Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries

The BlackBerry Research & Intelligence Team ⁝⁝ 10/23/2022

Summary

The previously unknown RomCom RAT threat actor is now targeting Ukrainian military institutions. The same threat actor is known to deploy spoofed versions of popular software "Advanced IP Scanner." After being publicly exposed, it switched to another popular application called "PDF Filler." That indicates the group behind it is actively developing new capabilities.

Context

The initial "Advanced IP Scanner" campaign occurred on **July 23, 2022**. Once the victim installs a Trojanized bundle, it drops RomCom RAT to the system. On **October 10, 2022**, the threat actor improved evasion techniques by obfuscation of all strings, execution as a COM object, and others.

Attack Vector

Earlier versions of RomCom RAT were distributed via fake websites spoofing the legitimate "Advanced IP Scanner" application website. The Trojanized "Advanced IP Scanner" package was hosted on "advanced-ip-scaner[.]com" and "advanced-ip-scanners[.]com" domains. Both of those domains historically resolved to the same IP address of 167[.]71[.]175[.]165. The threat actor also ensured that both fake websites looked near identical to the original one - "advanced-IP-scanner.com."

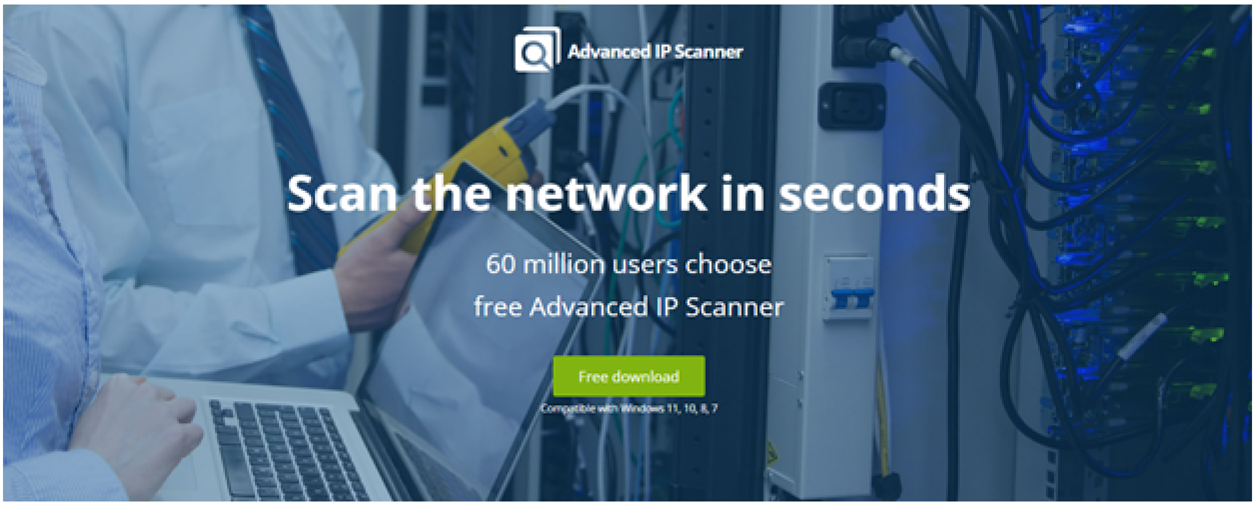


Figure 1 – Fake “Advanced IP Scanner” website

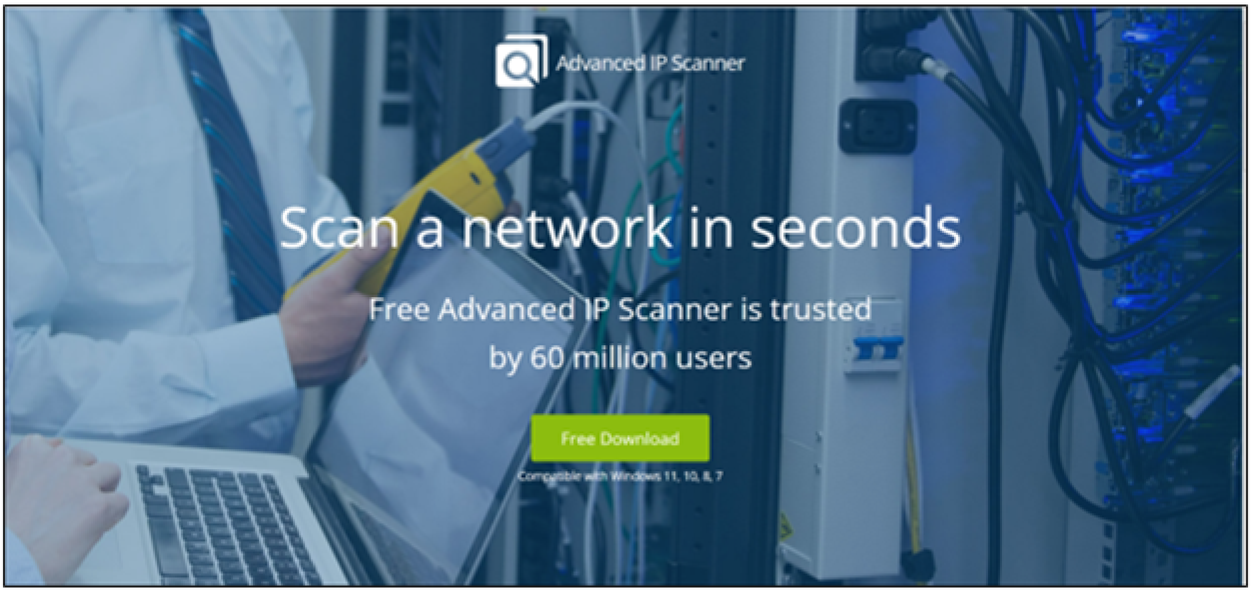

Advanced IP Scanner
Scan a network in seconds
Free Advanced IP Scanner is trusted
by 60 million users
Free Download
Compatible with Windows 11, 10, 8, 7

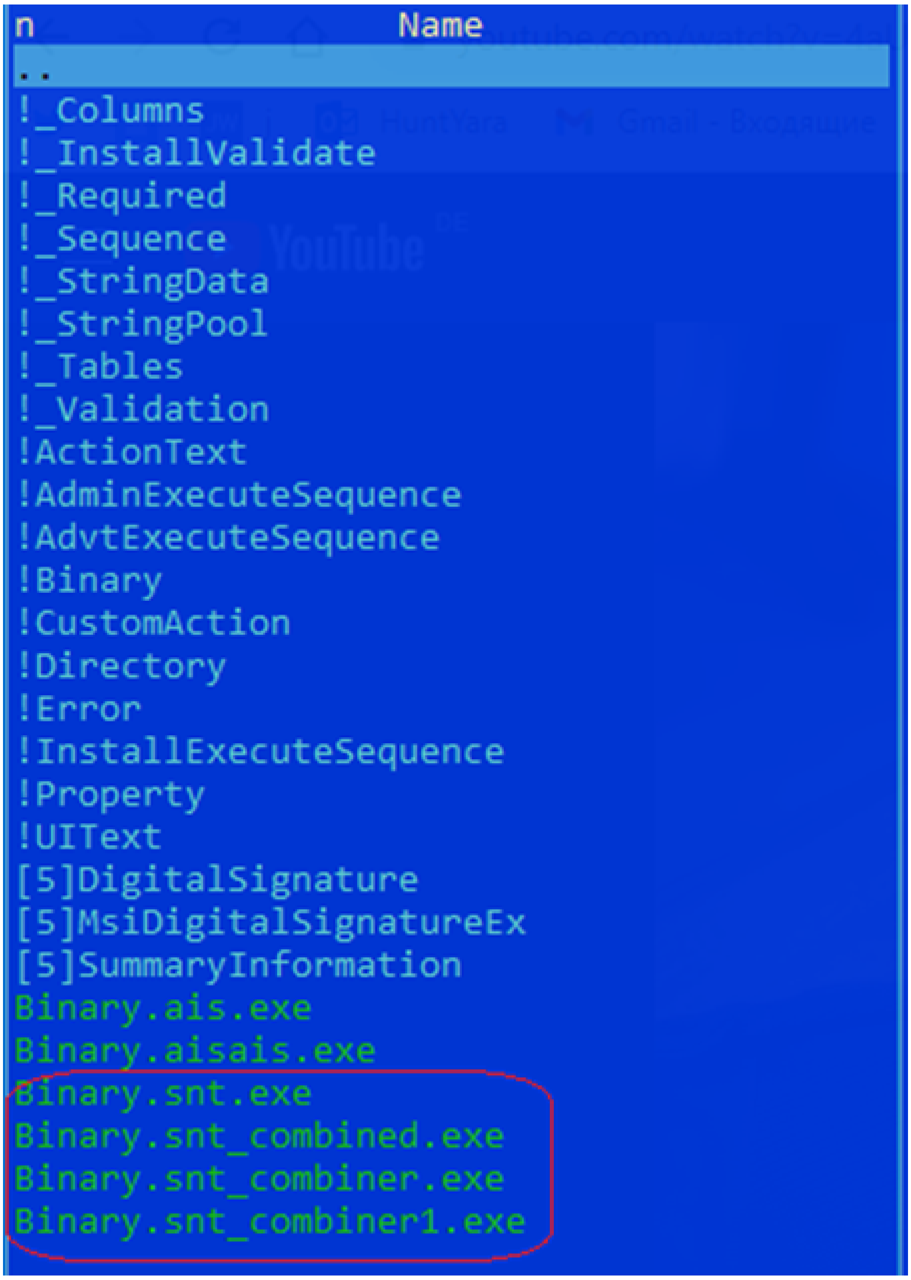
Figure 2 – Legitimate “Advanced IP Scanner” website

