


Is There Really Such a Thing as a Low-Paid Ransomware Operator?

 mcafee.com/blogs/enterprise/mcafee-enterprise-atr/is-there-really-such-a-thing-as-a-low-paid-ransomware-operator/

ARCHIVED STORY

By **Thibault Seret** · October 18, 2021

Introduction

Going by recent headlines you could be forgiven for thinking all ransomware operators are raking in millions of ill-gotten dollars each year from their nefarious activities.

Lurking in the shadows of every large-scale attack by organized gangs of cybercriminals, however, there can be found a multitude of smaller actors who do not have access to the latest ransomware samples, the ability to be affiliates in the [post-DarkSide RaaS world](#) or the financial clout to tool up at speed.

So what is a low-paid ransomware operator to do in such circumstances?

By getting creative and looking out for the latest malware and builder leaks they can be just as devastating to their victims and, in this blog, we will track the criminal career of one such actor as they evolve from homemade ransomware to utilizing major ransomware through the use of publicly leaked builders.

The Rich Get Richer

For years, the McAfee Enterprise Advanced Threat Research (ATR) team has observed the [proliferation of ransomware](#) and the birth and [\(apparent\) death](#) of large organized gangs of operators. The most notorious of these gangs have extorted huge sums of money from their victims, by charging for decryption of data or by holding the data itself to ransom against the threat of publication on their 'leak' websites.

With the income of such tactics sometimes running into the millions of dollars, such as with the [Netwalker ransomware](#) that generated 25 million USD between 1 March and 27 July 2020, we speculate that much of those ill-gotten funds are subsequently used to build and maintain arsenals of offensive cyber tools, allowing the most successful cybercriminals to stay one step ahead of the chasing pack

 Figure 1. Babuk group looking for a corporate VPN 0-Day

Figure 1. Babuk group looking for a corporate VPN 0-Day

As seen in the image above, cybercriminals with access to underground forums and deep pockets have the means to pay top dollar for the tools they need to continually generate more income, with this particular Babuk operator offering up 50,000 USD for a 0-day targeting a corporate virtual private network (VPN) which would allow easy access to a new victim.

The Lowly-Paid Don't Necessarily Stay That Way

For smaller ransomware operators, who do not have affiliation with a large group, the technical skills to create their own devastating malware or the financial muscle to buy what they need, the landscape looks rather different.

Unable to build equally effective attack chains, from initial access through to data exfiltration, their opportunities to make illegal profits are far slimmer in comparison to the behemoths of the ransomware market.

Away from the gaze of researchers who typically focus on the larger ransomware groups, many individuals and smaller groups are toiling in the background, attempting to evolve their own operations any way they can. One such method we have observed is through the use of leaks, such as the recent online posting of Babuk's builder and source code.

 Figure 2. Babuk builder public leak on Twitter

Figure 2. Babuk builder public leak on Twitter


 Figure 3. Babuk source code leak on underground forum

Figure 3. Babuk source code leak on underground forum

McAfee Enterprise ATR has seen two distinct types of cybercriminal taking advantage of leaks such as this. The first group, which we presume to be less tech-savvy, has merely copied and pasted the builder, substituting the Bitcoin address in the ransom note with their own. The second group has gone further, using the source material to iterate their own versions of Babuk, complete with additional features and new packers.

Thus, even those operators at the bottom of the ransomware food chain have the opportunity to build on others' work, to stake their claim on a proportion of the money to be made from data exfiltration and extortion.

ATR's Theory of Evolution

A Yara rule dedicated to Babuk ransomware triggered a new sample uploaded on VirusTotal, which brings us to our 'lowly-paid' ransomware actor.

