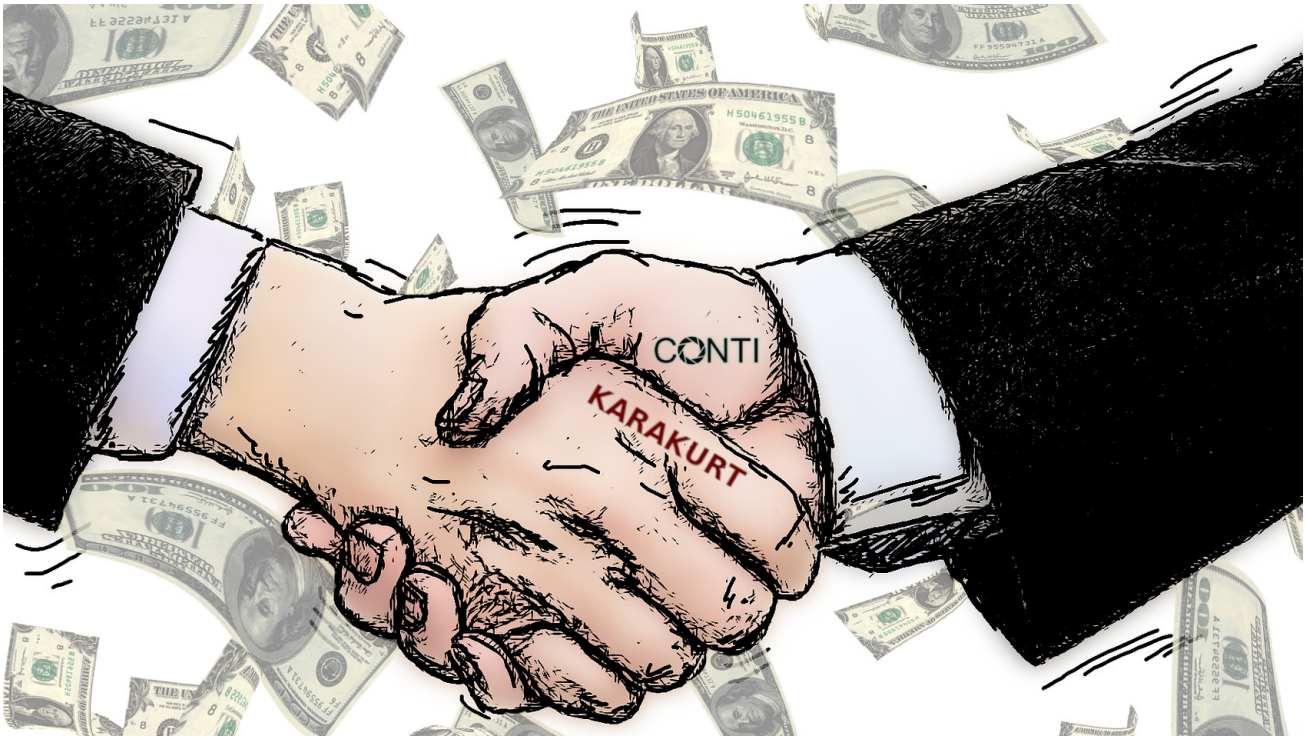
Karakurt revealed as data extortion arm of Conti cybercrime syndicate

bleepingcomputer.com/news/security/karakurt-revealed-as-data-extortion-arm-of-conti-cybercrime-syndicate/

Ionut Ilascu

By
Ionut Ilascu

- April 15, 2022
- 09:28 AM
- 2



After breaching servers managed by the cybercriminals, security researchers found a connection between Conti ransomware and the recently emerged Karakurt data extortion group, showing that the two gangs are part of the same operation.

The Conti ransomware syndicate is one of the most prolific cybercriminal groups today that operates unabated despite the massive leak of internal conversations and source code that a hacking group already used to cripple Russian organizations.

