CALIFORNIA STATE UNIVERSITY SAN MARCOS

THESIS SIGNATURE PAGE

PROJECT SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE

MASTER OF SCIENCE

IN

CYBERSECURITY

PROJECT TITLE: INTERSHIP EXPERIENCE

AUTHOR: Chelsie Power

DATE OF SUCCESSFUL DEFENSE: 5/5/2017

THE PROJECT HAS BEEN ACCEPTED BY THE THESIS COMMITTEE IN
PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER SCIENCE IN
CYBERSECURITY.

Teresa Macklin PROJECT COMMITTEE CHAIR	SIGNATURE	5 May 2017 DATE
Yi Sun PROJECT COMMITTEE MEMBER	SIGNATURE	5-5-17 DATE

EXECUTIVE SUMMARY

Internship Experiences at Company X

Chelsie Power

April 2017

Professional Masters Degree Program

Cal State University San Marcos

My Semester-in-Residence Project was conducted at Company X. Company X operates a large data center. After an application and interview process, I was invited to intern with Company X and did so for 8 hours every week for 15 weeks.

My project goals were to observe, learn, and practice concepts from my cybersecurity education as they applied to real-world applications. I was given many resources including access to equipment, access to tools, and unrestricted access to Company X employees to ask any questions or request clarification.

The term “IP” is part of a longer abbreviation, TCP/IP, which stands for Transmission Control Protocol/Internet Protocol. Each device connected to the internet is assigned an IP. Some of my assigned work during the internship was to hunt and isolate malicious external IPs as well as compromised internal IPs. Using this information, certain outside IP ranges, identified as malicious, were added to a blocklist. Additionally, I created malware fact sheets for distribution, created flowcharts for reactive and proactive hunting methodologies as it pertains to the SIEM QRadar and saved customized QRadar searches for future use. During the hunting process, many types of attacks were encountered such as DNS Amplification Attacks and DDoS attacks. Dashboard visualizations of these attacks were generated by tools such as Stealthwatch and Arbor SP for analysis.

While I was at Company X, I participated in a technology analysis to determine the cost effectiveness of malware remediation. The approach chosen for this was to do a malware study, translating exploited customer devices, (the incidence of which is on the rise), to network utilization. Many exploits such as botnets or DDoS attacks unnecessarily consume bandwidth. This not only causes unnecessary expense, but impacts of consumer satisfaction with network performance. Company X is considering offering remediation as a service and they opened a Security Operations Center. I created a flowchart to demonstrate the path data takes when it is sent into the SOC, parsed, and made available for searching, alerting, correlation, threat prevention and incident response.

An additional assigned task was to migrate virtual machines from the existing unsupported VMware environment to the OpenStack environment. I ran into several issues with this, and eventually discovered that Windows images are not designed to properly bootstrap into an OpenStack environment

and would require at least a week of fine-tuning to get right. Company X ultimately decided to stick with the working but unsupported VMware environment.

Company X has a pentesting team that performs penetration tests and vulnerability scans for internal and external customers. I was able to learn some of the tools and techniques they used, as well as the importance of contracts that specify the rules of engagement.

One challenge is that I was also only there 8 hours a week, so it was difficult to start on a project only to arrive on site nearly a week later with a different threat in the spotlight or having missed important developments.

I appreciate my internship experiences at Company X and will carry them with me throughout my professional career.

