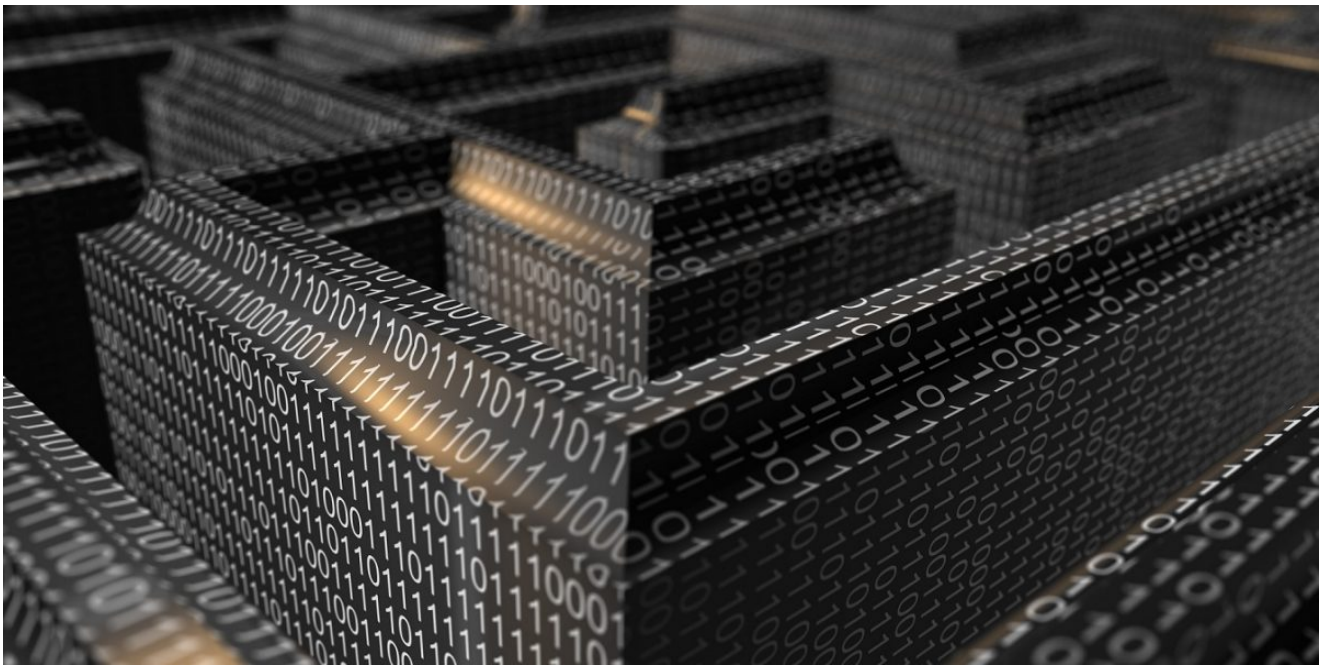
Life of Maze ransomware

SL securelist.com/maze-ransomware/99137/

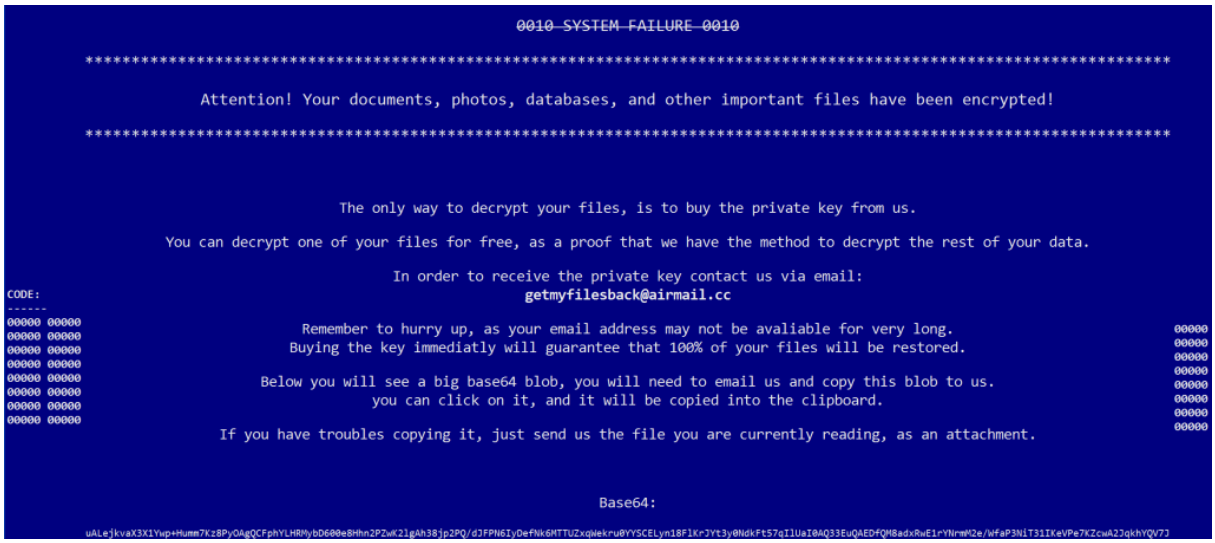


Authors

- Expert Fedor Sinitsyn
- Expert Nikita Galimov
-  Vladimir Kuskov

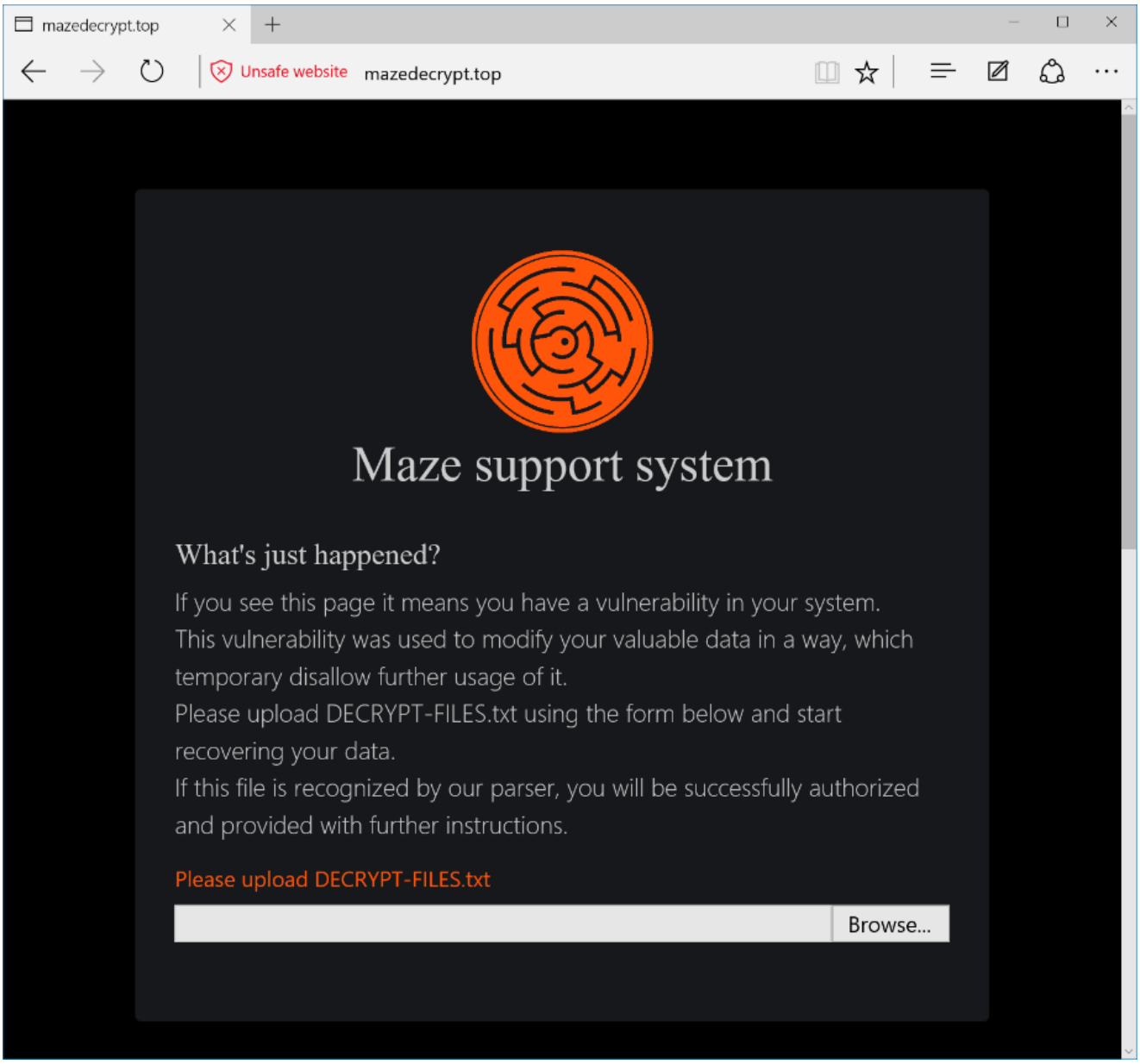
In the past year, Maze ransomware has become one of the most notorious malware families threatening businesses and large organizations. Dozens of organizations have fallen victim to this vile malware, including LG, Southwire, and the City of Pensacola.