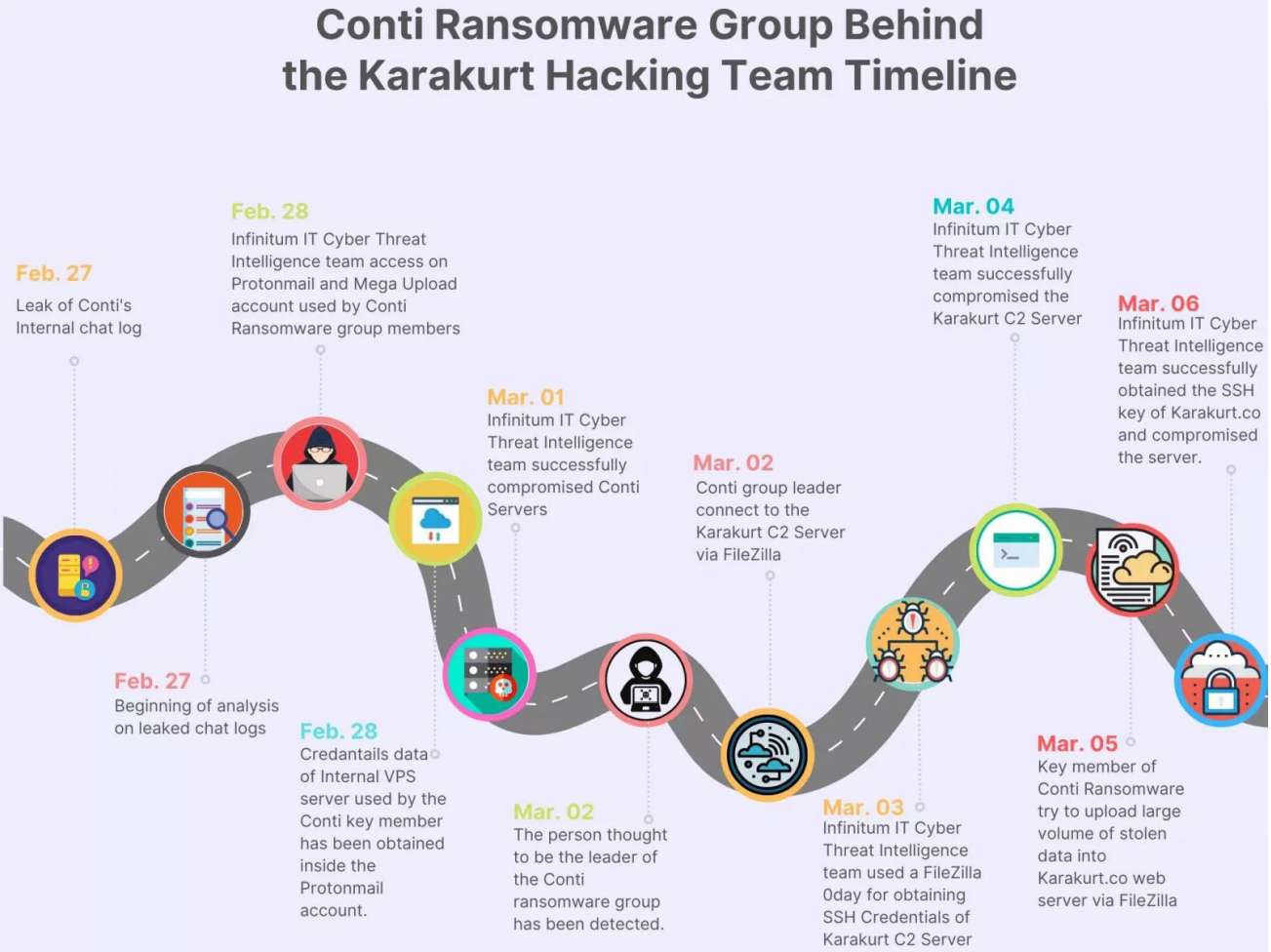
Karakurt is a gang active since at least June 2021 that focuses on stealing data from companies and forcing them into paying a ransom by threatening to publish the information.

