WastedLocker malware analysis

seguranca-informatica.pt/wastedlocker-malware-analysis/

January 25, 2022

Introduction

WastedLocker is the name of a data encryption malware, also called ransomware, which will be analyzed in this article. Systems infected with this piece of malware are encrypted and a message, typically inside an HTML or TXT file, is dropped with the ransom details.

The WastedLocker ransomware has been a hot topic in 2020, with several organizations seeing their data damaged and encrypted by criminals. Ransomware attacks are a big threat to companies: their data is encrypted and the ransom price does not guarantee that criminals will return what they stole.

The tech giant Garmin is an example of an organization that was affected by the WastedLocker threat, back in June of 2020.

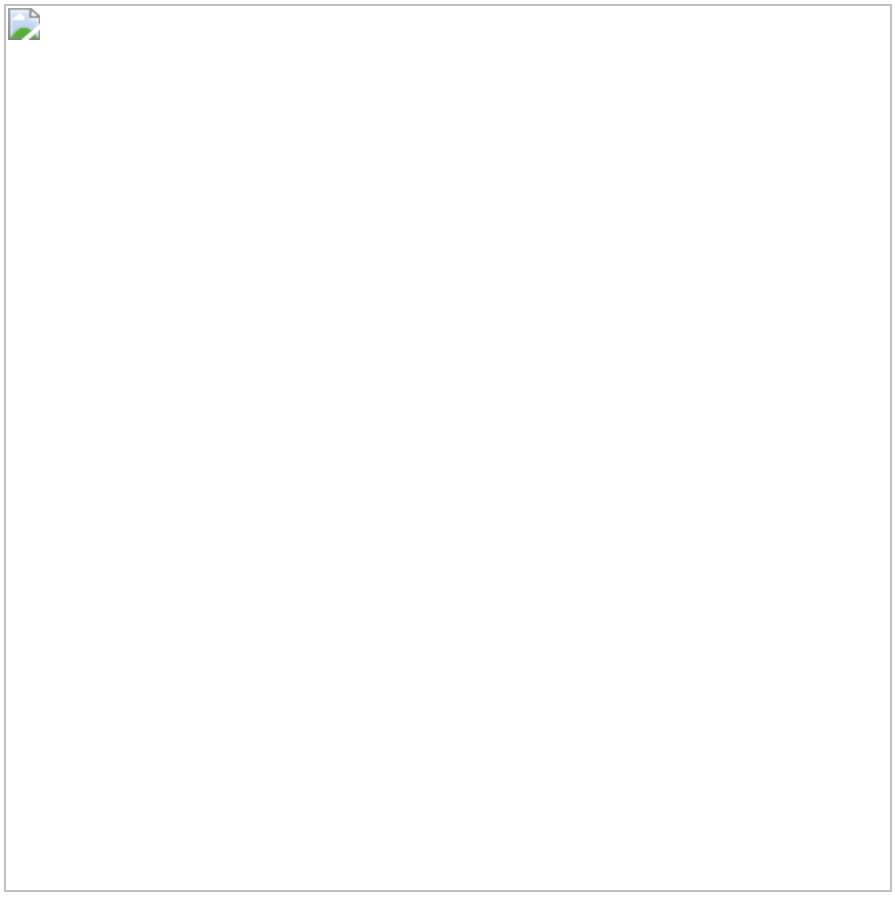

Figure 1: *Message from Garmin confirming the outage as a result of a ransomware attack (WastedLocker).*

The Garmin Connect service was down, but the cyberattack also caused damage to technical services and in the support of their navigation applications. As a mitigation activity, all the employees were asked to shut down any computer that had access to their systems. In the Garmin incident, criminals requested $10 million for the release of the stolen data.

How WastedLocker works

WastedLocker is ransomware operated by a criminal group known as the Evil Corp gang — the same organization associated with Dridex and BitPaymer. This malware is very different from BitPaymer, however. They only share the characteristic of adding specific modules for different scopes and destinations.

The attacks carried out using WastedLocker are highly targeted. It is suspected that during a first penetration attempt, an assessment of active defenses is made and the next attempt is specifically designed to bypass active security software and other perimeter protections. Figure 2, from PaloAlto, is a high-level diagram of how this threat is proliferated through the infrastructure.