The history of this ransomware began in the first half of 2019, and back then it didn't have any distinct branding – the ransom note included the title "0010 System Failure 0010", and it was referenced by researchers simply as 'ChaCha ransomware'.



Ransom note of an early version of Maze/ChaCha ransomware

Shortly afterwards, new versions of this Trojan started calling themselves Maze and using a relevantly named website for the victims instead of the generic email address shown in the screenshot above.

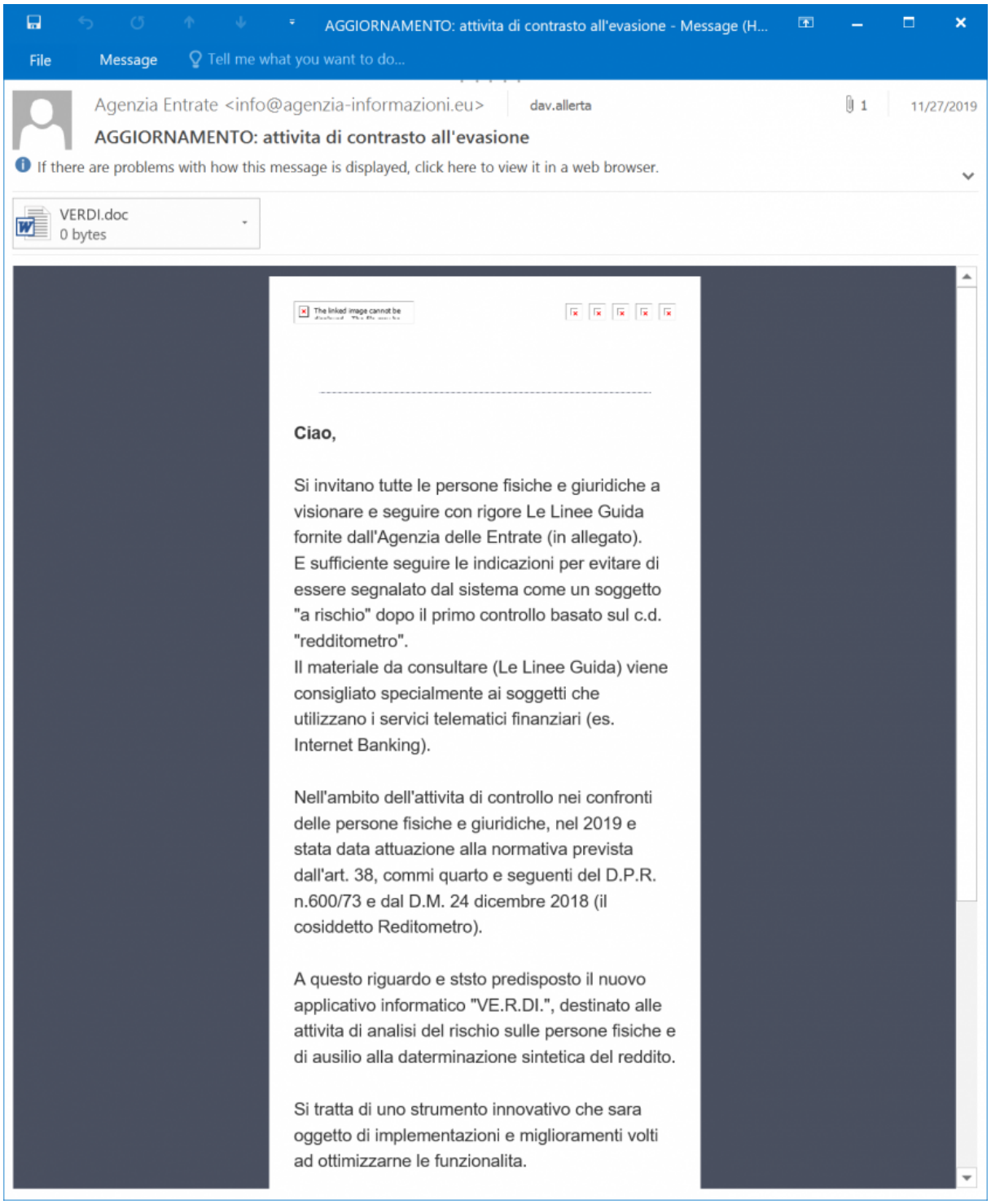


Website used by a recent version of Maze ransomware

Infection scenarios

Mass campaigns

The distribution tactic of the Maze ransomware initially involved infections via exploit kits (namely, Fallout EK and Spelevo EK), as well as via spam with malicious attachments. Below is an example of one of these malicious spam messages containing an MS Word document with a macro that's intended to download the Maze ransomware payload.



If the recipient opens the attached document, they will be prompted to enable editing mode and then enable the content. If they fall for it, the malicious macro contained inside the document will execute, which in turn will result in the victim's PC being infected with Maze ransomware.

Tailored approach

