Maze ransomware: extorting victims for 1 year and counting

news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/

Sophos May 12, 2020

It's been a year since the Maze ransomware gang began its rise to notoriety. Previously identified as "ChaCha ransomware" (a name taken from stream cipher used by the malware to encrypt files), the Maze "brand" was first affixed to the ransomware in May, 2019.

Initial samples of Maze were tied to fake websites loaded with exploit kits. Since then, Maze has been delivered by multiple means: exploit kits, spam emails, and—as the group's operations have become more targeted—Remote Desktop Protocol attacks and other network exploitation.

But aside from the gang's adjustments in initial compromise approaches, the Maze group has risen in prominence largely because of its extortion tactics: following through on threats of public exposure of victims' data in public "dumps" of victims' stolen data, and offering victim data on cybercrime forums if no payment is made.

While Maze did not invent the data-theft/extortion racket, it was among the first ransomware operations to use data theft as a way of twisting the arms of victims to pay up. The Maze gang has made public exposure central to their "brand" identity, and actively seeks attention from press and researchers to promote their brand—and make it easy for victims who might hesitate to pay them to find out their reputation.

Stepping into the spotlight

Maze rose to greater attention in October of 2019, when the ransomware's operators launched a massive spam campaign that masqueraded as messages from government agencies. One campaign sent messages claiming to be from Germany's Bundeszentralamt fur Steuern (Ministry of Finance), while another posed as a tax message from Italy's Agencia Entrate (Internal Revenue Service).

The Italian version of the attack claimed to be instructions to avoid being designated as tax cheats, with further details in the attached file VERDI.doc—described as an “interactive tool”, a ploy to trick the user to enable Visual Basic for Applications (VBA) macros. When macros were enabled, the scripts within the document downloaded the Maze ransomware to %TEMP% folder, and then executed it.

Agenzia Entrate

Ciao,

Si invitano tutte le persone fisiche e giuridiche a visionare e seguire con rigore Le Linee Guida fornite dall'Agenzia delle Entrate (in allegato).
E sufficiente seguire le indicazioni per evitare di essere segnalato dal sistema come un soggetto "a rischio" dopo il primo controllo basato sul c.d. "redditometro".
Il materiale da consultare (Le Linee Guida) viene consigliato specialmente ai soggetti che utilizzano i servici telematici finanziari (es. Internet Banking).

Nell'ambito dell'attivita di controllo nei confronti delle persone fisiche e giuridiche, nel 2019 e stata data attuazione alla normativa prevista dall'art. 38, commi quarto e seguenti del D.P.R. n.600/73 e dal D.M. 24 dicembre 2018 (il cosiddetto Redditometro).

A questo riguardo e ststo predisposto il nuovo applicativo informatico "VE.R.DI.", destinato alle attivita di analisi del rischio sulle persone fisiche e di ausilio alla daterminazione sintetica del reddito.

Si tratta di uno strumento innovativo che sara oggetto di implementazioni e miglioramenti volti ad ottimizzarne le funzionalita.

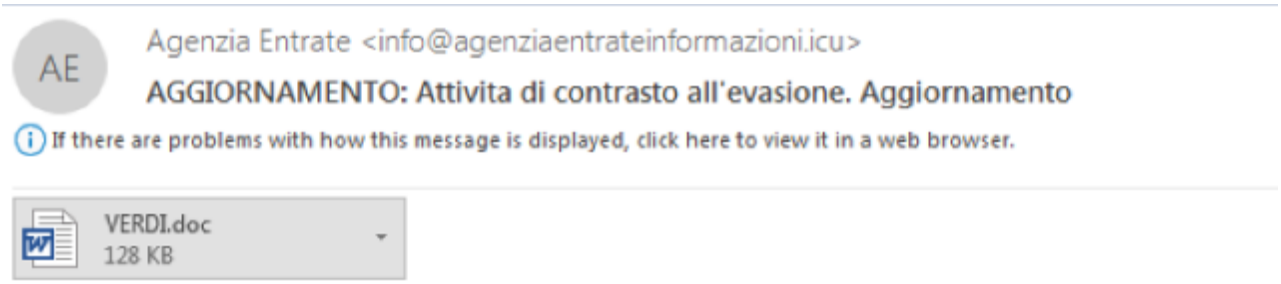
Riscossione Agenzia Entrate | La tua dichiarazione precompilata | FATTURA PA | Fattura elettronica | Corrispettivi elettronici

Agenzia delle Entrate - via Giorgione n. 106, 00147 Roma
Codice Fiscale e Partita Iva: 06363391001

Prenota un appuntamento e recapiti uffici
Siti regionali

Link utili
Archivio
Privacy e note legali

The fake email sent by Maze's operators to Italian targets.



The attachment, VERDI.doc

Since then, Maze ransomware has gained notice largely from stealing and publishing victims' data as a means to coerce payment. While threatening to expose victims' data has long been part of ransomware operators' playbook, Maze was among the first to follow through on such a threat in a public fashion—starting with the November 2019 exposure of data from Allied Universal.

Maze is not alone in adopting this tactic. REvil/Sodinokibi began releasing data at about the same time as Maze; the DoppelPaymer and Clop ransomware rings have followed suit, and LockBit has added threats of data exposure to its ransom note. But the Maze "team" was the first to go as far as to engage news media to draw attention to its victims, going as far as to include a "press release" on their website.

