NCFTA
The National Cyber-Forensics and Training Alliance

Maze Ransomware

Analyst Code: 0334
December 02, 2019

Executive Summary

Maze is ransomware that was first discovered in May 2019. The ransomware is distributed by threat actor TA2101 by a variety of means. Once deployed, the ransomware scans all folders and encrypts all files except itself and .ini file extensions and creates a ransom note in each folder. The ransom amount is not stated in the ransom note, and victims are directed to email the threat actor at one of two email addresses. At this time there is no known publicly available decryptor.

NCFTA | **PITTSBURGH** 2000 Technology Drive, Suite 450, Pittsburgh, PA 15219 | 412-802-8000
NCFTA | **NEW YORK** One Penn Plaza, 250 West 34th Street, Suite 2124, New York, NY 10119
NCFTA | **LOS ANGELES** Wilshire Building, 601 S. Figueroa Street, Suite 1460, Los Angeles, CA 90017

Findings

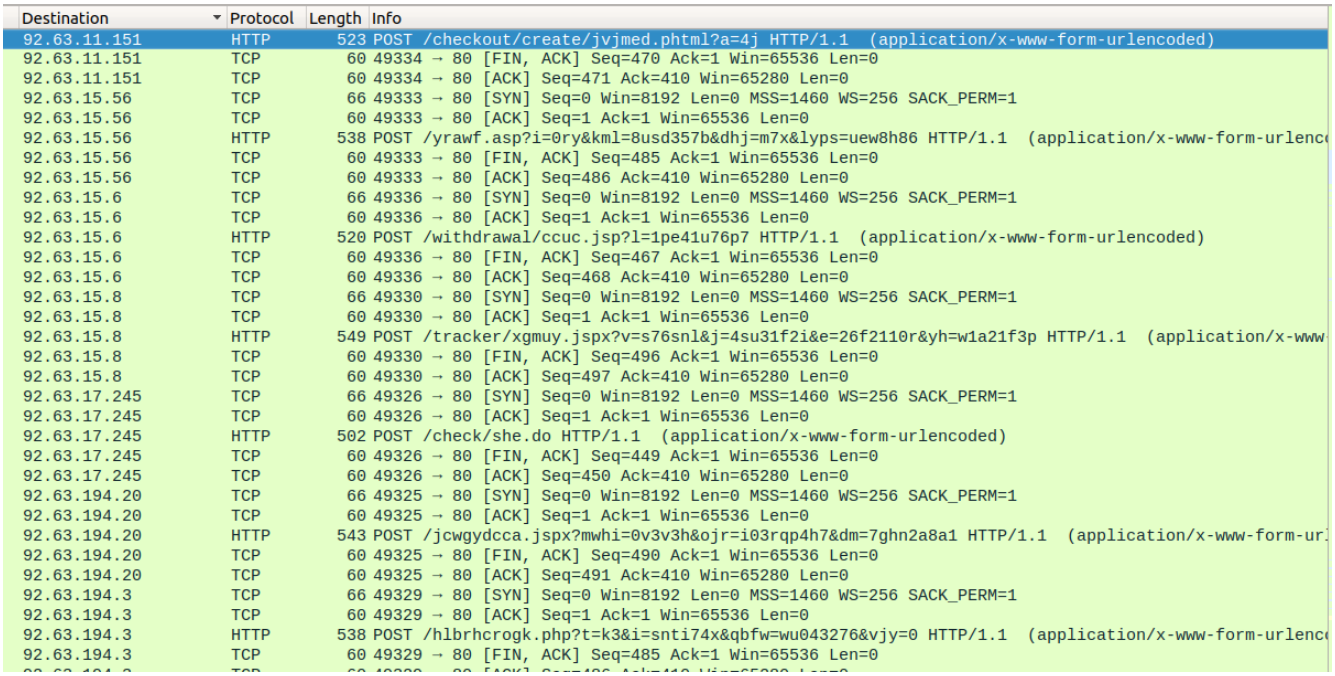
Background

Maze is a trojan which was first reported as a variant of ChaCha Ransomware in May 2019 by a Malwarebytes security research. Proofpoint identified the threat actor responsible as TA2101, reporting that the discovery of hundreds of phishing emails impersonating German and Italian government agencies in targeted attacks against those nations. The industries that seemed to be most frequently targeted were those of healthcare, manufacturing, business, and IT services. In phishing emails, the threat actors used stolen branding as well as spoofed domains to make messages appear more legitimate.[1] In November, Maze ransomware threat actors released stolen data after Allied Universal refused to pay the ransom.[2] At this time, there is no free decryptor available for Maze ransomware.

