SAN JOAQUIN COUNTY

Greatness grows here.

SJ County Security Session Protecting Critical Assets

October 8, 2020 For Treasurer and Tax Collector

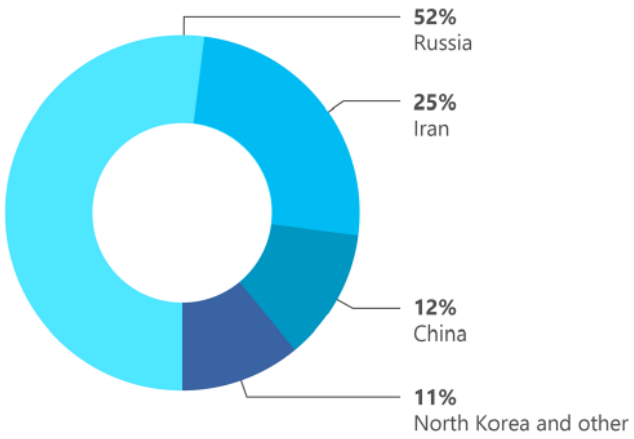
Chris Cruz, Chief Information Officer (CIO)
Director, Information System Division (ISD)

Cyber Threat Landscape

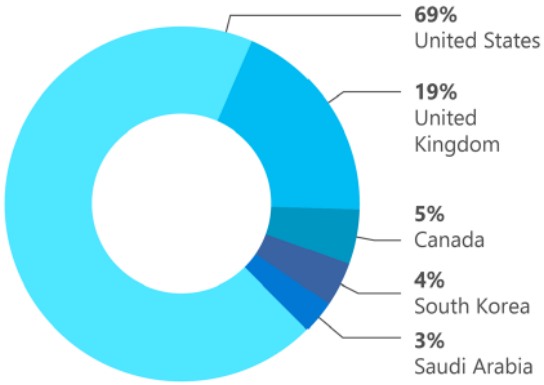
Top 6 targeted industry sectors

- Non-Governmental organizations (32%)
- Government organizations (13%)
- Information technology firms (7%)
- Higher Education (7%)
- Professional services (31%)
- International organizations (10%)

Support services and trusted third parties can serve as launch points for intrusions or collection against government targets, whose systems might have more robust security protocols in place



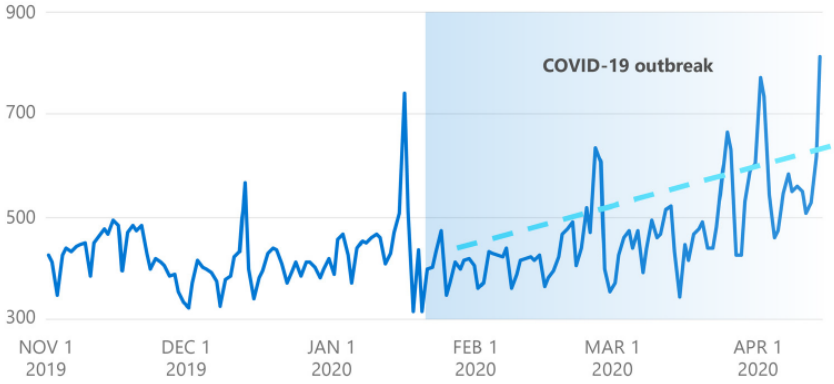
Country of activity origin for NSNs (July 2019–June 2020)



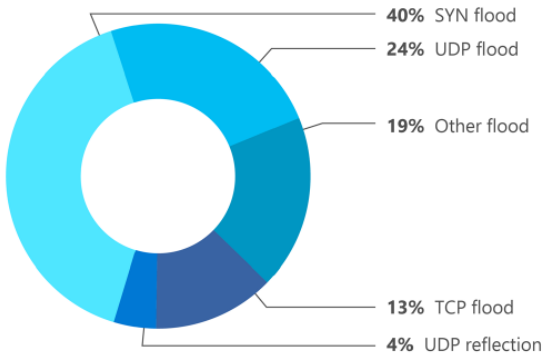
Top 5 targeted geographic regions based on NSNs (July 2019–June 2020)

Source : Microsoft Digital Defense Report, September 2020

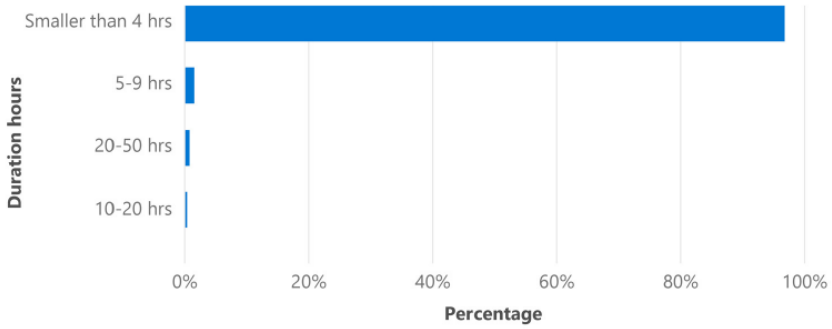
Number of DDoS attacks during COVID-19 outbreak



