MIT Research and Engineering

Cyber Threat Intelligence – Threat Hunting

Lot of automation and scripting

Works at Santander (Europe and Spain)

Banks usually buy foreign banks to enter country

City of Seattle – Information Security Analyst Intern

Tata Consultancy Service – Security Operations Center Analyst

F5 Networks (load balancer company) – Security Operations Center Analyst

Did more phishing and malware. Gathering intel. What banks it is targeting. What industry.

Santander – Cyber Threat Intelligence Analyst (working as incident response)

OSCP certification

* Penetrate through

vs CEH?

* Pass HR. doesn’t provide you with anything. Only information in tooling.

Security+

* Basics, shows interest.

CISSP more on managerial

SANS very expensive but good

In security, failure in good.

*Azure security incidents?*

What is threat intelligence?

Provides the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner.

1. Foreseeing attacks in context
2. Detection with accuracy
3. Faster response on incidents

Behavior analysis has more false positive.

Certain malwares are specific to organizations/companies.

Threat Intelligence Collections

Private Intelligence Feeds (Paids Sources)

Virtustotal – ability to download malware samples

Yrayr rules – you can look for strings and hashes

* i.e. check for dot file. Searches in multiple antivirus engines

*virtual machine acts like a sandbox?*

Not too sure. A lot of times it gives hash results.

Peer Institutions

* MS-ISAC
* FS-ISAC
* IT-ISAC

Usually IP address, hash or domain name is compromised

Open Source

* Articles & Buildings
* KrebsOnSecurity
* PhishTank (if your website is here, you can try to contest)

*Would PhishTank track unwanted applications?*

Ads not usually not block by security-pliance

Operational

* Indicators of Compromise (IOCs)

Tactical

* Tactics, Techniques and Procedures (TTPs)

Strategic

* Long-term issues
* Timely warning of threats

**Threat Intelligence Platform (TIP)**

Technology discipline that helps organizations aggregate, correlate, and analyze threat data from multiple sources in real time to support defensive actions

Into Threat Stream

* Open Source
* 3rd party
* Anomali labs
* STIX / TAXII
* ISAC / ISAO

Out of threat stream

* SIEM
* Firewall
* IPS
* End Point
* API

SIEM (Security Information and Event Management)

*Think of it as a log-in tool.*

*What you shouldn’t be seeing in the internal organization, was some tip.*

*Investigation on why having a Tor node on DNS server*

*Does SIEM is in active directory*

*What is the serious challenge in banking industry?*

*A lot of third world countries have a fraud problem. i.e. using fake version of fake Windows XP. Key log*

*Front-end capabilities in malware make it easy to fool people*

*JavaScript*

*Banks in India are not allowed to use Windows XP now.*

*Legacy systems are hard to patch*

*Supply chain problem. Trust me.*

*Top 10 design issue*

*Input data validation*

*Learned throw and exception first instead of defend. Problem of computer science.*

*External attack*

*Haven’t had a bid incident yet.*

*Insider threats*

*Happens all the time*

*Credit card numbers, bank vault numbers*

*Data loss programs are installed on end-user agents i.e. printers/computers/usbs*

*Azure security incidents?*

*Different passwords on services. A lot of the times people are doing brute-force attacks*

*Microsoft was brute-force attacking Azure. Server was compromised.*

Participants

Simon

Sam

Khan

Karthik

Cory

Neil

Name: Yuge Cheng

Email: [chengyuge925@gmail.com](mailto:chengyuge925@gmail.com)

Name: Rohan Ali  
email: [alirohan@cityuniversity.edu](mailto:alirohan@cityuniversity.edu)

Name: Junxin Ren

Email: jxren@cityuniversity.edu