

# Pure Coder Sells Malware On Dark Web Forums

Published: 2022-12-27 · Archived: 2026-04-05 17:05:42 UTC

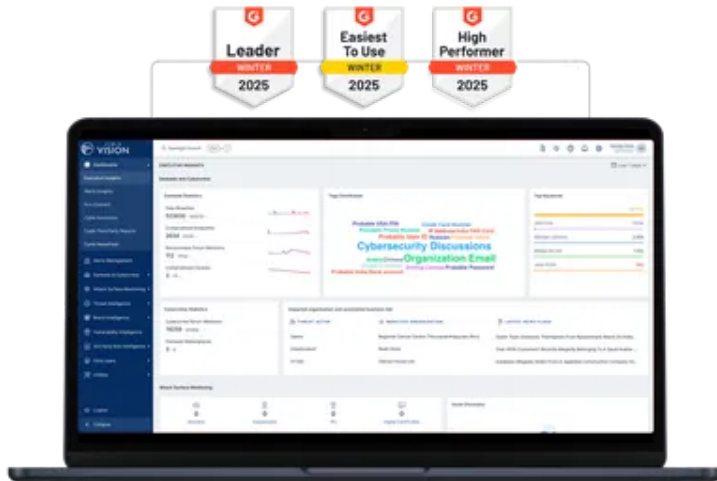
Cyble Research and Intelligence Labs analyzes a spam campaign dropping PureLogs stealer aimed at Italian users.

## Italians Users Targeted by PureLogs Stealer Through Spam Campaigns

### Executive Summary

During a routine threat-hunting exercise, Cyble Research and Intelligence Labs (CRIL) came across a [tweet](#) about PureLogs information stealer by TG Soft. This tool is used by the Threat Actor (TA) “Alibaba2044” to launch a malicious spam campaign at targets based in Italy on the 14th of December 2022.