More than 40 organizations have fallen victim to Karakurt in about two months, between September and November 2021.

Cybercriminal infrastructure pwned

The connection between the two groups was possible after security researchers gained access to an internal Conti VPS server with credentials for a user they believe to be the leader of the entire syndicate.

Logging into the server was possible after the researchers breached the threat actor's ProtonMail account and found the necessary access credentials.



source: Infinitum IT

When researchers accessed the VPS server, it stored more than 20TB of data that Conti stole from their victims before deploying the encryption stage of the attack.

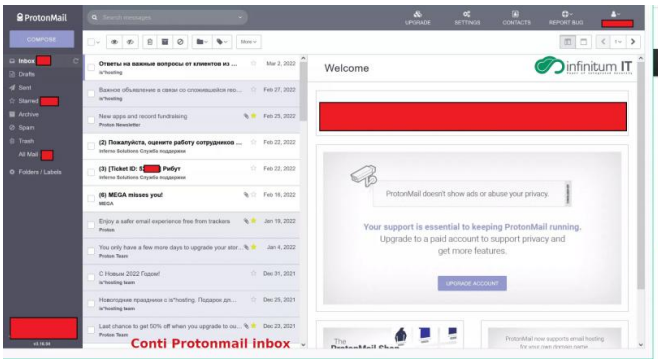
Security researchers at Infinitum Turkey-based security consulting company Infinitum IT say that the VPS server is hosted by Inferno Solutions, a provider in Russia that supports anonymous payment methods and accepts orders over VPN and TOR connections.

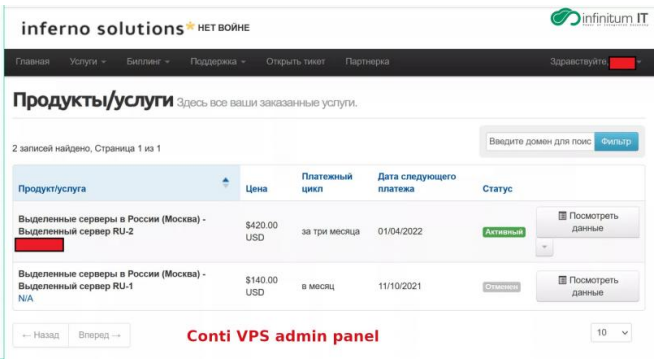
At the same time, Inferno Solutions claims that they “don't tolerate spammers, scammers or cybercriminals,” that they always side with the client, and that they “do not disturb clients in case of dubious and unlawful complaints (abuse).”

In a recent report, Infinitum IT details that they were able to gain access to Conti's infrastructure when the Conti leaks started, on February 27, after logging into multiple ProtonMail and Mega storage accounts used by one Conti member.

"At the beginning of Conti leak on February 27, 2022, we are able to get inside multiple Protonmail and Mega Upload accounts used by one of the key members of Conti Ransomware group" - Infinitum IT

Once inside the email accounts, the researchers observed incoming emails from Inferno Solutions hosting provider, which allowed them to gain remote access to the VPS server's administration panel.





source: Infinitum IT

The analysis of the information on the storage server revealed that Conti had data with an older timestamp belonging to victims that have not been disclosed publicly. Infinitum IT contacted the victims to return the stolen data.

The researchers noticed that the Conti member whose accounts they breached was using the FileZilla FTP client to connect to multiple servers for uploading and downloading stolen data.

One connection was to the IP address **209[.]222[.]98[.]19**, which is where the Karakurt extortion group hosted their site where they published stolen data from non-paying victims.

BleepingComputer learned months ago from Vitali Kremez of Advanced Intelligence that Karakurt is a side business of the Conti syndicate to monetize from failed encryption attacks.