INTERNSHIP AT AN ISP

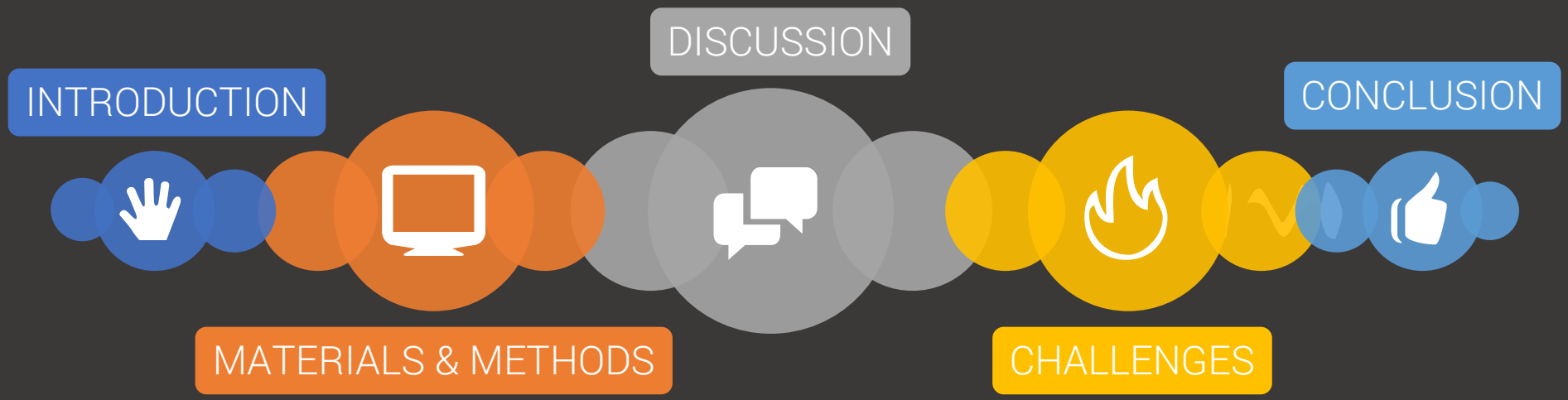
Chelsie Power

Faculty Advisors
Project Chair: Teresa Macklin
Committee Member: Yi Sun

California State University
SAN MARCOS

SIR Report

FIVE PRESENTATION TOPICS



INTRODUCTION

COMPANY X WELCOMES ME

PROCESS

FIND A CONTACT

SENT RESUME

PHONE INTERVIEW

FIRST DAY

Met with Security – Badge, Proof of Citizenship

Met the Team

Setup: Assigned an office with laptop and docking station.

Scope: Quickly learned that scope of my project had changed.

MATERIALS & METHODS

TOOLS I OBSERVED OR WORKED WITH

01 ARBOR TMS

DDoS mitigation

Detects attack and sends data to a blackhole or "loopback 0". Sends logs to Stealthwatch.

02 QRADAR

Netflow Collection

Data collection, processing, and searching.

03 STEALTHWATCH

Network Visibility

Turns data into real-time intelligence to provide network visibility.

04 SPLUNK

Syslog Collection

Software for searching, monitoring and analyzing machine generated big data via a web interface

05 ANOMALI

Threat Intelligence Platform

Uses info gathered from 200 feeds to provide additional threat info. Some free, some not.

06 SANDVINE

Shapes and Classifies Traffic

Prioritizes traffic based on predefined constraints using policies. Classify as "mail", "video", etc.

DIFFERENCE BETWEEN NETFLOW AND SYSLOG

Both at a 1/1000 sample data rate.

Netflow records: IP traffic statistics that includes IP (source, dest), protocol information

Syslog: Logging protocol. May include security events, error logs, warnings, etc.

MATERIALS & METHODS

ONLINE TOOLS

Name	Capabilities	URL
IPVOID	Scans an IP through IP reputation services and DNS-based blacklists (DNSBL). This allows us to detect IPs flagged as malicious and used for spamming activity.	http://www.ipvoid.com
Shodan	A search engine for internet-connected devices.	http://www.shodan.io
MXTOOLBOX	A search of MX Records, whois search, and reverse IP lookup tool.	http://www.virustotal.com
VirusTotal	A tool that analyzes suspicious files and urls.	http://www.mxtoolbox.com
Web Scraper	A chrome extension that creates a sitemap of any website that can be exported as a CSV.	http://www.webscraper.io

DISCUSSION

HUNTING

BUSINESS CONSIDERATIONS

SOC IMPLEMENTATION

PENTESTING TEAM

PENTESTING LAB

DISCUSSION
HUNTING

What is hunting?

- Researching and isolating malicious IPs communicating on the ISP network.
- Created hunting flowcharts for use with QRadar.
- Created custom searches.
- Created vulnerability/threat factsheets.
- End result is to add to the ACL Blacklist.

From: <soc@us-cert.gov>
Date: February 22, 2017 at 7:27:59 AM MST
To: [redacted]
Subject: NCCIC Avalanche Notification INC0[redacted]