Fame and fortune

Maze's operators seek attention in many ways, in an effort to spread their reputation—and increase the likelihood that their "clients" (as they call their victims) pay quickly. Name recognition is important to them, even as they remain anonymous. One way they seek attention through their provocation of security researchers.

The developers of Maze often drop the names of researchers into strings contained within ransomware binaries or the "packers" that deliver them. For instance, Maze's authors frequently put researchers' names in the filenames or file paths for the program database (.pdb) file generated during development.

```
youaremyshame
you are nothing
sudo apt-get purge brains
--silkroad
Democracy
(.)(.)
Hillary 2020
siri stop patching jnz
string too long
invalid string position
C:\demonslay335\emsisoft_work\ransomware\hutchins.pdb
```

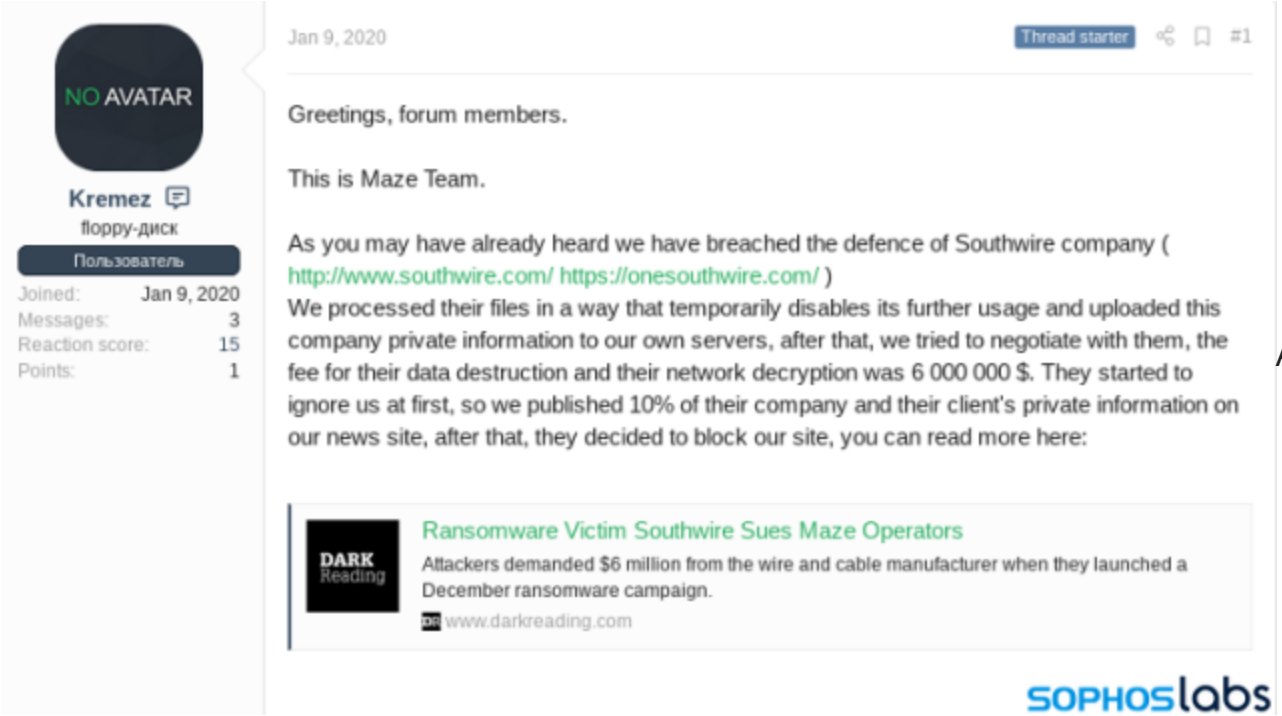
References to the Twitter account of researcher Michael Gillespie, the antivirus company Emisoft, and researcher Marcus Hutchins in the PDB path of one Maze binary sample, along with other meaningless strings.

The Maze authors have put names into the .pdb filename and path so frequently that it seems they may be running out of ideas about what to call them:

```
C:\hdDufhidsf\sdfsdf\dsfds\there_can_be_your_name.pdb
```

Sometimes, the Maze authors leave provocative messages to researchers within strings in the code itself. Often these strings have no function, though occasionally they're used as "kill switches" that shut down the malware's execution.

The Maze team's provocation of researchers extends into its presence in web forums. On one board, the Maze team uses the account name "Kremez", after prominent ransomware researcher Vitali Kremez, to post links to dumps of data from companies that failed to pay.