From a quick glance at the sample we can deduce that it is a copied and pasted binary output from Babuk's builder, with an edited ransom note naming the version "Delta Plus", two recovery email addresses and a new Bitcoin address for payments:



Figure 4. Strings content of "Delta Plus" named version of Babuk

We've seen the two email recovery addresses before – they have been used to deliver random ransomware in the past and, by using them to pivot, we were able to delve into the actor's resume:

The first email address, retrievedata300@gmail.com, has been used to drop a .NET ransomware mentioning "Delta Plus":

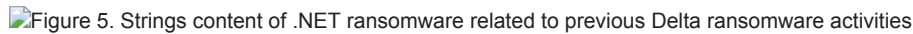


Figure 5. Strings content of .NET ransomware related to previous Delta ransomware activities

Filename	Setup.exe
Compiled Time	Tue Sep 7 17:58:34 2021
FileType	Win32 EXE
FileSize	22.50 KB
Sha256	94fe0825f26234511b19d6f68999d8598a9c21d3e14953731ea0b5ae4ab93c4d

The ransomware is pretty simple to analyze; all mechanisms are declared, and command lines, registry modification, etc., are hardcoded in the binary.



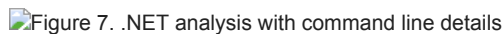


Figure 7. .NET analysis with command line details

In fact, the actor's own ransomware is so poorly developed (no packing, no obfuscation, command lines embedded in the binary and the fact that the .NET language is easy to analyze) that it is hardly surprising they started using the Babuk builder instead.

By way of contrast, their new project is well developed, easy to use and efficient, no to mention painful to analyze (as it is written in the [Golang language](#)) and provides executables for Windows, Linux and network attached storage (NAS) systems.

The second email address, deltapaymentbitcoin@gmail.com, has been used to drop an earlier version of the .NET ransomware



Figure 8. Strings content from first version of .NET ransomware

Filename	test2.exe
Compiled Time	Mon Aug 30 19:49:54 2021
FileType	Win32 EXE
FileSize	15.50 KB
Sha256	e1c449aa607f70a9677fe23822204817d0ff41ed3047d951d4f34fc9c502f761

Tactics, Techniques and Procedures

By checking the relationships between "Delta ransomware", the Babuk iteration and the domains contacted during process execution, we can observe some domains related to our sample:

suporte01928492.redirectme.net
suporte20082021.sytes.net
24.152.38.205

Thanks to a misconfiguration, files hosted on those two domains are accessible through Open Directory (OpenDir), which is a list of direct links to files stored on a server:

 Figure 9.

 Figure 10. Open Directories website where samples are hosted

Figure 10. Open Directories website where samples are hosted

bat.rar: A PowerShell script used to perform several operations:

- Try to disable Windows Defender
- Bypass User Account Control (UAC)
- Get system rights via runasti

 Figure 11. Privilege escalation to get system rights

Figure 11. Privilege escalation to get system rights

- exe.rar: Delta Plus ransomware
- reg.rar: Registry values used to disable Windows Defender

 Figure 12. Registry value modifications to disable Windows Defender

Figure 12. Registry value modifications to disable Windows Defender

Other domains where files are hosted contain different tools used during attack operations:

We've found two methods employed by the operator, which we assume to be used for initial access: First, a fake Flash Player installer and, secondly, a fake Anydesk remote tool installer used to drop the ransomware. Our theory about Flash Player initial access has been confirmed by checking the IP that hosts most of the domains:

 Figure 13. Fake Flash website used to download fake Flash installer

Figure 13. Fake Flash website used to download fake Flash installer

When logging in, the website warns you that your Flash Player version is outdated and tries to download the Fake Flash Player installer:


 Figure 14. JavaScript variables used to drop fake Flash Installer

Figure 14. JavaScript variables used to drop fake Flash Installer

A secondary site appears to have also been utilized in propagating the fake Flash Player, though it is currently offline :


 Figure 15. JavaScript function to download the fake Flash Installer from another website

Figure 15. JavaScript function to download the fake Flash Installer from another website

- Portable Executable (PE) files used to launch PowerShell command lines to delete shadow copies, exclude Windows Defender and import registry keys from "Update.reg.rar" to disable Windows defender.
- A PE file used for several purposes: Exfiltrating files from the victim, keylogging, checking if the system has already been held to ransom, getting system information, obtaining user information and to create and stop processes.

 Figure 16.

 Figure 17. Functions and C2 configuration from ransomware sample

Figure 17. Functions and C2 configuration from ransomware sample

(host used for extraction)

In addition to the above, we also found evidence that this actor tried to leverage another ransomware builder leak, Chaos ransomware.

