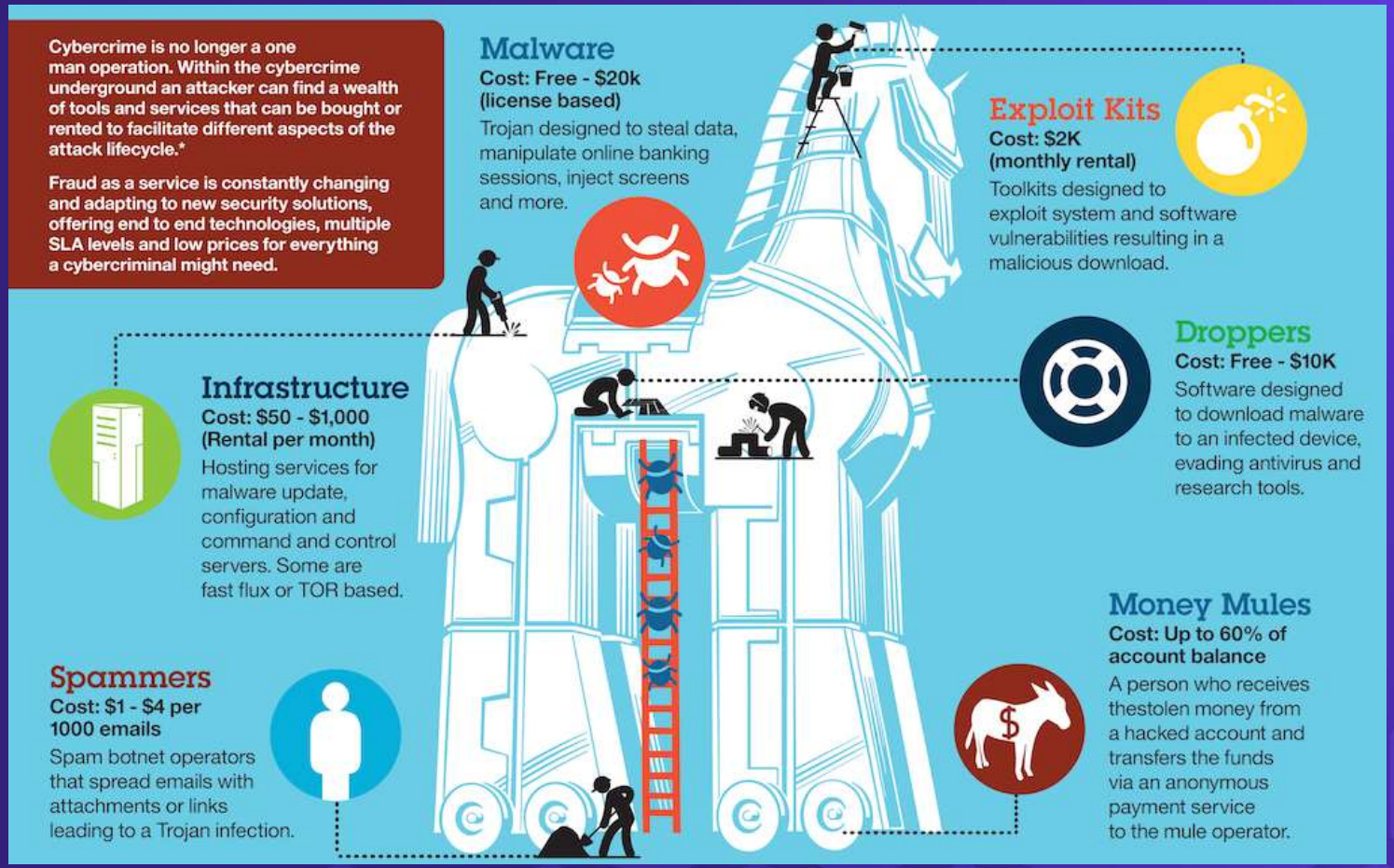
