AXLocker, Octocrypt, and Alice: Leading a new wave of Ransomware Campaigns

blog.cyble.com/2022/11/18/axlocker-octocrypt-and-alice-leading-a-new-wave-of-ransomware-campaigns/

November 18, 2022

AXLocker Ransomware Stealing Victim's Discord Tokens

Ransomware is one of the most critical cybersecurity problems on the internet and possibly the most powerful form of cybercrime plaguing organizations today. It has rapidly become one of the most important and profitable malware families among Threat Actors (TAs). In a typical scenario, the ransomware infection starts with the TA gaining access to the target system. Depending on the type of ransomware, it can infect the entire operating system or encrypts individual files. The TAs will then typically demand payment from the victim for the decryption of their files.

While organizations are protecting themselves from ransomware attacks, new ransomware groups are also emerging proportionally every year. New ransomware groups are evolving by expanding the scope of their operations for financial gain. Multiple new ransomware groups have emerged recently, highlighting the widespread adoption of ransomware attacks by TAs for monetary growth.

Cyble Research and Intelligence Labs (CRIL) came across three new ransomware families: AXLocker, Octocrypt, and Alice Ransomware.

AXLocker Ransomware

Ransomware operators now have one newer tool, named AXLocker, which can encrypt several file types and make them completely unusable. Additionally, the ransomware steals Discord tokens from the victim's machine and sends them to the server. Later, a ransom note is displayed on the victim's system to get the decryption tool used for recovering the encrypted files.

Technical Analysis

We have taken the following sample hash for our analysis: (SHA256), *c8e3c547e22ae37f9eeb37a1efd28de2bae0bfae67ce3798da9592f8579d433c,* which is a 32-bit GUI-based .NET binary executable targeting Windows operating systems as shown below.

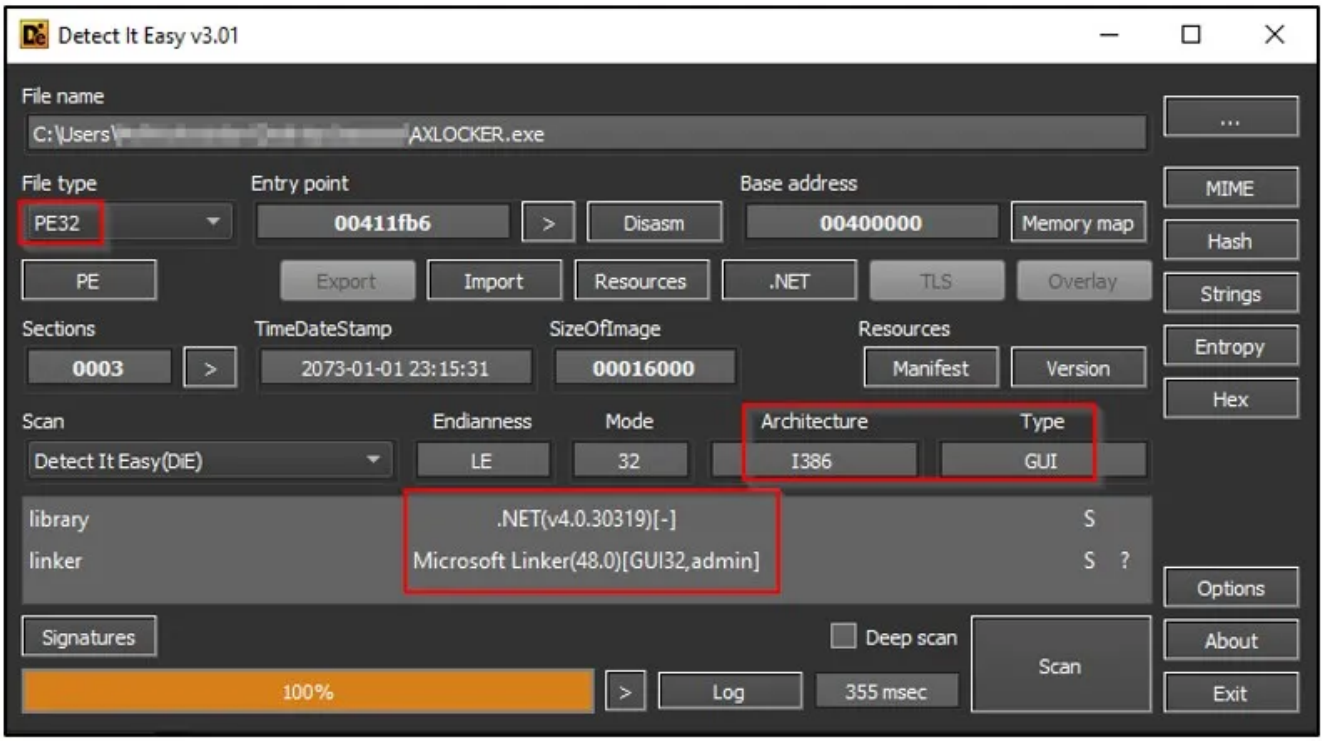

Figure 1 – Static file details of AXLocker ransomware

Upon execution, the ransomware hides itself by modifying the file attributes and calls the *startencryption()* function to encrypt files, as shown below.

```
// Token: 0x06000016 RID: 22 RVA: 0x000034B3 File Offset: 0x000016B3
[STAThread]
private static void Main()
{
    Program.hidefile();
    Program.startencryption();
    Program.show();
}
```

Figure 2 – AXLocker main function

The *startencryption()* function contains code to search files by enumerating the available directories in the C:\ drive. It looks for specific file extensions to encrypt and excludes a list of directories from the encryption process, as shown in the figure below.

