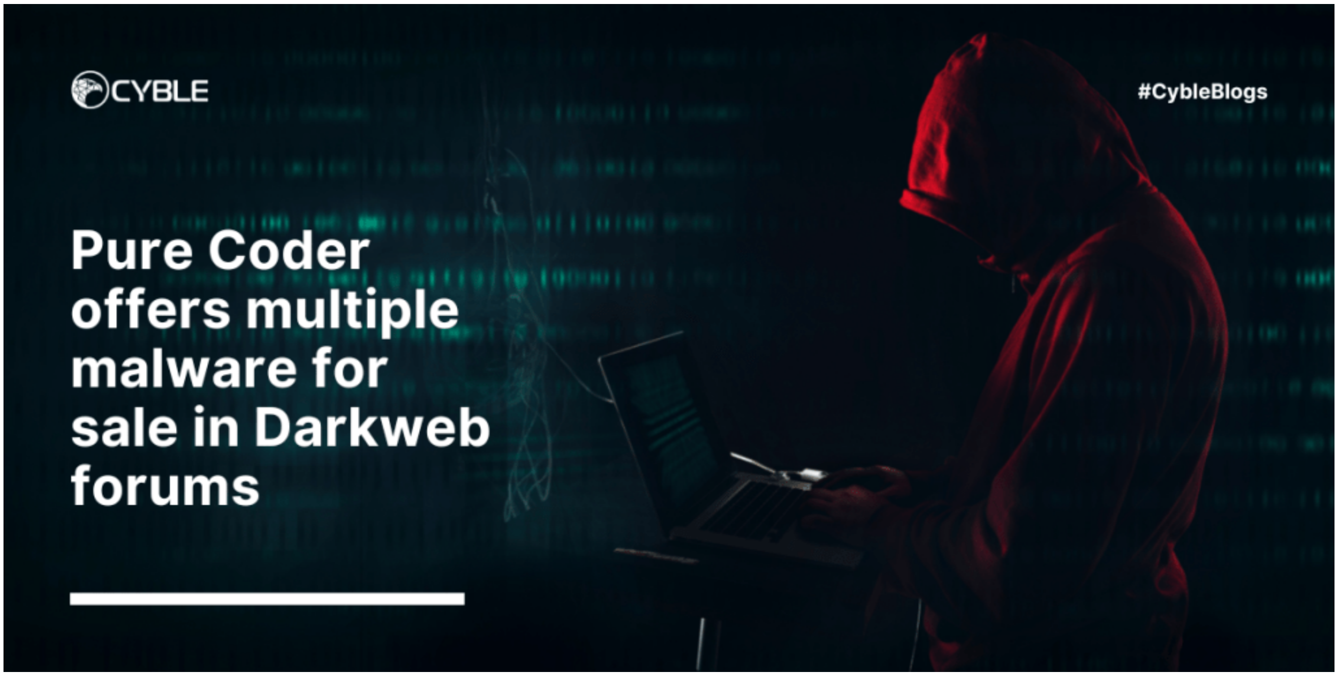
Pure coder offers multiple malware for sale in Darkweb forums

cyble.com/blog/pure-coder-offers-multiple-malware-for-sale-in-darkweb-forums/

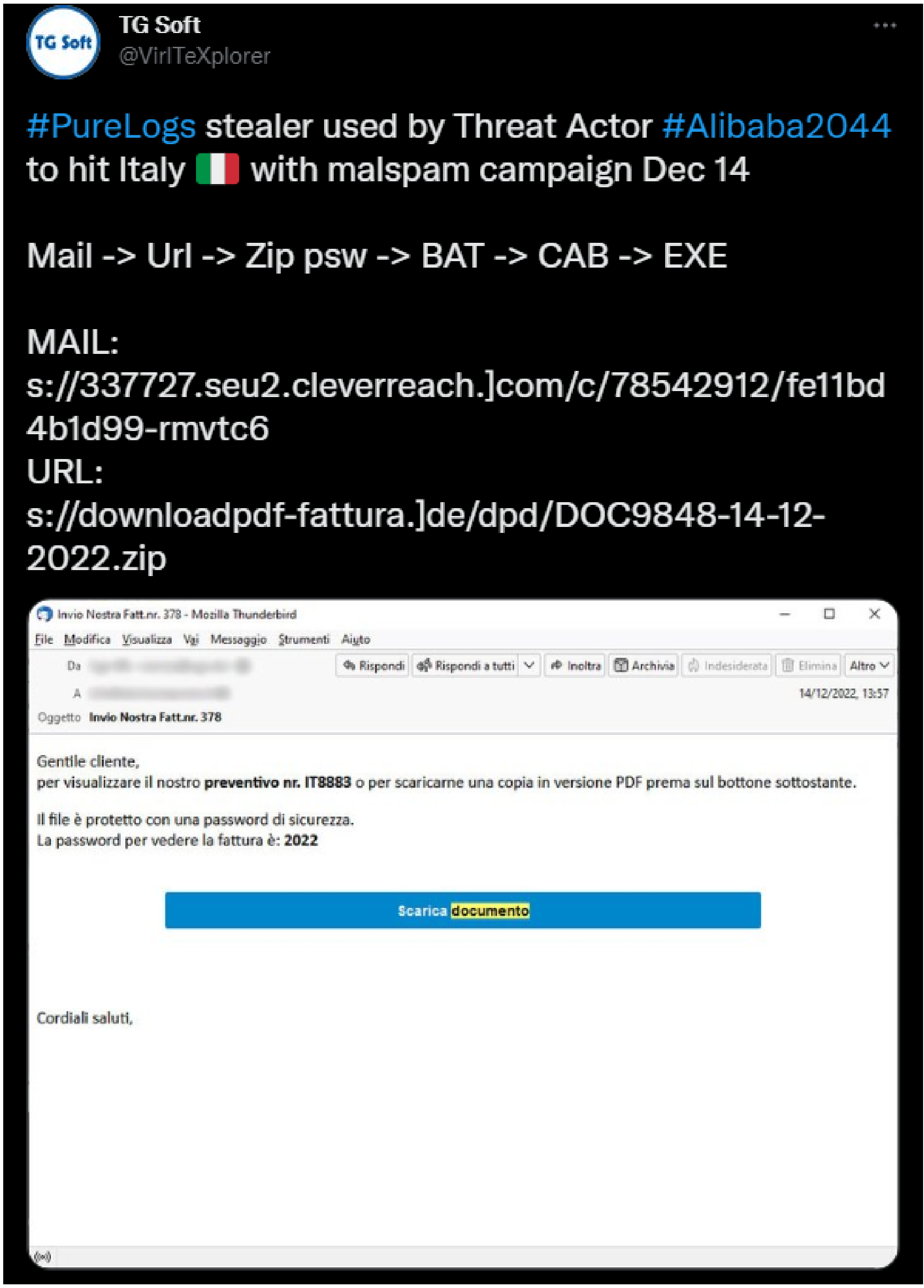
December 27, 2022


CYBLE
#CybleBlogs
Pure Coder offers multiple malware for sale in Darkweb forums

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.