In addition to these typical infection vectors, the threat actors behind Maze ransomware started targeting corporations and municipal organizations in order to maximize the amount of money extorted.

The initial compromise mechanism and subsequent tactics vary. Some incidents involved spear-phishing campaigns that installed Cobalt Strike RAT, while in other cases the network breach was the result of exploiting a vulnerable internet-facing service (e.g. Citrix ADC/Netscaler or Pulse Secure VPN). Weak RDP credentials on machines accessible from the internet also pose a threat as the operators of Maze may use this flaw as well.

Privilege escalation, reconnaissance and lateral movement tactics also tend to differ from case to case. During these stages, the use of the following tools has been observed: mimikatz, procdump, Cobalt Strike, Advanced IP Scanner, Bloodhound, PowerSploit, and others.

During these intermediate stages, the threat actors attempt to identify valuable data stored on the servers and workstations in the compromised network. They will then exfiltrate the victim's confidential files in order to leverage them when negotiating the size of the ransom.

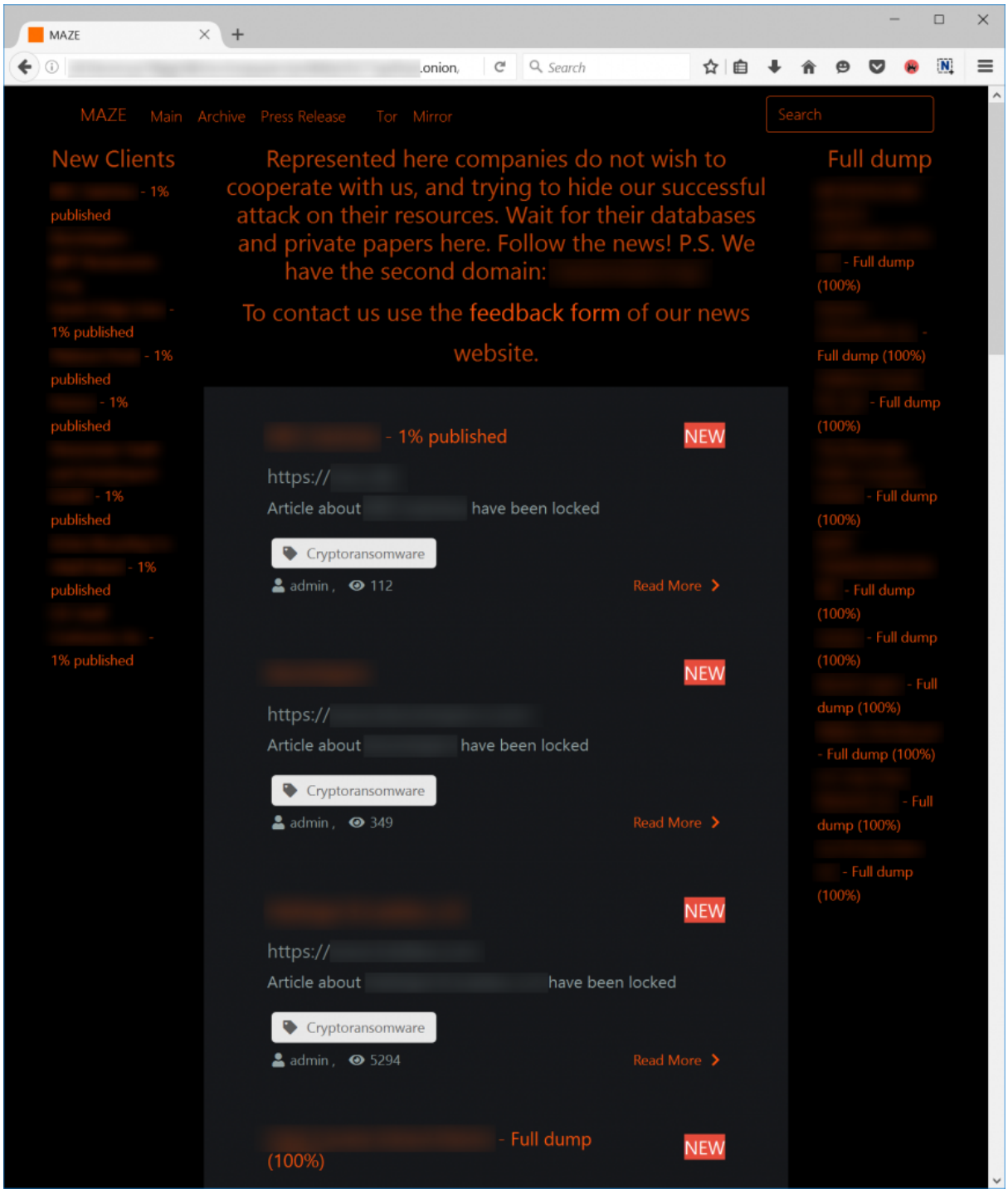
At the final stage of the intrusion, the malicious operators will install the Maze ransomware executable onto all the machines they can access. This results in the encryption of the victim's valuable data and finalizes the attack.

