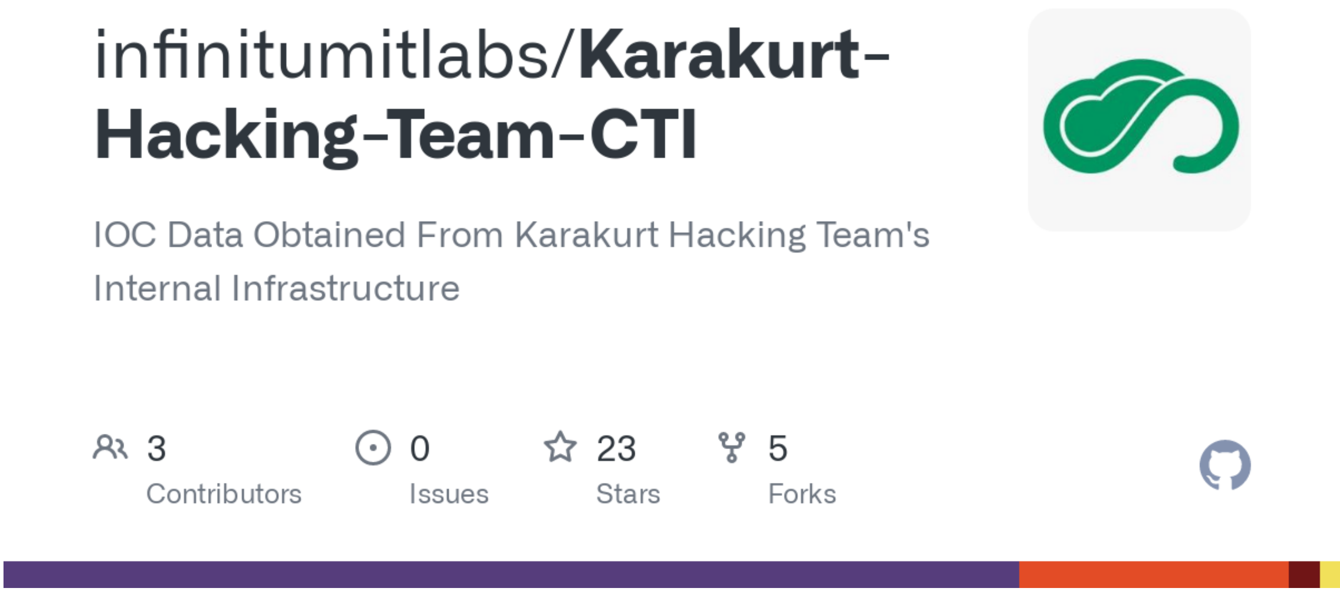
Karakurt Hacking Team Indicators of Compromise (IOC)

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

infinitumitlabs



infinitumitlabs/**Karakurt-Hacking-Team-CTI**

IOC Data Obtained From Karakurt Hacking Team's Internal Infrastructure

3 Contributors

0 Issues

23 Stars

5 Forks

These IOCs were released as part of CTI team research by Infinitum IT. The full report is available here

