Rook ransomware analysis

seguranca-informatica.pt/rook-ransomware-analysis/

March 17, 2022

Rook ransomware is relatively recent, and one of the advantages of this line's other threats is the multithreading engine that pulverizes the encryption speed during its execution. In this article, we will go through the details of rook, describe the most effective techniques, and provide some measures to fight ransomware in general.

Rook is a recent malware and a fresh variant of the leaked Babuk ransomware code. The source code was leaked in a Russian underground forum in September 2021, and now criminals can perform changes or simply improve their arsenal by using the intelligence of this piece.

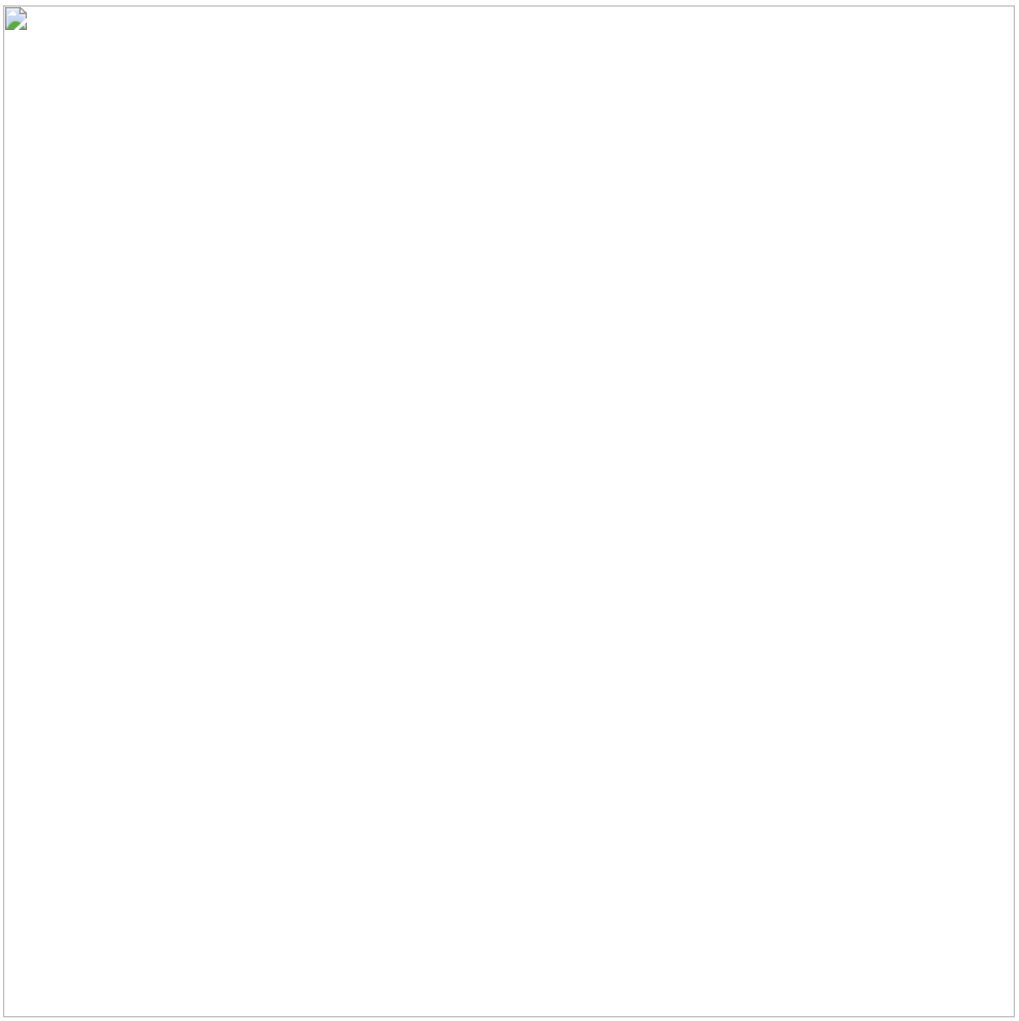


Figure 1: *Babuk — source code leaked September 2021.*

The malware was observed during a threat hunting activity by malware experts on VirusTotal. On Nov. 30th, 2021, the Rook operators claimed the first victim: a Kazakh financial organization where criminals stole 1,123 GB of information.

As usual, this kind of threat is often implanted on internal networks via CobalStrike after a well-succeeded cyberattack. However, security researchers found some phishing emails and torrent downloads with MS Office files infected with CobalStrike beacons to distribute the threat around the globe.

At first glance, the executable seems to be packed with UPX according to the section names, and a string with suspicious length can be observed — probably related to the key used during the encryption process.