Behavior

Once the ransomware is deployed, it will look for files to encrypt while attempting at least 24 network connections, including 15 HTTP POST requests and TCP traffic over port 80 to IP addresses beginning with 92:

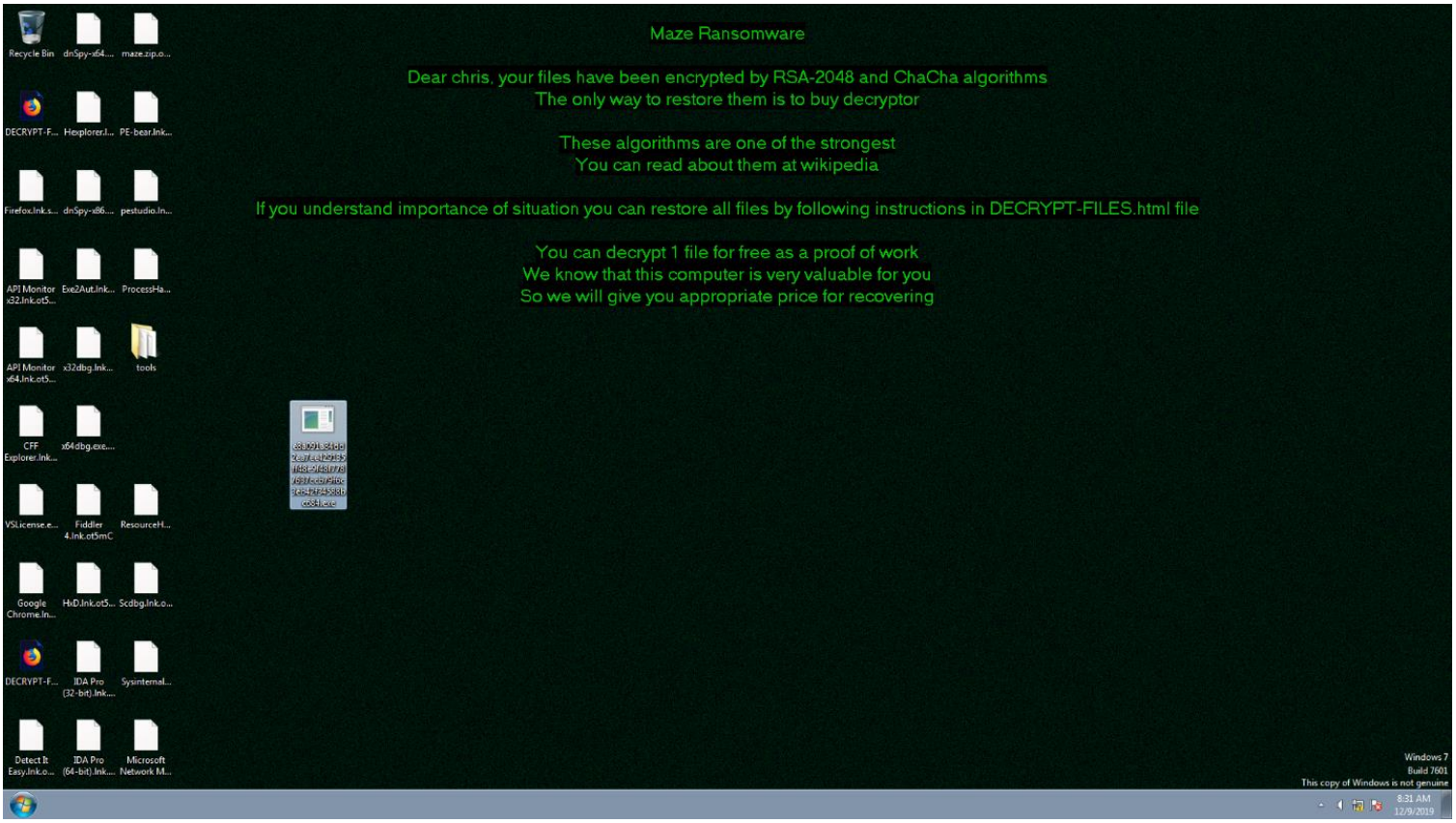
- 92.63.32[.]2
- 92.63.37[.]100
- 92.63.194[.]20
- 92.63.17[.]245
- 92.63.32[.]55
- 92.63.11[.]151
- 92.63.194[.]3
- 92.63.15[.]8
- 92.63.29[.]137
- 92.63.32[.]57
- 92.63.15[.]56
- 92.63.32[.]52
- 92.63.8[.]47
- 92.63.15[.]6



