



Anatomy of a Ransomware Negotiation

Douglas Domin

Supervisory Special Agent, Boston Cybercrime Squad, FBI

Larry Slusser

Vice President & Global Head Professional Services Delivery, SecurityScorecard

Cybercrime is no longer a one man operation. Within the cybercrime underground an attacker can find a wealth of tools and services that can be bought or rented to facilitate different aspects of the attack lifecycle.*

Fraud as a service is constantly changing and adapting to new security solutions, offering end to end technologies, multiple SLA levels and low prices for everything a cybercriminal might need.

Malware

Cost: Free - \$20k
(license based)

Trojan designed to steal data, manipulate online banking sessions, inject screens and more.



Exploit Kits

Cost: \$2K
(monthly rental)

Toolkits designed to exploit system and software vulnerabilities resulting in a malicious download.



Infrastructure

Cost: \$50 - \$1,000
(Rental per month)

Hosting services for malware update, configuration and command and control servers. Some are fast flux or TOR based.



Spammers

Cost: \$1 - \$4 per
1000 emails

Spam botnet operators that spread emails with attachments or links leading to a Trojan infection.



Droppers

Cost: Free - \$10K

Software designed to download malware to an infected device, evading antivirus and research tools.



Money Mules

Cost: Up to 60% of
account balance

A person who receives the stolen money from a hacked account and transfers the funds via an anonymous payment service to the mule operator.





Your network has been infected by Avaddon

Don't worry, we can help you to restore all your files!

Avaddon General Decryptor price is 30000 USD

4 : 23 : 57 : 11

If you don't pay before the time runs out, the price will be doubled!

If you don't cooperate with us, your documents, photos, databases and other important files will be published at our blog - <https://www.avaddondecryptor.com/>! Where they will be freely available and anyone can watch them absolutely free. What will entail the loss of clients, money and lawsuits.



All your documents, photos, databases and other important files have been encrypted!



To restore all your files you need to buy our special software - Avaddon General Decryptor!



You can do it right now. Follow the instruction below. But remember that you do not have much time!



0.84328544 BTC

30000 USD

NOT PAID

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 exceeds !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.

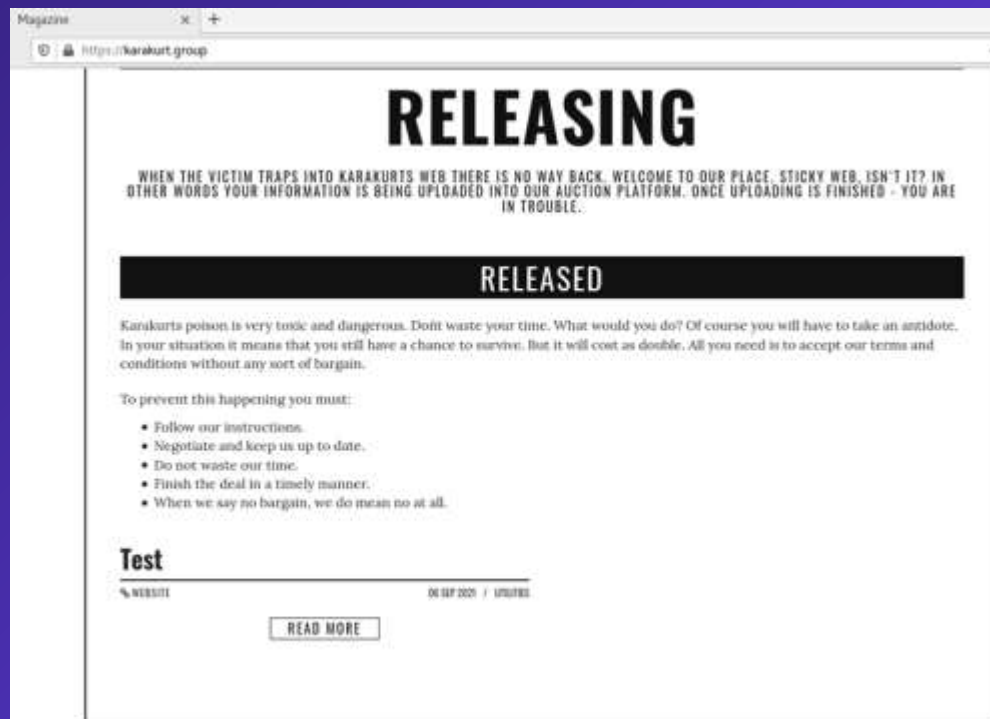
This link is available via "Tor Browser" only!

