infinitum IT
Power of integrated Security

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team

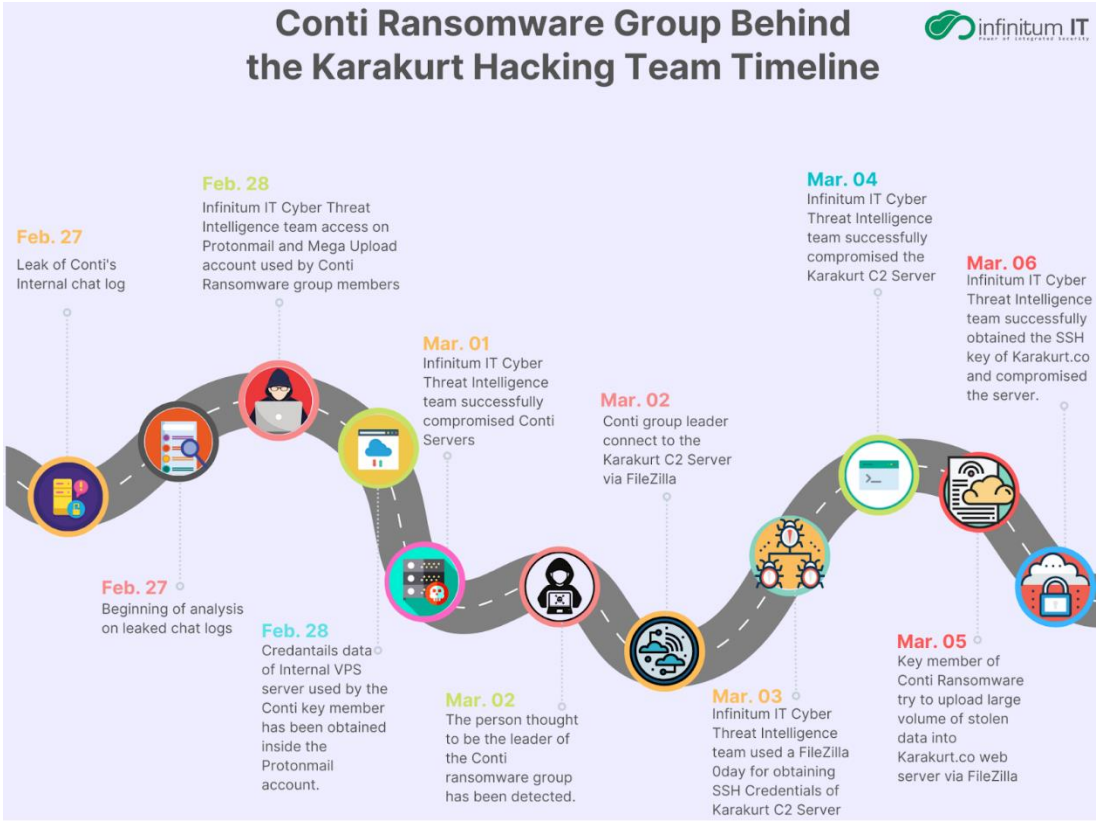
TABLE OF CONTENTS

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team

Report Summary

In this report we would like to share the strong connection between two notorious Cyber Threat Actors called **Conti and Karakurt**. Both of them worked for the same end result and it is the ransom money. The Infinitum IT Cyber Threat Intelligence team successfully monitored one of the key members of Conti Ransomware group, at this stage we don't want to disclose the nickname of the group member but we will share details about how the connection between two cyber threat groups occurred, tactics and techniques used by Karakurt hacking team and details about internal infrastructure of Conti / Karakurt.

Infinitum IT Cyber Threat Intelligence team able to obtain remote access on multiple servers, they are being actively used by members of threat actors as command and control server, storage server that have stolen private data from various victims and web server that is being used by **Karakurt Hacking team** as a blog page. Threat actors like Ransomware group used their web pages to share large numbers of exfiltrate data that are being stolen from victims, they are using data to threaten the victim companies to pay the ransom money.