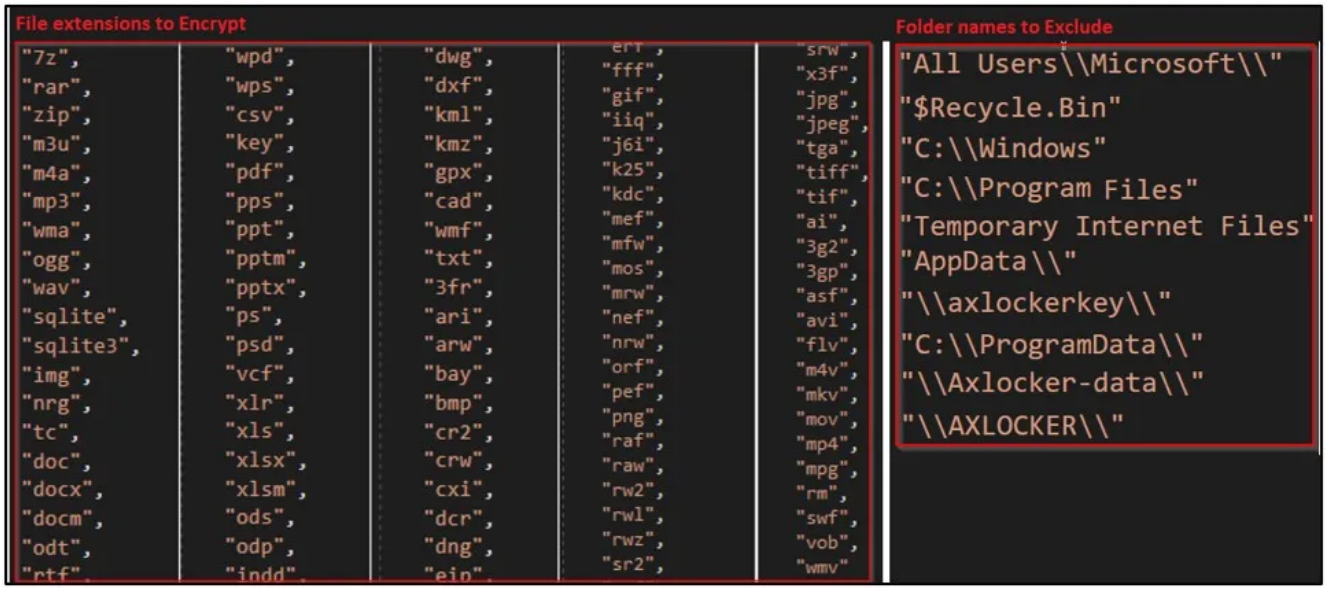

Figure 3 – File extension to encrypt and directories to exclude from encryption

After that, the ransomware calls the *ProcessFile* function, which further executes an *EncryptFile* function with the *fileName* as an argument to encrypt the victim's system files.

This ransomware uses the AES encryption algorithm to encrypt files. The figure below shows a ransomware code snippet searching and encrypting the victim's files.

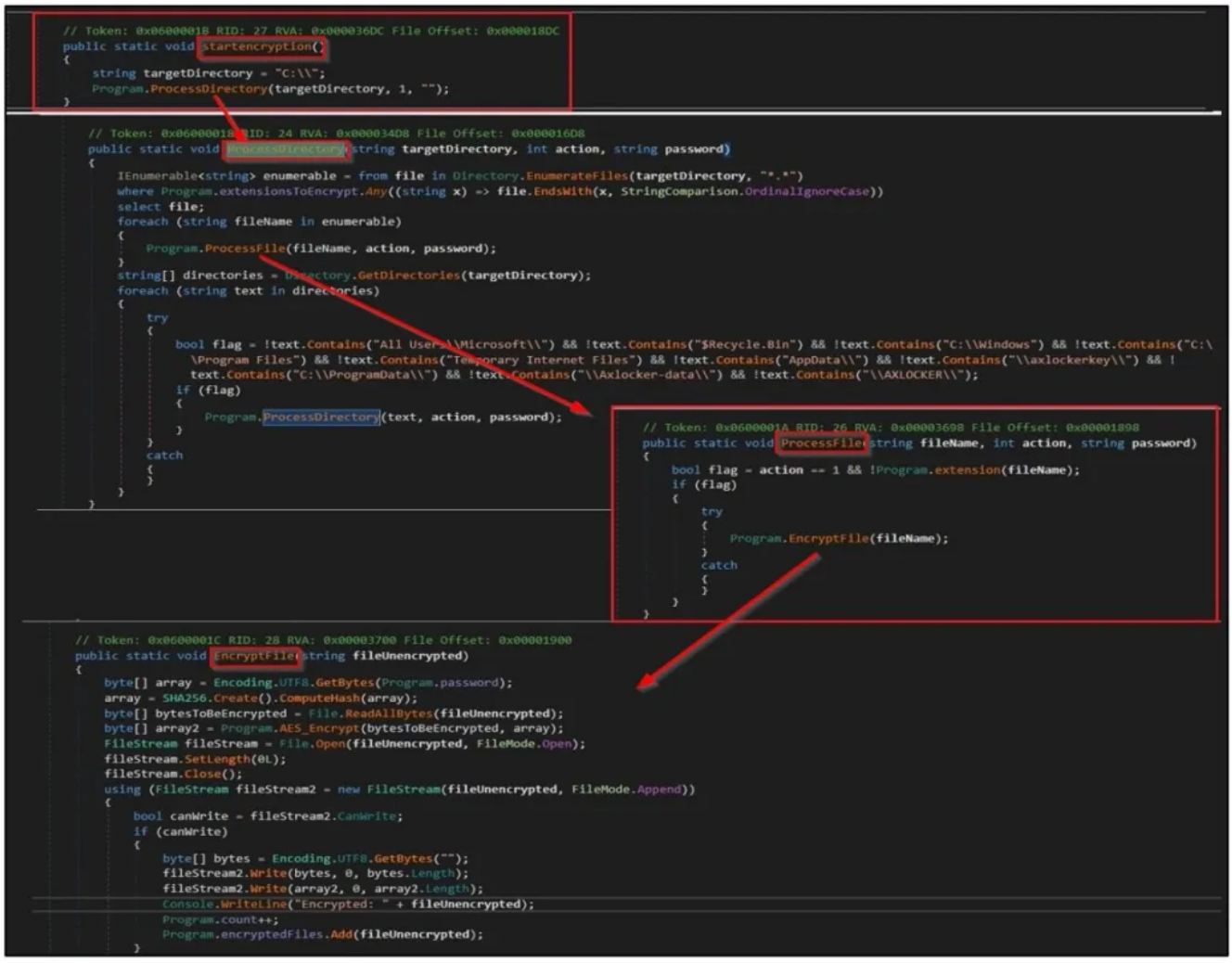

Figure 4 – AXLocker ransomware searching and encrypting files

The image below shows the code snippet of the encryption function and the original/infected file content before and after encryption.