Destination	Protocol	Length	Info
92.63.11.151	HTTP	523	POST /checkout/create/jvjmed.phtml?a=4j HTTP/1.1 (application/x-www-form-urlencoded)
92.63.11.151	TCP	60	49334 → 80 [FIN, ACK] Seq=470 Ack=1 Win=65536 Len=0
92.63.11.151	TCP	60	49334 → 80 [ACK] Seq=471 Ack=410 Win=65280 Len=0
92.63.15.56	TCP	66	49333 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92.63.15.56	TCP	60	49333 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
92.63.15.56	HTTP	538	POST /yrawf.asp?i=0ry&kml=8usd357b&dhj=m7x&lyps=uew8h86 HTTP/1.1 (application/x-www-form-urlenc
92.63.15.56	TCP	60	49333 → 80 [FIN, ACK] Seq=485 Ack=1 Win=65536 Len=0
92.63.15.56	TCP	60	49333 → 80 [ACK] Seq=486 Ack=410 Win=65280 Len=0
92.63.15.6	TCP	66	49336 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92.63.15.6	TCP	60	49336 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
92.63.15.6	HTTP	520	POST /withdrawal/ccuc.jsp?l=1pe41u76p7 HTTP/1.1 (application/x-www-form-urlencoded)
92.63.15.6	TCP	60	49336 → 80 [FIN, ACK] Seq=467 Ack=1 Win=65536 Len=0
92.63.15.6	TCP	60	49336 → 80 [ACK] Seq=468 Ack=410 Win=65280 Len=0
92.63.15.8	TCP	66	49330 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92.63.15.8	TCP	60	49330 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
92.63.15.8	HTTP	549	POST /tracker/xgmuy.jspx?v=s76snl&j=4su31f2i&e=26f2110r&yh=w1a21f3p HTTP/1.1 (application/x-www
92.63.15.8	TCP	60	49330 → 80 [FIN, ACK] Seq=496 Ack=1 Win=65536 Len=0
92.63.15.8	TCP	60	49330 → 80 [ACK] Seq=497 Ack=410 Win=65280 Len=0
92.63.17.245	TCP	66	49326 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92.63.17.245	TCP	60	49326 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
92.63.17.245	HTTP	502	POST /check/she.do HTTP/1.1 (application/x-www-form-urlencoded)
92.63.17.245	TCP	60	49326 → 80 [FIN, ACK] Seq=449 Ack=1 Win=65536 Len=0
92.63.17.245	TCP	60	49326 → 80 [ACK] Seq=450 Ack=410 Win=65280 Len=0
92.63.194.20	TCP	66	49325 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92.63.194.20	TCP	60	49325 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
92.63.194.20	HTTP	543	POST /jcwgydcca.jspx?mwhi=0v3v3h&ojr=i03rqp4h7&dm=7ghn2a8a1 HTTP/1.1 (application/x-www-form-ur
92.63.194.20	TCP	60	49325 → 80 [FIN, ACK] Seq=490 Ack=1 Win=65536 Len=0
92.63.194.20	TCP	60	49325 → 80 [ACK] Seq=491 Ack=410 Win=65280 Len=0
92.63.194.3	TCP	66	49329 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
92.63.194.3	TCP	60	49329 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
92.63.194.3	HTTP	538	POST /hlbrhcrogk.php?t=k3&i=snti74x&qbfw=wu043276&vjy=0 HTTP/1.1 (application/x-www-form-urlenc
92.63.194.3	TCP	60	49329 → 80 [FIN, ACK] Seq=485 Ack=1 Win=65536 Len=0

[1] hxxps://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
[2] hxxps://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

The ransomware will exit certain applications such as Process Monitor and Microsoft Office applications, however, it will not close the task manager which shows the ransomware file running as well as various legitimate processes running in 32-bit mode. While running, the ransomware also attempts to make a number of connections. Maze will try and gather information about the system it is infecting, including the type of system, identifying it as 'standalone server,' 'server in corporate network,' 'home computer,' 'primary domain controller,' 'backup server,' or 'very valuable for you,' which seems to influence the ransom amount. Additionally, once files are encrypted, the ransomware leaves a ransom note, and changes the desktop background, which references the type of computer it has determined it has infected as well as where to find the ransom note:

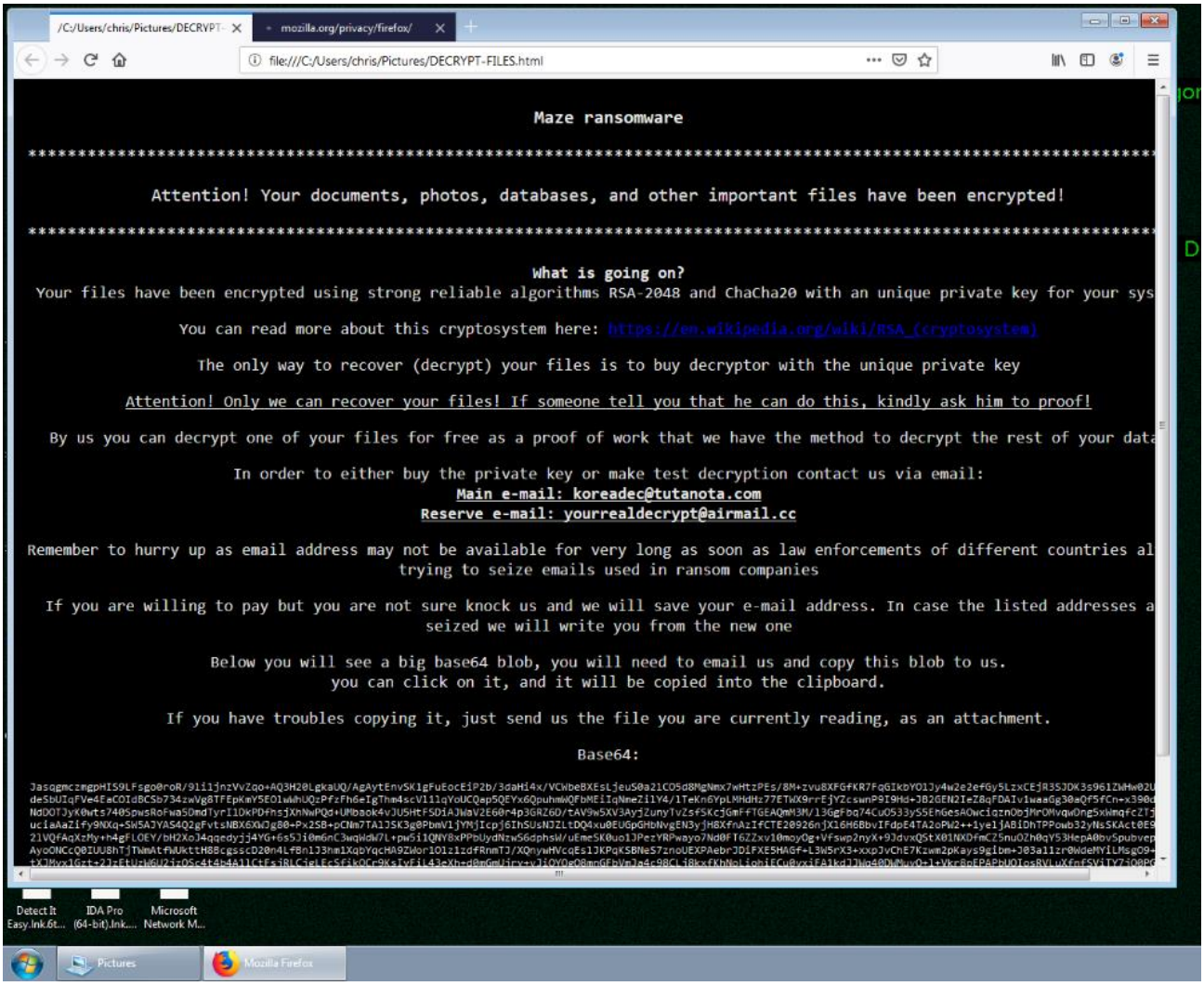


Encryption

The ransomware attempts to encrypt all files using RSA-2048 and ChaCha20 encryption which it boasts in its ransom note as "one of the strongest" algorithms. The files are given randomly generated extensions. It encrypts all files except for itself. Some variants have been stated to not encrypt .exe, .lnk, .sys, and .dll files, and one variant is stated to not encrypt files if it detects the file "C:\hutchins.txt" on the system.[3] It deletes shadow copies of files on the machine, changes the wallpaper, and creates a ransom note named 'DECRYPT-FILES.html,' preceded by the path to the files, in each location it scans. The ransom note does not indicate a price, but offers instructions to get files back, offering one free decryption. In previous variants of the ransomware, the ransom note indicated that victims should go to one of two links to websites to visit to begin the process of recovering files, one [.]onion site and the other

