Patchwork APT caught in its own web

blog.malwarebytes.com/threat-intelligence/2022/01/patchwork-apt-caught-in-its-own-web

January 7, 2022

Patchwork is an Indian threat actor that has been active since December 2015 and usually targets Pakistan via spear phishing attacks. In its most recent campaign from late November to early December 2021, Patchwork has used malicious RTF files to drop a variant of the BADNEWS (Ragnatela) Remote Administration Trojan (RAT).

What is interesting among victims of this latest campaign, is that the actor has for the first time targeted several faculty members whose research focus is on molecular medicine and biological science.

Instead of focusing entirely on victimology, we decided to shade some light on this APT. Ironically, all the information we gathered was possible thanks to the threat actor infecting themselves with their own RAT, resulting in captured keystrokes and screenshots of their own computer and virtual machines.

Ragnatela

We identified what we believe is a new variant of the BADNEWS RAT called Ragnatela being distributed via spear phishing emails to targets of interest in Pakistan. Ragnatela, which means spider web in Italian, is also the project name and panel used by Patchwork APT.

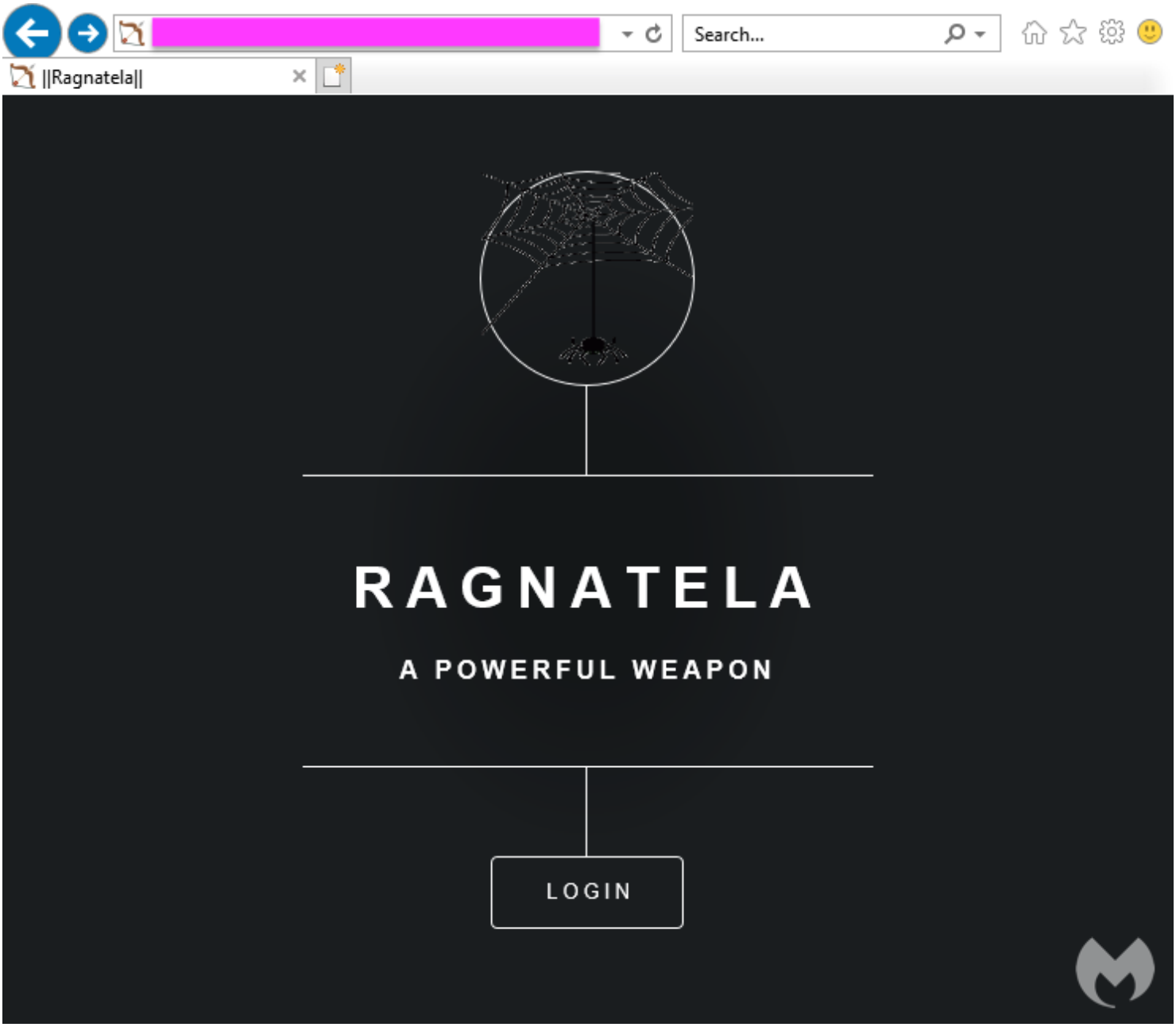

Figure 1: Patchwork's Ragnatela panel

Ragnatela RAT was built sometime in late November as seen in its Program Database (PDB) path *"E:\new_ops\jlitest __change_ops -29no – Copy\Release\jlitest.pdb"*. It features the following capabilities:

- Executing commands via cmd
- Capturing screenshots
- Logging Keystrokes
- Collecting list of all the files in victim's machine
- Collecting list of the running applications in the victim's machine at a specific time periods
- Downing addition payloads
- Uploading files

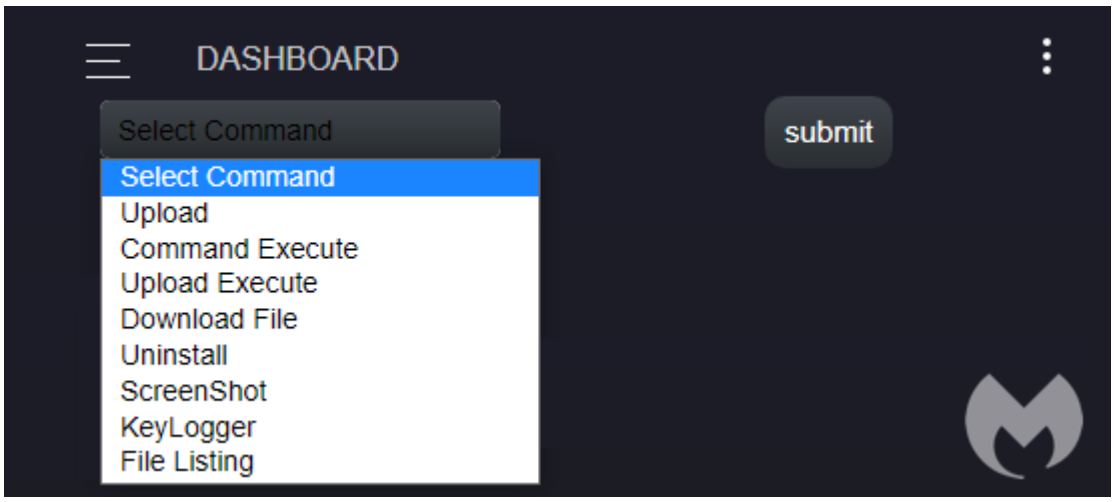

Figure 2: Ragnatela commands

In order to distribute the RAT onto victims, Patchwork lures them with documents impersonating Pakistani authorities. For example, a document called EOIForm.rtf was uploaded by the threat actor onto their own server at karachidha[.]org/docs/.

Figure 3: Threat actor is logged into their web control panel

That file contains an exploit (Microsoft Equation Editor) which is meant to compromise the victim's computer and execute the final payload (RAT).

