

Technical Analysis of PartyTicket Ransomware

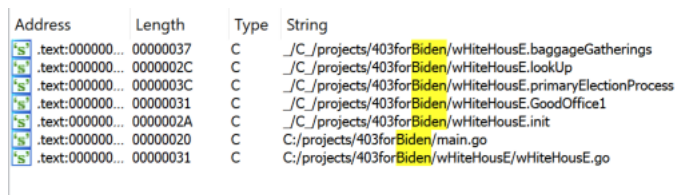
Key Points

- PartyTicket is an unsophisticated and poorly designed ransomware family that is likely intended to be a diversion from the Hermetic Wiper attack
- The ransomware generates a single AES key that is used to encrypt targeted files in GCM mode
- Files are decryptable because the AES key is generated using a random function that is deterministic

Technical Analysis

On 23rd Feb 2022, a new sophisticated malware family known as [Hermetic Wiper](#) was discovered that targeted organizations in the Ukraine with an objective of destroying data and causing business disruption. Hermetic Wiper appears to have been used in conjunction with another malware family that disguises itself as [ransomware](#). This secondary malware known as PartyTicket has the SHA256 4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382 and was written using the Go programming language. The first PartyTicket sample that was submitted to a public malware repository on 2022-02-23 22:29:59 UTC.

PartyTicket is quite distinct from typical ransomware families in that the design and implementation looks rushed and unsophisticated. For example, PartyTicket does not terminate processes such as databases and other business applications prior to encryption. Therefore, the number of potential files that can be encrypted is limited since many applications may have open file handles. In addition, the malware generates a 32 character alphanumeric key using the Go programming language's random function, which is deterministic. Therefore, the AES encryption key can be recovered and used to decrypt files. PartyTicket also stands out with numerous references that mock U.S. President Joe Biden as shown in Figure 1.



Address	Length	Type	String
.text:000000...	00000037	C	./C:/projects/403forBiden/wHiteHousE.baggageGatherings
.text:000000...	0000002C	C	./C:/projects/403forBiden/wHiteHousE.lookUp
.text:000000...	0000003C	C	./C:/projects/403forBiden/wHiteHousE.primaryElectionProcess
.text:000000...	00000031	C	./C:/projects/403forBiden/wHiteHousE.GoodOffice1
.text:000000...	0000002A	C	./C:/projects/403forBiden/wHiteHousE.init
.text:000000...	00000020	C	C:/projects/403forBiden/main.go
.text:000000...	00000031	C	C:/projects/403forBiden/wHiteHousE/wHiteHousE.go

Figure 1. PartyTicket code references mocking U.S. President Joe Biden

The malware takes a single command-line argument, which is the filename to encrypt. If the malware is launched without any arguments, it builds a list of files to encrypt. For every file in this list, the malware creates a new copy of itself using a name generated by calling the UUID Go library function, which is [based on the current timestamp and system's MAC address](#).

The new PartyTicket copy is then executed passing a filename to encrypt. This design choice is very odd because it slows the system down significantly, because a new process is created to encrypt every file. In addition, the numerous copies of the malware that are created fill up disk space, since the malware binary is larger than 3MB. Figure 2 shows an example of the numerous PartyTicket executables that were created during file encryption.