On **October 20th**, the threat actor deployed a new campaign spoofing the "pdfFiller" website, dropping a Trojanized version with RomCom RAT as the final payload.

Weaponization

The earliest versions of RomCom RAT came in the "Advanced IP Scanner" package. The BlackBerry Research and Intelligence team has identified two versions of it – "Advanced_IP_Scanner_V2.5.4594.1.zip" and "advancedipscanner.msi." The threat actor spoofed the legitimate tools named "Advanced_IP_Scanner_2.5.4594.1.exe" by adding a single letter "V" to the file's name.

Once unpacked, it contains 27 files, of which four are malicious droppers.



```
n               Name
..
!_Columns
!_InstallValidate
!_Required
!_Sequence
!_StringData
!_StringPool
!_Tables
!_Validation
!ActionText
!AdminExecuteSequence
!AdvtExecuteSequence
!Binary
!CustomAction
!Directory
!Error
!InstallExecuteSequence
!Property
!UIText
[5]DigitalSignature
[5]MsiDigitalSignatureEx
[5]SummaryInformation
Binary.ais.exe
Binary.aisais.exe
Binary.snt.exe
Binary.snt_combined.exe
Binary.snt_combiner.exe
Binary.snt_combiner1.exe
```

Figure 3 – Content of Trojanized "Advanced IP Scanner." RomCom RAT droppers are highlighted

Dropper RomCom extracts the payload from its resources and creates it in the following folder:

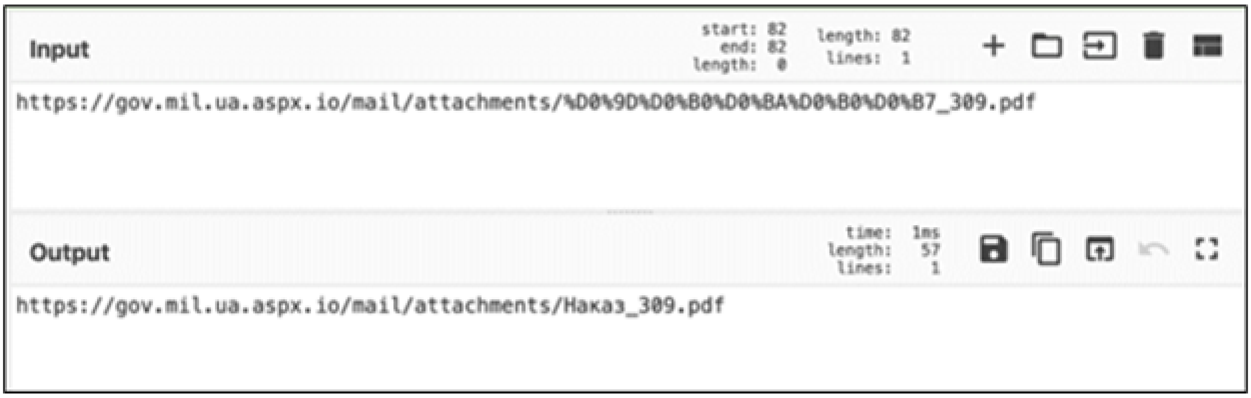
C:\Users\Username\AppData\Local\Temp\winver.dll

Main RomCom functionalities include, but are not limited to, gathering system information (disk and files information enumeration), and information about locally installed applications and memory processes. It also takes screenshots and transmits collected data to the hardcoded command-and-control (C2). If a special command is received, it supports auto-deletion from the victim's machine.

The latest version of RomCom RAT has been bundled in the "**PDFFiller.zip**" package.

Connection with Attacks on Military Institutions in Ukraine.