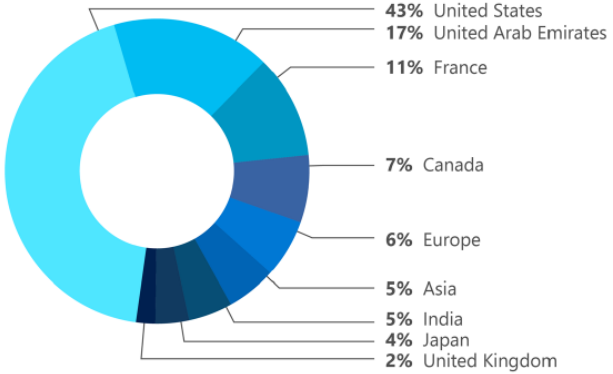
DDoS attack type (January–June 2020)



96.88% of attacks are of small duration (January–June 2020)



Destination region distribution (January–June 2020)



Source : Microsoft Digital Defense Report, September 2020

Top Botnets

Botnet
Description

A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform Distributed Denial-of-Service attacks, steal data, send spam, and allows the attacker to access the device and its connection. Wikipedia

Source - Check point software security report 2020

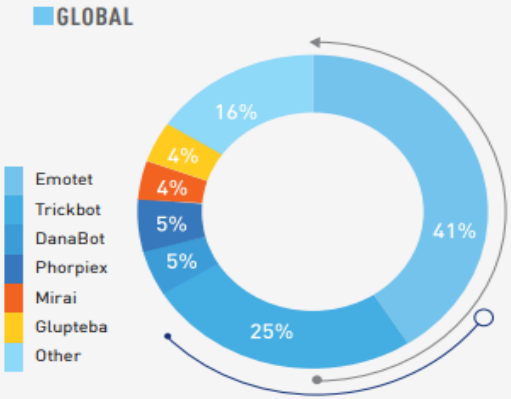


Figure 16: Most Prevalent Botnets Globally

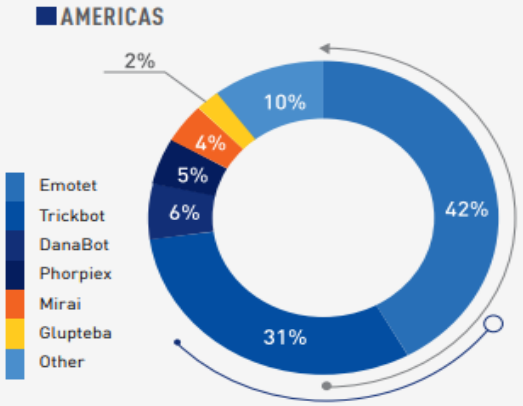


Figure 17: Most Prevalent Botnets in the Americas

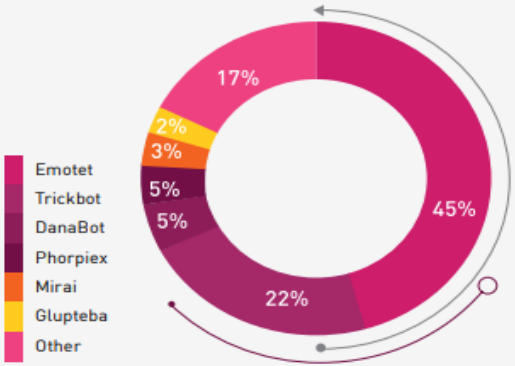


Figure 18: Most Prevalent Botnets in EMEA

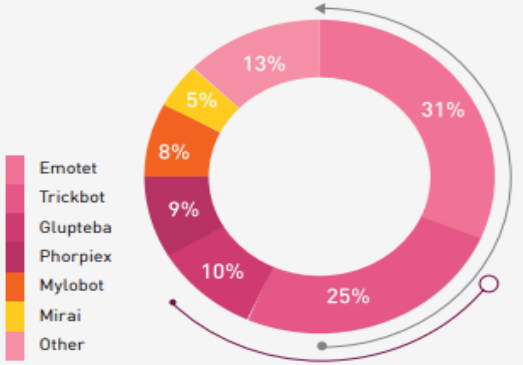


Figure 19: Most Prevalent Botnets in APAC

TOP MALICIOUS FILE TYPES: WEB VS EMAIL

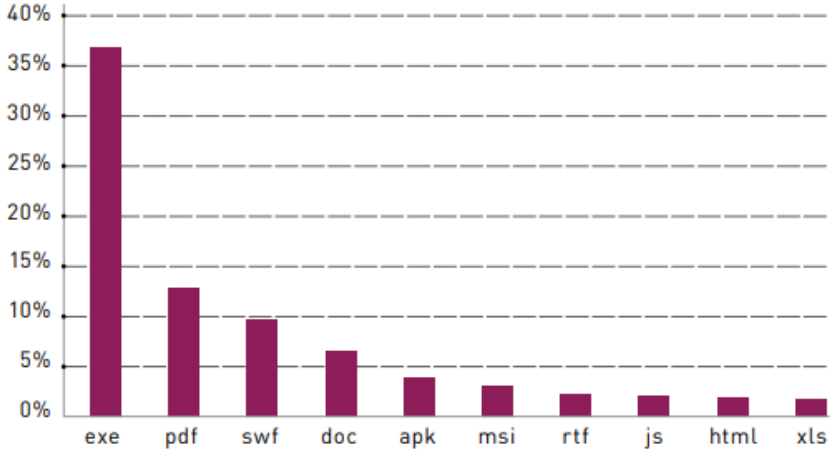


Figure 1: Web – Top malicious file types

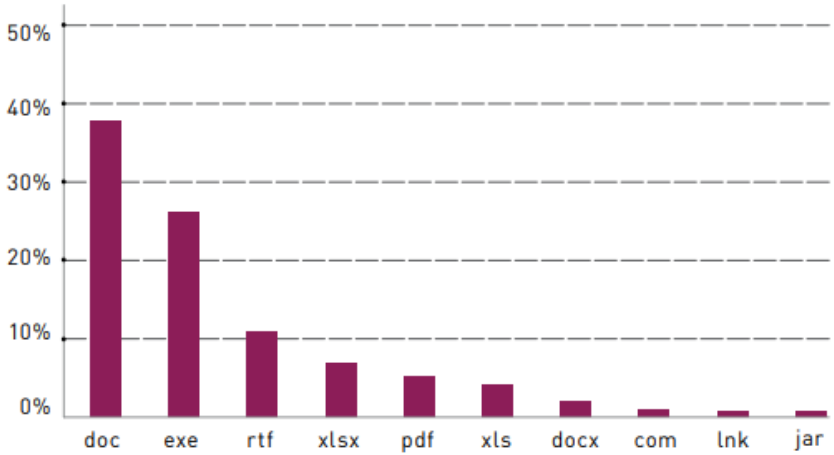
