Campaign Abusing Legitimate Remote Administrator Tools Uses Fake Cryptocurrency Websites

trendmicro.com/en_us/research/21/k/campaign-abusing-rats-uses-fake-websites.html

November 29, 2021

Malware

We have been tracking a campaign involving the SpyAgent malware that abuses well-known remote access tools (RATs) for some time now. While previous versions of the malware have been covered by other researchers, our blog entry focuses on the malicious actor's latest attacks.

By: Jaromir Horejsi November 29, 2021 Read time: (words)

Introduction

We have been tracking a campaign involving the SpyAgent malware that abuses well-known remote access tools (RATs) — namely TeamViewer — for some time now. While previous versions of the malware have been covered by other researchers, our blog entry focuses on the malicious actor's latest attacks.

We've observed a new cryptocurrency related campaign that abuses a legitimate Russian RAT known as Safib Assistant via a newer version of the malware called SpyAgent. This involves the exploit of a DLL sideloading vulnerability, which causes a malicious DLL to load. This DLL hooks and patches various API functions called by the RAT. This results in the RAT windows being hidden from a user.

The malicious DLL then begins reporting the RAT's ID, which the malware operator needs to connect to and control the infected machine. The malware sets the access password to a fixed one, so that merely knowing the RAT's ID is enough for the attacker to successfully connect to the infected machine.

Infection vector

The malware dropper of SpyAgent is distributed via fake cryptocurrency-related websites that are usually in the Russian language. The dropper poses as a fake cryptocurrency wallet, miner, or surfing plug-in. Figures 1 to 4 are some examples of these fake websites.

argent

Установить Argent

**Мультифункциональный криптокошелек**

Все монеты в одном кошельке

Оплачивайте без комиссии и выводите ваши монеты в любое направление мгновенно!

Получите в подарок 30$ которые Вы можете обменять и вывести мгновенно!

Установить Argent

Phantom

Мультивалютный Phantom

Первый мультивалютный кошелёк с возможностью онлайн заработка в интернете и бонусом 200 DOGE за установку

Добавить в Chrome

Wallet 1 (BP1z...cGvC)

SOL $10,230.92
         +$1,399.22

oin $7,281.49
DC   +$2.01
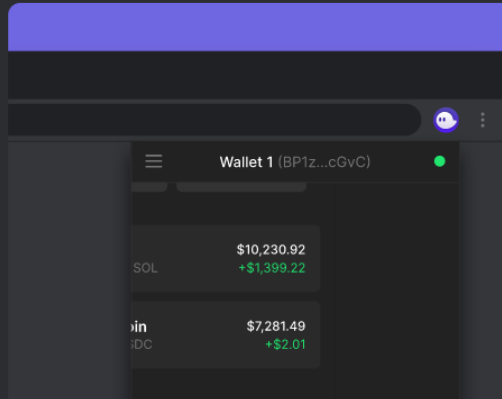
Превратите свой браузер в крипто заработок

ГЛАВНАЯ ПРИЛОЖЕНИЕ КРИПТОНАТОР

Получите подарок от Криптонатора

Установив расширение для серфинга и заработка криптовалюты

|		
50$	**~285**	**0,23$**
За установку приложения моментально на счёт Bitcoin	Сайтов доступны для серфинга прямо сейчас	Доход за каждый просмотренный сайт

Figure 1. Fake cryptocurrency wallets in Russian

DOGE MINER PRO
CPU & GPU DOGE MINER С АВТОМАТИЧЕСКИМИ ВЫПЛАТАМИ

ЗАРАБАТЫВАЙТЕ ОТ 50 DOGE В ДЕНЬ, ДОБЫВАЯ
МОНЕТЫ DOGE НА СВОЕМ ОБОРУДОВАНИИ.
НАШ МАЙНЕР ДАЕТ МАКСИМАЛЬНУЮ СКОРОСТЬ ЗАРАБОТКА
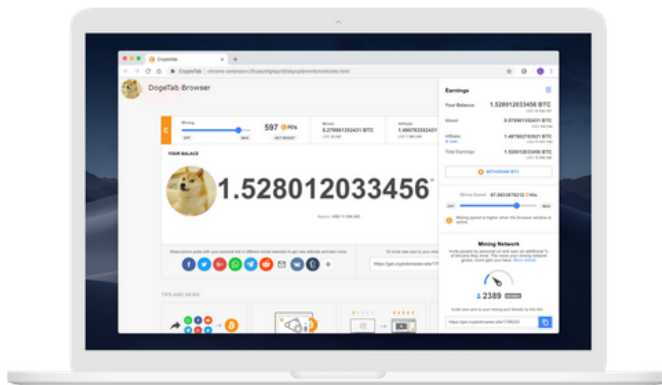ЗА СЧЕТ ИСПОЛЬЗОВАНИЯ НЕ ТОЛЬКО CPU, НО И GPU.

