Technical Analysis of Industrial Spy Ransomware

zscaler.com/blogs/security-research/technical-analysis-industrial-spy-ransomware

Industrial Spy is a relatively new ransomware group that emerged in April 2022. In some instances, the threat group appears to only exfiltrate and ransom data, while in other cases they encrypt, exfiltrate and ransom data. Industrial Spy started as a data extortion marketplace where criminals could buy large companies' internal data; they promoted this marketplace using README.txt files that were downloaded using malware downloaders disguised as cracks and adware. After these initial promotional campaigns, the threat group introduced their own ransomware to create double extortion attacks that combine data theft with file encryption. The threat group appears to have also seemingly tried Cuba ransomware briefly before developing their own ransomware in May 2022.

Key points

- Industrial Spy is a relatively new group that emerged in April 2022 that started by ransoming stolen data and more recently has combined these attacks with ransomware.
- The threat group exfiltrates and sells data on their dark web marketplace, but does not always encrypt a victim’s files.
- The ransomware utilizes a combination of RSA and 3DES to encrypt files.
- Industrial Spy lacks many common features present in modern ransomware families like anti-analysis and obfuscation.
- The threat group is consistently adding roughly two to three victims per month on their data leak portal.

Industrial Spy Market Promoter

There are two primary executables associated with Industrial Spy. The first binary does not implement any destructive functionality, while the second performs file encryption. The former has been mainly distributed using cracks, adware and other malware loaders. Zscaler ThreatLabz has observed this binary being distributed in-the-wild with other loaders and stealers involving SmokeLoader, GuLoader and Redline Stealer. The sole purpose of this malware is to promote their dark web marketplace; it does not inflict any actual damage to the targeted system.

Technical Details

This malware is very basic and performs the following actions before deleting itself:

Display a text-based note promoting the Industrial Spy data leak site (as shown in Figure 1).

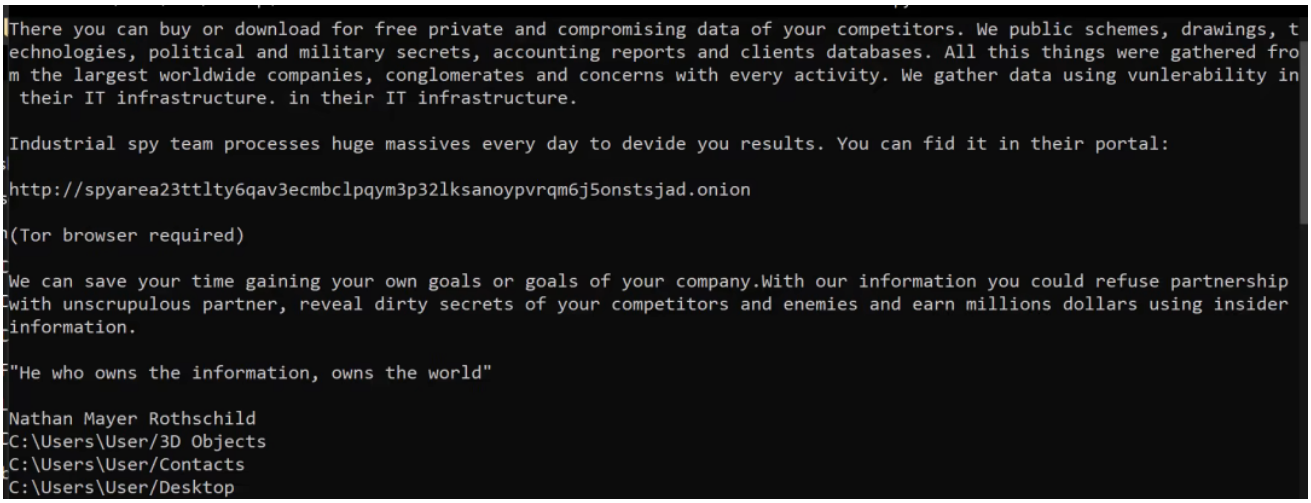

Figure 1: Industrial Spy data leak marketplace promotion note

- Enumerate paths under the registry key *SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList* and drop the file *readme.txt* recursively under all paths with the same note content.
- Change the wallpaper (shown in Figure 2) to advertise the Industrial Spy data leak marketplace.

