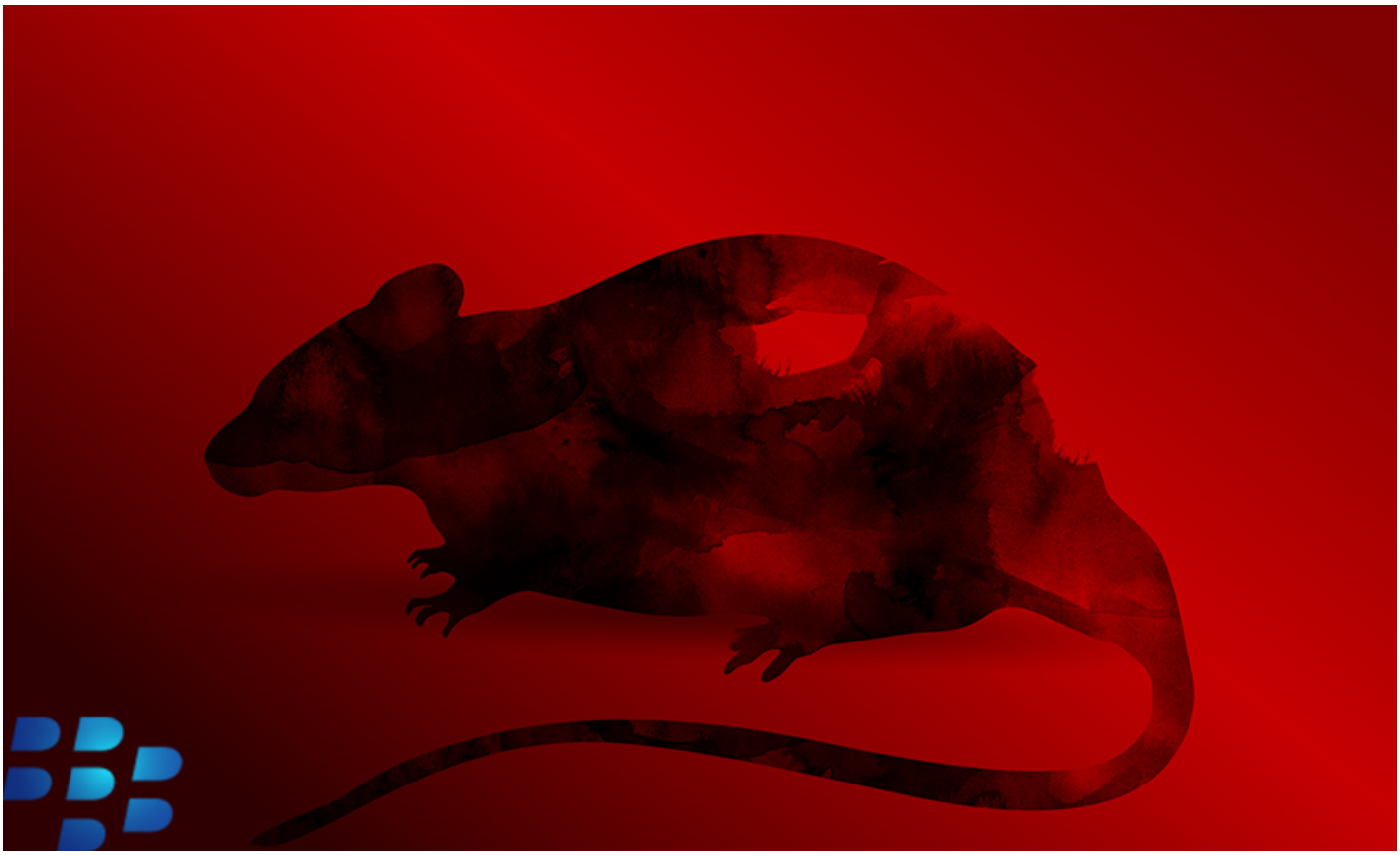
blogs.blackberry.com /en/2022/11/romcom-spoofing-solarwinds-keepass

# RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom

The BlackBerry Research & Intelligence Team ⋮⋮ 11/2/2022



## Summary

The threat actor known as RomCom is running a series of new attack campaigns that take advantage of the brand power of SolarWinds, KeePass, and PDF Technologies. The BlackBerry Threat Research and Intelligence Team uncovered the campaigns while analyzing network artifacts unearthed during our recent report on RomComRAT, which was targeting Ukrainian military institutions through spoofed versions of Advanced IP Scanner software.