! ВНИМАНИЕ !
ПЕРВЫЕ 1000 ЧЕЛОВЕК ПОЛУЧАЮТ НА СВОЙ БАЛАНС БОНУС В
100 DOGE!!

⬇ Скачать DogeMine Pro v1.0

СТАТУС- РАБОТАЕТ
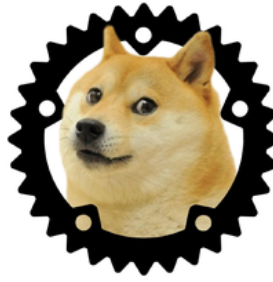
Попробуйте новый DogeTab Браузер со встроенным алгоритмом майнинга и увеличьте скорость до 8 раз по сравнению с Google Chrome. Легкий, быстрый и готовый к майнингу!

Установите **DogeTab Браузер**® и получите увеличенную скорость майнинга в сочетании со знакомым интерфейсом и функциями Chrome, а также 100 DOGE в подарок!

⬇ ЗАГРУЗИТЕ DOGETAB БРАУЗЕР

Загрузка и настройка занимает менее минуты.

Figure 2. Fake cryptocurrency miners in Russian

DOGECOIN   ГЛАВНАЯ   НАШИ ПРЕИМУЩЕСТВА

Уникальный серфинг плагин для заработка DogeCoin

Начните получать DogeCoin уже спустя час работы
Получите 100 DOGE в подарок после установки плагина

Установить на Chrome   ⭘ Установить на другие браузеры

Figure 3: Fake surfing plug-in to earn dogecoin

Figure 4. Fake surfing plug-ins to earn bitcoin

When a user visits one of these websites, a file-downloading dialog box (offering to download a SpyAgent dropper) usually appears immediately, after which the victim is prompted to save and run the executable file.

How a victim winds up on these fake websites varies. One kind of social engineering technique that we observed involves advertisements published on "earn cryptocurrency for browsing" websites, such as the ad in Figure 5. It should be noted that not all websites offering cryptocurrency in exchange for views are necessarily malicious. In the following screenshot, however, the screenshot shows a malicious website that promotes a fake cryptocurrency-related website.
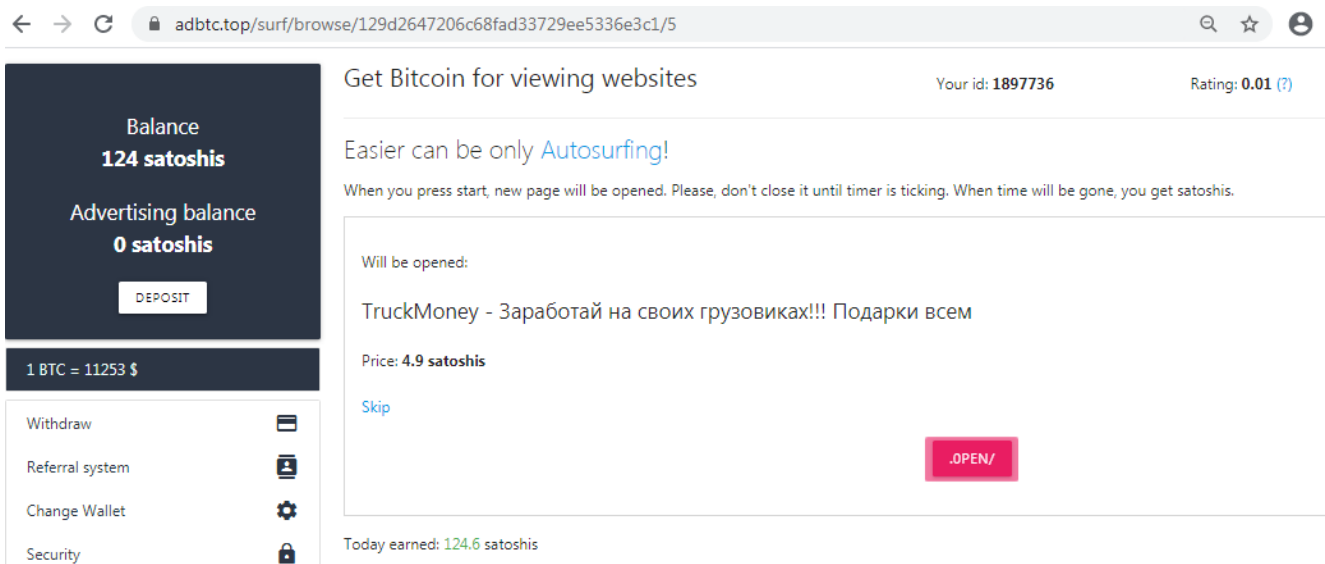

