OSINT Basics for Threat Hunters & Practitioners

Megan DeBlois

What I'll cover?

- Background
- OSINT Basics
- Use Cases
- Practice / Project Ideas
- Q&A

{hello}

- Non-traditional path into infosec
- Nonprofit for 7 years, focus on journos and human rights
- Now at Censys!
- Current grad student at Uni of Oxford
- Non-work things?
  - Quarantine Project, COVID19 App Tracker
  - Affiliate Board Member, WiCyS San Diego
  - Cycling in San Diego

{who is censys?}

2012

Zmap

Censys founders start an open source Internet search engine at the University of Michigan.

2017

Censys Company Launch

Censys raises funds after spinning out of the University of Michigan.

2020

Product Launch

Censys develops even better scanning engines and evolves its Attack Surface Management (ASM) Platform.

{a friendly advisory}

- Remember that entering any system that is not your own or without permission is illegal. Even if you see something on the public facing Internet.

- Some laws:
  - Computer Fraud and Abuse Act
  - California Penal Code

What is OSINT?

{a definition}

- **What it is?**
  - **<u>O</u>**pen **<u>S</u>**ource **<u>Int</u>**elligence **(OSINT)**
  - Collection and analysis of publicly available information to accomplish a particular objective. The objective could be anything from finding a person to attacking a system or defending it!
  - Different types: Google dorking (other search engines too) to social media to Internet infrastructure.
- **Why it's important?**
  - Identify publicly facing assets from an adversary to your organization.
  - Find relevant information outside the organization such as social media posts.
  - Analyze for actionable insights.

Some good tools useful for OSINT

Realized by : @Guillaume_Lpl

Maltego

- **Collecting** & **Analyzing** Open Source Intelligence
- Generate **graphical** results
- Use to determine the **relationships** and **links** between people, groups of people, companies, websites, IP, domain, documents...

Shodan

- Use to discover which **devices** are connected to the Internet, where they are **located** and **who is using them**.
- World's first search engine for **IoTs**

SpiderFoot

- **Reconnaissance** tool that automatically queries over **100 public data sources** to gather intelligence on IP, DNS, e-mail addresses, names...

CheckUsernames

- Allows you to search if a **nickname** is used on different social networks or onlines services.
- Search in more than **160 social networks**
- Fast and easy to use

Google Dorks

- This technique is based on the results of the **exploration** and **indexing** of websites by the **Googlebot** robots
- Easy to use
- Example: **site**:"toto.com" file:"pdf" intext:"topsecret"

Censys

- Search engine that collects all the data it can on **connected devices**

Realized by : @Guillaume_Lpl

- You can search by keywords, IP, domain, protocol,...

Source: https://twitter.com/SecurityGuill/status/1136304404984991744?s=20

Some good tools useful for OSINT

Realized by : @Guillaume_Lpl

WireShark

- Packets Analyser
- GUI & Command line (tshark)
- Can see & capture the network traffic and **detailled informations** about packets. .

TinEye

- A reverse image search engine, gives users the ability to search a specific url for **images**, where you can see how many times the images were found on the web and **where they were used**

Recon-ng

- Tool written in **python** mostly used in **information gathering** with its depend modules wich use online search engines plugins, API, ...

Metagoofil

- Information gathering tool designed for extracting **metadata** of **public documents** (pdf, doc, xls, ppt...) belonging to a target
- Metagoofil will perfom a search in Google to **identify** and **download the documents** to local disk and will extract the metadata with different libraries...

Nmap

- Security Scanner
- **Identify** the devices on a network
- Can detect **OS** running and **ports** open
- Can discover **services** running and **versions**

TheHarvester

- Gather **emails**, hosts, employee names, open ports,...

Realized by : @Guillaume_Lpl

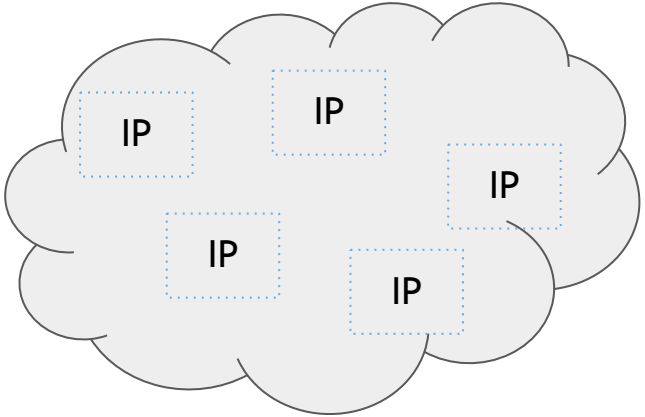
- From **different public sources** like search engines, PGP key servers **Shodan** database...