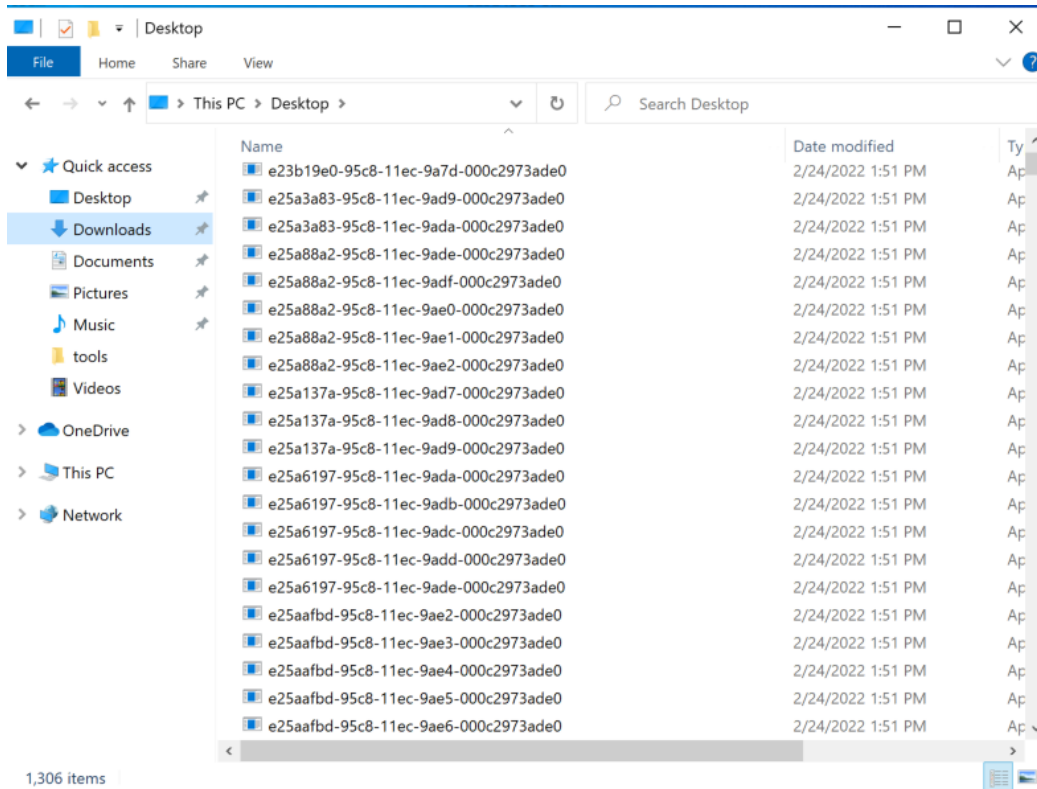


Figure 2. Copies of PartyTicket executables during file encryption

PartyTicket enumerates all files that have the extensions shown in Table 1.

```
.docx .doc .dot .odt
.pdf .xls .xlsx .rtf
.ppt .pptx .one .xps
.pub .vsd .txt .jpg
.jpeg .bmp .ico .png
.gif .sql .xml .pgsql
.zip .rar .exe .msi
.vdi .ova .avi .dip
.epub .iso .sfx inc
.contact .url .mp3 .wmv
.wma .wtv .cab .acl
.cfg .chm .crt .css
.dat .dll .html .htm
```

Table 1. Extensions targeted by PartyTicket

Files that are located in the *Windows* and *Program Files* folders are skipped. Before file encryption, the targeted file is renamed with the extension `.[vote2024forjb@protonmail.com].encryptedJB` as shown in Figure 3.