Infrastructure

The majority of domains used by this actor are hosted on the same IP: "24.152.38.205" (AS 270564 / MASTER DA WEB DATACENTER LTDA).

But as we saw by "analyzing" the extraction tool used by the actor, another IP is mentioned: "149.56147.236" (AS 16276 / OVH SAS). On this IP, some ports are open, such as FTP (probably used to store exfiltrated data), SSH, etc.

By looking at this IP with Shodan, we can get a dedicated hash for the SSH service, plus fingerprints to use on this IP, and then find other IPs used by the actor during their operations.

By using this hash, we were able to map the infrastructure by looking for other IPs sharing the same SSH key + fingerprintings.

At least 174 IPs are sharing the same SSH pattern (key, fingerprint, etc.); all findings are available in the IOCs section.

Some IPs are hosting different file types, maybe related to previous campaigns:


 Figure 18. Open Directory website probably used by the same actor for previous campaigns

Figure 18. Open Directory website probably used by the same actor for previous campaigns

Bitcoin Interests

Most of the ransomware samples used by the actor mention different Bitcoin (BTC) addresses which we assume is an effort to obscure their activity.

By looking for transactions between those BTC addresses with CipherTrace, we can observe that all the addresses we extracted (see the circle highlighted with a yellow “1” below) from the samples we’ve found are related and eventually point to a single Bitcoin wallet, probably under control of the same threat actor.

From the three samples we researched, we were able to extract the following BTC addresses:

- 3JG36KY6abZTnHBdQCon1hheC3Wa2bdyqs
- 1Faiem4tYq7JQki1qeL1djjenSx3gCu1vk
- bc1q2n23xxx2u8hqsnvezl9rewh2t8myz4rqvmdzh2

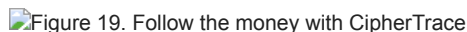
Figure 19. Follow the money with CipherTrace

Figure 19. Follow the money with CipherTrace

Ransomware Isn’t Just About Survival of the Fittest

As we have seen above, our example threat actor has evolved over time, moving from simplistic ransomware and demands in the hundreds of dollars, to toying with at least two builder leaks and ransom amounts in the thousands of dollars range.

While their activity to date suggests a low level of technical skill, the profits of their cybercrime may well prove large enough for them to make another level jump in the future.

Even if they stick with copy-pasting builders and crafting ‘stagers’, they will have the means at their disposal to create an efficient attack chain with which to compromise a company, extort money and improve their income to the point of becoming a bigger fish in a small pond, just like the larger RaaS crews.

In the meantime, such opportunistic actors will continue to bait their hooks and catch any fish they can as, unlike affiliated ransomware operators, they do not have to follow any rules in return for support (pentest documentation, software, infrastructure, etc.) from the gang’s operators. Thus, they have a free hand to carry out their attacks and, if a victim wants to bite, they don’t care about ethics or who they target.

The good news for everyone else, however, is the fact that global law enforcement isn’t gonna need a bigger boat, as it already casts its nets far and wide.

Mitre Att&ck

Technique ID	Technique Description	Observable
T1189	Drive By Compromise	The actor is using a fake Flash website to spread fake a Flash installer.
T1059.001	Command Scripting Interpreter: PowerShell	PowerShell is used to launch command lines (delete shadow copies, etc.).
T1059.007	Command and Scripting Interpreter: JavaScript	JavaScript is used in the fake Flash website to download the fake Flash installer.
T1112	Modify Registry	To disable Windows Defender, the actor modifies registry. “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender” and “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection”.
T1083	File and Directory Discovery	The actor is listing files on the victim system.
T1057	Process Discovery	The actor is listing running processes on the victim system.
T1012	Query Registry	To perform some registry modifications, the actor is first querying registry path.
T1082	System Information Discovery	Before encrypting files, the actor is listing hard drives.

T1056.001	Input Capture: Keylogging	The exfiltration tool has the capability to log user keystrokes.
T1005	Data from Local System	
T1571	Non-Standard Port	The actor is using port "1177" to exfiltrate data.
T1048	Exfiltration Over Alternative Protocol	
T1486	Data Encrypted for Impact	Data encrypted by ransomware.
T1490	Inhibit System Recovery	Delete Shadow Copies.