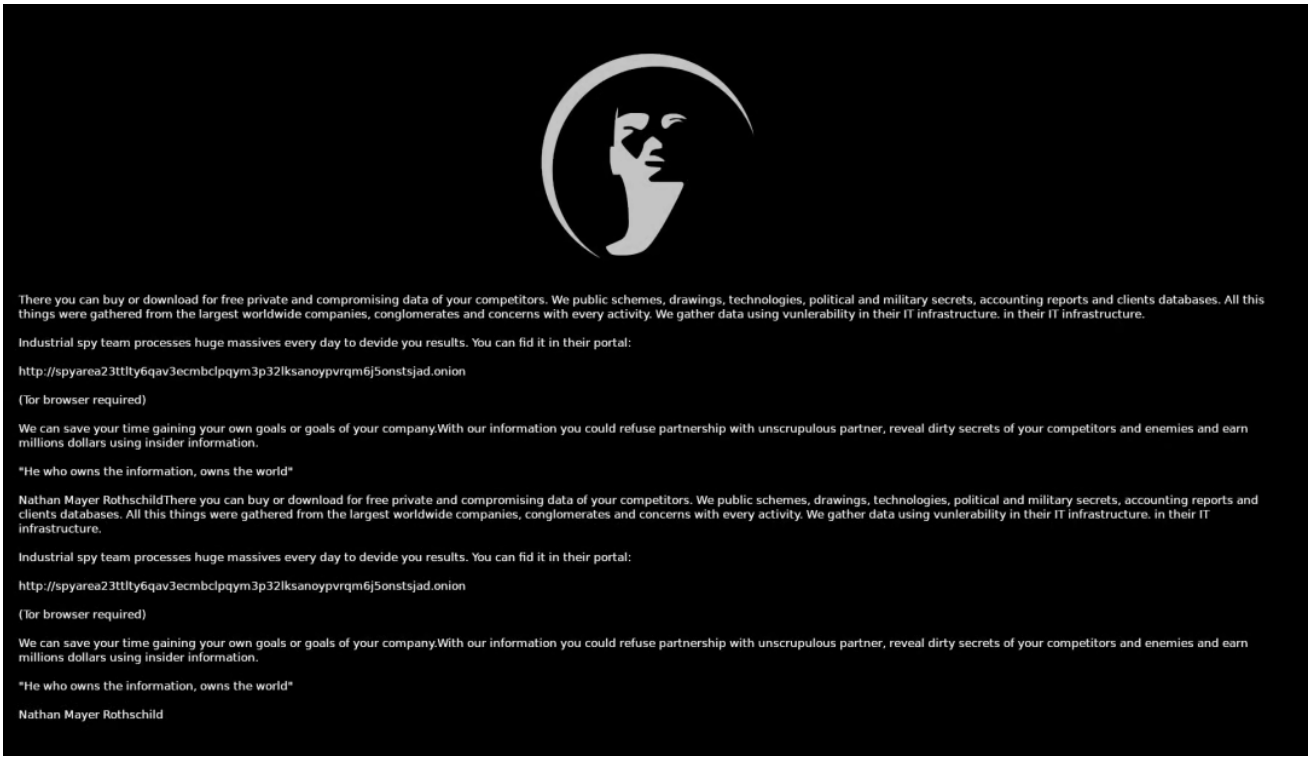

Figure 2: Desktop wallpaper set by the Industrial Spy marketplace promotion binary

Industrial Spy Ransomware

The Industrial Spy threat group introduced their own ransomware in May 2022. The Industrial Spy ransomware family is relatively basic and parts of the code appear to be in development. Industrial Spy utilizes very few obfuscation methods other than building strings on the stack at runtime. The ransomware also lacks many of the features commonly seen in modern ransomware families (such as anti-debug, anti-sandbox, etc.), although this may change in the future.

Currently, there are not many Industrial Spy ransomware samples that have been observed in-the-wild. However, the group is consistently adding roughly two new victims per month on their data leak portal.