In our latest discovery, our team found RomCom leveraging the following products in their campaigns: **SolarWinds Network Performance Monitor**, **KeePass Open-Source Password Manager**, and **PDF Reader Pro.**

While Ukraine still appears to be the primary target of this campaign, we believe some English-speaking countries are being targeted as well, including the United Kingdom. This is based on the terms of service (TOS) of two of the malicious websites and the SSL certificates of a newly created command-and-control (C2).

Given the geography of the targets and the current geopolitical situation, it's unlikely that the RomCom RAT threat actor is cybercrime-motivated.

## Attack Vector

In preparation for an attack, the RomCom threat actor performs the following simplified scheme: scraping the original legitimate HTML code from the vendor to spoof, registering a malicious domain similar to the legitimate one, Trojanizing a legitimate application, uploading a malicious bundle to the decoy website, deploying targeted phishing emails to the victims, or in some instances, using additional infector vectors, which we will go into in more detail below.

## RomCom Weaponization

### RomCom SolarWinds Network Performance Monitor Campaign

Take a look at the two screen shots below to see how the real SolarWinds NPM site and the spoofed site compare.

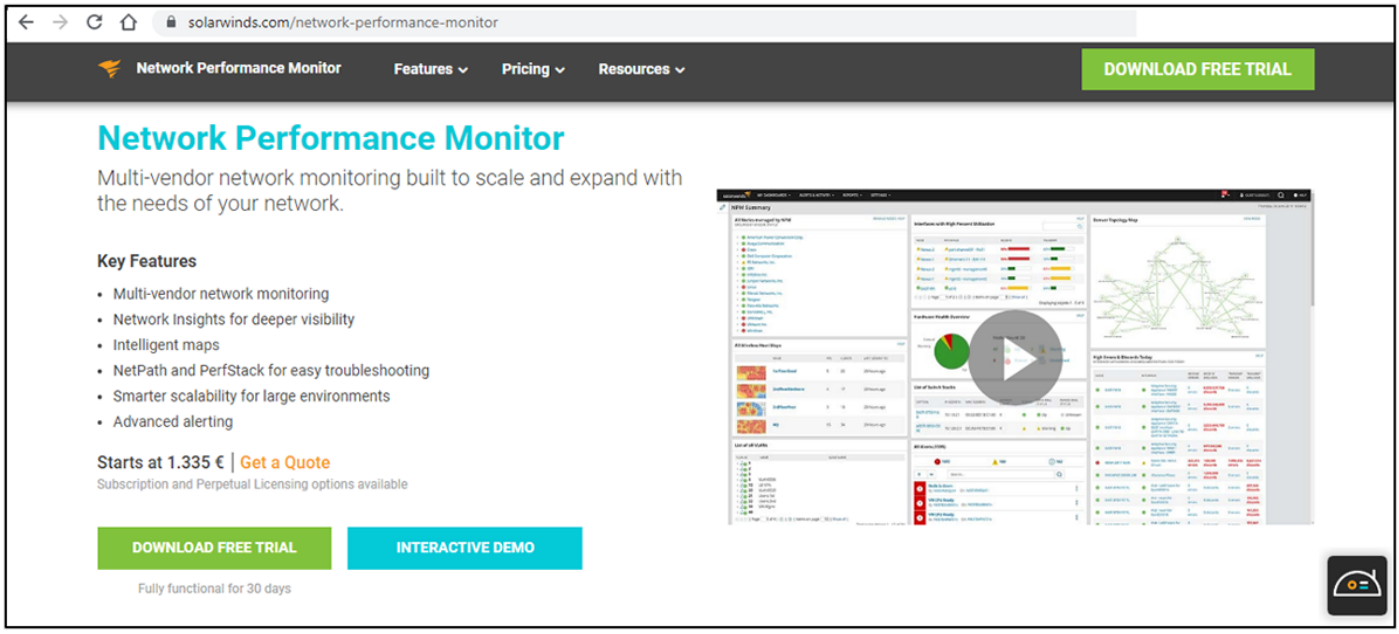



*Figure 1 – Legitimate SolarWinds website*

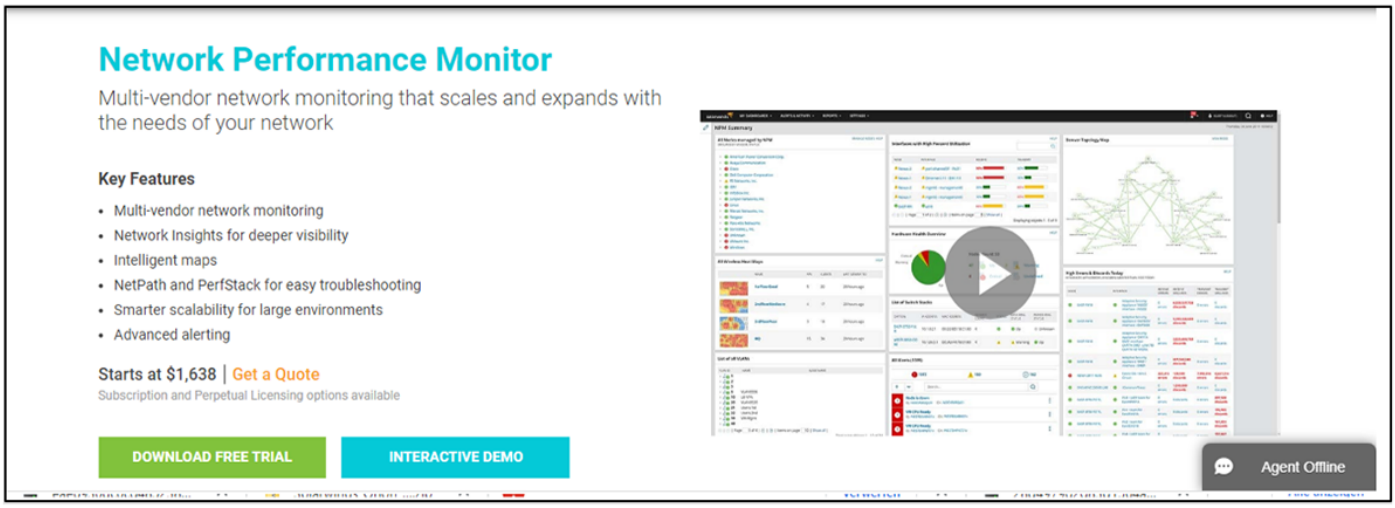
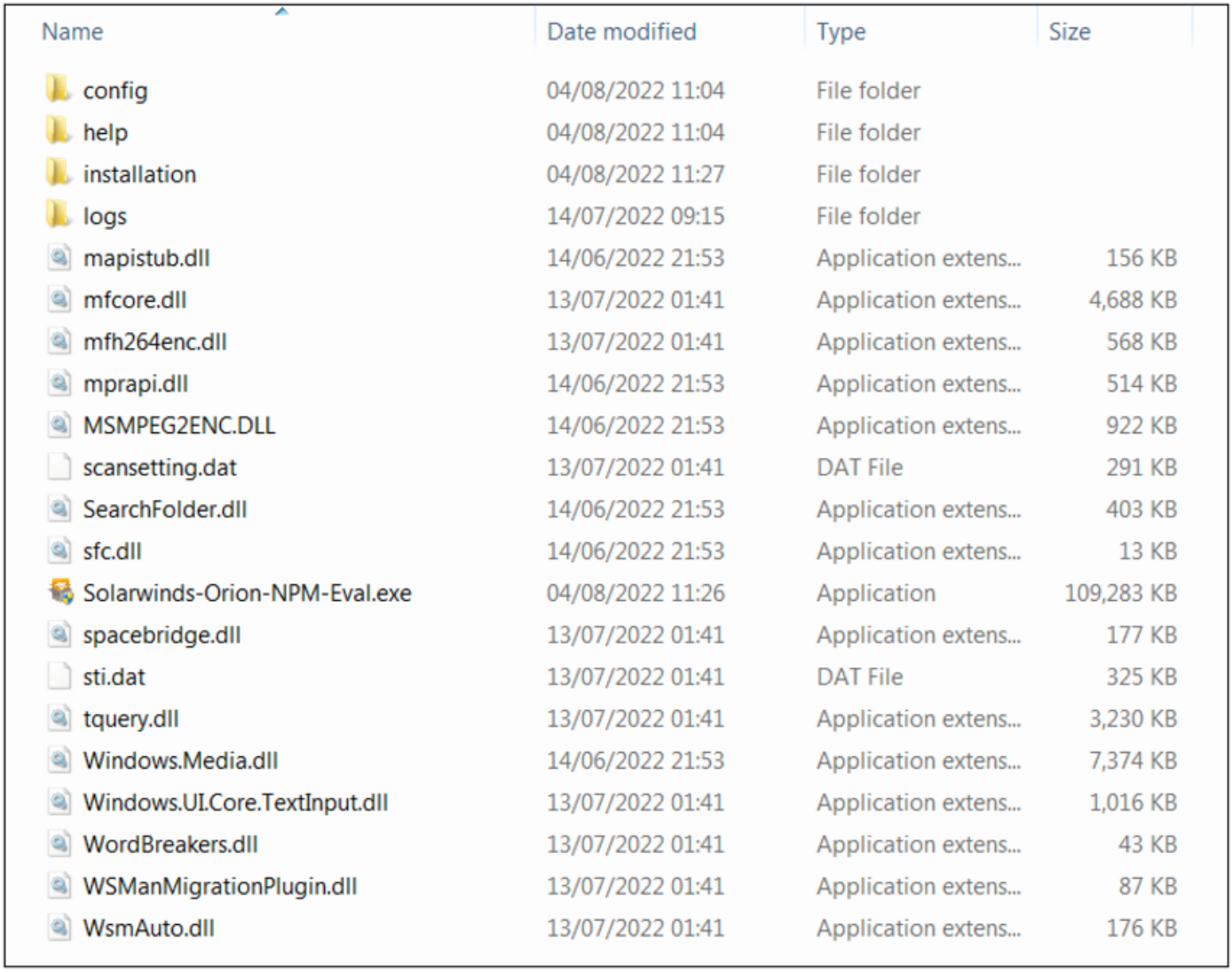