World's Best AI-Native Threat Intelligence



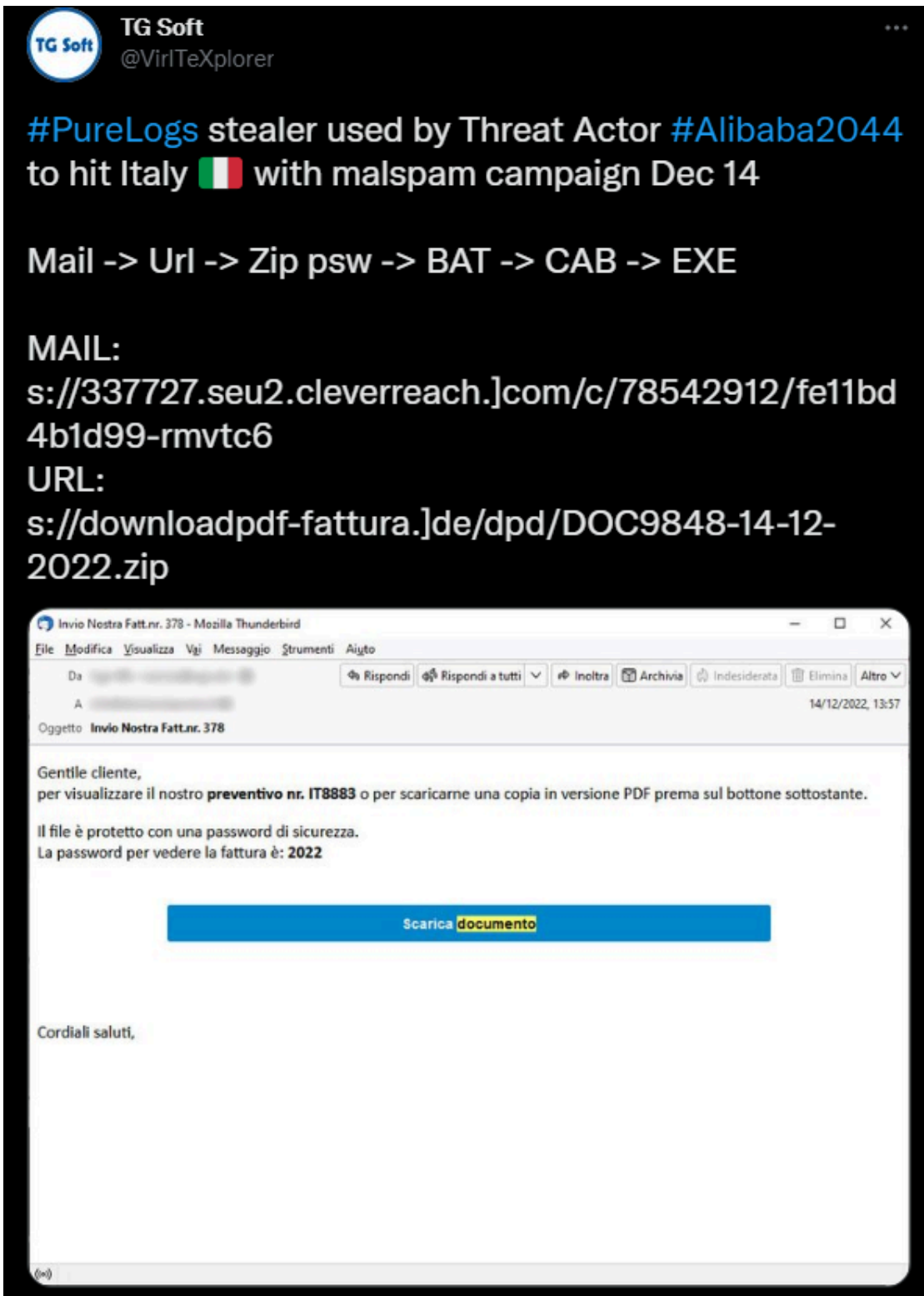


Figure 1 – Tweet Related to PureLogs Malware

The spam email includes a link to download a password-protected zip file; the password is provided in the same email. The zip file contains a cabinet file disguised as a batch file, which holds a malicious executable. Once the target opens the batch file, the [malware](#) will start running on their machine.

PureLogs stealer is developed by TA with the name PureCoder. The threat actor offers sales for multiple malicious software programs on their website for various operations, such as miners, [information stealers](#), VNC, and crypters. The

figure below shows the post by the Purecoder TA.