Technical Details

The Industrial Spy ransomware encryption and decryption both are handled by the same binary. Simplified steps taken by the ransomware are as follows:

- Parse command-line arguments
- Delete shadow copies
- Start an encryption thread to encrypt all drives or given paths
- Self-delete

Delete Shadow copies

Similar to other ransomware families, Industrial Spy deletes Windows shadow copies to make file recovery more difficult as shown in Figure 3.

```
*(_DWORD *)Operation = 0x70006F;              // open
v2 = 0x6E0065;
v3 = 0;
*(_DWORD *)File = 0x730076;                   // vssadmin.exe
v5 = 0x610073;
v6 = 0x6D0064;
v7 = 0x6E0069;
v8 = 0x65002E;
v9 = 0x650078;
v10 = 0;
*(_DWORD *)Parameters = 0x650064;             // delete shadows /all /quiet
v12 = 0x65006C;
v13 = 0x650074;
v14 = 0x730020;
v15 = 0x610068;
v16 = 0x6F0064;
v17 = 0x730077;
v18 = 0x2F0020;
v19 = 0x6C0061;
v20 = 0x20006C;
v21 = 0x71002F;
v22 = 0x690075;
v23 = 0x740065;
v24 = 0;
ShellExecuteW(0i64, Operation, File, Parameters, 0i64, 0);
return 0i64;
```

Figure 3: Industrial Spy pseudocode to delete Windows shadow copies

Mode of Operation

On execution, Industrial Spy checks whether an RSA public or RSA private key is embedded in the binary. Depending on the type of key, the ransomware will encrypt or decrypt files as shown below:

```
if ( mw_ptr_key_encryption_public == 0x1F ){
  if ( mw_ptr_key_decryption_private != (char)0xF1 ) {
   // decrypt files
   }
} else {
   // encrypt files
}
```

Interestingly, it will always delete shadow copies irrespective of the mode.

If command-line arguments are provided, Industrial Spy will start a thread to recursively encrypt files for each path argument that is provided. If no arguments are given, Industrial Spy will enumerate all drives and start one thread per volume (if it is not read-only). Each thread will recursively enumerate and encrypt files. All files for which the extension and path does not fall under the exclusion list will be encrypted. Paths containing the following strings are excluded:

- *microsoft*\
- *google**chrome*
- *mozilla**firefox*
- *opera*\

The following file extensions are also excluded:

.	.mst	.inf1	.shs	.dll	.scr	.cmd	.ps1	.jse
.bat	.paf	.ins	.u3p	.exe	.sct	.com	.reg	.vbscript
.bin	.pif	.inx	.vb	.gadget	.shb	.cpl	.rgs	.msi
.job	.vbs	.isu	.vbe	.lnk	.ws	.msc	.wsf	.wsh

During encryption, if the targeted file is locked by another process, Industrial Spy will attempt to terminate the process that holds the corresponding file handle, using the Restart Manager API.

File Encryption

Industrial Spy encrypts each file's content with the Triple DES (3DES) algorithm. Each 3DES key and initialization vector (IV) are then encrypted with a hardcoded RSA public key. The result is appended with a footer to the encrypted file data. Industrial Spy will encrypt up to the first 100MB of data. Since 3DES is a block cipher, each block is padded accordingly with NULL (0x00) bytes to form a multiple of 24 bytes.

After encryption, the original file content is overwritten with the following data shown in Figure 4.