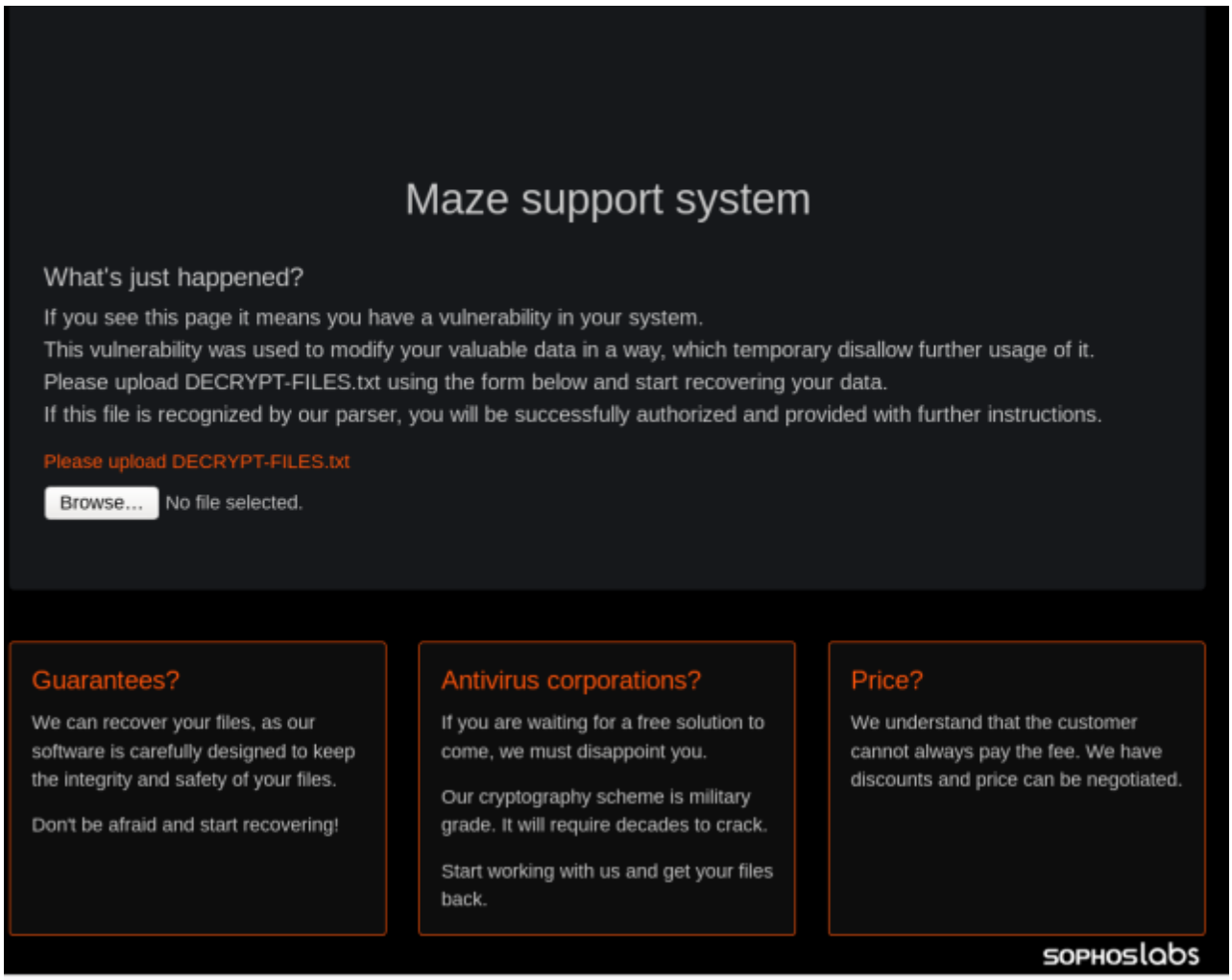
A web board post by the Maze team, using the account name "Kremez."

But the main platform used to promote the Maze brand is the Maze team's websites—one specifically for its victims, and another to communicate with the world at large (and encourage victims publicly to pay up).

"Keeping the world safe"

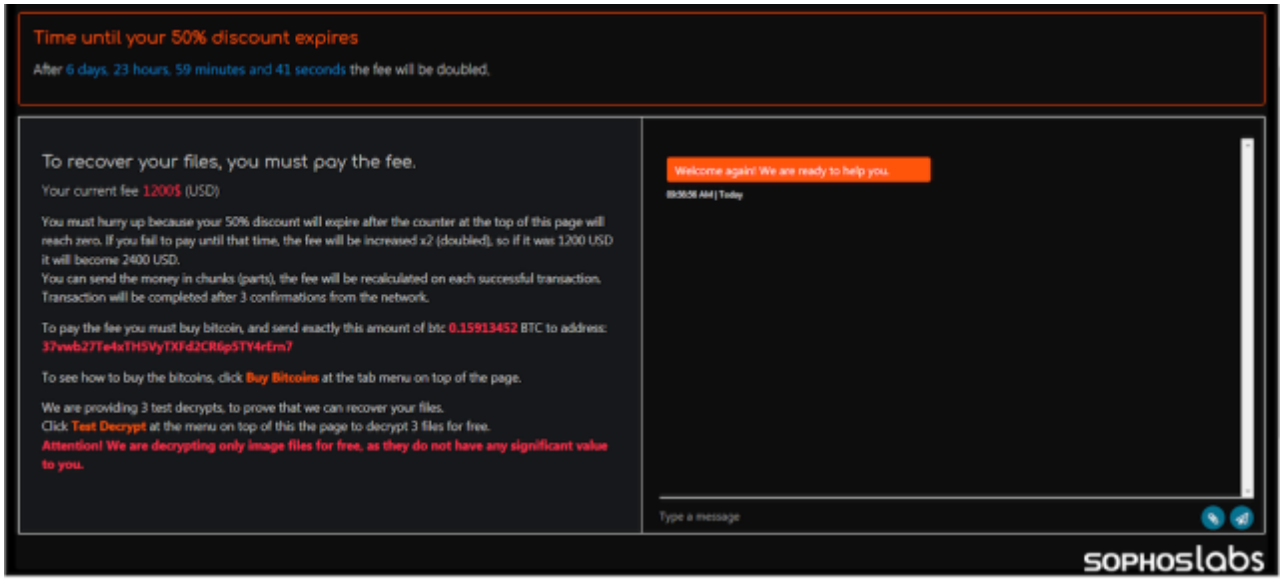
The web panel for victims features the ring's ironic slogan, "*Maze team: Keeping the World safe.*"

Victims arriving at the site after following the URL in the ransom note are asked to provide the file DECRYPT-FILES.txt dropped by the ransomware, which contains the identification number assigned to the victim.