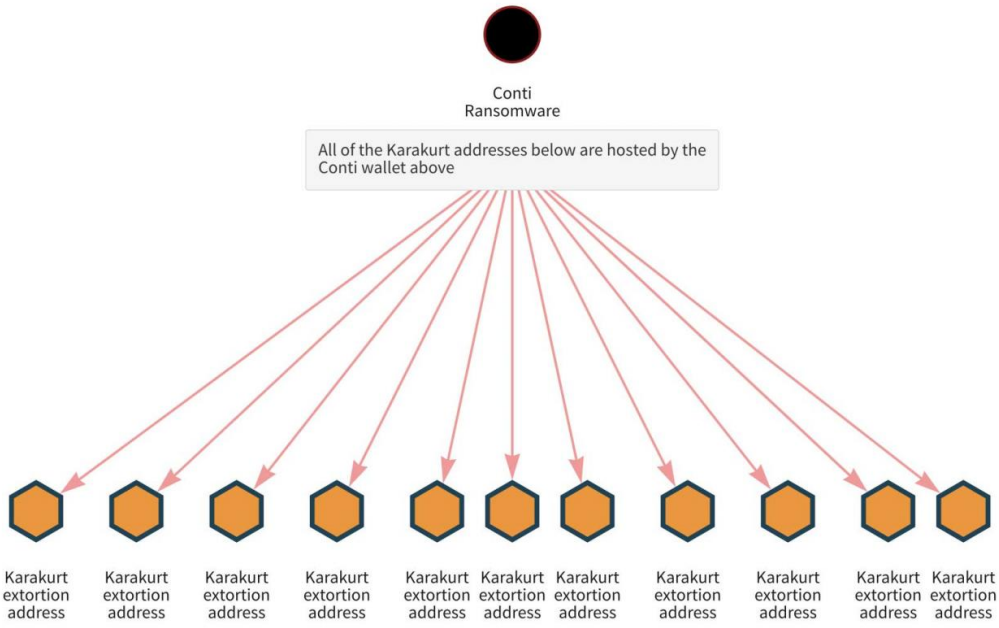
When Conti's ransomware payload is blocked and the attack does not enter the encryption stage, the hackers release the already exfiltrated information as Karakurt for data extortion.

This was confirmed today in a report from cybersecurity company Arctic Wolf stating that, during an investigation at a client that had previously paid Conti to unlock their data, found that said client was later breached by Karakurt via a Cobalt Strike backdoor that Conti had left behind.

The research from Arctic Wolf is a collaboration between its computer security service Tetra Defense, cybersecurity company Northwave and blockchain analysis firm Chainalysis and it follows clues from more than a dozen Karakurt incidents and from cryptocurrency transactions involving Conti and Karakurt operators.

Chainalysis' investigation revealed several Karakurt wallets that sent cryptocurrency to wallets controlled by Conti. According to the researchers, payments from victims are between $45,000 and $1 million.