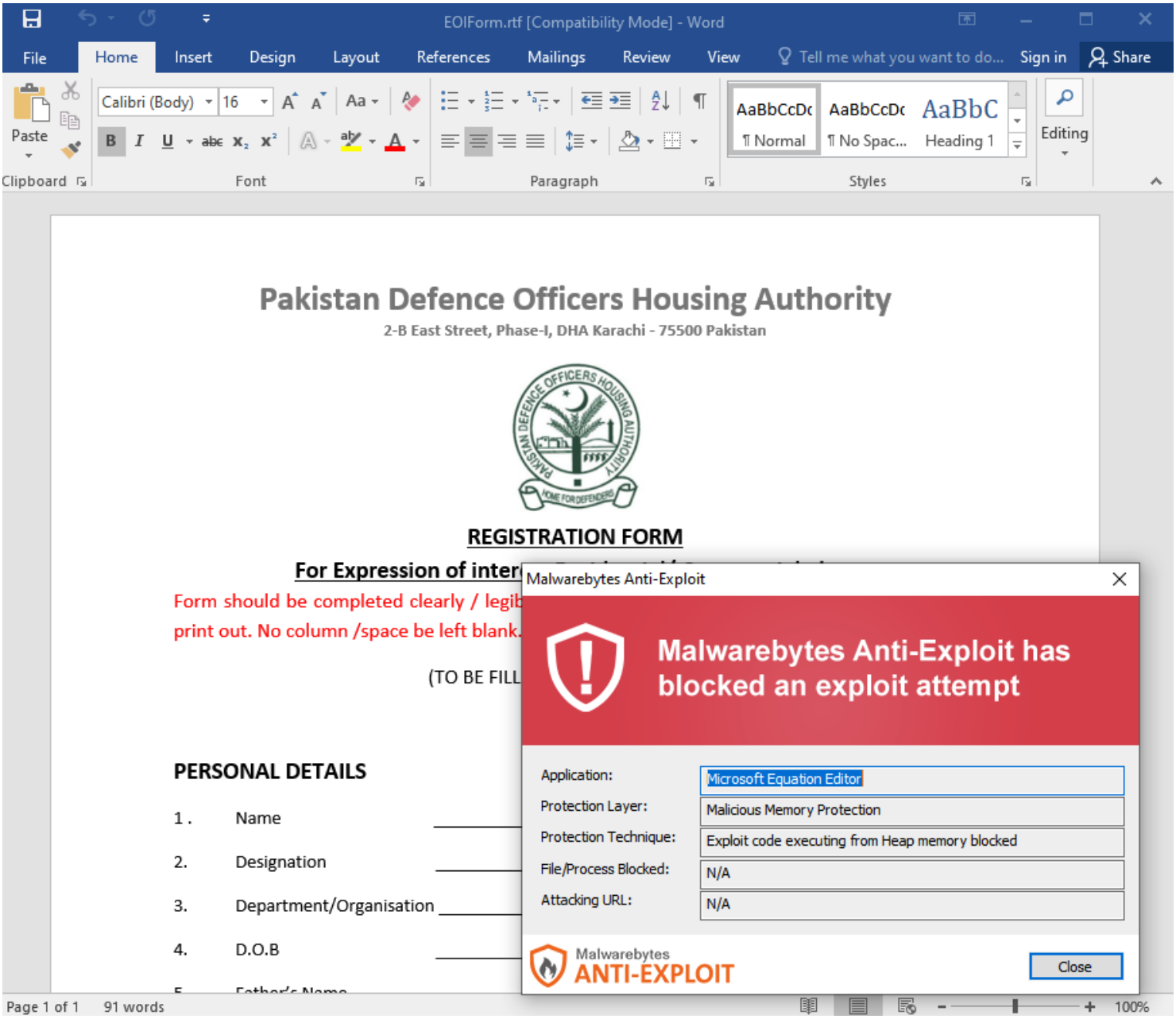

Figure 4: Malicious document triggers exploit

That payload is stored within the RTF document as an OLE object. We can deduce the file was created on December 9 2021 based on the source path information.