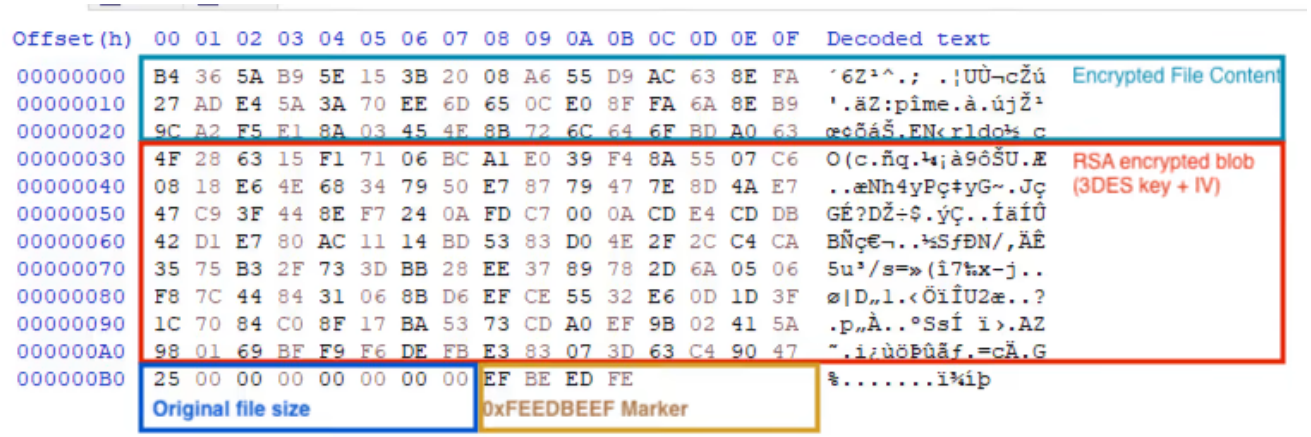

Figure 4: Industrial Spy encrypted file structure

The encrypted file data structure is as follows:

```
struct encrypted_file {
    byte 3des_encrypted_file_content[encrypted_size];
    byte rsa_encrypted_key_blob[128];
```

```
    qword original_file_size;
    dword end_of_encrypted_file_marker;  // 0xFEEDBEEF
};
```

The encryption parameters data structure is the following:

```
struct rsa_encrypted_key_blob {
    word block_type; // 0x200 (used to validate RSA decryption result)
    byte  random_bytes[77];  // random byte padding
    byte null; // 0x00
    byte  3des_key[24];  // used for file data encryption
    byte  iv[24];   // only the first 8 bytes are used
};
```

Unlike nearly all ransomware families, Industrial Spy does not change the file extension after encryption. Therefore, the filename itself cannot be used to determine the files that have been encrypted. Instead, Industrial Spy appends a file footer that can be used to identify encrypted files using the last four bytes: **0xFEEDBEEF**.

RSA Key

The RSA code used by Industrial Spy is very similar to the **ISFB trojan's source code**. This RSA library was also used by the ransomware known as WastedLocker. Each Industrial Spy ransomware sample contains a hardcoded 1,024-bit RSA key that is unique to each victim in the following format:

```
00040000D614C843C04CAF61ECEA5DB83FED16FC15D194317C741FB1794D2AC2F4831849CF1788C3F451CF61
976C90BAF9DEDBE5CFF34E6CB920326B78957BAA61566F78154C810B2A7158530B3E926AAC9A4E34D00306DD
00CB434F5445B30C04AE20302C6E8B8F33FE2CF6EDCDE90191923929E54F18441B1F0A94735AB42D68502BD90
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000
```

Figure 5: Embedded Industrial Spy RSA public key

The first dword (4-bytes) in blue is the size of the RSA key in bits (0x400), which is 1,024 bits. The RSA key size is then followed by the modulus highlighted above in turquoise. The modulus contains a number of NULL bytes for padding, finally followed by the RSA public exponent (in orange) along with additional padding.

Key Generation

Industrial Spy generates a per file 3DES key and IV using the RSA library's random function *R_GenerateBytes()*. This function takes a random structure as an argument to generate these values. The random structure itself is seeded by calling the x86/x64 CPU instruction *rdtsc*,

which returns the processor's timestamp. The CPU processor timestamp records the number of CPU clock cycles since the last reset. The result of *rdtsc* is passed to the RSA random function *R_RandomUpdate()*.

The *R_GenerateBytes()* function is called twice to generate two 24-byte pseudorandom buffers. The first buffer is used as a 3DES key for encrypting the file's data, and the first 8 bytes from the second buffer are used as the IV.

A Python-based proof-of-concept Industrial Spy ransomware decryptor can be found in the Zscaler ThreatLabz GitHub tools repository.

Ransom Note

A file with the name *readme.html* is dropped in each directory that contains a ransom note as shown in Figure 6.