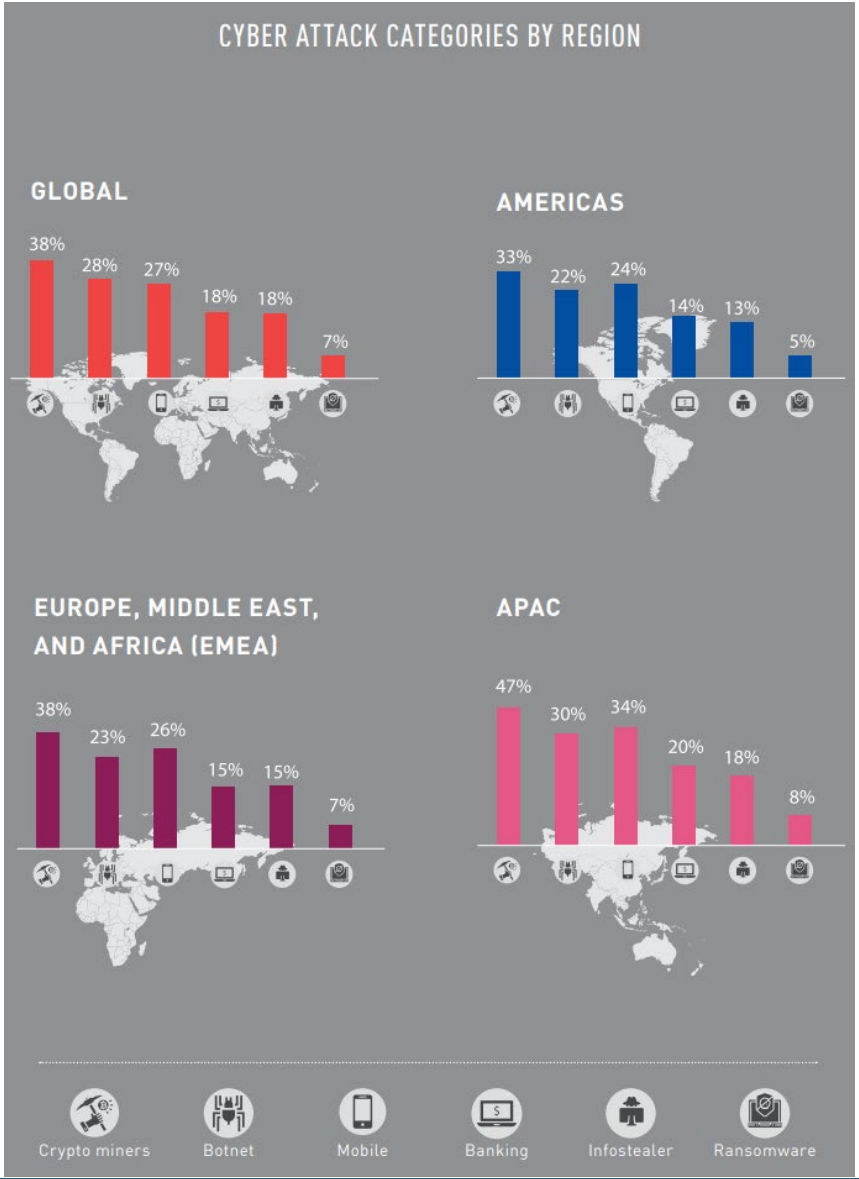


Figure 2: Email – Top malicious file types

Key call outs –

1. .exe file type is #1 in Web based attacks
2. .doc file type is #1 in email based attacks
3. .doc/.exe/.pdf are in top 5 for both type of attacks

Source - Check point software security report 2020



Key call outs –

1. Crypto miners are #1 in all 3 world regions (Americas/EMEA/A PAC)
2. Mobile attacks are on the rise
3. Ransomware distribution has shifted from a numbers game to a more targeted approach of “big game hunting,”

Source - Check point software security report 2020

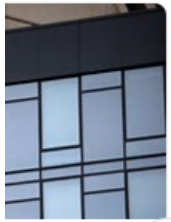
Couple of Recent Cyber Security Breaches

CYBERCRIME · **Published** July 1

University of California pays over $1M to ransomware gang

On **April 20, 2020**, Cognizant learned that the attackers staged and likely exfiltrated a limited amount of data from Cognizant's systems. Based on our investigation, we understand that this activity occurred between April 9 and 11." reads the notice of data breach.

vork



if hackers
Ms after

Cognizant admitted data breach in April Ransomware ...
securityaffairs.co/wordpress/104951/data-breach/cognizant-data-breach.html

Time · 2d

MSN · 2d

YAHOO! · 2d

PRICE LIST FOR HACKER GOODS AND SERVICES

CREDIT CARD WITH CVV NUMBERS									
VISA/MASTERCARD					AMEX/DISCOVER				
US	UK	CANADA	AUSTRALIA	EU	US	UK	CANADA	AUSTRALIA	EU
$5-12	$15-20	$10-20	$5-25	$18-35	$5-12	$10-25	$15-25	$8-30	$18-35

PAYPAL ACCOUNTS							
AVG. PRICE	$50	$60	$80	$100	$200	$250-300	$500-550
BALANCE	$500	$600	$800	$1,000-2,000	$1,500-4,500	$2,500-8,500	$5,000-13,000

CLONED ATM CARDS FOR BANK ACCOUNTS										
AVG. PRICE	$300-450	$600-800	$850-1,000	€150	€300	€450	€550	£154	£270	£385
BALANCE	$5,000	$10,000	$15,000	€2,000	€5,000	€8,000	€10,000	£2,000	£3,000	£5,000

FULLZ DATA			
ORIGIN	AVG. PRICE	ORIGIN	AVG. PRICE
US	$30-40	SWEDEN	$20-25
UK	$35-50	FRANCE	$20-25
CANADA	$30-45	GERMANY	$20-25
AUSTRALIA	$17-50	IRELAND	$20-25
ITALY	$20-25	MEXICO	$15-20
SPAIN	$20-25	ASIA	$15-20
DENMARK	$25-30	Other EU	$17-60
Includes: Full Name, Date of Birth, Address, City, Zip Code, State, Country, Phone Number, Mother's Maiden Name, Social Security Number, Driver's License Number			

BUSINESS FULLZ DATA	
Includes: Bank Acct Numbers, Employee Identification Number (EIN), Certificate of Business, Corporate Officers' Names, Birth Dates, SSN.)	$35-60

$ = U.S. dollars; € = Euro; £ = British pound

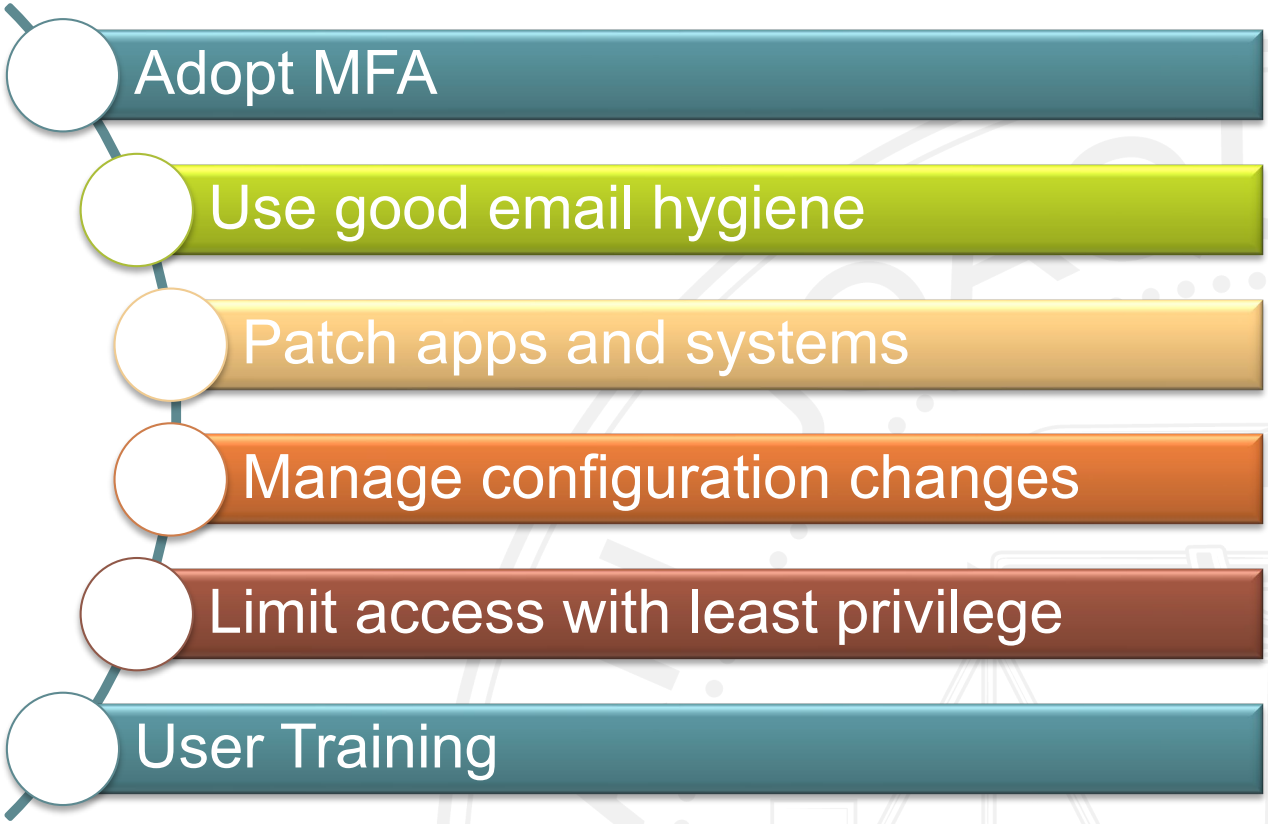
Source : Dark Market Report 2020 by Armor

Multi-Factor Authentication(MFA)

- Multi-Factor Authentication
  - Something you have (as hardware token)
  - Something you know (as password)
  - Something you are (as biometric)
- Security is enhanced via the use of Multi-Factor Authentication since a second token is required in addition to a password
- Chance of account compromise goes down drastically (70%+) with MFA
- Examples of a second factor
  - Secure ID token (as Yubikey)
  - Smart card with encrypted credential
- MFA will be highly advised / enforced in the near future
- All administrative access to the O365 tenant is already MFA enabled for all tenant administrator

SJC

Steps you can take today



Tanium

S.No.	Module	Description
1	Asset	Know what software and hardware we have at all times
2	Deploy	Manage software at enterprise scale
3	Discover	Take control of unmanaged endpoints and rogue devices
4	Integrity Monitor	Simplify regulatory compliance and file integrity monitoring
5	Patch	Distribute and report on operating system updates quickly
6	Comply	Perform compliance checks and vulnerability scans on-demand
7	Protect	Modernize and simplify endpoint protection
8	Threat Response	Detect, investigate, and respond to threats.

Tanium use across various industries –

- 12 of the top 15 U.S. banks
- 6 of the top 10 global retailers
- 4 of the 5 US armed forces branches

SJC

Using Tanium for threat hunting

TLP:AMBER

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

5 MAY 2020

Alert Number

MU-000126-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered**

Commands Used by Ryuk

- Ryuk leverages the iCACLS command to avoid permission issues. The iCACLS command gives the ability to display or change Access Control Lists (ACLs) for files and folders on the file system. Ryuk leverages iCACLS by using the following command:

```
icacls "M:\*" /grant Everyone: F /T /C /Q
```

- Ryuk is commonly seen using the vssadmin command, which administers settings for System Restore. Ryuk uses the vssadmin to delete all shadow copies using the following command:

```
cmd.exe /c "vssadmin.exe Delete Shadows /all /quiet"
```

- Ryuk also uses Windows Management Interface Command (WMIC) to delete shadow copies using the following command:

```
cmd /c "WMIC.exe shadowcopy delete"
```

- Ryuk uses the following commands to disable the built-in Windows Automatic Startup Repair:

```
cmd.exe /c "bcdedit /set {default} recoveryenabled No &bcdedit /set {default}"
cmd.exe /c "bootstatuspolicy ignoreallfailures"
```

Systems that have RDP disabled by default, or Group Policy Object, should monitor for changes in firewall settings via built in commands such as:

```
netsh advfirewall
```

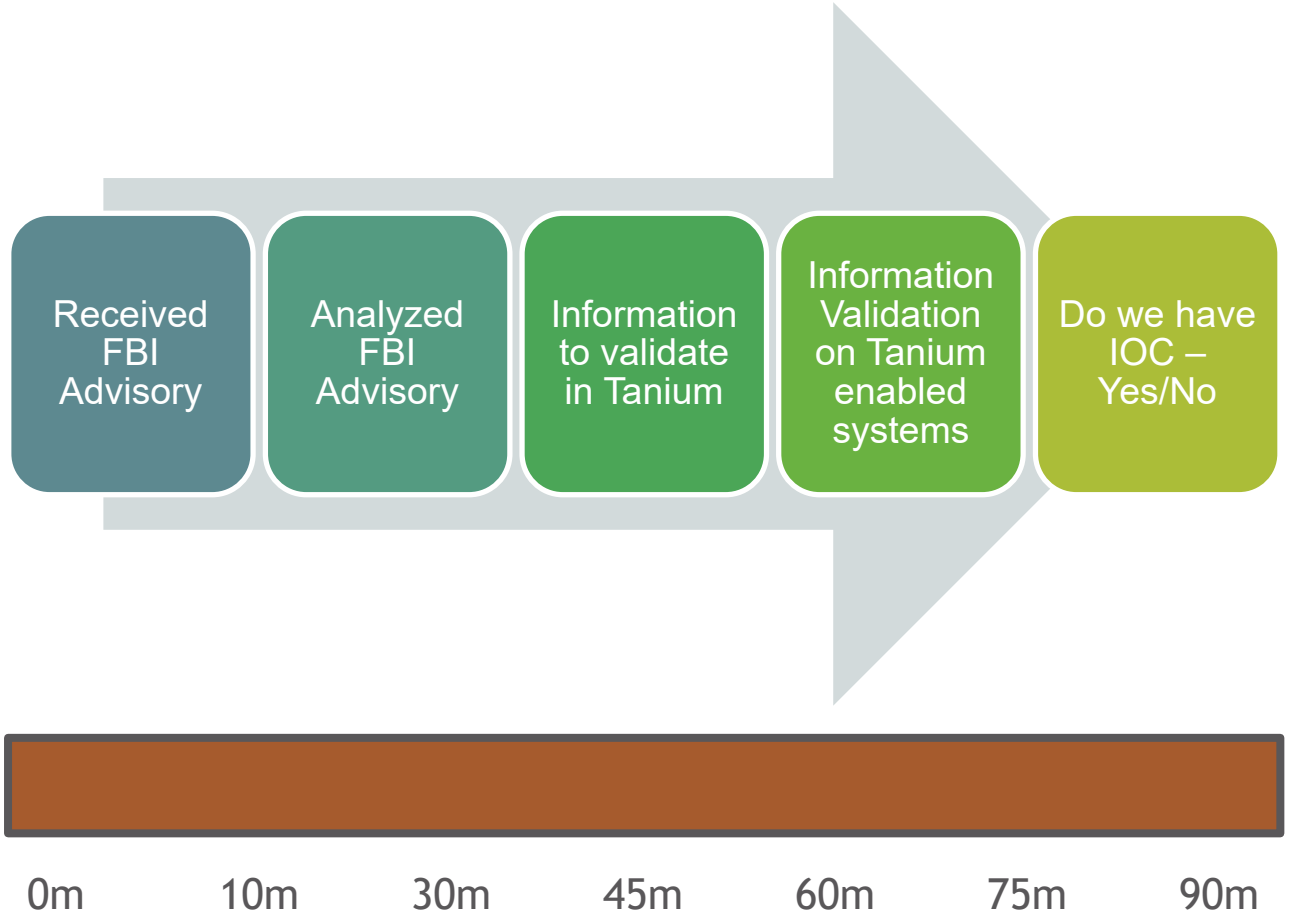
Detect modified registry keys allowing actors access remotely via Terminal Services using the string:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server
```

Network Indicators (not common)	
HTTP GET request:	GET /Lfkgnt5lkgngl3knfl3.php?UI=v9&ID=1140 HTTP/1.1;
User-Agent string:	Microsoft Internet Explorer
IP address:	5.188.231.138

Host Based Indicators		
Mutex:	efkrm4tgkl4ytg4, FakeMutex	
Registry:	Key Name:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
	Value:	svchos
	Date Type:	REG_SZ
File:	Depending on the Windows version, one of the following: C:\users\Public\sys C:\Documents and Settings\Default User\sys	
Ransom note Files:	RyukReadMe.txt" and numerous encrypted filed, which were not renamed, but have the "HERMES" tag followed by an encrypted key at the end of the file (alternatively filed with the .RYK extension	

Validating Indication Of Compromise (IOC) using Tanium



CrowdStrike (NGAV)

Magic Quadrant

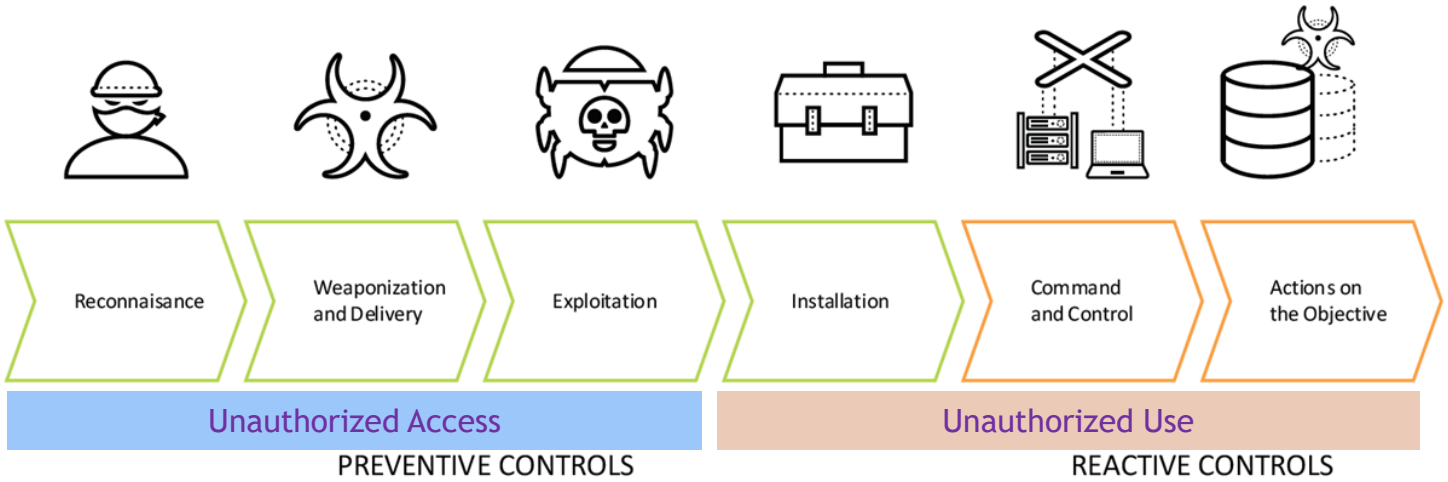
Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (August 2019)