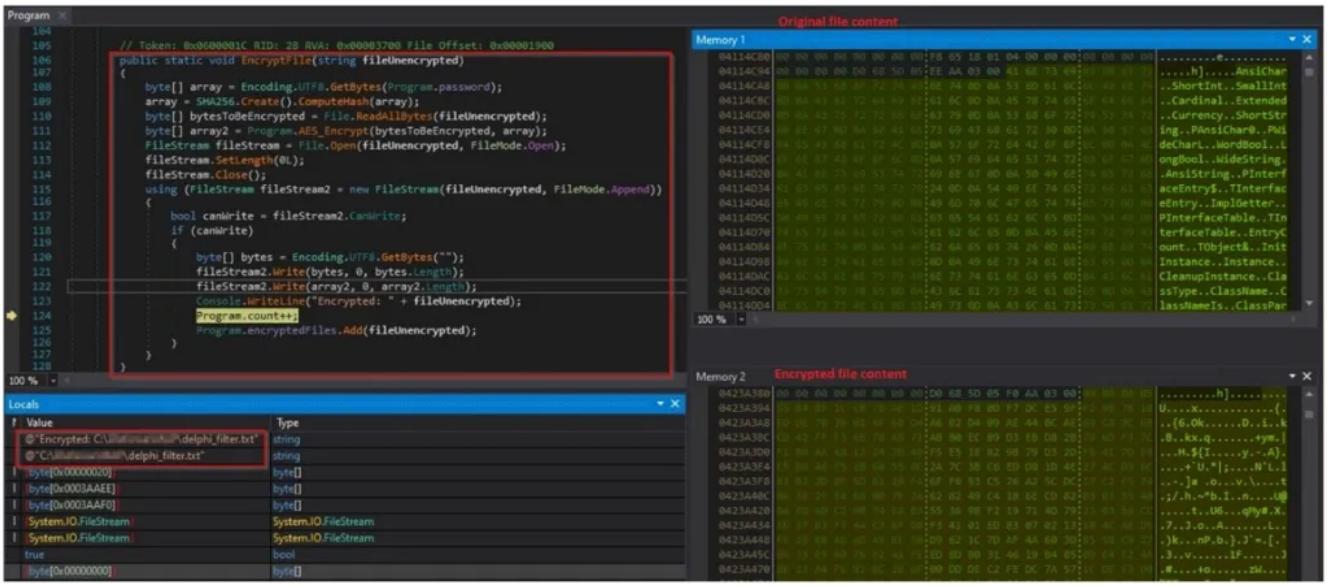

Figure 5 – Encryption function and the original/encrypted file content

We observed that the ransomware does not change the file name or extension after the encryption. The image below shows the encrypted file of the ransomware after the successful infection on the victim's machine.

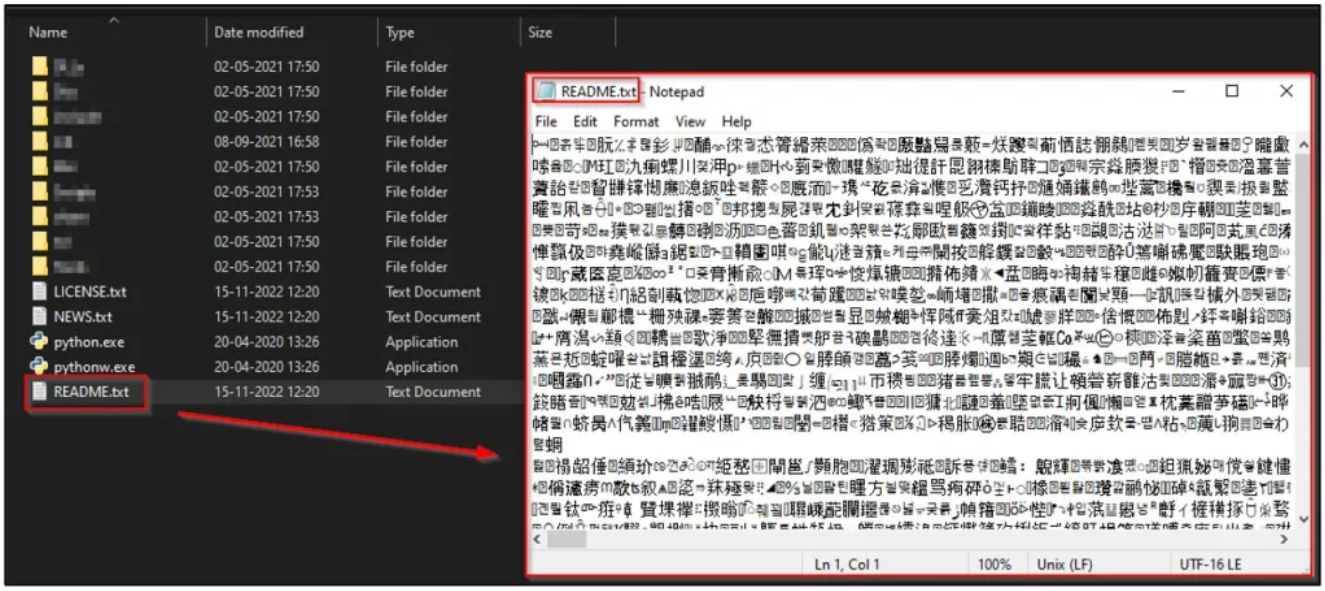

Figure 6 – Encrypted file by AXLocker ransomware

After encrypting the victim's files, the ransomware collects and sends sensitive information such as Computer name, Username, Machine IP address, System UUID, and Discord tokens to TA, as shown in the below figure.

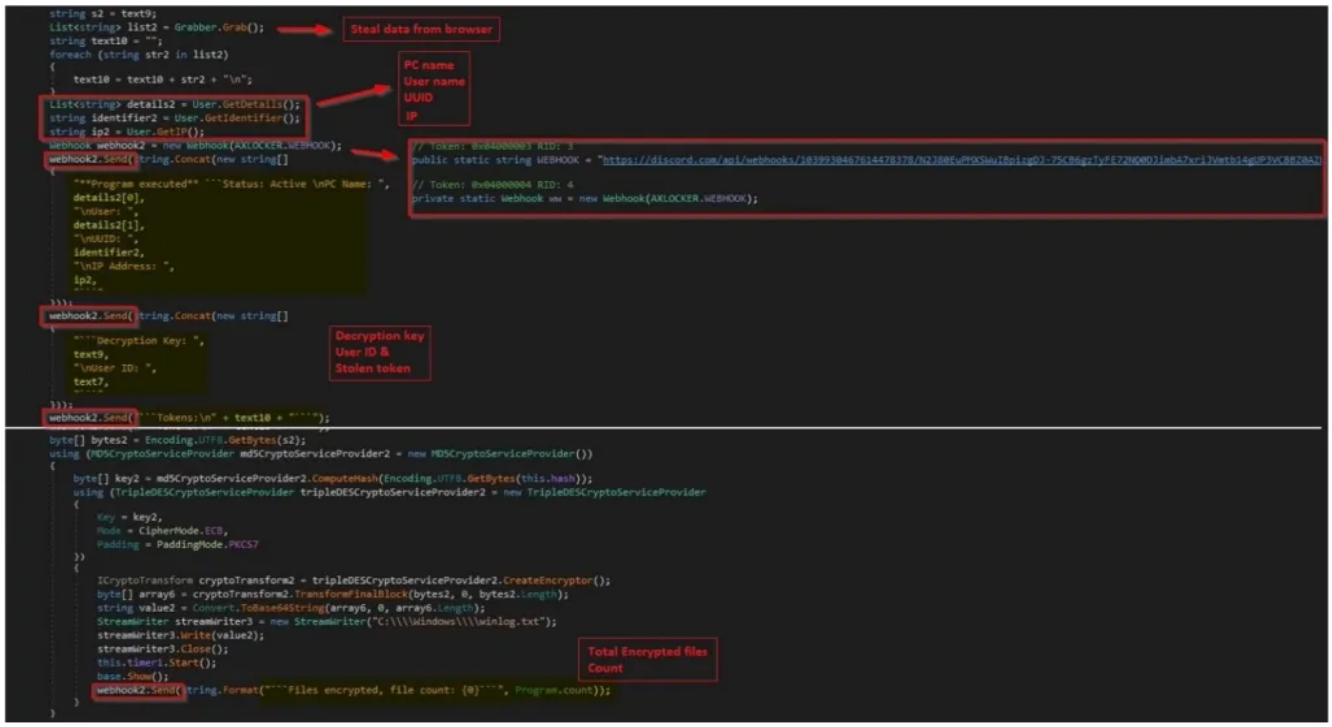

Figure 7 – Exfiltrate victim stolen details

For stealing Discord tokens, the malware targets the following directories:

- *Discord\Local Storage\leveldb*
- *discordcanary\Local Storage\leveldb*
- *discordptb\leveldb*

- *Opera Software\Opera Stable\Local Storage\leveldb*
- *Google\Chrome\User Data\\Default\Local Storage\leveldb*
- *BraveSoftware\Brave-Browser\User Data\Default\Local Storage\leveldb*
- *Yandex\YandexBrowser\User Data\Default\Local Storage\leveldb*

It uses *regex* to find the Discord tokens in the local storage files and saves them in the list, then sends them to the Discord server along with other information using the below URL:

> *hxxps://discord[.]com/api/webhooks/1039930467614478378/N2J80EuPMXSWuIBpizgDJ-75[Redacted]DJimbA7xriJVmtb14gUP3VCBBZ0AZR*

```
private static void Scan()
{
    string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
    string folderPath2 = Environment.GetFolderPath(Environment.SpecialFolder.LocalApplicationData);
    Grabber.target.Add(folderPath + "\\Discord");
    Grabber.target.Add(folderPath + "\\discordcanary");
    Grabber.target.Add(folderPath + "\\discordptb");
    Grabber.target.Add(folderPath + "\\\\Opera Software\\Opera Stable");
    Grabber.target.Add(folderPath2 + "\\Google\\Chrome\\User Data\\Default");
    Grabber.target.Add(folderPath2 + "\\BraveSoftware\\Brave-Browser\\User Data\\Default");
    Grabber.target.Add(folderPath2 + "\\Yandex\\YandexBrowser\\User Data\\Default");
}

// Token: 0x06000002 RID: 2 RVA: 0x00002108 File Offset: 0x00000308
public static List<string> Grab()
{
    Grabber.Scan();
    List<string> list = new List<string>();
    foreach (string text in Grabber.target)
    {
        bool flag = Directory.Exists(text);
        if (flag)
        {
            string path = text + "\\Local Storage\\leveldb";
            DirectoryInfo directoryInfo = new DirectoryInfo(path);
            foreach (FileInfo fileInfo in directoryInfo.GetFiles("*.ldb"))
            {
                string input = fileInfo.OpenText().ReadToEnd();
                foreach (object obj in Regex.Matches(input, "[\\w-]{24}\\.[\\w-]{6}\\.[\\w-]{27}"))
                {
                    Match match = (Match)obj;
                    list.Add(match.Value);
                }
                foreach (object obj2 in Regex.Matches(input, "mfa\\.[\\w-]{84}"))
                {
                    Match match2 = (Match)obj2;
                    list.Add(match2.Value);
                }
            }
        }
    }
    return list;
}
```

Regex to match

Figure 8 – Grab function to Steal Discord tokens

Finally, the AXLocker ransomware shows a pop-up window that contains a ransom note that gives instructions to victims on contacting the TAs to restore their encrypted files, as shown below.

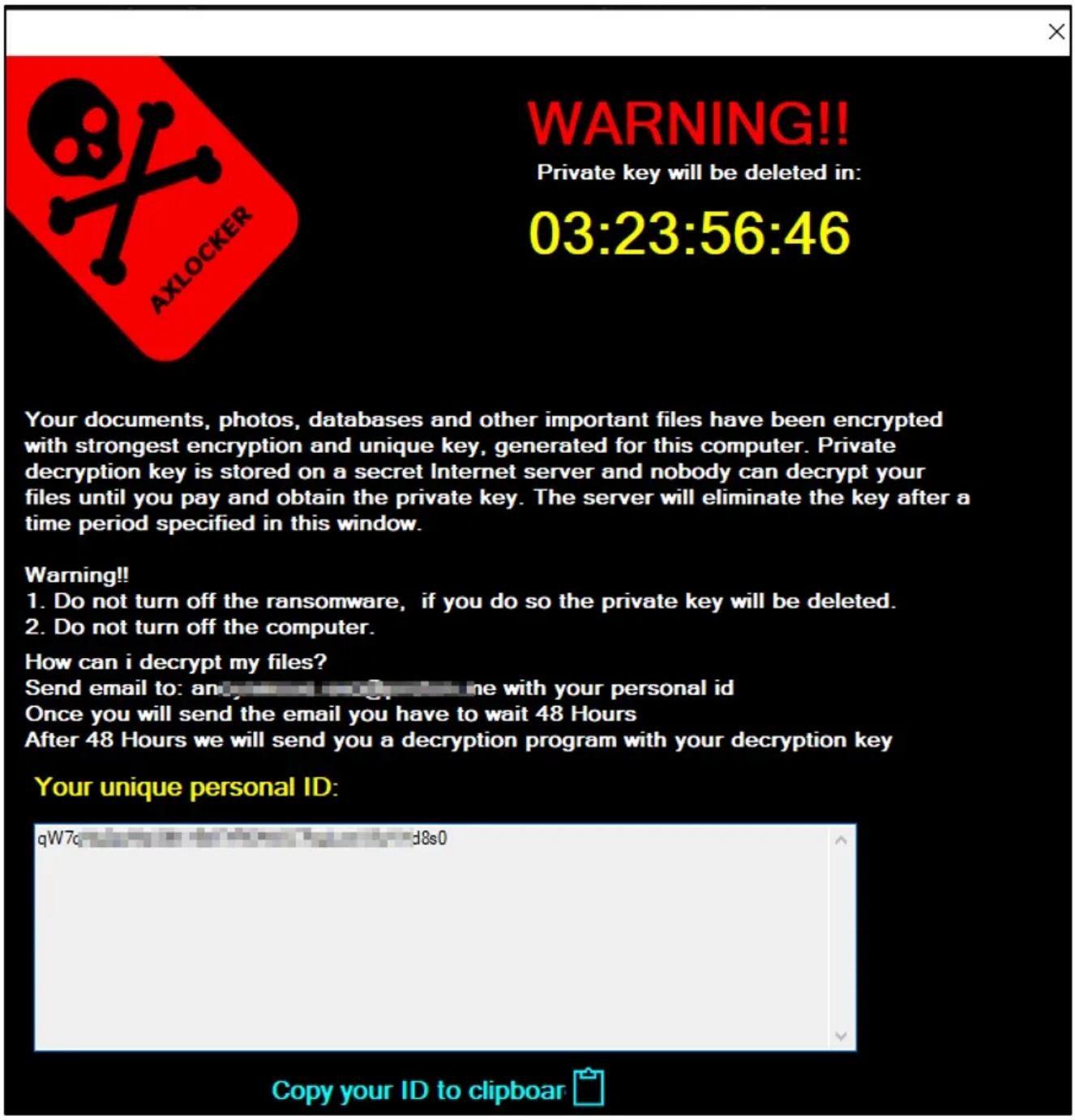

Figure 9 – AXLocker ransom note window

Octocrypt Ransomware

Octocrypt is a new ransomware strain that targets all Windows versions. The ransomware builder, encryptor, and decryptor are written in *Golang*. The TAs behind Octocrypt operate under the Ransomware-as-a-Service (RaaS) business model and surfaced on cybercrime forums around October 2022 for USD400.