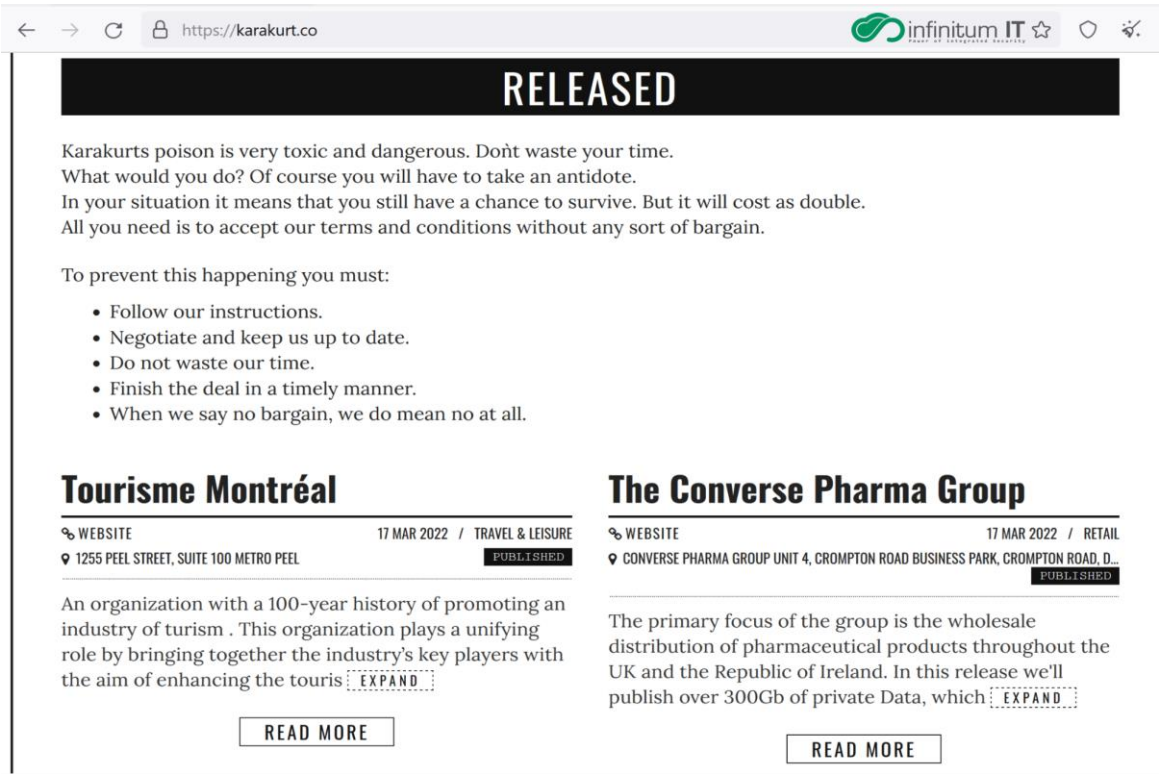


All of the data in this report has been shared with the Government authorized, to help them in further investigation. The data from Command and Control Servers will be used for preventing future cyber attacks and help various organizations across the globe, in this report we shared **TTP and IOC list** that contains analyzed data that is coming from attackers internal servers. Our main goal is to help the victims of these attacks and prevent the feutre cyber attacks against various institutions and organizations.

Information About Karakurt (Russian: Каракурт) Threat Actors

Karakurt is a well known threat actor group that has launched cyberattack against several Canadian and US organizations. On December 29, 2021, the Karakurt group claimed on its website that it had struck 11 organizations as part of its "**Winter Data Leak Digest**." Of the 11, six were based in Canada. The group claimed to have compromised more than 40 victims between September and November 2021, sharing the stolen files on its name and shame blog website.

Karakurt focuses exclusively on the **Data Exfiltration**, they are not using Ransomware to encrypt victims files. The group accomplishes this by first using VPN credentials to access victims' networks, through phishing attacks against victims.



Blog web page used by Karakurt team (karakurt[.]co)

Karakurt had previously employed the **Cobalt Strike** remote access tool, but we also observed that it had since switched to using **AnyDesk**. **Afterwards**, the group steals additional credentials from administrators by using the password-stealing tool **Mimikatz** and Active Directory enumeration tool called **ADfind.** No ransomware is employed at any stage of the attacks, but the group uses the threat of leaking the stolen data for its ransom demands.

We also observed that attackers use **Mega** upload accounts to store large volumes of stolen data.

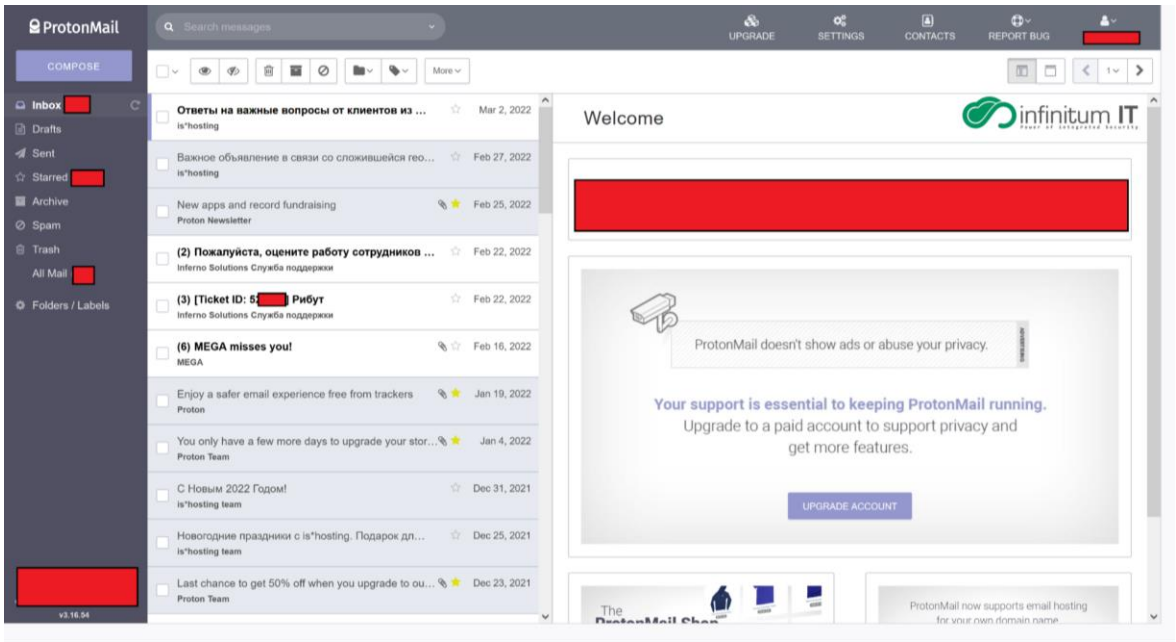
Tactic and Techniques Used by Karakurt Hacking Team

