

BlackBerry Blog

[BlackBerry Blog](#) › RomCom Resurfaces: Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine

RomCom Resurfaces: Targeting Politicians in Ukraine and U.S.-Based Healthcare Providing Aid to Refugees from Ukraine

[CYBERSECURITY](#) / 06.07.23 / [The BlackBerry Research and Intelligence Team](#)



Summary

The RomCom threat actor has been carefully following geopolitical events surrounding the war in Ukraine, targeting [militaries](#), food supply chains, and [IT companies](#). In RomCom's latest campaign, the BlackBerry Threat Research and Intelligence team observed RomCom targeting politicians in Ukraine who are working closely with Western countries, and a U.S.-based healthcare company providing humanitarian aid to the refugees fleeing from Ukraine and receiving medical assistance in the U.S.

This report is the first part of our research covering the details of RomCom's latest malicious campaign, while the second part will cover RomCom's behaviors, including detection engineering.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

[Cookie Settings](#)

[Decline](#)

[Accept](#)

[Cybersecurity](#)[Automotive & IoT](#)[Critical Communications](#)

TA0001	T1103
TA0002	T1559, T1218, T1204,
TA0003	T1546.015
TA0005	T1027, T1140, T1036, T1564.001, T1112
T15007	T1057, T1083, T1082, T1217
TA0009	T1113
TA0010	T1041
TA0011	T1090, T1071, T1071.001, T1095, T1573.002, T1105
TA0040	T1486

Weaponization and Technical Overview

Weapons	Trojanized applications, x64 dll payloads
Attack Vector	Spear-phishing
Network Infrastructure	Cloned websites, C2 servers using self-signed SSL certificates
Targets	Politicians from Ukraine; U.S.-based Healthcare organizations

Technical Analysis

Context

In mid-March 2023, we noticed an uptick in telemetry related to our tracking of the operator behind the RomCom remote access trojan (RAT). This uptick encompassed the creation of several new domains and associated artifacts, one of which, “startleague[.]net”, was linked to a file correlating to the SHA256 – c94e889a6c9f4c37f34f75bf54e6d1b2cd7ee654cd397df348d46abe0b0f6ca3, and titled RemoteDesktopManager.2022.3.35.0.exe.

What is Remote Desktop Manager?

As its name suggests, Devolutions Remote Desktop Manager (RDM) is a legitimate utility designed to help facilitate secure remote connectivity. It is compatible with many commonly used remote connection utilities and technologies such as Citrix, FTP, Apple Remote Desktop, TeamViewer, LogMeIn, Microsoft Remote Desktop (RDP), SSH Shell, and many more.

According to the [developer's](#) website:

“Remote Desktop Manager is an application that integrates a comprehensive set of tools and managers to meet the needs of any IT team. It is designed to centralize remote connection technologies, credentials, and secure access to these resources. Most connections are established using either an external library or third-party software.”

Attack Vector

Although it is unclear at this point what initial infection vector was used to kick off the execution chain, [previous RomCom attacks](#) used targeted phishing emails to point a victim to a cloned website hosting Trojanized versions of popular software. There is a high likelihood that this is the same in this case, as

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

up online infrastructure with one thing in common: trying to fool the user into believing they are interacting with the real company or organization, by making their fake website look as much like the real one as possible. It is important to understand that just because a website has a company name you know and trust in the URL, that doesn't mean the site you are visiting is owned or operated by that company.

Real Domain	Fake Domain
devolutions[.]net	rdp-devolutions[.]com

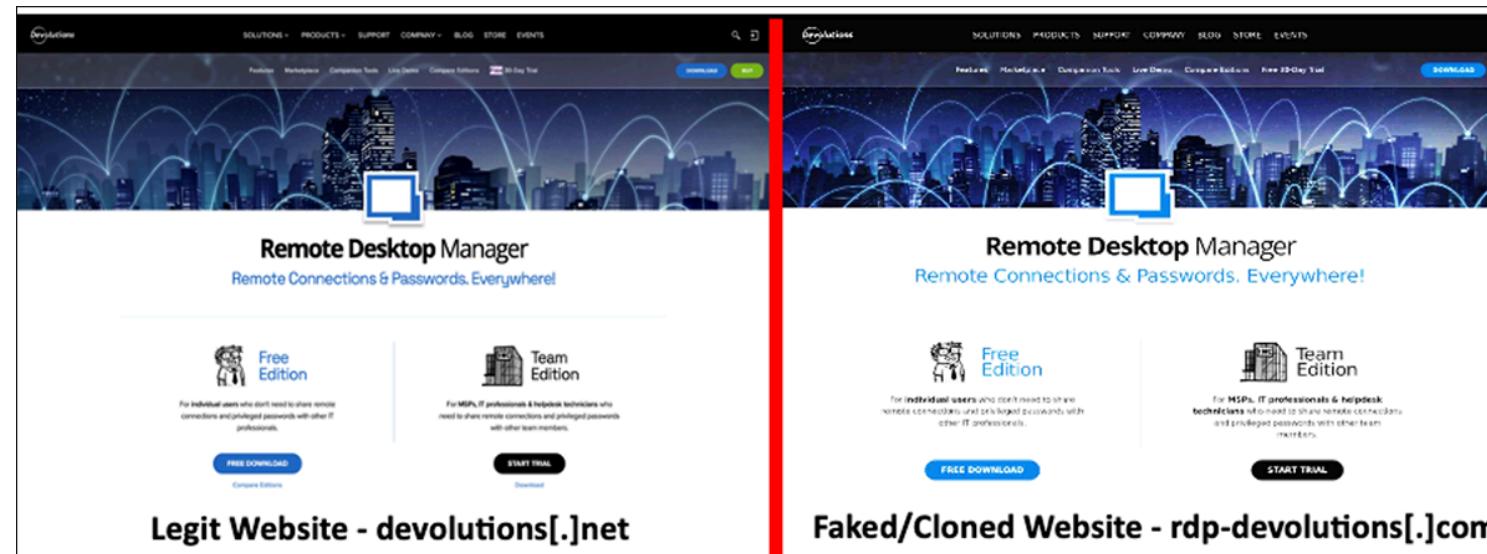


Figure 1: Example of the real and fake Remote Desktop Manager websites side by side

As shown in Figure 2 below, the malicious file "*Installer.RemoteDesktopManager.2022.3.35.0.exe*" is hosted on the observed cloned/fake website.

Scanned	Detections	Status	URL
2023-04-06	1 / 88	200	https://rdp-devolutions.com/download/remote-desktop-manager.php

Figure 2: rdp-devolutions[.]com malware URL

Weaponization

Once downloaded by the user, the Trojanized installer from the cloned website makes every attempt to appear legitimate. Statically, it is a 64-bit executable (.exe) which is signed by an in-date digital signature.

However, further analysis into the *legitimate* download of **Devolutions RDM** suggests the signing information does not correlate and is, in fact, issued by a completely different organization. The fraudulent certificate obtained from the malicious installer is shown below in Figure 3.