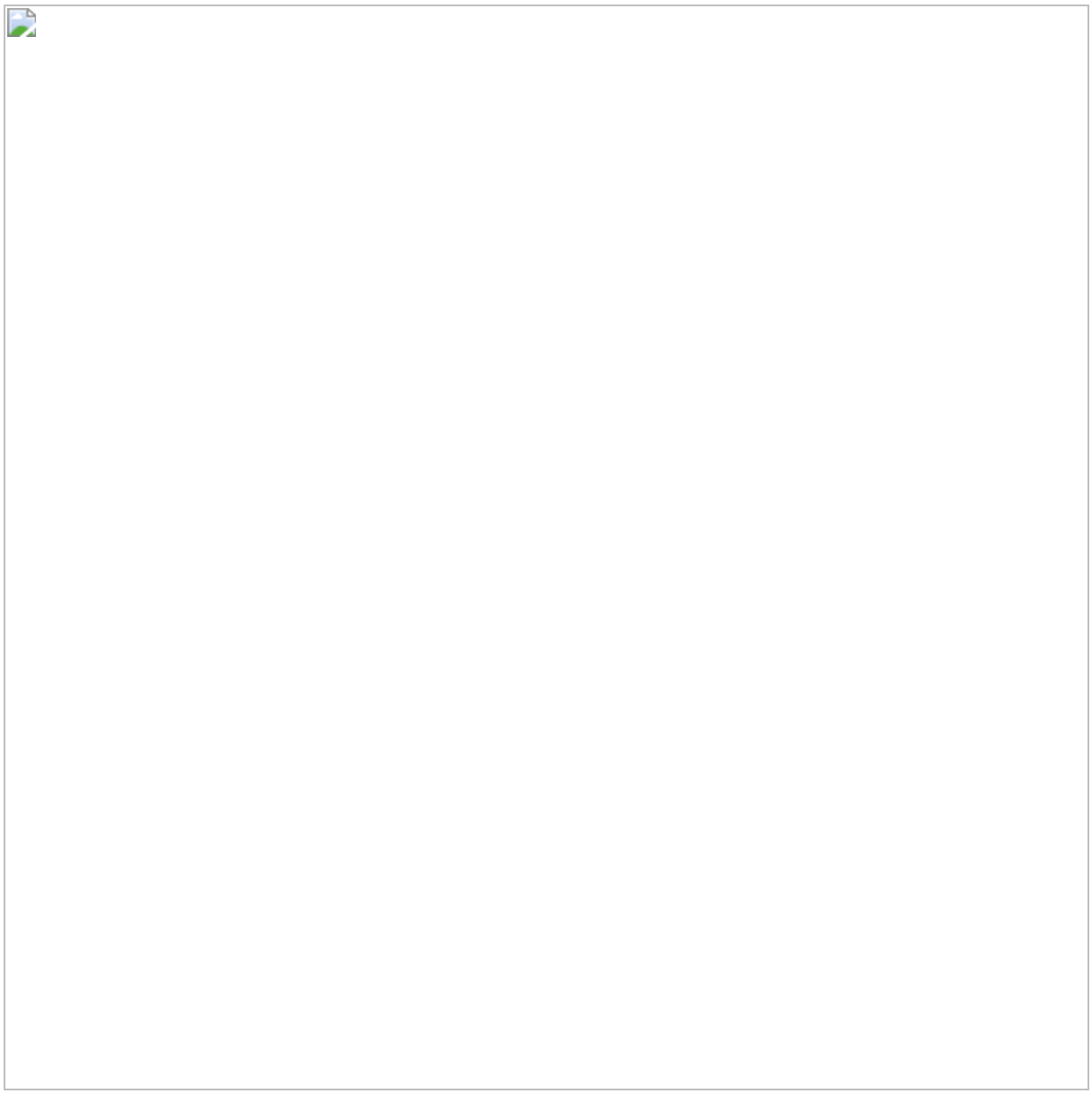

***Figure 2**: WastedLocker killchain.*

According to Figure 2, the most common path used by criminals are ZIP files — the decoy file — containing SocGholish JavaScript framework loader components that profile the victim system and use PowerShell to ultimately deploy Cobalt Strike payloads.

When the Cobalt Strike payload is installed on the victim's side, it is used to perform a lateral movement from the victim's machine through the network. With this approach in place, criminals can identify additional systems and deploy new payloads enlarging the initial footprint.

The group behind this malware has also been observed using legitimate Windows utilities (LOL Bins) such as Windows Management Instrumentation (WMI) and PsExec.

As observed on other groups and ransomware such as **Netwalker** and **Ragnar_Locker**, high-value targets are particularly affected by criminals. These include high-use and high-visibility internal systems and systems that contain backups — in order to prevent easy data restoration.

When the target system is affected, the damaged files are renamed during the encryption process and include an abbreviation of the name of the target organization with the “wasted” string at the end (e.g., GARMINWASTED).