MITRE ATT&CK Table

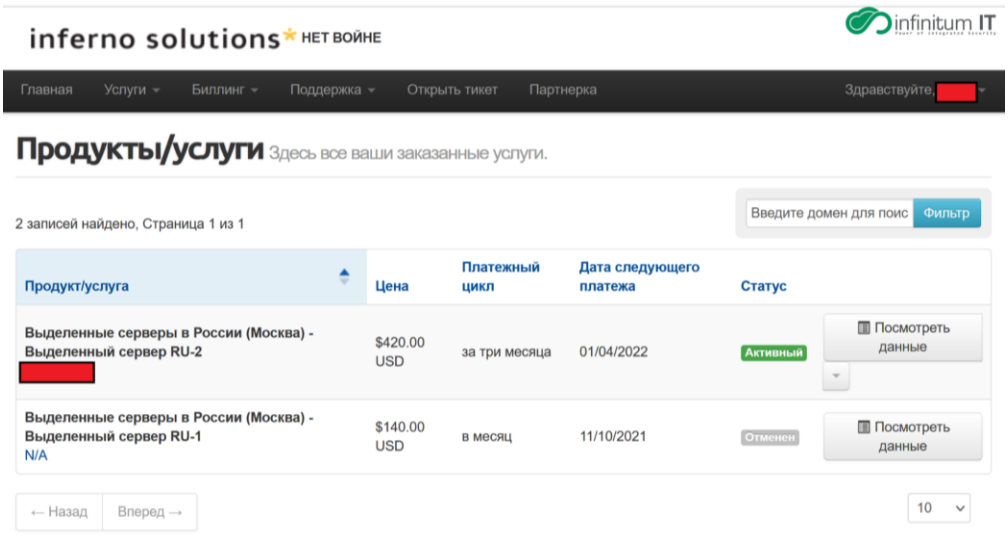
Tactic	Technique
Initial Access	T1133: External Remote Services T1078: Valid Accounts
Execution	T1059: Command and Scripting Interpreter T1086: PowerShell T1035: Service Execution
Persistence	T1050: New Service
Defense Evasion	T1078: Valid Accounts T1036: Masquerading T1027: Obfuscated Files or Information
Credential Access	T1110: Brute Force T1003: Credential Dumping T1557.001: LLMNR/NBT-NS Poisoning and SMB Relay
Discovery	T1083: File and Directory Discovery T1082: System Information Discovery T1087: Account Discovery T1135: Network Share Discovery T1069: Permission Groups Discovery T1018: Remote System Discovery T1016: System Network Configuration Discovery
Lateral Movement	T1021.001: Remote Desktop Protocol T1021.006: Windows Remote Management
Collection	T1005: Data from Local System T1039: Data from Network Shared Drive
Command & Control	T1436: Commonly Used Port T1105: Remote File Copy T1071: Standard Application Layer Protocol T1572: Protocol Tunneling
Exfiltration	T1560: Archive Collected Data T1048: Exfiltration Over Alternative Protocol

Internal Infrastructure Used by Conti and Karakurt Group

At the beginning of Conti leak in 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**, after further investigation we observed threat actors used multiple Protonmail accounts for OPSEC reason,we are able to archived the content of mail traffic and we observed multiple email coming from Russian VPS Service called Inferno solutions, we got remote access on one of the Windows VPS Server that being used data storage system. That has more than 20 TB+ of stolen victim data.



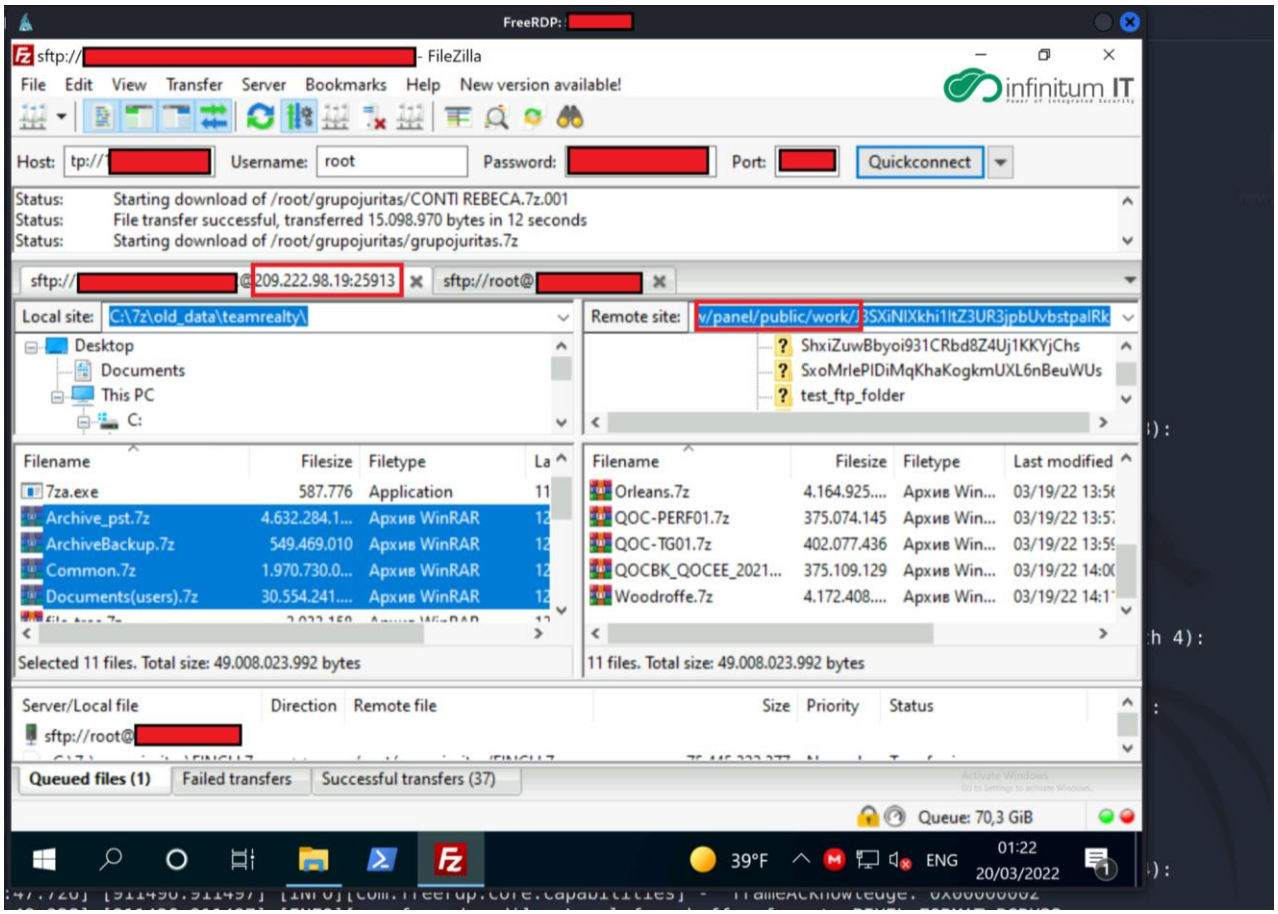
Proton mail account used by key member of Conti Ransomware group



VPS Server Admin Panel

Windows Data Storage Server Used by Conti Ransomware

Our first stage of analysis is this data storage server that is being used for storing large volumes of **stolen data from victims**. We can also observe that some of the data was old but not published publicly. We contact the victims to give their data back, on every Cyber Attacks we saw the usage of Mega Upload accounts to manage this overall **20TB+ data**.