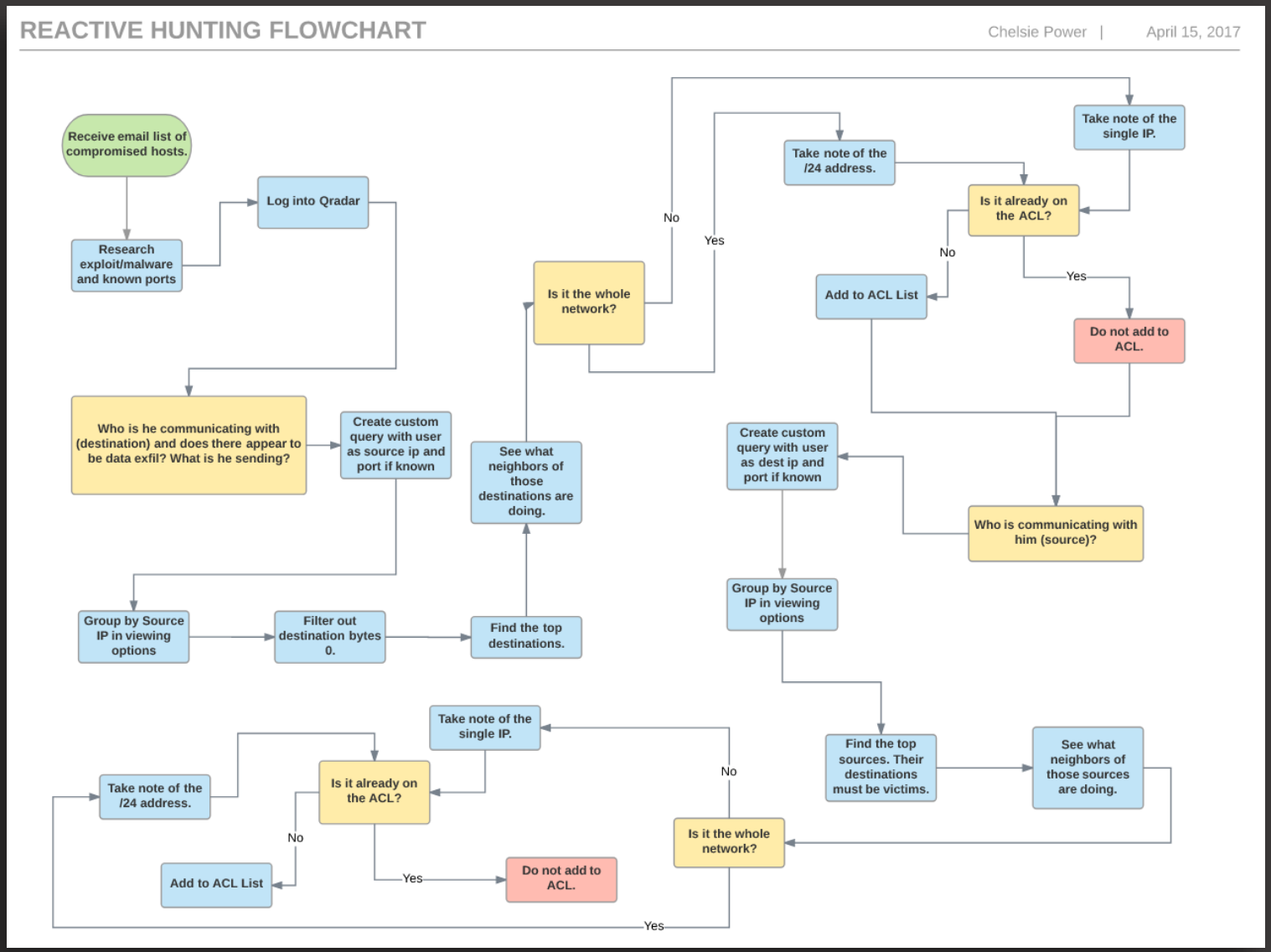
A trusted third party notified the Department of Homeland Security United States National Cybersecurity & Communications Integration Center (NCCIC) that one or more machines on your network was infected with malware associated with the Avalanche botnet infrastructure during December 2016. Avalanche is a large global network hosting infrastructure used by cyber criminals to conduct phishing and malware distribution campaigns and money mule schemes. A system infected with Avalanche associated malware may be subject to malicious activity including the theft of user credentials and other sensitive data, such as banking and credit card information. Some of the malware has the capability to encrypt user files and demand a ransom be paid by the victim to regain access to those files. In addition, the malware may allow criminals unauthorized remote access to the infected computer. Infected systems could be used to conduct distributed denial-of-service (DDoS) attacks. For additional information, please see the following US-CERT Technical Alert (TA16-336A): https://urldefense.proofpoint.com/v2/url?u=https-3A__www.us-2Dcert.gov_ncas_alerts_TA16-2D336A&d=DwIFaQ&c=jcv3orpCsv7C4ly8-ubDob57ycZ4jvhoYZNDBA06fPk&r=i8DPA13ymPIVU4GA-ducNAk_wjn0F7yUvr2LJp_Jn5Q&m=WKOUSH8Y1ynQsRoy592yZN-mNNqJ-Q2_EeoO6W2WIVk&s=HsZ3jAzBIA2p22OhTNhxp9zobARUANfKvAiOXBUip1Y&e=

The following IP addresses associated with your network were observed communicating to one of the Avalanche servers (i.e. IPs or domains).