*Figure 2 – Fake SolarWinds website*

The deployment of this attack is through a Trojanized version of the SolarWinds Network Performance Monitoring (NPM) application. While downloading a free trial from the spoofed SolarWinds site, a *legitimate* registration form appears. If filled out, real SolarWinds sales personnel might contact the victim to follow up on the product trial. That technique misleads the victim into believing that the recently downloaded and installed application is completely legitimate. Instead, the victim has unknowingly downloaded a dropper for the malicious RomCom remote access Trojan (RAT).

| | |
|---|---|
| **Hashes (md5, sha-256)** | 7c003b4f8b3c0ab0c3f8cb933e93d301<br><br>246dfe16a9248d7fb90993f6f28b0ebe87964ffd2dcdb13105096cde025ca614 |
| **File Name** | Solarwinds-Orion-NPM-Eval.zip |
| **File Size** | 124,671,897 bytes |



| Name | Date modified | Type | Size |
|---|---|---|---|
| config | 04/08/2022 11:04 | File folder | |
| help | 04/08/2022 11:04 | File folder | |
| installation | 04/08/2022 11:27 | File folder | |
| logs | 14/07/2022 09:15 | File folder | |
| mapistub.dll | 14/06/2022 21:53 | Application extens... | 156 KB |
| mfcore.dll | 13/07/2022 01:41 | Application extens... | 4,688 KB |
| mfh264enc.dll | 13/07/2022 01:41 | Application extens... | 568 KB |
| mprapi.dll | 14/06/2022 21:53 | Application extens... | 514 KB |
| MSMPEG2ENC.DLL | 14/06/2022 21:53 | Application extens... | 922 KB |
| scansetting.dat | 13/07/2022 01:41 | DAT File | 291 KB |
| SearchFolder.dll | 14/06/2022 21:53 | Application extens... | 403 KB |
| sfc.dll | 14/06/2022 21:53 | Application extens... | 13 KB |
| Solarwinds-Orion-NPM-Eval.exe | 04/08/2022 11:26 | Application | 109,283 KB |
| spacebridge.dll | 13/07/2022 01:41 | Application extens... | 177 KB |
| sti.dat | 13/07/2022 01:41 | DAT File | 325 KB |
| tquery.dll | 13/07/2022 01:41 | Application extens... | 3,230 KB |
| Windows.Media.dll | 14/06/2022 21:53 | Application extens... | 7,374 KB |
| Windows.UI.Core.TextInput.dll | 13/07/2022 01:41 | Application extens... | 1,016 KB |
| WordBreakers.dll | 13/07/2022 01:41 | Application extens... | 43 KB |
| WSManMigrationPlugin.dll | 13/07/2022 01:41 | Application extens... | 87 KB |
| WsmAuto.dll | 13/07/2022 01:41 | Application extens... | 176 KB |

*Figure 3 – Extracted contents of "SolarWinds-Orion-NPM-Eval.zip"*

The “Solarwinds-Orion-NPM-Eval.exe” file contains a digital certificate from “Wechapaisch Consulting & Construction Limited.” The threat actor previously used the same certificate information in the “advancedipscanner.msi” file, a detail which we uncovered in our previous investigation into this threat actor. It is important to note that the legitimate file is digitally signed by “SolarWinds Worldwide, LLC.”