And Censys!

Source: https://twitter.com/SecurityGuill/status/1136304404984991744?s=20

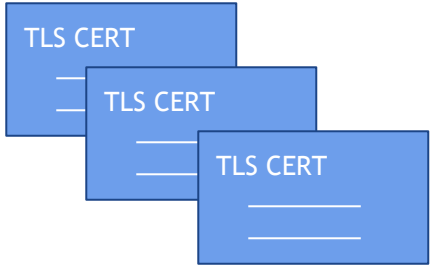
{this talk}

- Internet Infrastructure Data (as OSINT)
- Passive Scanning
  - potential misconfigurations like open ports or
  - assets on the Internet that shouldn't be or vulnerable or
  - outdated software (Apache, etc.)
- Recent examples:
  - SolarWinds
  - Microsoft Exchange Server 0-Day



Domain Name

- Subdomain
- Subdomain



{how it relates to censys?}

- Searchable Internet Data
  - Censys Search: https://censys.io/ipv4
  - Free Account
- How much Internet data?
- Why does it matter?
  - Better visibility
  - More confidence in accuracy of the assets you're searching for

	Censys	Competitor	Difference (%)
Total Services	871,606,680	442,068,682	97%
SSH Services	25,428,558	20,438,611	24%
FTP Services	11,591,726	3,486,605	232%
RDP Services	5,710,291	4,384,237	30%
Dedicated Certificate Database	4,405,452,496	N/A	
Full scan completed:	Weekly	Monthly	4x

The OSINT “Cast”

{use cases}

The
Threat Hunter

The
Defender

The
Researcher

{the threat hunter}

The Threat Hunter

Goal: Identify adversary infrastructure or assets on the Internet to help defenders better protect their systems.

- Find Indicators of Compromise (or IoCs) that can be operationalized for better defense.
- Take down malware or adversary operations and disrupt.
- Examples:
  - IP addresses
  - domain names perpetrating malicious campaigns,
  - TLS certificates being used in their infrastructure

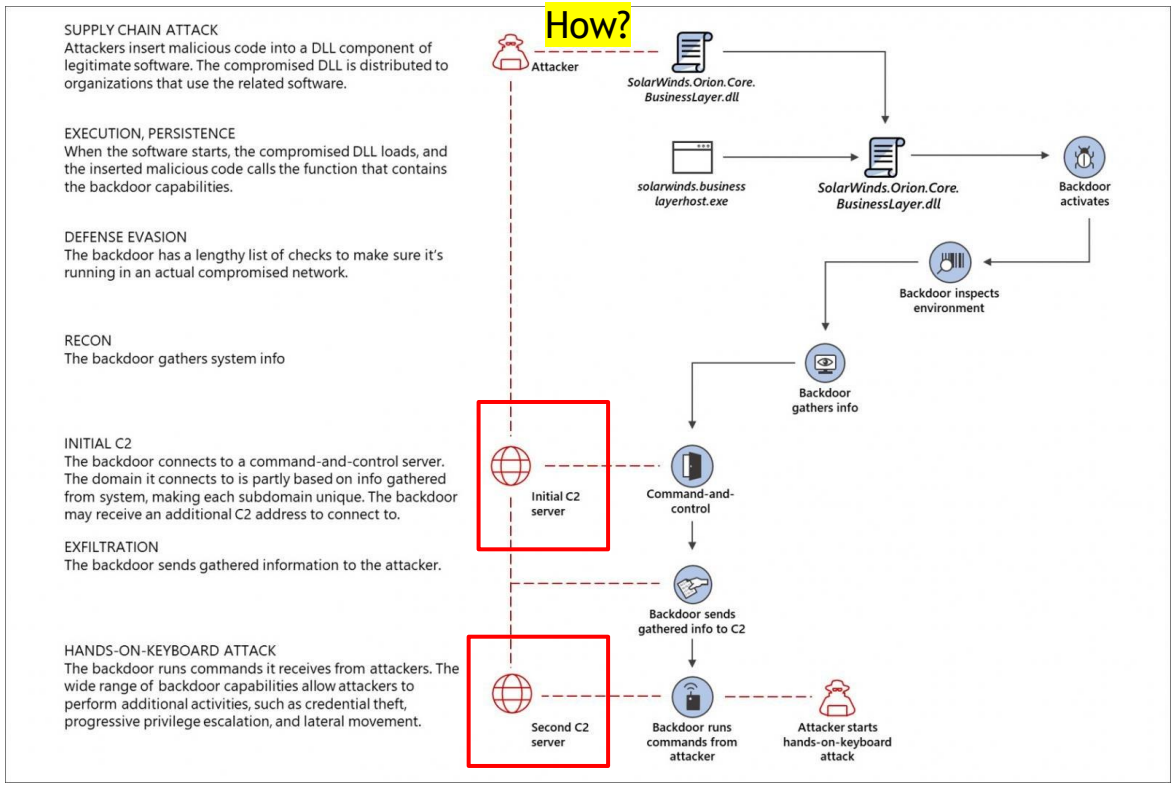
{the threat hunter} Finding C2 Infrastructure: SolarWinds