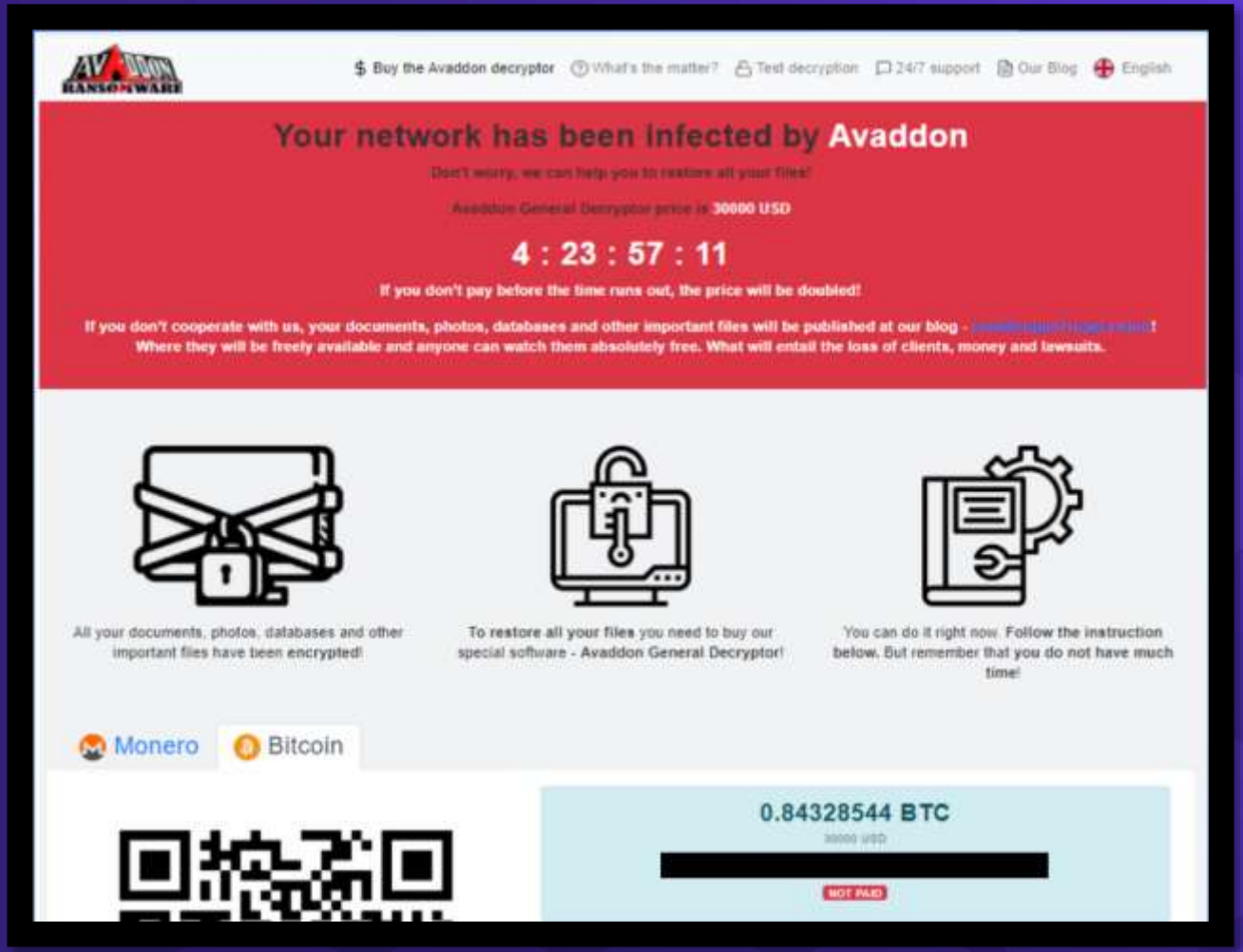
SecurityScorecard