TG Soft
@VirITeXplorer

#PureLogs stealer used by Threat Actor #Alibaba2044 to hit Italy 🇮🇹 with malspam campaign Dec 14

Mail -> Url -> Zip psw -> BAT -> CAB -> EXE

MAIL:
s://337727.seu2.cleverreach.]com/c/78542912/fe11bd4b1d99-rmvtc6
URL:
s://downloadpdf-fattura.]de/dpd/DOC9848-14-12-2022.zip

Invio Nostra Fatt.nr. 378 - Mozilla Thunderbird

Da [redacted]
A [redacted]
14/12/2022, 13:57
Oggetto **Invio Nostra Fatt.nr. 378**

Gentile cliente,
per visualizzare il nostro **preventivo nr. IT8883** o per scaricarne una copia in versione PDF prema sul bottone sottostante.

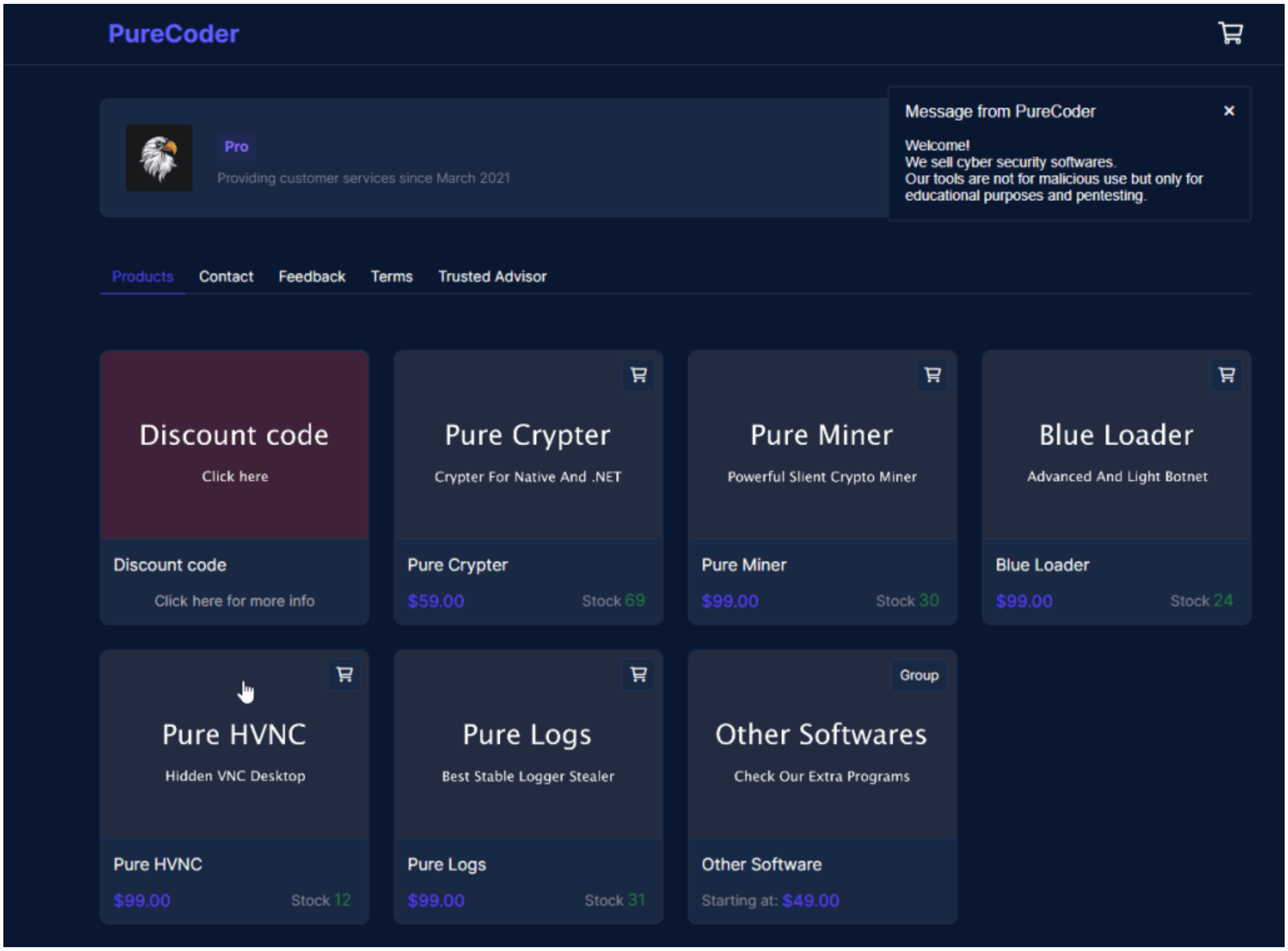
Il file è protetto con una password di sicurezza.
La password per vedere la fattura è: **2022**

Cordiali saluti,

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.



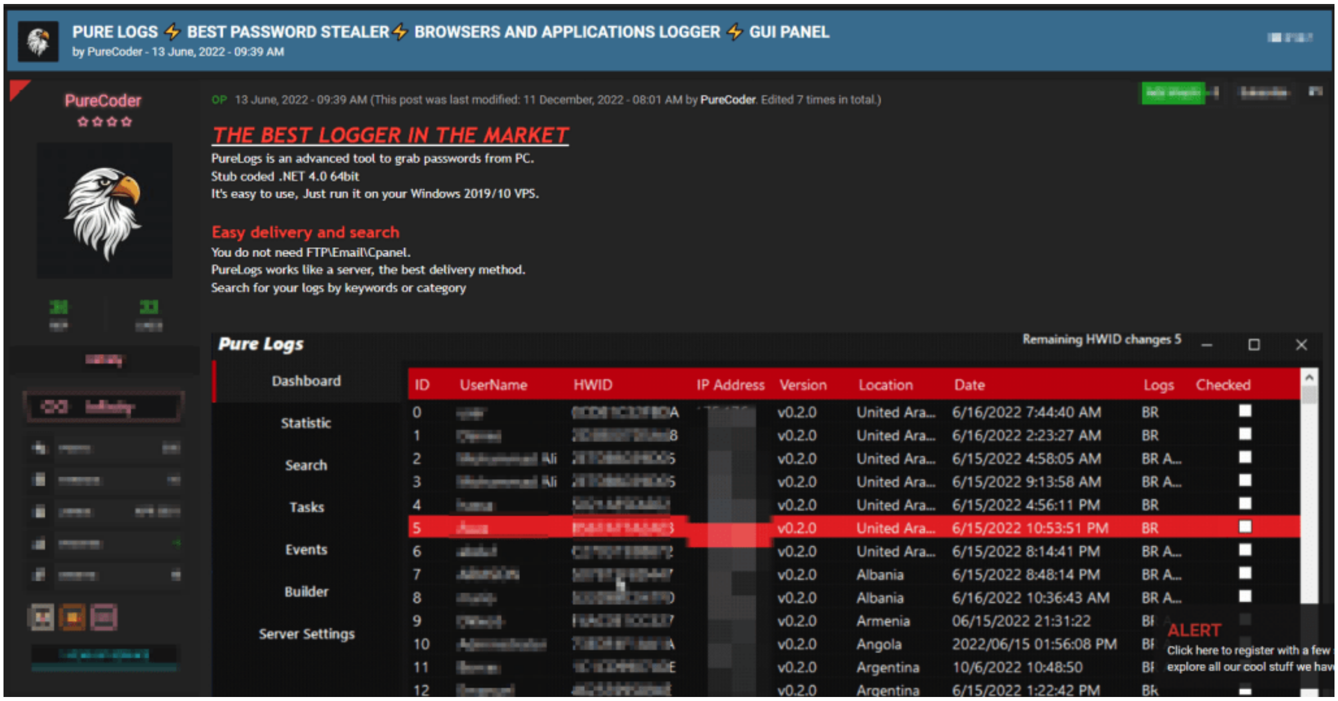
Message from PureCoder ×

Welcome!
We sell cyber security softwares.
Our tools are not for malicious use but only for educational purposes and pentesting.