Greetings! Unfortunately ,we have to report you that your company was compromised. All your files were encrypted and you can not restore them without our private key. Trying to restore it without our help may cause complete loss of your data.
Also we researched whole your corporate network and downloaded all your sensitive data to our servers,. if we will not get any contact from you in 3 next days we will publish your data on the site Industrial 即py market
you can find it there (http://spyarea23ttlty6qav3ecmbclpqym3p32lksanoypvrqm6j5onstsjad.onion)
tor browser is needed (https://www.torproject.org/download/)
Also, we respect your work and time and we are open for communication in that case we are ready to discuss recovering your files and work. we can grant absolute privacy and compliance with agreements by our side. Also we can provide all necessary evidence to confirm performance of our products and statements.

Feel free to contact us with mail:

---
inbox@supports24.net
inbox@supticket.com

Please contact us by both of email addresses shown below to keep in touch with us.
mark your messages with your personal id:6e9686fecf202eef5ae1e6a45e0b7849

Figure 6: Example Industry Spy ransom note

A copy of the Industrial Spy ransom note can be found in the ThreatLabz GitHub ransom note repository here.

Victim ID

The Victim ID referred to as the *personal id* in the ransom note is just the MD5 hash of the modulus component of the embedded RSA public key.

Dark Web Market

The Industrial Spy leak portal is protected with a username and password as shown below in Figure 7.

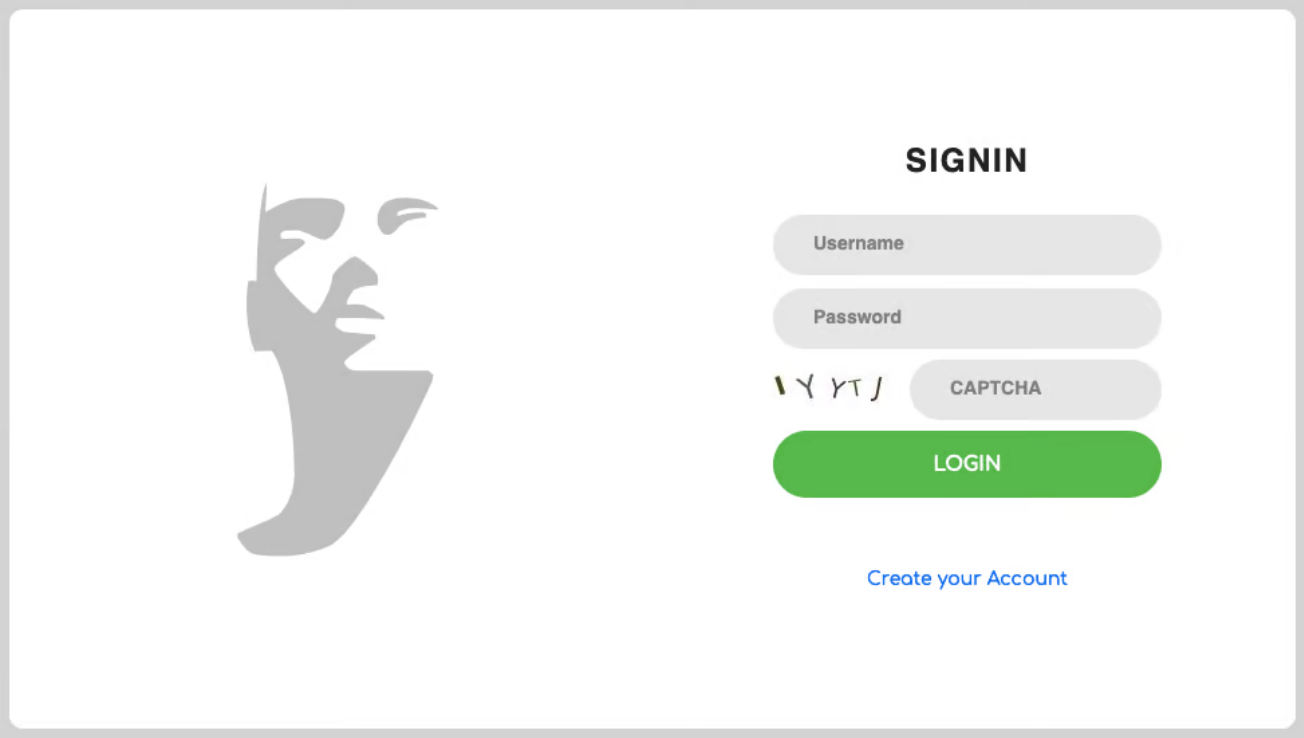

Figure 7: Industrial Spy market login page

After authentication, the Industrial Spy home page is displayed as shown in Figure 8.