- What is SolarWinds compromise all about?(*the quick version*)
  - 3rd party compromise spreading malicious code update via legitimate channels.
  - Expansive and unique adversary infrastructure to run the operation.
  - Victims: FireEye, Microsoft via the SolarWinds compromised system
  - Resources:
    - https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html
    - https://censys.io/solarwinds-internet-wide-assessment/

solarwinds

{the threat hunter} Finding C2 Infrastructure: SolarWinds

A **C2 server** is short for **“command and control” server**, or server controlled by the malicious actor that delivers instructions to the compromised device.



Source: Microsoft

{the threat hunter} Finding C2 Infrastructure: SolarWinds

- FireEye released indicators to help defenders hunt and protect their systems post SolarWinds compromise

fireeye / sunburst_countermeasures

Notifications | Star 517 | Fork 187

Code | Issues 5 | Pull requests 3 | Actions | Projects | Security | Insights

main | sunburst_countermeasures / indicator_release / Indicator_Release_NBIs.csv | Go to file | ...

jhsmith Indicator update push — Latest commit da5b570 on Dec 16, 2020 — History

1 contributor

17 lines (17 sloc) | 1.67 KB — Raw | Blame

Search this file...

	Associated Malware	DNS Record Type	FQDN	IP	Target	First Seen	Last Seen
2	SUNBURST	CNAME	6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud[.]com		freescanonline[.]com	2020-06-13 09:20:41	2020-06-13 09:20:41
3	SUNBURST	CNAME	7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud[.]com		deftsecurity[.]com	2020-06-11 22:37:33	2020-06-11 22:37:33

{the defender}

Goal: Protect and defend the systems belonging to the organization.

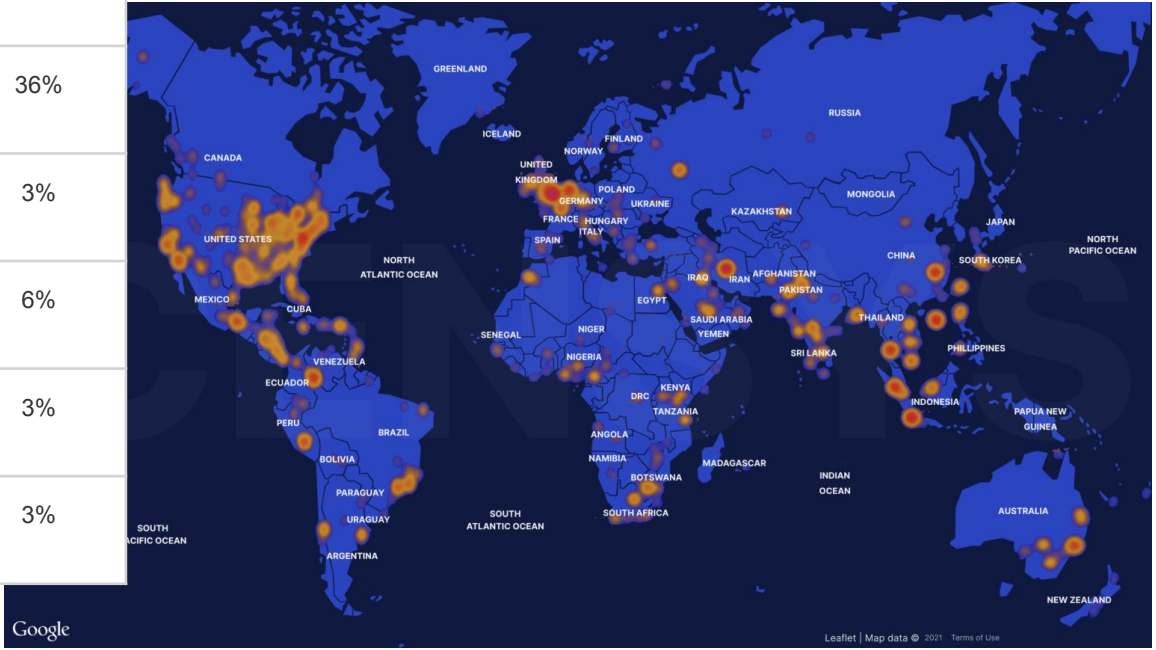
- Identify assets.
- Ensure they are secure.
- Continually validate the risk management program.
- Capture metrics to show security status of the organization.

