B4 BF 0C  (#™ô…Çz...i:.´¿.
51 2F 9B 78 7B 86 5D 1B 29 EF 16 8A 3B BB 40 C5  Q/›x{†].)ï.Š;»@Å
B0 8F 71 D6 A0 F2 62 09 55 FD FA 90 82 A4 40 B0
```

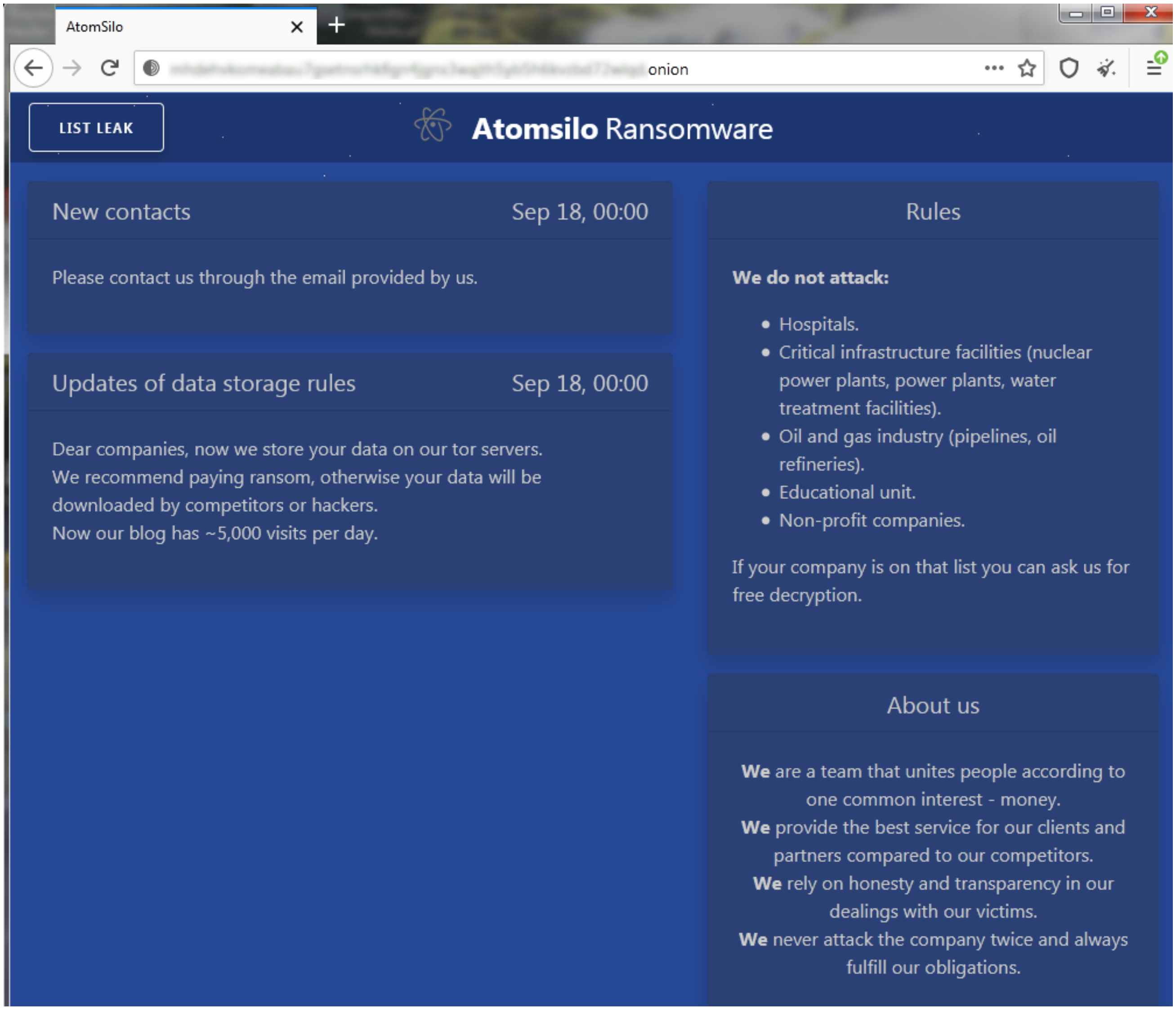
Figure 4: Original vs Encrypted file

Data Leak site

According to their leak sites, AtomSilo actors won't attack the following types of organizations:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Educational unit.
- Non-profit companies.

They also promise to provide free decryption if the victim company is on the above list.



Atomsilo Ransomware

New contacts Sep 18, 00:00

Please contact us through the email provided by us.

Updates of data storage rules Sep 18, 00:00

Dear companies, now we store your data on our tor servers.