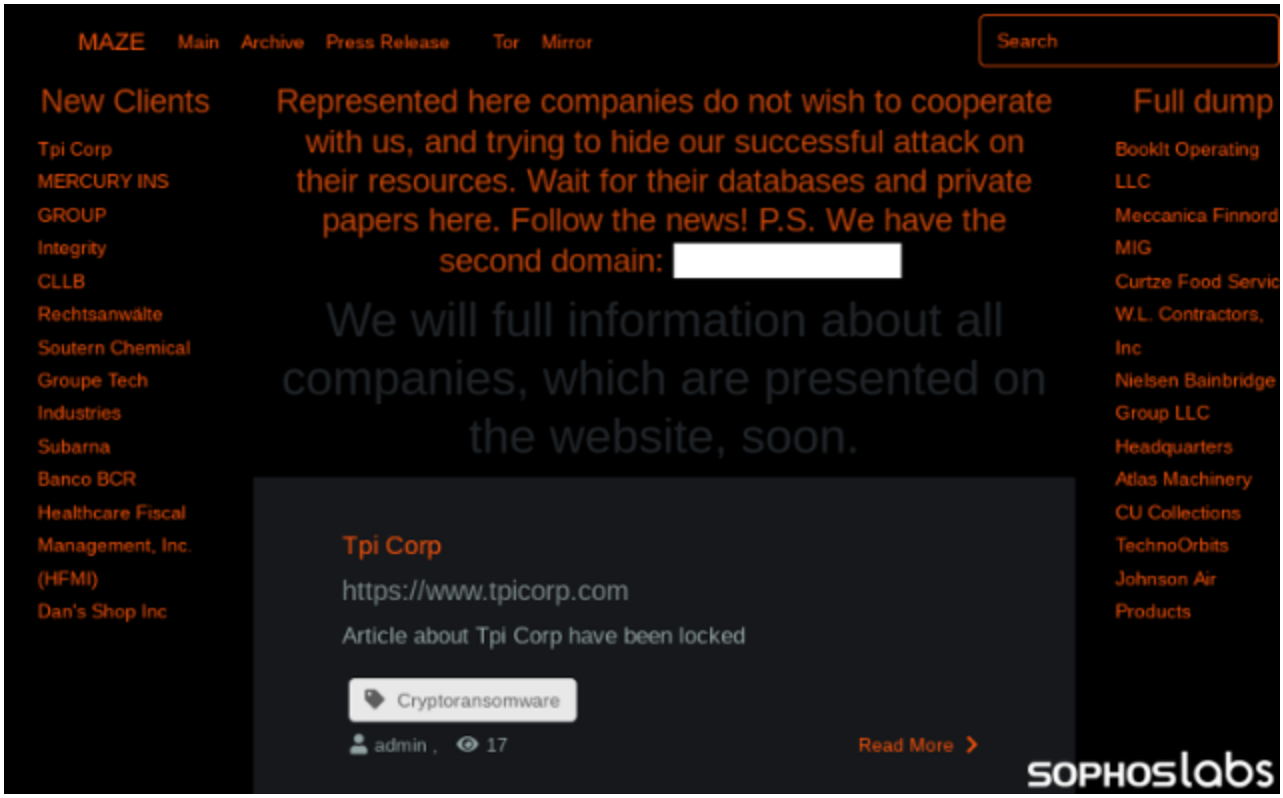


Once they've identified themselves, victims can upload three files for decryption as proof that the Maze crew can truly restore their data. (Only image files are supported, so no real critical data can be recovered for free.)

The site also provides a chat window, so the victim can communicate with the Maze team's customer support representatives, who are standing by to answer any questions and negotiate a payment.



Aside from the private web panel provided to victims, the Maze group also maintains a "news" site (hosted both on Tor and on the public Internet) that hosts samples of stolen data for companies that have recently been hit by the ransomware, as well as "full dumps" of data from some companies that failed to negotiate a payment.



On April 17, 2020, Maze posted a ”press release” dated April 17, 2020. It is really a message to victims, explaining all the bad things that will happen if they ignore Maze’s ransom demand and do not contact them about payment. (The page has recently been updated with information about alleged victim Banco BCR.)

MAZE Main Archive Press Release Tor Mirror Search

Maze Team official press release. April 17, 2020

Note for our Clients

You've be locked. What you shouldn't do

1. Hope to be forgotten after being locked. We never forget about our clients

2. Hope that it's all about encrypting of your data. In our work we use two bases. Encrypting of information and getting private data. Usually we have over 100Gb of data from single client. Sometimes up to 10Tb of commercial and private information. We are looking for NDA marked information and everything that can be used as a base for the lawsuit agains our client.

3. If you were locked, you have 3-5 days for get in contact with us. Otherwise all the info will be listed at our news website mazenews.top and sent to bloggers and journalists.

4. If you have decided to ignore the case of being locked and nobody will know about it, it's a mistake. Press Release will be sent to media, private info will be posted at mazenews.top, access credentials will be used for attacksignore on your partners and clients.