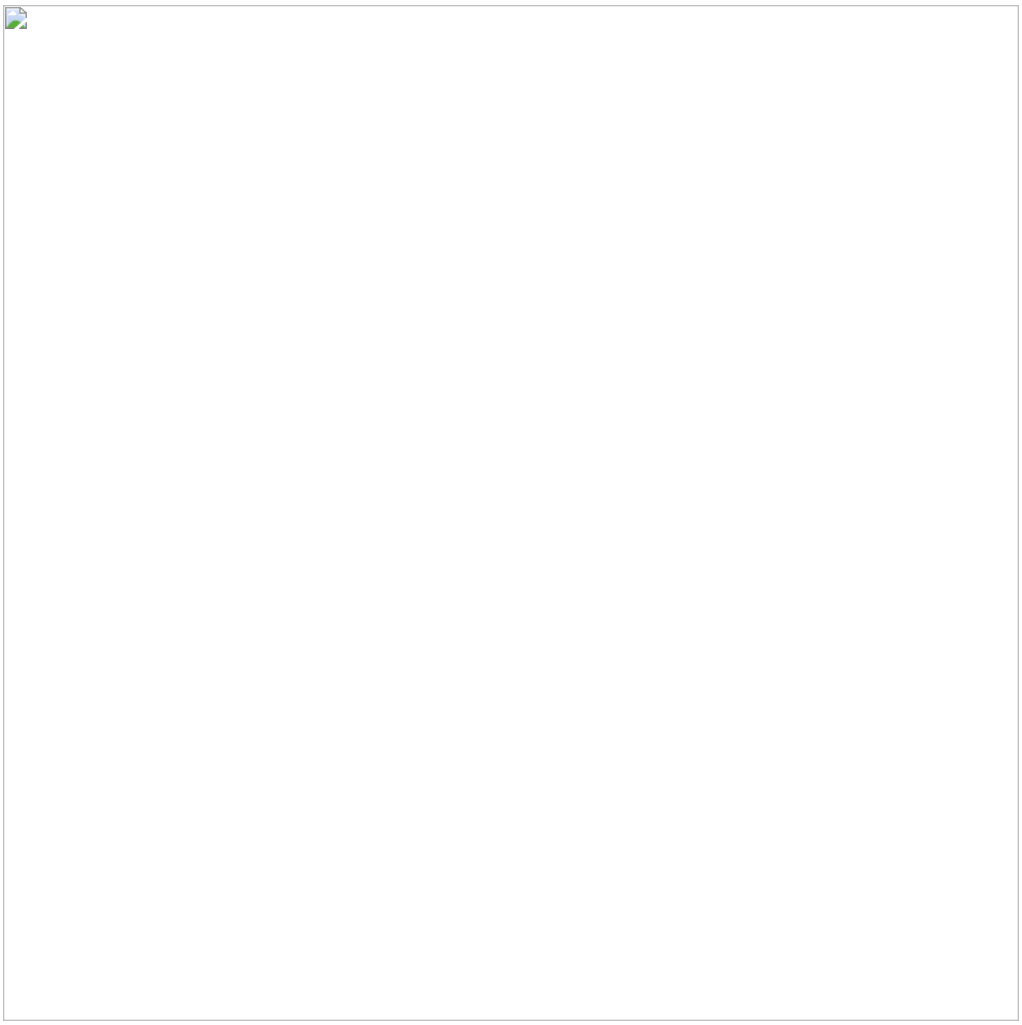


Figure 2: *Details about the Rook ransomware sections and suspicious string size.*

Rook — technical details

After executing on the target machine, Rook tries to find a specific mutex “asfgjkl878645165456fa888” to avoid re-infection or simply create it if the machine is a good candidate.

Figure 3: *Mutex created after the Rook execution. If the mutex is valid, the malware terminates the execution.*

Drives and network resources with multi-threading power

Next, the malicious process continues, and the network resources and local drives are enumerated. After that, a multi-thread mechanism is used to speed up the encryption process, as observed in Figure 4 below.

Figure 4: *Multi-thread mechanism implemented by Rook operators to speed up the encryption process.*

In detail, the malware calculates the number of threats that it needs to encrypt the files simultaneously (24 times the number of processors).