Data leaks/doxing

Maze ransomware was one of the first ransomware families that threatened to leak the victims' confidential data if they refused to cooperate.

In fact, this made Maze something of a trendsetter because this approach turned out to be so lucrative for the criminals that it's now become standard for several notorious ransomware gangs, including REvil/Sodinokibi, DoppelPaymer, JSWorm/Nemty/Nefilim, RagnarLocker, and Snatch.

The authors of the Maze ransomware maintain a website where they list their recent victims and publish a partial or a full dump of the documents they have managed to exfiltrate following a network compromise.



Website with leaked data published by Maze operators

Ransomware cartel

In June 2020, the criminals behind Maze teamed up with two other threat actor groups, LockBit and RagnarLocker, essentially forming a 'ransomware cartel'. The data stolen by these groups now gets published on the blog maintained by the Maze operators.

It wasn't just the hosting of exfiltrated documents where the criminals pooled their efforts – apparently they are also sharing their expertise. Maze now uses execution techniques that were previously only used by RagnarLocker.

Brief technical overview

The Maze ransomware is typically distributed as a PE binary (EXE or DLL depending on the specific scenario) which is developed in C/C++ and obfuscated by a custom protector. It employs various tricks to hinder static analysis, including dynamic API function imports, control flow obfuscation using conditional jumps, replacing RET with JMP dword ptr [esp-4], replacing CALL with PUSH + JMP, and several other techniques.

To counter dynamic analysis, this Trojan will also terminate processes typically used by researchers, e.g. procmon, procexp, ida, x32dbg, etc.

The cryptographic scheme used by Maze consists of several levels:

- To encrypt the content of the victim's files, the Trojan securely generates unique keys and nonce values to use with the ChaCha stream cipher;
- The ChaCha keys and nonce values are encrypted by a session public RSA-2048 key which is generated when the malware is launched;
- The session private RSA-2048 key is encrypted by the master public RSA-2048 key hardcoded in the Trojan's body.

This scheme is a variation of a more or less typical approach used by developers of modern ransomware. It allows the operators to keep their master private RSA key secret when selling decryptors for each individual victim, and it also ensures that a decryptor purchased by one victim won't help others.