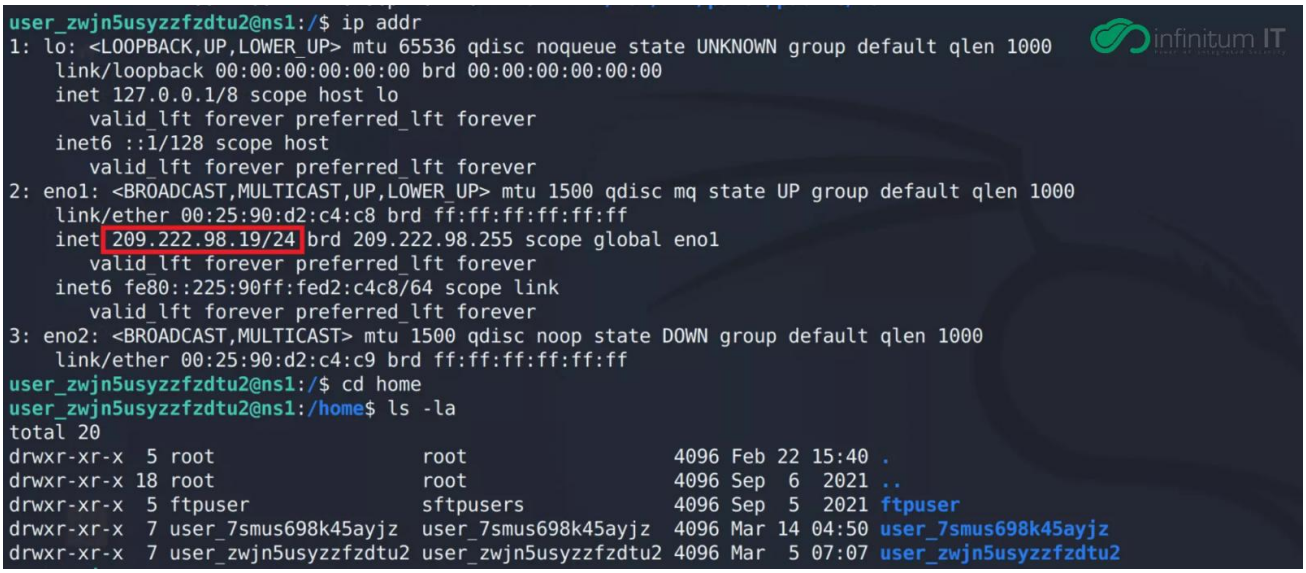
The blockchain analyitics company also found Karakurt victim payment addresses hosted by a Conti wallet, indicating that both gangs are managed by the same party.



Accessing Karakurt servers

While the Conti admin did not save the passwords in the FTP client, Infinitum IT researchers say that they were able to obtain the SSH credentials for the Karakurt command and control (C2) server by exploiting an unpatched vulnerability in FileZilla.

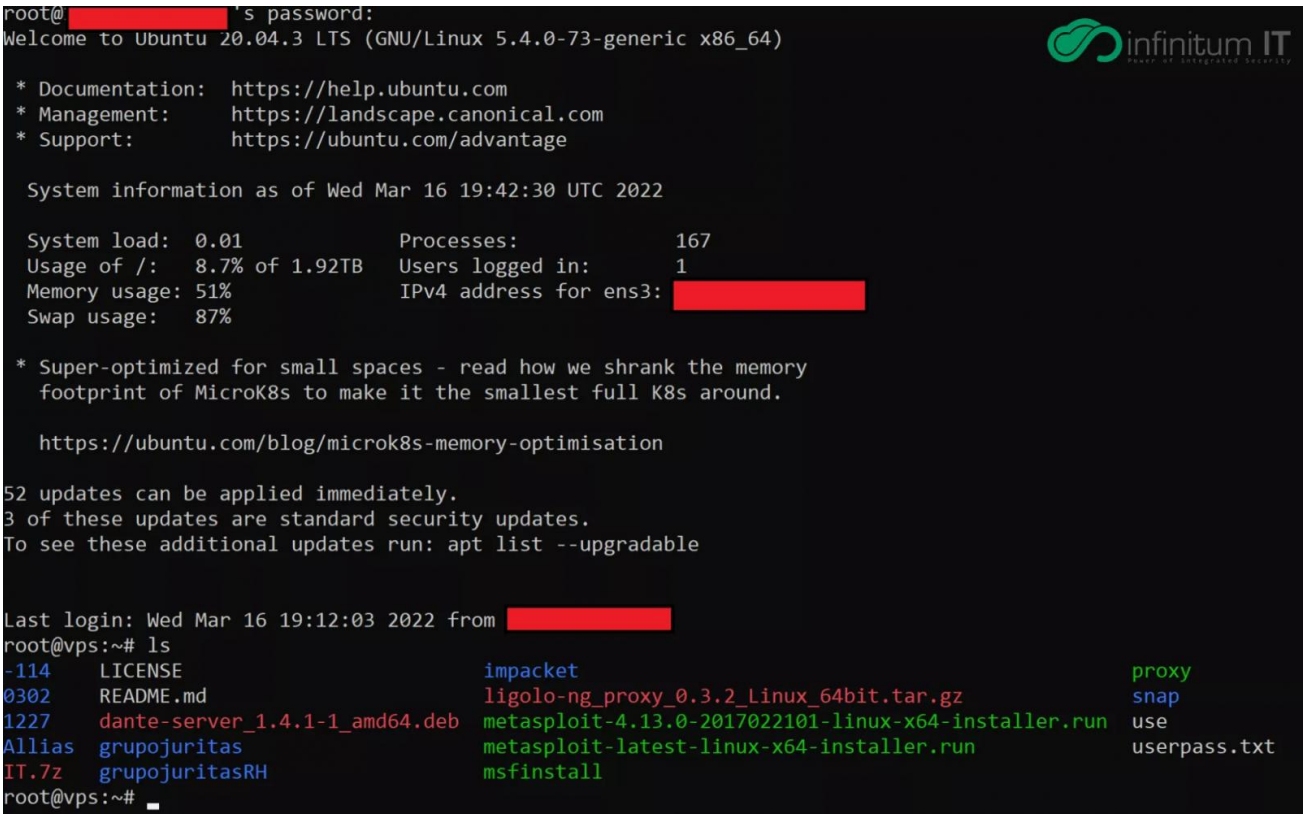
The researchers also obtained this way an SSH private key that allowed connecting to the Karakurt gang’s web server for their leak site, which is also served over the TOR network