Anatomy of a Ransomware Negotiation

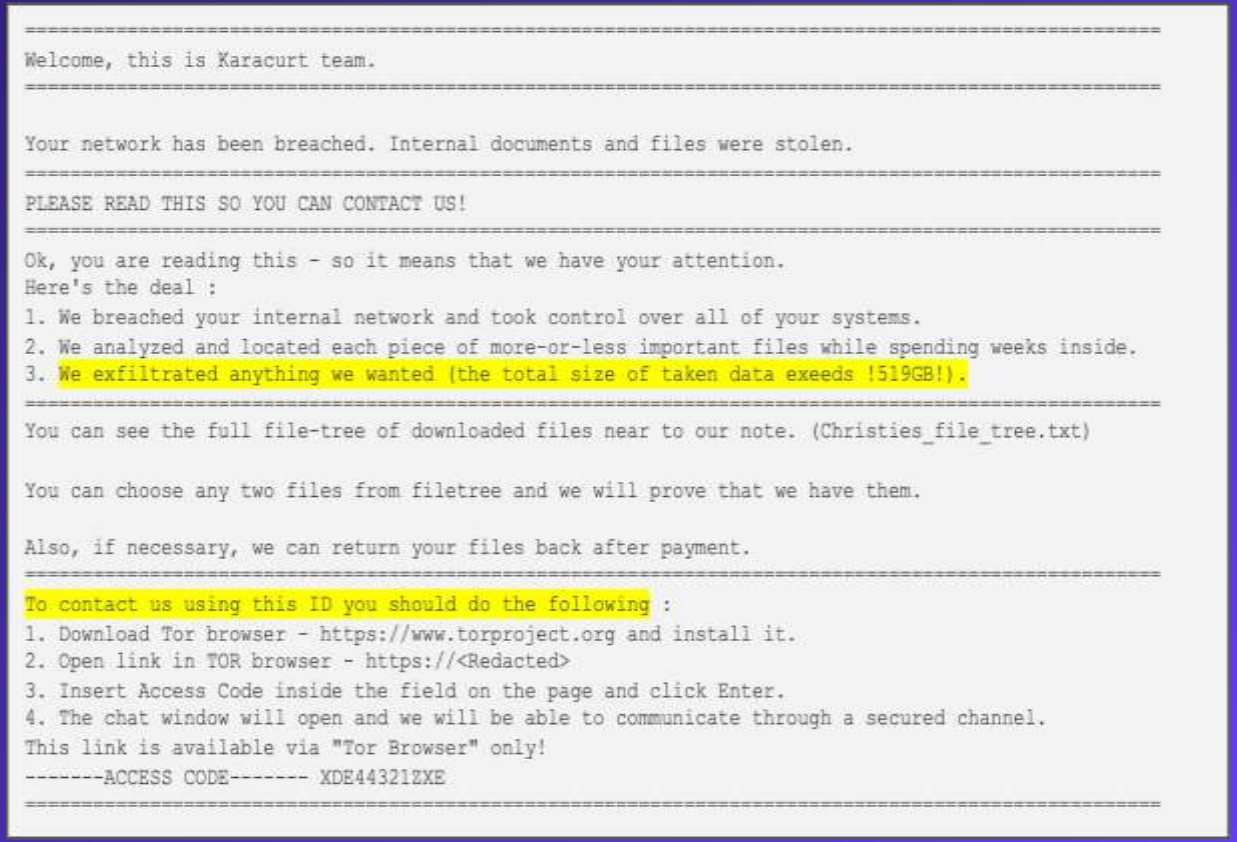
Douglas Domin
Supervisory Special Agent, Boston Cybercrime Squad, FBI

Larry Slusser
Vice President & Global Head Professional Services Delivery, SecurityScorecard