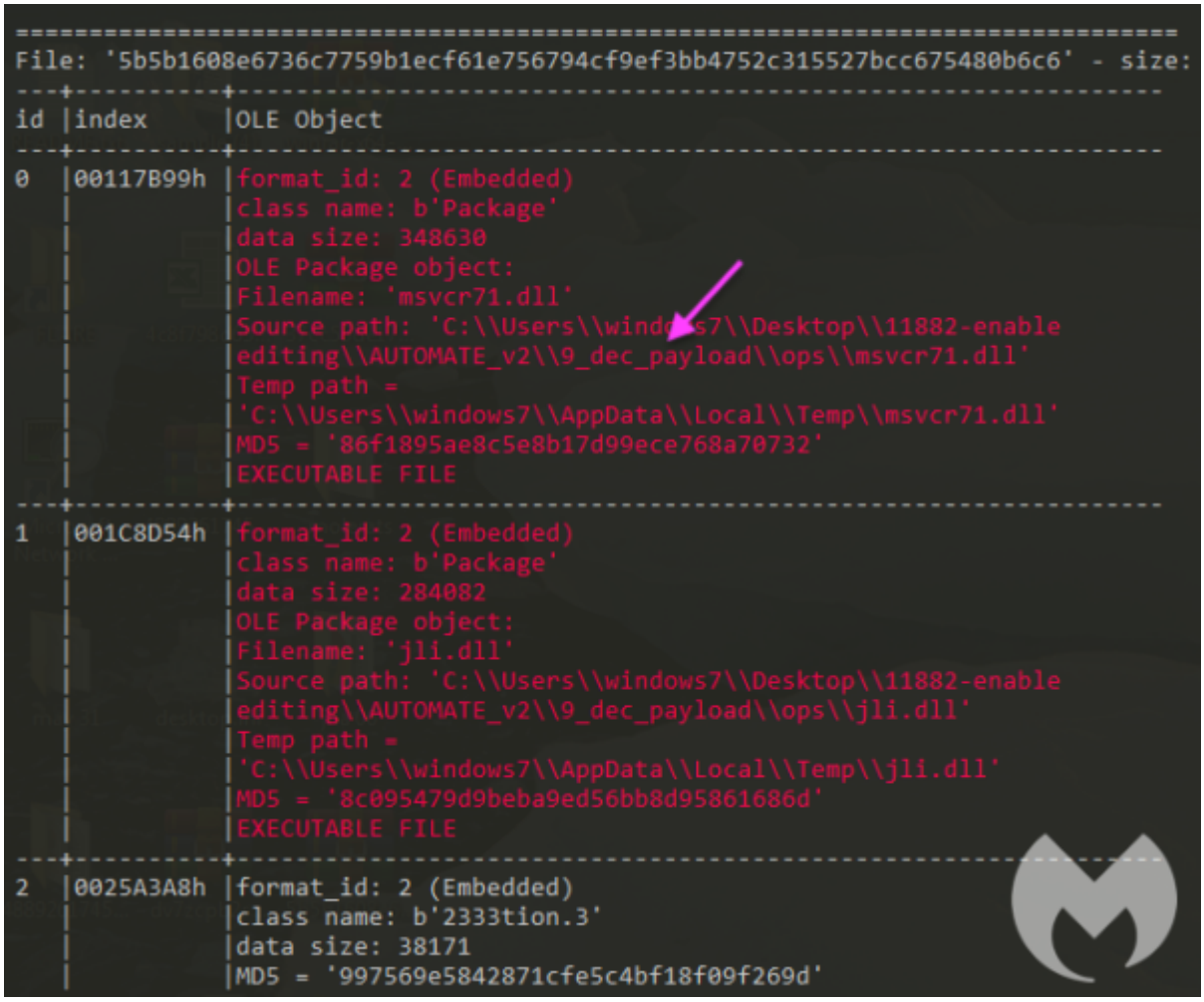

Figure 5: OLE object containing RAT

Ragnatela RAT communicates with the attacker's infrastructure via a server located at bgre.kozow[.]com. Prior to launching this campaign (in late November), the threat actor tested that their server was up and running properly.