Product	Description	Name	Price	Stock
Discount code	Click here	Discount code	Click here for more info	
Pure Crypter	Crypter For Native And .NET	Pure Crypter	$59.00	Stock 69
Pure Miner	Powerful Slient Crypto Miner	Pure Miner	$99.00	Stock 30
Blue Loader	Advanced And Light Botnet	Blue Loader	$99.00	Stock 24
Pure HVNC	Hidden VNC Desktop	Pure HVNC	$99.00	Stock 12
Pure Logs	Best Stable Logger Stealer	Pure Logs	$99.00	Stock 31
Other Softwares	Check Our Extra Programs	Other Software	Starting at: $49.00	Group

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.



PURE LOGS ⚡ BEST PASSWORD STEALER ⚡ BROWSERS AND APPLICATIONS LOGGER ⚡ GUI PANEL
by PureCoder - 13 June, 2022 - 09:39 AM

OP 13 June, 2022 - 09:39 AM (This post was last modified: 11 December, 2022 - 08:01 AM by PureCoder. Edited 7 times in total.)

THE BEST LOGGER IN THE MARKET
PureLogs is an advanced tool to grab passwords from PC.
Stub coded .NET 4.0 64bit
It's easy to use, Just run it on your Windows 2019/10 VPS.

Easy delivery and search
You do not need FTP\Email\Cpanel.
PureLogs works like a server, the best delivery method.
Search for your logs by keywords or category

ID	UserName	HWID	IP Address	Version	Location	Date	Logs	Checked
0	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/16/2022 7:44:40 AM	BR	☐
1	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/16/2022 2:23:27 AM	BR	☐
2	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/15/2022 4:58:05 AM	BR A...	☐
3	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/15/2022 9:13:58 AM	BR A...	☐
4	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/15/2022 4:56:11 PM	BR	☐
5	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/15/2022 10:53:51 PM	BR	☐
6	[redacted]	[redacted]	[redacted]	v0.2.0	United Ara...	6/15/2022 8:14:41 PM	BR A...	☐
7	[redacted]	[redacted]	[redacted]	v0.2.0	Albania	6/15/2022 8:48:14 PM	BR A...	☐
8	[redacted]	[redacted]	[redacted]	v0.2.0	Albania	6/16/2022 10:36:43 AM	BR A...	☐
9	[redacted]	[redacted]	[redacted]	v0.2.0	Armenia	06/15/2022 21:31:22	BI	
10	[redacted]	[redacted]	[redacted]	v0.2.0	Angola	2022/06/15 01:56:08 PM	BI	
11	[redacted]	[redacted]	[redacted]	v0.2.0	Argentina	10/6/2022 10:48:50	BI	
12	[redacted]	[redacted]	[redacted]	v0.2.0	Argentina	6/15/2022 1:22:42 PM	Bk	☐

ALERT
Click here to register with a few
explore all our cool stuff we hav

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.

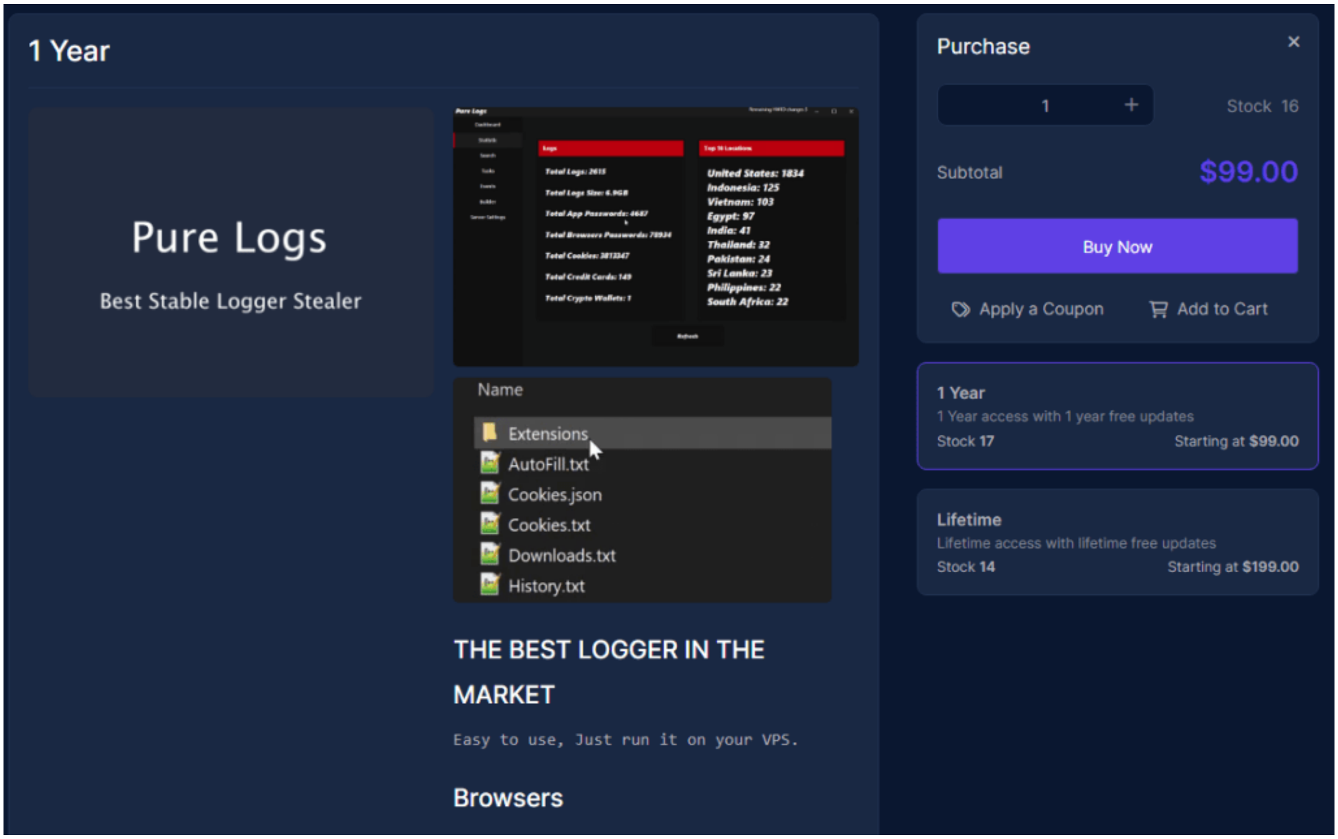
PureLogs

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, GAuth Authenticator, Authenticator.

The figure below illustrates the post related to PureLogs Stealer.



1 Year

Pure Logs

Best Stable Logger Stealer

Pure Logs

Total Logs: 2615
Total Logs Size: 6.9GB
Total App Passwords: 4687
Total Browsers Passwords: 78934
Total Cookies: 3813347
Total Credit Cards: 149
Total Crypto Wallets: 1

United States: 1834
Indonesia: 125
Vietnam: 103
Egypt: 97
India: 41
Thailand: 32
Pakistan: 24
Sri Lanka: 23
Philippines: 22
South Africa: 22

Name

Extensions
AutoFill.txt
Cookies.json
Cookies.txt
Downloads.txt
History.txt

THE BEST LOGGER IN THE MARKET

Easy to use, Just run it on your VPS.

Browsers

Purchase

1 Stock 16

Subtotal $99.00

Buy Now

Apply a Coupon Add to Cart

1 Year
1 Year access with 1 year free updates
Stock 17 Starting at $99.00

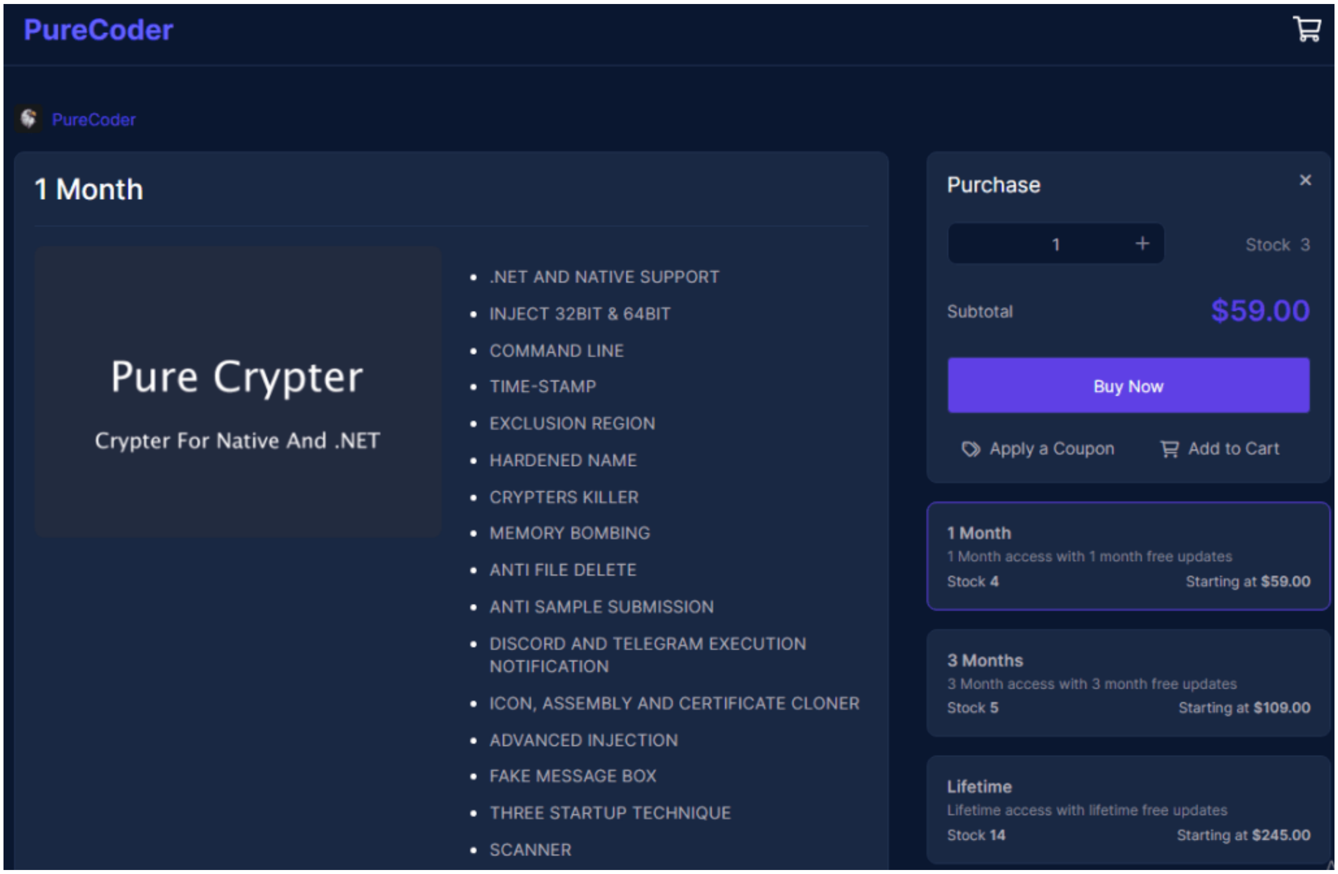
Lifetime
Lifetime access with lifetime free updates
Stock 14 Starting at $199.00

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.



PureCoder

PureCoder

1 Month

Pure Crypter

Crypter For Native And .NET

- .NET AND NATIVE SUPPORT
- INJECT 32BIT & 64BIT
- COMMAND LINE
- TIME-STAMP
- EXCLUSION REGION
- HARDENED NAME
- CRYPTERS KILLER
- MEMORY BOMBING
- ANTI FILE DELETE
- ANTI SAMPLE SUBMISSION
- DISCORD AND TELEGRAM EXECUTION NOTIFICATION
- ICON, ASSEMBLY AND CERTIFICATE CLONER
- ADVANCED INJECTION
- FAKE MESSAGE BOX
- THREE STARTUP TECHNIQUE
- SCANNER

Purchase ×

1 + Stock 3

Subtotal $59.00

Buy Now

Apply a Coupon Add to Cart

1 Month
1 Month access with 1 month free updates
Stock 4 Starting at $59.00

3 Months
3 Month access with 3 month free updates
Stock 5 Starting at $109.00

Lifetime
Lifetime access with lifetime free updates
Stock 14 Starting at $245.00

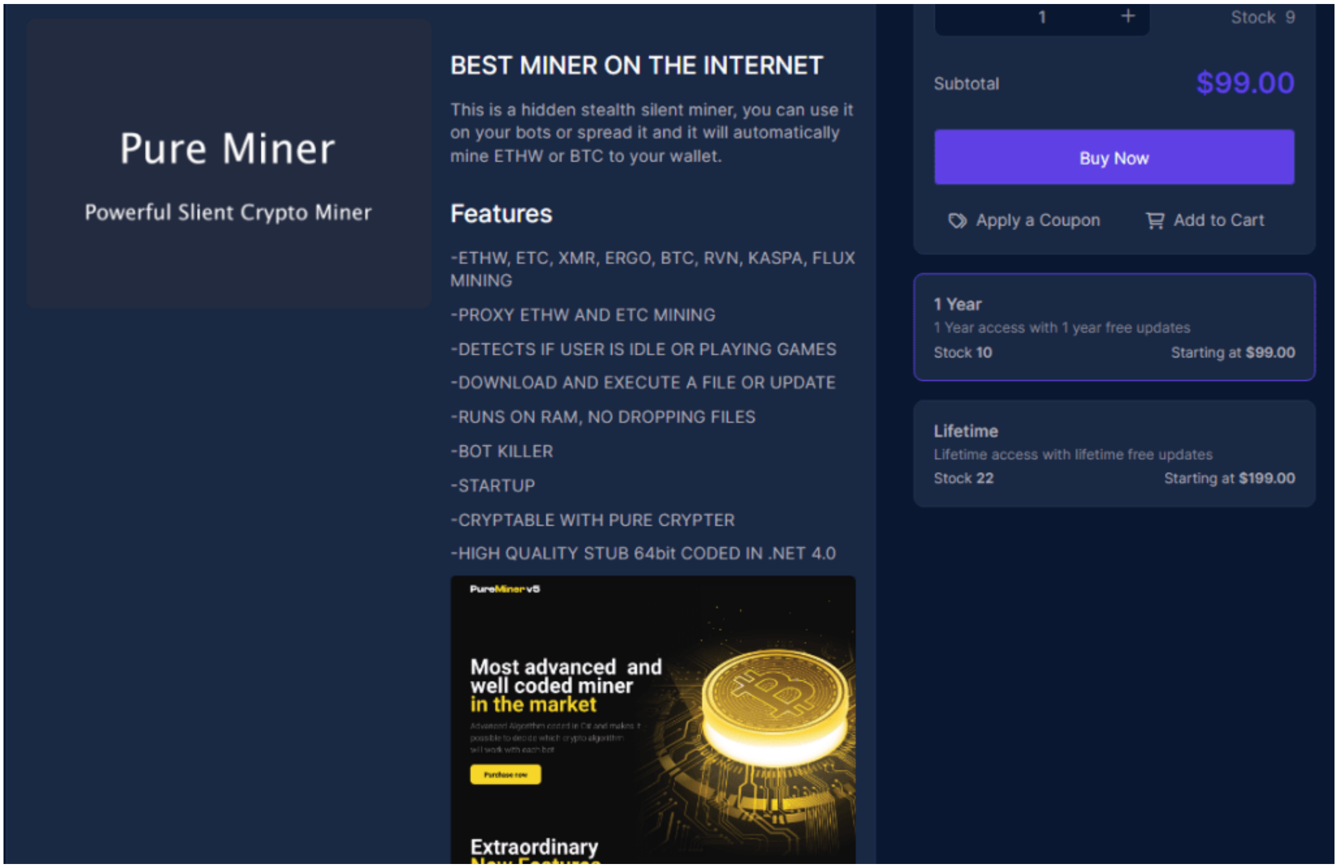
Figure 5 – PureCrypter Post by Purecoder

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.



Pure Miner

Powerful Slient Crypto Miner

BEST MINER ON THE INTERNET

This is a hidden stealth silent miner, you can use it on your bots or spread it and it will automatically mine ETHW or BTC to your wallet.

Features

-ETHW, ETC, XMR, ERGO, BTC, RVN, KASPA, FLUX MINING

-PROXY ETHW AND ETC MINING

-DETECTS IF 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

PureMiner v5

Most advanced and well coded miner in the market

Advanced Algorithm coded in C# and makes it possible to decide which crypto algorithm will work with each bot

Purchase now

Extraordinary

1 + Stock 9

Subtotal $99.00

Buy Now

Apply a Coupon Add to Cart

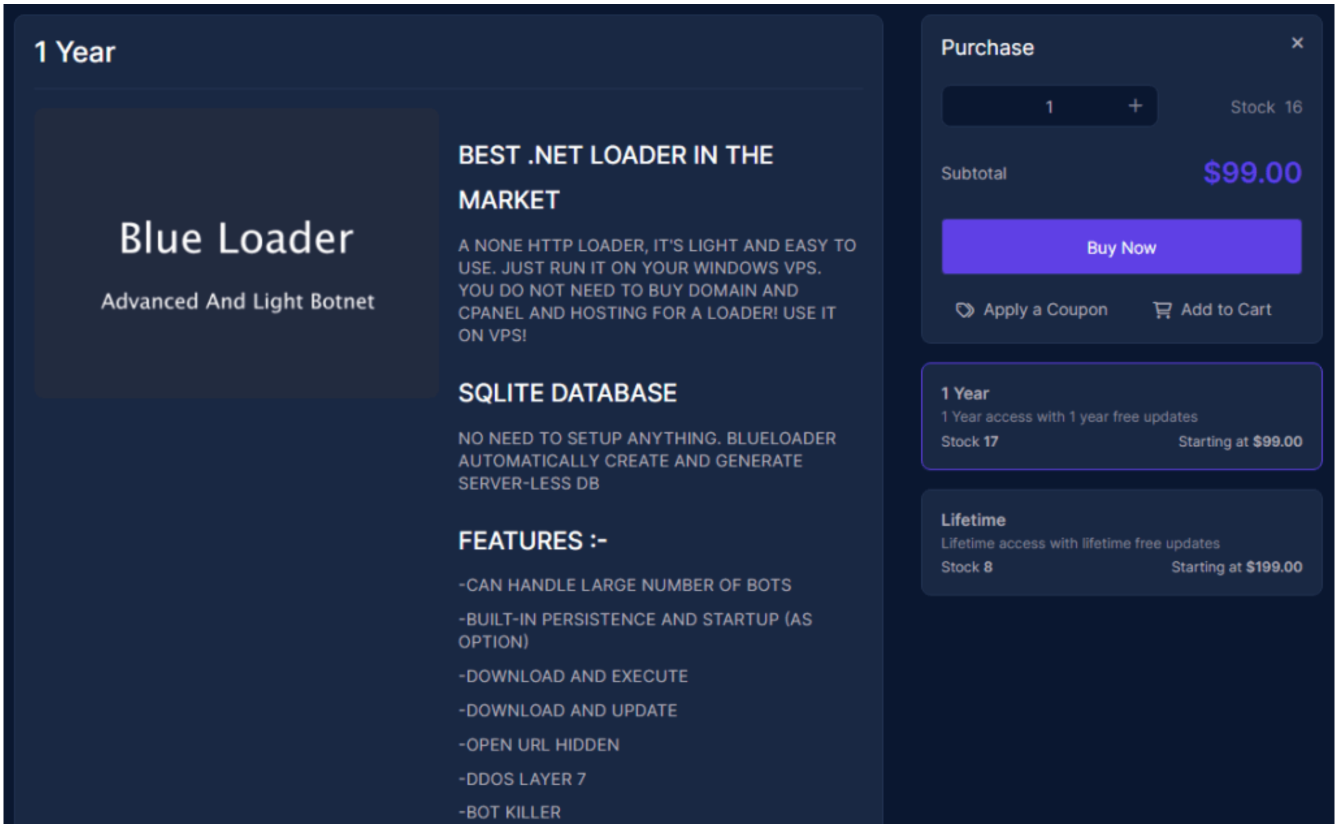
1 Year
1 Year access with 1 year free updates
Stock 10 Starting at $99.00

Lifetime
Lifetime access with lifetime free updates
Stock 22 Starting at $199.00

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.



1 Year

Blue Loader

Advanced And Light Botnet

BEST .NET LOADER IN THE MARKET

A NONE HTTP LOADER, IT'S LIGHT AND EASY TO USE. JUST RUN IT ON YOUR WINDOWS VPS. YOU DO NOT NEED TO BUY DOMAIN AND CPANEL AND HOSTING FOR A LOADER! USE IT ON VPS!

SQLITE DATABASE

NO NEED TO SETUP ANYTHING. BLUELOADER AUTOMATICALLY CREATE AND GENERATE SERVER-LESS DB

FEATURES :-

-CAN HANDLE LARGE NUMBER OF BOTS

-BUILT-IN PERSISTENCE AND STARTUP (AS OPTION)

-DOWNLOAD AND EXECUTE

-DOWNLOAD AND UPDATE

-OPEN URL HIDDEN

-DDOS LAYER 7

-BOT KILLER

Purchase

1 Stock 16

Subtotal $99.00

1 Year
1 Year access with 1 year free updates
Stock 17 Starting at $99.00

Lifetime
Lifetime access with lifetime free updates
Stock 8 Starting at $199.00

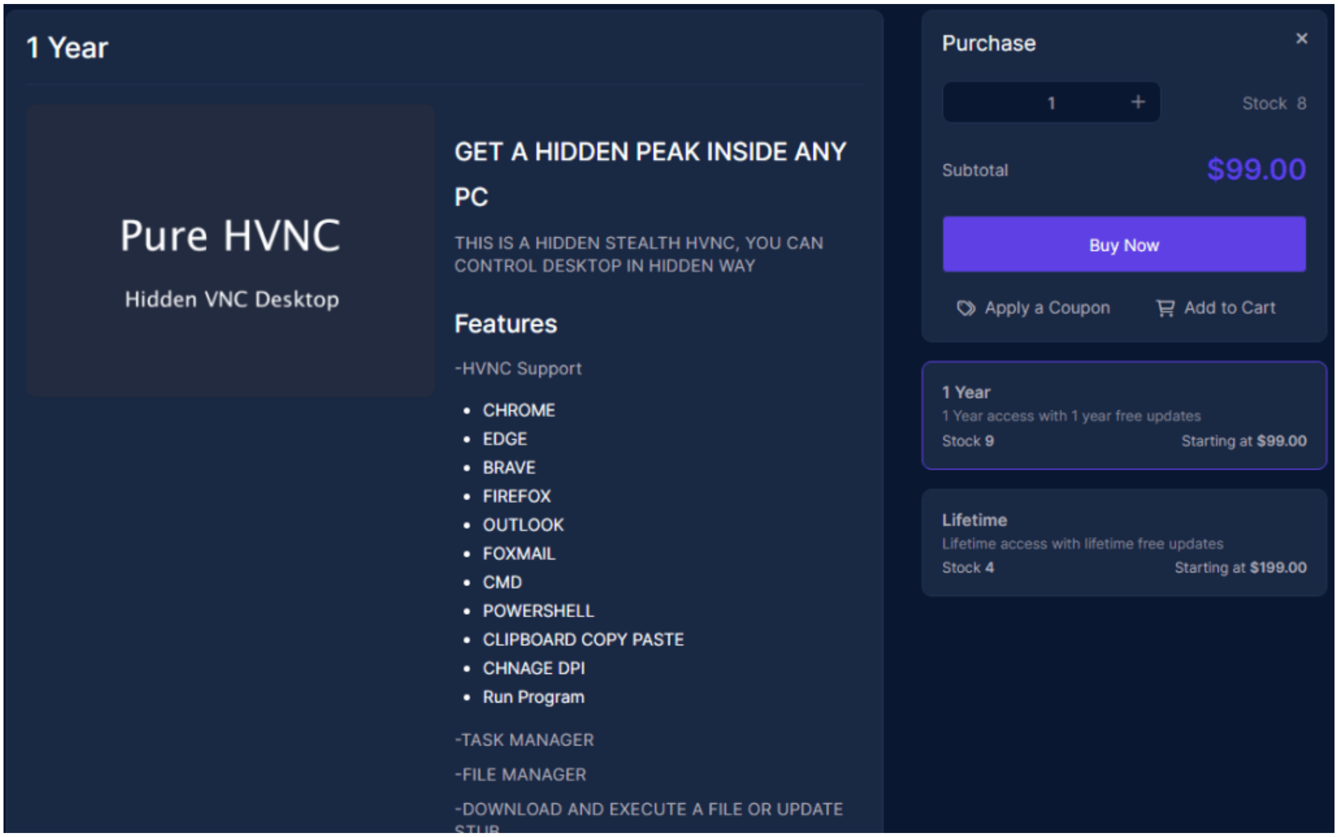
Figure 7 – BlueLoader Post by Purecoder

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.



1 Year

Pure HVNC

Hidden VNC Desktop

GET A HIDDEN PEAK INSIDE ANY PC

THIS IS A HIDDEN STEALTH HVNC, YOU CAN CONTROL DESKTOP IN HIDDEN WAY

Features

-HVNC Support

- CHROME
- EDGE
- BRAVE
- FIREFOX
- OUTLOOK
- FOXMAIL
- CMD
- POWERSHELL
- CLIPBOARD COPY PASTE
- CHNAGE DPI
- Run Program

-TASK MANAGER

-FILE MANAGER

-DOWNLOAD AND EXECUTE A FILE OR UPDATE STUB

Purchase

1 + Stock 8

Subtotal $99.00

1 Year
1 Year access with 1 year free updates
Stock 9 Starting at $99.00

Lifetime
Lifetime access with lifetime free updates
Stock 4 Starting at $199.00

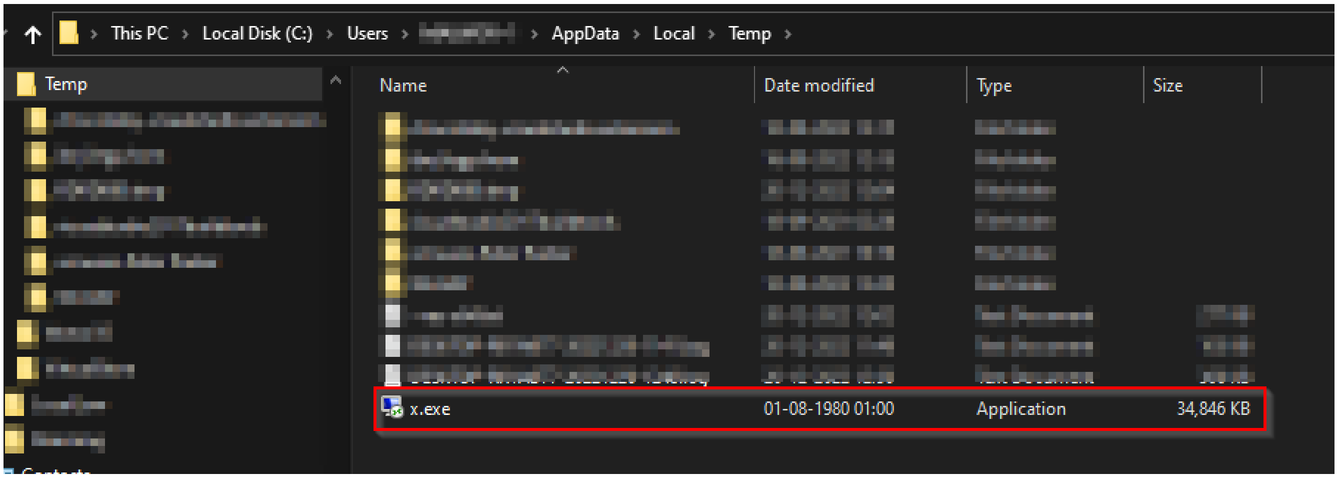
Figure 8 – PureHVNC Post by Purecoder

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.

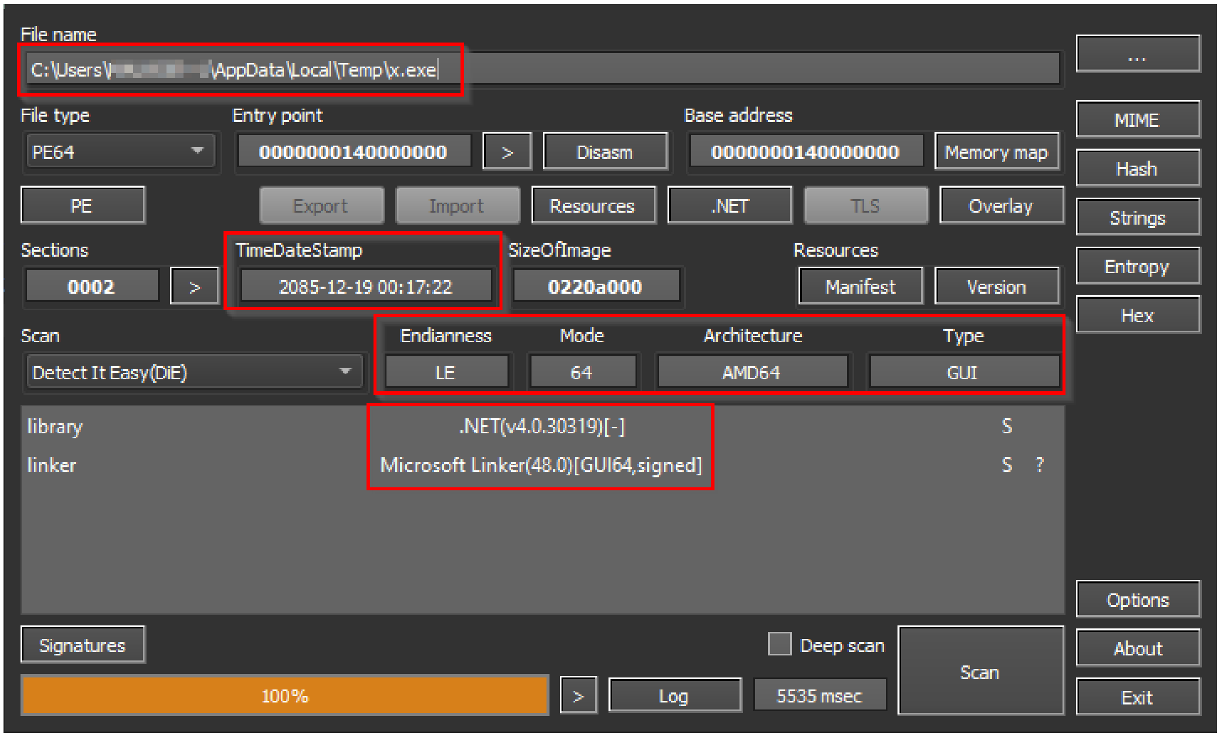


This PC › Local Disk (C:) › Users › [redacted] › AppData › Local › Temp ›

Name	Date modified	Type	Size
[redacted]	[redacted]	[redacted]	[redacted]
x.exe	01-08-1980 01:00	Application	34,846 KB

Figure 9 – Malware Dropped in Temp Folder

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



File name: C:\Users\[redacted]\AppData\Local\Temp\x.exe

File type: PE64
Entry point: 0000000140000000
Base address: 0000000140000000
Sections: 0002
TimeDateStamp: 2085-12-19 00:17:22
SizeOfImage: 0220a000
Scan: Detect It Easy(DiE)
Endianness: LE
Mode: 64
Architecture: AMD64
Type: GUI

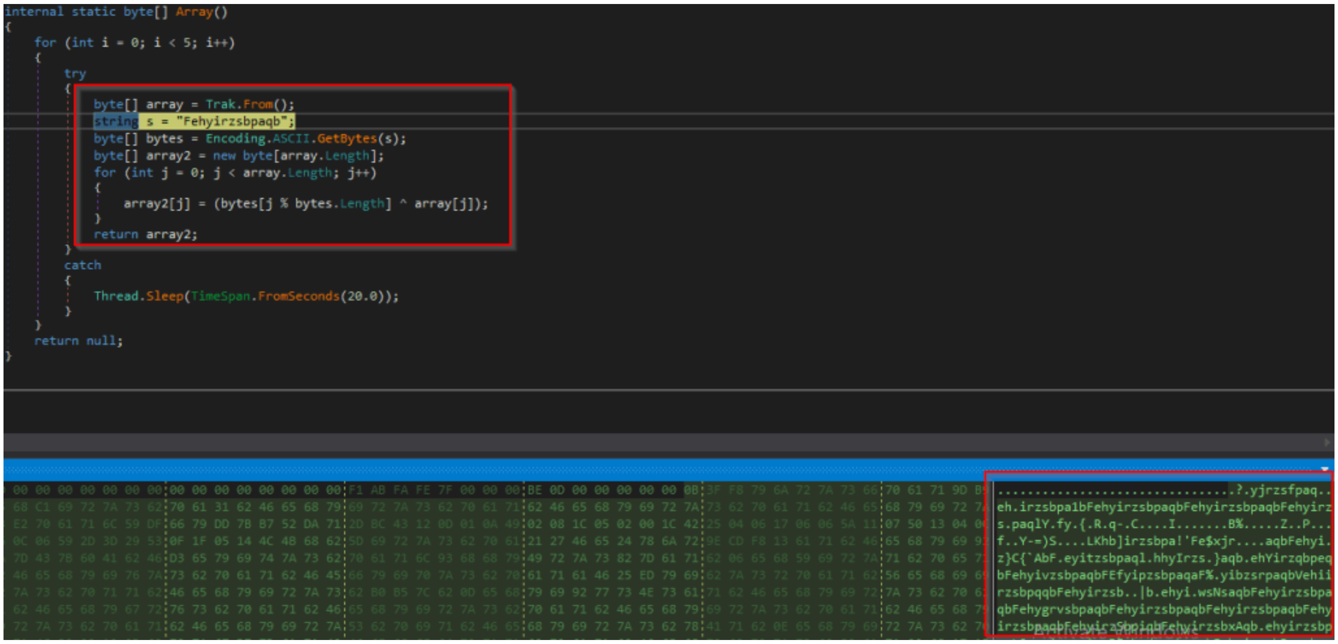
```
library    .NET(v4.0.30319)[-]                    S
linker     Microsoft Linker(48.0)[GUI64,signed]   S ?
```

☐ Deep scan
100%
5535 msec

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.



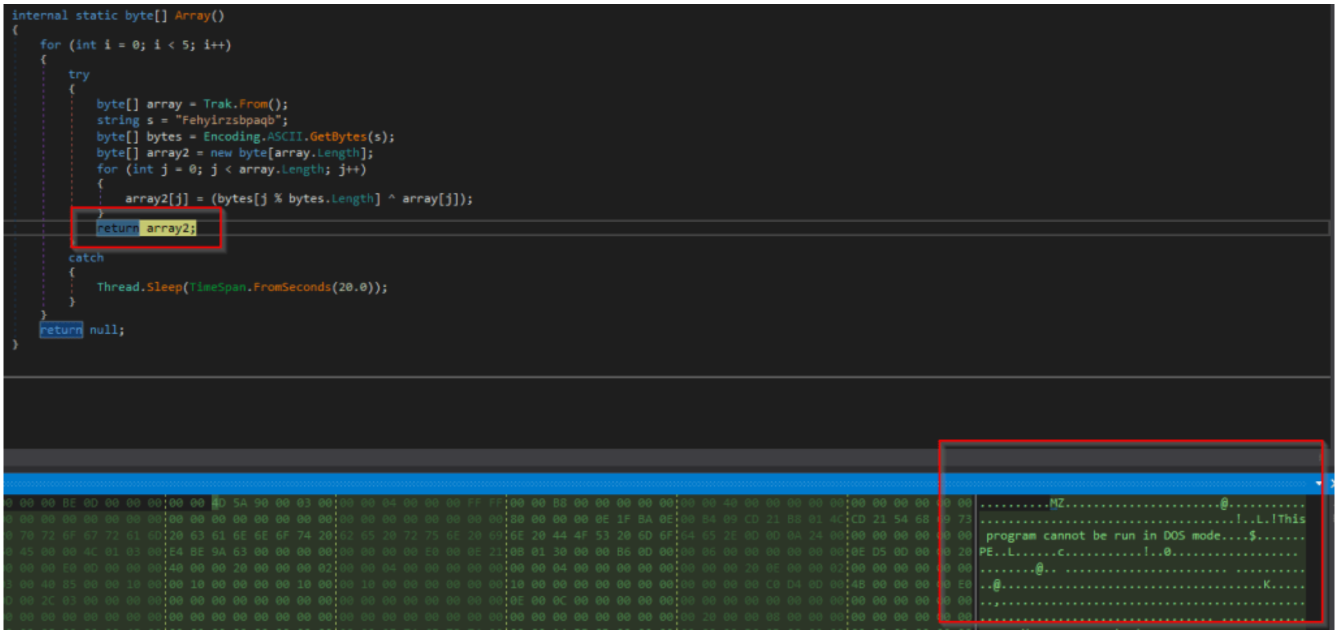
```
internal static byte[] Array()
{
    for (int i = 0; i < 5; i++)
    {
        try
        {
            byte[] array = Trak.From();
            string s = "Fehyirzsbpaqb";
            byte[] bytes = Encoding.ASCII.GetBytes(s);
            byte[] array2 = new byte[array.Length];
            for (int 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;
}
```

```
...............................?.yjrzsfpaq..
eh.irzsbpa1bFehyirzsbpaqbFehyirzsbpaqbFehyirz
s.paqlY.fy.{.R.q-.C....I.......B%.....Z..P...
f..Y-=)S....LKhb]irzsbpa!'Fe$xjr....aqbFehyi.
z}C{`AbF.eyitzsbpaql.hhyIrzs.}aqb.ehYirzqbpeq
bFehyivzsbpaqbFEfyipzsbpaqaF%.yibzsrpaqbVehii
rzsbpqqbFehyirzsb..|b.ehyi.wsNsaqbFehyirzsbpa
qbFehygrvsbpaqbFehyirzsbpaqbFehyirzsbpaqbFehy
irzsbpaqbFehyirzSbpiqbFehyirzsbxAqb.ehyirzsbp
```

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.



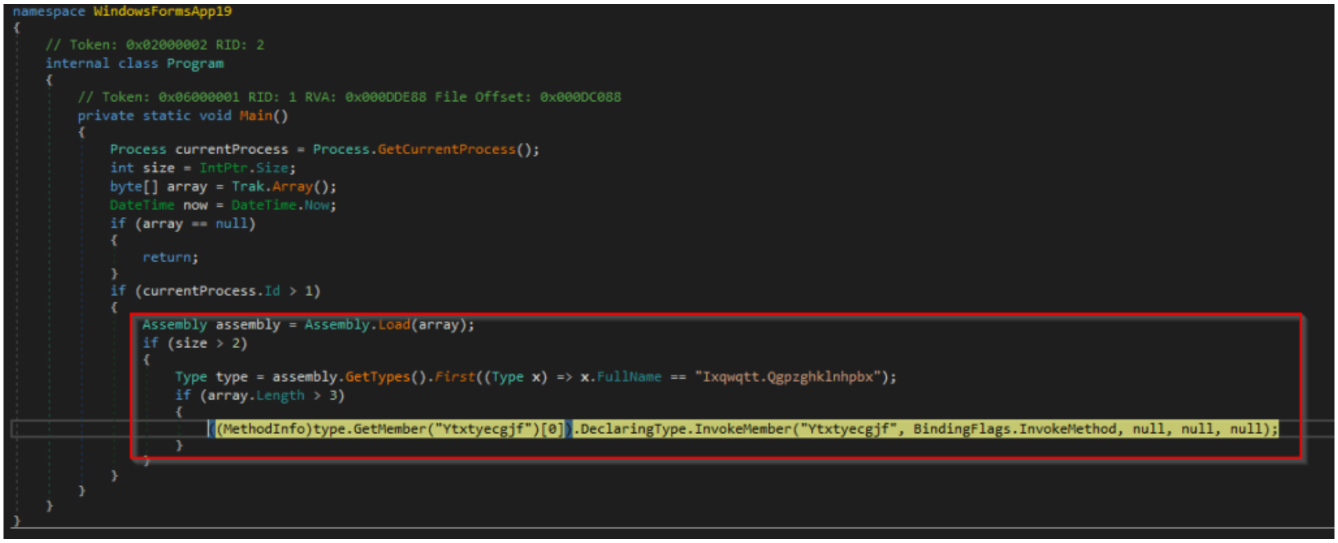
```
internal static byte[] Array()
{
    for (int i = 0; i < 5; i++)
    {
        try
        {
            byte[] array = Trak.From();
            string s = "Fehyirzsbpaqb";
            byte[] bytes = Encoding.ASCII.GetBytes(s);
            byte[] array2 = new byte[array.Length];
            for (int 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;
}
```

```
0 00 00 BE 0D 00 00 00 00 00 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 0 00 ..........MZ......................@..........
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 9 73 ....................................!..L.!This
0 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 0 00  program cannot be run in DOS mode....$.......
0 45 00 00 4C 01 03 00 E4 BE 9A 63 00 00 00 00 00 00 00 00 E0 00 0E 21 0B 01 30 00 00 B6 0D 00 00 06 00 00 00 00 00 00 0E D5 0D 00 0 20 PE..L......c...........!..0.................
0 00 00 E0 0D 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0E 00 00 02 00 00 00 00 0 00 ........@.. ...................... ..........
3 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 C0 D4 0D 00 4B 00 00 00 0 E0 ..@.................................K.....
0 00 2C 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0E 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 00 ..,.........................................
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 0 00 ..................... ......................
```

Figure 12 – Decrypted Payload in the Memory

The decrypted payload is a PureLogs DLL file with the name “Ixqwqtt.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: 0x000DDE88 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.GetTypes().First((Type x) => x.FullName == "Ixqwqtt.Qgpzghklnhpbx");
                    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	T1204	User Execution
Defense Evasion	T1140 T1562	Deobfuscate/Decode Files or Information Impair Defences
Discovery	T1082 T1083	System Information Discovery File and Directory Discovery
Collection	T1119 T1005	Automated Collection Data from the Local System
Command and Control	T1071	Application Layer Protocol
Exfiltration	T1020	Automated Exfiltration

Indicators of Compromise (IoCs)

Indicators	Indicator Type	Description
5e5276abac4f39ed674c8783d12212dc **c055b968ae48bd35342a4aebfe6195e67529d84e** **c59559275fb8af4bbc59d47c267a94fbe44151e40a8606414d1b1f76a99852b1**	MD5 SHA1 SHA256	DOC9848-14-12-2022 .zip

743ea515bb5bab8929c6d280a3d0feaa **58326656b86f43fdaa65b5493da1cb13e7cf6a2d** **887cabc0d136a86a6be444883b62c90d073fd1f83989684023315047 5bd149c8**	MD5 SHA1 SHA256	DOC9848_pdf.bat
460834754a0e145320380e54400b9509 **992c119799b3b3899263605930bf9fc2b656afe8** **a843517b019e86af42252b568e06dfe91a22f9034ceb996f5b0df32dcc1e4274**	MD5 SHA1 SHA256	x.exe
86a9edac11733b9985d977b330389593 **79c0f5242a3a95beeddd2761c092ed166332707c** **db61b7e783969a2050c9e18b667c2a7d418d757a0c986183b8ef2f6e6eccaa48**	MD5 SHA1 SHA256	lxqwqtt.dll

Comments are closed.