CS-Joy

Cyber Security

Cisco balexey@cisco.com
UNIT Team born2code@unit.ua

Summary: This project aims to give the opportunity to create a software product with real hardware. This subject was made in collaboration with Cisco.

Chapter I

Forewords

Natus Vincere (Na'Vi)

Electronic video gaming has extended from being a hobby into a serious sports and business. Over 2.3 billion people play games every day on different platforms and devices.

Natus Vincere (Na'Vi) is an eSports organisation based in Ukraine with teams and players competing in Counter Strike: Global Offensive, Dota 2, FIFA, World of Tanks, Paladins and League of Legends.

Dota 2 is an astoundingly complex game in which two teams of 5 players compete to siege and destroy the opposing team's base. The game features 113 playable heroes who each possess unique abilities, as well as dozens of items that can enhance and extend each hero's capabilities — meaning the full extent of the game's possibilities are virtually incomprehensible, at least to a player with human limitations.

In August 10 2017 the bot from OpenAI, the $1 billion artificial-intelligence research nonprofit cochaired by Tesla Motors CEO Musk and Y Combinator President Sam Altman, beat Danylo "Dendi" Ishutin (the world's best Dota 2 players) from Na'Vi.

Chapter II

Introduction

What if defenders could see the future? If they knew an attack was coming, they could stop it, or at least mitigate its impact and help ensure what they need to protect most is safe. The fact is, defenders can see what's on the horizon. Many clues are out there—and obvious.

Some cybersecurity trends:

Encrypted malicious web traffic
The expanding volume of encrypted web traffic—both legitimate and malicious—creates even more challenges and confusion for defenders trying to identify and monitor potential threats. Encryption is meant to enhance security, but it also provides malicious actors with a powerful tool to conceal command-and-control (C2) activity, affording them more time to operate and inflict damage. Cisco threat researchers observe an annual increase in encrypted traffic. Gartner predicts that by 2019, 80 percent of web traffic will be encrypted. One factor driving that increase is the availability of low-cost or free SSL certificates. Another is Google Chrome's stepped- up practice of flagging unencrypted websites that handle sensitive information, like customers' credit card information, as "non-secure." Businesses are motivated to comply with Google's HTTPS encryption requirement unless they want to risk a potentially significant drop in their Google search page rankings.

Abuse of cloud and other legitimate resources
As applications, data, and identities move to the cloud, security teams must manage the risk involved with losing control of the traditional network perimeter. Attackers are taking advantage of the fact that security teams are having difficulty defending evolving and expanding cloud and IoT environments. One reason is the lack of clarity around who exactly is responsible for protecting those environments. To meet this challenge, enterprises may need to apply a combination of best practices, advanced security technologies like machine learning, and even some experimental methodologies, depending on the services they use for their business and how threats in this space evolve.

Email threats
No matter how much the threat landscape changes, malicious email and spam remain vital tools for adversaries to distribute malware because they take threats straight to the endpoint. By applying the right mix of social engineering techniques, such as phishing and

malicious links and attachments, adversaries need only to sit back and wait for unsuspecting users to activate their exploits.

Chapter III

Goals

This project aims to make you familiar with:

- Enhanced Telemetry Data Types
- Process PCAP files
- Using Sleuth for Crypto Audit
- Malware analysis (bonus part)

Chapter IV

General instructions

- This project will be evaluated only by humans
- This project must use Cisco open source project Joy
- You must use PCAP file(s) from resources

You can also register on Cisco DevNet site developer.cisco.com and try to find some useful information

Chapter V

The project

V.1 Mandatory part

The rapid rise in encrypted traffic is changing the threat landscape. As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. More specifically, encrypted traffic has increased by more than 90 percent year over year, with more than 40 percent of websites encrypting traffic in 2016 versus 21 percent in 2015. Gartner predicts that by 2019, 80 percent of web traffic will (if this year has already come, you can check this forecast) be encrypted.

What data is available for analysis in encrypted traffic?

	Client	Session	Server
TCP/IP	Source Address Source Port	# Bytes # Packets	Destination Address Destination Port
Intraflow		Packet Lengths Packet Arrival Times	
TLS	Ciphersuite Offer Vector Extensions Offer Supported Elliptic Curves SNI	Record Length Record Times Record Types	Certificate Chain Selected Ciphersuite
DNS	Name		Response Code TTL
HTTP	Headers	Headers File Magic	Headers

Contextual Flows

As you could read in the introduction

Here's what you must do:

- Write script or program that show flows with probability of malware greater than 91% (you need parameters like: source address, destination address, destination port) (file `133d773a8ca64c24bd81b594cf5240dd.pcap`)
- Using data from the previous task and find all destination address with malicious traffic and write it to file for future adding to firewall blacklist
- Using Joy, Sleuth and your own code find TLS server certificate chains where one or more of the keys is less than 2048 bits (file `capture.pcap`)
- You should be able to write down and work with the following options : source address, destination address, protocol (UDP), source port, destination port (DNS), number outbound bytes, number outbound packets, number inbound bytes, number inbound packets.
- Find all TLS Fingerprinting (file `capture.pcap`)
- Analyze SSH brute-force attack (file `kali-password-attack_hydra-eof.pcap`)
- Add IP Blacklist from https://www.talosintelligence.com to your firewall blacklist. Try to work with other security databases.

Write all data in file(s), and work with it throw program/frameworks that you chose. If everything works perfectly, certain things can be hidden. So, find a way to prove that everything works as expected. You should make everything visible, therefore, it can be shown in order to help streamlining the correction.

You can use programming languages, frameworks and libraries that you need.

You can also use Project Joy Sandbox. This sandbox can give you environment for run your code or testing from any place

V.2 Bonus

As long as the mandatory part rules and the general instructions are respected, you can always add all the bonuses you wish, they will be graded directly by your corrector. For example:

- Make stream analytics with network
- Automatic threats notification
- Useful dashboard
- Malware analysis
- Make your fork or pull request to Joy repo
- ...
  Bonuses will be taken into account only if the mandatory part is flawless

Chapter VI

Turn-in and peer-evaluation

Turn-in and peer-evaluation. Turn your work and author file in using your GiT repository, as usual. Only work present on your repository will be graded in defense.