Karakurt Group



```
==========
Welcome, this is Karacurt team.
==========

Your network has been breached. Internal documents and files were stolen.
==========
PLEASE READ THIS SO YOU CAN CONTACT US!
==========
Ok, you are reading this - so it means that we have your attention.
Here's the deal :
1. We breached your internal network and took control over all of your systems.
2. We analyzed and located each piece of more-or-less important files while spending weeks inside.
3. We exfiltrated anything we wanted (the total size of taken data exeeds !519GB!).
==========
You can see the full file-tree of downloaded files near to our note. (Christies_file_tree.txt)

You can choose any two files from filetree and we will prove that we have them.

Also, if necessary, we can return your files back after payment.
==========
To contact us using this ID you should do the following :
1. Download Tor browser - https://www.torproject.org and install it.
2. Open link in TOR browser - https://<Redacted>
3. Insert Access Code inside the field on the page and click Enter.
4. The chat window will open and we will be able to communicate through a secured channel.
This link is available via "Tor Browser" only!
-------ACCESS CODE------- XDE44321ZXE
==========
```

Karakurt Group

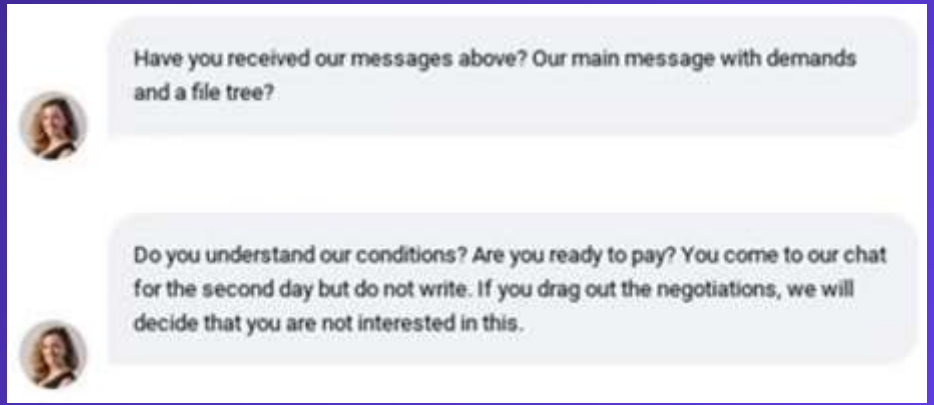
- Appeared in September 2021
- Threat actor started to publish stolen data on karakurt[.]tech and karakurt[.]group

Karakurt Group

- Threat actor asks for a ransom in Bitcoin
- Promises to delete the stolen data after payment