[3] hxxps://www.pcrisk.com/removal-guides/16145-maze-2019-ransomware

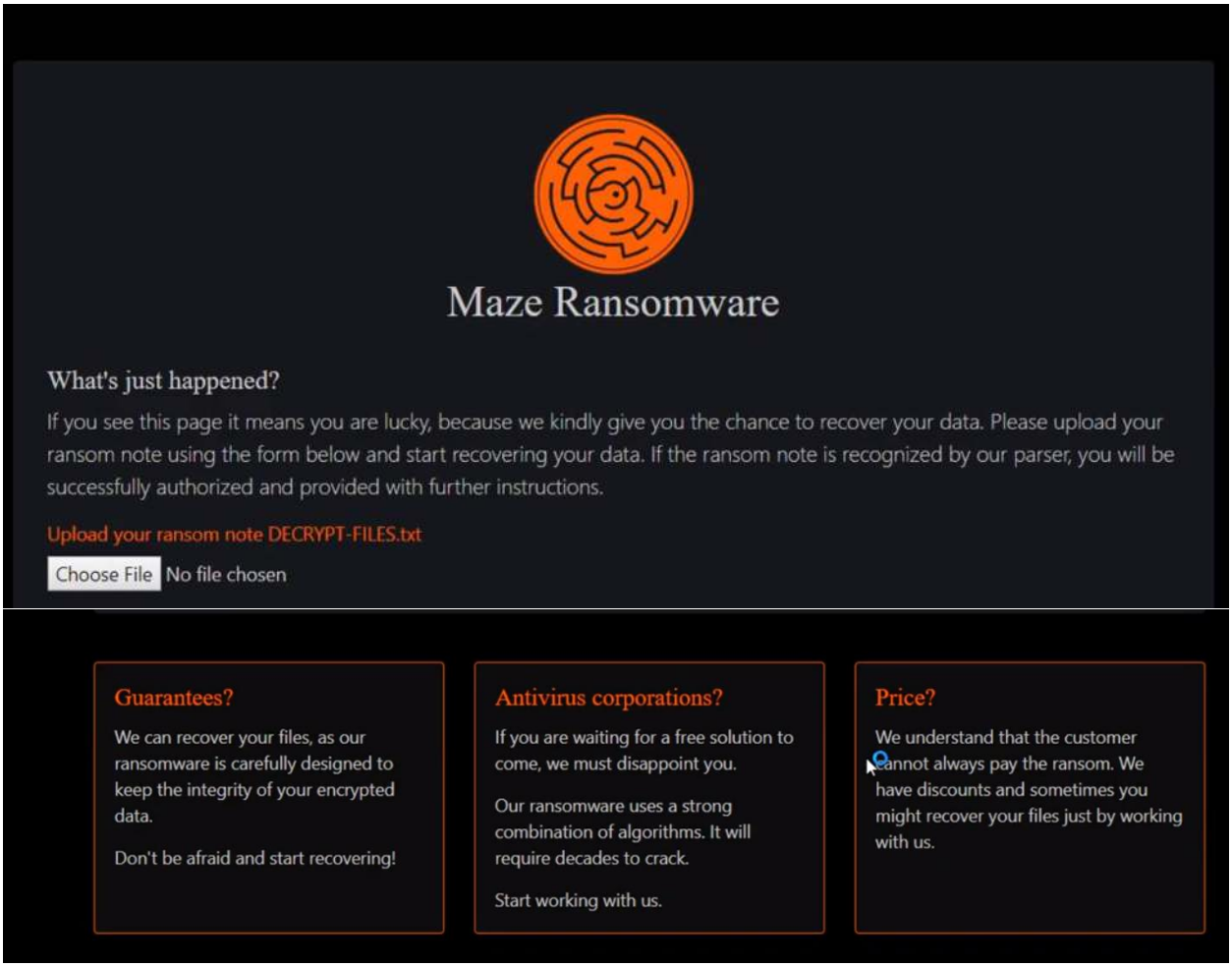
a clear net address.[4] In the sample analyzed internally, instead, only two email addresses were provided to contact, noting that if their address is seized by law enforcement, they may write from a new one:



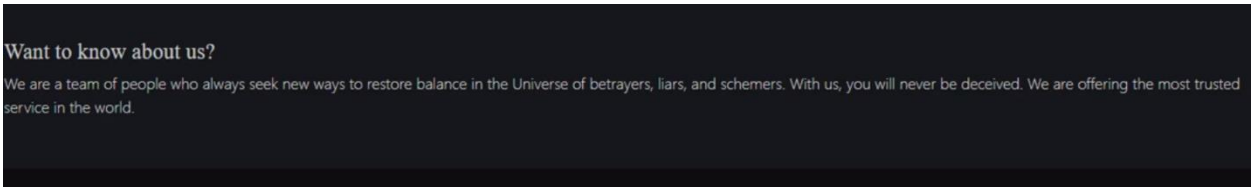
[4] Ibid.

Maze Website

In previous samples of the ransomware, the threat actors included a links to two websites for victims to make payments and get their files decrypted, one on TOR, hxxp://aoacugmutagkwctu[.]onion/1dcb0b851e857d00, and one on the clear net, hxxps://mazedecrypt[.]top/1dcb0b851e857d00. Upon first visiting the website, only the following screen is viewable until the ransom note is uploaded:



After the ransom note, with the Base64 string at the bottom, is uploaded, the victim is granted access to the full website which is complete with functionality to decrypt up to three files for free, a chat portal for support, a link to buy bitcoins using a bank account, credit card, or PayPal, and an “About Us” section.



In a video posted by independent researcher GrujaRS, the threat actor comments in the chat that “we see you are using our test decrypt system,” and suggest purchasing a decryptor, and subsequently address

the researcher by name, indicating that the chat is not automated.[5] On the chat page the ransom amount is displayed and a Bitcoin wallet address is provided. Additionally, a countdown of approximately one week indicates that the ransom will double when time runs out.