[redacted] was infected at 2/21/2017 13:15 UTC with avalanche-nymaim
[redacted] was infected at 2/21/2017 0:40 UTC with avalanche-tiny-banker
[redacted] was infected at 2/21/2017 3:26 UTC with avalanche-nymaim
[redacted] was infected at 2/21/2017 0:49 UTC with avalanche-rovnix

GENERATED MATERIALS

REACTIVE HUNTING



GENERATED MATERIALS

VULNERABILITY/THREAT FACT SHEETS

SIP Attack Fact Sheet

Name:	SIP Attacks
First Discovered:	Gained popularity in 2015
Description:	SIP is a VOIP protocol. This is an attack on SIP devices to gain access with the purpose of making international calls.
Affects:	SIP Servers
# of devices affected:	According to Shodan, there are over 500K SIP devices visible from the internet.
How it works:	Attackers will scan for SIP servers. Once identified, they try to enumerate the server configuration and gain access by trying different passwords.
Detection of infected host:	Outbound calls to external PSTN (Public Switched Telephone Network) numbers, usually to place international calls.
Detection of malicious scanners:	Port 5060/UDP (default SIP port)
Business Impact	unknown

SIP Attacks

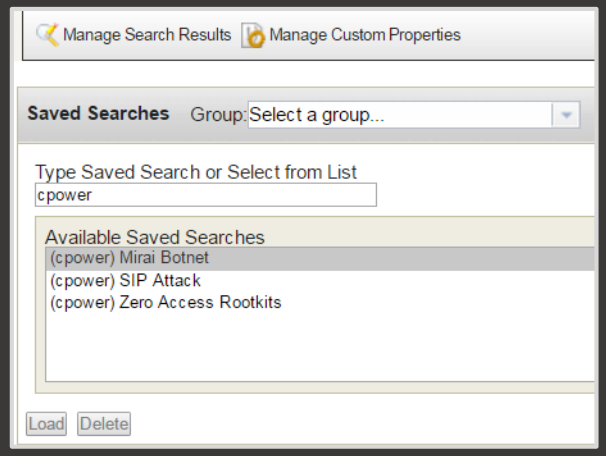
Mirai Botnet Fact Sheet

Name:	Mirai
First Discovered:	August 2016
Description:	Part of a DDoS-for-hire service that launches DDoS attacks against specified targets in exchange for bitcoin payment. Paid subscription database checks are visible in the released code.
Affects:	Linux machines. Most commonly affects internet enabled DVRs and surveillance cameras.
# of devices affected:	approximately 500,000
How it works:	Has a list of 61 usernames and passwords that it tries. Many IoT devices do not allow you to change the default passwords. When it connects it looks for other malware on the device, cleans it, and installs its own malware. It stays in memory and gets commands from the C&C servers.
Detection of infected host:	Look for closed ports TCP 22, TCP 23, and TCP 80
Detection of malicious scanners:	Look for scanning activity on ports TCP 7547, TCP 2323 (SSH), 23 (telnet), TCP 103 and TCP 101
Business Impact	These customers' devices become part of a botnet and the traffic causes them to go over their DAT, causing issues with data availability and customer satisfaction.