When executing on a machine, Maze ransomware will also attempt to determine what kind of PC it has infected. It tries to distinguish between different types of system ('backup server', 'domain controller', 'standalone server', etc.). Using this information in the ransom note, the Trojan aims to further scare the victims into thinking that the criminals know everything about the affected network.

```
.rdata:0044A9A8                         aMazeRansomware:
.rdata:0044A9A8 4D 00 61 00 7A 00 65 00+                text "UTF-16LE", 'Maze Ransomware',0
.rdata:0044A9C8                         aSDearSYourFile:
.rdata:0044A9C8 25 00 73 00 0A 00 0A 00+                text "UTF-16LE", '%s',0Ah
.rdata:0044A9C8 44 00 65 00 61 00 72 00+                text "UTF-16LE", 0Ah
.rdata:0044A9C8 20 00 25 00 73 00 2C 00+                text "UTF-16LE", 'Dear %s, your files have been encrypted by RSA-2048'
.rdata:0044A9C8 20 00 79 00 6F 00 75 00+                text "UTF-16LE", ' and ChaCha algorithms',0Ah
.rdata:0044A9C8 72 00 20 00 66 00 69 00+                text "UTF-16LE", 'The only way to restore them is to buy decryptor',0Ah
.rdata:0044A9C8 6C 00 65 00 73 00 20 00+                text "UTF-16LE", 0Ah
.rdata:0044A9C8 68 00 61 00 76 00 65 00+                text "UTF-16LE", 'These algorithms are one of the strongest',0Ah
.rdata:0044A9C8 20 00 62 00 65 00 65 00+                text "UTF-16LE", 'You can read about them at wikipedia',0Ah
.rdata:0044A9C8 6E 00 20 00 65 00 6E 00+                text "UTF-16LE", 0Ah
.rdata:0044A9C8 63 00 72 00 79 00 70 00+                text "UTF-16LE", 'If you understand the importance of situation you c'
.rdata:0044A9C8 74 00 65 00 64 00 20 00+                text "UTF-16LE", 'an restore all files by following instructions in D'
.rdata:0044A9C8 62 00 79 00 20 00 52 00+                text "UTF-16LE", 'ECRYPT-FILES.txt file',0Ah
.rdata:0044A9C8 53 00 41 00 2D 00 32 00+                text "UTF-16LE", 0Ah
.rdata:0044A9C8 30 00 34 00 38 00 20 00+                text "UTF-16LE", 'You can decrypt 3 files for free as a proof of work'
.rdata:0044A9C8 61 00 6E 00 64 00 20 00+                text "UTF-16LE", 0Ah
.rdata:0044A9C8 43 00 68 00 61 00 43 00+                text "UTF-16LE", 'We know that this computer is ',0
.rdata:0044AD08                         aAStandaloneSer:                ; DATA XREF: .text:loc_438769↑o
.rdata:0044AD08 61 00 20 00 73 00 74 00+                text "UTF-16LE", 'a standalone server',0
.rdata:0044AD30                         aAServerInCorpo:                ; DATA XREF: .text:loc_438770↑o
.rdata:0044AD30 61 00 20 00 73 00 65 00+                text "UTF-16LE", 'a server in corporate network',0
.rdata:0044AD6C                         aAWorkstationIn:                ; CODE XREF: .text:004386F0↑j
.rdata:0044AD6C 61 00 20 00 77 00 6F 00+                text "UTF-16LE", 'a workstation in corporate network',0
.rdata:0044ADB2                         aAPrimaryDomain:                ; DATA XREF: .text:loc_43877E↑o
.rdata:0044ADB2 61 00 20 00 70 00 72 00+                text "UTF-16LE", 'a primary domain controller',0
.rdata:0044ADEA                         aABackupServer:                 ; DATA XREF: .text:loc_438777↑o
.rdata:0044ADEA 61 00 20 00 62 00 61 00+                text "UTF-16LE", 'a backup server',0
.rdata:0044AE0A                         aVeryValuableFo:
.rdata:0044AE0A 76 00 65 00 72 00 79 00+                text "UTF-16LE", 'very valuable for you',0
.rdata:0044AE36                         aSoWeWillGiveYo:                ; DATA XREF: .text:004387D5↑o
.rdata:0044AE36 0A 00 53 00 6F 00 20 00+                text "UTF-16LE", 0Ah
.rdata:0044AE36 77 00 65 00 20 00 77 00+                text "UTF-16LE", 'So we will give you appropriate price for recoverin'
.rdata:0044AE36 69 00 6C 00 6C 00 20 00+                text "UTF-16LE", 'g',0Ah,0
```