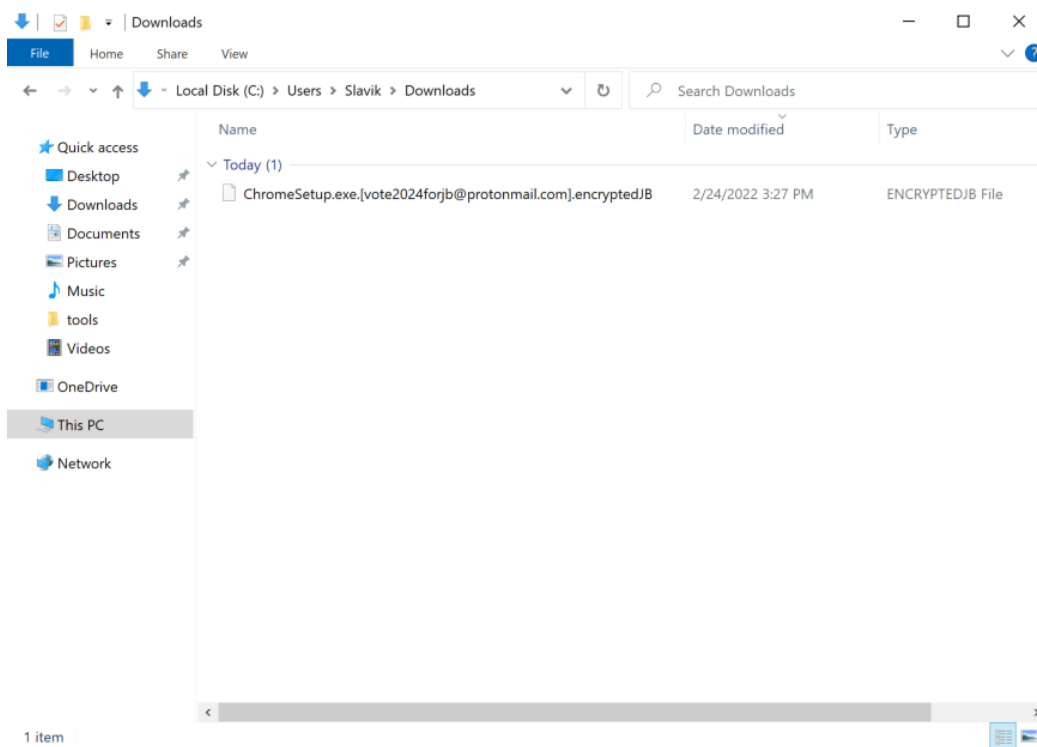


Figure 3. Example file extension encrypted by PartyTicket

The malware embeds a hardcoded 2,048-bit RSA key that is Base64 encoded. The modulus and exponent after the string has been Base64 decoded is the following:

```
{"N":257177505385644458758837704503150101577005970875073349074035004439130737027209399318246082709800202065660175
```

PartyTicket uses this RSA public key to encrypt the AES key that is used for file encryption. Files are encrypted with AES in GCM mode using a 32-byte alphanumeric string that is created using the Go function `math.rand.Int()`, which is deterministic and therefore not cryptographically secure. The encrypted file format consists of the first 12 bytes used as the AES-GCM nonce, followed by the AES encrypted data, a 16-byte AES-GCM authentication tag, the RSA encrypted AES key, and finally appended with the string marker `ZVL2KH87ORH3OB1J1PO2SBHWJSNFSB4A`.

After each file is encrypted, the corresponding temporary copy of the ransomware is then deleted.

The ransom note is written to the user's desktop using the filename `read_me.html`. An example ransom note, when rendered in a web browser, is shown in Figure 4.

"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: `e2232904-95e8-11ec-9517-000c2973ade0`

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instructions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

- 1) `vote2024forjb@protonmail.com`
- 2) `stephanie.jones2024@protonmail.com` - if we don't answer you during 3 days

Have a nice day!

Figure 4. Example PartyTicket ransom note

The `special ID` value is generated by calling the Go UUID function and does not serve any purpose.

Zscaler coverage

We have ensured coverage for the payloads seen in these attacks via advanced threat signatures as well as our advanced cloud sandbox.

Advanced Threat Protection

Win32.Trojan.HermeticWiper

Advanced Cloud Sandbox

Win32.Trojan.HermeticWiper

Figure 5 below shows the sandbox detection report for PartyTicket.

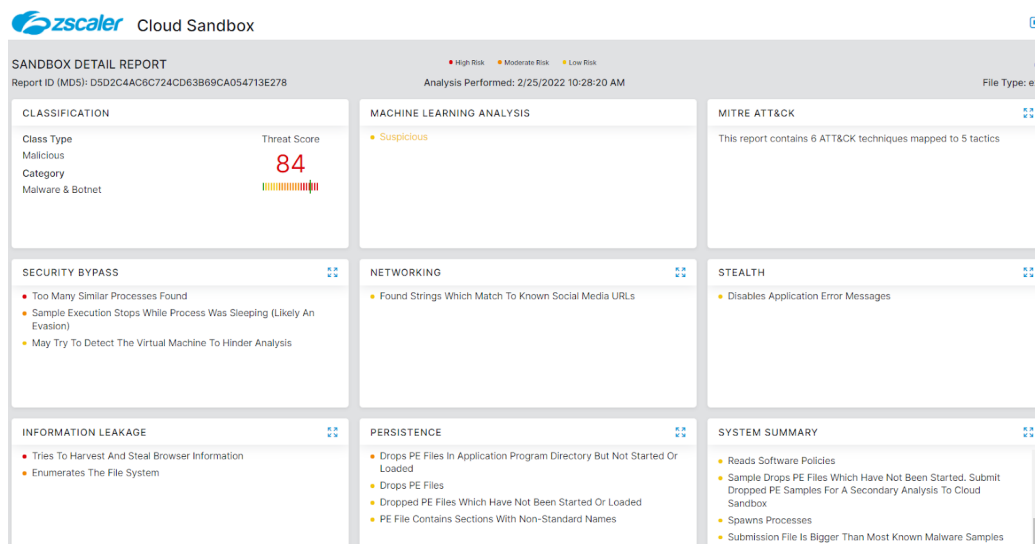


Figure 5. Zscaler Cloud Sandbox Report - PartyTicket