-----ACCESS CODE----- XDE443212XE

=====

Karakurt Group

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



Karakurt Group

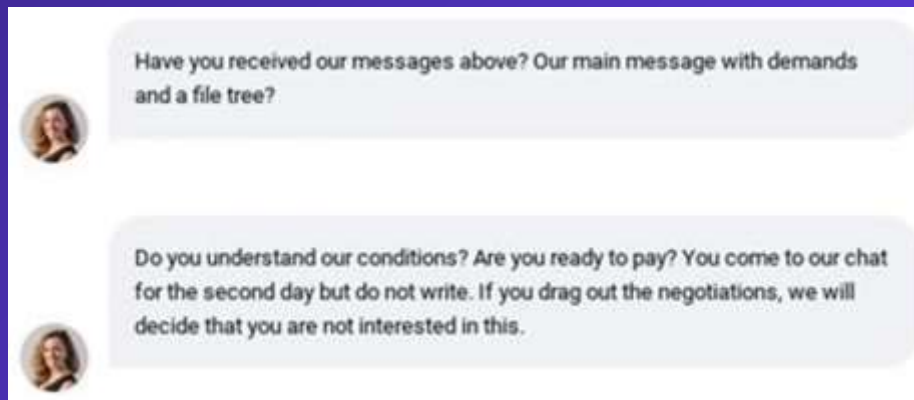
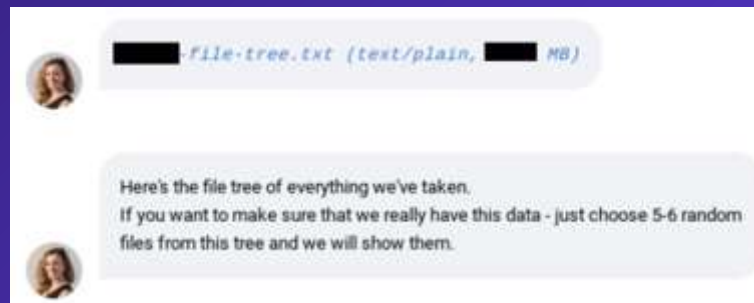
- Threat actor asks for a ransom in Bitcoin
- Promises to delete the stolen data after payment

Before we start, I would like to tell you how we operate. Unlike other teams or groups with similar modus operandi we do not like negotiations nor we negotiate at all. We will not lower our demand, but keeping it from the start within your reach. Our price is just \$300000 in bitcoin. When we have the money we will completely delete all the taken data from our servers, rewrite the hard disks and later delete the virtual images where it was kept. Currently we have all the offline copies, so none of law enforcement agencies can trace it or deny access. We are ready to give you time by [REDACTED] to decide whether you are ready to pay or not. If you will remain silent by Friday we shall consider that you are not interested in keeping the incident private and we shall start further actions to get back your attention.