Cybersecurity

Automotive & IOT

Critical Communications

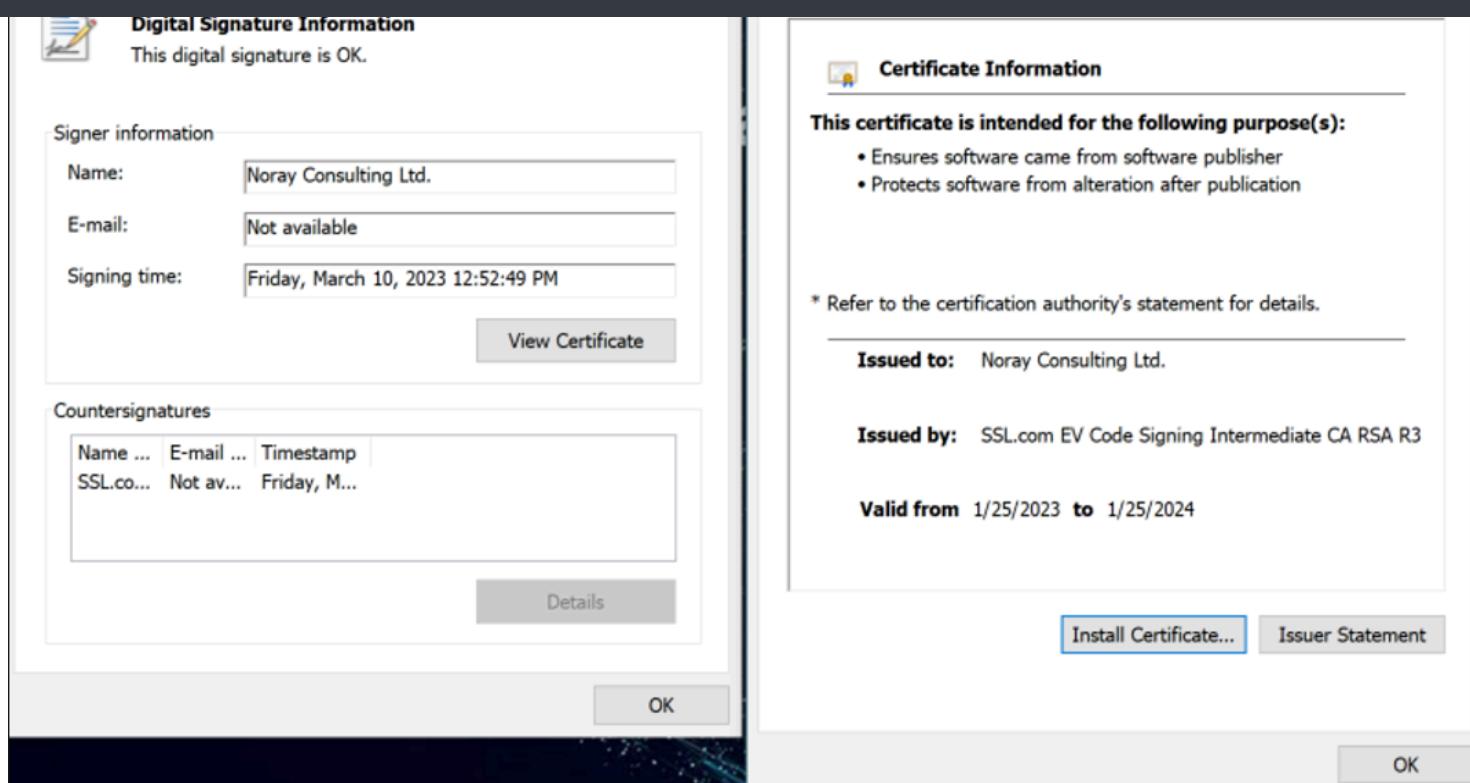


Figure 3: Digital Signature of the Trojanized Installer

Upon execution of the Trojanized main setup file, *Installer.RemoteDesktopManager.2022.3.35.0.exe*, the user is prompted to select the destination path of where they'd like the file(s) to be installed.

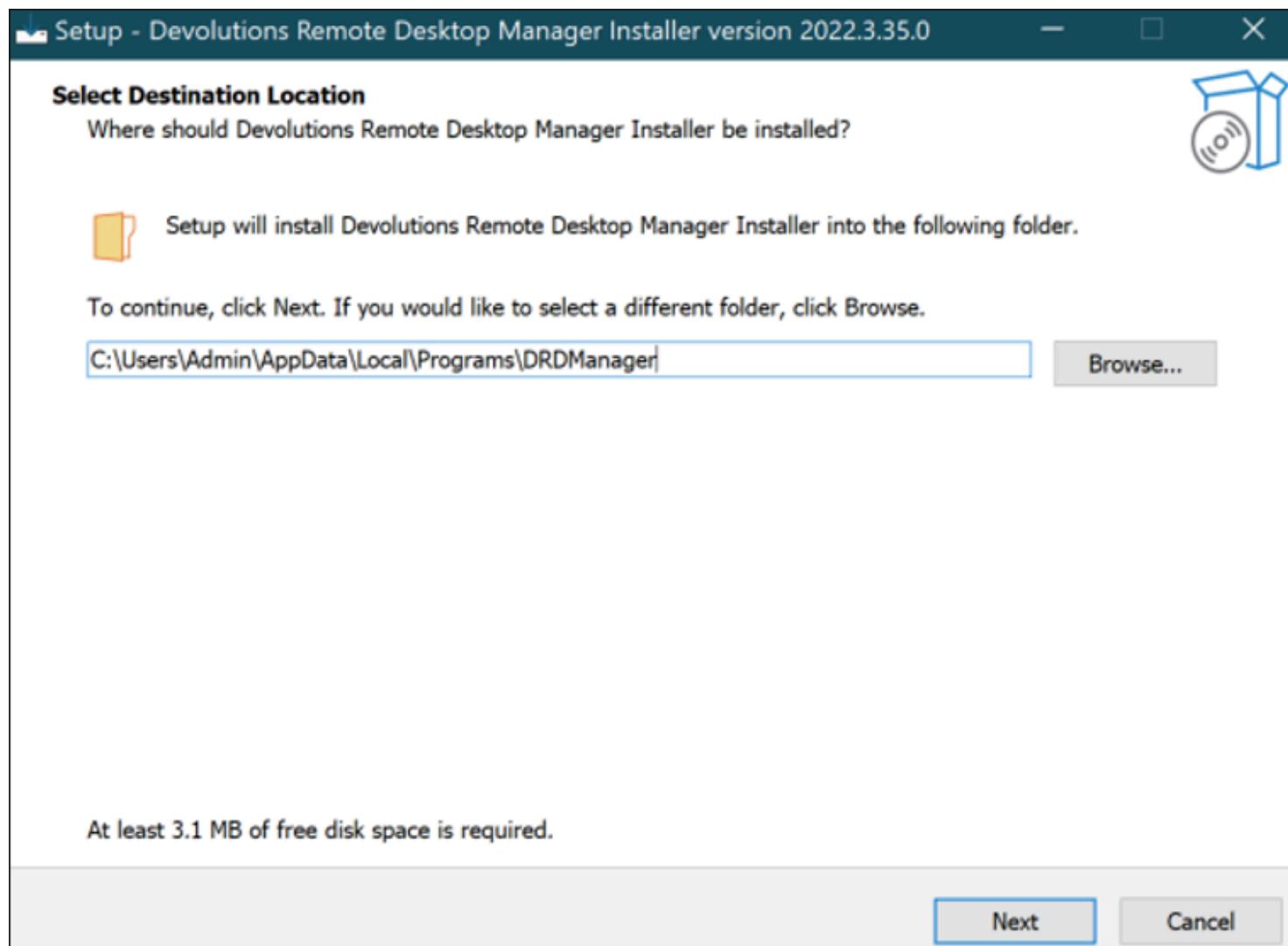


Figure 4: Setup Installer for Trojanized DRDM

Unbeknownst to the victim, during this prompt, the malware has already begun its execution chain. The malware drops various components into a hidden path via C:\Users\Public\Libraries. (Further details can be found below in Appendix 1: IoC's.)