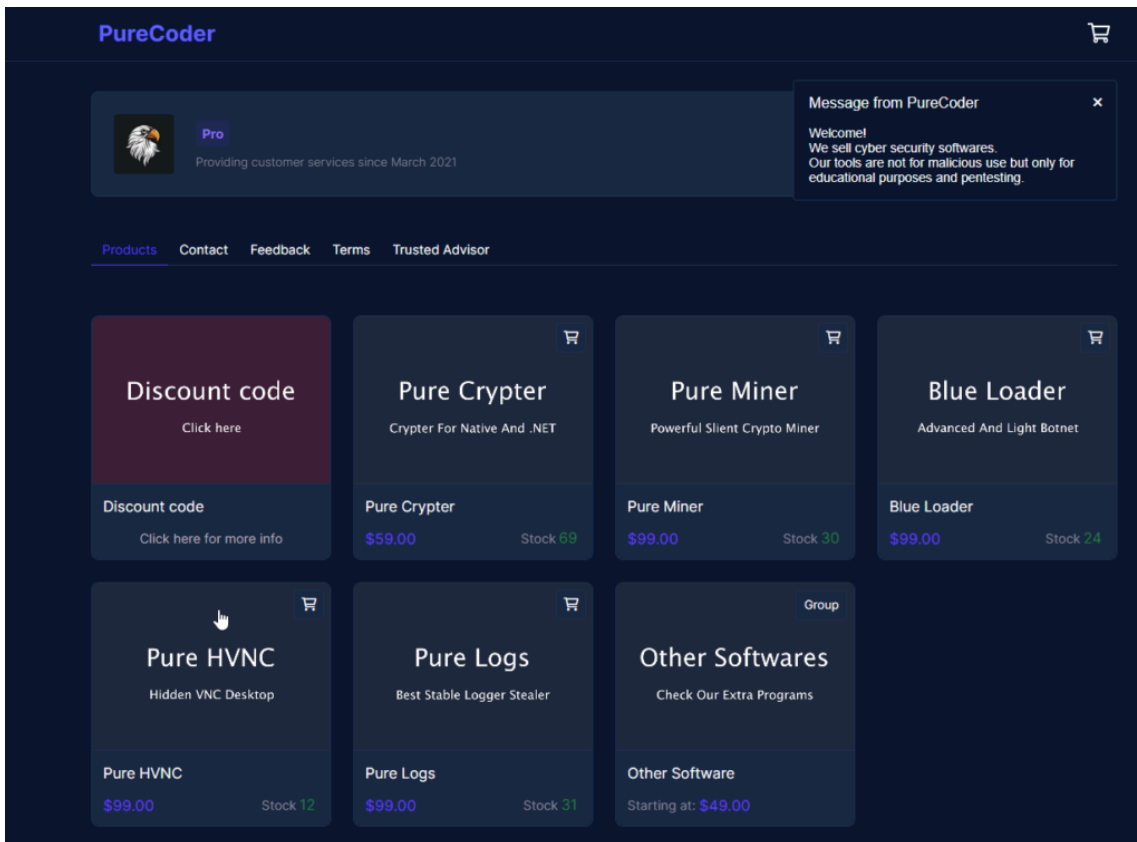


Figure 2 – Purecoder Website Selling Malicious Programs

The TAs developing this malware have also posted the tool information in the cybercrime forums to attract potential customers. The figure below shows the TA's post on a cybercrime forum.

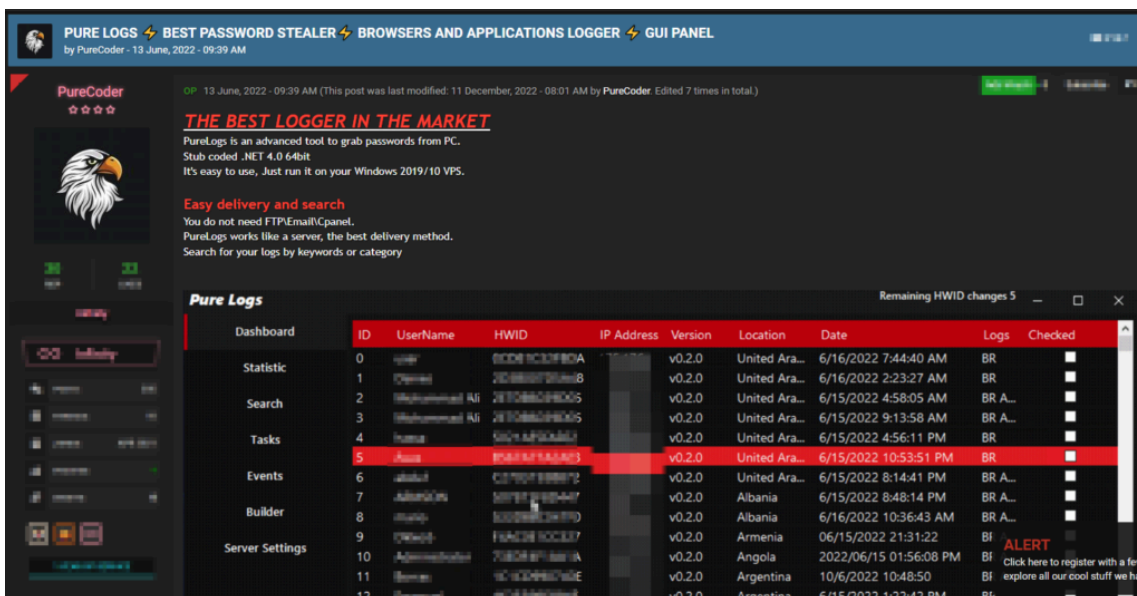
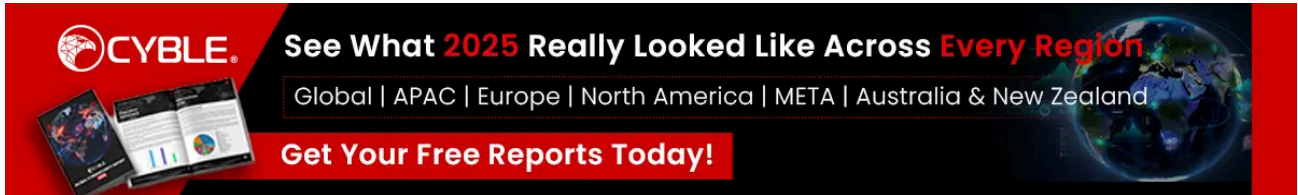


Figure 3 – Cyber Crime Forum Post by Threat Actors

PureLogs and PureCrypt are the most impactful malwares created by PureCoder. Multiple other TAs are using these malwares in their campaigns. Below, we have shared information regarding multiple malicious programs.