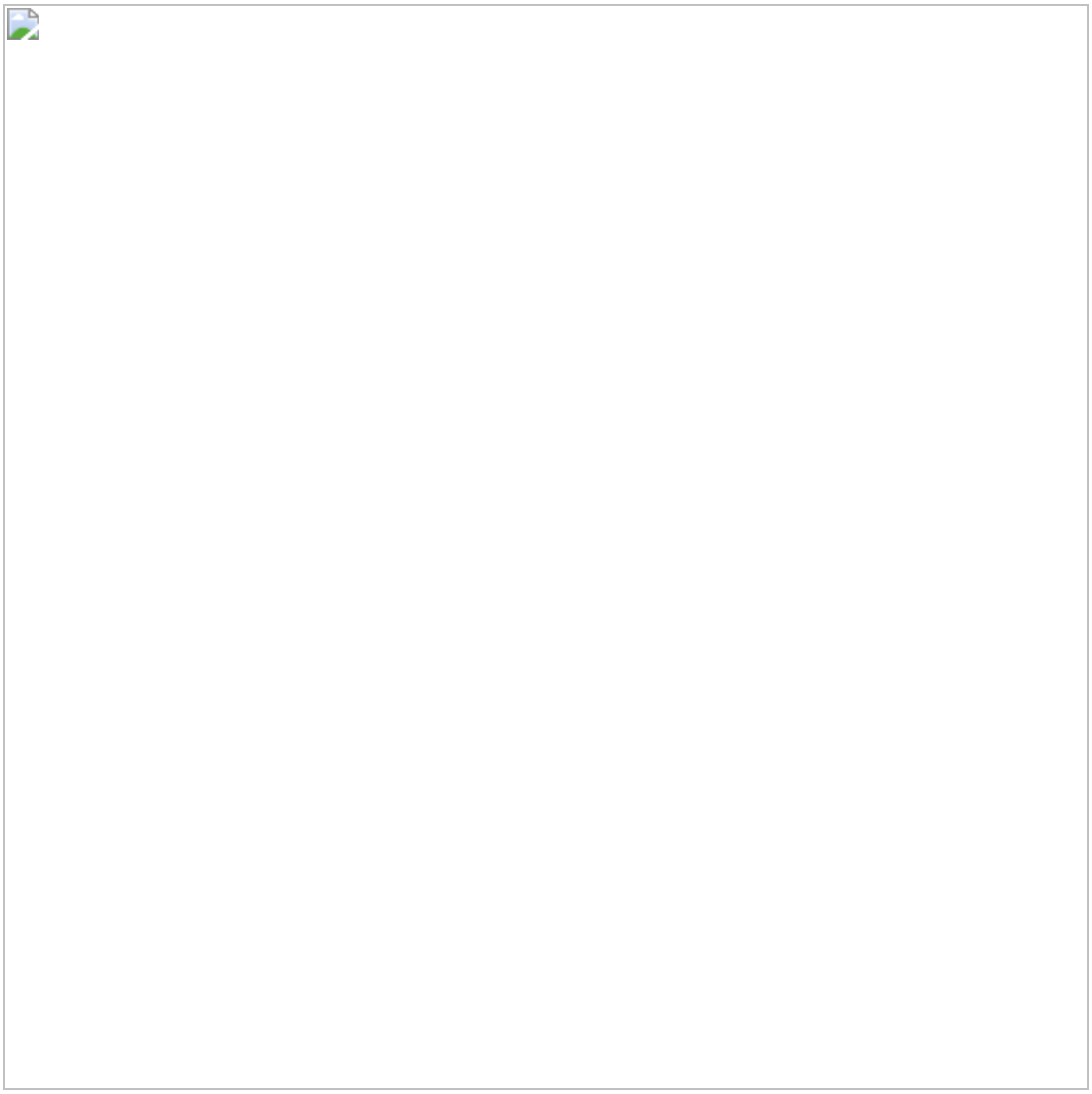

Figure 3: *Sample of damage data from Garmin.*

For each encrypted file, an additional file is dropped containing the ransomware note. The ransom note has the same name as the file associated with the addition of “**_info**”.