5. Please do not start the conversation with the phrases like «Guys, I can give 50 dollars». In previous cases after the few days conversations were started with the words «Guys, we have fired that clown, what to do next?»

6. If you've been locked and you are feeling to shy to tell your boss about the case, we will help you by sending emails with all the info to all company's executives

7. Finally, if you were locked and you were trying to ignore it, you should know that:

- All the information about security breach will be released to public
- Commercially valuable information will be sold on dark market
- All the breach information will be sent to Mass Media
- All the stock exchanges you are listed at will be notified that you were hacked, locked and lost sensitive information
- We will use the information gotten to attack your clients and partners. We will also notify them about the source of information.

What you should do if being locked?

1. Get info communication with us using the information on the locked computers or using the feedback form at our news website. Everything is absolutely confidential.

2. If you think that the price is too high you can make your offer. If it's reasonable we will always listen.

sophoslabs

They assure “clients” that they honor their side of any agreement and delete stolen data, as their reputation is important to them to conduct business. And they claim to be ready to cut a deal for those hurt by the COVID-19 induced global economic downturn.

In the past, the Maze group has withdrawn data posted to its site due to extenuating circumstances, such as when the group backed off blackmail demands against the City of Pensacola following the shooting of two members of the US Navy at the naval air station

there. And in March, the Maze team announced that it would stop attacks on medical organizations until the COVID-19 pandemic “stabilizes.”

In the most recent “press release” (dated April 17, 2020), the operators of Maze wrote:

> We are living in the same reality as you are. That’s why we prefer to work under the arrangements and we are ready for compromise. But only with those partners who can understand what is reputation and what are the real consequences of private data loss.

Evasion and anti-analysis in the Maze main binary

Maze ransomware is mostly written in C++. However, it heavily uses pure assembly with control flow obfuscation This obfuscation includes:

- Unconditional jumps that use combinations of conditional jump commands, such as putting a jz (jump if zero) instruction directly after a jnz (jump if not zero) instruction to the same location.
- Jumps into the middle of instructions;
- Instructions that point to strings within the .text section of the binary as a return address.
- Necessary API names are hashed, and compared with the hash of the DLL function names, then the matched functions are resolved dynamically with the usual LoadLibrary and GetProcAddress functions.

The Maze team is very proud of their main binary’s code obfuscation—in a message in the text of the malware’s binary, they challenged researchers to write an IDAPython script to deobfuscate it. On May 1, Crowdstrike’s Shaun Hurley published a report showing just such a deobfuscation in detail.

Whoa, @malwrhunterteam, good last discussion in twitter thread.
Answering to @MalwareTechBlog @kravietz_ @hasherezade @f0wlsec and others, It is unfortunately neither paranoia nor insulting nor marketing etc. It serves like honeypots on shitty AV which are 90% of AVs used in enterprise (anyway they dont read your twitter as it is painful for them), who just places signatures on data section in packer layer. It is funny to change these strings everytime and see how it is FUDing packer. Keep doing it, conspiracy theory adepts :)
@hasherezade, I dont know why you took this as insulting, but indeed I always liked your tools. I even use some of them in my regular malware analysis.
Also, lets play some game. Write IDAPython script to deobfuscate the code of the core payload working for all samples correctly without breaking conditional jumps and then you can write whatever you want about us, right?
Finally, literally all researcher mentions in both Maze and other malwares are neither insulting nor fam-syndrome or air conditioner. It is just like to have some fun&games with each other, otherwise it takes to be too boring, doesnt it? FUDing sample for each target on the one side and reversing shit-packers (literally what all Maze analysis do) on the daily basis on the other side of infosec. So Fuck infosec. Without malware your work will be boring as hell, what will you cover? Breaches? (Oh wait...) I know you hate us, but you need to know that we love you researchers, without you our job also would be fucking boring as hell.

Several of the Maze samples we’ve analyzed contain “kill” switches, which when triggered result in the malware not encrypting files. Many of these are there just to grab the attention of researchers, either to send some message or (as mentioned earlier) to name researchers that they know have been examining their code.

```
push    0               ; hTemplateFile
push    0               ; dwFlagsAndAttributes
push    OPEN_EXISTING   ; dwCreationDisposition
push    0               ; lpSecurityAttributes
push    1               ; dwShareMode
push    GENERIC_READ    ; dwDesiredAccess
push    offset FileName ; "C:\\2433\\kremez"
call    ds:CreateFileW
mov     [ebp+hObject], eax
cmp     [ebp+hObject], INVALID_HANDLE_VALUE
jz      short loc_100063F9
```

```
push    10h             ; uType
push    offset Caption  ; "sg"
push    offset Text     ; "fdgssg"
push    0               ; hWnd
call    ds:MessageBoxW
mov     eax, [ebp+hObject]
push    eax             ; hObject
call    ds:CloseHandle
push    0               ; uExitCode
call    ds:ExitProcess
```

```
loc_100063F9:
push    offset OutputString ; "Kremez and Hasherezade. Two polish rese"...
call    ds:OutputDebugStringW
mov     [ebp+var_1; const WCHAR OutputString
mov     [ebp+lpAdd OutputString:                    ; DATA XREF: begin:loc_100063F9↑o
push    5BFE1h                  text "UTF-16LE", 'Kremez and Hasherezade. Two polish researchers. Why'
call    ??2@YAPAXI              text "UTF-16LE", ' are still not married?',0Dh,0Ah
add     esp, 4                  text "UTF-16LE", 'CryptoInsane, be careful or we will lock your colle'
mov     [ebp+var_1              text "UTF-16LE", 'ge and rename maze to CryptoInsane ransomware',0Dh,0Ah
mov     ecx, [ebp+              text "UTF-16LE", 'What if we pay some niggaman to throw Molotov to so'
mov     [ebp+lpAdd              text "UTF-16LE", 'uthwire office?',0
```