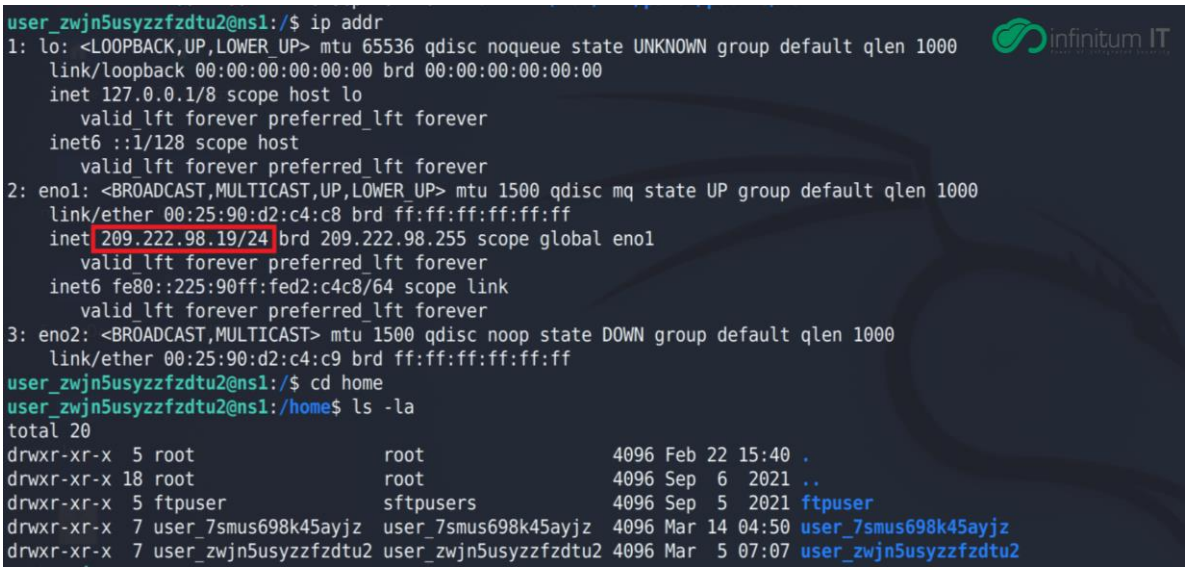


During our investigation we observed that, Conti member used **FileZilla** to connect multiple remote servers, the main purpose is to upload the stolen data to another server for preparing the public release.

When we take a closer look at the IP address **209[.]222[.]98[.]19** the DNS record shows us, it belongs to the **karakurt[.]co** blog page which it is being used for sharing the stolen files.During connection of remote server via FileZilla, Conti member don't save any Password credentials, but Infinitum IT Cyber Threat Intelligence team successfully obtained the SSH Credentials via **a 0day vulnerability affected by FileZilla** and used this credentials to get inside the Command and Control Server.Attacker also used a SSH Private key to connect karakurt[.]co blog page, we also managed to obtained the private key.

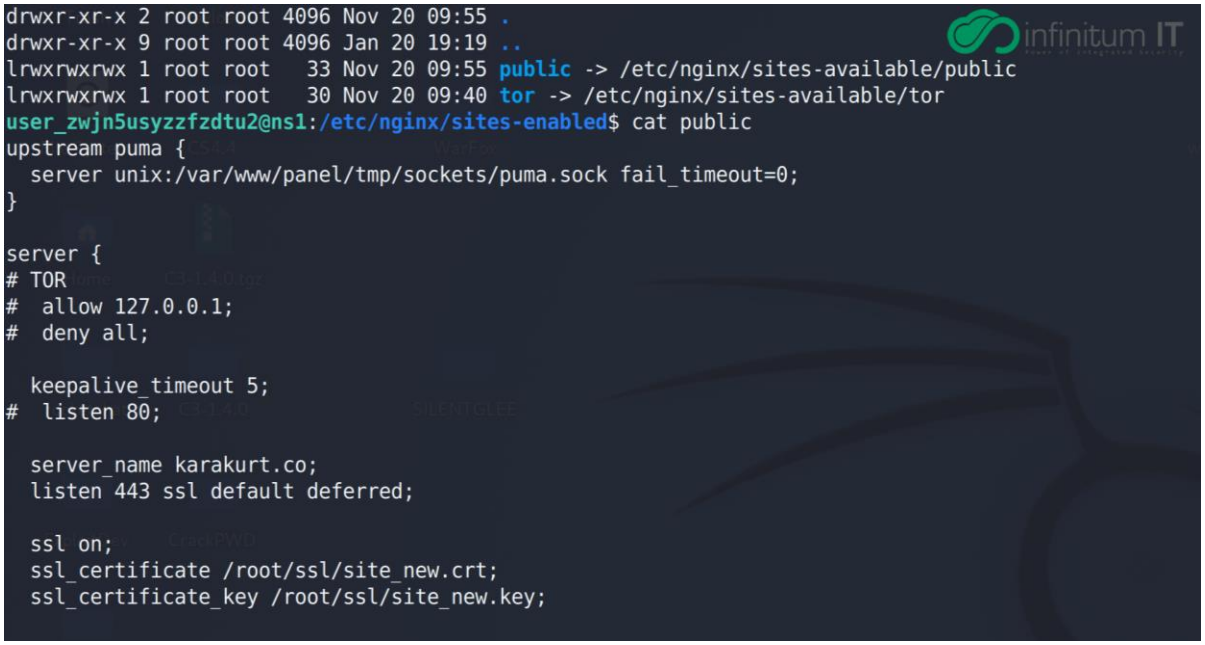
Karakurt Blog Web Server

When we connected to the **Karakurt Blog Web Server**, we saw that all of the stolen data had been categorized by a Software that was being developed by Karakurt members. During our analysis we are able to find an Admin Panel used by Karakurt and Server LOG data. Admin panel is being used for visualizing and filtering all stolen files.



Web Server of karakurt[.]co

The Infinitum IT Cyber Threat Intelligence team found this server also being used by the **TOR network** to serve itself on Darknet.



All of the stolen data has been uploaded by multiple Karakurt members on one file called Work,this data then being categorized as public or not public. We can easily see the Karakurt hacker team being more interested in Financial data from victims' devices.