Dropped binaries:

- *update.conf*
- *Installer.RemoteDesktopManager.2022.3.35.0.exe*
- *netid4050320587.dll*

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

Cybersecurity	Automotive & IOT	Critical Communications	
Installer.RemoteDesktopManager.2022.3.35.0.exe	5/2/2023 2:10 PM	Application	1,633 KB
netid4050320587.dll0	5/2/2023 2:10 PM	DLL0 File	2,634 KB
prxym4050320587.dll	5/2/2023 2:10 PM	Application extension	2,599 KB
Recorded TV	3/19/2019 4:49 AM	Library	1 KB
update.conf	5/2/2023 2:10 PM	CONF File	1 KB

Figure 5: Components dropped by RomCom are deployed, regardless of 'Setup'

The core malicious binary related to RomCom is the file %**netid4050320587.dll0**. This Dynamic-Link Library (.DLL) is executed via the Windows host process RunDLL32 in the background while the unsuspecting victim tries installing the fake software.

This malicious binary is executed, as seen in Figure 6, via: "**C:\Windows\System32\rundll32.exe C:\Users\Public\Libraries\netid4050320587.dll0,Main netid4050320587.dll0**".

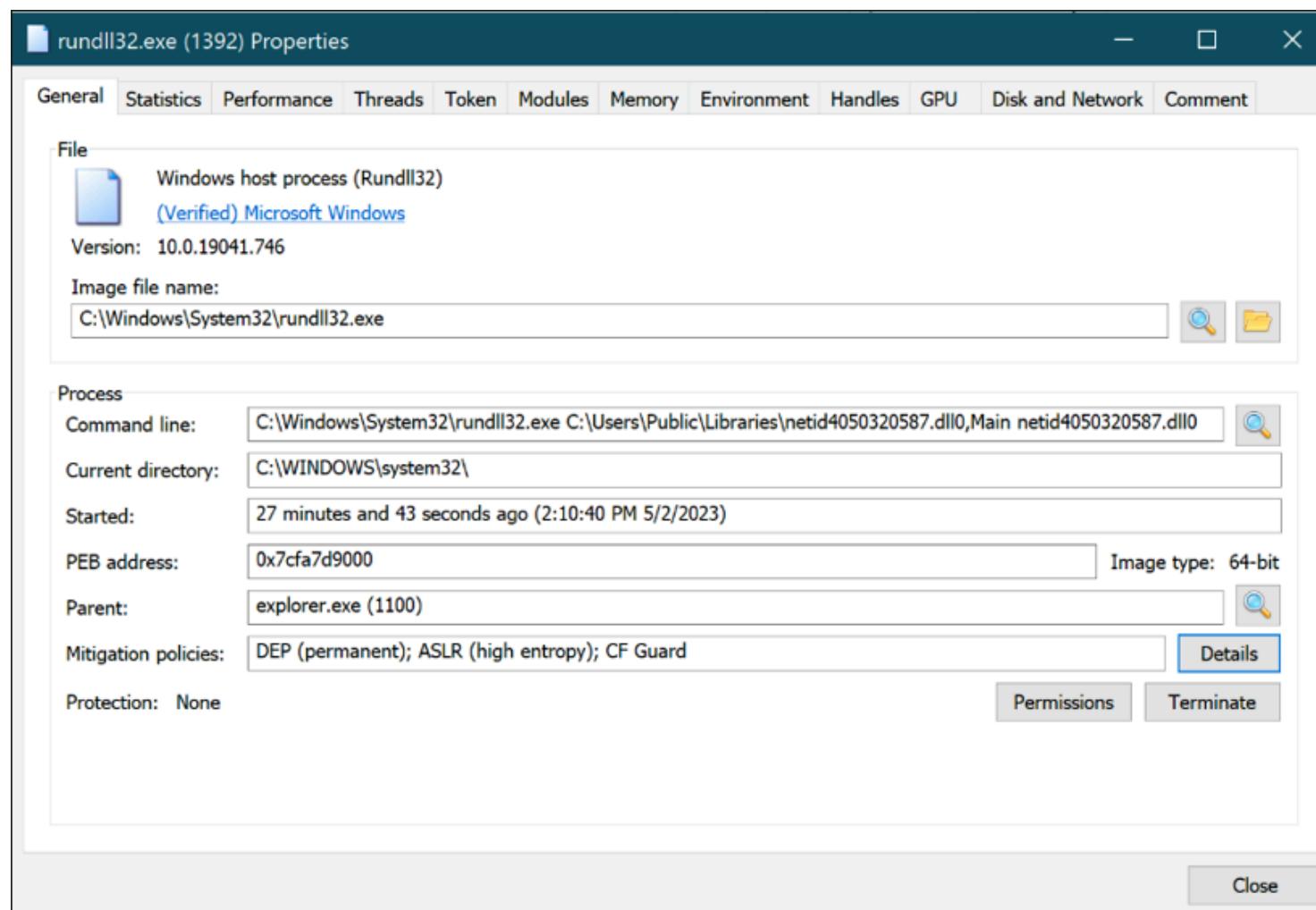


Figure 6: Execution of the core RomCom DLL

The malicious dropper contains a legacy installer for the legitimate program to masquerade its purposes further. This installer is dropped both in **C:\Users\User\AppData\Local\Temp%\js-TIDj8.tmp%**\ and **C:\Users\Public\Library**.

SHA256: b1b015f3762b4b9fce928401a3b13beee5fb70c989b97a03d57545fc00a1978

In addition to deploying and executing its payload of malware, this Installer will continue seemingly as intended, so the user is left none the wiser.

On execution (as of April 2023), the Installer for the fake Devolutions Remote Manager will fail its setup as it cannot send data to the real Devolutions server. When the Installer receives this error, the installation terminates.

Meanwhile, the malware has been stealthily deployed on the victim host by the decoy Installer and has begun to carry out its malicious activities.

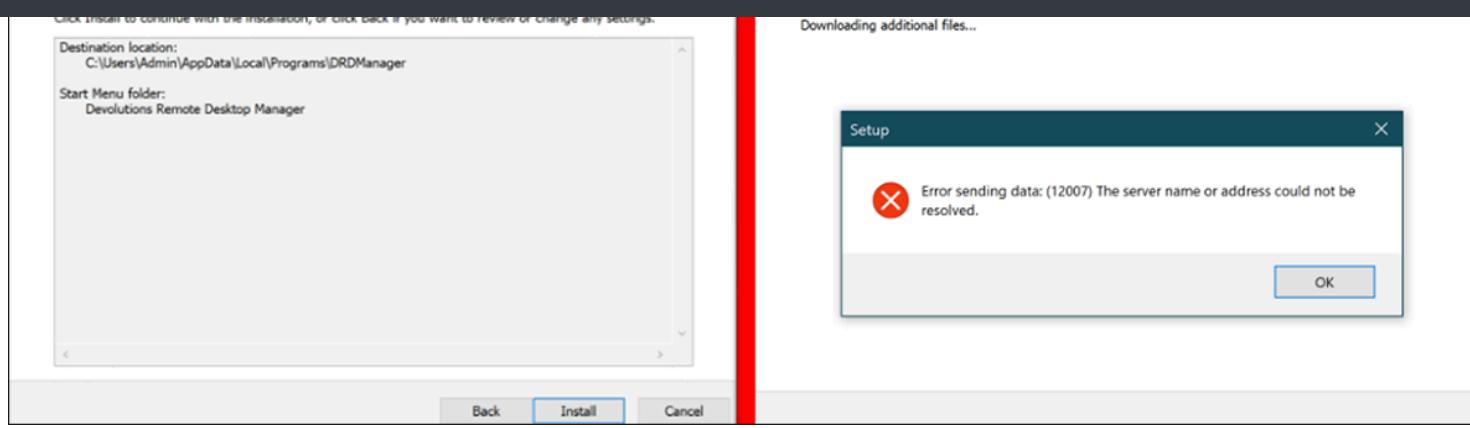


Figure 7: Continuation of Trojanized installer

The function of the malicious files dropped is as follows:

- %netid3231462335.dll% – This is the core RomCom RAT payload. It is a new version of the implant we initially [uncovered last Fall](#). Improvements were made to its obfuscation to thwart static analysis.
- The application's core functionality remains relatively the same, enabling the threat actor full access to the victim's device.
- %prxym1500330613.dll% – This is the RomCom Loader file. This file is used to execute RomCom via the command line.
- procsys.dll – This is a browser stealer, and steals browser data such as passwords, browsing history, and site cookies.
- update.conf – A small supporting configuration file for RomCom.

The full execution chain is described below in Figure 8.

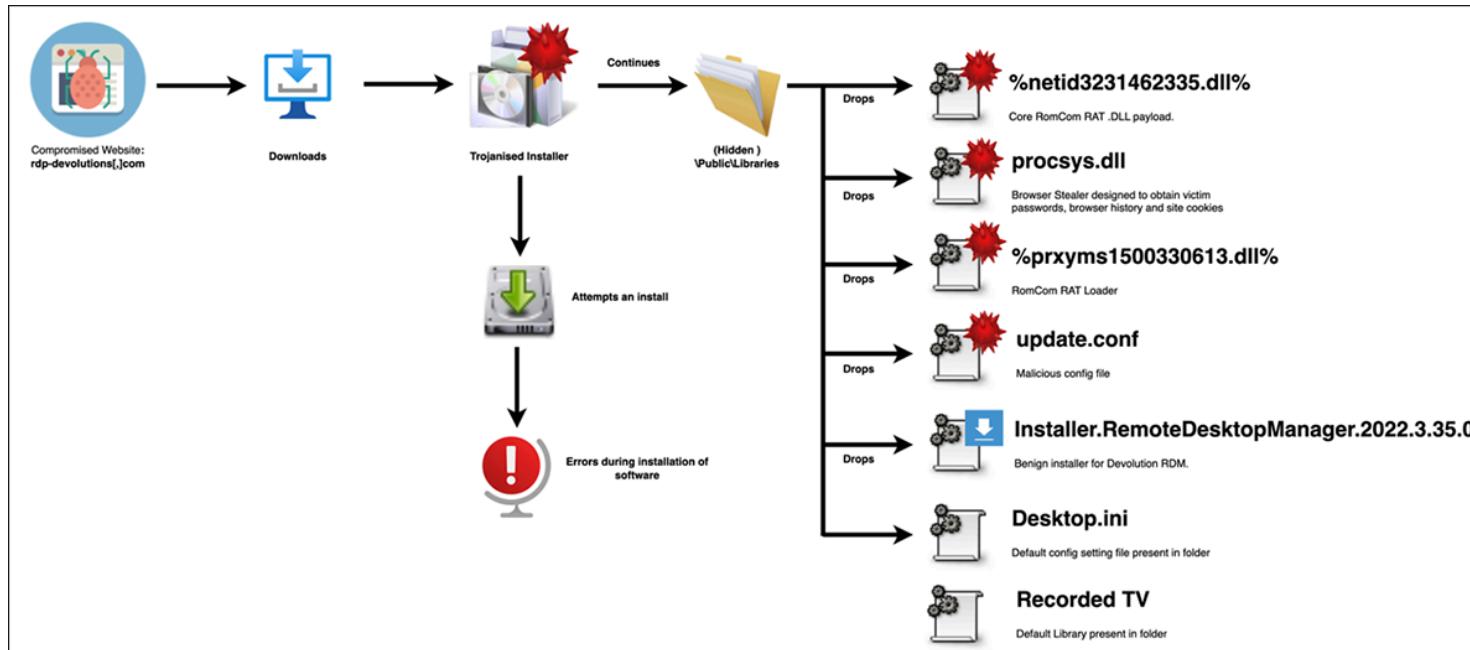


Figure 8: Execution of Trojanized RomCom Installer

Networking

Upon successful installation, RomCom will enumerate the infected host and gather some basic host and user metadata, which is then sent to its command-and-control (C2) server – [startleague\[.\]net](http://startleague[.]net) – to “check in”.

```

05/04/23 03:03:53 PM [      Diverter] rundll32.exe (2108) requested TCP 192.0.2.123:443
05/04/23 03:03:53 PM [  HTTPListener443] POST / HTTP/1.1
05/04/23 03:03:53 PM [  HTTPListener443] Connection: Keep-Alive
05/04/23 03:03:53 PM [  HTTPListener443] User-Agent: WinHTTP Example/1.0
05/04/23 03:03:53 PM [  HTTPListener443] Content-Length: 1300
05/04/23 03:03:53 PM [  HTTPListener443] Host: startleague.net
05/04/23 03:03:53 PM [  HTTPListener443] @ <htmno worker for task completion

```

Figure 9: Request sent via the WinHTTP API

Additionally, this can be noted via the TCP Stream shown in Figure 10 below.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

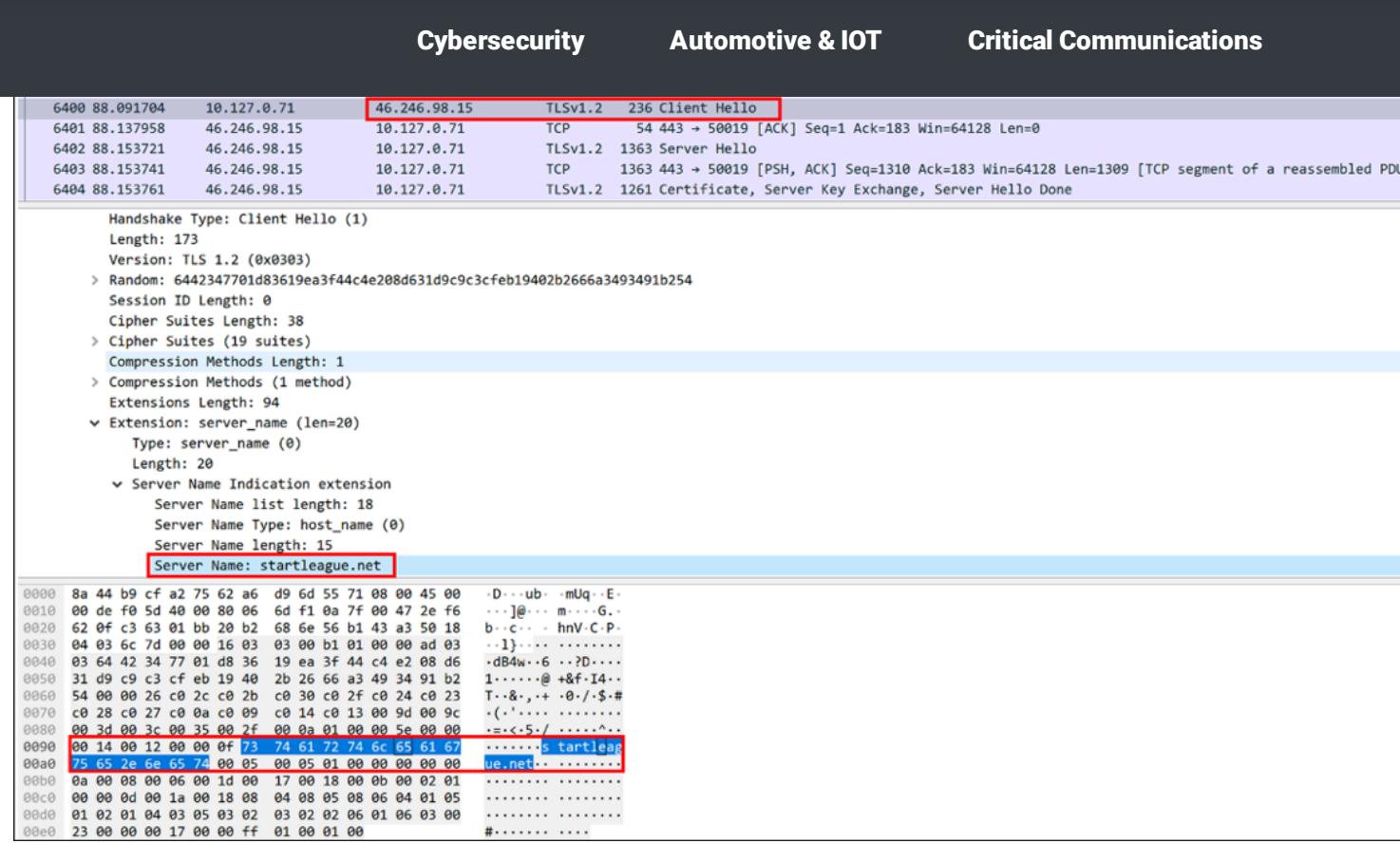


Figure 10: Wireshark capture of initial RomCom communication

If, for any reason, a connection attempt to its C2 is unsuccessful, the malware appears to have some redundancy. If its initial requests cannot be handled, it will attempt to connect via ICMP Requests instead.

```
05/04/23 03:03:53 PM [           Divter] rundll32.exe (2108) requested TCP 192.0.2.123:443
05/04/23 03:03:53 PM [           Divter] ICMP type 3 code 3 172.16.2.161->172.16.2.161
05/04/23 03:03:53 PM [ HTTPListener443] POST / HTTP/1.1
05/04/23 03:03:53 PM [ HTTPListener443] Connection: Keep-Alive
05/04/23 03:03:53 PM [ HTTPListener443] User-Agent: WinHTTP Example/1.0
05/04/23 03:03:53 PM [ HTTPListener443] Content-Length: 121
05/04/23 03:03:53 PM [ HTTPListener443] Host: startleague.net
05/04/23 03:03:53 PM [ HTTPListener443] 33de3134-cdb7-4b53-b147-3e9d549bbe8d@ADMIN@netid4050320587.dll0@not_
exist:19043-0:err geo:ADMIN:\DESKTOP-8GC80CM:
```

Figure 11: Request sent via ICMP to RomCom's C2

Additionally, this can be seen in Figure 12 (below) in a network capture.

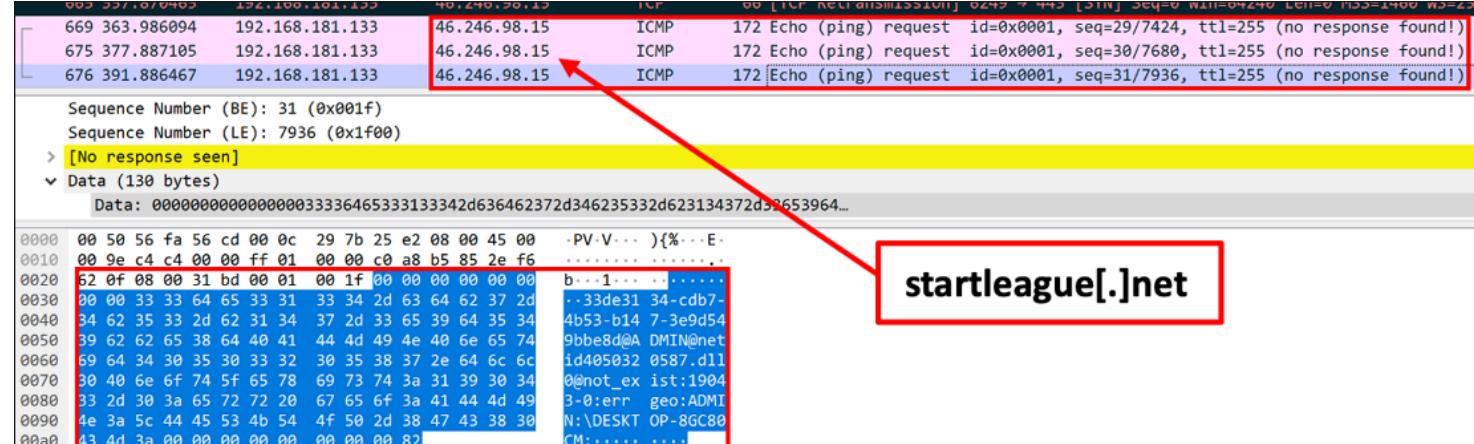


Figure 12: ICMP Request to C2 Related to RomCom

Network Infrastructure

As mentioned previously, the purpose of the domain **rdp-devolutions[.]com** is to host RomCom's cloned website, both hosting and delivering a Trojanized/fake version of the Devolutions' Remote Desktop Manager software.

The domain was registered on 2023-03-09 and initially tied to the IP address 91[.]235[.]116[.]232 for the time period 2023-03-11 > 2023-03-30, when it was updated to resolve to the IP address 74[.]119[.]239[.]234.

Domain name	IP	ASN	Purpose
rdp-devolutions[.]com	74.119.239.234	AS3356	Hosts RomCom's cloned website

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

		MEDIA SRL, RO		
startleague[.]net	46[.]246[.]98[.]15	AS42708	C2 server	

The domain **startleague[.]net** was registered on **2022-12-19** and tied to the IP address **2[.]57[.]90[.]16**. This continued until **2023-01-30**, when it began resolving to the IP address **46[.]246[.]98[.]15**.

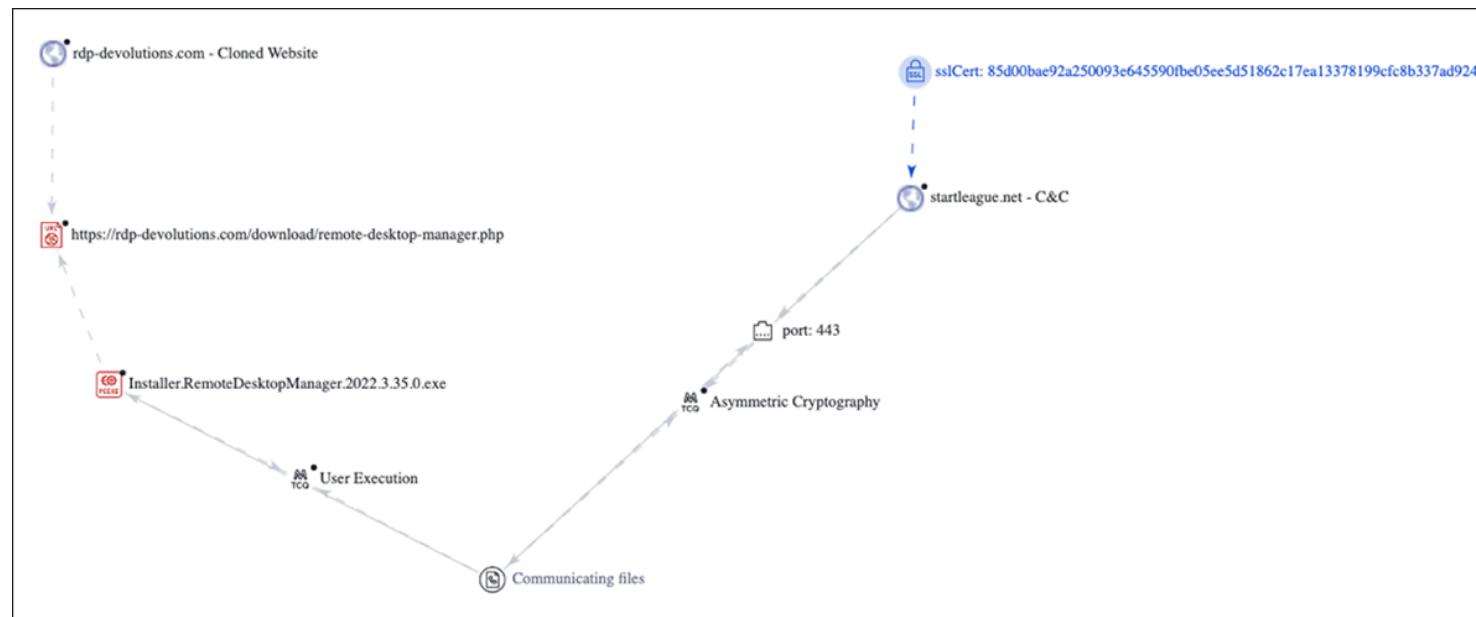
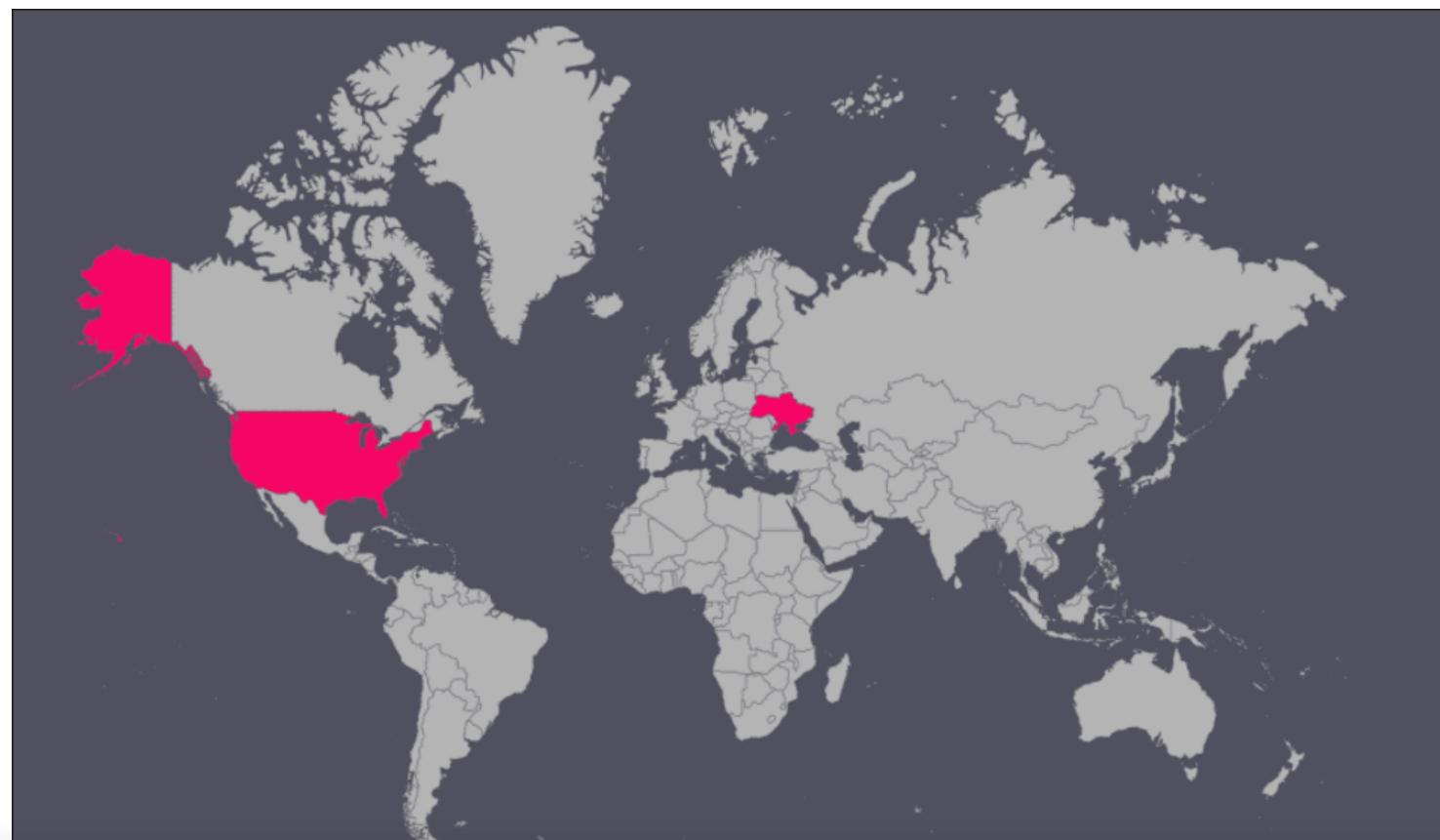


Figure 13: VirusTotal graph showing the network infrastructure

Targets

During the course of our investigations, BlackBerry has identified several victims primarily based in Ukraine. This aligns with previously seen geolocations targeted by RomCom. We have also observed evidence of at least one target based in the United States.

The victims targeted are involved in several dissimilar industries such as Military and Healthcare, united by the common thread of Russia's invasion of Ukraine.



BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

implant. This time it was deployed within a Trojanized installation of “GoTo Meeting”, a popular video conference software commonly used by a variety of enterprises, both large and small.

Following similar TTP’s of previously observed samples of RomCom, the initial attack vector is a faked/cloned website that appears identical to the legitimate one. Below is an example of the cloned website for “GoTo Meeting”.

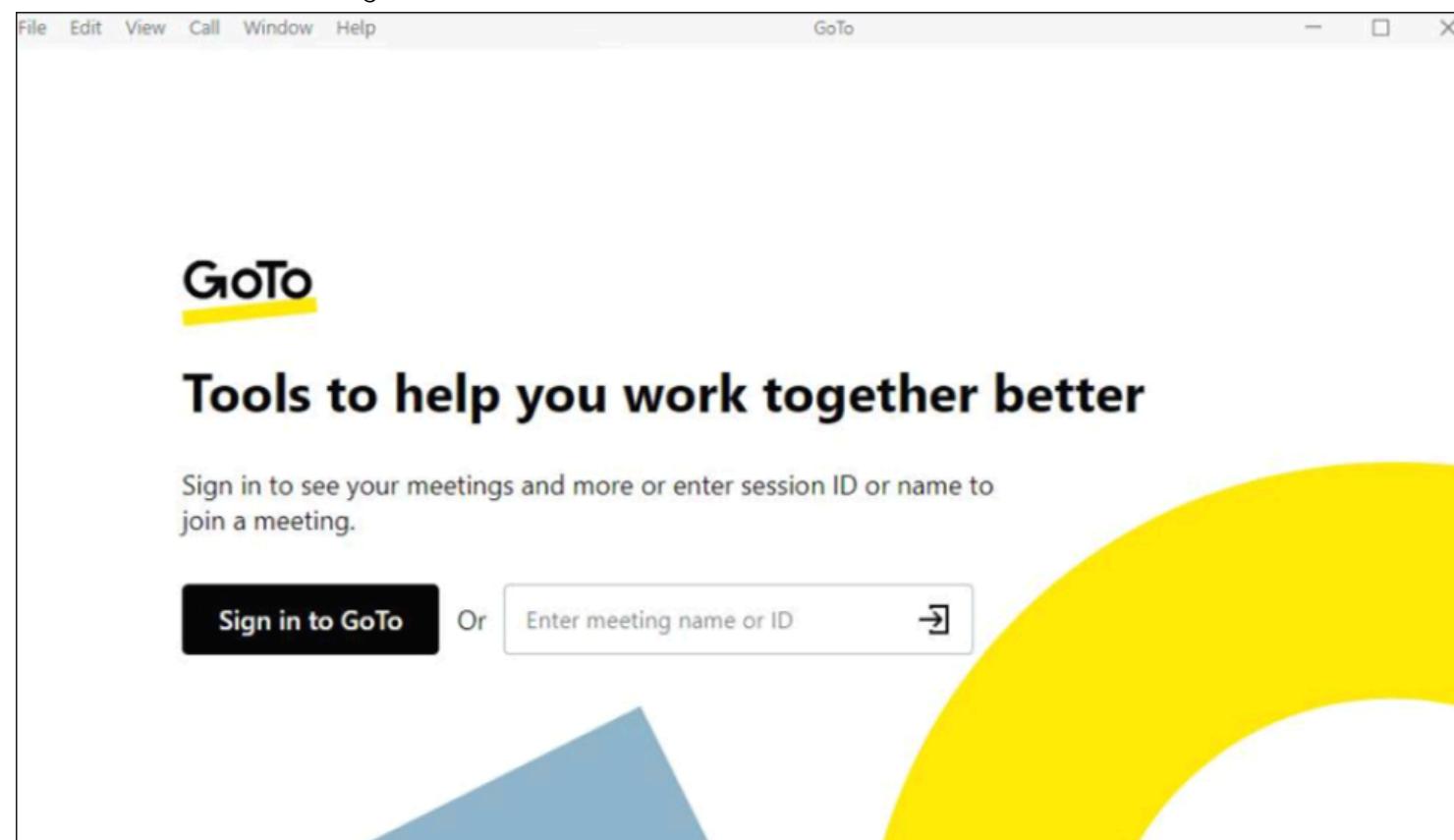


Figure 15: Faked/cloned website of the video conferencing app “GoTo Meeting”

Like other samples of RomCom, it too hosts a Trojanized installer containing a legitimate binary related to the intended product/service, whilst also containing a RomCom implant that will execute during installation by the user.

Details of this observed find are below:

Hash (sha-256)	a552b0b1c948e0ef4e51088f059c280a967ff40bf93ff9d62ebcb74e80f36fc5
File name	GoTo Meeting Opener.msi
File Size	21.02 MB (22040576 bytes)
Created	2022-06-30 12:11:22 UTC
Description	Trojanized installer containing RomCom RAT

WINSCP

Furthermore, at the beginning of May 2023, the Twitter user “@TLP_R3D” identified a “potential RomCom C2” infrastructure noted via [this tweet](#). Upon analyzing the noted IoC’s, the BlackBerry Threat Research and Intelligence team confirmed that the samples in the attack chain indeed contained a RomCom payload.

Unlike previous samples of RomCom observed through our own investigations, this sample of RomCom masqueraded as the popular SSH file-transfer tool “WinSCP”, but it does not contain the RomCom payload itself.

Upon execution of WinSCP-5.21.8-Setup.exe, the malware will attempt to reach out to the noted IoC’s (below) to download and execute itself.

- hxxp://104.234.10.207:7931/itrdd/kcrs/file1[.]txt

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

RomCom	
File name	WinSCP-5.21.8-Setup.exe
File Size	1.22 MB (1280048 bytes)
Created	2023-05-03 10:15:01 UTC
Description	RomCom downloader

Timeline of RomCom Attacks

Below is a timeline of all known RomCom attacks to date, including the name of the software Trojanized to deliver the malware payload in each attack.

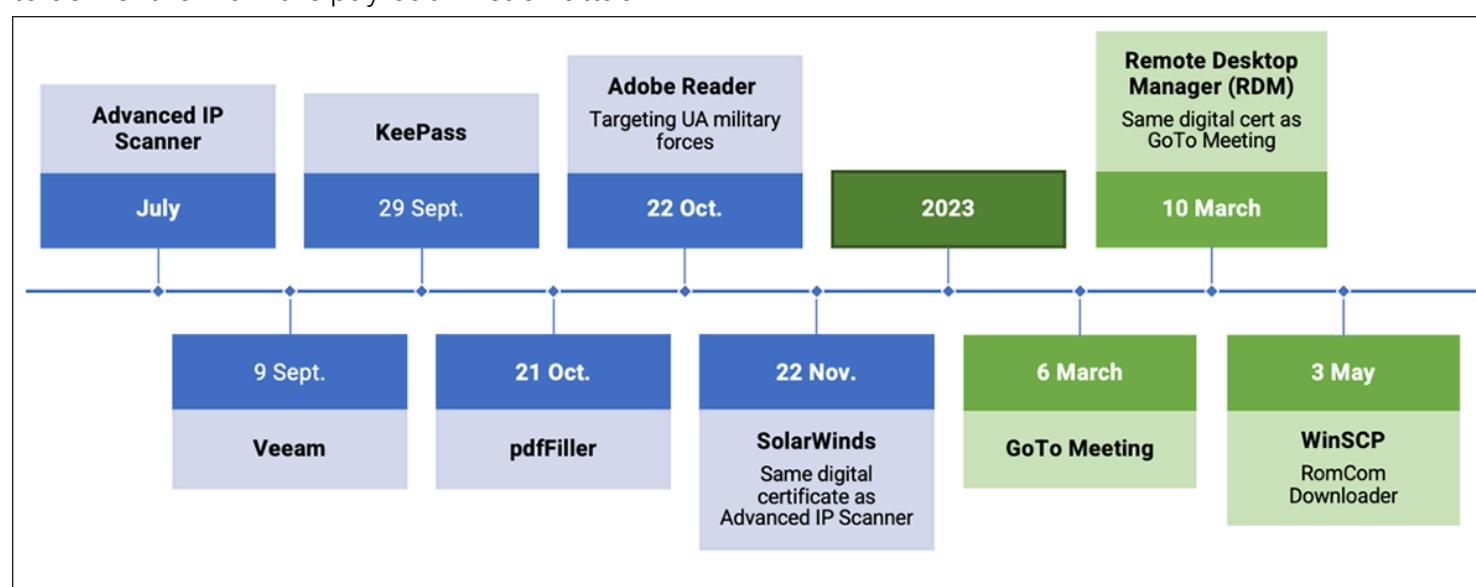


Figure 16: Timeline of known RomCom attacks

Conclusions

Since at least mid-2022, RomCom has been a persistent threat affecting largely Ukrainian-based organizations, including both Government and Military. As the conflict between Ukraine and Russian forces escalates in Eastern Europe, the world becomes increasingly polarized by their support of one side or the other, whether on the ground in Ukraine via the provision of military supplies, or on a country's own home turf via healthcare provided to those fleeing the conflict.

Following its observed Ukrainian-based targets, the RomCom group has been sighted by BlackBerry targeting other possibly pro-Ukrainian affiliated organizations – namely those based in the U.S. – in recent months. The last-observed campaigns target politicians in Ukraine, and a U.S.-based healthcare institution running a humanitarian aid program for refugees fleeing from Ukraine.

The threat actor behind the RomCom RAT appears to be actively interested in what Western countries are doing to support Ukraine, what Ukraine is doing, and who the refugees are receiving help from in the United States. If medical records stored electronically are stolen, it would be easy for the threat actor (and those they are affiliated with) to profile the patient and use that data in future war scenarios and in geopolitics in general. Even the extraction of partial information, such as name, sex, date of birth, and related data, poses a potential risk to that person and those who provide them with any type of aid in future.

The second part of this research will cover behavioral detection engineering covering RomCom operations. Stay tuned to the [BlackBerry blog](#) for this and future updates.

APPENDIX 1 – Indicators of Compromise (IoCs)

MAIN BINARY

Hash	6d3ab9e729bb03ae8ae3fc824474c5052a165de6cb4c27334969a542c7b261d
------	---

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

[Cybersecurity](#)[Automotive & IoT](#)[Critical Communications](#)

Created: 2023-03-10 11:53:07 UTC

Details	Main Windows 64-bit (Signed Binary) contains installer and bundled RomCom malware
---------	---

MAIN BINARY - DIGITAL CERTIFICATE

Name	Noray Consulting Ltd.
Serial Number	56 E1 49 7E FD DA B4 55 B2 35 E6 0C 3C 53 E7 F4
Name	SSL.com Timestamping Unit 2022
Serial Number	1A D6 08 A7 D6 34 B5 CD DE 97 CB A3 CC F0 D0 4B

MAIN BINARY - DROP FILES (%USERS%\PUBLIC\LIBRARIES)

Hash (sha-256)	c94e889a6c9f4c37f34f75bf54e6d1b2cd7ee654cd397df348d46abe0b0f6ca3
File name	installer.RemoteDesktopManager.2022.3.35.0.exe
File Size	1.59 MB (1671808 bytes)
Created	2023-02-15 14:54:16 UTC
Description	Legitimate Devolutions RDM installer

Hash (sha-256)	0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5b866b2a
File Name	netid3231462335.dll0 netid3283347891.dll netid [0-9] .dll
File Size	2.57 MB (2696704 bytes)
Created	2023-03-10 10:56:58 UTC
Description	Core RomCom binary

Hash (sha-256)	65778e3afc448f89680e8de9791500d21a22e2279759d8d93e2ece2bc8dae04d
File Name	prxym3231462335.dll
File Size	2.54 MB (2660864 bytes)
Created	2023-03-10 10:57:01 UTC
Description	RomCom Loader

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

File Information	
File Name	procsys.dll
File Size	3.67 MB (3848704 bytes)
Created	2023-03-23 04:16:43 UTC
Description	Additional infostealer

GOTO MEETING OPENER DROP FILES (%USERS%\PUBLIC\LIBRARIES)

Hash (sha-256)	3b26e27031a00a32f3616de5179a003951a9c92381cd8ec552d39f7285ff42ee
File Name	MSI420A.tmp
File Size	20.88 MB (21899264 bytes)
Created	2023-02-15 06:04:43 UTC
Description	RomCom RAT Dropper created by GoTo Meeting opener

Hash (sha-256)	3e293680e0f78e404fccb1ed6daa0b49d3f6ea71c81dbaa53092b7dd32e81a0d
File Name	netid [0-9] .dll
File Size	5.02 MB (5266432 bytes)
Created	2023-02-14 13:59:54 UTC
Description	Core RomCom binary

Hash (sha-256)	916153d8265a2f9344648e302c6b7b8d7e1f40f704b0df83edde43986ab68e56
File Name	prxym[0-9] .dll
File Size	4.97 MB (5215744 bytes)
Created	2023-02-14 13:58:54 UTC
Description	Loader RomCom binary

Hash (sha-256)	e7914f823ed0763c7a03c3cfbcf9344e1da93597733ac22fe3d31a5a4e179aa
File Name	winipfile[0-9] .dll
File Size	5.41 MB (5676544 bytes)
Created	2023-02-14 14:00:20 UTC

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)

Cybersecurity

Automotive & IoT

Critical Communications



Hash (sha-256)	a5da9b711882761699eece44eb4018311b1de0be19e159c417ba021a9491744
File Name	bnert.dll0
File Size	390.00 KB (399360 bytes)
Created	2023-05-03 10:01:38 UTC
Description	RomCom binary

Hash (sha-256)	1308146f161ed60c86532dd2d2de8de8b0401e27023fc56f83903f137fccacfd
File Name	xlmtdm.dll
File Size	185.50 KB (189952 bytes)
Created	2023-05-03 10:04:11 UTC
Description	RomCom loader

NETWORKING

Domain	rdp-devolutions[.]com
IP	74[.]119[.]239[.]234
Domain	startleague[.]net
IP	46[.]246[.]98[.]15
IP	104[.]234[.]10[.]207:7931

APPENDIX 2 – Applied Countermeasures

Sigma Rules

Available upon request – see below.

Yara Rules

Available upon request – see below.

APPENDIX 3 – Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique Name/ Context
Available upon request – see below.		

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

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)



Cybersecurity

Automotive & IoT

Critical Communications



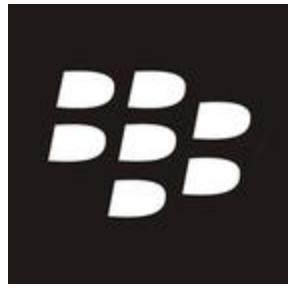
- Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries
- Industroyer2 Malware Takes Aim at Ukraine Infrastructure
- HeaderTip Backdoor Shows Attackers from China Preying on Ukraine

BlackBerry.
Intelligent Security. Everywhere.

THE BEST DEFENSE IS ABOUT TO BE A BEST SELLER.

BlackBerry.com/beacon





About The BlackBerry Research and Intelligence Team

The [BlackBerry Research and Intelligence team](#) is a highly experienced threat research group specializing in a wide range of cybersecurity disciplines, conducting continuous threat hunting to provide comprehensive insights into emerging threats. We analyze and address various attack vectors, leveraging our deep expertise in the cyberthreat landscape to develop proactive strategies that safeguard against adversaries.

Whether it's identifying new vulnerabilities or staying ahead of sophisticated attack tactics, we are dedicated to securing your digital assets with cutting-edge research and innovative solutions.



Corporate

Company
Newsroom
Investors
Careers
Leadership
Corporate Responsibility
Certifications
Customer Success

Developers

Enterprise Platform & Apps
BlackBerry QNX Developer Network
Blogs
BlackBerry ThreatVector Blog
Developers Blog
Help Blog

Legal

Overview
Accessibility
Patents
Trademarks
Privacy Policy

© 2024 BlackBerry Limited. All rights reserved.

BlackBerry uses cookies to help make our website better. Some of the cookies are necessary for proper functioning of the site, while others are to help us understand how you use it. [Learn More](#)