Campaigns

Fallout was first discovered in August 2018, and was modified June 28, 2019. The exploit kit targets CVE-2018-4878 and CVE-2018-8174 which are a use after free vulnerability in Flash Player versions before 20.0.0.161 and a VBScript vulnerability, respectively. Both allow for remote code execution.

October 16, 2019 – October 23, 2019

Maze began a concentrated spam campaign targeting IT service companies in Germany. In the emails, threat actors posed as the German Federal Ministry of Finance (Bundeszentralamt fur Steuern), utilizing stolen branding and lookalike [.]icu domains. The body of the email claims that a tax refund of possibly "several hundred euros" is due and that the victim has three days to return the completed request form, an attached malicious word document. The document claims to have been created with an older version of Microsoft Word, and directs users to click "Enable Content" to continue. Doing so results in macros executing a PowerShell script which downloads and deploys the ransomware.[6]

October 29, 2019

Maze began a spam campaign, sending out phishing emails to users in manufacturing companies in Italy pretending to be from the agency responsible for collecting taxes and revenue, the Italian Revenue Agency (Agenzia delle Entrate). The subject line used, "AGGIORNAMENTO: Attivita di contrasto all'evasione. Aggiornamento," roughly translates to "UPDATE: Activities to combat evasion. Update" and attached a malicious word document called "VERDI.doc" or "GREEN.doc." The body of the email reads that citizens are to read and "strictly follow" the attached guidelines at the risk of being identified as "at risk." It particularly suggests that those who use services such as internet banking pay attention and claims that the new IT application "Ve.R.DI." is a risk analysis tool to assist in summarizing income. The document entices the victim to "Enable Content" by claiming that it is encrypted using RSA encryption. Once enabled, the macro used a PowerShell script to download and deploy the ransomware on the user's system.[7]

November 6, 2019

Maze began a new campaign targeting German IT service companies, again posing as the German Ministry of Finance and using stolen branding and lookalike domains. This time, the malicious document follows the structure of that used in the campaign against Italian manufacturers, claiming to be RSA encrypted. [8]

November 7, 2019

Maze used the same infection chain seen in previous campaigns to target German businesses and IT services companies. This time, threat actors impersonated an internet service provider, 1&1 Internet AG, and sent a malicious Word document claiming to be RSA encrypted to persuade victims to enable macros.[9]

---

[5] hxxps://youtu.be/MTed3ffpmNY
[6] hxxps://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
[7] hxxps://www.bleepingcomputer.com/news/security/maze-ransomware-attacks-italy-in-new-email-campaign/
[8] hxxps://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
[9] Ibid.

November 2019

Beginning on November 15, 2019, threat actors claiming to be the “Maze Crew” contacted Bleeping Computer reporting that they had breached Allied Universal security firm and exfiltrated their data before deploying Maze ransomware onto their network. Through multiple emails, they purported that the company refused to pay a ransom above $50,000 and that they had initially demanded 300 BTC (approximately $2.3 million). After releasing 700 MB worth of leaked files to Bleeping Computer forums, which were deleted, they sent a link to a Russian hacking and malware forum where they released 10% of the 5 GB of data they had stolen. Threat actors also claimed that they raised the price required by 50% before releasing the rest of the data. In the same post, TA2101 also reported breaching an unnamed Canadian insurance company. It is noteworthy that this is the first example of ransomware threat actors releasing stolen data after ransom was unpaid.[10]

December 7, 2019

On December 11, 2019, the “Maze Crew” again contacted Bleeping Computer and reported that the attack on the city of Pensacola, Florida in the early morning on December 7, 2019, was their doing. They also reported that they have shared documents stolen from the city and are waiting for a ransom of $1 million.[11] At this time, there is no corroboration of this on the part of city officials. In correspondences with Bleeping Computer, the threat actors stated that there was no connection with the recent NAS shooting, claiming it was a coincidence and that they did not know of it. They also stated: “we want to emphasize that no one of the socially significant services has suffered (for example 911)," as well as stating that they do not attack medical care centers and if someone uses their software in such a way that they will provide a free decryptor.[12]

Infection Vectors

Fallout Exploit Kit

Fallout was first discovered in August 2018, and was modified June 28, 2019. The exploit kit targets CVE-2018-4878 and CVE-2018-8174 which are a use after free vulnerability in Flash Player versions before 20.0.0.161 and a VBScript vulnerability, respectively, and both allow for remote code execution. Fallout uses shellcode to deliver the malicious payload. In the past it has also been used to deliver GandCrab ransomware and AZORult malware.[13] The first observation of Maze, in May 2019, was seen being distributed by Fallout through a site pretending to be a Abra cryptocurrency exchange app which purchased traffic from ad networks and selectively redirected traffic to the exploit kit. [14]