In this example, it tell us storing critical data in device without Encrypting can cause the mass data exfiltration.

```
user_zwjn5usyzzfzdtu2@ns1:/work/4YACvvWck115yrVX55PKq9jymQNI4hA7$ cd published
user_zwjn5usyzzfzdtu2@ns1:/work/4YACvvWck115yrVX55PKq9jymQNI4hA7/published$ ls -la
total 88
drwxr-xr-x  19 root                  root        4096 Mar 17 17:48 .
drwxr-xr-x   4 user_zwjn5usyzzfzdtu2 workfolder  4096 Mar 15 18:48 ..
drwxr-xr-x 106 root                  root        4096 Mar 17 17:48 123Corp
drwxr-xr-x   3 root                  root        4096 Mar 16 09:10 2021kj
drwxr-xr-x   3 root                  root        4096 Mar 15 16:02 88
drwxr-xr-x   3 root                  root        4096 Mar 15 17:44 Administration
drwxr-xr-x  12 root                  root        4096 Mar 17 17:48 Assn987
drwxr-xr-x  40 root                  root        4096 Mar 15 18:49 Assnlku
drwxr-xr-x   3 root                  root        4096 Mar 15 17:27 Comptabilite1
drwxr-xr-x  67 root                  root        4096 Mar 17 17:48 Corfnp
drwxr-xr-x  85 root                  root        4096 Mar 16 10:49 Corpsfgb
drwxr-xr-x   6 root                  root        4096 Mar 17 17:48 Evenq5wts
drwxr-xr-x   3 root                  root        4096 Mar 15 17:42 Finances12309
drwxr-xr-x   5 root                  root        4096 Mar 15 17:46 iis_full_p2erms
drwxr-xr-x   4 root                  root        4096 Mar 15 16:00 Partne34rs
drwxr-xr-x  13 root                  root        4096 Mar 17 17:48 Partners76
drwxr-xr-x   3 root                  root        4096 Mar 17 17:48 Salles_de_conf
drwxr-xr-x   3 root                  root        4096 Mar 15 17:40 SecrétariatCorporatif1
drwxr-xr-x 177 root                  root       16384 Mar 17 17:48 ventes1
user_zwjn5usyzzfzdtu2@ns1:/work/4YACvvWck115yrVX55PKq9jymQNI4hA7/published$
```

Inside the server directory we can observed source code of the **Admin Panel**.

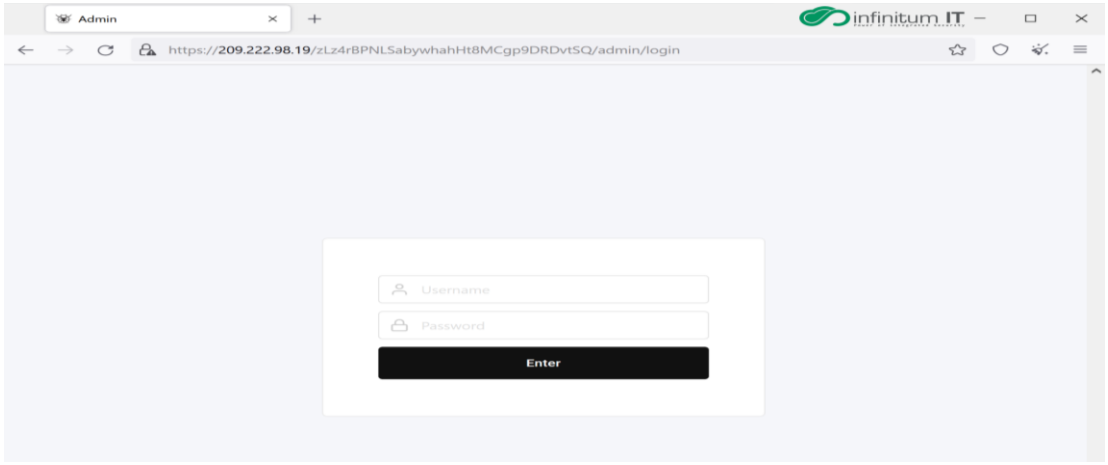
```
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp/cache$ cd ..
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp$ ls
cache  pids  restart.txt  sockets  storage
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp$ cd storage
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp/storage$ ls -la
total 8
drwxrwxr-x 2 root root 4096 Sep  2  2021 .
drwxrwxr-x 6 root root 4096 Sep  1  2021 ..
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp/storage$ cd ..
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp$ cd ..
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel$ ls
app  bin  config  config.ru  db  Gemfile  Gemfile.lock  gems  log  magazine.zip  public  Rakefile  tmp
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel$ ls -la
total 72
drwxr-xr-x 11 root                  root                  4096 Mar 14 04:56 .
drwxr-xr-x  4 root                  root                  4096 Sep  1  2021 ..
drwxrwxr-x  9 root                  root                  4096 Sep  2  2021 app
drwxrwxr-x  2 root                  root                  4096 Sep  2  2021 bin
drwxr-xr-x  2 root                  root                  4096 Sep  1  2021 .bundle
drwxrwxr-x  6 root                  root                  4096 Mar 10 18:39 config
-rw-rw-r--  1 root                  root                   160 Sep  2  2021 config.ru
drwxrwxr-x  3 root                  root                  4096 Sep  1  2021 db
-rw-rw-r--  1 root                  root                   880 Feb 27 19:30 Gemfile
-rw-r--r--  1 root                  root                  5825 Feb 27 19:31 Gemfile.lock
drwxrwxr-x  3 root                  root                  4096 Feb 26 10:05 gems
drwxrwxr-x  2 root                  root                  4096 Mar 10 18:43 log
-rwxr-x---  1 user_7smus698k45ayjz user_7smus698k45ayjz 5067 Mar 14 04:46 magazine.zip
drwxr-xr-x  4 root                  root                  4096 Nov 18 10:06 public
-rw-rw-r--  1 root                  root                   227 Sep  2  2021 Rakefile
drwxrwxr-x  6 root                  root                  4096 Sep  1  2021 tmp
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel$
```

If we see the routing code developed in **Ruby on Rails**, we can identify the Admin panel file path on live Web Server.