Detection Mechanisms

Sigma Rules

- Shadow Copies Deletion Using Operating Systems Utilities: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.yml
- Drops Script at Startup Location: <https://github.com/joesecurity/sigma-rules/blob/master/rules/dropsscriptatstartuplocation.yml>
- File Created with System Process Name: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/sysmon_creation_sysmon.yml
- Suspicious Svchost Process: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost.yml
- System File Execution Location Anomaly: https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_system_execution_location_anomaly.yml
- Delete Shadow copy via WMIC: <https://github.com/joesecurity/sigma-rules/blob/master/rules/deleteshadowcopyviawmic.yml>
- Always Install Elevated Windows Installer: https://github.com/SigmaHQ/sigma/blob/59000b993d6280d9bf063eefdcdf30ea0e83aa5e/rules/windows/process_creation/sysmon_always_install.yml

Yara Rules

Babuk Ransomware Windows

```

rule Ransom_Babuk {
meta:

description = "Rule to detect Babuk Locker"

author = "TS @ McAfee Enterprise ATR"

date = "2021-01-19"

hash = "e10713a4a5f635767dcd54d609bed977"

rule_version = "v2"

malware_family = "Ransom:Win/Babuk"

malware_type = "Ransom"

mitre_attack = "T1027, T1083, T1057, T1082, T1129, T1490, T1543.003"

strings:

$s1 = {005C0048006F007700200054006F00200052006500730074006F0072006500200059006F00750072002000460069006C00650073002E00
// \ How To Restore Your Files .txt

$s2 = "delete shadows /all /quiet" fullword wide

$pattern1 = {006D656D74617300006D65706F63730000736F70686F730000766565616D0000006261636B75700000477856737300000047784;
000047784657440000004778435644000000477843494D6772004465665761746368000000063634576744D67720000000063635365744D67;
0536176526F616D005254567363616E005142464353657276696365005142494450536572766963650000000496E747569742E517569636B4

$pattern2 =
{004163725363683253766300004163726F6E69734167656E7400000004341534144324457656253766300000434141524355706461746553

$pattern3 = {FFB0154000C78584FDFFFFB8154000C78588FDFFFFC0154000C7858CFDFFFFC8154000C78590FDFFFFD0154000C78594FD
000C78598FDFFFFE0154000C7859CFDFFFFE8154000C785A0FDFFFFF0154000C785A4FDFFFFF8154000C785A8FDFFFF00164000C785A
00C785B0FDFFFF10164000C785B4FDFFFF18164000C785B8FDFFFF20164000C785BCDFFFF28164000C785C0FDFFFF30164000C785C4
0C785C8FDFFFF40164000C785CCFDFFFF48164000C785D0FDFFFF50164000C785D4FDFFFF581640

$pattern4 = {400010104000181040002010400028104000301040003810400040104000481040005010400058104000601040006C10400078104
41040008C10400094104000A0104000B0104000C8104000DC104000E8104000F01040000011400008114000181140002411400038114000501
11400064114000741140008C114000A8114000C0114000E0114000F411400010124000281240003412400044124000541240006412400074124
24000A0124000B8124000D4124000EC1240000C1340002813400054134000741340008C134000A4134000C4134000E8134000FC134000141
4000501440006C144000881440009C144000B4144000CC144000E8144000FC144000141540003415400048154000601540007815}

condition:

filesize >= 15KB and filesize <= 90KB and

1 of ($s*) and 3 of ($pattern*)

}