Figure 5. Malicious advertisement leading to the malicious website

After opening the link, the victim is immediately redirected to one of the fake cryptocurrency websites where a dialog box for saving the fake application immediately appears.
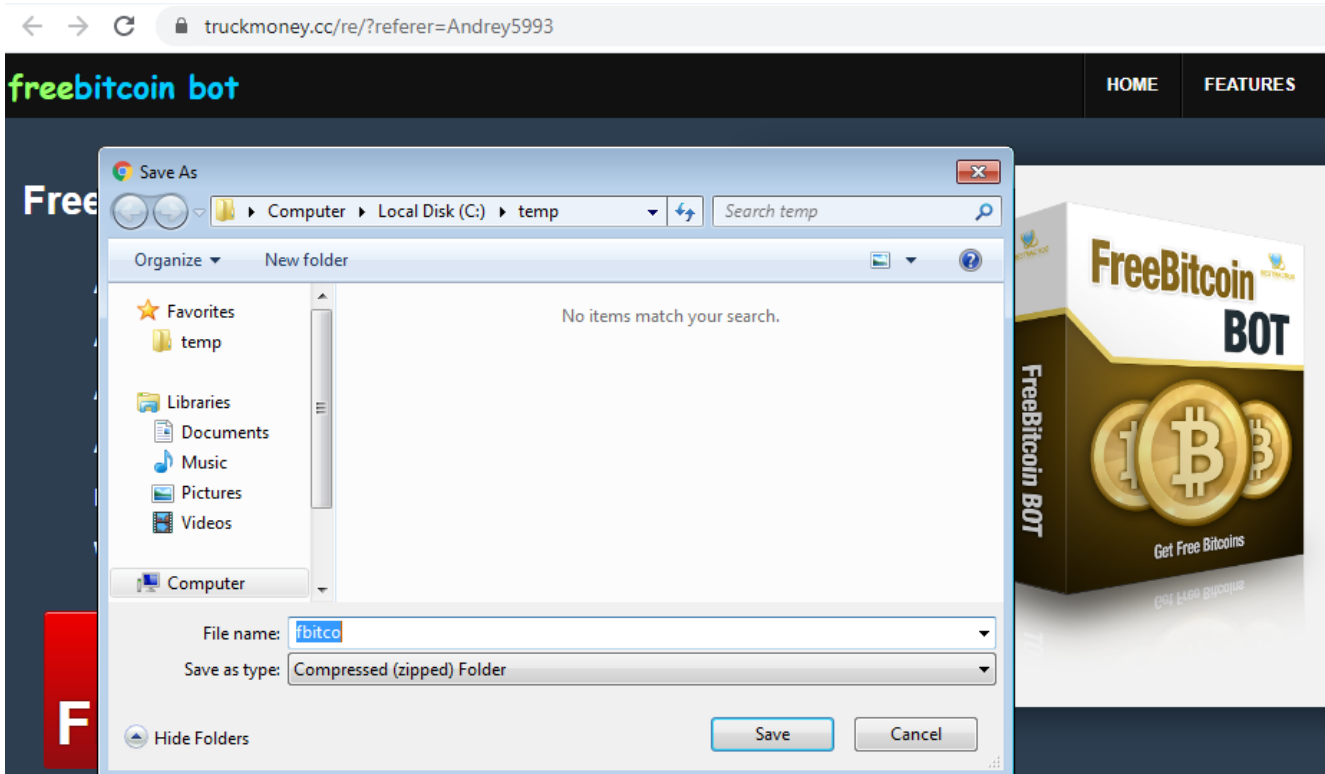
Figure 6. Website with a fake bitcoin bot

Social media is also used as an infection vector, as shown in the tweet in Figure 7. Interestingly, the Twitter account behind it seems to be legitimate, although possibly compromised.