routes.rb

```
Rails.application.routes.draw do
  root to: 'public#index'

  match "/403", to: "errors#forbidden", via: :all
  match "/404", to: "errors#not_found", via: :all
  match "/500", to: "errors#internal_server_error", via: :all

  get '/about',       to: 'public#about'
  get '/auction',     to: 'public#auction'
  get '/contact_us',  to: 'public#contact_us'
  post '/contact_us', to: 'public#message_create'

  resources :press_releases, param: :uuid
  resources :companies, param: :uuid do
    get 'files', to: 'companies#download_list_files'
    get 'download/:uuid', to: 'companies#download', as: :download_file
  end

  scope 'zLz4rBPNLSabywhahHt8MCgp9DRDvtSQ' do
    namespace :admin do
      get '/',              to: 'public#index'
      get 'system',         to: 'system#index'
      get 'system/visits',  to: 'system#visits'
      post '/save_app_config', to: 'system#save_app_config'

      resources :press_releases
      resources :companies, param: :uuid do
        get 'download/:uuid',  to: 'companies#download', as: :download_file
      end
      get 'companies/id/:id',  to: 'companies#show_by_id', as: :company_by_id
```

Ruby on Rails URL Routing



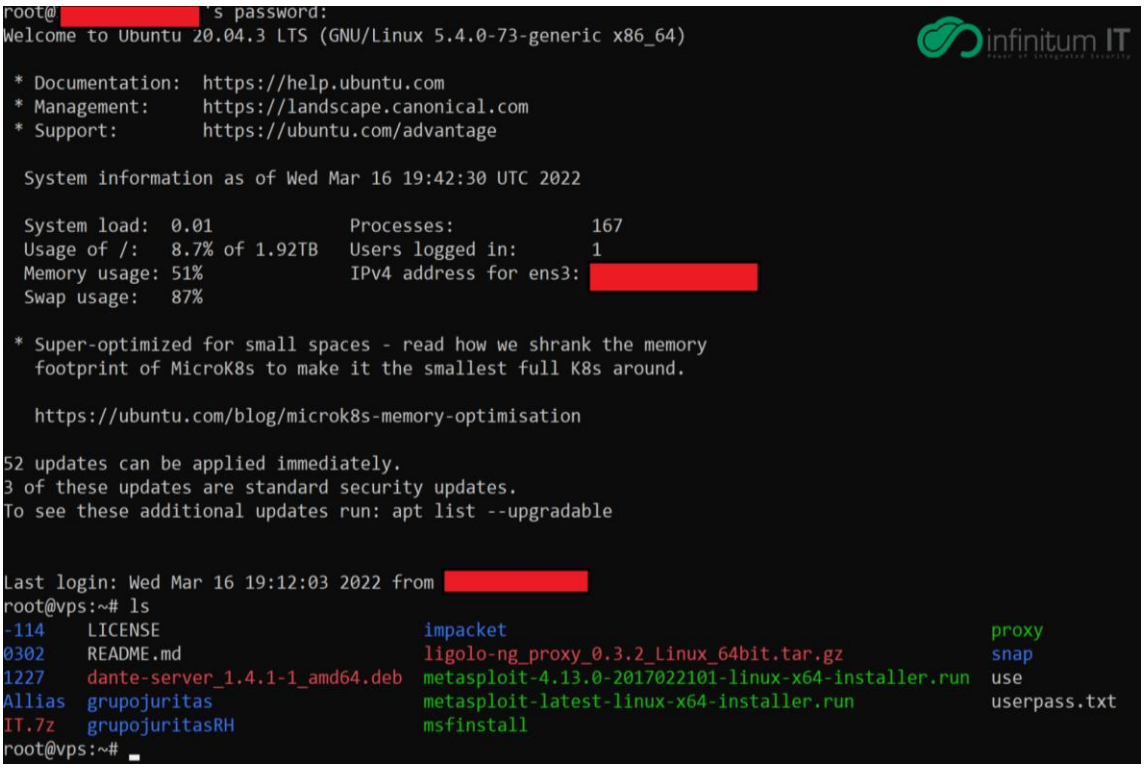
Admin Panel used by Karakurt Hacking Team

Overall storage capacity of **karakurt[.]co**

```
user_zwjn5usyzzfzdtu2@ns1:/home/ftpuser/work$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            7.8G     0  7.8G   0% /dev
tmpfs           1.6G  145M  1.5G  10% /run
/dev/sda4        15T  4.1T  9.7T  30% /
tmpfs           7.9G   16K  7.9G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/sda2       454M   80M  347M  19% /boot
tmpfs           1.6G     0  1.6G   0% /run/user/1003
```