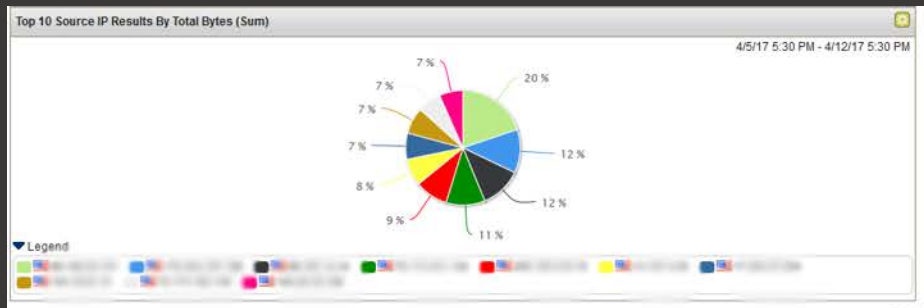
Mirai Botnet

DISCUSSION

ATTACKS



CUSTOM SEARCHES

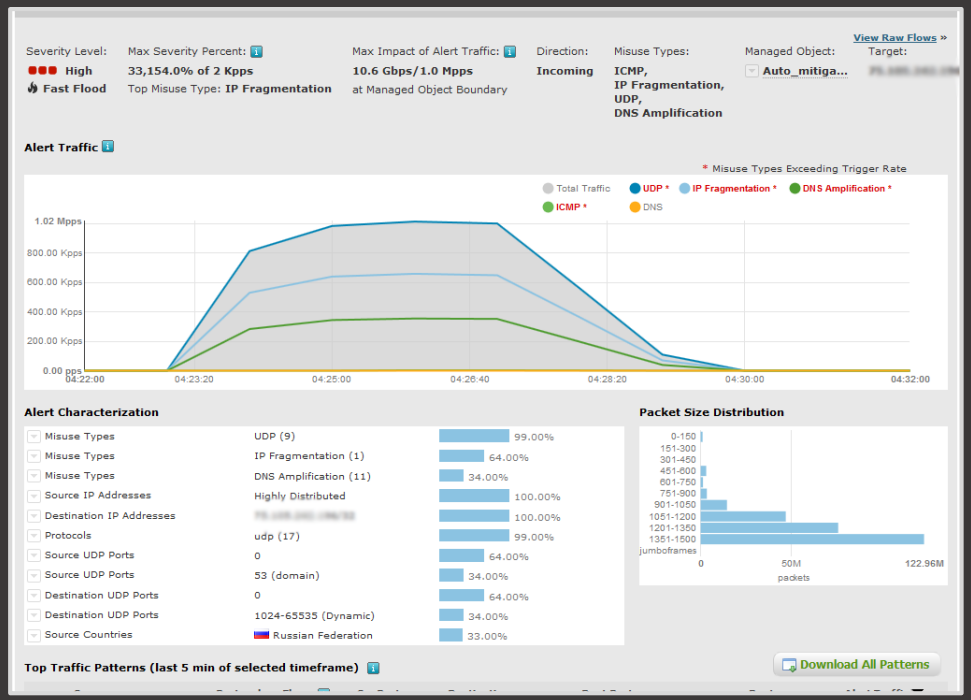


(Hide Charts)

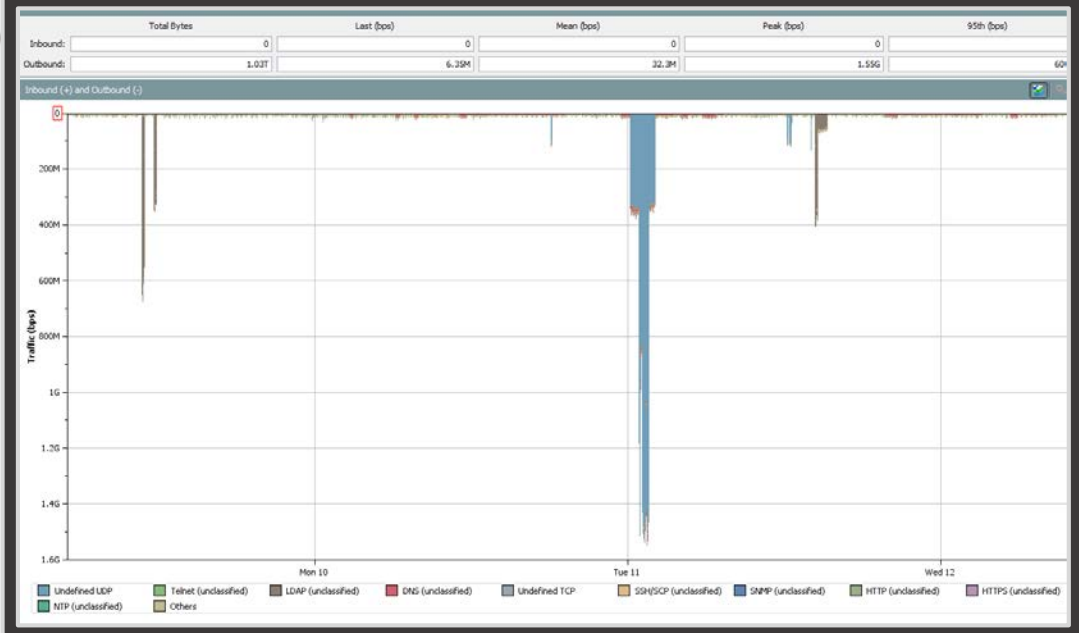
Source IP	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Application (Unique Count)	Destination Bytes (Sum)	Source Bytes (Sum)	Total Bytes (Sum)	Destination Packets (Sum)	Source Packets (Sum)	Total Packets (Sum)	Count
		Multiple (14,951)	2323	Multiple (4)	Other	120	672,165	672,285	3	15,005	15,008	14,98
		Multiple (8,959)	2323	Multiple (2)	Other	40	415,389	415,429	1	8,975	8,976	8,96
		Multiple (8,706)	2323	Multiple (2)	Other	204	393,917	394,121	4	8,723	8,727	8,71
		Multiple (8,080)	2323	other	Other	71	373,387	373,458	1	8,091	8,092	8,08
		Multiple (4,987)	2323	Multiple (2)	Other	0	225,643	225,643	0	5,002	5,002	4,99
		Multiple (4,918)	2323	other	Other	0	227,597	227,597	0	4,928	4,928	4,92
		Multiple (4,726)	2323	Multiple (2)	Other	0	189,484	189,484	0	4,727	4,727	4,72