The Octocrypt ransomware has a simple web interface for building the encryptor and decryptor, and the web panel also displays the infected victim's details.

The below figure shows a post made by the Octocrypt Ransomware Developer on a cybercrime forum

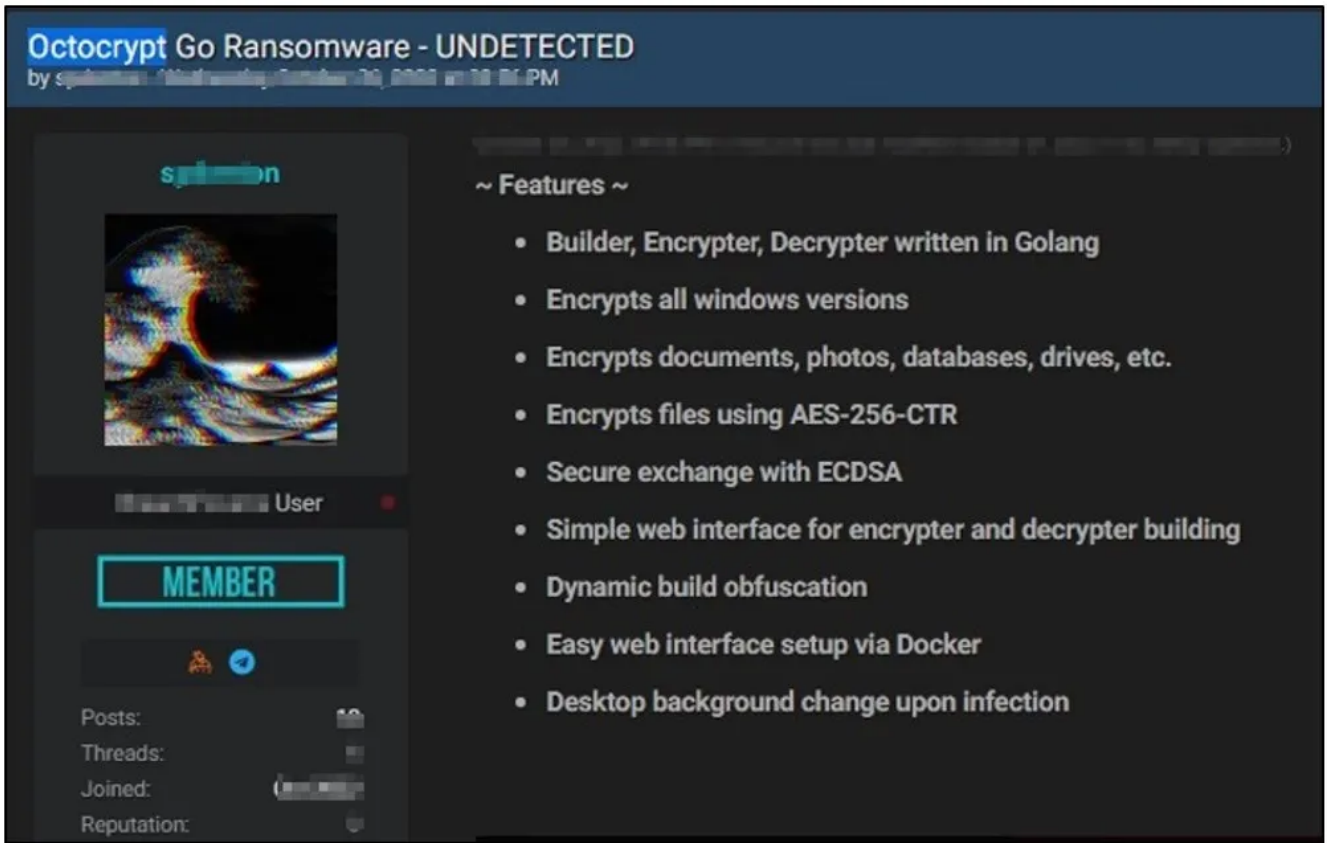

Figure 10 – Post Made by the Octocrypt developer on Cybercrime Forum

Ransomware Builder: Octocrypt

The Octocrypt web panel builder interface allows TAs to generate ransomware binary executables by entering options such as API URL, Crypto address, Crypto amount, and Contact email address.

TAs can download the generated payload file by clicking the URL provided in the web panel under payload details. The below figure shows the payload options to build the ransomware executable and generated URL to download the file.

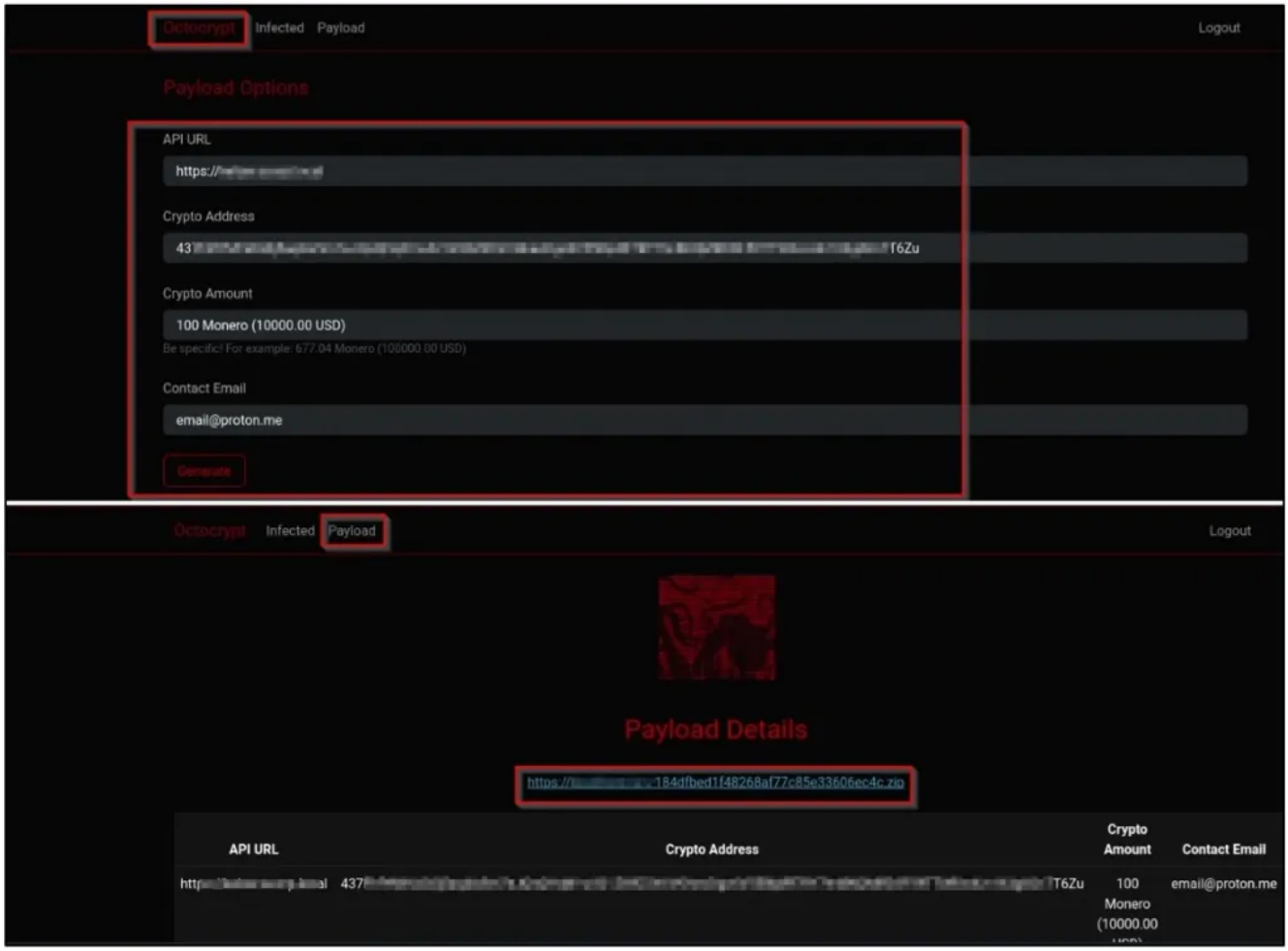

Figure 11 – Octocrypt builder and payload URL

Technical Details

The sample hash (SHA256), *9a557b61005dded36d92a2f4dafdfe9da66506ed8e2af1c851db57d8914c4344,* was taken for this analysis.

Based on static analysis, we found that the ransomware is a console-based 64-bit GoLang binary executable. Upon execution, the ransomware initially ensures the system's internet connection and then checks the TCP connection to access the API URL, as shown below.

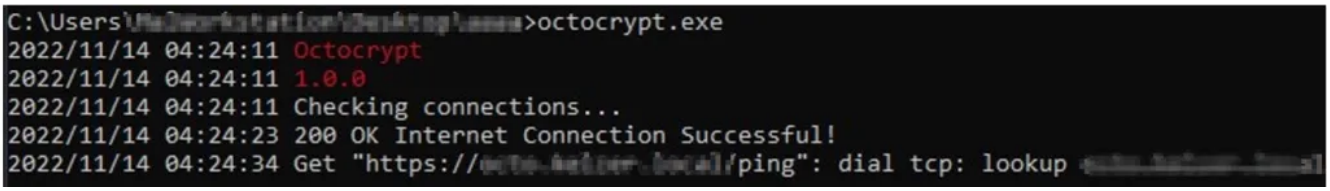

Figure 12 – Checking system internet and TCP connection

After that, the malware starts the encryption process by enumerating the directories and encrypts the victim's files using the AES-256-CTR algorithm, appending the extension as "*.octo"*.

Then, the ransomware drops the ransom note in multiple folders with the file name "*INSTRUCTIONS.html*". Finally, the ransomware changes the victim's wallpaper which displays a message that threatens the victim to send a ransom amount to a specific Monero wallet address, as

shown below.

Figure 13 – Octocrypt changing desktop background

Alice Ransowmare

One more new ransomware dubbed “Alice” also appeared on cybercrime forums under the TAs project of “Alice in the Land of Malware”. The Alice ransomware also works under the Ransomware-as-a-Service (RaaS) business model. The Indicators of Compromise of this ransomware strain are unavailable in the wild.

The figure below shows TA’s advertisements on a cybercrime forum.

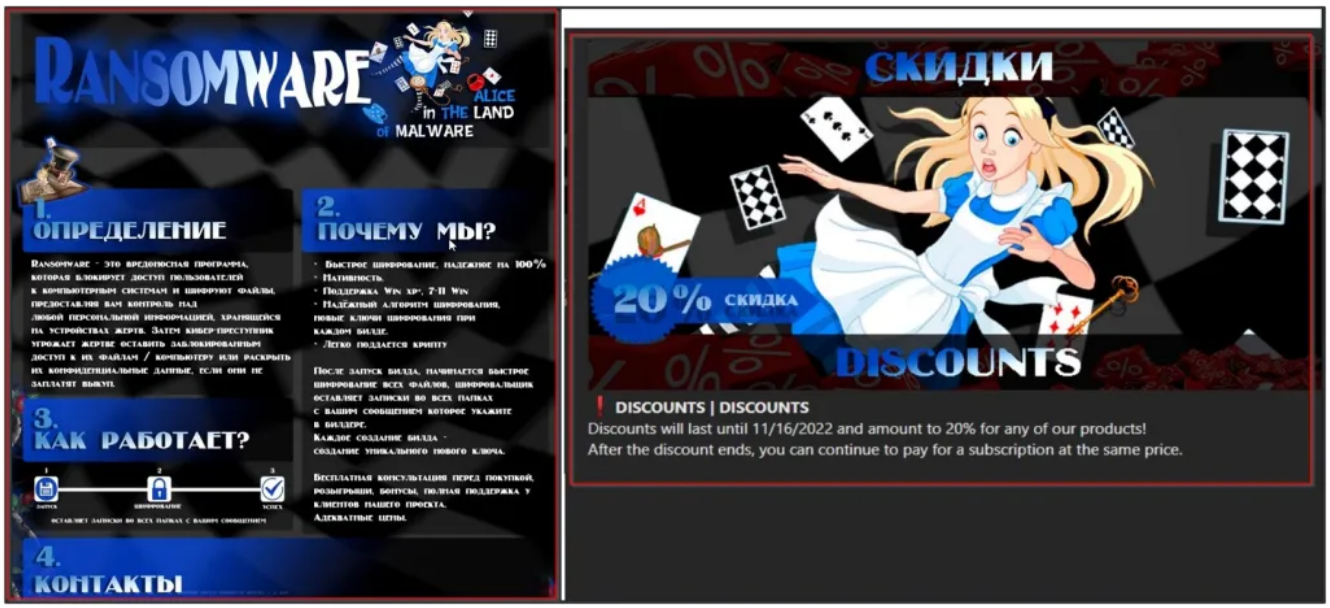

Figure 14 – Alice ransomware post shared by TA on a Cybercrime Forum
The TA sells this Alice ransomware builder for the prices listed below:

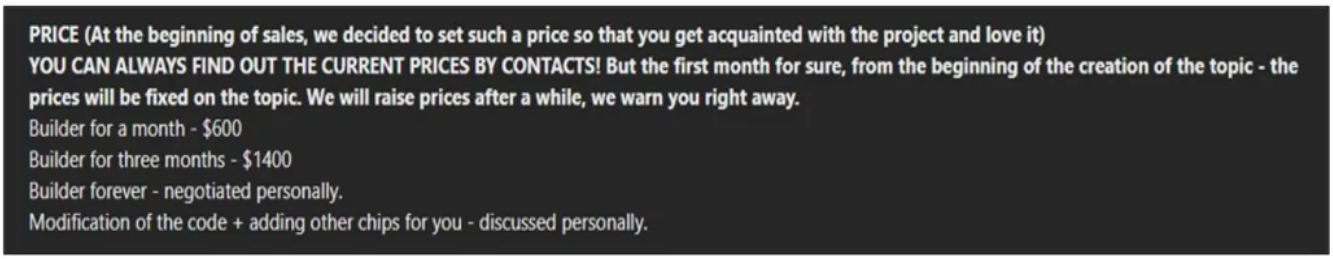

Figure 15 – Alice ransomware price details

As specified by the developer on the forum, the below figure shows the functionality and advantages of Alice ransomware.

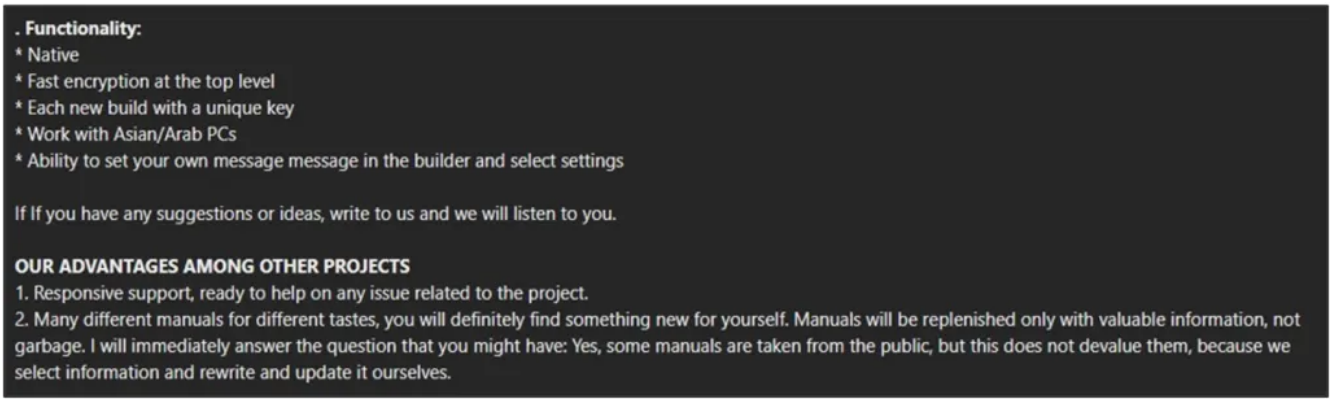

Figure 16 – Alice ransomware functionalities and advantages

Ransomware Builder: Alice

The Alice ransomware builder permits the TAs to generate ransomware binary files with a customized ransom note. After entering the ransom message and clicking the “New Build” button in the builder, it will generate two executable files named “Encryptor.exe” and “Decryptor.exe”, as shown in the figure below.

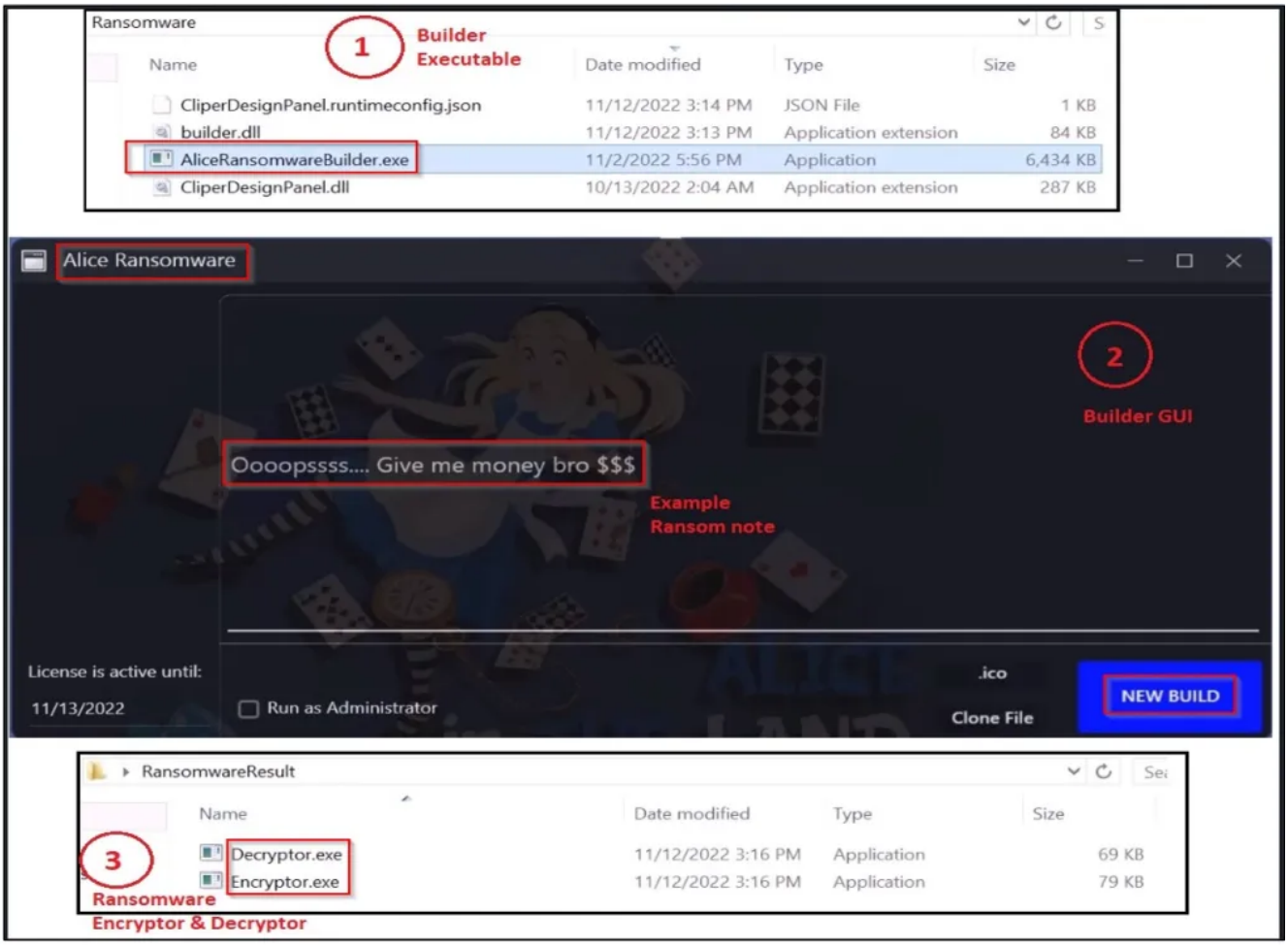

Figure 17 – Alice ransomware builder

Successful execution of Alice ransomware encrypts the victim's files and appends the extension as "*.alice*". Also, the malware drops ransom notes named "*How to Restore Your Files.txt*" in multiple folders.