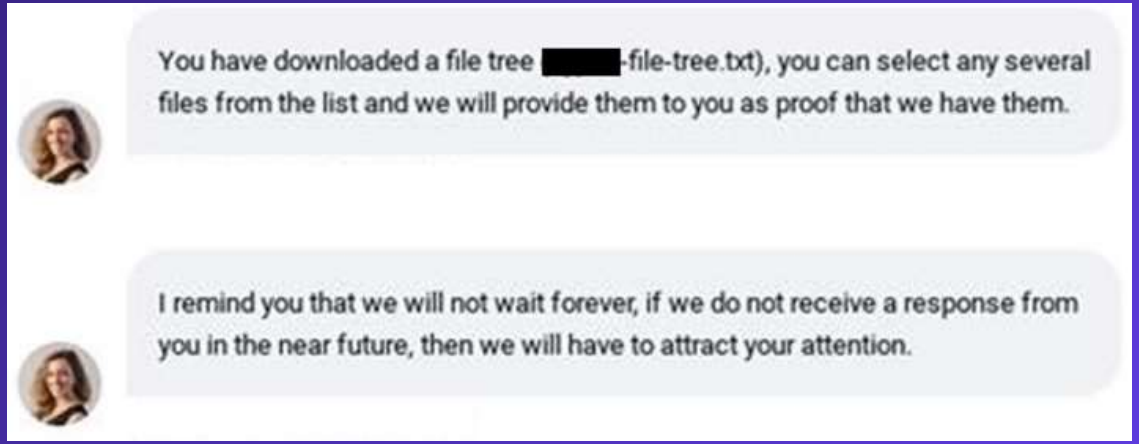
Karakurt Group

- Proof is given to the victim that multiple files were exfiltrated



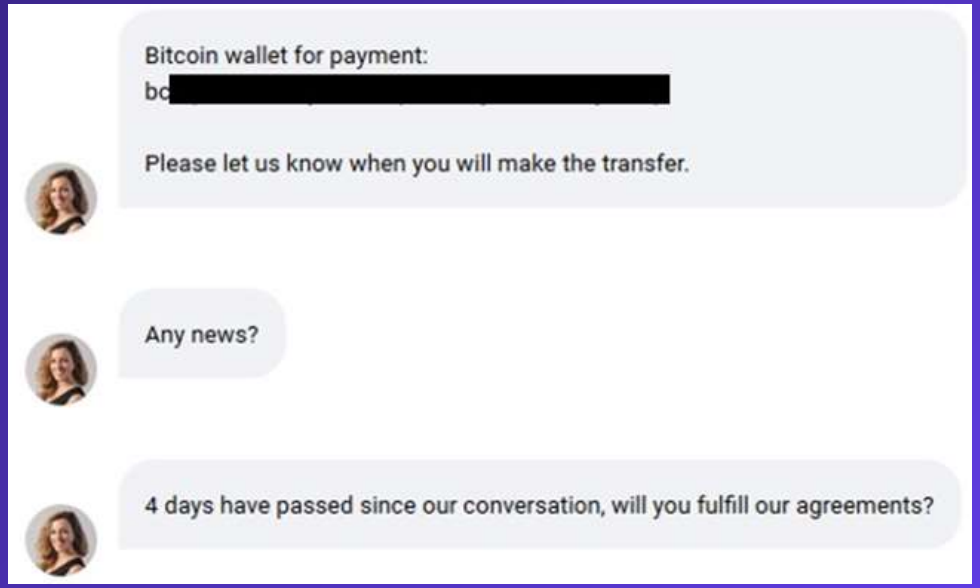
Karakurt Group

- Threat actor is willing to provide several files to the victim as a stronger proof of exfiltration