		Multiple (3,656)	2323	other	Other	0	161,903	161,903	0	3,658	3,658	3,65
		Multiple (3,648)	2323	other	Other	0	159,070	159,070	0	3,671	3,671	3,66
		Multiple (3,647)	2323	other	Other	0	161,544	161,544	0	3,665	3,665	3,66
		Multiple (2,462)	2323	other	Other	0	105,655	105,655	0	2,463	2,463	2,46
		Multiple (2,163)	2323	Multiple (3)	Other	0	98,805	98,805	0	2,185	2,185	2,18
		Multiple (2,038)	2323	other	Other	40	92,195	92,235	1	2,043	2,044	2,04
		Multiple (1,918)	2323	other	Other	0	86,689	86,689	0	1,922	1,922	1,92
		Multiple (1,908)	2323	other	Other	0	85,355	85,355	0	1,912	1,912	1,91
		Multiple (1,760)	2323	other	Other	0	79,792	79,792	0	1,762	1,762	1,76
		Multiple (1,717)	2323	other	Other	0	78,240	78,240	0	1,719	1,719	1,71
		Multiple (1,579)	2323	other	Other	0	78,042	78,042	0	1,585	1,585	1,57
		Multiple (1,507)	2323	other	Other	40	79,278	79,318	1	1,605	1,606	1,60
		Multiple (1,503)	2323	other	Other	0	79,229	79,229	0	1,598	1,598	1,59