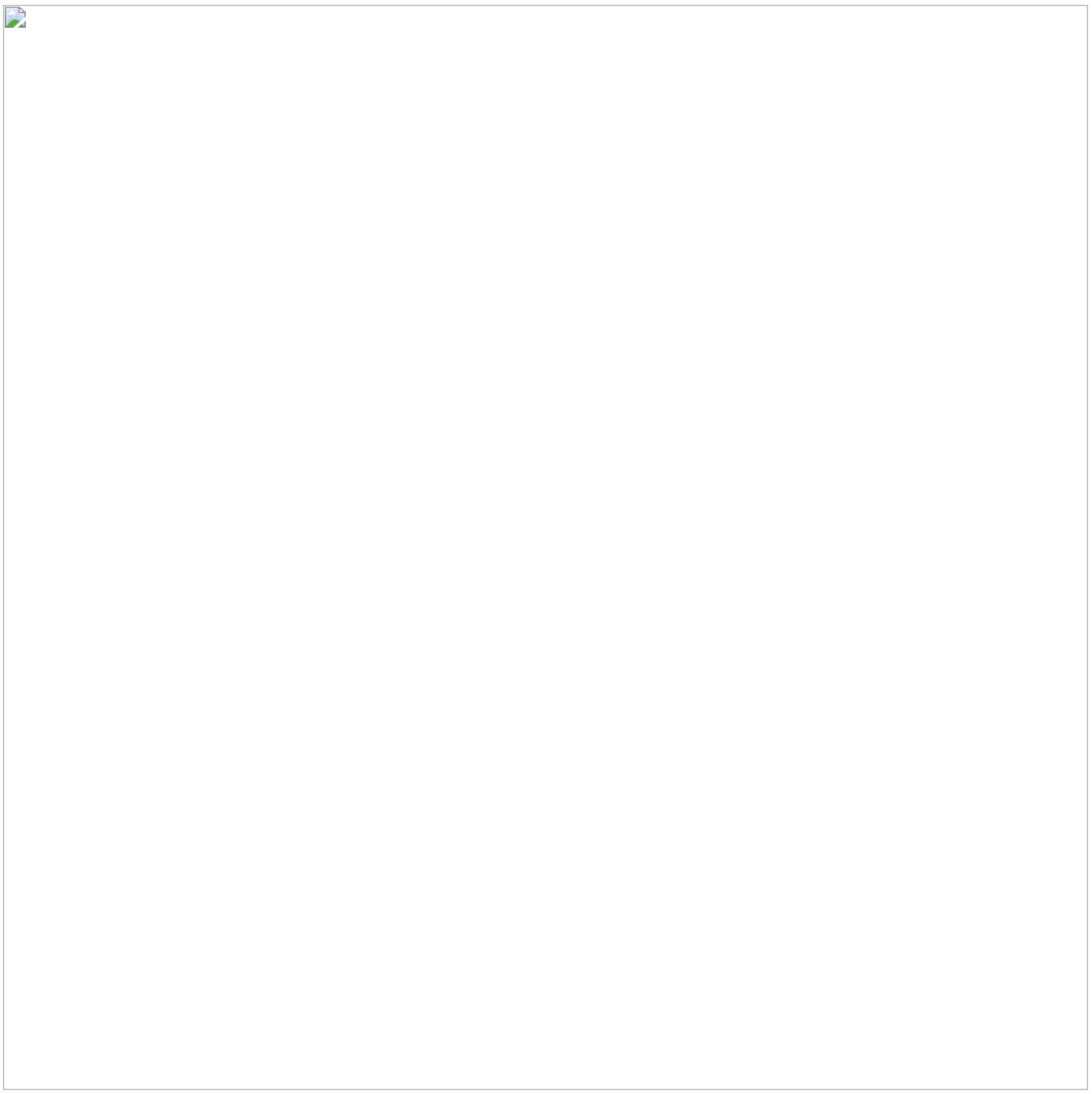