On October 21, the threat actor behind the RomCom RAT targeted the military institutions of Ukraine. The initial infection vector is an email with an embedded link leading to a fake website dropping the next stage downloader. The lure is a fake document in the Ukrainian language called "**Наказ_309.pdf**" (translated to English as "Order_309.pdf").

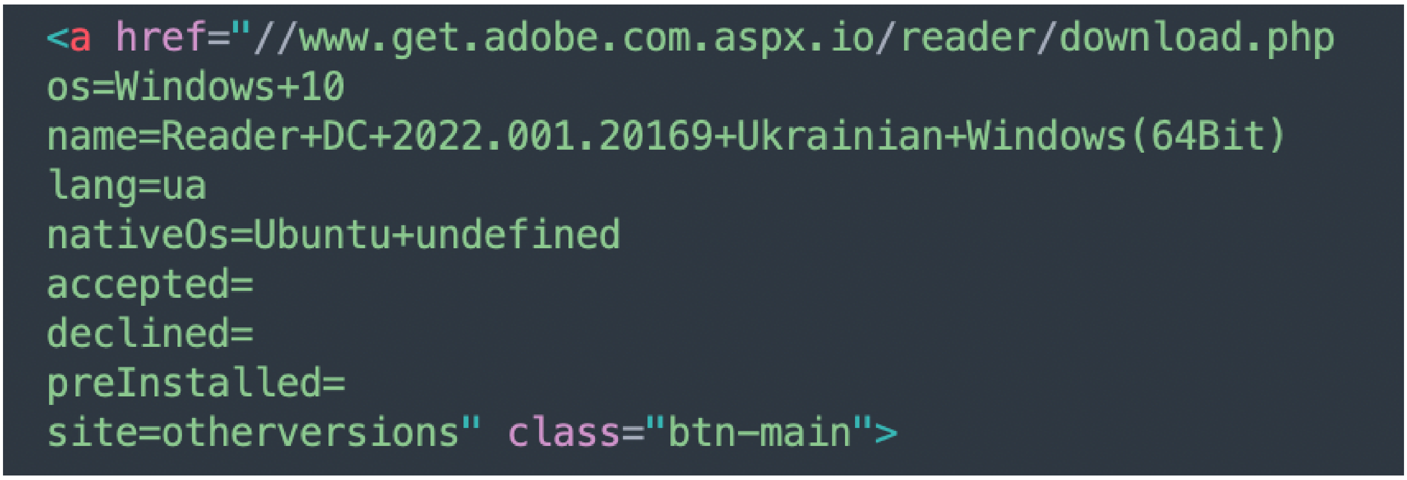


```
https://gov.mil.ua.aspx.io/mail/attachments/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7_309.pdf
```

```
https://gov.mil.ua.aspx.io/mail/attachments/Наказ_309.pdf
```

Figure 4 – The original link leads with a lure in the Ukrainian language spoofing the original Ministry of Defense of Ukraine Website