Deployed across the San Joaquin County on workstations and servers.

Raising network security posture

Cyber - Attack Lifecycle

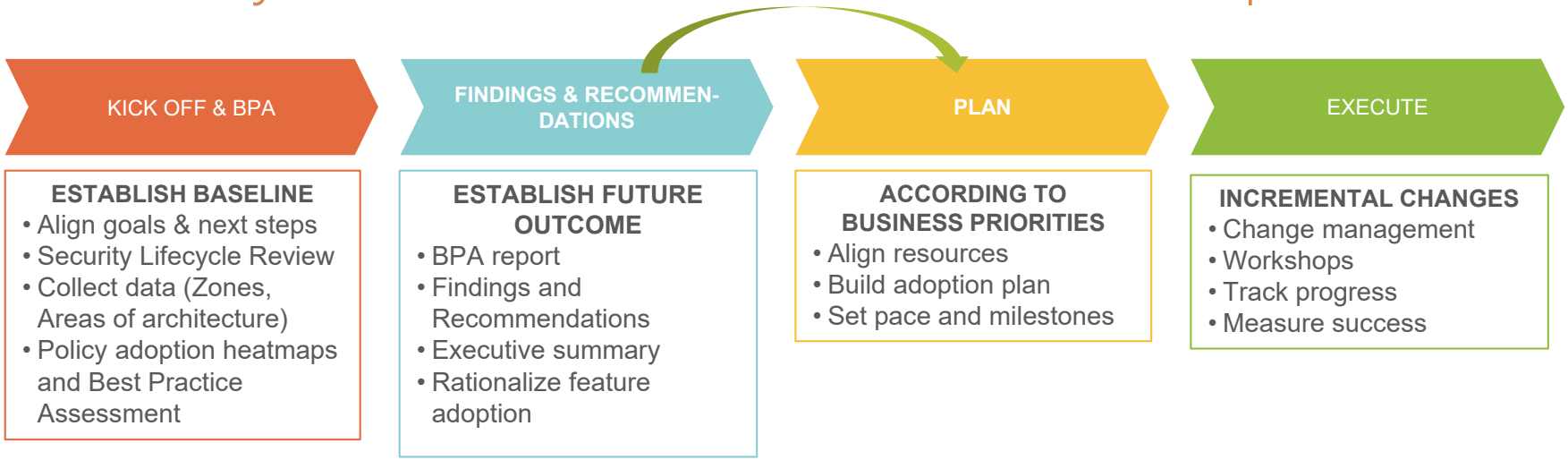


Cyber-attack lifecycle

Cyber Espionage	Actor Group: Deep Panda	Country of Origin: China	21.5M stolen PII records
$350M in Known breach response contracts	$1B class action lawsuit	Leak impacts may last up to 40 yrs	

https://blog.paloaltonetworks.com/2016/02/securing-government-heres-what-we-should-learn-from-2015/

Quarterly Cadence Delivers Consistent Improvement



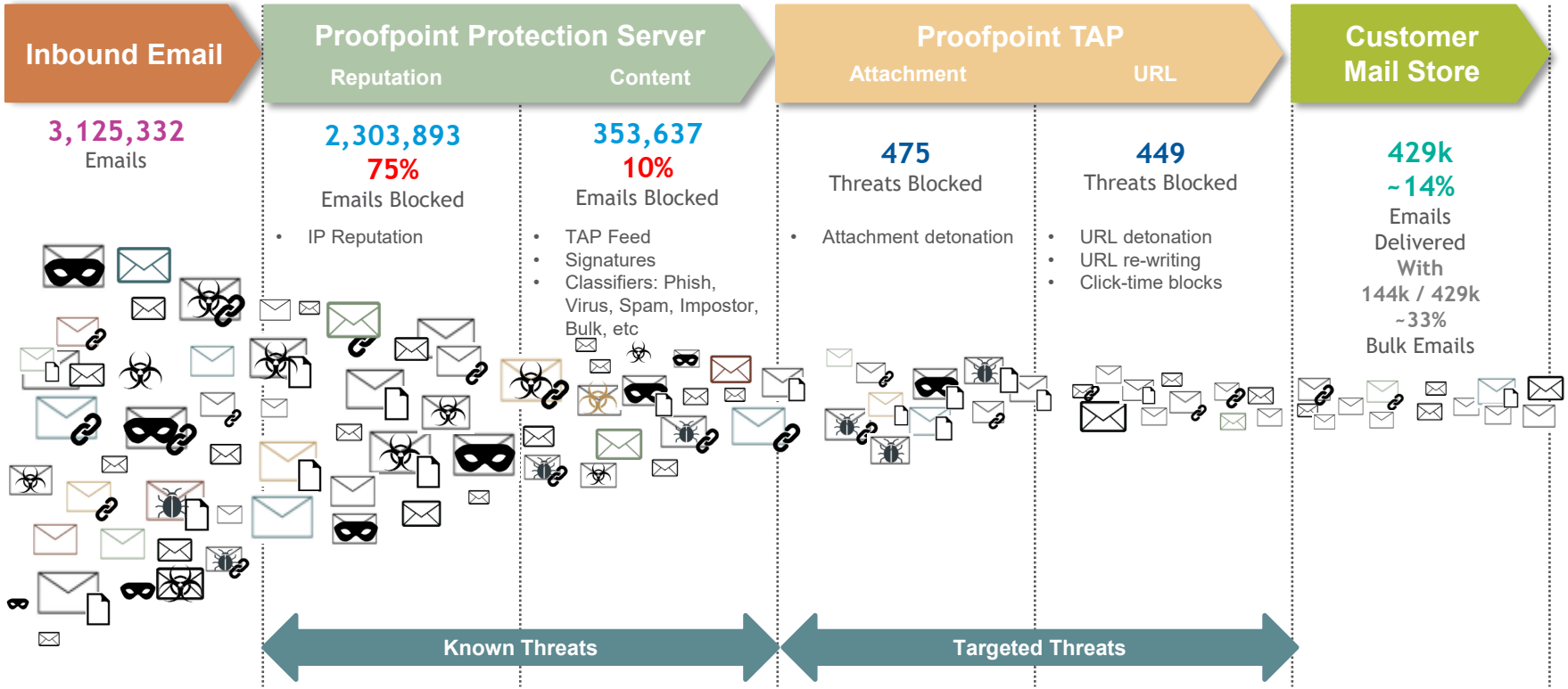
- San Joaquin County
  - Review findings and recommendations.
  - Prioritize how, where and when to improve the security posture.
  - Recurring cadence between SJC Departments/Palo Alto

- San Joaquin County and Palo Alto Networks Account Team
  - Work together to align priorities, POCs and finalize action plan.
  - Set milestones and regular cadence.

Security Awareness (People)

23

Threat protection statistics



Social Engineering