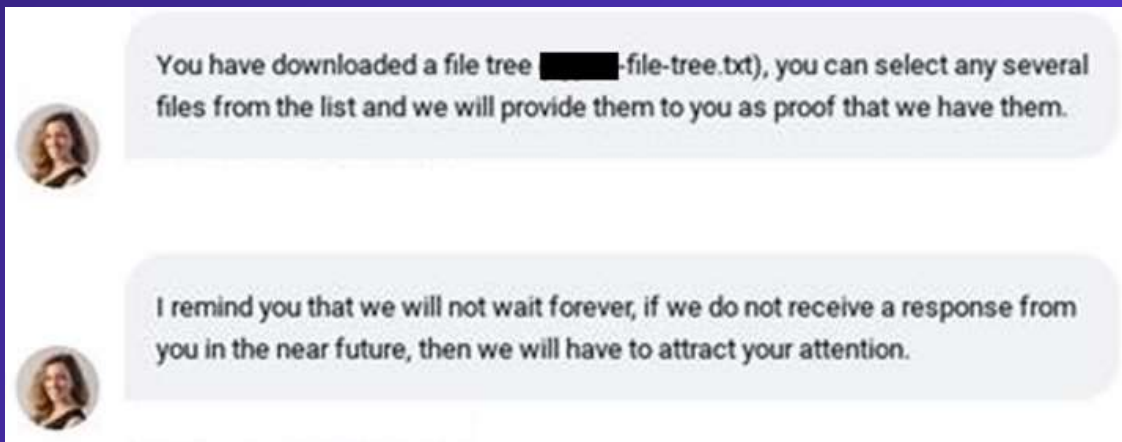
Karakurt Group

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



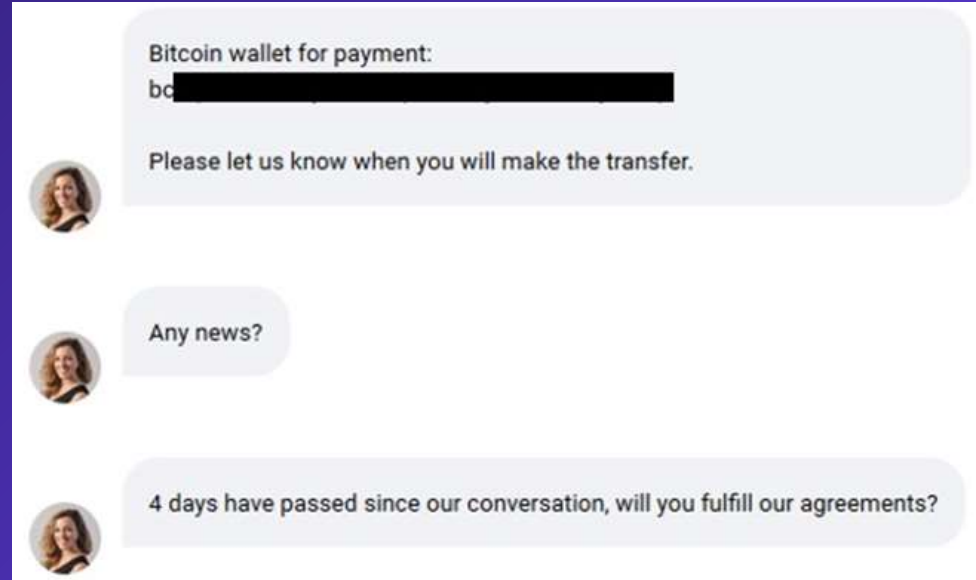
Karakurt Group

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