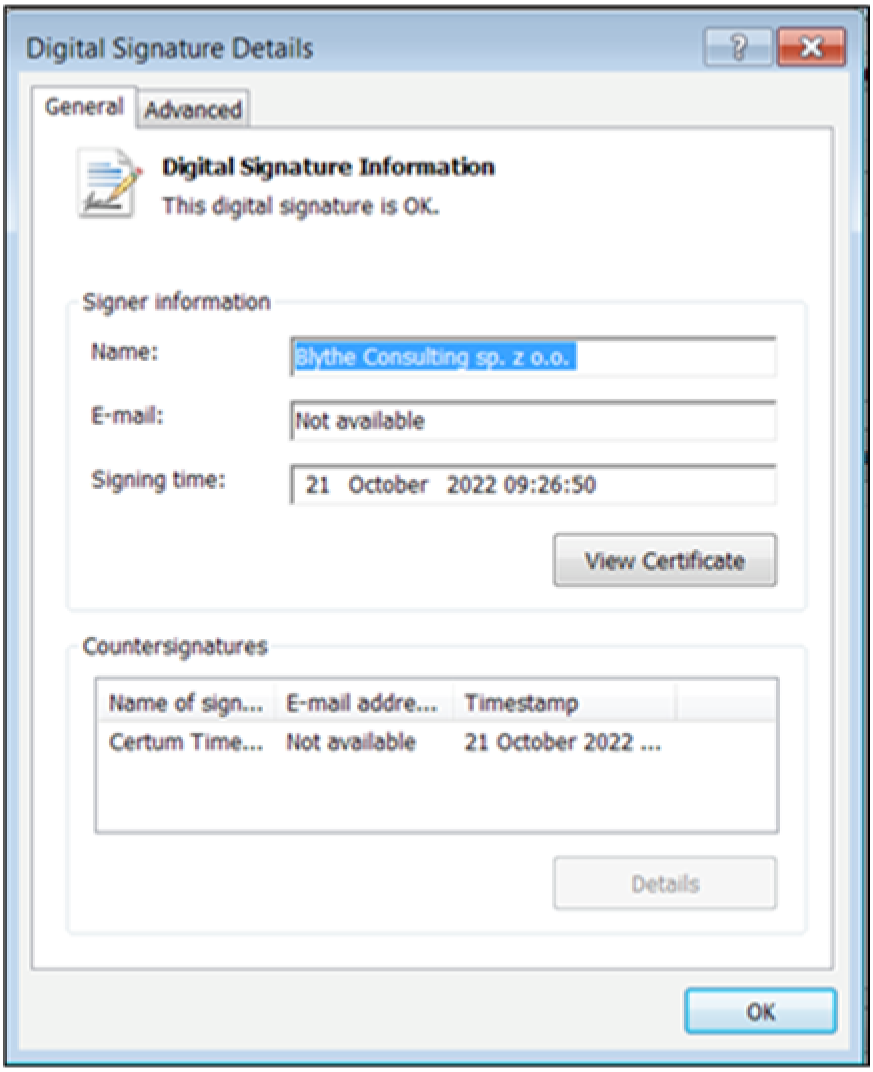
That is an HTML file with a download URL of the next stage malicious Portable Executable (PE) file.



```
<a href="//www.get.adobe.com.aspx.io/reader/download.php
os=Windows+10
name=Reader+DC+2022.001.20169+Ukrainian+Windows(64Bit)
lang=ua
nativeOs=Ubuntu+undefined
accepted=
declined=
preInstalled=
site=otherversions" class="btn-main">
```

Figure 5 – Part of the HTML code from the initial "Наказ_309.pdf" lure

Dropped malicious "AcroRdrDCx642200120169_uk_UA.exe" file has a valid digital signature by Signer "Blythe Consulting sp. z o.o.".



Digital Signature Information
This digital signature is OK.

Signer information

Name:	Blythe Consulting sp. z o.o.
E-mail:	Not available
Signing time:	21 October 2022 09:26:50

Countersignatures

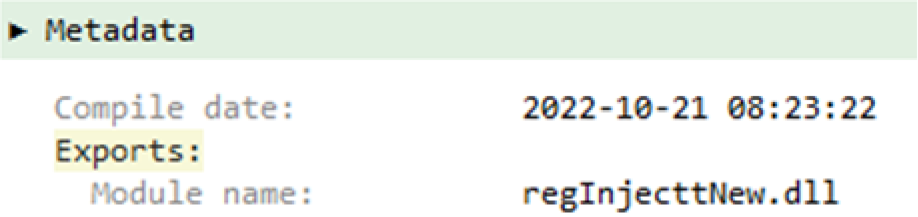
Name of sign...	E-mail addre...	Timestamp
Certum Time...	Not available	21 October 2022 ...

Figure 6 – Malicious “AcroRdrDCx642200120169_uk_UA.exe” with a valid digital signature

Upon execution, it drops the following file: "C:\Users\Public\Libraries\WinApp.dll". The dropped "WinApp.dll" file contains a single export – "fwdTst". By invoking the "rundll32.exe" proce3ss, the export is run. Just like previously, the RomCom RAT final payload is extracted from the resource and saved as "C:\Users\Public\Libraries\rtmpak.dll".

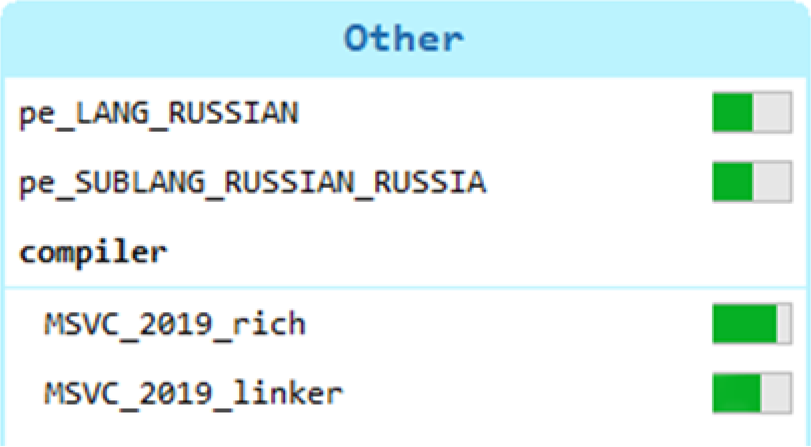
A legitimate clean "pdfFiller" application uses the same signer, "Blythe Consulting sp. z o.o.". As mentioned above, the app has been abused in the latest campaigns by the RomCom RAT threat actor.