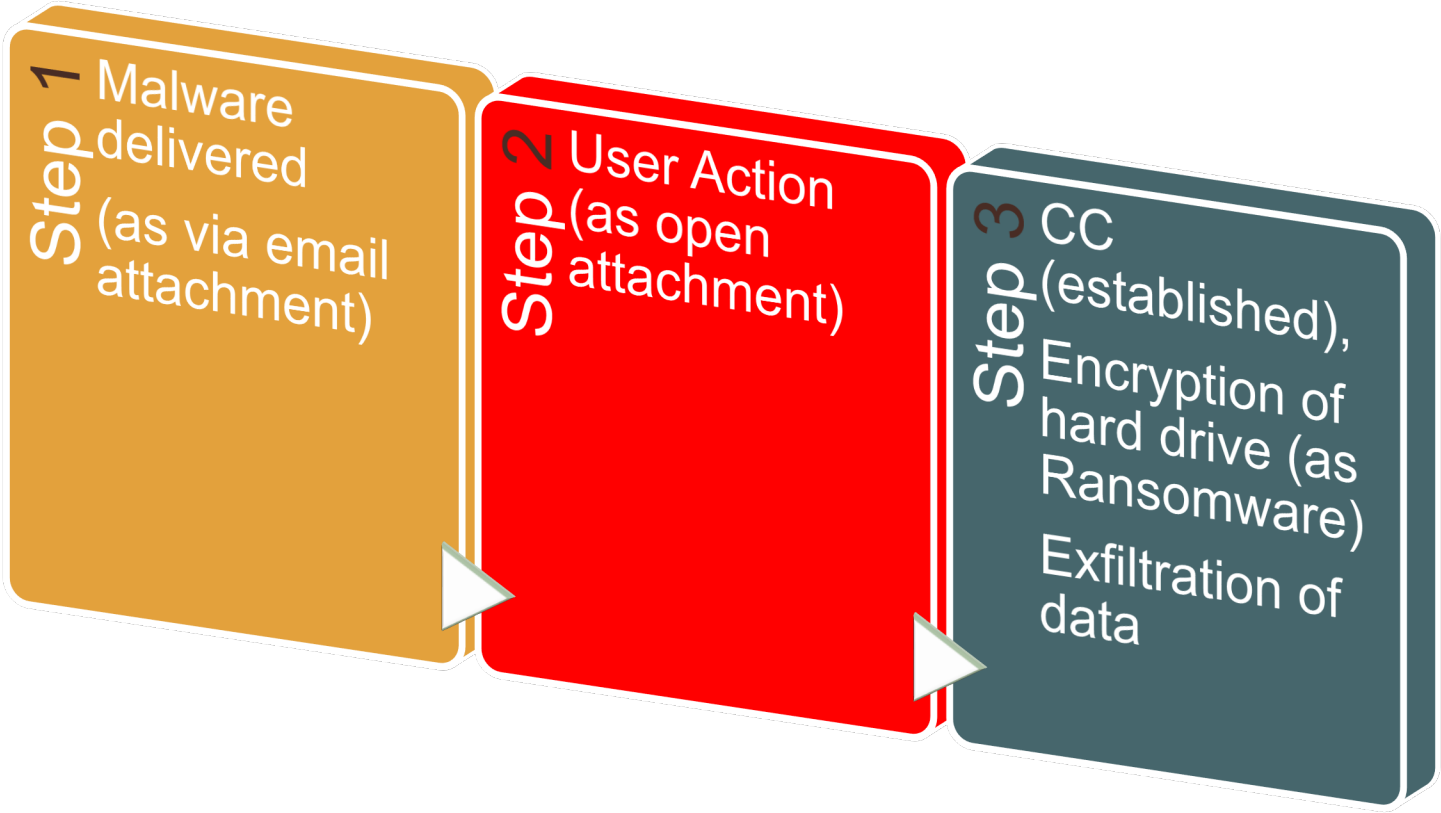
Social engineering is the art of manipulating, influencing or deceiving you in order to gain control over your computer system - by KnowBe4

Humans may be the **greatest security risk** we face in protecting our information from theft and misuse, perhaps even greater than direct hacking of our systems.

https://en.wikibooks.org/wiki/The_Computer_Revolution/What_Is_Phishing

What is Phishing?

It is a fraudulent attempt, usually made via email, to steal sensitive information.



Why do we run regular phishing tests in SJC?

1. *Our goal is to increase security awareness and decrease the number of clicks on malicious emails.*

2. *To establish an Awareness Training that will help us create a "human firewall" which can protect us against malicious emails.*

Cybersecurity Partnership

CDT Security Operations Center (SOC)

- 24/7 shift work
- Staffed by State and Military staff

DHS/CISA (ROV)

Central California Intelligence Center (HSA/ROV/SJCERA)

CISO of CA state / Other counties

SJC

Questions?

Thank You

ccruz@sjgov.org