## PureLogs

PureLogs is a malicious .NET program that [developers sell](#) at \$99 for a one-year subscription. It is specifically designed to steal browser data, crypto wallets, and various applications such as FTP Clients, email clients, and VPNs installed on a system. The following table shows the data targeted by PureLogs.



Browsers	Crypto Wallets	Crypto Wallets
Passwords	Armory	FileZilla
Cookies	Atomic	WinSCP
History	BitcoinCore	Outlook
Autofill	DashCore	Thunderbird
Extensions*	Electrum	DiscordToken
	Ethereum	Telegram
	Exodus	Pidgin
	Jaxx	InternetDM
	LitecoinCore	Steam
	Monero	OpenVPN
	Zcash	ProtonVPN

**\*Extensions:** TronLink, MetaMask, Binance Chain Wallet, Yoroi, Coinbase Wallet, Jaxx Liberty, BitApp Wallet, iWallet, Terra Station, BitClip, EQUAL Wallet, Wombat, Cyano Wallet, Nifty Wallet, Math Wallet, Guarda, Coin98 Wallet, TezBox, Trezor Password Manager, EOS Authenticator, Authy, GAAuth Authenticator, Authenticator.

The figure below illustrates the post related to PureLogs Stealer.

Figure 4 – PureLogs Stealer Post by PureCoder

## PureCrypter

PureCrypter malware has been observed distributing multiple RATs and information stealers. It is a .NET-based executable, obfuscated with SmartAssembly, that is further protected with compression, encryption, and obfuscation to make it difficult to detect.

The malware is sold for \$59 for a one-month subscription. [Zscaler](#) has provided a deeper technical analysis of the PureCrypter in a blog. The figure below shows TA's post.

Figure 5 – PureCrypter Post by Purecoder

## PureMiner

This is a hidden stealth silent miner; an attacker can use it for bots or spread it, and it will automatically mine ETHW or BTC to TAs wallet. TAs are currently providing PureMiner for \$99. The following are the features provided by PureMiner:

- ETHW, ETC, XMR, ERGO, BTC, RVN, KASPA, FLUX MINING
- PROXY ETHW AND ETC MINING
- DETECTS IF THE USER IS IDLE OR PLAYING GAMES
- DOWNLOAD AND EXECUTE A FILE OR UPDATE
- RUNS ON RAM, NO DROPPING FILES
- BOT KILLER
- STARTUP
- CRYPTABLE WITH PURE CRYPTER
- HIGH-QUALITY STUB 64bit CODED IN .NET 4.0

The figure below shows the post by the TA.