Researcher Vitali Kremez's name is used here as a killswitch filename (C:\\2433\\kremez), along with a threatening message to another researcher in the binary text.

```
10006500 55                 push    ebp
10006501 8B EC              mov     ebp, esp
10006503 51                 push    ecx
10006504 FF 15 08 10 01+call    ds:GetCommandLineA
1000650A 89 45 FC           mov     [ebp+var_4], eax
1000650D 83 7D FC 00        cmp     [ebp+var_4], 0
10006511 74 1D              jz      short loc_10006530
```

```
10006513 68 F4 56 01 10 push    offset aSouthwirethesh ; "southwiretheshit"
10006518 8B 45 FC       mov     eax, [ebp+var_4]
1000651B 50             push    eax             ; char *
1000651C E8 4F FE FF FF call    my_strstr
10006521 83 C4 08       add     esp, 8
10006524 85 C0          test    eax, eax
10006526 74 08          jz      short loc_10006530
```

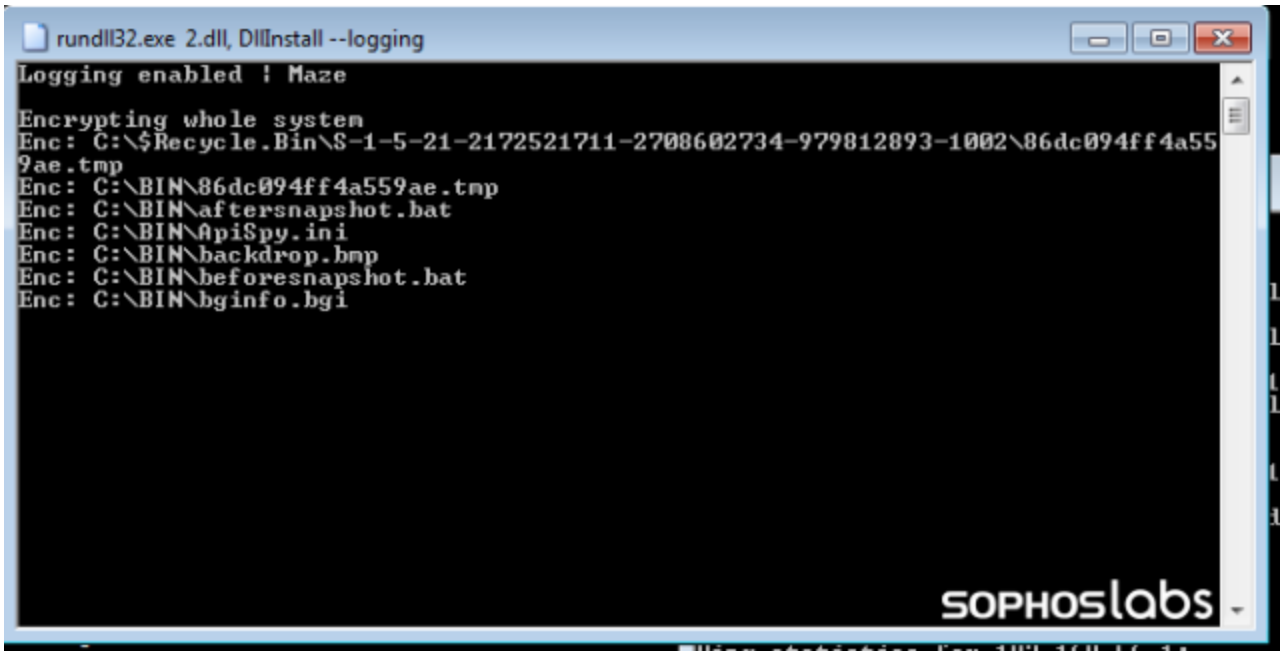
```
10006528 6A 00              push    0               ; uExitCode
1000652A FF 15 00 10 01+call    ds:ExitProcess
```

```
10006530
10006530                loc_10006530:
10006530 68 D1 04 00 00 push    4D1h
```

Another killswitch setting taunts a company that did not pay Maze's ransom.

There are also some samples that can be run with more meaningful, functional switches, such as:

- **–nomutex** which allow to run multiple instances;
- **–logging** turns on detailed console output, which logs each file encrypted, the time required to do so, and some error messages;
- **–noshares** turns off encryption of network shares;
- –path specifies a folder to be encrypted.



Output from the Maze binary with the –logging switch passed at startup.