{the defender} Identifying Org Assets: SolarWinds

https://censys.io/solarwinds-internet-wide-assessment

{the defender} Identifying Org Assets: SolarWinds

Country	# of Hosts	% of Total
United States	543	36%
China	49	3%
United Kingdom	85	6%
Iran	42	3%
Australia	40	3%



https://censys.io/solarwinds-internet-wide-assessment

{the researcher}

Goal: Answer security questions about Internet-wide trends across the Internet that are wide ranging.

- Vulnerability impact (e.g., heartbleed)
- Understanding botnets
- Encryption strength across the Internet

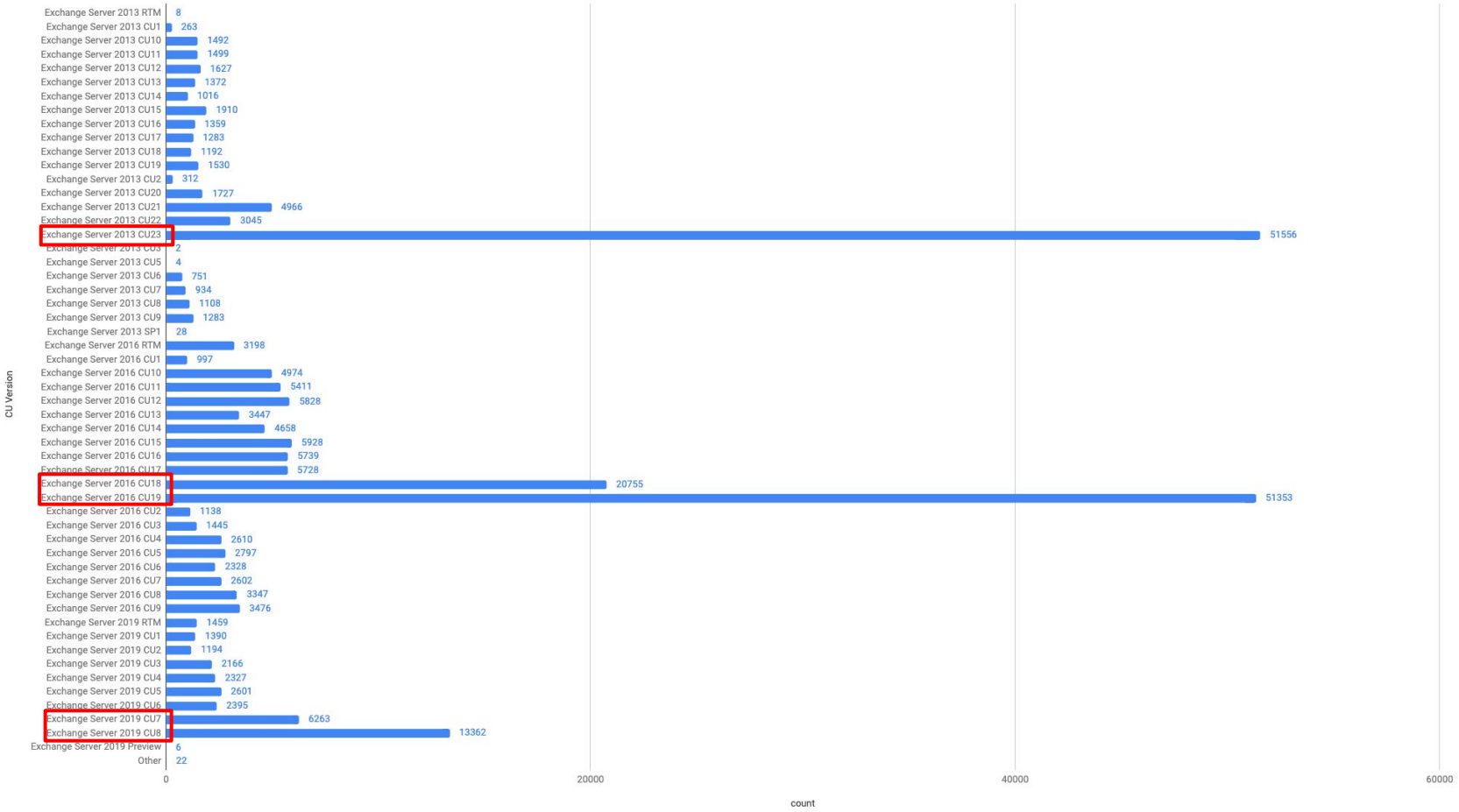
{the researcher} Microsoft Exchange Vulnerabilities