INCOMING MIRAI SCANNING —USING PORT 2323 TO SCAN AND RUN DICTIONARY ATTACKS AGAINST IOT ALTERNATE TELNET PORT

DISCUSSION
ATTACKS



BLENDED DDOS ATTACK - ARBOR



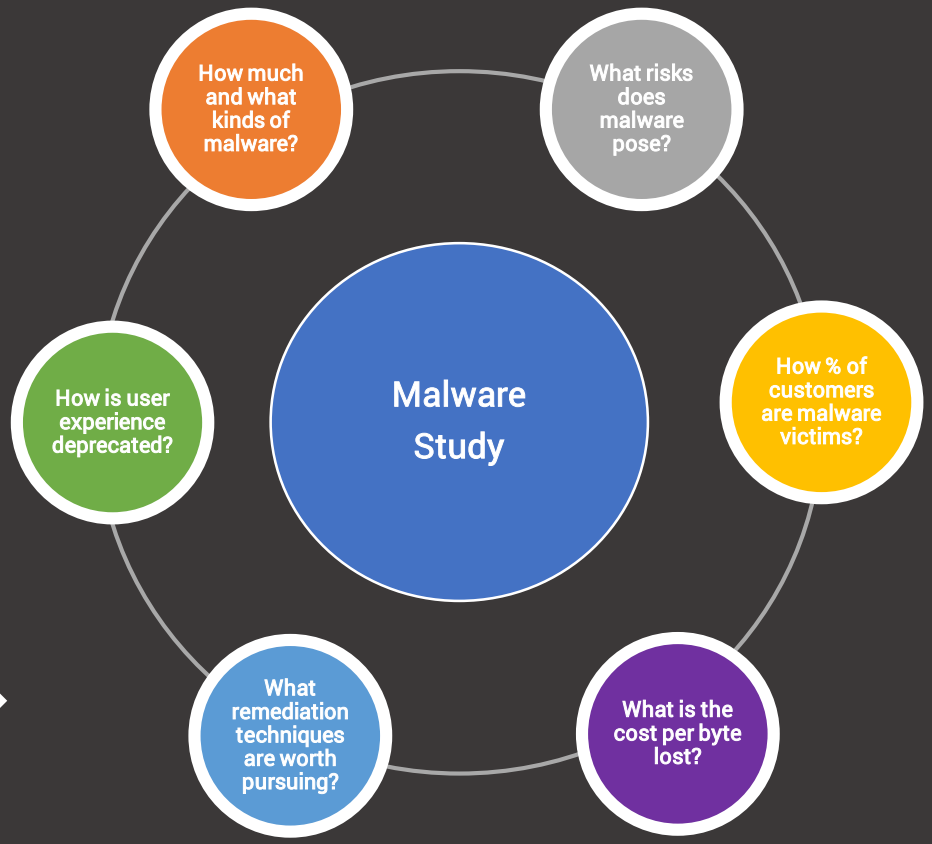
TRAFFIC REDIRECTED TO BLACKHOLE - STEALTHWATCH

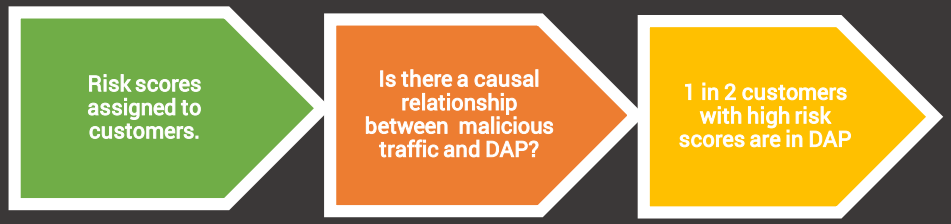
DISCUSSION

BUSINESS CONSIDERATIONS

MALWARE STUDY

Investigate malware on ISP with goal of increasing a return on investment and customer experience.





DISCUSSION

BUSINESS CONSIDERATIONS

Offer remediation as a service?

Loss of Consumer Confidence, Hurt Customer Experience, Damage Brand

Customers on Blacklists
Lose ability to navigate to websites.

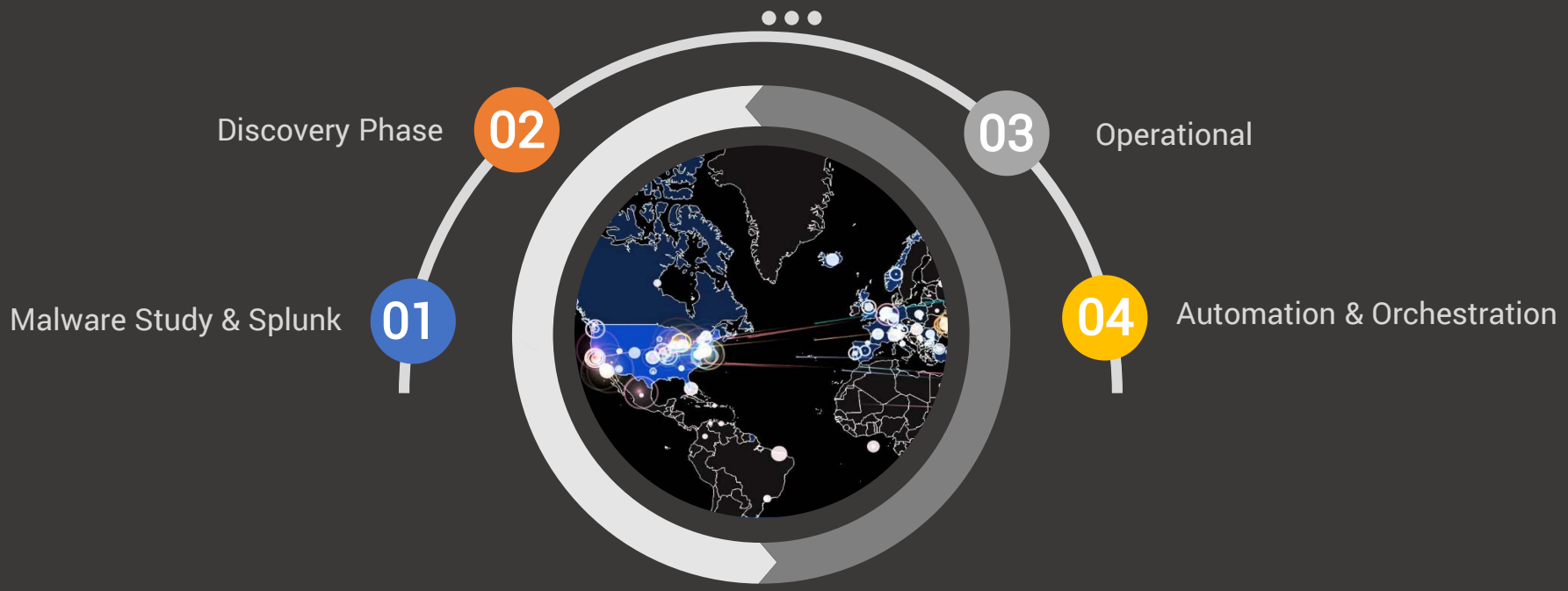
Hackers Selling ISP Bandwidth

DISCUSSION

ISP SECURITY OPERATIONS CENTER

- Physical location staffed by analysts.
- Takes hunting to the next level.
- Suite of tools.
- Analysts real time incident response, threat analytics, data correlation and alerting.