Strings that Maze uses to generate the ransom note

```
.text:00438763 8B 6C 24 08                      mov     ebp, [esp+8]
.text:00438767 EB 66                            jmp     short loc_4387CF
.text:00438769                          ; ---------------------------------------------------------------------------
.text:00438769
.text:00438769                          loc_438769:                             ; DATA XREF: .rdata:0044A998↓o
.text:00438769 68 08 AD 44 00                   push    offset aAStandaloneSer ; "a standalone server"
.text:0043876E EB 13                            jmp     short loc_438783
.text:00438770                          ; ---------------------------------------------------------------------------
.text:00438770
.text:00438770                          loc_438770:                             ; DATA XREF: .rdata:0044A99C↓o
.text:00438770 68 30 AD 44 00                   push    offset aAServerInCorpo ; "a server in corporate network"
.text:00438775 EB 0C                            jmp     short loc_438783
.text:00438777                          ; ---------------------------------------------------------------------------
.text:00438777
.text:00438777                          loc_438777:                             ; DATA XREF: .rdata:0044A9A0↓o
.text:00438777 68 EA AD 44 00                   push    offset aABackupServer ; "a backup server"
.text:0043877C EB 05                            jmp     short loc_438783
.text:0043877E                          ; ---------------------------------------------------------------------------
.text:0043877E
.text:0043877E                          loc_43877E:                             ; DATA XREF: .rdata:0044A9A4↓o
.text:0043877E 68 B2 AD 44 00                   push    offset aAPrimaryDomain ; "a primary domain controller"
.text:00438783
.text:00438783                          loc_438783:                             ; CODE XREF: .text:loc_4386EB↑p
.text:00438783                                                                  ; .text:0043876E↑j ...
.text:00438783 56                               push    esi
.text:00438784 68 CF 87 43 00                   push    offset loc_4387CF
```

Fragment of the procedure that generates the ransom note

How to avoid and prevent

Ransomware is evolving day by day, meaning a reactive approach to avoid and prevent infection is not profitable. The best defense against ransomware is proactive prevention because often it is too late to recover data once they have been encrypted.

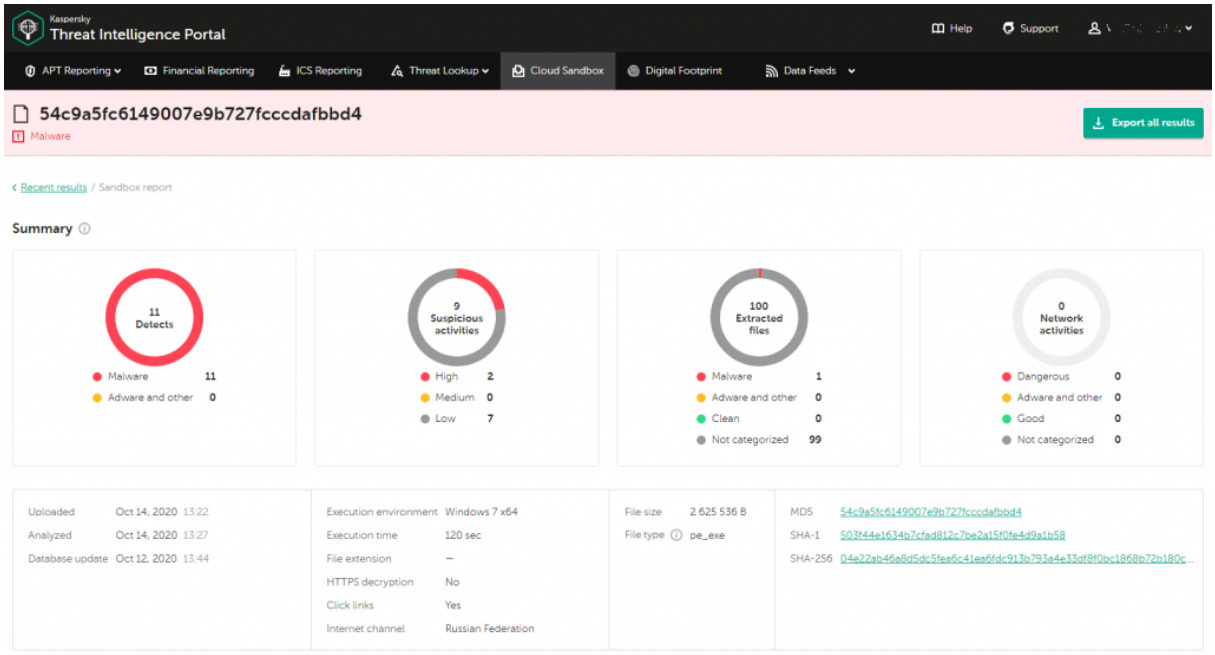
There are a number of recommendations that may help prevent attacks like these:

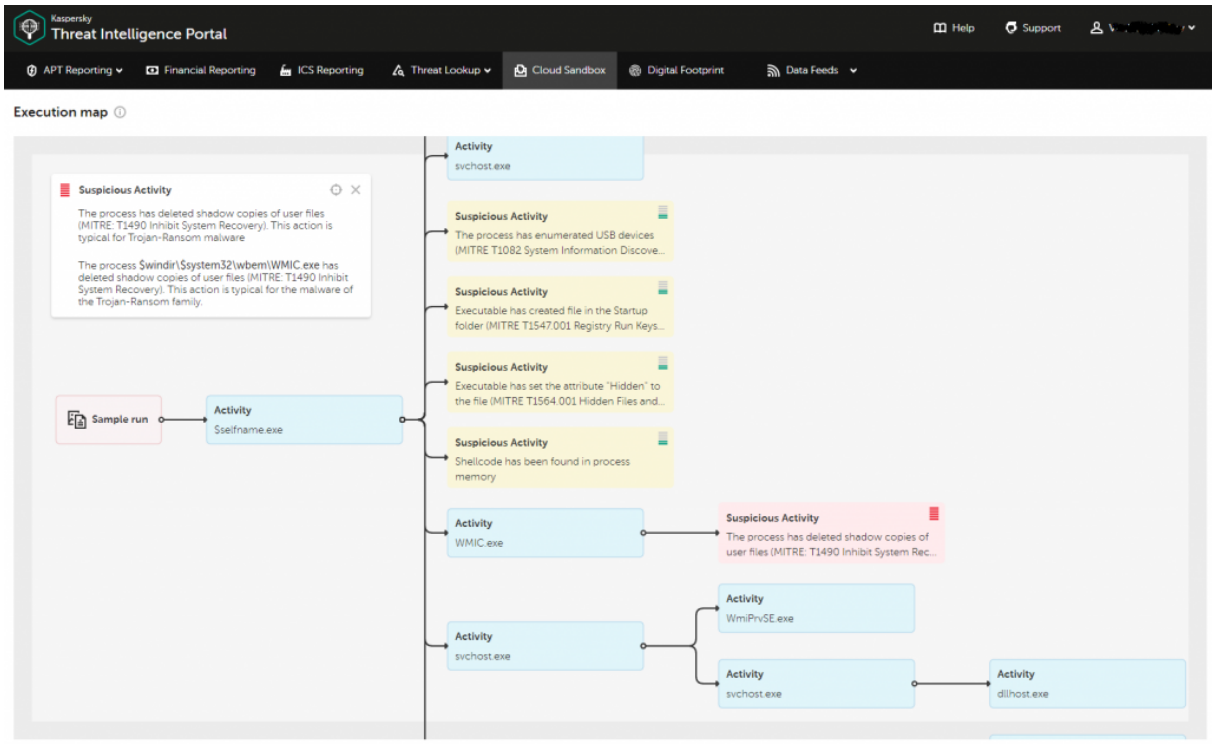
1. Keep your OS and applications patched and up to date.
2. Train all employees on cybersecurity best practices.
3. Only use secure technology for remote connection in a company local network.
4. Use endpoint security with behavior detection and automatic file rollback, such asKaspersky Endpoint Security for Business.
5. Use the latest threat intelligence information to detect an attack quickly, understand what countermeasures are useful, and prevent it from spreading.

Detection

Kaspersky products protect against this ransomware, detecting it as Trojan-Ransom.Win32.Maze; it is blocked by Behavior-based Protection as PDM:Trojan.Win32.Generic.

We safeguard our customers with the best Ransomware Protection technologies.





TIP Cloud Sandbox report summary and execution map with mapping on MITRE ATT&CK Framework

IOCs

2332f770b014f21bcc63c7bee50d543a
CE3A5898E2B2933FD5216B27FCEACAD0
54C9A5FC6149007E9B727FCCCDAFBBD4
8AFC9F287EF0F3495B259E497B30F39E

- Cybercrime
- Data leaks
- Doxing
- Exploit Kits
- Malware Technologies
- Phishing
- Ransomware
- Trojan

Authors

- Expert Fedor Sinitsyn

- Expert Nikita Galimov
-  Vladimir Kuskov

Life of Maze ransomware

Your email address will not be published. Required fields are marked *