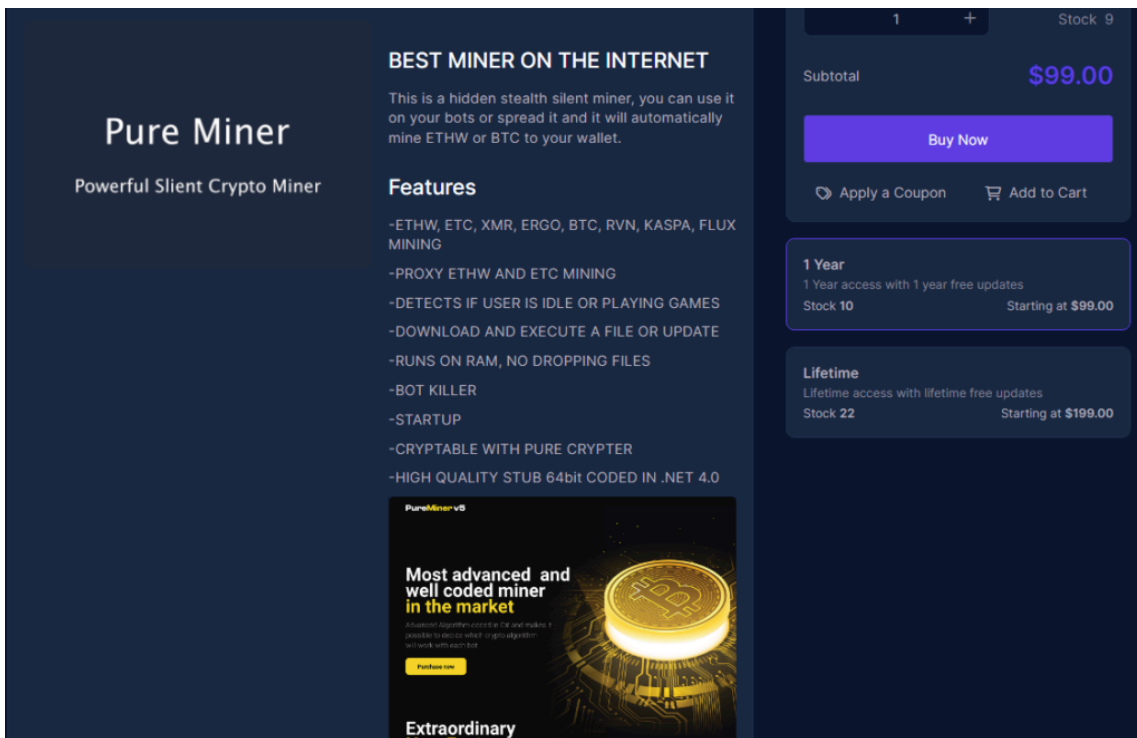


Figure 6 – PureMiner Post by Purecoder

## BlueLoader

According to the developers, the BlueLoader [botnet](#) can manage a sizable quantity of bots, start up again automatically, launch DDoS attacks, and also possess a bot-eliminating capability. BlueLoader is sold for \$99 by TAs. The figure below shows the post by TAs.

The image shows a product page for 'Blue Loader' on a dark-themed website. The main content area on the left includes a '1 Year' label, the product name 'Blue Loader', and the subtitle 'Advanced And Light Botnet'. It features three sections: 'BEST .NET LOADER IN THE MARKET' with a description, 'SQLITE DATABASE' with a description, and 'FEATURES :-' with a list of capabilities. On the right, a 'Purchase' sidebar shows a quantity of 1, a subtotal of \$99.00, and a 'Buy Now' button. Below this, two subscription options are listed: '1 Year' for \$99.00 and 'Lifetime' for \$199.00.

Figure 7 – BlueLoader Post by Purecoder

## PureHVNC

Pure HVNC is a hidden stealth VNC used to [control systems](#) covertly. TAs are selling one-year subscriptions for \$99. The features TAs as posted on the blog are:

- HVNC Support
  - CHROME
  - EDGE
  - BRAVE
  - FIREFOX
  - OUTLOOK
  - FOXMAIL
  - CMD
  - POWERSHELL
  - CLIPBOARD COPY PASTE
  - CHANGE DPI
  - Run Program
- TASK MANAGER
- FILE MANAGER
- DOWNLOAD AND EXECUTE A FILE OR UPDATE STUB
- RUNS ON RAM, NO DROPPING FILES
- STARTUP
- CRYPTABLE WITH PURE CRYPTER
- HIGH-QUALITY STUB CODED IN .NET 4.0

The figure below shows the TA’s post.