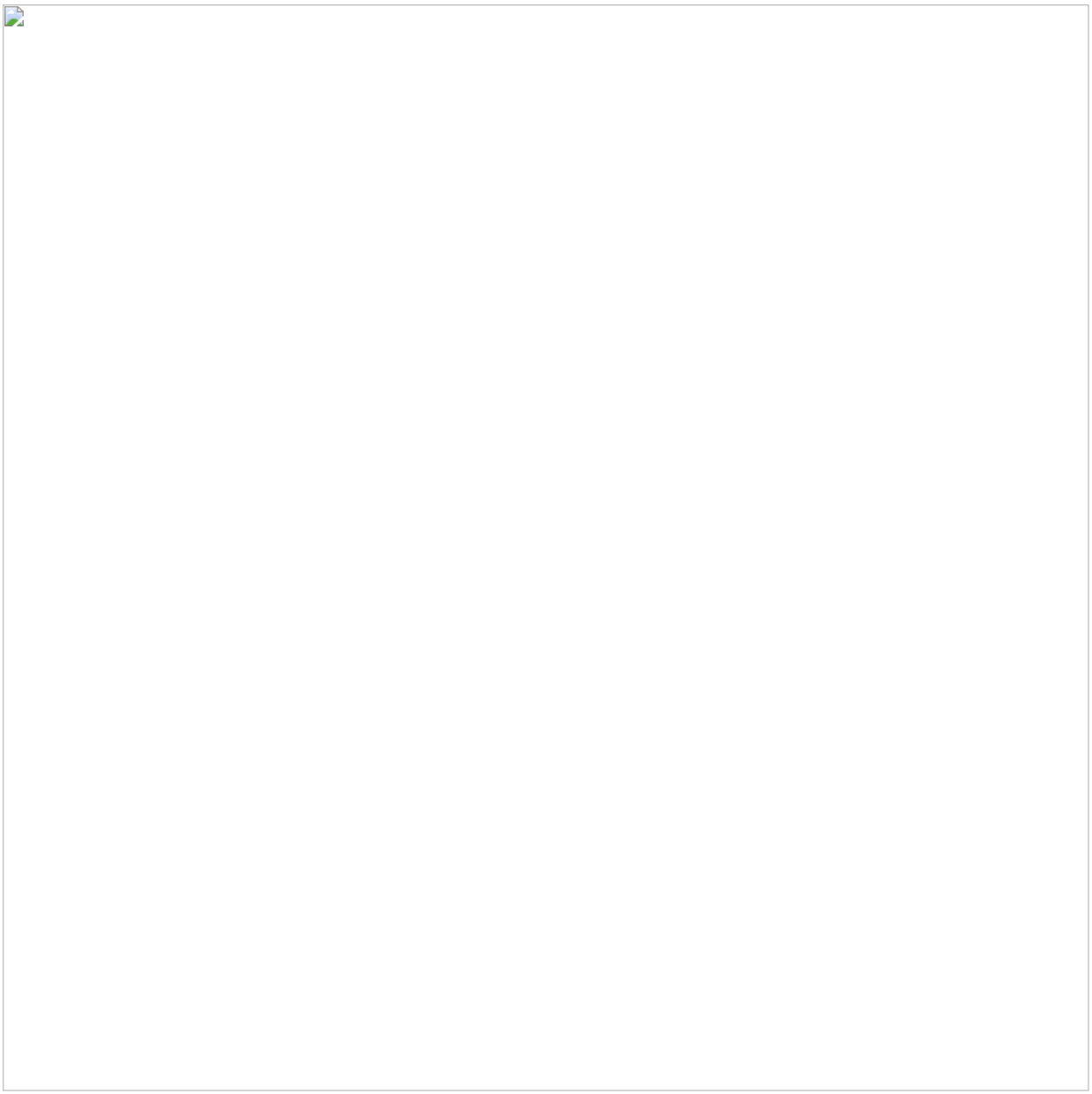


Figure 5: *Calculation of the number of threats to use to encrypt files.*

Preparing the encryption process

One of the main tasks before starting the encryption process is the creation of the RSA asymmetric keys. The ransomware uses the RegCreateKeyExW API call to open the Software subkey available on “HKEY_CURRENT_USER.” If the public key exists, Rook uses it. On the other hand, an RSA key pair is generated: “RookPublicKey” and “aRookprivatekey,” and the values are stored on the Windows Registry. The described process is illustrated in Figure 6 below.



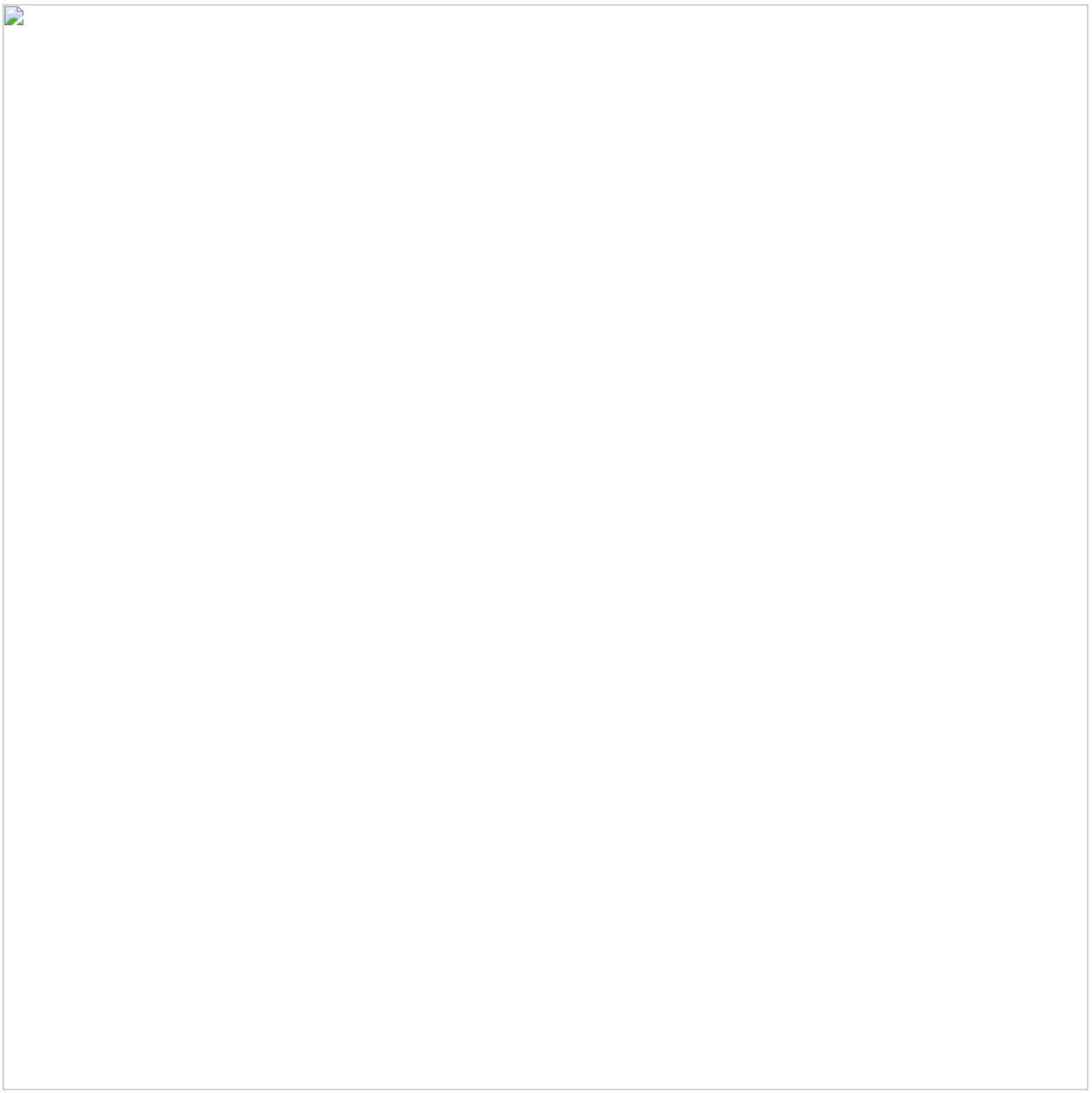


Figure 6: *Rook — generation of RSA public-private key pair during execution.*

Terminate services and processes and skip folders and files

As observed in other ransomware families, Rook has hardcoded a list of services to be terminated before starting the encryption task, preventing, thus, any errors affecting the encryption process.

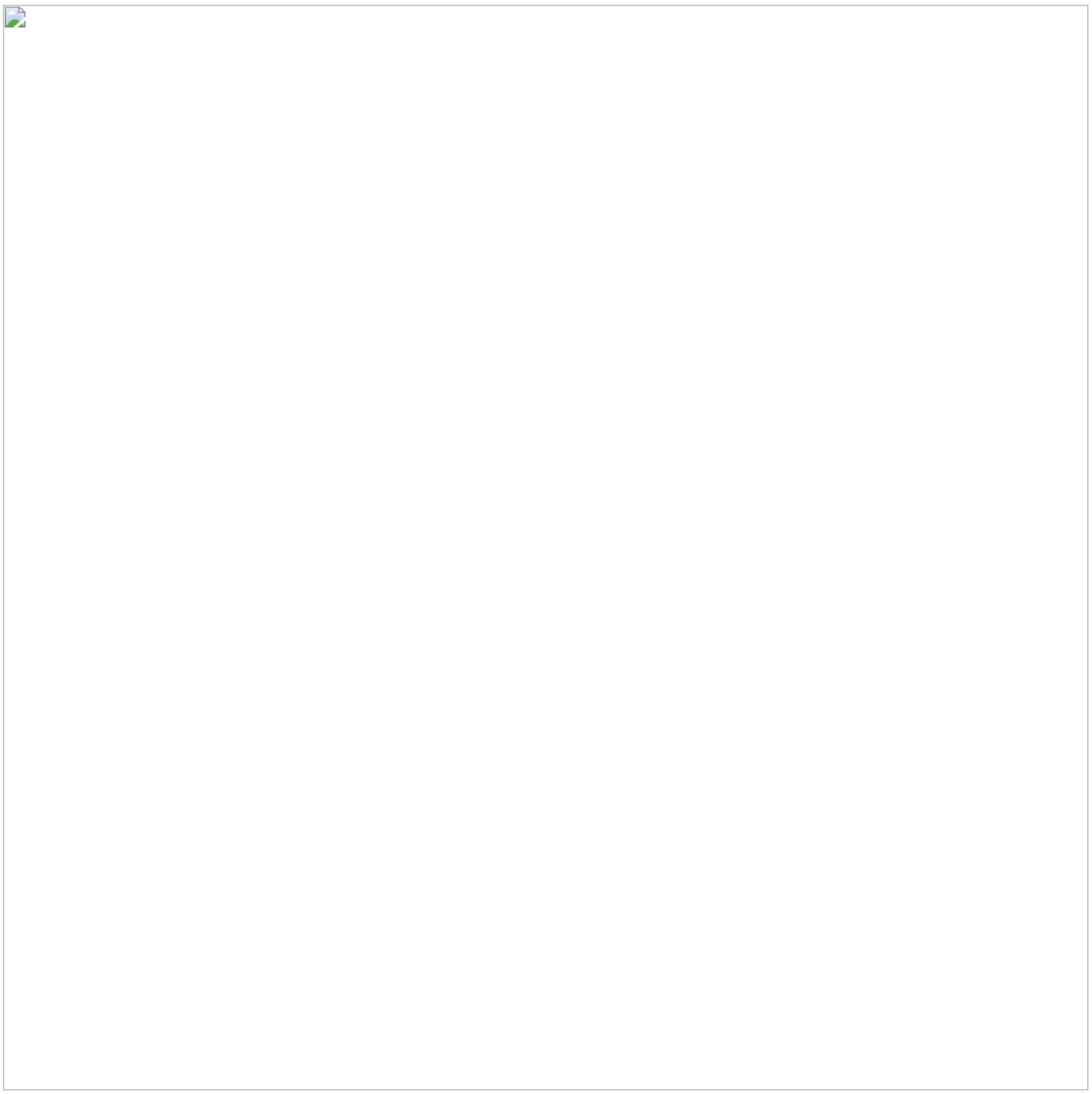


Figure 7: *Block of code responsible for terminating a list of hardcoded services.*

The complete list of services is presented below.

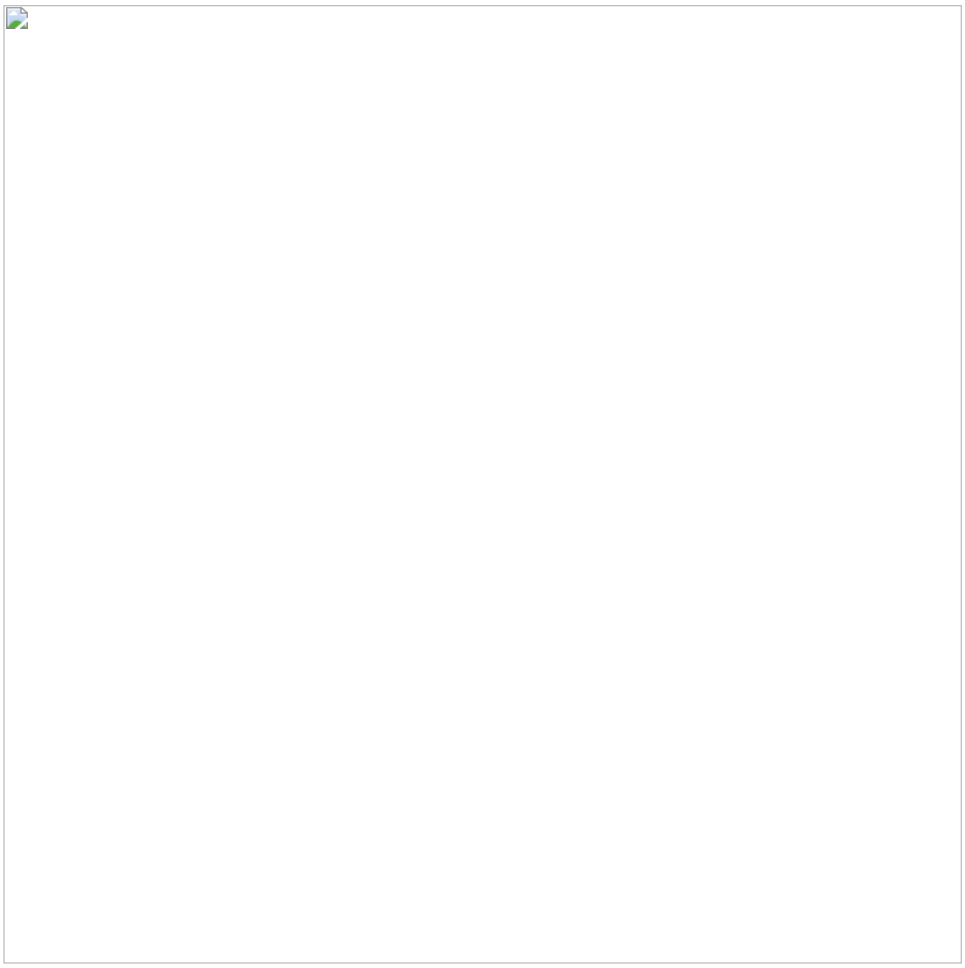


Figure 8: *List of processes terminated during the Rook execution.*

Some specific folders can’t be encrypted and damaged during the ransomware execution, or the entire operating system breaks. A list of target folders and files is also coded in a wide char array by Rook operators, as observed in Figure 9.

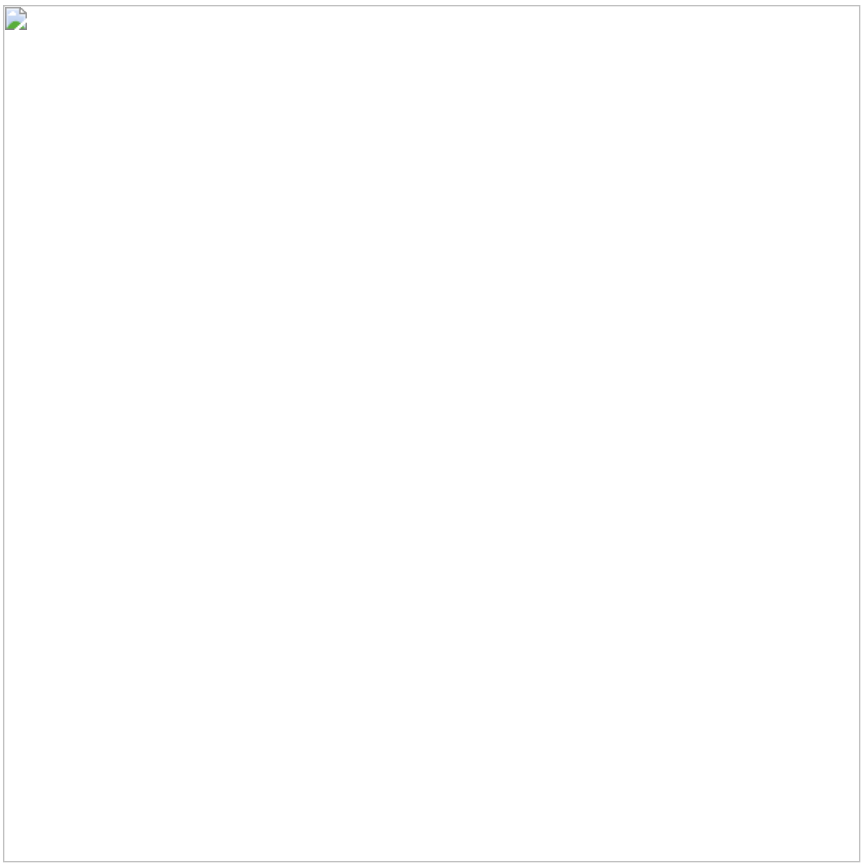


Figure 9: *List of folders and specific files skipped during the Rook execution.*

Ransomware note and encrypted files

A file called “HowToRestoreYourFiles.txt” is dropped during the ransomware execution with the instructions (ransomware note) to follow to recover the damaged files.