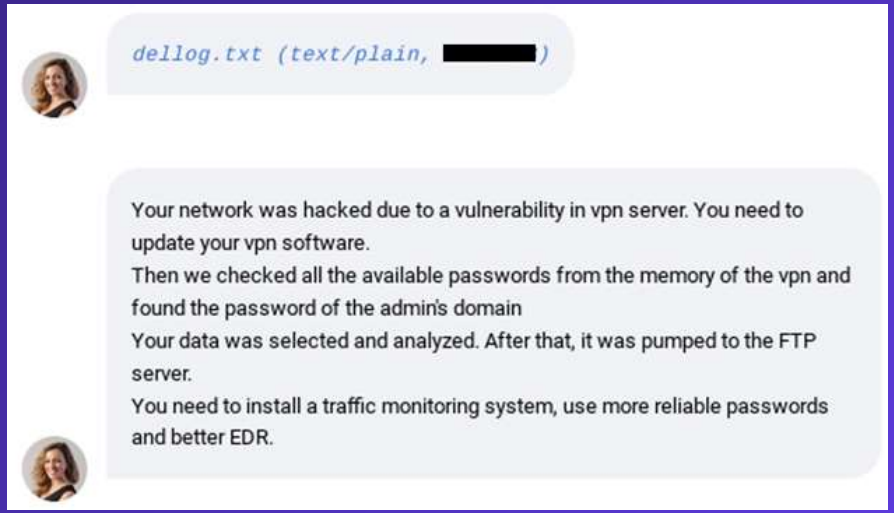
Karakurt Group

- Bitcoin address is provided for payment and the group asks for regular updates

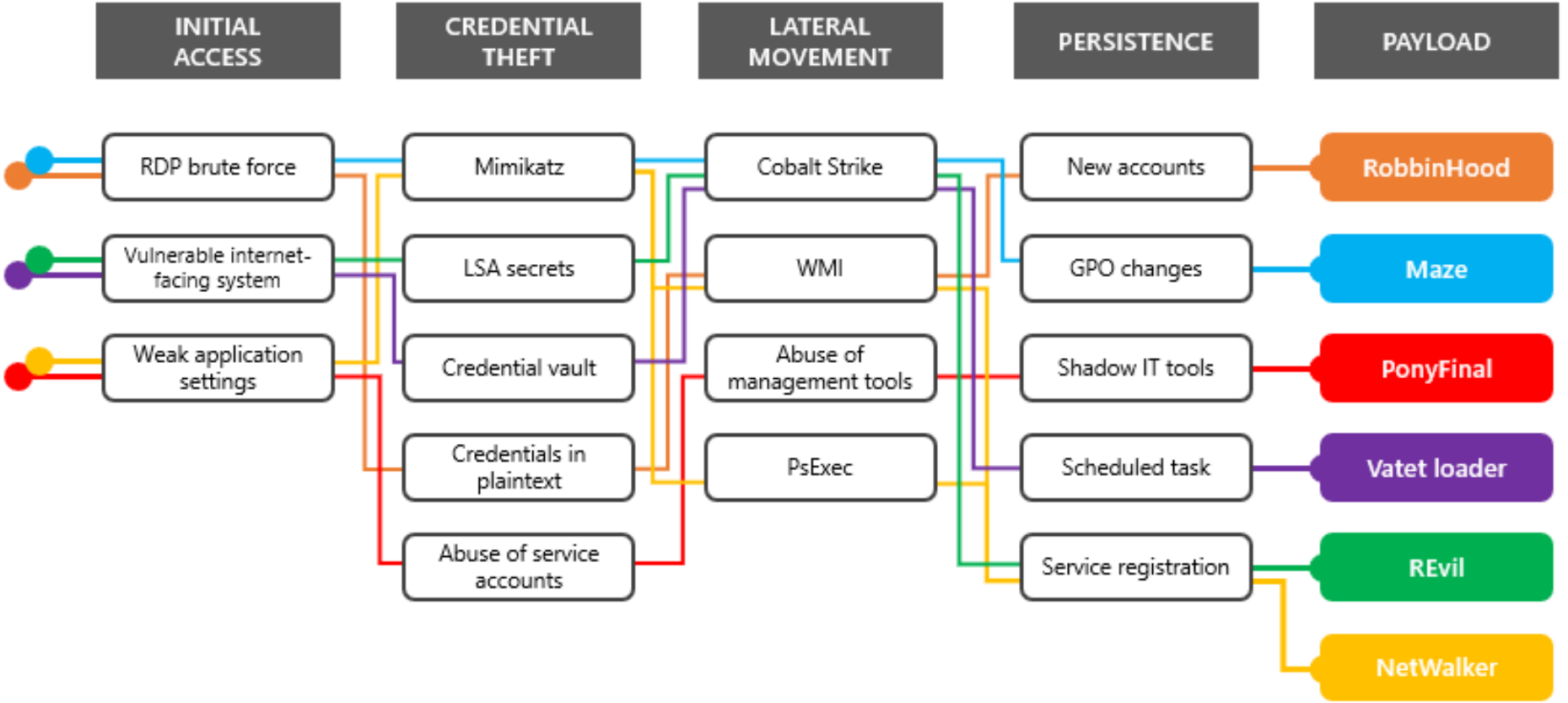


Karakurt Group

- After the victim paid the ransom, the threat actor provided evidence that the stolen data was deleted
- Karakurt explained the infection vector and gave recommendations to the victim



Never trust the threat actor!



Thank You