Figure 7. User

spreading a link to a fake website via Twitter

Due to search engine optimization (SEO), simply searching for the right keywords might result in the inclusion of these websites in search results.

https://omnitailer.com · Translate this page

Doge Miner Pro

Doge Miner Pro · Зарабатывайте от 50 DOGE в день, добывая монеты DOGE на своем оборудовании.Наш майнер дает максимальную скорость заработка за счет...

Figure 8. Search engine returning the link to a fake "Doge Miner" website

Dropper analysis

The dropper is usually created using the Nullsoft Scriptable Install System (NSIS) installer (although in the past we have seen variants created with Inno Setup), a powerful tool for creating scriptable program installers. The dropper (NSIS installer) file contains just one randomly named encrypted binary file.

Name	Size	Packed Size
$PLUGINSDIR	0	224 726
6082og1r.bin		6 401 017

Figure 9. Installer with one randomly named binary file

The NSIS installer script then calls Microsoft CryptoAPIs to decrypt the binary file, which then becomes a 7-Zip archive that will extract the files. Figure 10 shows a string (tno7wul0zusmglmdl) used for deriving the decryption key on line 578.

```
575    ..File.6082og1r.bin
576    ..SendMessage.$_13_.0x0180.0.STR:111
577    ..SendMessage.$_13_.0x0180.0.STR:222
578    ..StrCpy.$_24_.tno7wul0zusmglmdl
579    ..SendMessage.$_13_.0x0180.0.STR:333
580    ..Push.$_24_
581    ..Push.$TEMP\6082og1r.bin
582    ..Call.func_299
```

Figure 10. Code showing a password to derive the RC4 decryption key used to decrypt random binary files

This string is then hashed with MD5 algorithm (see constant 0x00008003).

```
454    ..StrCpy.$8.2::CryptC
455    ..System::Call.ADVAPI3$8reateHash(ir4,i0x00008003,i0,i0,*i.r5)i.r0
456    ....;.Call.Initialize_____Plugins
```

Figure 11. MD5 hashing of the password

```
471    ..StrCpy.$8.2::CryptE
472    ..System::Call.ADVAPI3$8eriveKey(ir4,i0x00006801,ir5,i0x280011,*i.r6)i.r0
473    ....;.Call.Initialize_____Plugins
```

Figure 12. Deriving RC4 key

The dwFlags parameter (see value 0x280011) tells us the length of the key modulus in bits, which is set with the upper 16 bits (0x28 / 8 = 40 / 8 = 5 bytes). Lower 16 bits are flags CRYPT_EXPORTABLE and CRYPT_NO_SALT.

Therefore, the first five bytes of the MD5 of the string for key derivation is the RC4 key used to decrypt the 7-Zip archive.

The sizes of a session key can be set when the key is generated. The key size, representing the length of the key modulus in bits, is set with the upper 16 bits of this parameter. Thus, if a 128-bit RC4 session key is to be generated, the value

Figure 13. Documentation explaining the computation of the length of the key

The extracted 7-Zip archive contains several files, most of which are legitimate non-malicious files belonging to the RAT. In Figure 14, only those files in red indicate the additions by malware developers.

The batch file (.bat) is a starter of the main executable (Assistant, ast.exe) file, while the Config file (.cfg) contains encrypted configuration. The bitmap file (.bmp) is used for deriving the key to decrypt the config file. Finally, the quartz.dll is the malicious DLL containing the malware that is

sideloaded by ast.exe. Although the real length of the quartz DLL is several dozens of kilobytes, its length is artificially inflated by appending a huge overlay of zeroes. This is likely to prevent or discourage some security solutions from uploading these large files for further analysis.

Figure 14. Contents of the 7-Zip archive with the RAT. The files in red are the ones added by the malware developer.