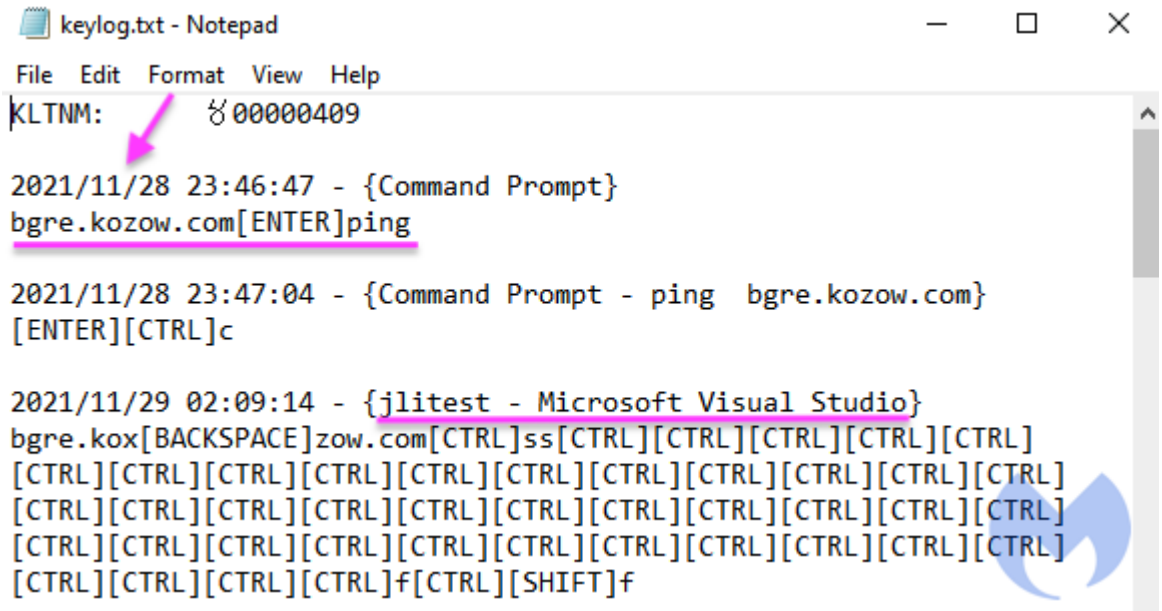

Figure 6: Log of threat actor typing a ping command

The RAT (jli.dll) was also tested in late November before its final compilation on 2021-12-09, along with MicroScMgmt.exe used to side-load it.

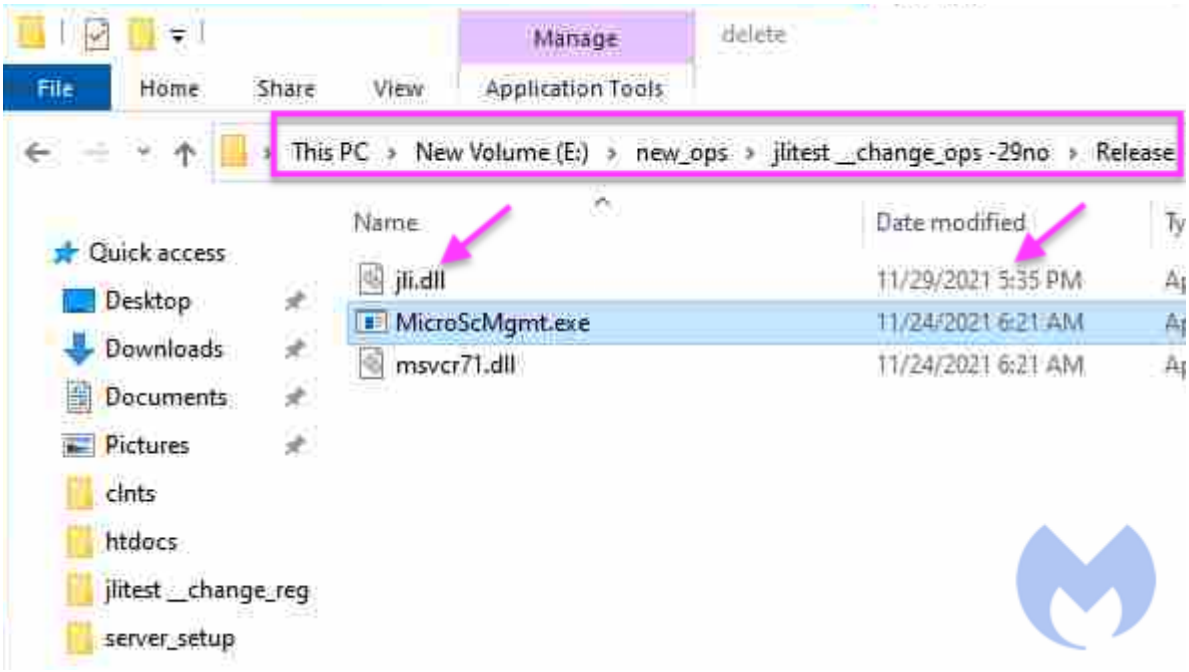

Figure 7: DLL for the RAT being compiled

Also in late November, we can see the threat actor testing the side-loading in a typical victim machine.