The “Solarwinds-Orion-NPM-Eval.exe” contains three embedded x64 files in the resource section:

- **X86** – Contains “c:\users\123\source\repos\ins_asi\win32\release\instlib.pdb,” the same PDB path we have previously seen in the “setup.exe” files.
- **X87** – A clean, digitally signed, SolarWinds Orion installer.
- **X88** – RomCom RAT dropper. This DLL invokes “rundll32.exe” and runs the “fwdTst” export, which drops x64 RomCom RAT in “C:\Users\user\AppData\Local\Temp\winver.dll” location.

| | |
|---|---|
| **Hashes (md5, sha-256)** | 4E4ECA58B896BDB6DB260F21EDC7760A<br><br>ABE9635ADBFEE2D2FBAEA140625C49ABE3BAA29C44FB53A65A9CDA02121583EE |
| **ITW File Name** | combase32.dll, winver.dll |
| **Compilation Stamp** | Tue Aug 02 16:20:43 2022 |
| **File Type/Signature** | PE 64 DLL |
| **File Size** | 623616 bytes |
| **Compiler Name/Version** | Microsoft Visual C++ |
| **C2** | combinedresidency[.]org |

## KeePass RomCom Campaign

On Nov. 1, the BlackBerry Threat Research and Intelligence Team made another discovery. The RomCom team created a new attack campaign abusing a popular password keeper called KeePass. When someone downloads the application from the fake but l*egitimate-looking* KeePass website, the attacker drops a malicious bundle onto the victim’s machine with the name "KeePass-2.52."