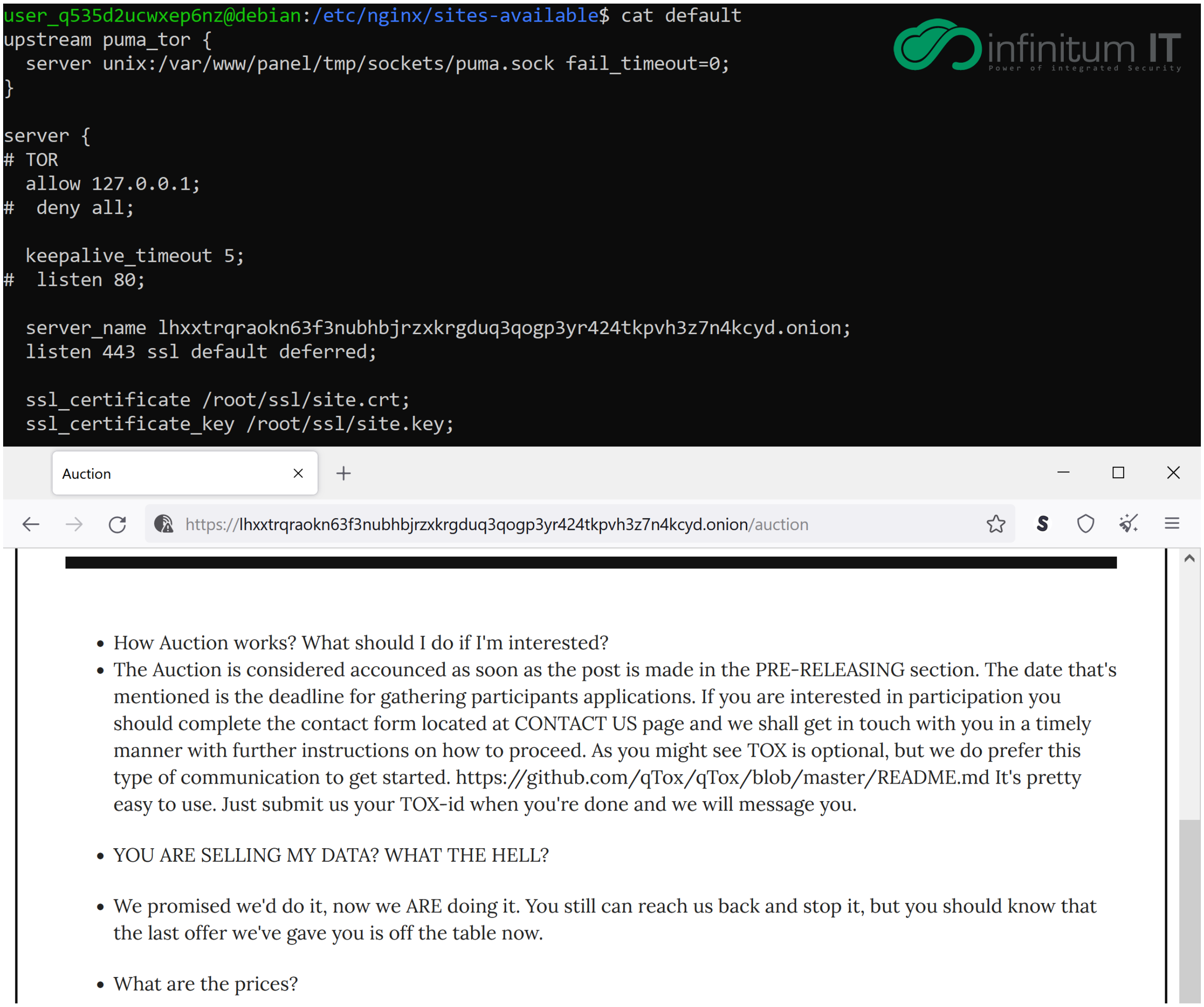
One of the most valuable pieces of threat intelligence we discovered during this CTI investigation was the the IP address of the data storage and Command and Control Servers used by Karakurt / Conti.

Domain	IP
karakurt.co	209.222.98.19
stok-061153.stokermate.com	104.238.61.153

Real IP Address of Onion site used by Karakurt Hacking Team as a public leak page

Onion site	IP
lhxxtrqraokn63f3nubhbjrzxkrgduq3qogp3yr424tkpvh3z7n4kcyd.onion	104.243.34.214

Karakurt Leak Site


infinitum IT
Power of integrated Security
Auction
https://lhxxtrqraokn63f3nubhbjrzxkrgduq3qogp3yr424tkpvh3z7n4kcyd.onion/auction

```
user_q535d2ucwxep6nz@debian:/etc/nginx/sites-available$ cat default
upstream puma_tor {
  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 lhxxtrqraokn63f3nubhbjrzxkrgduq3qogp3yr424tkpvh3z7n4kcyd.onion;
  listen 443 ssl default deferred;

  ssl_certificate /root/ssl/site.crt;
  ssl_certificate_key /root/ssl/site.key;
```

- How Auction works? What should I do if I'm interested?
- The Auction is considered accounced as soon as the post is made in the PRE-RELEASING section. The date that's mentioned is the deadline for gathering participants applications. If you are interested in participation you should complete the contact form located at CONTACT US page and we shall get in touch with you in a timely manner with further instructions on how to proceed. As you might see TOX is optional, but we do prefer this type of communication to get started. https://github.com/qTox/qTox/blob/master/README.md It's pretty easy to use. Just submit us your TOX-id when you're done and we will message you.
- YOU ARE SELLING MY DATA? WHAT THE HELL?
- We promised we'd do it, now we ARE doing it. You still can reach us back and stop it, but you should know that the last offer we've gave you is off the table now.
- What are the prices?

Following table contains the authentication logs of the subject Karakurt servers with IP **209.222.98.19** and **104.238.61.153**

Detected TCP Connections on Karakurt Servers
45.8.119.60
212.220.115.145
5.45.83.32
31.14.40.64
95.170.133.54
1.116.139.11
45.141.84.126
185.5.251.35
49.232.93.149
61.177.173.17

Detected TCP Connections on Karakurt Servers
80.93.19.227
139.219.4.103
61.19.125.2
159.65.140.76
23.99.177.202
109.169.14.109
104.243.34.214
37.252.0.143
46.166.143.114

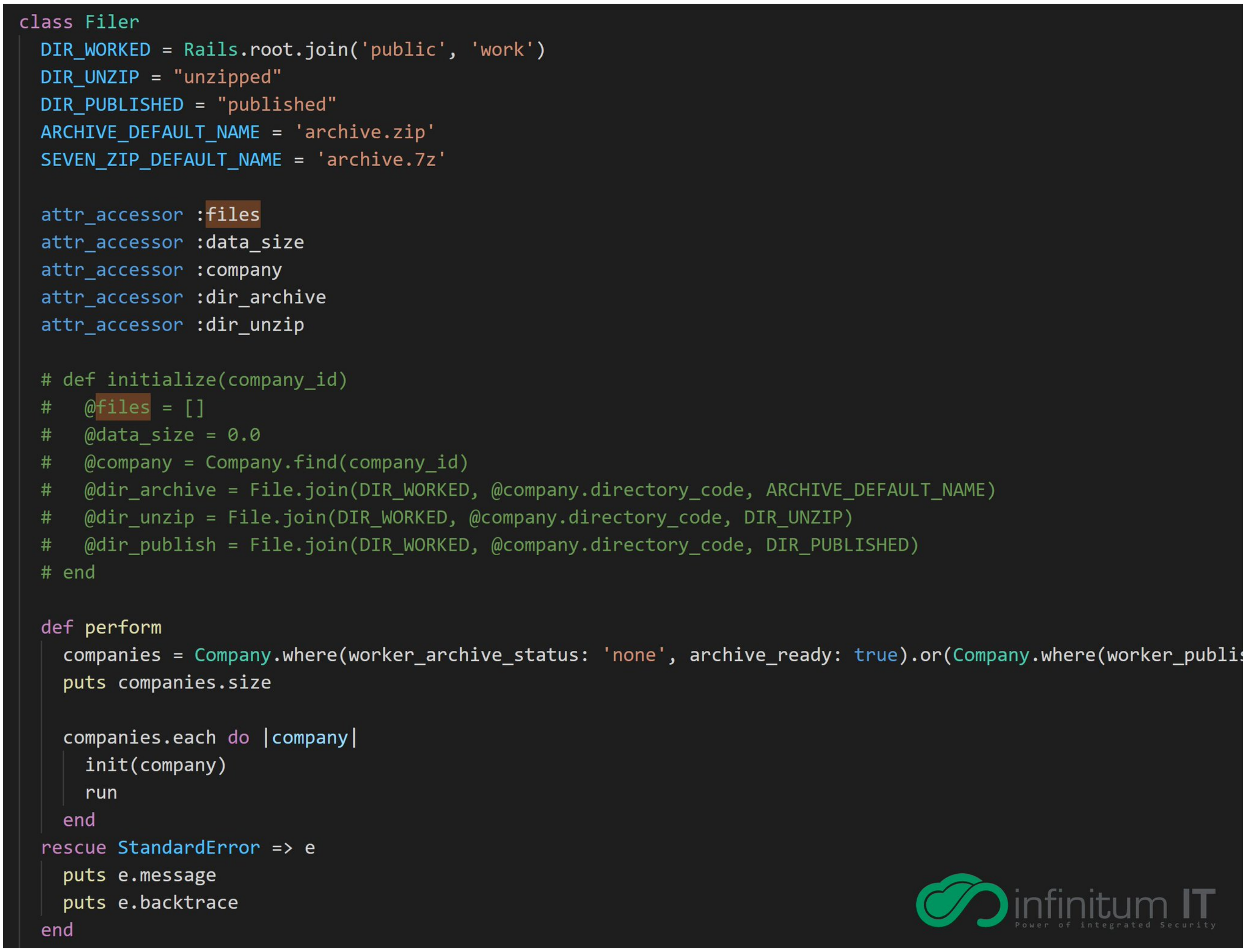
Durring our CTI research on Karakurt / Conti Servers we are able to identify the use of SOCKS proxy pivoting technique with a open source tool called Ligolo-ng against multiple victims.

Following table contains the Ligolo-ng Agent and Command and Control Server used by Karakurt Hacking Team Members

Ligolo-ng Agent and Command and Control Servers
104.194.9.238/download/lig.ext
104.194.9.238:455/download/lig2.ext
104.238.61.153

Source Code of Data Leak Page Used by Karakurt Threat Group [Update - Published]

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.



```
class Filer
  DIR_WORKED = Rails.root.join('public', 'work')
  DIR_UNZIP = "unzipped"
  DIR_PUBLISHED = "published"
  ARCHIVE_DEFAULT_NAME = 'archive.zip'
  SEVEN_ZIP_DEFAULT_NAME = 'archive.7z'

  attr_accessor :files
  attr_accessor :data_size
  attr_accessor :company
  attr_accessor :dir_archive
  attr_accessor :dir_unzip

  # def initialize(company_id)
  #   @files = []
  #   @data_size = 0.0
  #   @company = Company.find(company_id)
  #   @dir_archive = File.join(DIR_WORKED, @company.directory_code, ARCHIVE_DEFAULT_NAME)
  #   @dir_unzip = File.join(DIR_WORKED, @company.directory_code, DIR_UNZIP)
  #   @dir_publish = File.join(DIR_WORKED, @company.directory_code, DIR_PUBLISHED)
  # end

  def perform
    companies = Company.where(worker_archive_status: 'none', archive_ready: true).or(Company.where(worker_publi
    puts companies.size

    companies.each do |company|
      init(company)
      run
    end
  rescue StandardError => e
    puts e.message
    puts e.backtrace
  end
```

Cobalt Strike Server and Malware Samples [Update - Published]

This data has been obtanied from an Encrypted ZIP folder inside Karakurt C2 Server

IP	Domian Name
108.177.235.127	kisizo[.]com

VT Link
https://www.virustotal.com/gui/file/b7ae3b6f2c04a8d05478509b5047bf50bd880d32125923f093b2ea65fe48fac1/relations
https://www.virustotal.com/gui/file/8cfdb99185fba9abd91d915425826ca9c6ce360fe68f4c8430c358ceab0acf24/relations