The below figure shows the encrypted files and dropped ransom note by Alice ransomware.

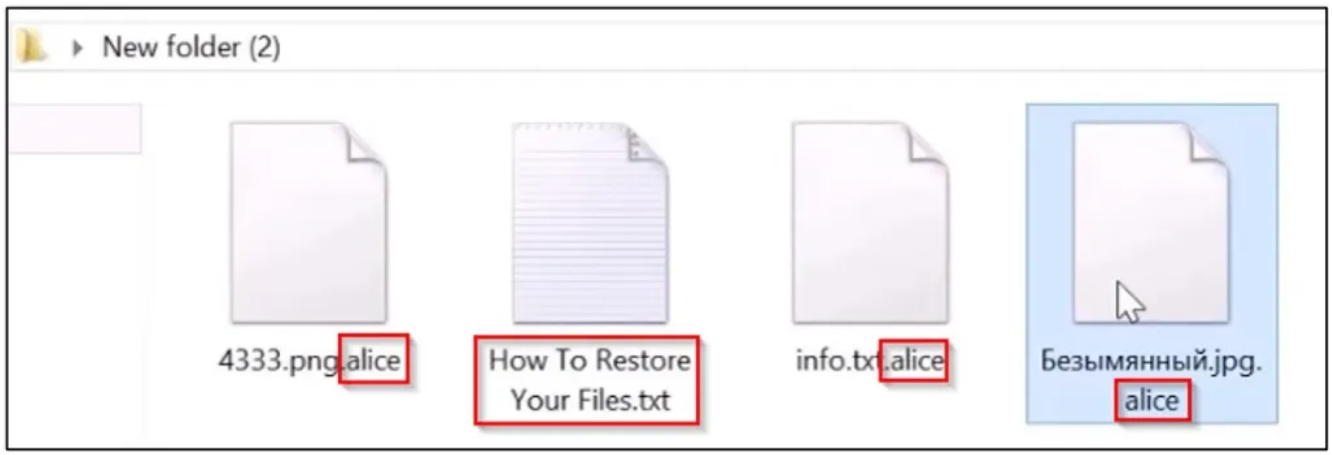

Figure 18 – Encrypted files and dropped ransom note by Alice ransomware

Conclusion

Ransomware groups continue to pose a serious risk to firms, individuals, and even entire governments, as we recently observed in the case of Costa Rica. The victims are at risk of losing valuable data as a result of such attacks, resulting in financial and productivity loss. In extreme cases, compromising government and law enforcement credentials can even result in cyberwarfare with grave implications for national security and diplomatic relations.

CRIL has also observed a considerable increase in cybercrime through Telegram channels and cybercrime forums where TAs sell their products without any regulation. TAs are increasingly attempting to maintain a low profile to avoid drawing the attention of Law Enforcement agencies. Enterprises need to stay ahead of the techniques used by TAs and implement the requisite security best practices and security controls, or they will become the victims of increasingly sophisticated and aggressive ransomware.

Regularly monitoring the dark web and acting upon early warning indicators such as compromised credentials, accesses, and identifying vulnerabilities traded on cybercrime forums can forewarn enterprises of potential threats and allows them to take corrective action based on real-time, actionable threat intel. CRIL continuously monitors new ransomware campaigns and will keep our readers updated.

Our Recommendations

We have listed some of the essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety Measures Needed to Prevent Ransomware Attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Users Should Take the Following Steps After the Ransomware Attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impact And Cruciality of Ransomware

- Loss of valuable data.
- Loss of the organization’s reputation and integrity.
- Loss of the organization’s sensitive business information.
- Disruption in organization operation.
- Financial loss.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name

Execution	T1204 T1059 T1047	User Execution Command and Scripting Interpreter Windows Management Instrumentation
Persistence	T1547.001 T1053	Registry Run Keys / Startup Folder Scheduled Task/Job
Defense Evasion	T1497	Virtualization/Sandbox Evasion
Credential Access	T1528	Steal Application Access Token
Discovery	T1087 T1082 T1083	Account Discovery System Information Discovery File and Directory Discovery
Impact	T1486	Data Encrypted for Impact
Command and Control	T1071	Application Layer Protocol
Exfiltration	T1020	Automated Exfiltration

Indicators of Compromise

Indicators	Indicator type	Description
ab2c19f4c79bc7a2527ab4df85c69559 60a692c6eaf34a042717f54dbec4372848d7a3e3 d51297c4525a9ce3127500059de3596417d031916eb9a52b737a62fb159f61e0	MD5 SHA-1 SHA256	AXLocker Ransomware executable
07563c3b4988c221314fdab4b0500d2f a5f53c9b0f7956790248607e4122db18ba2b8bd9 0225a30270e5361e410453d4fb0501eb759612f6048ad43591b559d835720224	MD5 SHA-1 SHA256	AXLocker Ransomware executable
a18ac3bfb1be7773182e1367c53ec854 c3d5c1f5ece8f0cf498d4812f981116ad7667286 c8e3c547e22ae37f9eeb37a1efd28de2bae0bfae67ce3798da9592f8579d433c	MD5 SHA-1 SHA256	AXLocker Ransomware executable
9be47a6394a32e371869298cdf4bdd56 ca349c0ddd6cda3a53ada634c3c1e1d6f494da8a 9e95fcf79fac246ebb5ded254449126b7dd9ab7c26bc3238814eafb1b61ffd7a	MD5 SHA-1 SHA256	AXLocker Ransomware executable
ad1c2d9a87ebc01fa187f2f44d9a977c 03d871509a7369f5622e9ba0e21a14a7e813536d d9793c24290599662adc4c9cba98a192207d9c5a18360f3a642bd9c07ef70d57	MD5 SHA-1 SHA256	AXLocker Ransomware executable
346e7a626d27f9119b795c889881ed3d ce25203215f689451a2abb52d24216aec153925a 9a557b61005dded36d92a2f4dafdfe9da66506ed8e2af1c851db57d8914c4344	MD5 SHA-1 SHA256	Octocrypt Ransomware executable
5a39a2c4f00c44e727c3a66e3d5948c2 07e7341b86ace9935c4f1062d41a94f3b31f9bf6 65ad38f05ec60cabdbac516d8b0e6447951a65ca698ca2046c50758c3fd0608b	MD5 SHA-1 SHA256	Octocrypt Ransomware executable

2afdbca6a8627803b377adc19ef1467d	MD5	Octocrypt
13a0ce1c3ac688c55ba3f7b57fb6c09ad0e70565	SHA-1	Ransomware
e65e3dd30f250fb1d67edaa36bde0fda7ba3f2d36f4628f77dc9c4e766ee8b32	SHA256	UPX packed executable