Both RomCom RAT droppers and the final RAT include as language and locale Russian and Russian from Russia languages:



```
▶ Metadata

  Compile date:           2022-10-21 08:23:22
  Exports:
    Module name:          regInjecttNew.dll
```



Other

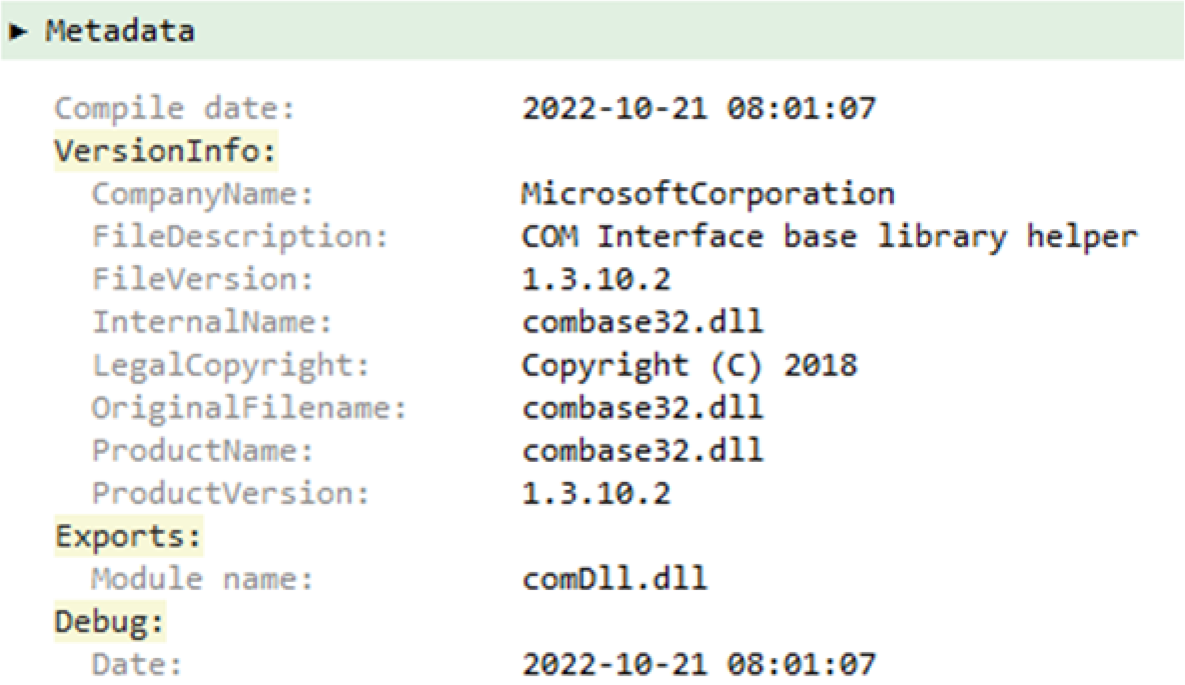
pe_LANG_RUSSIAN

pe_SUBLANG_RUSSIAN_RUSSIA

compiler

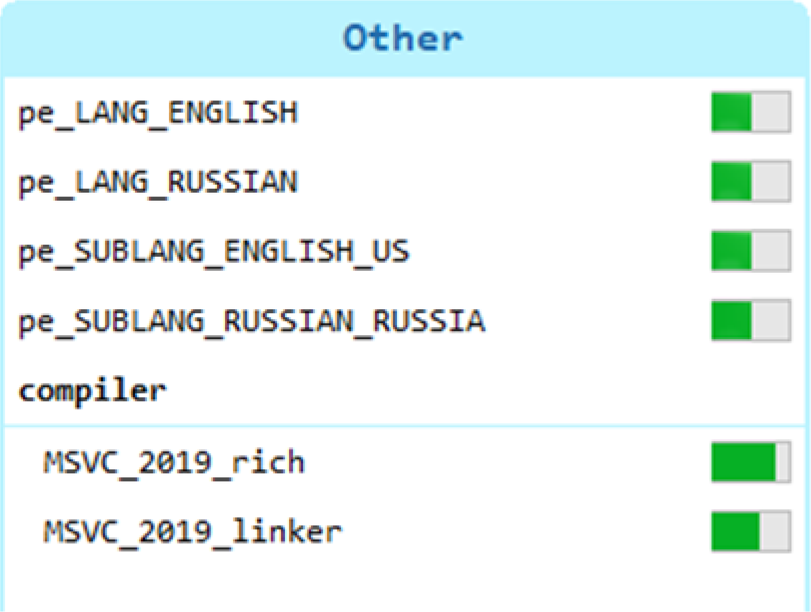
MSVC_2019_rich

MSVC_2019_linker



```
▶ Metadata

  Compile date:             2022-10-21 08:01:07
  VersionInfo:
    CompanyName:            MicrosoftCorporation
    FileDescription:        COM Interface base library helper
    FileVersion:            1.3.10.2
    InternalName:           combase32.dll
    LegalCopyright:         Copyright (C) 2018
    OriginalFilename:       combase32.dll
    ProductName:            combase32.dll