Aside from the obfuscation, the Maze main binary's authors applied a number of anti-analysis techniques to the malware. It checks debugging environment in multiple ways. In addition to using the IsDebuggerPresent API and PEB.BeingDebuggedFlag check , the Maze main binary contains hardcoded hashes of the names for known analysis processes, including procmon.exe, procmon64.exe, x32dbg.exe, x64dbg.exe, ollydbg.exe, procexp.exe, and procexp64.exe. The code enumerates the running processes present, checks processes' names against the hashed list, and terminates itself if any are detected.

```
process_checks:                         ; DATA XREF: .text:008D3085↑o
                add     esp, 0Ch
                cmp     eax, 55B00592h
                jle     loc_8D3150
                cmp     eax, 627005EBh
                jle     near ptr unk_8D3200
                cmp     eax, 6DE0062Fh
                jg      loc_8D32F8
                cmp     eax, 6B88060Dh
                mov     ebp, esi
                jle     loc_8D3515
                cmp     eax, 6D100623h
                jg      loc_8D390A
                cmp     eax, 6B88060Eh
                jz      catch
loc_8D32F8:                             ; CODE XREF: .text:008D30DC↑j
                cmp     eax, 7802063Fh
                mov     ebp, esi
                jle     near ptr unk_8D370D
                cmp     eax, 79EC0660h
                jg      near ptr unk_8D3A7C
                cmp     eax, 78020640h  ; procexp64.exe
                jz      catch
```

Setting up shop and phoning home

The Maze binary creates persistence by adding itself to Windows' autorun registry. And it uses a mutex to ensure that another instance of Maze doesn't execute (unless it's a sample that has been executed with the –nomutex switch).

As with most ransomware, it deletes shadow copies with the Windows Management Instrumentation command line utility WMIC.exe. The binary also uses the WMI interface to query for antivirus information, executing the Windows Management Instrumentation Query Language (WQL) command "Select * from AntiVirusProduct" within WMI namespace root\SecurityCenter2.

The ransomware collects information about the computer and its user, including information about the system drives, operating system version, default language setting, username, and computer name. As with some other ransomware, Maze will terminate without encrypting files if certain languages are detected (such as those used in Commonwealth of Independent States nations).

Information about the local network its target is connected is also gathered by the malware, by creating a null session connection and enumerating network resources. It tries to find out the role of that the current machine in the network, in order to reuse it in the extortion—Maze varies the amount of the ransom depending on whether the target is a home computer, or a workstation or server on a corporate network.

This information is exfiltrated back to the command and control server using a standard port 80 HTTP POST method, connecting using Windows' socket library, WS2_32.dll. The URI path is created from a hard-coded string list to building up the URI path.

```
0319FD7C  00A50000  ¥
0319FD80  00000000
0319FD84  002193D8  Ø■!  ASCII ".php"
0319FD88  002193DD  Ý■!  ASCII ".asp"
0319FD8C  002193E2  â■!  ASCII ".aspx"
0319FD90  002193E8  è■!  ASCII ".cgi"
0319FD94  002193ED  í■!  ASCII ".jsp"
0319FD98  002193F2  ò■!  ASCII ".jspx"
0319FD9C  002193F8  ø■!  ASCII ".do"
0319FDA0  002193FC  ü■!  ASCII ".action"
0319FDA4  00219404  ┘■!  ASCII ".html"
0319FDA8  0021940A   ■!  ASCII ".phtml"
0319FDAC  00219411  ◄■!  ASCII ".shtml"
0319FDB0  002194C0  À■!  ASCII "news"
0319FDB4  002194C5  Å■!  ASCII "login"
0319FDB8  002194CB  Ë■!  ASCII "register"
0319FDBC  002194D4  Ô■!  ASCII "logout"
0319FDC0  002194DB  Û■!  ASCII "edit"
0319FDC4  002194E0  à■!  ASCII "content"
0319FDC8  002194E8  è■!  ASCII "private"
0319FDCC  002194F0  ð■!  ASCII "messages"
0319FDD0  002194F9  ù■!  ASCII "account"
0319FDD4  00219501   ■!  ASCII "view"
0319FDD8  00219506  —■!  ASCII "webauth"
0319FDDC  0021950E  ♬■!  ASCII "webaccess"
0319FDE0  00219518  ↑■!  ASCII "archive"
0319FDE4  00219520   ■!  ASCII "forum"
0319FDE8  00219526  &■!  ASCII "post"
0319FDEC  0021952B  +■!  ASCII "signin"
0319FDF0  00219532  2■!  ASCII "signout"
0319FDF4  0021953A  :■!  ASCII "update"
0319FDF8  00219541  A■!  ASCII "support"
0319FDFC  00219549  I■!  ASCII "ticket"
0319FE00  00219550  P■!  ASCII "task"
0319FE04  00219555  U■!  ASCII "tracker"
0319FE08  0021955D  ]■!  ASCII "analytics"
0319FE0C  00219567  g■!  ASCII "check"
0319FE10  0021956D  m■!  ASCII "checkout"
0319FE14  00219576  v■!  ASCII "payout"
0319FE18  0021957D  }■!  ASCII "withdrawal"
0319FE1C  00219588  ■■!  ASCII "sepa"
0319FE20  0021958D   ■!  ASCII "create"
0319FE24  00219594  ■■!  ASCII "transfer"
0319FE28  0021959D   ■!  ASCII "wire"
0319FE2C  00590000   Y   ASCII "91.218.114.491.218.114.
0319FE30  00AA0000   ª   ASCII "91.218.114.4"
```

The malware sends information including the username, drive information, drive free space, language, antivirus product present, and OS version back to the server.