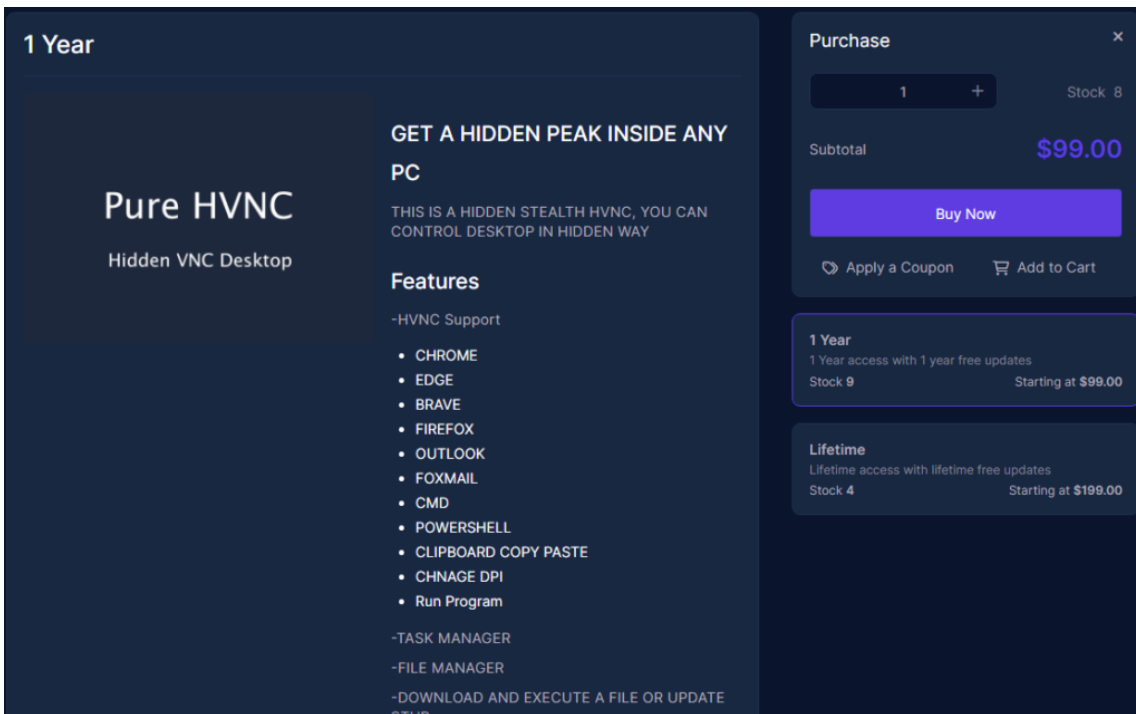


Figure 8 – PureHVNC Post by Purecoder

## Pure Logs Technical Analysis

The TA “Alibaba2044”’s malware campaign begins by sending out a malicious spam email linked to a zip file called *DOC9848-14-12-2022.zip*. This zip is password-protected to conceal its content and avoid detection.

Additionally, the zip file includes a Windows cabinet file that has been disguised as a bat file *DOC9848\_pdf.bat*. When the user clicks on this cab file, it will drop .NET-executable *x.exe* with sha256 *a843517b019e86af42252b568e06dfe91a22f9034ceb996f5b0df32dcc1e4274* in the *temp* folder and execute it.

The figure below shows the malicious executable in the *temp* folder.

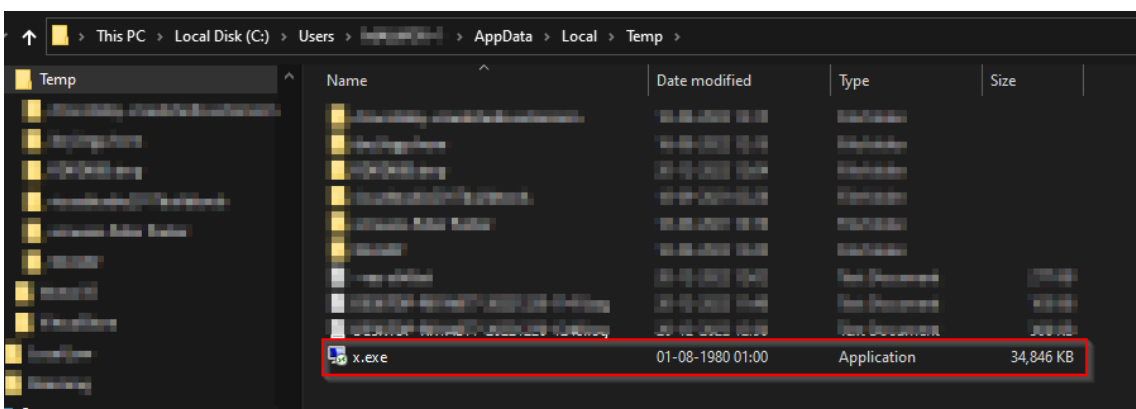


Figure 9 – Malware Dropped in Temp Folder

The figure below shows the details of the malicious file *x.exe*.