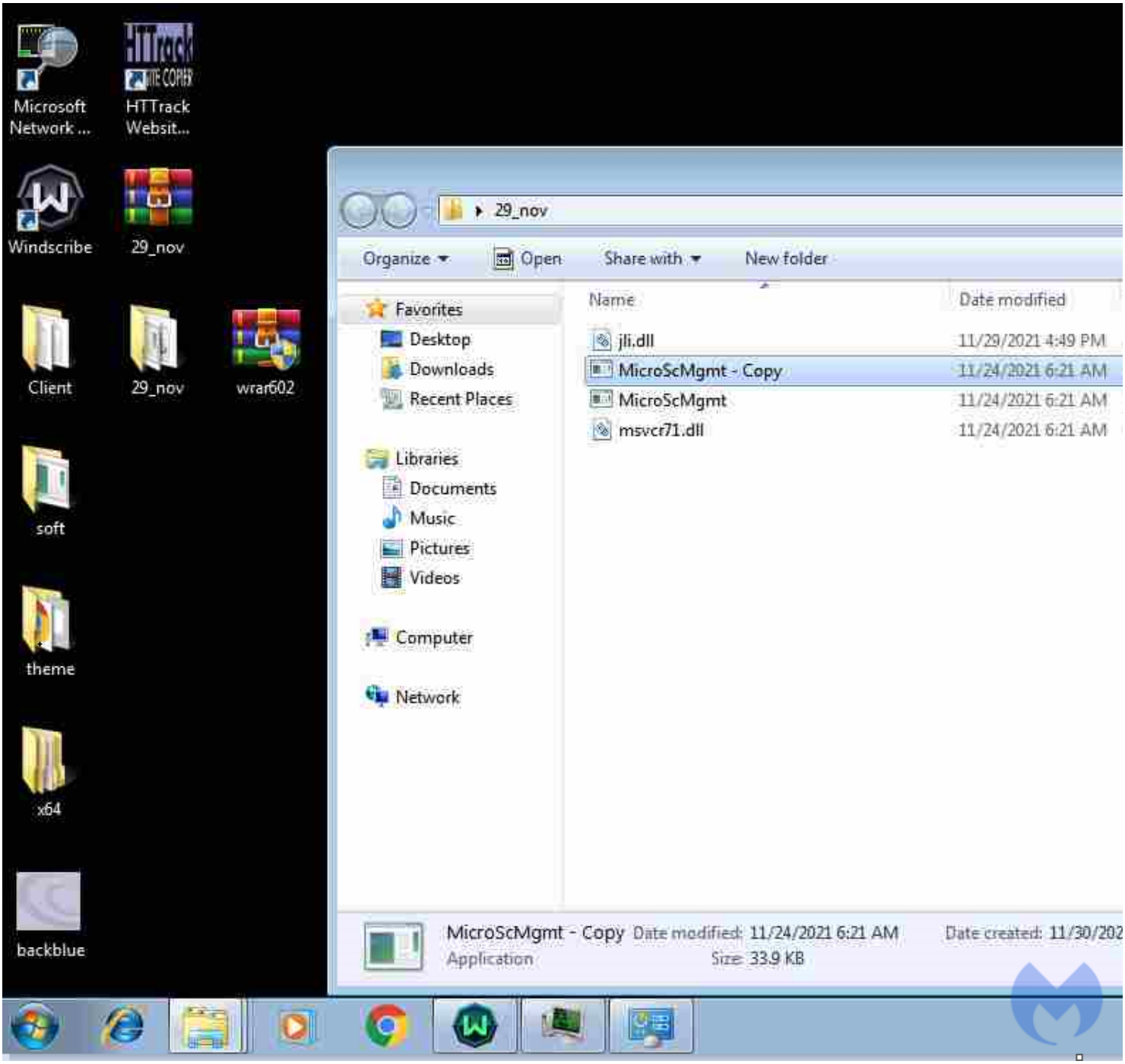

Figure 8: Threat actor tests RAT

Victims and victim

We were able to gain visibility on the victims that were successfully compromised:

- Ministry of Defense- Government of Pakistan
- National Defense University of Islam Abad
- Faculty of Bio-Science, UVAS University, Lahore, Pakistan
- International center for chemical and biological sciences
- HEJ Research institute of chemistry, International center for chemical and biological sciences, univeristy of Karachi
- SHU University, Molecular medicine

Another – unintentional – victim is the threat actor himself which appears to have infected is own development machine with the RAT. We can see them running both VirtualBox and VMware to do web development and testing. Their main host has dual keyboard layouts (English and Indian).