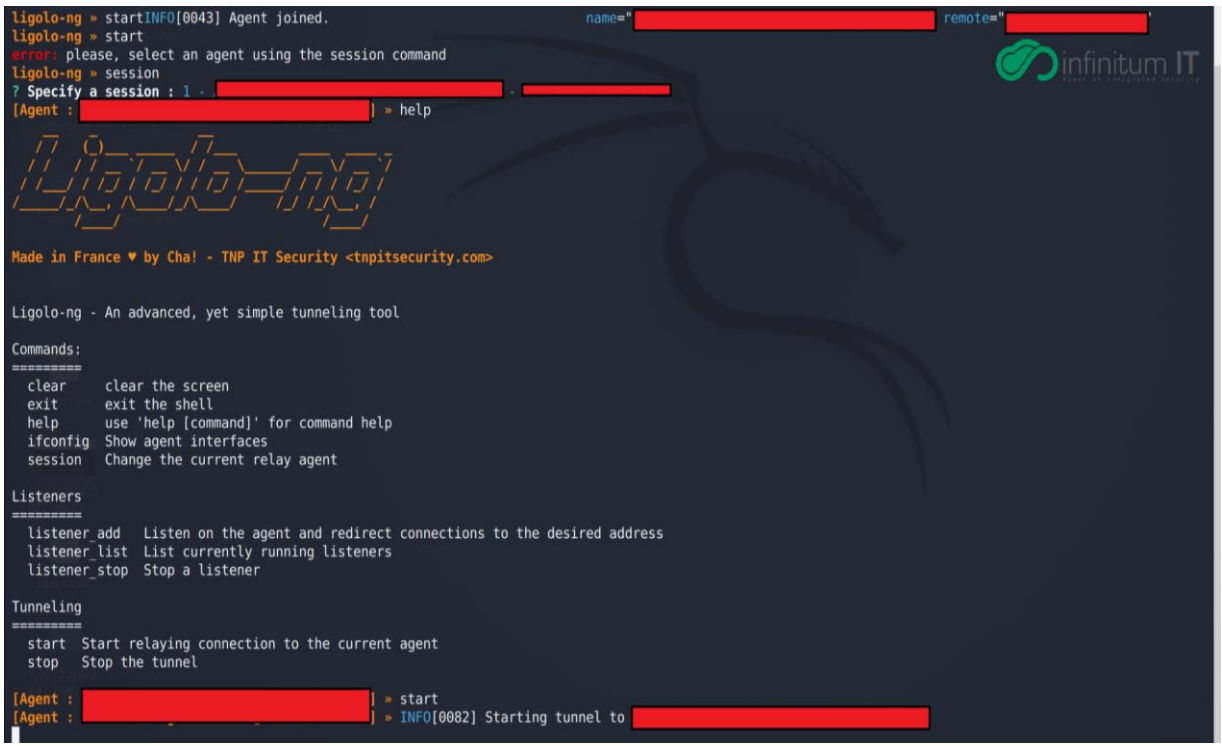
Command and Control Server

The Infinitum IT Cyber Threat Intelligence team is able to access the Command and Control Server that is being actively used by the Karakurt Hacking team on cyber attack operations. As a summary of the attack chain, we observed the use of open source tools like



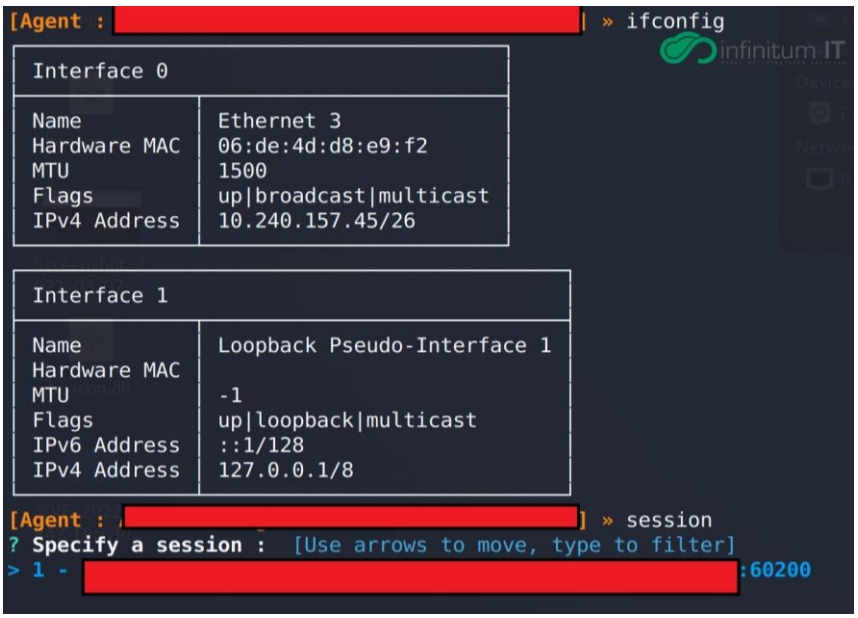
- Ligolo-ng : Getting Initial Access on companies network via Reverse Tunneling, this technique being used for bypassing miss configured Firewall systems.
- Metasploit : Karakurt used Metasploit as C2 server and in post exploitation phase details can be seen on Metasploit log file that was obtained and shared by the Infinitum IT Cyber Threat Intelligence team on IOC part.
- Impacket: After getting Initial Access on the victim company network, Karakurt hacking team use Impacket to perform NTLM relay attacks. This tool mainly used for Lateral Movement
- Danted: Fast script for installing & configuring Danted--Socks5 Proxy Server. That being used for Reverse Tunneling.

On a misconfigured Firewall, Threat actors can abuse this issue and they are able to get Initial Access on remote networks by **Reverse Proxy Tunneling** technique.In this report we don't disclose the victim but we want to raise an evarinse on usage of such technique is not a sophisticated attack, there are plenty of Open Source tools used by cyber attackers and if your network doesn't prepared against such an attack you may became the target.