Dear User, I've encrypted your files

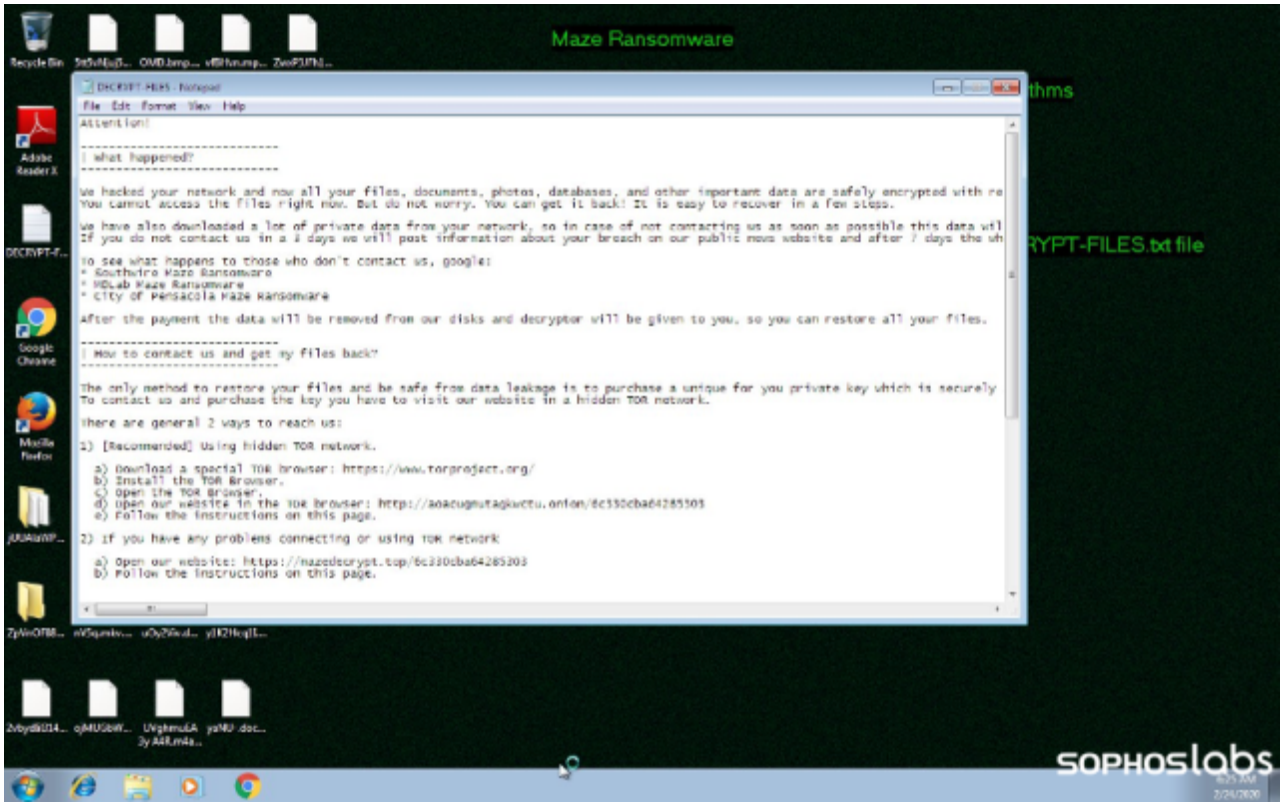
Maze uses RSA and ChaCha20 stream cipher encryption to lock victims' files. The malware generates an RSA key pair, which is in turn encrypted using the main RSA public key embedded in the malware. As it traverses the file system to encrypt files, it skips the following directories:

- \\Program Files

- \\Windows
- \\Games\\
- \\Tor Browser\\
- \\ProgramData\\
- \\cache2\\entries\\
- \\Low\\Content.IE5\\
- \\User Data\\Default\\Cache\\
- \\All Users
- \\IETldCache\\
- \\Local Settings\\
- \\AppData\\Local
- AhnLab
- {0AFACED1-E828-11D1-9187-B532F1E9575D}

Maze also doesn't encrypt .lnk, .exe, .sys, and .dll files, and specifically avoids the following files:

- DECRYPT-FILES.txt (the file dropped with the victim's ID code)
- inf
- ini
- ini
- dat
- db
- bak
- dat.log
- db
- bin



The ransom note, on the altered desktop.

At the end of the encryption, a desktop wallpaper .bmp is dropped—and a voice message is played:

“Alert! *User* Alert! Dear *User*, Your files have been encrypted…”

Both the wallpaper and the voice message are stored in text forms within the binary. The background text is converted to bmp with the use of the DrawTextW and GetDIBits APIs, and is dropped as 000.bmp and set to the wallpaper. The voice message is created using the Microsoft Speech API with the default voice and default audio. Just before playing the message, Before the speech, it uses the operating system’s Beep function to be sure to catch the attention of the victim.

In the latest version of the ransom note, the Maze crew leaves a “friendly” warning for the IT support staff of the victim organization:

```
P.S. Dear system administrators, do not think you can handle it by yourself. Inform leadership as soon as possible.
By hiding the fact of the breach you will be eventually fired and sometimes even sued.
```

IOCs

SHA256	filename
4acba1590552c9b2b82f5a786cedc8a12ca457e355c94f666efef99073827f89	love.dll

20ea5a9b5b2e47aa191132ac12c1d6dea6b58d7a0467ea53d48e96f8a79c6acd	argfdg, arsgt35yy, maze.exe
3c2be967cbaaafecf8256167ba32d74435c621e566beb06a1ead9d33d7e62d64	Attack!.rar
7a84d10ac55622cdac25f52170459ae5b8181ee3fc345eb1b1dcbd958b344aa6	Ave Kim, Emperor.exe