Analysis of the sideloaded DLL

The DLL is responsible for decrypting the config file. Initially, the first byte of the config file is checked. If its value is 0x01, it means that the malware runs for the first time and the config file is encrypted with a key derived from the bitmap file.

Otherwise, if the value of the first byte in the config file is 0x00, it means that the config file is encrypted with a key derived from the *SOFTWARE\Microsoft\Cryptography\MachineGuid* value.

The key derivation has four steps:

1) The CRC32 checksum of the input (.bmp file) is computed.

2) The checksum is converted to a hexadecimal string (eight characters), and all characters are converted to uppercase.

3) The MD5 hash is computed.

4) The hexadecimal string representation of the hash (32 characters) is used as the RC4 password to decrypt the config file.

After decryption, the configuration file contains the URL address of the command-and-control (C&C) server. From this URL address, the domain part is used as a key for another decryption — this time the decryption of part of the DLL's executable code, since a part of the DLL is a self-modifying code.

Figure 15. Function call to the encrypted code before decryption (top) and after decryption (bottom)

The first decrypted function is responsible for resolving the API function addresses, while the second decrypted function is responsible for hooking various functions and altering the default behavior of the RAT.

The following table shows the important hooked functions and their effects on the RAT:

Function	Details
RegCreateKeyEx	Changes the registry using the RAT configuration from **\ast\SS** to **\ast\SS1**
RegSetValueKeyEx	Extracts the RAT's ID when it is saved to the registry. It then starts two threads, a C&C communication thread and an idleness monitoring thread.
FindWindow	Ensures that the RAT's window is not shown
RegisterClass	Ensures that the RAT's window is not shown
ShowWindow	Disables showing the RAT's windows
CreateFile	Disables the log file that the RAT creates by default

GetCommandLine	Sets command-line parameters to start the RAT as a hidden process in the background, sets the connection password stored in registry to a known fixed password, and starts a thread responsible for killing task manager and process explorer

Table 1. The important hook functions of the decrypted function

When the RAT is run normally and is not hijacked by malware, a window like the screenshot shown in Figure 17 will appear. It is important to note the nine-digit number (captured by the hook of RegSetValueKeyEx) and the four-digit number (overridden by the registry setting set by the hook of GetCommandLine). This window is not shown at all as an effect of hooking FindWindow, RegisterClass, and ShowWindow.
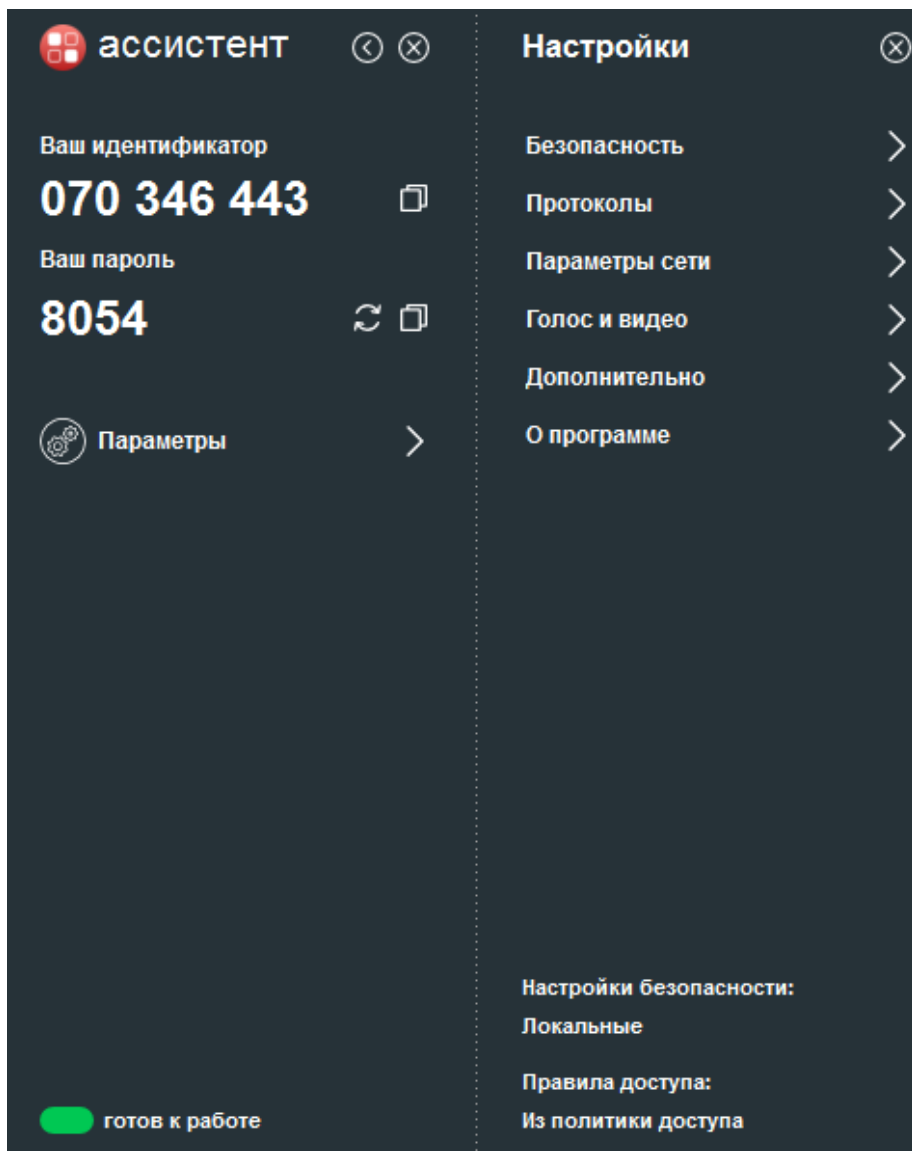