We recommend paying ransom, otherwise your data will be downloaded by competitors or hackers.
Now our blog has ~5,000 visits per day.

Rules

We do not attack:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Educational unit.
- Non-profit companies.

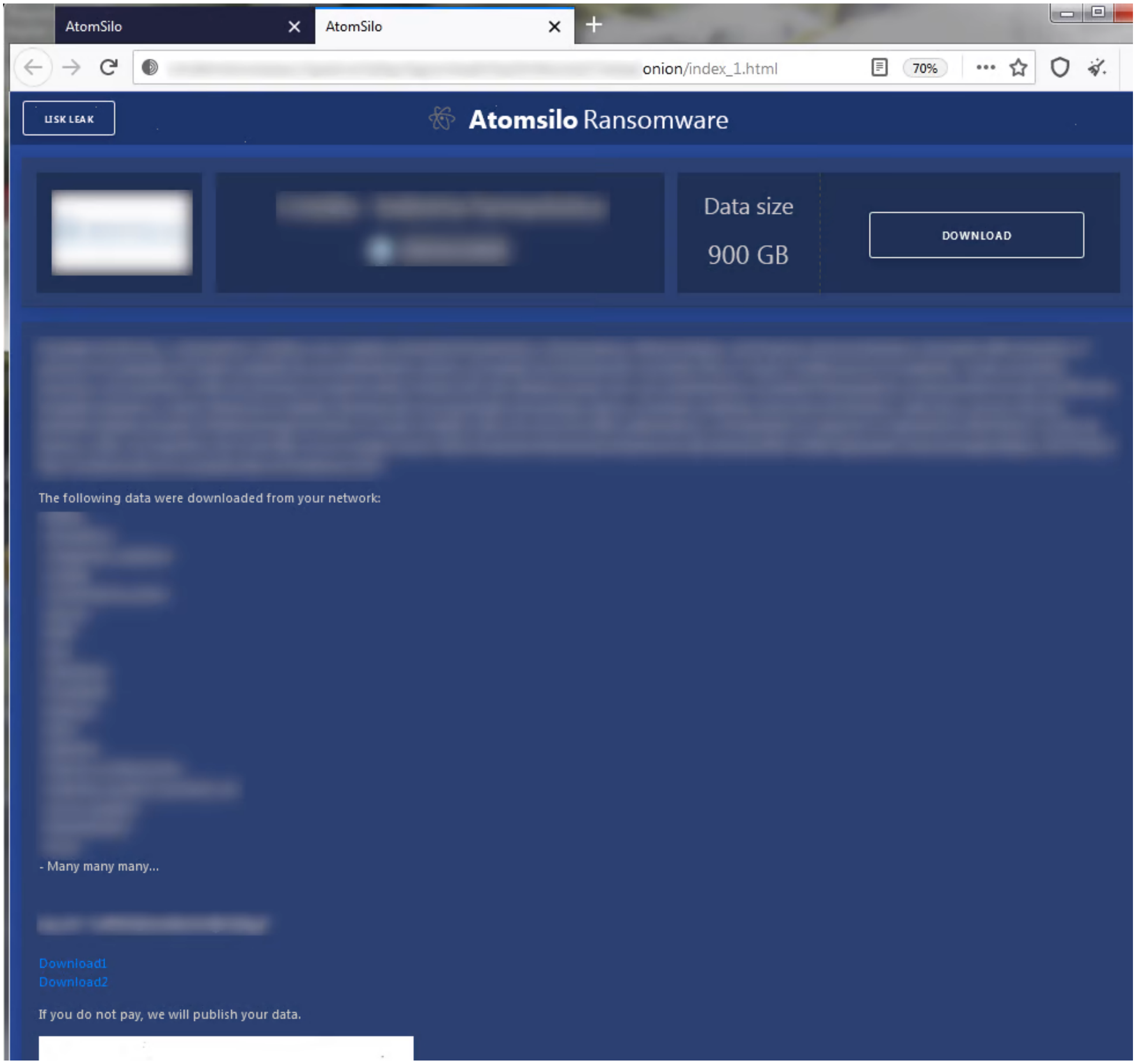
If your company is on that list you can ask us for free decryption.

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.

Figure 5: Data leak site

The first data leak was from a Brazilian Pharmaceutical company. AtomSilo published around 900 GB data as shown in the below screenshot:



Atomsilo Ransomware

[redacted]

Data size

900 GB

[redacted]

The following data were downloaded from your network:

[redacted]

- Many many many...

