Liam Clement

12/2/2022

CS462

For many people, a significant source of stress when it comes to daily life in the computer age is the constant worry about one's data, their privacy, their identity. We often worry about the potential of an outside actor using who we are and what we do against us. For those of us that are exceptionally security conscious, we cope with our worries by refusing to give the figurative keys to the kingdom to others as much as possible. Unfortunately, we also worry about having access to goods and services, ones we cannot produce ourselves, and thus we must sometimes accept that we must open ourselves up to others and grant them the privilege to these keys. And unfortunately, sometimes when we extend trust, those that we extend our trust to fail to keep that trust. In August of this year, a major natural gas distributor in the Hellenic Republic known as DESFA reported it had suffered an incredibly significant cyberattack that had resulted in a leak of information to a hacker group. During their incident response, DEFSA attempted to mitigate damage and reduce the size of the leak by deactivating a significant portion of their online services in hopes damage would be minimized during their recovery from the incident. (Arghire)

In the wake of this attack, DEFSA revealed that they had been contacted by Ragnar Locker, with demands of ransom in return for not releasing customer data. DEFSA refused communications or payment, citing a refusal to cooperate or communicate with cyber criminals. (TRUTA) Two weeks later, the Boston based cybersecurity technology company Cybereason released a Threat Analysis Report from their Global Security Operations Center regarding Ragnar Locker's tool of choice, the attack, and DEFSA's response. Ragnar Locker shares its name with the malware they have developed and used against DEFSA. An analysis of the malware used against DEFSA shows that its binary shows this.

Ragnar Locker, as a software, works over the course of several stages to attack a victim machine. It specifically targets Windows machines and filesystems. While it is unknown how Ragnar Locker achieved access to DEFSA's systems, Ragnar Locker has been active in the past, and in prior attacks have targeted unsecure RDP connections for other services, before deploying their malware. After the software is inserted onto a victim machine, the process begins as "ragnarlocker.exe" executes on a drive. Immediately, "ragnarlocker.exe" begins to interact with the machine's file system through the Windows API, first checking the victim's machine to find out if it is in one of several countries using the command "GetLocaleInfoW,". The list of countries, interestingly, corresponds directly to all countries that are current or former members of the Commonwealth of Independent States, the successor union to the Soviet Union. If the victim machine is in any of the countries and ragnarlocker.exe detects it, the process is immediately terminated. If this process does not find the machine to be in any of the countries it is prohibited from attacking, it then runs the commands "GetComputerNameW" and "GetUserNameW" to begin to extract info about the infected machine. Following this, it begins to use commands such as "RegOpenKeyExW" to search the machine's registry for information on the version of Windows that is currently being used, along with Globally Unique Identifiers (GUIDs). All this information is coalesced into a chain of data that is hashed with a proprietary function, obfuscating it. Ragnarlocker.exe then uses the hashes of all the information as a name for a newly created Event Object, an object in the Windows operating system used to coordinate and synchronize actions that access resources within the OS. (Microsoft)

Next, the malware uses the command “CreateFileW” to access a physical drive, before searching for all memory volumes on the drive. Here, ragnarlocker.exe extracts a hidden payload within its binary code sections. This payload is encrypted via RC4, and ragnarlocker.exe decrypts it over the course of several executions. The decrypted data is a list of several process names, such as “vss,” “sql,” “Hyper-V,” and several more. These processes are all associated with functions of Windows machines that are important to allowing quick recoveries and prevention of data-loss, such as the creation of “Shadow Copies” and “Snapshots,” (Microsoft) or hardware virtualization. (Microsoft) When these processes are detected, ragnarlocker.exe forcibly terminates them. Finally, ragnarlocker.exe begins to decrypt an RSA public key from its binary, before passing it to another process. Next, ragnarlocker decrypts a text-file from its binary, before opening 2 Windows processes. The 2 executables delete any Shadow Copy files from the system that a victim may use to attempt recovery. Using the information used to identify the machine and its user that had been hashed earlier, ragnarlocker edits the text-file to be customized to each victim and their machine.

Finally, ragnarlocker.exe begins its final stage. First, ragnarlocker searches for all drives and directories, searching for specific files that are either important to the Windows boot process or related to certain web browsers, as well as all files with certain extensions. All files that do not meet the criteria are then passed to another function, where a Salsa20 algorithm encrypts each file, before ragnarlocker adds a custom identifier to the now-encrypted files’ filenames. Finally, ragnarlocker opens the Windows Notepad text-file editor, using it to display the customized ransom note to the victim. (Salem and Castel)

The attack by Ragnar Locker disabled some, but not all systems that DEFSA had been using, but according to an announcement from the company, did not impact their ability to continue to supply natural gas to their customers. During their incident response, DEFSA actively disabled some of their systems to prevent Ragnar Locker from being able to draw any further data from their infrastructure and prevent the spread of any malware. (Toulas) In addition, Ragnar Locker published the data that they had stolen from DEFSA, including some confidential data regarding business operations, as well as some designs for their products, although this is likely not the direct result of Ragnar Locker's ransomware, and more a result of their infiltration of DEFSA's IT network. (Radiflow)

When breaches like this occur, it is often the result of poorly configured machines allowing an exploit, such as a port known to be usable as an attack surface, to be exposed. Often, a breach may also be the result of a failure by the victim organization to properly ensure that they do not grant an attacker an exploit that had once previously been prevented from having exposure. Finally, data-loss such as that caused by Ragnar Locker's ransomware could have been prevented with better data preservation techniques. Ultimately, preventing these attacks all comes down to the victim organization and their attentiveness, and how they go about implementing techniques such as offsite backups, 2-factor authentication, and properly configuring machines and networks to prevent known exploits.

Works Cited

Arghire, Ionut. *Ransomware Gang Leaks Data Allegedly Stolen From Greek Gas Supplier*. 23 August 2022. News column. 1 December 2022.

Microsoft. *Event Objects (Synchronization)*. 29 June 2021. Document. 2 December 2022.

—. *Introduction to Hyper-V on Windows 10*. 25 April 2022. Document. 2 December 2022.

—. *Volume Shadow Copy Service*. 29 2022 August. Document. 2 December 2022.

Radiflow. *Behind the News: The Ragnar Locker Attack on Greek Natural Gas Supplier DESFA*. 30 August 2022. News article. 2 December 2022.

Salem, Eli and Loïc Castel. *THREAT ANALYSIS REPORT: Ragnar Locker Ransomware Targeting the Energy Sector*. 1 September 2022. Blog. 1 December 2022.

Toulas, Bill. *Greek natural gas operator suffers ransomware-related data breach.* 22 August 2022. News Article. 2 December 2022.

TRUTA, Filip. *Greek Natural Gas Supplier DESFA Hacked by Ragnar Locker Ransomware Crew*. 23 August 2022. News article. 2 December 2022.