```

Exfiltration Tool

```
rule CRIME_Exfiltration_Tool_Oct2021 {
meta:

description = "Rule to detect tool used to exfiltrate data from victim systems"
author = "TS @ McAfee Enterprise ATR"
date = "2021-10-04"
hash = "ceb0e01d96f87af0e9b61955792139f8672cf788d506c71da968ca172ebddccd"

strings:

$pattern1 = {79FA442F5FB140695D7ED6FC6A61F3D52F37F24B2F454960F5D4810C05D7A83D4DD8E6118ABDE2055E4D
CCFE28EBA2A11E981DB403C5A47EFB6E367C7EC48C5EC2999976B5BC80F25BEF5D2703A1E4C2E3B30CD26E92570DAF1F9BD7B48B3}

$pattern2 = {B4A6D4DD1BBEA16473940FC2DA103CD64579DD1A7EBDF30638A59E547B136E5AD113835B8294F53B8C3A
435EB2A7F649A383AA0792DD14B9C26C1BCA348920DFD37DA3EF6260C57C546CA51925F684E91239152DC05D5161A9064434}

$pattern3 = {262E476A45A14D4AFA448AF81894459F7296633644F5FD061A647C6EF1BA950FF1ED48436D1BD4976BF8
1EE84AE09D638BD2C2A01FA9E22D2015518280F6692EB976876C4045FADB71742B9579C13C7482A44A}

$pattern4 = {F2A113713CCB049AFE352DB8F99160855125E5A045C9F6AC0DCA0AB615BD34367F2CA5156DCE5CA286CC
C55E37DFCDC5AAD14ED9DAB3CDB9D15BA91DD79FF96E94588F30}

condition:

3 of ($pattern*)

}
```

IOCs

Infrastructure URLs

<http://atualziarsys.serveirc.com/Update4/>
<http://services5500.sytes.net/Update6/Update.exe.rar>
<http://suporte20082021.sytes.net/Update5/>
<http://atualziarsys.serveirc.com/update4/update.exe.rar>
<http://suporte20082021.sytes.net/Update3/>
<http://suporte01928492.redirectme.net/>
<http://atualziarsys.serveirc.com/Update3/>
<http://services5500.sytes.net/update8/update.exe.rar>
<http://suporte20082021.sytes.net/update/>
<http://suporte20082021.sytes.net/Update5/Update.exe.rar>
<http://suporte01928492.redirectme.net/AppMonitorPlugIn.rar>
<http://suporte01928492.redirectme.net/Update5/Update.exe.rar>
<http://services5500.sytes.net/update7/update.exe.rar>
<http://services5500.sytes.net/Update8/Update.exe.rar>
<http://services5500.sytes.net/Update8/Update.bat.rar>
<http://suporte01092021.myftp.biz/update/>
<http://services5500.sytes.net/Update7/Update.exe.rar>
<http://suporte01928492.redirectme.net/Update7/Update.bat.rar>
<http://suporte01928492.redirectme.net/Update7/Update.exe.rar>
<http://services5500.sytes.net/update6/update.exe.rar>
<http://suporte01092021.myftp.biz/>
<http://services5500.sytes.net/Update6/Update.bat.rar>

<http://suporte01928492.redirectme.net/update6/update.exe.rar>
<http://suporte01928492.redirectme.net/update5/update.exe.rar>
<http://services5500.sytes.net/>
<http://suporte01928492.redirectme.net/Update6/Update.exe.rar>
<http://atualziarsys.serveirc.com/Update3>
<http://atualziarsys.serveirc.com/update3/update.reg.rar>
http://24.152.38.205/pt/flashplayer28_install.zip
<http://suporte01928492.redirectme.net/Update7>
<http://atualziarsys.serveirc.com/>
<http://atualziarsys.serveirc.com/update3/mylink.vbs.rar>
<http://suporte01928492.redirectme.net/update7/update.exe.rar>
<http://atualziarsys.serveirc.com/Update4/Update.exe.rar>
<http://suporte01928492.redirectme.net/appmonitorplugin.rar>
<http://atualziarsys.serveirc.com/update3/update.exe.rar>
<http://suporte20082021.sytes.net/>
<http://suporte20082021.sytes.net/update3/update.exe.rar>
<http://atualziarsys.serveirc.com/Update4/Update.exe2.rar>
<http://suporte20082021.sytes.net/Update3/Update.exe.rar>
<http://suporte20082021.sytes.net/Update5/Update.reg.rar>
<http://atualziarsys.serveirc.com/Update4/Update.exe2.rar/>
<http://atualziarsys.serveirc.com/Update4>
<http://suporte01092021.myftp.biz/update/WindowsUpdate2.rar>
<http://suporte01092021.myftp.biz/update>
<http://atualziarsys.serveirc.com/Update3/Update.reg.rar/>
<http://atualziarsys.serveirc.com/Update3/Update.exe.rar>
<http://suporte20082021.sytes.net/Update3/Update.exe.rar/>
<http://suporte01092021.myftp.biz/update/WindowsUpdate2.rar/>
<http://atualziarsys.serveirc.com/Update4/Update.exe.rar/>
<http://atualziarsys.serveirc.com/Update3/mylink.vbs.rar>
<http://atualziarsys.serveirc.com/update4>
<http://atualziarsys.serveirc.com/update3>
<http://suporte01092021.myftp.biz/update/Update.rar>
<http://suporte01928492.redirectme.net/AppMonitorPlugIn.rar/>
<http://suporte20082021.sytes.net/update5/update.exe.rar>
<http://suporte01092021.myftp.biz/update5/update.exe.rar>
<http://atualziarsys.serveirc.com/update4/update.exe2.rar>
<http://suporte01092021.myftp.biz/update/windowsupdate2.rar>
<http://suporte20082021.sytes.net/update2/update.exe.rar>
<http://suporte20082021.sytes.net/update/windowsupdate2.rar>
<http://atualziarsys.serveirc.com/Update4/mylink.vbs.rar>
<http://atualziarsys.serveirc.com/favicon.ico>
<http://24.152.38.205/1.rar>