*Figure 4 – Legitimate KeePass website*

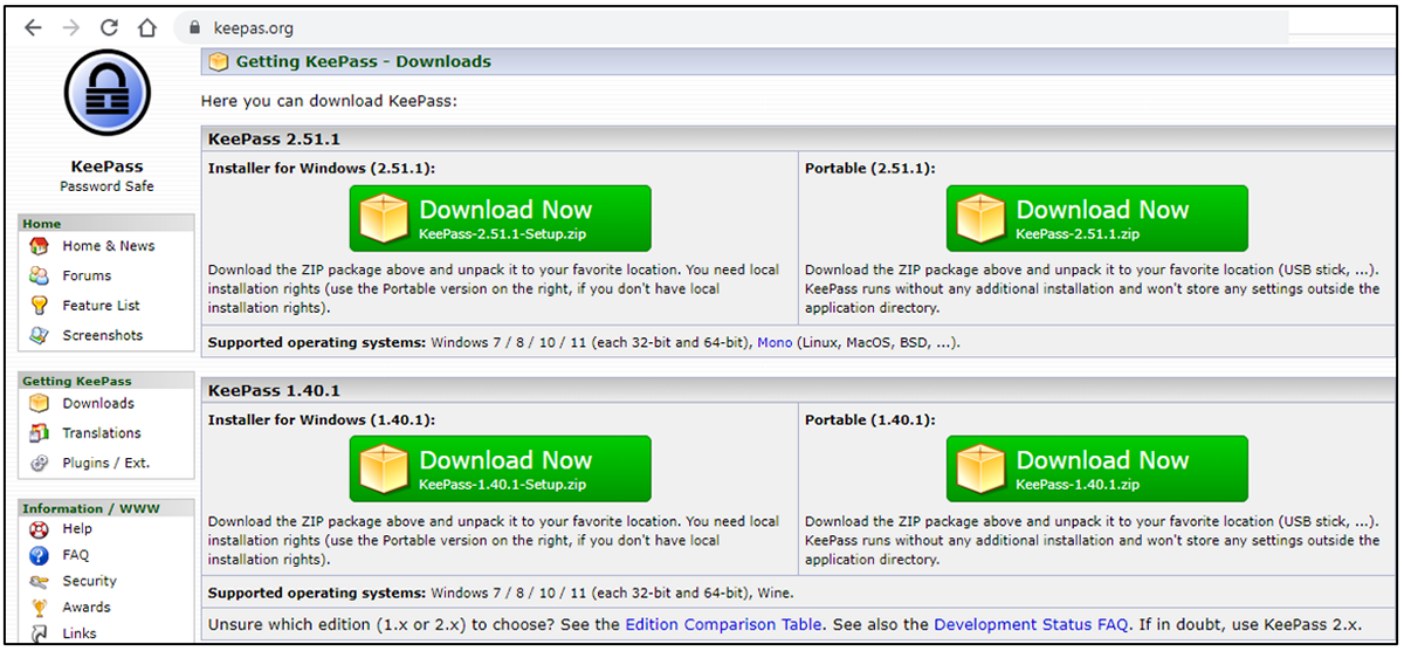



*Figure 5 – Fake KeePass website*

The fake KeePass.org website drops a Trojanized bundle called "KeePass-2.52.zip." Once unpacked, it contains the following files:

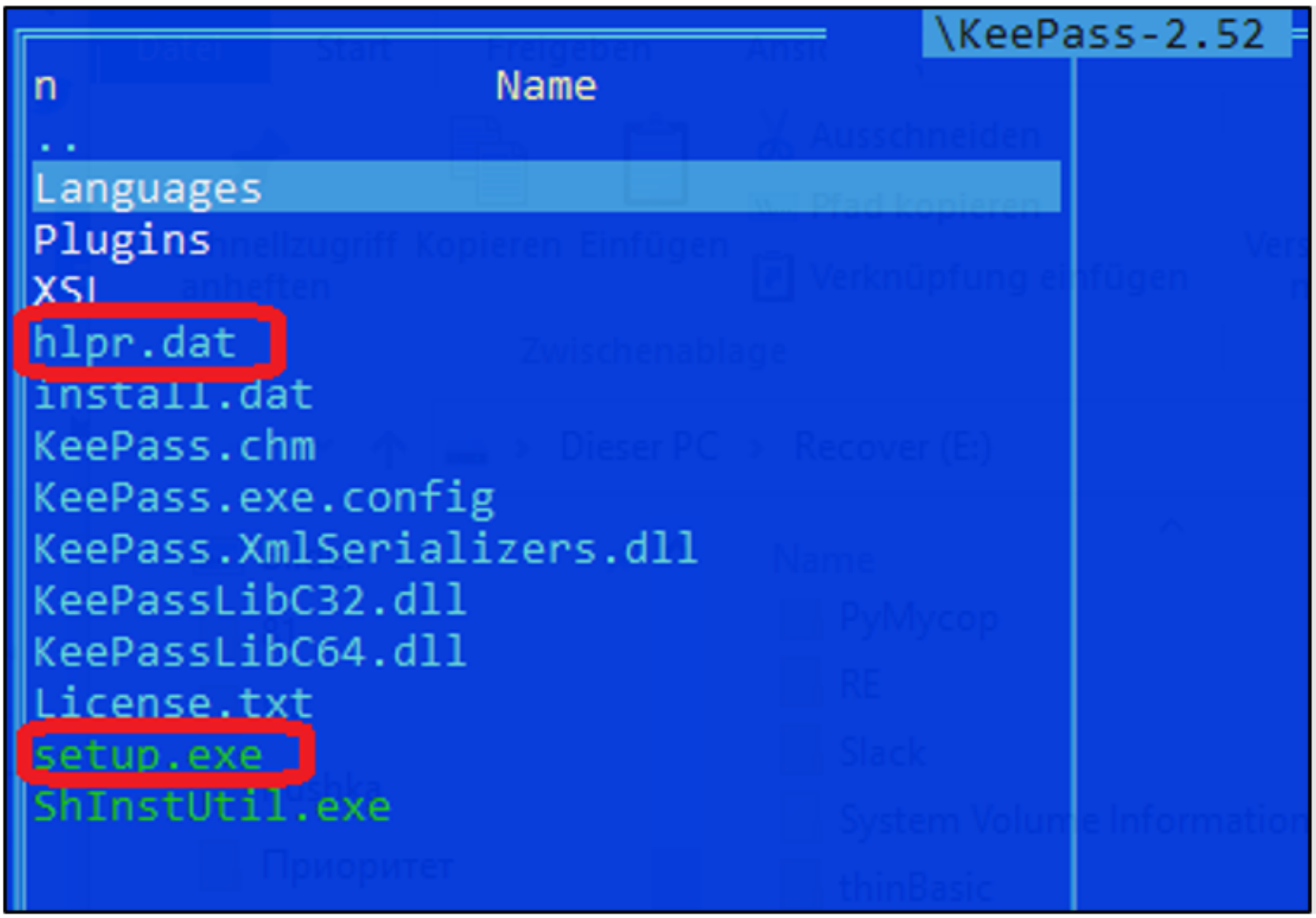



*Figure 6 – Contents of the malicious archive*

As shown in the screenshot above, two malicious files are contained in the **KeePass-2.52.zip** file:

- **Setup.exe** – The file that launches the RomCom RAT dropper: PDB C:\Users\123\source\repos\ins_asi\Win32\Release\setup.pdb
- **hlpr.dat** is a RomCom RAT dropper.

Our team followed the RomCom Netflows and uncovered both spoofed KeePass and PDF Reader Pro sites in Ukrainian language. Both of these spoofed websites host their terms of service pages on the same URL and imply the software providers are hosted by UK companies.

href="privacy/uk_privacy.html"
href="privacy/uk_term.html"
href="privacy/uk_disclaimer.html"

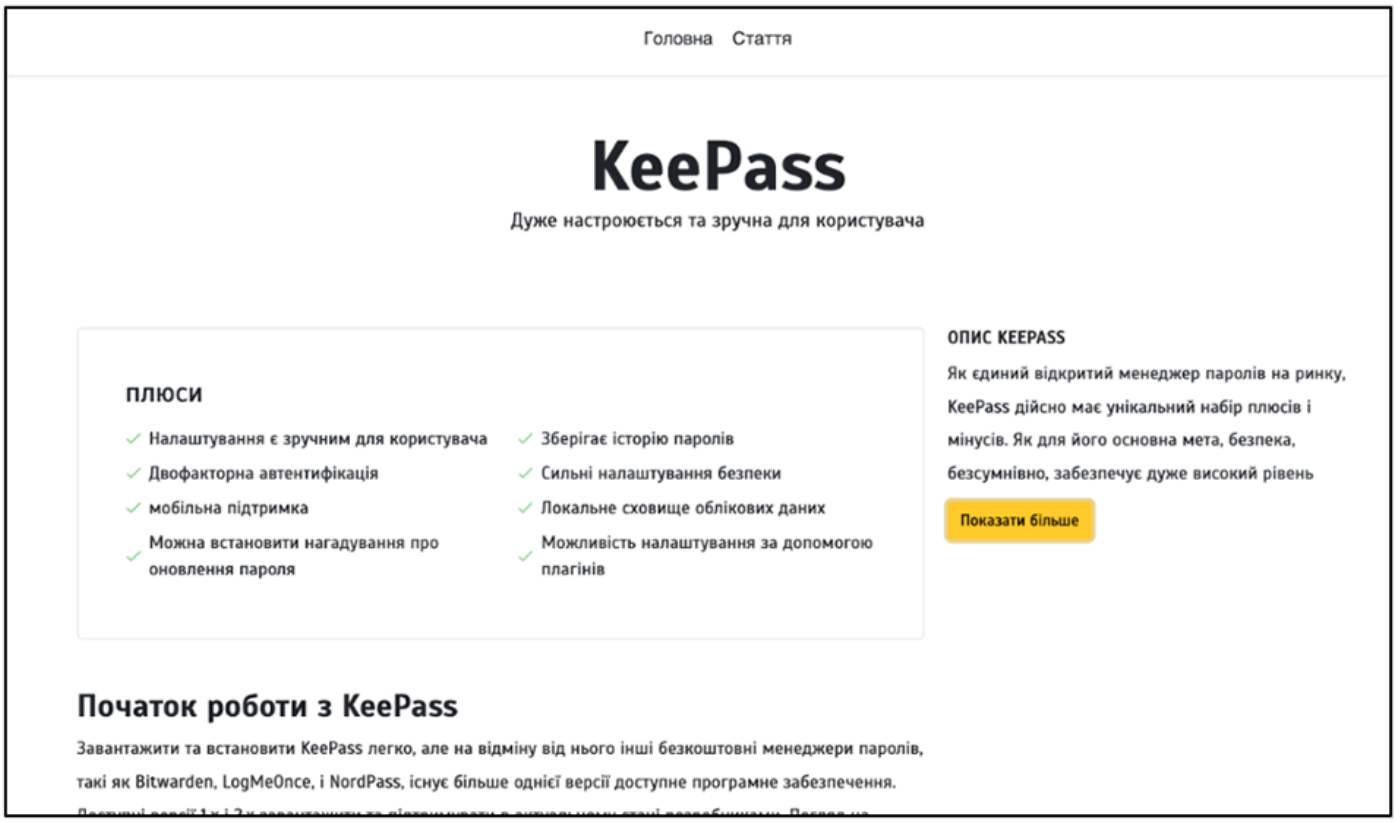



*Figure 7 – KeePass spoofed website in Ukrainian*


*Figure 8 – PDF Reader Pro spoofed website in Ukrainian*

Netflow analysis by the BlackBerry Research and Intelligence Team also led to the discovery of a new C2 registered on Oct. 27, utilizing SSL certificates that emulate UK ownership:

Issuer: C=GB, ST=Greater London, L=Harmondsworth, O=British Government, OU=dgtlocean.com, CN=ca dgtlocean.com/emailAddress=ca(at)mail.com Issuer: C=GB, ST=Greater London, L=London, O=Government Digital Service, OU=you-supported.com, CN=ca you-supported.com/em

depth=0 C = GB, ST = British, L = Chesterfield, O = Royal Mail Group Ltd, OU = Group1, CN = Group1.A, emailAddress = server(at)mail.com

## Conclusions

The RomCom threat actor is actively deploying new campaigns targeting victims in Ukraine and English-speaking targets worldwide. Based on the TOS, it is possible that victims in the United Kingdom are a new target, while Ukraine continues to be the main focus.

RomCom RAT, Cuba Ransomware, and Industrial Spy have an apparent connection. Industrial Spy is a relatively new ransomware group that emerged in April 2022. However, given the targets' geography and characteristics, combined with the current geopolitical situation, it's unclear if the real motivation of the RomCom threat actor is purely cybercriminal in nature.

## RomCom RAT Indicators of Compromise (IoCs)

| | |
|---|---|
| **Filename** | **Solarwinds-Orion-NPM-Eval.zip** |
| **MD5** | 7C003B4F8B3C0AB0C3F8CB933E93D301 |
| **SHA256** | 246DFE16A9248D7FB90993F6F28B0EBE87964FFD2DCDB13105096CDE025CA614 |
| **Filename** | **KeePass-2.52.zip** |
| **MD5** | 1a21a1e626fd342e794bcc3b06981d2c |
| **SHA256** | 596eaef93bdcd00a3aedaf6ad6d46db4429eeba61219b7e01b1781ebbf6e321b |
| **Filename** | **Solarwinds-Orion-NPM-Eval.exe** |
| **MD5** | D1A84706767BFB802632A262912E95A8 |
| **SHA256** | 9D3B268416D3FAB4322CC916D32E0B2E8FA0DE370ACD686873D1522306124FD2 |
| **Type** | **RomCom RAT Dropper** |
| **MD5** | CB933F1C913144A8CA6CFCFD913D6D28 |
| **SHA256** | AC09CBFEE4CF89D7B7A755C387E473249684F18AA699EB651D119D19E25BFF34 |
| **MD5** | 8284421bbb94f3c37f94899cdcd19afd |
| **SHA256** | 8b8dff5d30802fd79b76ee1531e7d050184a07570201ef1cd83a7bb8fa627cb0 |
| **Type** | **RomCom RAT Launcher (Setup.exe)** |
| **MD5** | 6310A2063687800559AE9D65CFF21B0A |
| **SHA256** | F7013CE417FCBA0F36C4B9BF5F8F6E0E2B14D6ED33FF4D384C892773508E932E |
| **MD5** | 550f42c5b555893d171285dc8b15b4b5 |
| **SHA256** | 5f187393acdeb67e76126353c74b6080d3e6ccf28ae580658c670d8b6e4aacc1 |
| **Type** | **RomCom RAT Payload** |
| **MD5** | 4E4ECA58B896BDB6DB260F21EDC7760A |
| **SHA256** | ABE9635ADBFEE2D2FBAEA140625C49ABE3BAA29C44FB53A65A9CDA02121583EE |
| **MD5** | a7172aef66bb12e1bb40a557bb41e607 |
| **SHA256** | 3252965013ec861567510d54a97446610edba5da88648466de6b3145266386d9 |