Spelevo Exploit Kit

Spelevo was first discovered in March 2019 and was modified October 17, 2019. The exploit kit targets CVE-2018-15982, a use after free vulnerability in Flash Player versions 31.0.0.153 and earlier, as well as 31.0.0.108 and earlier, which could allow for successful remote code execution. This exploit kit is also responsible for delivering IcedID as well as Dridex.[15]

---

[10] hxxps://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/
[11] hxxps://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/
[12] Ibid.
[13] hxxps://www.cybereason.com/blog/watch-where-you-browse-the-fallout-exploit-kit-stays-active
[14] hxxps://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/
[15] hxxps://blog.talosintelligence.com/2019/06/spelevo-exploit-kit.html

Brute Force Attack

The ransomware has also attacked victims by targeting open Remote Desktop Services (RDP) ports by scanning for systems running RDP (TCP port 3389) and attempting a brute force attack.[16]

IOCs

- C:\f\ojo\..\..\system32\som\vnt\..\..\wbem\q\wdun\jnw\..\..\..\wmic.exe" shadowcopy delete
- hxxp://92.63.8[.]47/content/news/snjw.jsp?a=c6&l=qf8g8tqly
- hxxp://92.63.32[.]2/bf.aspx?kwh=j4438k31h
- hxxp://92.63.37[.]100/qn.do?juw=aj
- hxxp://92.63.194[.]20/jcwgydcca.jspx?mwhi=0v3v3h&ojr=i03rqp4h7&dm=7ghn2a8a1
- hxxp://92.63.17[.]245/check/she.do
- hxxp://92.63.32[.]55/content/view/ov.jsp?pb=p8&afvb=6cfp5w&i=7f76t2v&au=54p5
- hxxp://92.63.11[.]151/webaccess/webauth/pqcadpkov.asp?cf=p4&h=ej&kchk=416
- hxxp://92.63.194[.]3/hlbrhcrogk.php?t=k3&i=snti74x&qbfw=wu043276&vjy=0
- hxxp://92.63.15[.]8/tracker/xgmuy.jspx?v=s76snl&j=4su31f2i&e=26f2110r&yh=w1a21f3p
- hxxp://92.63.29[.]137/doqlgpv.php?rgbf=23tkkklxs
- hxxp://92.63.32[.]57/view/b.phtml?tlqv=r088&agf=uj
- hxxp://92.63.15[.]56/yrawf.asp?i=0ry&kml=8usd357b&dhj=m7x&lyps=uew8h86
- hxxp://92.63.11[.]151/checkout/create/jvjmed.phtml?a=4j
- hxxp://92.63.32[.]52/ticket/ciqwisje.jspx?cdgn=005205lg1
- hxxp://92.63.15[.]6/withdrawal/ccuc.jsp?l=1pe41u76p7
- hxxp://104.168.198[.]208/wordupd.tmp
- hxxp://104.168.215[.]54/wordupd.tmp
- hxxp://104.168.174[.]32/wordupd_3.0.1.tmp
- hxxp://192.119.68[.]225/wordupd1.tmp
- hxxp://91.218.114[.]38/ticket/qrerqapv.jsp
- hxxp://91.218.114[.]25/check/evjgdec.jspx
- hxxp://91.218.114[.]79/archive/eqsuxsjii.aspx
- hxxp://91.218.114[.]32/yelwkdt.shtml
- hxxp://91.218.114[.]4/webaccess/sepa/aos.action
- hxxp://91.218.114[.]79/archive/eqsuxsjii.aspx
- hxxp://91.218.114[.]77/withdrawal/wywbiubddg.php
- hxxp://91.218.114[.]11/kgtlakrun.phtml
- hxxp://91.218.114[.]37/messages/sepa/udopsfgpy.action
- hxxp://91.218.114[.]37/messages/sepa/udopsfgpy.action
- hxxp://91.218.114[.]31/edit/irtfdlapkb.jsp
- hxxp://91.218.114[.]26/post/update/u.asp
- DECRYPT-FILES.html
- %ProgramData%\foo.dat
- MD5: f83fb9ce6a83da58b20685c1d7e1e546
- SHA-1: 01c459b549c1c2a68208d38d4ba5e36d29212a4f
- SHA-256: e8a091a84dd2ea7ee429135ff48e9f48f7787637ccb79f6c3eb42f34588bc684
- MD5: 8205a1106ae91d0b0705992d61e84ab2
- SHA-1: 49cdc85728bf604a50f838f7ae941977852cc7a2
- SHA-256: 91514e6be3f581a77daa79e2a4905dcbdf6bdcc32ee0f713599a94d453a26fc1
- Windows "files waiting to be burned to disc" notification
- hxxps://mazedecrypt[.]top/1dcb0b851e857d00
- hxxp://aoacugmutagkwctu[.]onion/1dcb0b851e857d00
- filedecryptor[@]nuke[.]Africa