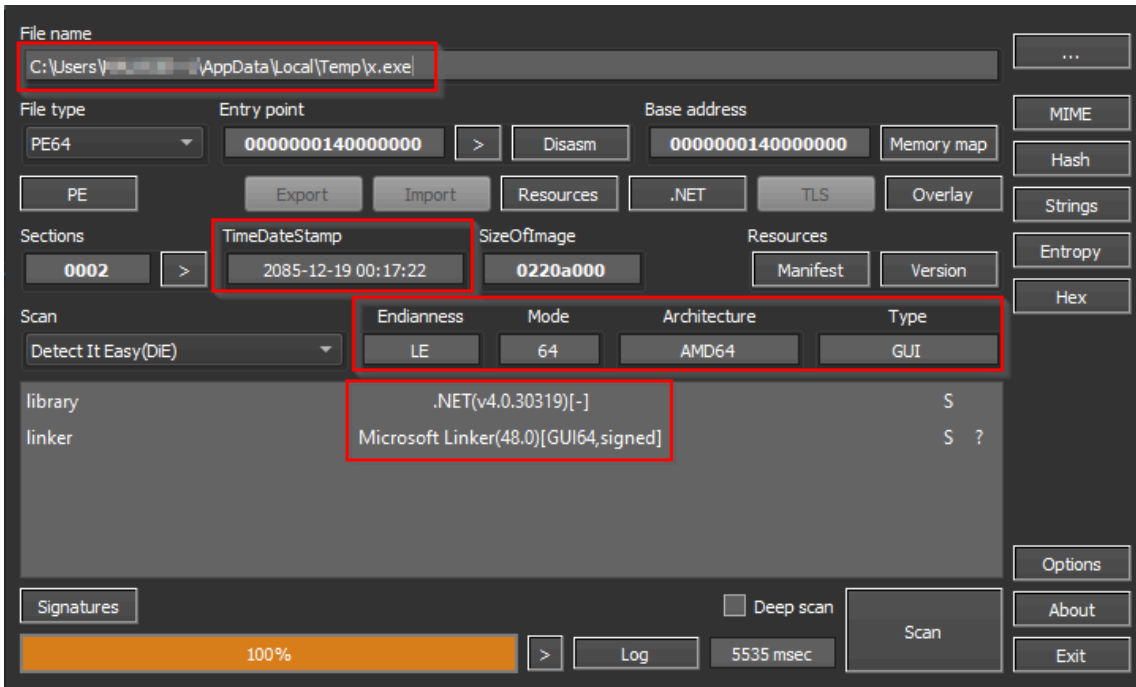


Figure 10 – x.exe file Details

The executable file contains a [malicious custom](#) encrypted payload in the form of an array. The [data is encrypted](#) using custom encryption.

The following figure shows the encrypted payload in the memory.

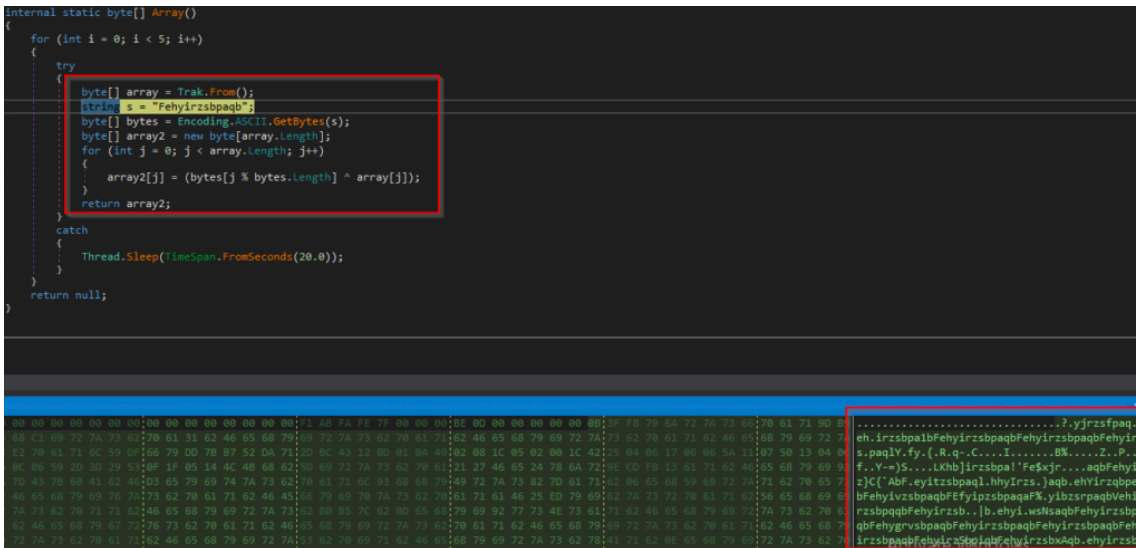


Figure 11 – Encrypted Data in the Memory

The malware decrypts the encrypted payload and stores it in memory at runtime.

The figure below shows the decrypted payload in the memory.

```

internal static byte[] Array()
{
    for (int i = 0; i < 5; i++)
    {
        try
        {
            byte[] array = Trak.From();
            string s = "Fehyirzsbpaqb";
            byte[] bytes = Encoding.ASCII.GetBytes(s);
            byte[] array2 = new byte[array.Length];
            for (int j = 0; j < array.Length; j++)
            {
                array2[j] = (bytes[j % bytes.Length] ^ array[j]);
            }
            return array2;
        }
        catch
        {
            Thread.Sleep(TimeSpan.FromSeconds(20.0));
        }
    }
    return null;
}
    
```

Figure 12 – Decrypted Payload in the Memory

The decrypted payload is a PureLogs DLL file with the name “Ixqwqt.dll” and sha256 db61b7e783969a2050c9e18b667c2a7d418d757a0c986183b8ef2f6e6eccaa48.

This malicious file is injected into running malware using *Assembly.Load()* method. The figure below shows the injection of malicious payload in the malware.

```

namespace WindowsFormsApp19
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x000DE88 File Offset: 0x000DC088
        private static void Main()
        {
            Process currentProcess = Process.GetCurrentProcess();
            int size = IntPtr.Size;
            byte[] array = Trak.Array();
            DateTime now = DateTime.Now;
            if (array == null)
            {
                return;
            }
            if (currentProcess.Id > 1)
            {
                Assembly assembly = Assembly.Load(array);
                if (size > 2)
                {
                    Type type = assembly.GetType().First((Type x) => x.FullName == "Ixqwqt.Qgzghklnhpbx");
                    if (array.Length > 3)
                    {
                        (MethodInfo)type.GetMember("Ytxtyecgjf")[0].DeclaringType.InvokeMember("Ytxtyecgjf", BindingFlags.InvokeMethod, null, null, null);
                    }
                }
            }
        }
    }
}
    
```

Figure 13 – Malware Injecting the Payload using InvokeMember()

## Conclusion

We have seen before that malware developers, with a lack of responsibility, can create malicious programs and sell them to different forums for monetary gain.

To attract more customers, they provide powerful and dangerous features like [information stealers](#), cryptocurrency miners, and HVNC to TAs. It is all for their own financial benefit. We will stay vigilant and monitor the latest threats and trends on the surface, deep and [dark web](#), keeping our readers updated.

## Our Recommendations

We have listed some 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 Malware Attacks

- Refrain from opening untrusted links and email attachments without verifying their authenticity.
- Use a reputed anti-virus and [Internet security](#) software package on your connected devices, including PC, laptop, and mobile.
- 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.

## Users Should Take the Following Steps After the Malware Attack

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

## Impact And Cruciality of Malware

- Loss of valuable data.
- Loss of the organization’s reputation and integrity.
- Loss of the organization’s [sensitive business information](#).
- Disruption in [organization operation](#).
- Monetary loss.

## MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	<a href="#">T1204</a>	User Execution
Defense Evasion	<a href="#">T1140</a> <a href="#">T1562</a>	Deobfuscate/Decode Files or Information Impair Defences
Discovery	<a href="#">T1082</a> <a href="#">T1083</a>	System Information Discovery File and Directory Discovery
Collection	<a href="#">T1119</a> <a href="#">T1005</a>	Automated <a href="#">Collection Data</a> from the Local System
Command and Control	<a href="#">T1071</a>	Application Layer Protocol
Exfiltration	<a href="#">T1020</a>	Automated Exfiltration

## Indicators of Compromise (IoCs)

Indicators	Indicator Type	Description
5e5276abac4f39ed674c8783d12212dc c055b968ae48bd35342a4aebfe6195e67529d84e	MD5 SHA1	DOC9848-14-12-2022 .zip

<b>c59559275fb8af4bbc59d47c267a94fbe44151e40a8606414d1b1f76a99852b1</b>	SHA256	
<b>743ea515bb5bab8929c6d280a3d0feaa</b> <b>58326656b86f43fdaa65b5493da1cb13e7cf6a2d</b> <b>887cab0d136a86a6be444883b62c90d073fd1f839896840233150475bd149c8</b>	MD5 SHA1 SHA256	DOC9848_pdf.bat
<b>460834754a0e145320380e54400b9509</b> <b>992c119799b3b3899263605930bf9c2b656afe8</b> <b>a843517b019e86af42252b568e06dfe91a22f9034ceb996f5b0df32dcc1e4274</b>	MD5 SHA1 SHA256	x.exe
<b>86a9edac11733b9985d977b330389593</b> <b>79c0f5242a3a95beeddd2761c092ed166332707c</b> <b>db61b7e783969a2050c9e18b667c2a7d418d757a0c986183b8ef2f6e6eccaa48</b>	MD5 SHA1 SHA256	Ixqwqt.dll

---

Source: <https://cyble.com/blog/pure-coder-offers-multiple-malware-for-sale-in-darkweb-forums/>