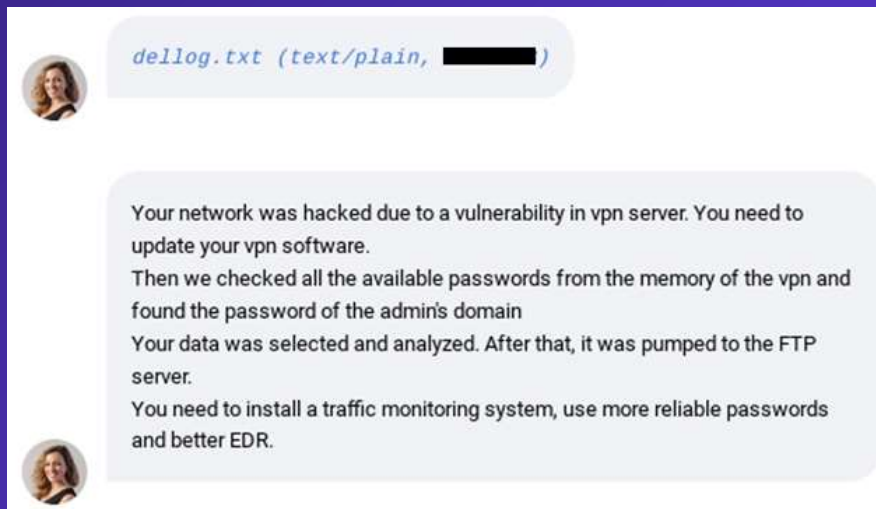
Karakurt Group

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

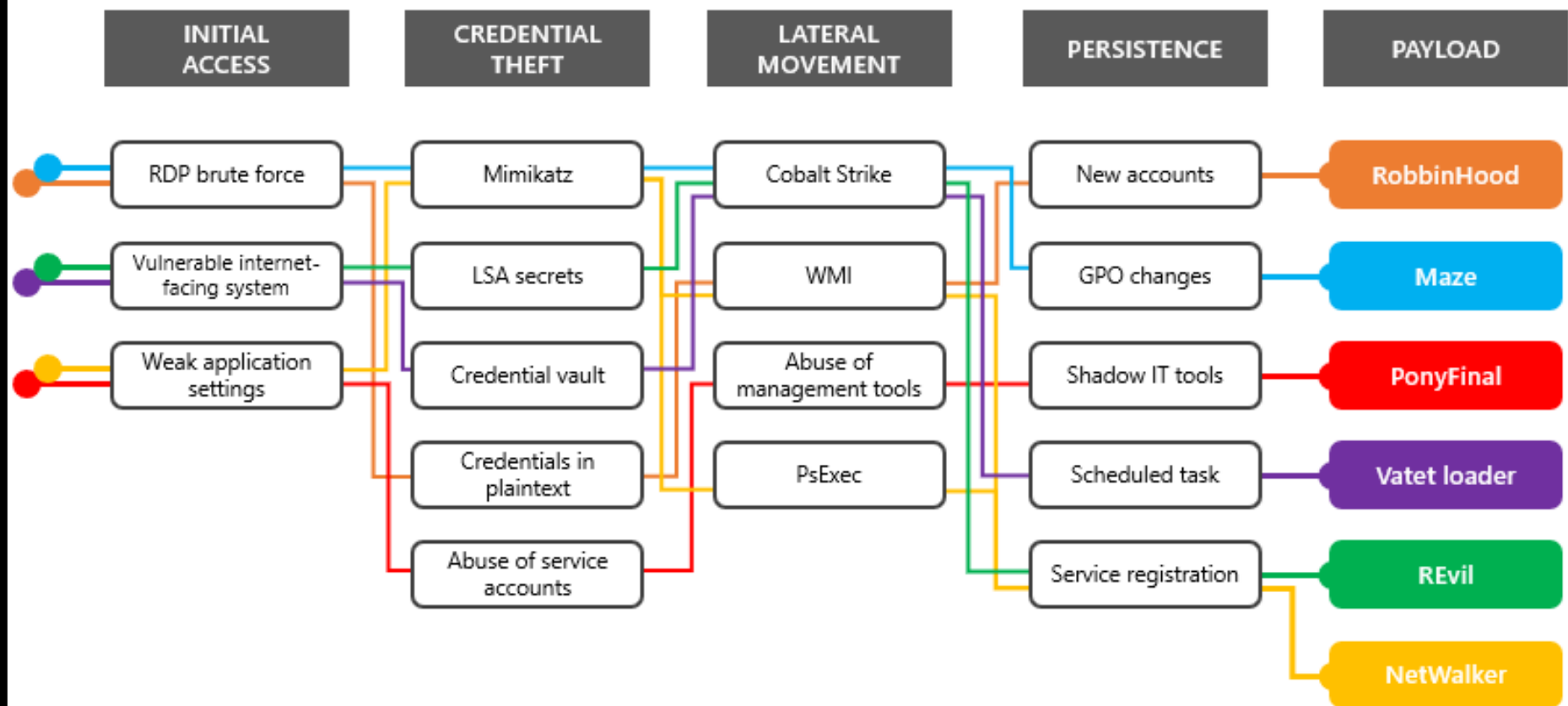


Karakurt Group

- 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**