http://24.152.38.205/1.exe
http://appmonitorplugin.sytes.net/appmonitorplugin.rar
http://suporte20082021.sytes.net/update/WindowsUpdate2.rar
http://appmonitorplugin.sytes.net/
http://suporte20082021.sytes.net/appmonitorplugin.rar
http://suportmicrowin.sytes.net/appmonitorplugin.rar
http://suportmicrowin.sytes.net/
http://suportmicrowin.sytes.net/AppMonitorPlugIn.rar
http://appmonitorplugin.sytes.net/AppMonitorPlugIn.rar
http://24.152.38.205/pt/setup.zip

Infrastructure Domains

services5500.sytes.net
atualziarsys.serveirc.com
suporte01092021.myftp.biz
suporte20082021.sytes.net
suporte01928492.redirectme.net
suportmicrowin.sytes.net
appmonitorplugin.sytes.net

Infrastructure IPs

149.56.147.236
24.152.38.205
54.38.122.66
149.56.38.168
149.56.38.170
24.152.36.48
66.70.170.191
66.70.209.174
142.44.129.70
51.79.107.245
46.105.36.189
178.33.108.239
54.39.193.37
24.152.37.115
144.217.139.134
24.152.36.58
51.38.19.201
51.222.97.177
51.222.53.150
144.217.45.69
87.98.137.173

144.217.199.24
24.152.37.19
144.217.29.23
198.50.246.8
54.39.163.60
54.39.84.55
24.152.36.30
46.105.38.67
24.152.37.96
51.79.63.229
178.33.107.134
164.132.77.246
54.39.163.58
149.56.113.76
51.161.120.193
24.152.36.210
176.31.37.238
176.31.37.237
24.152.36.83
24.152.37.8
51.161.76.193
24.152.36.117
137.74.246.224
51.79.107.134
51.79.44.49
51.222.173.152
51.79.124.129
51.79.107.242
51.222.173.148
144.217.117.172
54.36.82.187
54.39.152.91
54.36.82.177
142.44.146.178
54.39.221.163
51.79.44.57
149.56.38.173
24.152.36.46
51.38.19.198
51.79.44.59
198.50.246.11
24.152.36.35

24.152.36.239
144.217.17.186
66.70.209.169
24.152.36.158
54.39.84.50
51.38.19.200
144.217.45.68
144.217.111.5
54.38.164.134
87.98.171.7
51.79.124.130
66.70.148.142
51.255.119.19
66.70.209.168
54.39.239.81
24.152.36.98
51.38.192.225
144.217.117.10
144.217.189.108
66.70.148.136
51.255.55.134
54.39.137.73
66.70.148.137
54.36.146.230
51.79.107.254
54.39.84.52
144.217.61.176
24.152.36.150
149.56.147.236
51.38.19.196
54.39.163.57
46.105.36.133
149.56.68.191
24.152.36.107
158.69.99.10
51.255.55.136
54.39.247.244
149.56.147.204
158.69.99.15
144.217.32.24
149.56.147.205
144.217.32.213