Figure 16. The RAT's window when it is run normally. The nine-digit number is the ID and the four-digit number is the password.

Finally, we will analyze the two threads. The C&C communication thread regularly makes a GET request to <C&C domain>/<C&C path>?id=<9digit number>&stat=<environment hash>. The environment hash is computed as an MD5 hash of string created by concatenating the following

five values:

> Value 1 = to_uppercase(crc32(*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid*))
> Value 2 = to_uppercase(crc32(*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName*))
> Value 3 = to_uppercase(crc32(user name))
> Value 4 = to_uppercase(crc32(computer name))
> Value 5 = concatenate Value1 Value2 Value3 Value4

It might receive a response in the following format:

> !lexec;<url to download>
restart
delproc

The idleness monitoring thread monitors pressed keys and selecting or dragging movements. If the user is idle for more than one minute, it sends a sidl(start idle) request with the time when the user became idle:

> <C&C domain>/<C&C path>?id=<9digit number>&stat=<environment hash>&sidl=<time>

The length of idleness is then regularly submitted in a cidl (count of idle) parameter:

> <C&C domain>/<C&C path>?id=<9digit number>&stat=<environment hash>&cidl=<number of seconds>

When the user becomes active again, the malware sends an eidl (end of idle) request:

> <C&C domain>/<C&C path>?id=<9digit number>&stat=<environment hash>&eidl= <time>&cidl=<number of seconds>

The idleness monitoring thread allows the malware operator to choose the proper time when the victim is not present in order to stay unnoticed.

Associated malware

SpyAgent usually downloads other malware to perform additional tasks such as stealing important data.

We noticed using SpyAgent downloading the following commodity stealers:

- RedLine Stealer
- Ducky stealer
- AZOrult
- Cypress Stealer
- Clipper (a clipboard replacer that replaces various cryptocurrency addresses with those controlled by the malicious actor)

We also noticed other RATS being used in the campaign, such as:

- Remcos RAT
- NanoCore
- njRAT
- AsyncRAT

Conclusion

The threat actor behind this malware seems to have a straightforward financial motivation and typically aims to steal credentials and cryptocurrency wallets while also replacing cryptocurrency addresses shared via clipboard.

Fortunately, defending oneself against these attacks is also straightforward. Given the malicious actor's use of traditional social engineering techniques such as fake websites, malicious advertisements, and spurious social media posts, users should practice due diligence and avoid selecting any suspicious links or visiting dubious websites. We also encourage users to perform security best practices such as bookmarking trusted sites and practicing caution when visiting new websites, especially those that are prone to being abused for social engineering attacks.

Indicators of Compromise (IOCs)

The IOCs used in this analysis can be found here.