[16] hxxps://malwaretips.com/blogs/remove-maze-ransomware/

- koreadec[@]tutanota[.]com
- yourrealdecrypt[@]airmail[.]cc

TA2101

In correspondence with writers at Bleeping Computer, the group claiming to be responsible for the Maze ransomware attacks on Allied Universal and the City of Pensacola referred to itself as TA2101, the name given to this threat actor by Proofpoint, stating, "Ask them a question: would they like if next Monday TA2101 impersonate Allied Universal in a spam campaign using the next certs?" In the initial email sent from the threat actor, they referred to themselves as "we" and signed the email from the "Maze Crew." The group claimed, during the same correspondence, that they were financially motivated and were not an "espionage group nor any other type of APT." It could be possible that the group or a part of the group is operating from somewhere in Asia, as upon releasing the files early, the group stated, "We have already morning of Friday. Yes, it is friday in asia. Forgot to mention that deadline is a friday by our local time, and not US."[17] However, they also posted to a Russian language forum dedicated to malware and hacking, the same information about their interactions with Allied Universal and released a portion of the files stolen from the company. In this post, they also added a mocking post script aimed at researcher Malwarehunterteam, stating that Cylance and Sophos did not prevent them from stealing and encrypting data, as well as another post script mentioning an unnamed Canadian Insurance company and threatening for them to "collect money faster!"[18]

This threat actor is also believed to be responsible for distributing Buran ransomware and the banking trojan IcedID. For the German and Italian campaigns, TA2101 used Cobalt Strike to deploy and execute malware and ransomware.[19] In other correspondences with Bleeping Computer, they referred to Maze ransomware as "our software," indicating that they are responsible for more than just distributing the ransomware.

TTPs

- Spoofed email domains – usually using a variant of [.]icu for European campaigns
- Malspam or Phishing URLs formatted with "word_/.tmp" in the string
- Cobalt Strike – used in campaigns targeting Germany, the tool emulates a backdoor framework to deliver and deploy malware or ransomware
- Malicious Microsoft Word Documents – Sent as part of a phishing campaign and claiming to require macros be enabled due to RSA encryption
- Multiple uses of the same purported RSA encryption key
- The same Start of Authority (SOA) is listed for multiple phishing lure campaigns - gladkoff1991[@]yandex[.]ru

Other Campaigns

November 12, 2019

TA2101 began a spam campaign targeting U.S. healthcare companies to distribute the IcedID banking trojan. Using a spoofed email domain, uspsdelivery-service[.]com, the group impersonated the United States Postal Service and sent out emails with a malicious Word document attachment which claimed to be secured by RSA encryption, as seen in previous campaigns. [20]

---

[17] hxxps://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/
[18] Ibid.
[19] hxxps://www.proofpoint.com/us/threat-insight/post/ta2101-plays-government-imposter-distribute-malware-german-italian-and-us
[20] Ibid.

Additional TA 2101 IOCs

- SHA256: 44991186a56b0d86581f2b9cc915e3af426a322d5c4f43a984e6ea38b81b7bed
- SHA256: cfd8e3a47036c4eeeb318117c0c23e126aea95d1774dae37d5b6c3de02bdfc2a
- SHA256: 9f2139cc7c3fad7f133c26015ed3310981de26d7f1481355806f430f9c97e639
- SHA256: 5f1e512d9ab9b915b1fc925f546ed559cbfa49df53229e2f954a1416cf6f5ee4
- SHA256: 97043f23defd510607ff43201bb03b9916a23bd71b5bdf97db357e5026732506
- SHA256: d617fd4b2d0824e1a7eb9693c6ec6e71447d501d24653a8e99face12136491a8
- SHA256:7e3ab96d2628e0a9970802b47d0356dc9b99994d7f98492d4e70a5384891695a
- antowortensienicht[@]bzst-infomieren[.]icu
- gladkoff1991[@]yandex[.]ru
- info[@]agenziaentrate[.]icu
- antwortensienicht[@]bzstinform[.]icu
- uspsdelivery-service[.]com
- hxxp://198.50.168[.]67/wordpack.tmp
- hxxp://conbase[.]top/sys.bat
- hxxp://192.119.68[.]225/wordupd1.tmp
- hxxp://108.174.199[.]10/wordupd3.tmp
- hxxp://54.39.233[.]175/wupd19823.tmp
- hxxp://54.39.233[.]131/word1.tmp
- hxxp://104.168.198[.]230/wordupd.tmp
- Bitcoin address 3Gq4AkdyUtH1aCYU6hczZkHGn5UJ4D6PQN

Mitigation and prevention

- Update antivirus and other software on a regular basis
- Keep backups maintained and stored in a secondary location
- Routinely update vulnerabilities with patches
- Monitor all remote connections to the network such as remote desktop protocols and MSP connections
- Use multi-factor authentication when possible and limit user access
- Educate users/staff about phishing recognition and password security