Malware Analysis Report: “Practical3.exe”

CAP6137 Malware Reverse Engineering: P0x03

Naman Arora
naman.arora@ufl.edu

April 12, 2021

Contents

1 Executive Summary

The provided binary has been identified as a member of *Ryuk* family of *Ransomwares* [1]. This family of ransomwares gain access to victim systems via phishing [2] or social engineering attacks [3] and are known to be biased towards targeting commercial systems more as compared to personal systems. *FBI* warned against this campaign citing the malware authors as most profitable when compared to other authors of such malwares. Also, this malware family is known to attack *Windows* systems in general and *Windows 10* systems in particular.

The malware binary itself is very small in size, around *170 KB*, and has no significant obfuscation techniques built in. Nevertheless, on dynamic analysis, the malware injects itself into common *Windows* processes and installs a registry key to achieve persistance over reboots. Any new file created or drive *(for eg. USB etc.)* connected to the system is also targeted and encrypted. Before any encryption happens, the malware,

- Stops and kills multiple services and executables generally associated with commercial systems
- Enumerates all drives associated to the system and all the files within them.

The execution of malware is entirely offline and hence once infected, isolating the system from the network does not thwart its any malicious activities. This also means that leaking of sensitive information from the infected system is highly improbable as a result of this infection. After encryption, the malware installs multiple text files named *RyukReadme.txt* acknowledging the data loss, stating the ransom and providing correspondence email and *Bitcoin Wallet* addresses. This ransomware family has, however, built up a reputation of consistently decrypting the data once ransom has been paid.

Independent analysis as well as aggregated opinion from the community very strongly suggests that decrypting the data without paying the ransom amount is not possible. The cryptographic algorithms used for encryption are industry standard and hence extensively secure. The prime recommendation would be to pay the ransom unless,

- the data lost has been backed up and is tested to be recoverable to its fullest extent.
- the lost data cumulatively provides less value than ransom itself.

2 Static Analysis: Primary Executable

2.1 Basic Identification

2.2 Malware Sample Family Identification

2.3 PE Sections

2.4 A case for Packing

2.5 Interesting Imports

3 Dynamic Analysis

3.1 Network Based Analysis

3.2 File System Based Analysis

4 Indicators of Compromise

4.1 Network Based

4.2 Host Based

4.3 *YARA* Rule

Visit [**ghub**] for rule file if copying fails.

```
rule practical2_rat {
        meta:
                description = ”Detect Practical2.exe RAT”
                author = ”Naman Arora”
                date = ”2021-03-17”
                hash = ”9633d0564a2b8f1b4c6e718ae7ab48be921d435236a403cf5e7ddfbfd4283382”
        strings:
                $pdb = ”C:\\Users\\W7H64\\Desktop\\VCSamples-master\\VC2010Samples\\ATL\\General\\AtlCon\\bitcoin coinjoin op.pdb” fullword ascii
                $ops = {c6 04 0a c2 b8 01 00 00 00 c1 e0 00 8b 4d 84 c6 04 01 10 b8 01 00 00 00 d1 e0 8b 4d 84 c6 04 01 00 b8 01 00 00 00 6b c8 03 8b 55 84 c6 04 0a 90}
        condition:
                uint16(0) == 0x5a4d and filesize < 1500MB and all of them
}
```

5 Appendix A: Screenshots

References

[1] Federal Bureau of Investigation. *Ransomware*. `https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware`. [Online; accessed 11-April-2021].

[2] WikiMedia. *Phishing*. `https://en.wikipedia.org/wiki/Phishing`. [Online; accessed 11-April-2021].

[3] WikiMedia. *Social Engineering*. `https://en.wikipedia.org/wiki/Social_engineering_security`. [Online; accessed 11-April-2021].