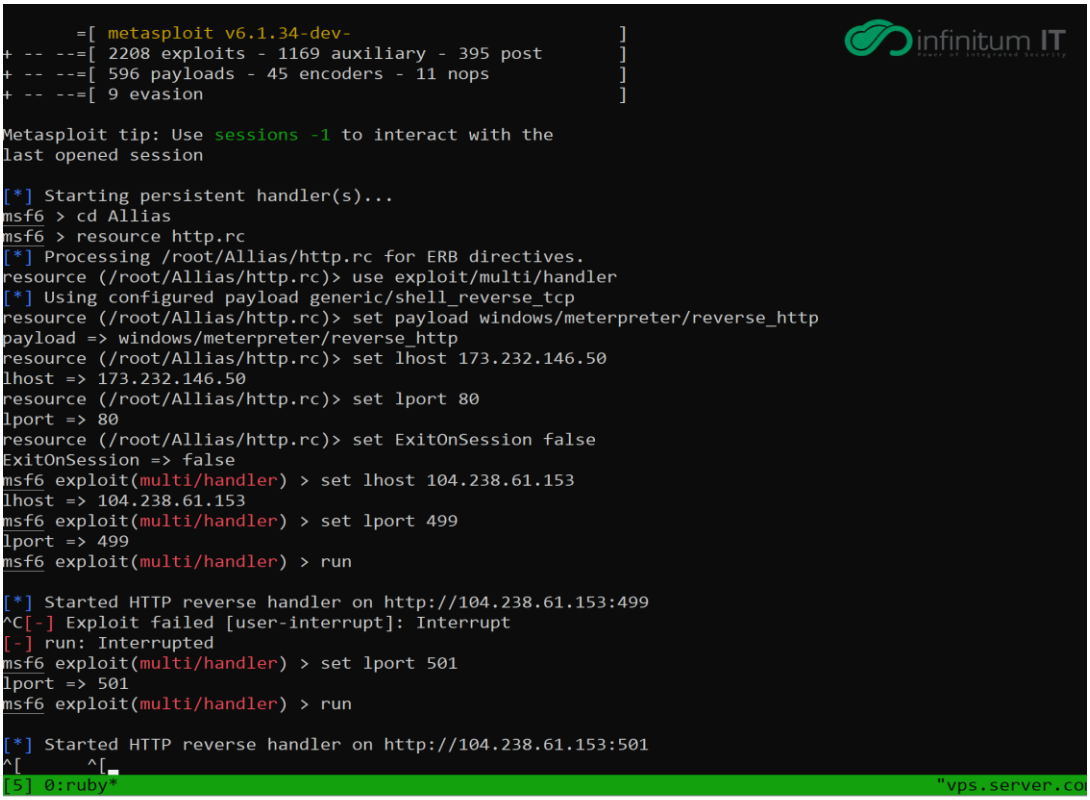


Ligolo Proxy Panel

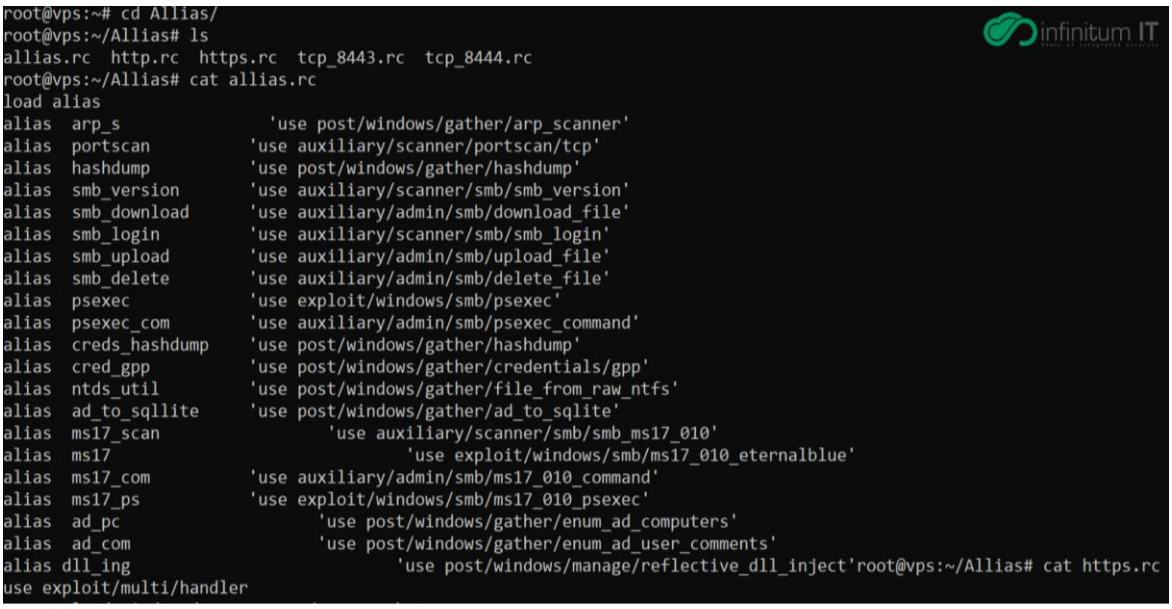
On below image can showed us, after getting Initial Access on the victim network with reverse tunneling, attacker able to obtained Internet interface data to perform the attack, just like they physically inside the network.



The Infinitum IT Cyber Threat Intelligence team, observed the usage of **Metasploit Framework** against multiple targets.Karakurt hacking team used Metasploit for getting **Reverse Shell** on victim devices, **brute forcing SMB shares** and **RDP sessions**.



Post exploitation techniques used by Karakurt group can be observed on Metasploit logs



Mitigation Against Conti / Karakurt Hacking Team

- Employ robust and routine user-awareness and training regimens for users of all systems.
- Ensure that a robust crisis management and incident response plan are in place in the event of a high impact intrusion.
- Maintain best practices against malware, such as patching, updating anti-virus software, implementing strict network egress policies, and using application whitelisting where feasible.
- Patch infrastructure to the highest available level, as threat actors are often better able to exploit older systems with existing vulnerabilities.
- Ensure all internet-facing security and remote access appliances are patched to the latest versions.
- Disable RDP on external-facing devices and restrict workstation-to-workstation RDP connections.
- Employ a strong corporate password policy that includes industry standards for password length, complexity, and expiration dates for both human and non-human accounts.
- Use MFA where possible for authenticating corporate accounts to include remote access mechanisms and security tools. Admin accounts should be cross-platform MFA enforced.
- Use admin accounts only for administrative purposes and never to connect to the network or browse the internet.
- Do not store unprotected credentials in files and scripts on shared locations.
- Deploy EDR across the environment, targeting at least 90% coverage of endpoint and workload visibility.
- Encrypt data at rest where possible and protect related keys and technology.
- Hunt for attacker TTPs, including common “living off the land” techniques, to proactively detect and respond to a cyber-attack and mitigate its impact.

IOC Data

https://github.com/infinitumitlabs/Karakurt-Hacking-Team-CTI

Acknowledgement

We would like to thank ”Federal Office for Information Security (BSI) / Germany” for their valuable guidance and support throughout this research.

During our research we also contacted companies who got affected by Conti / Karakurt Threat Actors to prevent the ongoing Cyber Attacks or notify them about the incident.

The public version of the report will be shared from our github page

https://github.com/infinitumitlabs

Readers can find the new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

References

Lozy. *danted.* 1 04 2022. https://github.com/Lozy/danted.

Nicocha30. *ligolo-ng.* 3 4 2022. https://github.com/Nicocha30/ligolo-ng.

rapid7. *metasploit-framework.* 5 4 2022. https://github.com/rapid7/metasploit-framework.

SecureAuthCorp. *impacket.* 01 04 2022. https://github.com/SecureAuthCorp/impacket.

infinitum IT
Power of integrated Security

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team