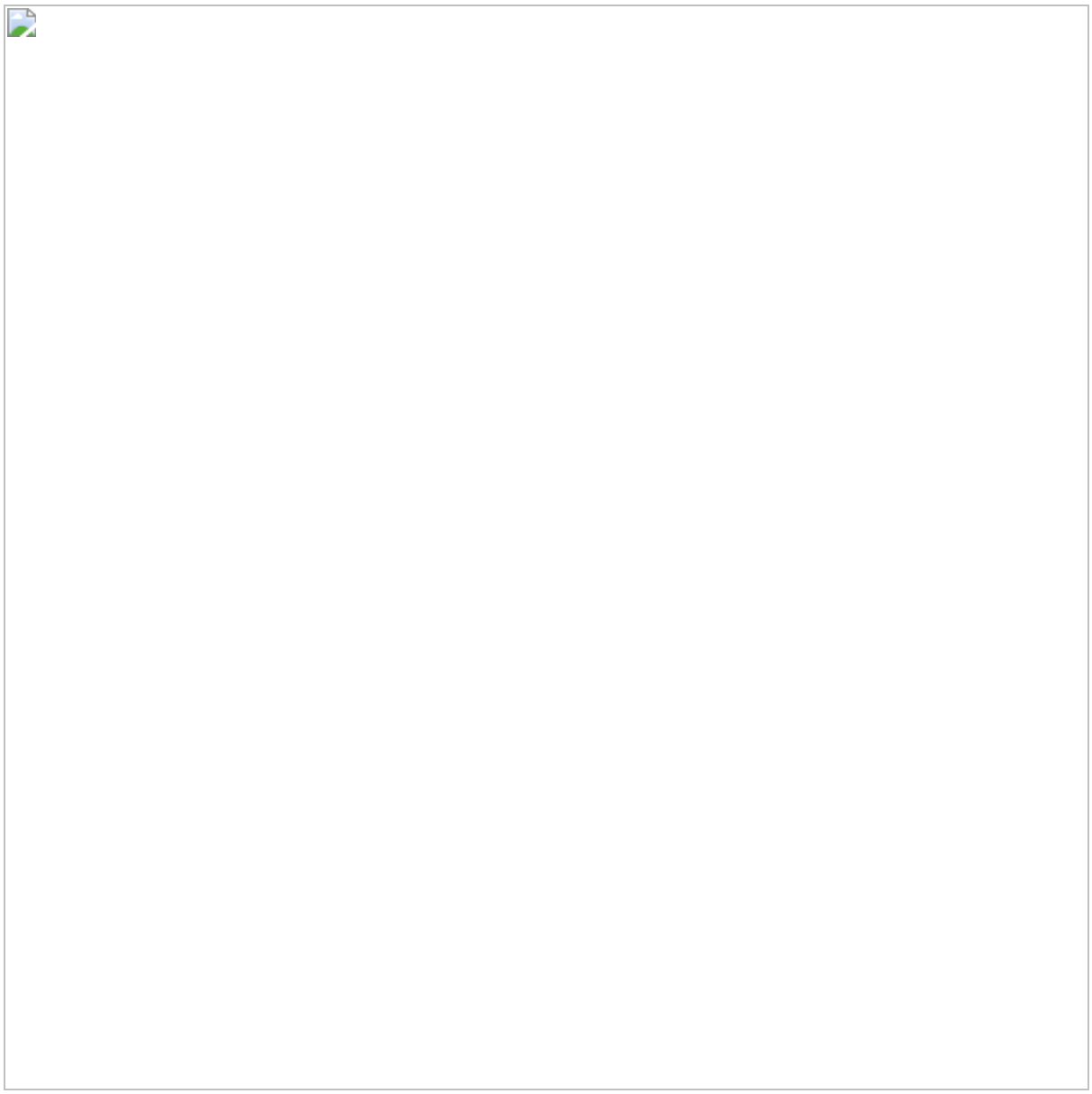

Figure 4: *Ransom note file — WastedLocker ransomware.*

Redemption requests are exorbitant, ranging from $500,000 to more than $10 million in Bitcoin.

During the malicious process, the malware tries to delete Volume Shadow copies with basic VSSADMIN commands:

```
vssadmin.exe Delete Shadows /All /Quiet
```

For now, victims' sensitive data is not shared online, as is in the case of other malware families. However, preventive measures are needed to contain this threat.

How to protect against WastedLocker attacks

Ransomware attacks are a trend in this digital era. The general recommendations for guarding against them are fairly standard:

- Keep software up to date, especially the operating systems and AV engines. Many malware types exploit public vulnerabilities
- Add a backup solution in two forms: offline and online
- Maintain the email over alert: Many different types of attacks arrive via email and a simple spam folder could provide protection against ransomware
- Use a VPN connection to protect the infrastructure, namely remote access to RDP services
- Use monitoring security solutions with anti-ransomware technologies
- And finally, but not least, promote employees' training in the basics of cybersecurity. Notice that several threats start via social engineering attacks through email

Conclusion

WastedLocker is one of the highly-aggressive ransomware families in operation in 2020. This ransomware follows the steps of other malware beasts such as REvil, **Netwalker**, and **Ragnar Locker**, and prevention is absolutely critical in this field.

Detecting and stopping criminals before they gain traction in some way is essential to protect assets and sensitive data. This last point will be true if the group behind WastedLocker decides to leak de victim's data.

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.