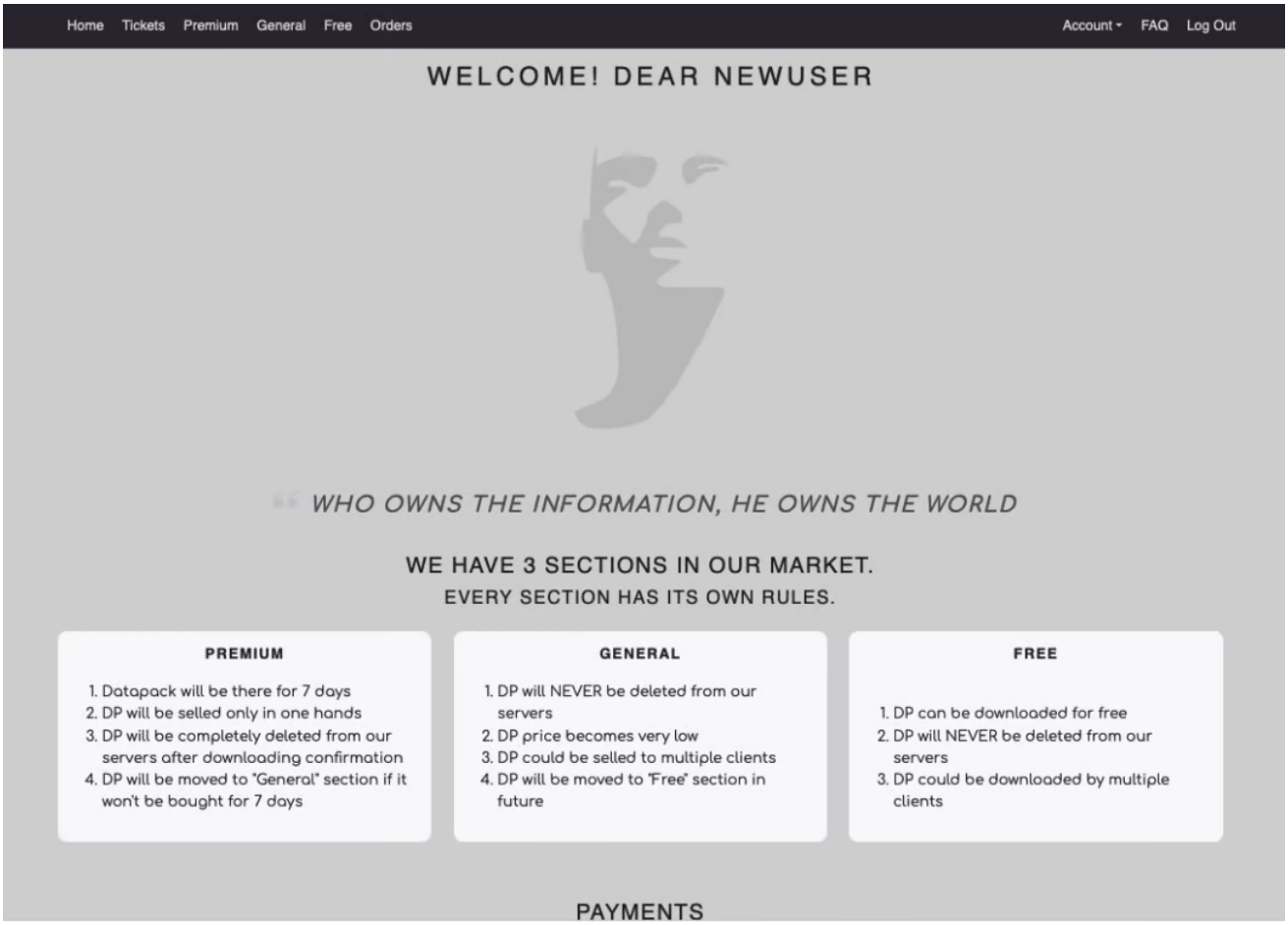

Figure 8: Industrial Spy market home page

The first victim on the leak site was listed on 03/15/2022. The total victim count as of 25 July 2022 was 37, and are broken down into the following categories:

- 24 Free
- 13 General
- 0 Premium

Industrial Spy is mostly selling individual files (in the *General* category) instead of file bundles in the price range from $1 to tens of thousands of dollars. The group likely reviews the files before deciding whether to put a high price tag on sensitive files, and dumps the rest of the files with a $1 to $2 price tag. ThreatLabz has observed operating system files that have limited value like desktop.ini, thumbs.db listed for $2 as shown in Figure 9.

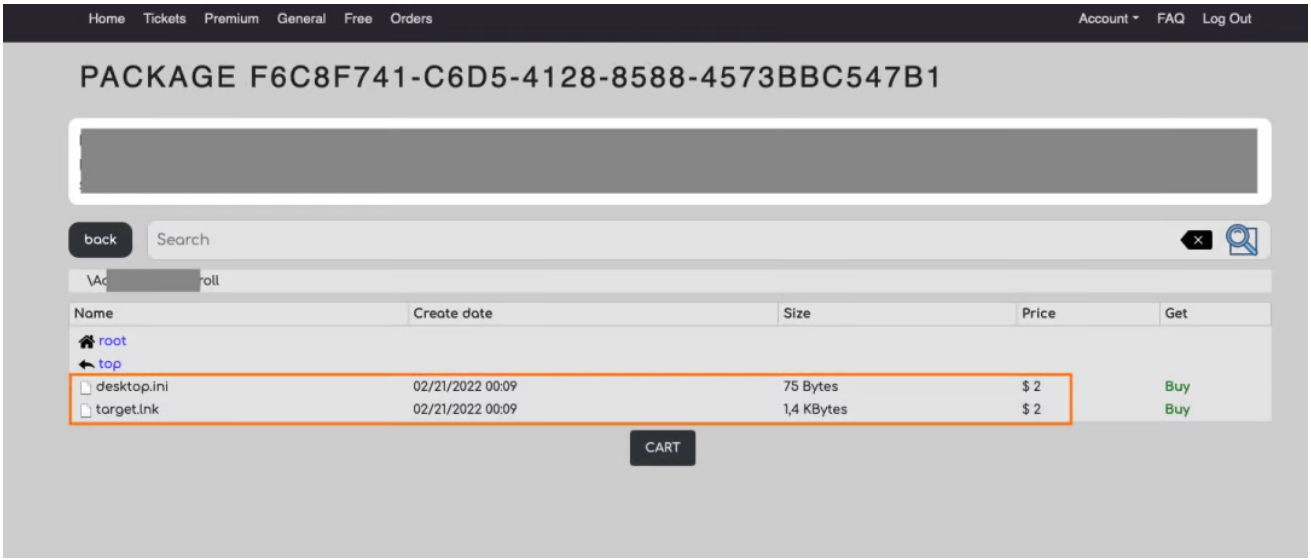

Figure 9: Operating system files (e.g., desktop.ini) listed by Industrial Spy for $2

Conclusion

Industrial Spy is a new entrant in the ransomware ecosystem. The malware is not currently very sophisticated, but the file encryption is functional making it a dangerous threat. Furthermore, Industrial Spy is consistently adding new victims, proving that the threat group has the capabilities to breach new organizations. Many players come and go in the ransomware market and it is difficult to determine the groups that will stay for the long term. However, this threat group is likely to stay at least in the near future with more ransomware updates and features to follow. ThreatLabz continues to monitor all kinds of threats and provide coverage to our customers.