    ProductVersion:         1.3.10.2
  Exports:
    Module name:            comDll.dll
  Debug:
    Date:                   2022-10-21 08:01:07
```



Other

pe_LANG_ENGLISH

pe_LANG_RUSSIAN

pe_SUBLANG_ENGLISH_US

pe_SUBLANG_RUSSIAN_RUSSIA

compiler

MSVC_2019_rich

MSVC_2019_linker

Targets

Besides the latest campaign against military institutions from Ukraine, we have found the RomCom threat actor targeting IT companies, food brokers, and food manufacturing in the U.S., Brazil, and the Philippines.

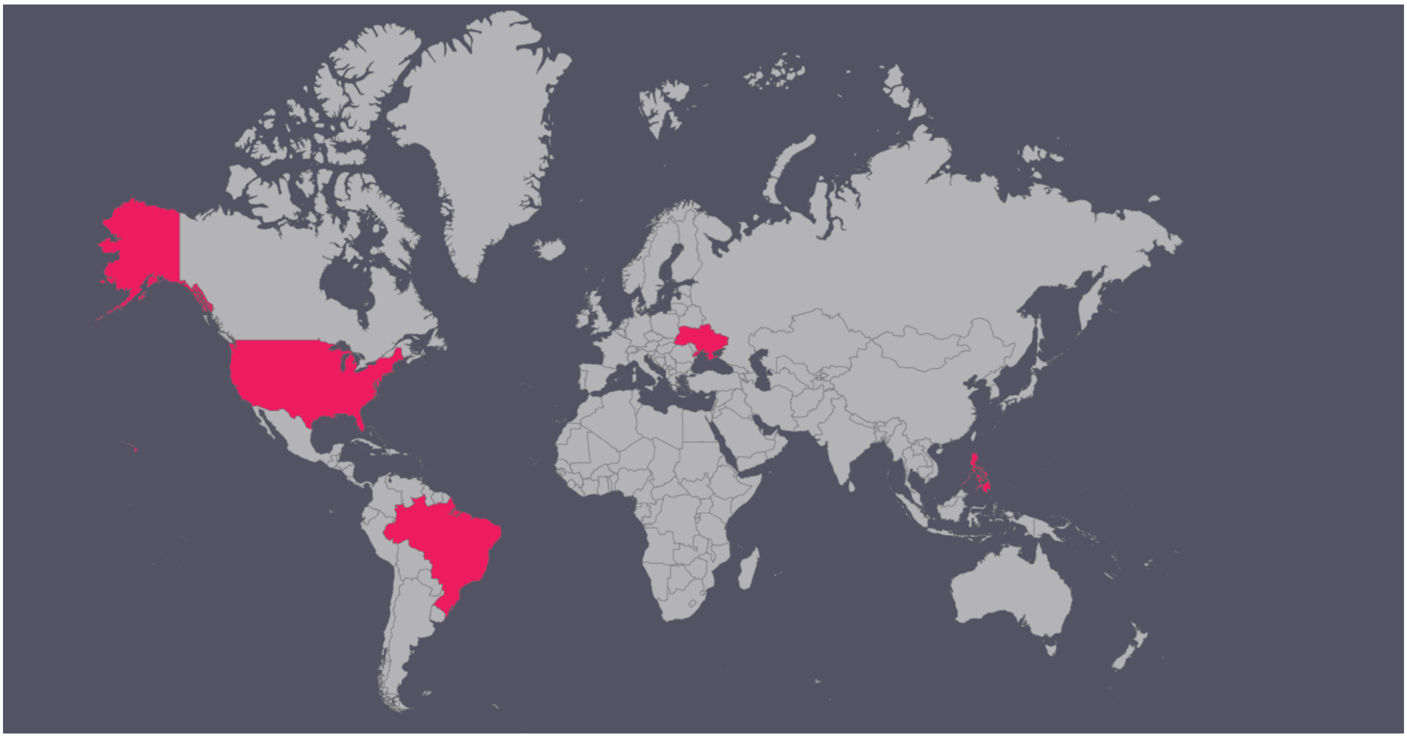


Figure 7 – RomCom RAT threat actor targets

Conclusions

RomCom RAT threat actor is actively developing new techniques targeting victims worldwide. It's highly likely to expect new threat actor campaigns. At the time of publication, there is no apparent link to any attributed threat actor.