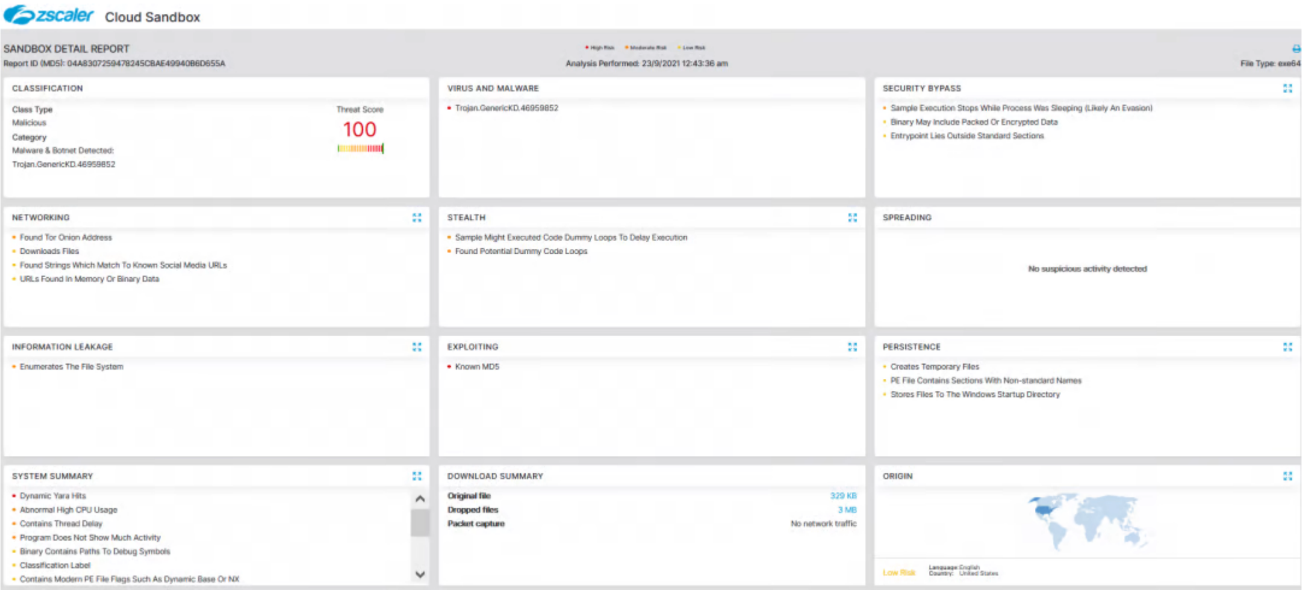
[redacted]

Download1
Download2

If you do not pay, we will publish your data.

Figure 6: Victim data published on data leak site

Cloud Sandbox Detection



SANDBOX DETAIL REPORT

Report ID (MD5): 04A8307259478245CBAE49940B6D655A

Analysis Performed: 23/9/2021 12:43:36 am

File Type: exe64

CLASSIFICATION

Class Type
Malicious
Category
Malware & Botnet Detected:
Trojan.GenericKD.46959852

Threat Score
100

VIRUS AND MALWARE

- Trojan.GenericKD.46959852

SECURITY BYPASS

- Sample Execution Stops While Process Was Sleeping (Likely An Evasion)
- Binary May Include Packed Or Encrypted Data
- Entrypoint Lies Outside Standard Sections

NETWORKING

- Found Tor Onion Address
- Downloads Files
- Found Strings Which Match To Known Social Media URLs
- URLs Found In Memory Or Binary Data

STEALTH

- Sample Might Executed Code Dummy Loops To Delay Execution
- Found Potential Dummy Code Loops

SPREADING

No suspicious activity detected

INFORMATION LEAKAGE

- Enumerates The File System

EXPLOITING

- Known MD5

PERSISTENCE

- Creates Temporary Files
- PE File Contains Sections With Non-standard Names
- Stores Files To The Windows Startup Directory

SYSTEM SUMMARY

- Dynamic Yara Hits
- Abnormal High CPU Usage
- Contains Thread Delay
- Program Does Not Show Much Activity
- Binary Contains Paths To Debug Symbols
- Classification Label
- Contains Modern PE File Flags Such As Dynamic Base Or NX

DOWNLOAD SUMMARY

Original file	329 KB
Dropped files	3 MB
Packet capture	No network traffic

ORIGIN

Low Risk
Language: English
Country: United States

Figure 7: Zscaler Cloud Sandbox detection of AtomSilo ransomware

In addition to sandbox detections, Zscaler's multilayered cloud security platform detects indicators at various levels.

Win64.Ransom.AtomSilo

IOC

Md5

04a8307259478245cbae49940b6d655a