source: Infinitum IT

According to Infinitum IT's analysis, members of the Karakurt gang upload stolen data to a "/work" folder and categorize it as public and non-public, their interest being mainly in financial information.

As Infinitum IT completely compromised the Karakurt gang's infrastructure, they were also able to access the C2 server and the tools used in attacks.



source: Infinitum IT

Below is an enumeration of the utilities Karakurt uses in attacks and their description:

- Ligolo-ng: tunneling and pivoting tool

- Metasploit: used as a C2 server in the post-exploitation phase for obtaining reverse shell and for brute-forcing SMB shares and RDP connections
- Impacket: used for NTLM-relay attacks for lateral movement after getting initial access
- Danted: auto-install and management script for Danted–Socks5 Proxy Server, for reverse tunneling

Infinitum IT's report is the first public evidence showing that Conti ransomware and the Karakurt data extortion gang are part of the same financially-motivated group.

After Conti took over the infamous TrickBot botnet and shut it down to focus on the development of BazarBackdoor and Anchor malware, researchers show that the syndicate's expansion is more aggressive.

Conti is now managing side businesses that either sustain its ransomware operations or monetize the initial network access already available.

***Update [March 15, 11:54 EST]**:* Article updated with information from cybersecurity company Arctic Wolf confirming that Karakurt and Conti are part of the same operation.

Related Articles:

The Week in Ransomware - April 15th 2022 - Encrypting Russia

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

- Conti
- Extortion
- Karakurt
- ProtonMail
- Ransomware
- Server

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Comments

- 

  Amigo-A - 1 month ago

  -
  -

  Legal address of Inferno Solutions company: 22 Brondesbury Park, Willesden, London, NW6 7DL

- 

  Amigo-A - 1 month ago

  -
  -

  The address range 209.222.98.19 - 209.222.98.255 belongs to the USA.

  An interesting picture: these studies, unwittingly, prove that
  - the Russian trace is fictitious, the dialogues of the hackers' correspondence are an empty set of phrases and letters;
  - Conti and Karakurt are controlled from the UK, based in the USA, transfer controlled bitcoins to wallets that merge into one, which is also in ...
  Or you need to believe that Russian hackers run the C2 and servers of these countries as if they were their own, which is unlikely.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: