Network Forensic Analysis Report

## Time Thieves

1. What is the domain name of the users' custom site?

frank-n-ted.com

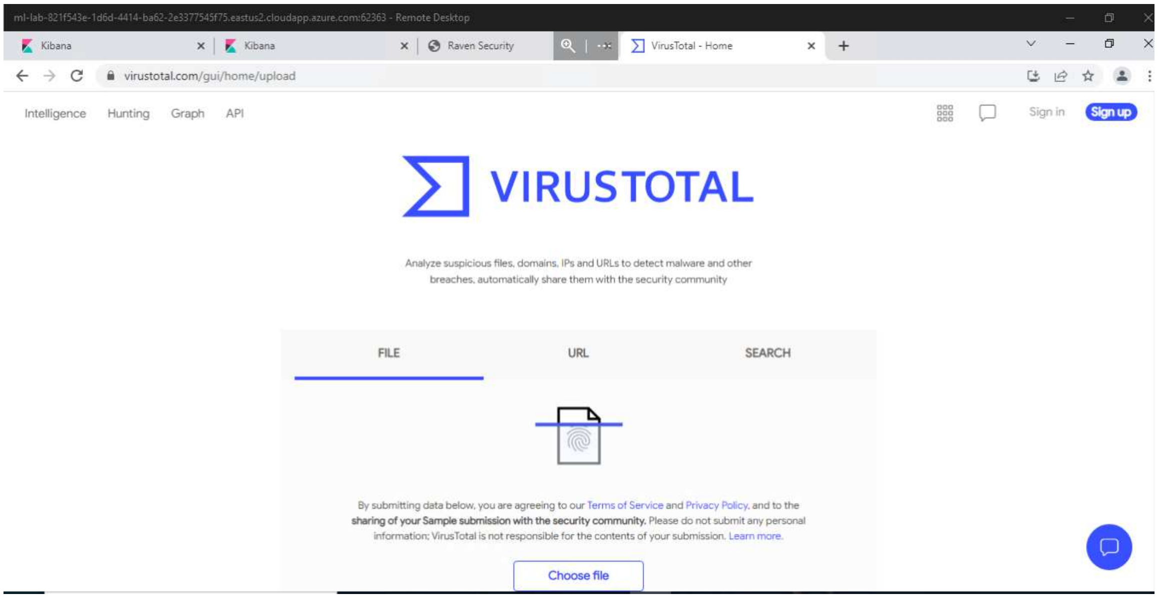
2. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

June11.dll

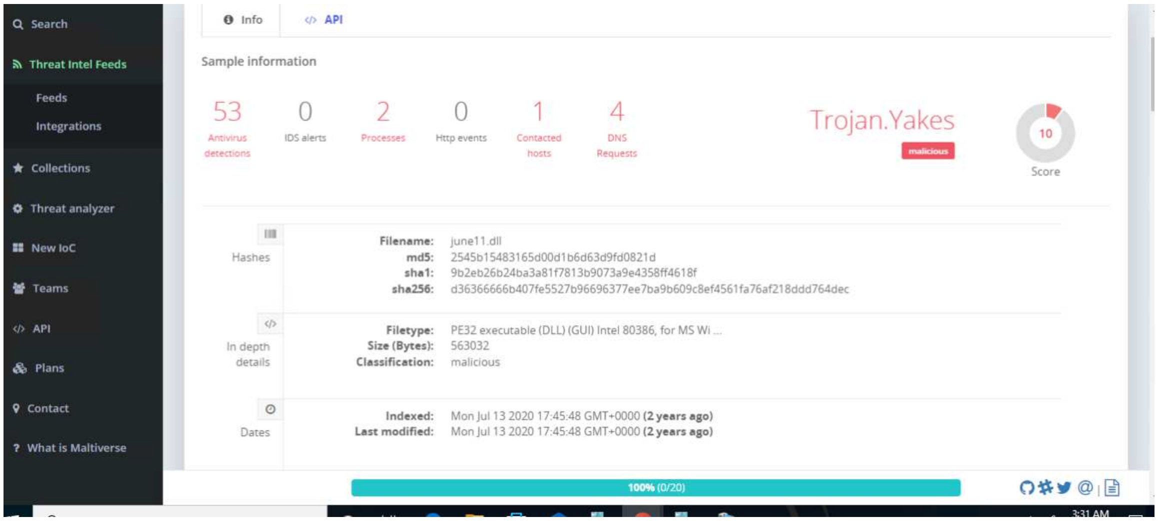
4. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/).


ml-lab-821f543e-1d6d-4414-ba62-2e3377545f75.eastus2.cloudapp.azure.com:62363 - Remote Desktop
Kibana
Kibana
Raven Security
VirusTotal - Home
virustotal.com/gui/home/upload
Intelligence
Hunting
Graph
API
Sign in
Sign up
VIRUSTOTAL
FILE
URL
SEARCH
Choose file

Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

5. What kind of malware is this classified as?



Sample information

53 Antivirus detections

0 IDS alerts

2 Processes

0 Http events

1 Contacted hosts

4 DNS Requests

Trojan.Yakes

malicious

10 Score

Hashes

Filename: june11.dll
md5: 2545b15483165d00d1b6d63d9fd0821d
sha1: 9b2eb26b24ba3a81f7813b9073a9e4358ff4618f
sha256: d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

In depth details

Filetype: PE32 executable (DLL) (GUI) Intel 80386, for MS Wi ...
Size (Bytes): 563032
Classification: malicious

Dates

Indexed: Mon Jul 13 2020 17:45:48 GMT+0000 **(2 years ago)**
Last modified: Mon Jul 13 2020 17:45:48 GMT+0000 **(2 years ago)**

100% (0/20)

3:31 AM