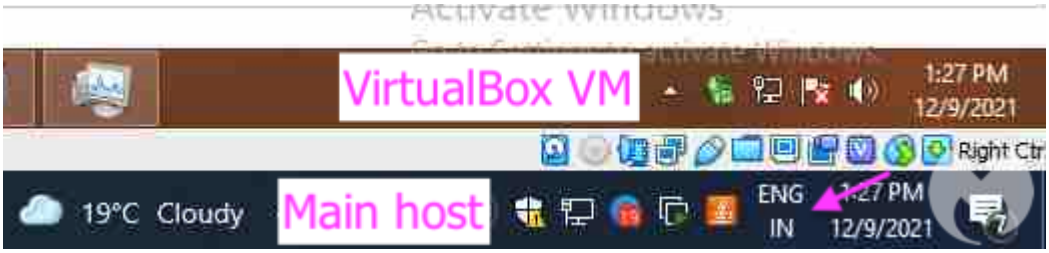

Figure 9: Virtual machine running on top of threat actor's main computer

Other information that can be obtained is that the weather at the time was cloudy with 19 degrees and that they haven't updated their Java yet. On a more serious note, the threat actor uses VPN Secure and CyberGhost to mask their IP address.

Figure 10: Threat actor uses VPN-S

Under the VPN they log into their victim's email and other accounts stolen by the RAT.

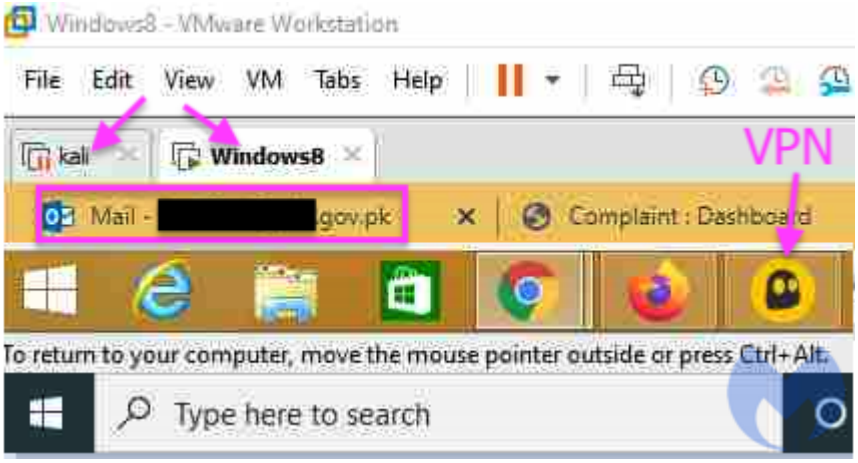

Figure 11: Threat actor logs into his victim's email using CyberGhost VPN

Conclusion

This blog gave an overview of the latest campaign from the Patchwork APT. While they continue to use the same lures and RAT, the group has shown interest in a new kind of target. Indeed this is the first time we have observed Patchwork targeting molecular medicine and biological science researchers.

Thanks to data captured by the threat actor's own malware, we were able to get a better understanding about who sits behind the keyboard. The group makes use of virtual machines and VPNs to both develop, push updates and check on their victims. Patchwork, like some other East Asian APTs is not as sophisticated as their Russian and North Korean counterparts.

Indicators of Compromise

Lure

karachidha[.]org/docs/EOIForm.rtf
5b5b1608e6736c7759b1ecf61e756794cf9ef3bb4752c315527bcc675480b6c6

RAT

jli.dll
3d3598d32a75fd80c9ba965f000639024e4ea1363188f44c5d3d6d6718aaa1a3

C2

bgre[.]kozow[.]com