Cloud Sandbox Detection

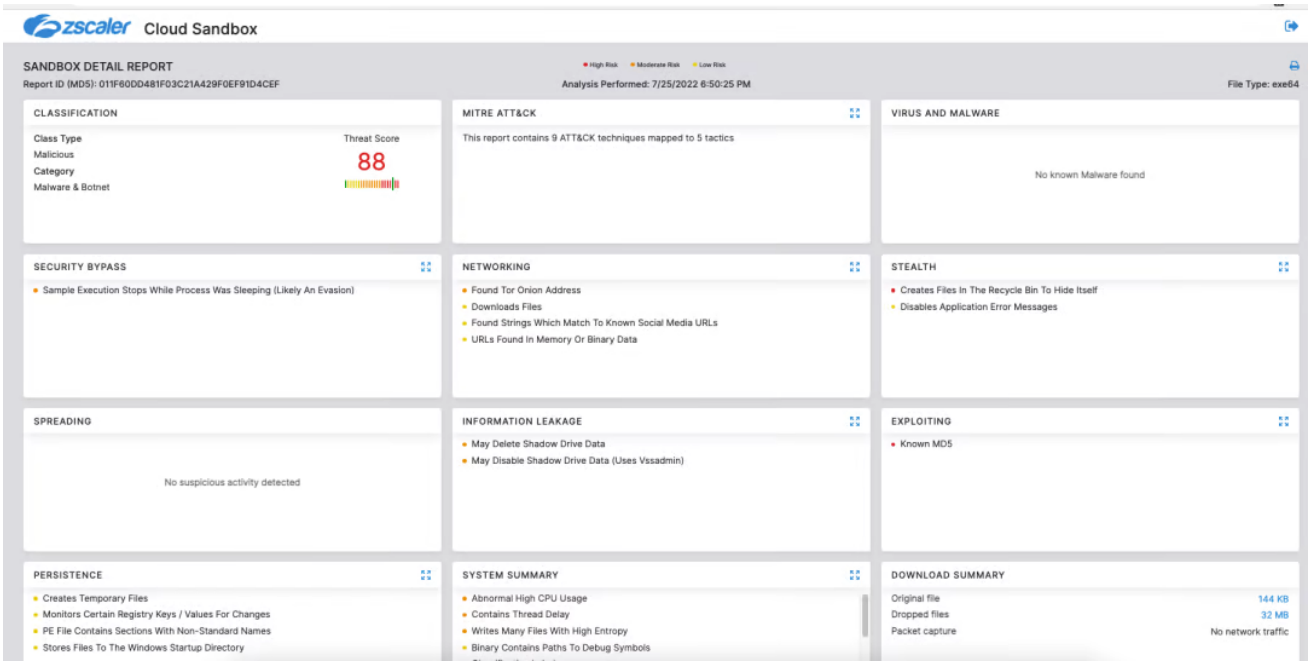

Figure 10: Zscaler Cloud Sandbox Report

In addition to sandbox detections, Zscaler's multilayered cloud security platform detects indicators related to the campaign at various levels with the following threat names:

Win32.Ransom.IndustrialSpy

Indicators of Compromise (IOCs)

SHA256	Description
8a5c7fff7a7a52dca5b48afc77810142b003b9dae1c0d6b522984319d44d135a	Industrial Spy ransomware (debug build)
dfd6fa5eea999907c49f6be122fd9a078412eeb84f1696418903f2b369bec4e0	Industrial Spy ransomware
5ed4ffbd9a1a1acd44f4859c39a49639babe515434ca34bec603598b50211bab	Industrial Spy market promoter trojan

62051ec55c990d2ff21f36a90115986e4ac0eada18306f39687e209f49f2c6ec	Industrial Spy market promoter trojan
911153af684ef3460bdf568d18a4356b84efdb638e3e581609eb5cd5223f0010	Industrial Spy market promoter trojan
85ea71c910ebb00ba8cae266bf18400a15b08bd341e37e12083ab9a79ff6c943	Industrial Spy market promoter trojan
c96b098cab47c0a33d0b6d8f14b24e7c9ba897b0c59a2ac1f3dc608ca7a2ed7e	Industrial Spy market promoter trojan