FOUR PHASES OF SECURITY OPERATIONS CENTER IMPLEMENTATION



GENERATED MATERIALS

SPLUNK

splunk> Search

Administrator App

Summary Search Status Dashboards & Views Searches & Reports

Search

host="[redacted]" wmi_type="WinEventLog:Application"

All time

258 matching events

Save

Hide Zoom out Zoom to selection Deselect

Linear scale

5
3

12:00 PM Mon Jul 23 2012 | 12:00 AM Tue Jul 24 | 12:00 PM | 12:00 AM Wed Jul 25 | 12:00 PM

Field discovery is: On

Hide

3 selected fields Edit

- host (1)
- source (1)
- sourcetype (1)

29 interesting fields

- Category (3)
- CategoryString (3)
- ComputerName (1)
- dest (1)
- dvc (1)
- dvc_nt_host (1)
- event_id (≥100)
- EventCode (4)
- EventIdentifier (4)
- EventType (1)
- eventtype (2)
- index (1)
- linecount (1)
- Logfile (1)

258 results over all time

Export Options

« prev 1 2 3 4 5 6 next » 50 per

Overlay: None

	_time	sourcetype	source	host	_raw
1	7/25/12 11:00:34.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230034.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84580
2	7/25/12 11:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84579
3	7/25/12 11:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230015.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84577
4	7/25/12 11:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725230015.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84578
5	7/25/12 10:16:57.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725221657.000000 Category=7 CategoryString=Core EventCode=10000 EventIdentifier=10000 EventType=3 Logfile=Application RecordNumber=84576 SourceName=
6	7/25/12 10:00:43.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220043.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84575
7	7/25/12 10:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84574
8	7/25/12 10:00:18.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220018.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84573
9	7/25/12 10:00:15.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725220015.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84572
10	7/25/12 9:09:11.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210911.000000 Category=0 CategoryString=NULL EventCode=1704 EventIdentifier=1073743528 EventType=3 Logfile=Application RecordNumber=84571 SourceN
11	7/25/12 9:00:41.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210041.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84570
12	7/25/12 9:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84569
13	7/25/12 9:00:17.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210017.000000 Category=10 CategoryString=Online Defragmentation EventCode=701 EventIdentifier=701 EventType=3 Logfile=Application RecordNumber=84568
14	7/25/12 9:00:16.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725210016.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84567
15	7/25/12 8:00:27.000 PM	WMI:WinEventLog:Application	WMI:WinEventLog:Application		20120725200027.000000 Category=10 CategoryString=Online Defragmentation EventCode=700 EventIdentifier=700 EventType=3 Logfile=Application RecordNumber=84565

DISCUSSION

PENETRATION TESTING TEAM PROCESS

DISCUSSION
PENTESTING LAB

Asked to migrate virtualizations environments for old pentesting lab images from VMware to Openstack due to lack of support.

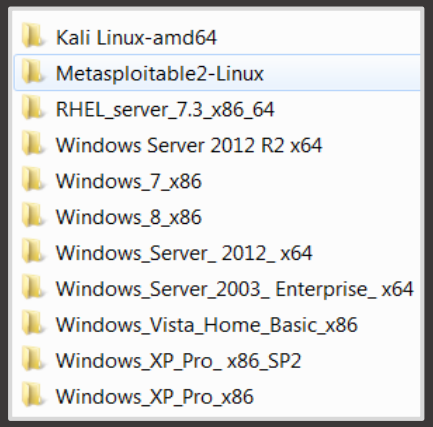
Successes

Tutorials

Replicated Firewall Rules

SSH, RDP, etc.

Obtained relevant images for starting from scratch.



Challenges

Access.

Downloading Images

Delivery of Images

Upload Failures

-Use OpenStack CLI for verbose logging.

VMDK Files

-Needed QCOW2

Converted Files Fail to Boot

-Bootstrap data will not convert properly.

Try To Setup Lab From Scratch

.IMG files not natively supported.

-Needed to convert to QCOW2

Kali Linux Setup Failure

-Contacted company Cloud Support.
-Setup locally (specify network, hostname, etc.)

Only WINDOWS OS's Newer than Server 2012 will work

-No Windows XP

Openstack designed for Linux OS. Each version of Windows will take at least a week of testing to boot properly.

CHALLENGES

Scope of Proposal Changed

Lack of Time
Project outside of normal internship.

CONCLUSION

- Felt extremely welcomed.
- Scope changed but that's okay.
- Real-world cybersecurity knowledge and experience.
- Classroom and career knowledge prepared me.
- Business considerations are key.

THANK YOU

HAVE A NICE DAY