- **January:** Several vulnerabilities discovered by Volexity in Microsoft Exchange.

- **March:**
  - Microsoft Released Security Updates for specific versions of 2013, 2016, and 2019 AND recently 2010.
  - Censys observed 251,211 Exchange Servers (2013, 2016, or 2019 versions).
  - Lots of exploitation going on! (ESET)

- **Who it impacts?** Everyone, but notable percentage (approximately 20%) of a random sampling of U.S. Exchange Servers are associated with education institutions like universities.

Prevalence of Exchange 2013, 2016, and 2019 by CU Version



{the researcher} Microsoft Exchange 0-Day Affected Versions

Exchange Version	Number of Servers	Percentage of Total 2013, 2016, 2019 versions
Exchange Server 2019 CU7	6,263	2.5%
Exchange Server 2019 CU8	13,362	5.3%
Exchange Server 2013 CU23	51,556	20.5%
Exchange Server 2016 CU18	20,755	8.3%
Exchange Server 2016 CU19	51,353	20.5%
Total 2013, 2016, 2019 Affected Versions	**143,289**	**57.1%**

Getting Practice

{projects}

- Challenge: Find weird devices on the Internet
  - Example: Roombas Around the World
    `8883.mqtt.banner.tls.certificate.parsed.issuer.common_name: "Roomba CA"`

- Analyze your local Internet
  - `location.city:"San Diego"`
  - `location.city:"San Diego" AND not 443.https.tls.validation.browser_trusted: true`
  - `location.city:"San Diego" AND protocols: "3389/rdp"`
  - `location.city:"San Diego" AND protocols: "445/smb"`
  - `location.city:"San Diego" AND tags: scada`
  - `(location.city:"San Diego" AND not 443.https.tls.validation.browser_trusted: true) AND autonomous_system.description.raw: "UCSD"`
  - `(ucsd.edu) AND autonomous_system.description.raw: "AMAZON-02" AND location.city: San Diego`

{projects}

- Find phishing websites
  - Community Tutorial by 0xpatrik
  - Assumption is the malicious actors are using Let's Encrypt

```
(apple.com*) AND parsed.issuer.organization.raw:"Let's Encrypt" and
parsed.validity.start: [2020-01-01 TO *]
```

- Perform a security assessment (**Get Consent!**)
  - Gather the assets (hosts, domains, IPs)
  - Find potential security issues (open ports, bad encryption, people spoofing your domain)

- And more!
  - Censys Search (free): https://censys.io/ipv4
  - Censys Definitions / Syntax: https://censys.io/ipv4/help/definitions?q=&

{student spotlight}

- New initiative at Censys, is working with educational institutions.
  - Censys Use Cases for Educators
  - Censys Student Research Highlights
  - Censys Researcher Spotlight

- Conducting a mini research project? Contact us for a student spotlight!
  - Contact: research@censys.io

- Interested in an internship?
  - Contact: megan@censys.io

{resources}

- SANS Free Resources for OSINT
  https://www.sans.org/blog/-must-have-free-resources-for-open-source-intelligence-osint-/

- Cyber Threat Intelligence Self Study Plan by Katie Nickels
  https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a

- Advanced Persistant Infrastructure Tracking by Nils Kuhnert
  https://censys.io/advanced-persistent-infrastructure-tracking/

Questions?

Thank you!

Email: megan@censys.io
Twitter: @realMegDeBlois