54.39.84.53
79.137.115.160
144.217.233.98
51.79.44.56
24.152.36.195
142.44.146.190
144.217.139.13
54.36.82.180
198.50.246.14
137.74.246.223
24.152.36.176
51.79.107.250
51.161.76.196
198.50.246.12
66.70.209.170
66.70.148.139
51.222.97.189
54.39.84.49
144.217.17.185
142.44.129.73
144.217.45.67
24.152.36.28
144.217.45.64
24.152.37.39
198.27.105.3
51.38.8.75
198.50.204.38
54.39.221.11
51.161.76.197
54.38.122.64
91.134.217.71
24.152.36.100
144.217.32.26
198.50.246.13
54.36.82.188
54.39.84.25
66.70.209.171
51.38.218.215
54.39.8.92
51.38.19.205
54.39.247.228
24.152.36.103

24.152.36.104
51.79.44.43
54.39.152.202
66.70.134.218
24.152.36.25
149.56.113.79
178.32.243.48
144.217.45.66
66.70.173.72
176.31.37.239
54.38.225.81
158.69.4.173
24.152.37.189
54.36.146.129
198.50.246.15
51.222.102.30
51.79.105.91
51.79.9.91
51.222.173.151
51.79.107.124
51.222.173.142
144.217.17.187
149.56.85.98
51.79.107.244
144.217.158.195
24.152.36.178
192.95.20.74
51.79.117.250

Ransomware Hashes

106118444e0a7405c13531f8cd70191f36356581d58789dfc5df3da7ba0f9223
e1c449aa607f70a9677fe23822204817d0ff41ed3047d951d4f34fc9c502f761
ae6020a06d2a95cbe91b439f4433e87d198547dec629ab0900ccfe17e729cff1
c3776649d9c0006caba5e654fa26d3f2c603e14463443ad4a5a08e4cf6a81994
63b6a51be736d253e26011f19bd16006d7093839b345363ef238eafcf5e7e85
94fe0825f26234511b19d6f68999d8598a9c21d3e14953731ea0b5ae4ab93c4d
c8d97269690d3b043fd6a47725a61c00b57e3ad8511430a0c6254f32d05f76d6
67bc70d4141d3f6aaf8f17963d56df5cee3727a81bc54407e90fdf1a6dc8fe2a
98a3ef26b346c4f47e5dfdba4e3e26d1ef6a4f15969f83272b918f53d456d099
c3c306b2d51e7e4f963a6b1905b564ba0114c8ae7e4bb4656c49d358c0f2b169

Bitcoin Addresses

3JG36KY6abZTnHBdQCon1hheC3Wa2bdyqs
1Faiem4tYq7JQki1qeL1djjenSx3gCu1vk

bc1q2n23xxx2u8hqsnevezl9rewh2t8myz4rqvmdzh2

PDB

C:\Users\workdreams\Desktop\Testes\Crypt_Final\Crazy_Crypt\Crazy\obj\Debug\AppMonitorPlugIn.pdb
C:\Users\workdreams\Desktop\test\Nopyfy-Ransomware-master\Nopyfy-Ransomware\Nopyfy-Ransomware\obj\Debug\Nopyfy-Ransomware.pdb

PowerShell Script

a8d7b402e78721443d268b682f8c8313e69be945b12fd71e2f795ac0bcadb353

Exfiltration Tool

ceb0e01d96f87af0e9b61955792139f8672cf788d506c71da968ca172ebddccd
c3323fbd0d075bc376869b0ee26be5c5f2cd4e53c5efca8ecb565afa8828fb53

Fake Flash Player installer

d6c35e23b90a7720bbe9609fe3c42b67d198bf8426a247cd3bb41d22d2de6a1f

Fake Anydesk Installer

e911c5934288567b57a6aa4f9344ed0f618ffa4f7dd3ba1221e0c42f17dd1390