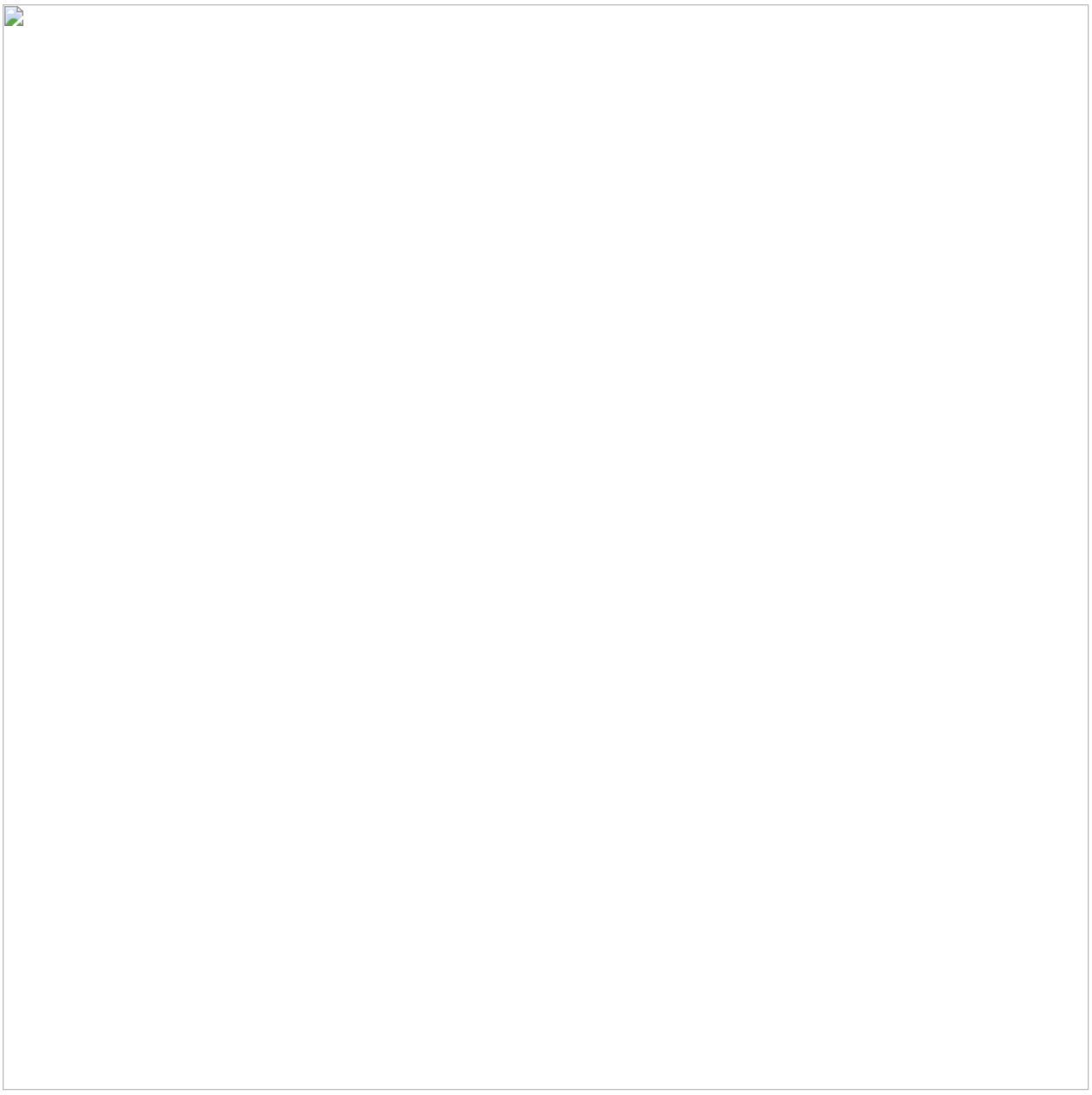


Figure 10: *Ranonsware note created during the ransomware execution.*

In addition, the extension ".rook" is also appended to the damaged files.

Rook – darkweb website

As observed with other ransomware threats, initially, a demand for payment to decrypt the damaged files is suggested. If the victims don't pay the ransom, the Rook operators leak the exfiltration data by parts in an extended extorsion schema. This type of extortion scheme creates tension and fear, forcing the victims to pay the ransom for the data.

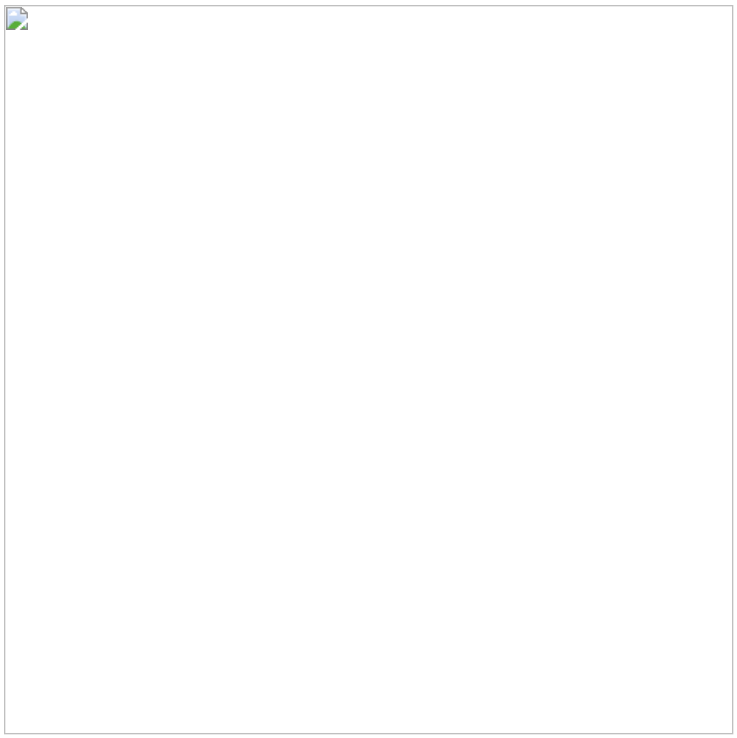


Figure 11: *Rook website available on the Tor network.*

Learning about rook ransomware

Rook ransomware is a recent threat within the malware landscape. It is based on the babuk leaked code and tunned into a powerful weapon that can encrypt a target machine in minutes due to its multi-threading mechanism. Although there is no perfect formula to stop ransomware infections, the implementation of monitoring and the usage of endpoint security solutions, updated antivirus, and the increasing use of canary files are some of the mechanisms that could prevent the dissemination of these threats in the wild.

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.