We are releasing referential IoCs from the previous and the latest campaign targeting Ukraine.

Indicators of Compromise (IoCs)

Hashes (sha-256)	3e3a7116eeadf99963077dc87680952cca87ff4fe60a552041a2def6b45cbeea 983833334d168cd4274467f48171489e019b86b51e687738565a93dd3f58d0aa 05681ff7cae6b28f5714628a269caa5115da49c94737ce82ec09b4312e40fd26 59f0c3b7890f11217ad37764f225cd1c9d27747495d80dadde40b78edfbfa21e e80d80521238008bf6f429e072eaf6030c06e2d3123d03ea9b36f5a232a1ec90 61e349518ca3f10d1e7aae0be95bc43dc23843c8acf177831cdfd48f26a07c72 a2511c5c2839bfbdf9c0f84f415d5eae168456e5d3f77f1becdbcd69fba4daa4 56a6fb2e2b6a801351175f2aa30a63d44e9ba69f177f6fe20dad348b4d6fb0d1

	9f61259c966f34d89b70af92b430ae40dd5f1314ee6640d16e0b7b0f4f385738 c116a0aafdc2765e38b4f5efdf89960997abf0db81daa8f5380ce3c893e9af96 4fc9202ff84ef84b8c5e6140b66ac3d04570daf886a7f1ae31661ade882f963e 494b43198db467f506e9857f39ebe8f8bf6d871776eba092a7e2f2140046e16d 068117b406940ac510ed59efd1d7c7651f645a31bd70db6de16aba12c055aae6 80d78703de91d292c031275b4493966e363f5fa065edd79e0fd63aa2573b44a4
C2	CombinedResidency[.]org optasko[.]com 4qzm[.]com notfiled[.]com

Applied Counter Measures

```
import "pe"
import "math"

rule targeted_RomComRat : RomCom deployed via trojanized legitimate apps
{
   meta:
      description = "Rule detecting RomCom RAT used to attack Military Institutions from Ukraine"
      author = " The BlackBerry Research & Intelligence team"
      date = "2022-18-10"
      license = "This Yara rule is provided under the Apache License 2.0
(https://www.apache.org/licenses/LICENSE-2.0) and open to any user or organization, as long as
you use it under this license and ensure originator credit in any derivative to the BlackBerry
Research & Intelligence Team"
      hash = "9f61259c966f34d89b70af92b430ae40dd5f1314ee6640d16e0b7b0f4f385738"

     strings:
      //comDll.dll
      $x0 = {636f6d446c6c2e646c6c}
      //combase32.dll
      $x1 = {63006f006d006200610073006500330032002e0064006c006c00}

   condition:
   uint16(0) == 0x5a4d and
   pe.number_of_sections == 7 and
   pe.sections[0].name == ".text" and
   math.entropy(pe.sections[0].raw_data_offset, pe.sections[0].raw_data_size) >= 6.5 and
   pe.sections[1].name == ".rdata" and
   math.entropy(pe.sections[1].raw_data_offset, pe.sections[1].raw_data_size) >= 5.2 and
   pe.sections[2].name == ".data" and
   pe.sections[3].name == ".pdata" and
   math.entropy(pe.sections[3].raw_data_offset, pe.sections[3].raw_data_size) >= 5.5 and
   pe.sections[4].name == "_RDATA" and
   math.entropy(pe.sections[4].raw_data_offset, pe.sections[4].raw_data_size) >= 2.4 and
   pe.sections[5].name == ".rsrc" and
```

```
    math.entropy(pe.sections[5].raw_data_offset, pe.sections[5].raw_data_size) >= 2.85 and
    pe.sections[6].name == ".reloc" and
    math.entropy(pe.sections[6].raw_data_offset, pe.sections[6].raw_data_size) >= 5.3 and
    pe.number_of_resources == 2 and
    pe.exports("startFile") and
    pe.exports("startInet") and
    all of ($x*)
}
```