Cyber Task Forces

- Leverage Federal, State and Local resources
- MOU's signed between agencies
- Full background investigations for TS clearance to work criminal and NatSec
- Provide O/T funding, training and equipment
- Build a deeper pool of skilled cyber investigators

SOUTHERN OREGON HIGH-TECH CRIMES TASK FORCE

OREGON CYBER TASK FORCE

Role of Law Enforcement

- Conduct Complex Network Investigations and successfully prosecute cyber criminals
- Outreach, Education and Training
- Intelligence Sharing
- Forensic expertise and documentation.

Federal Statute: 18 U.S.C. § 1030

Summary of CFAA Offenses and Penalties

Offense	Section	Sentence
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

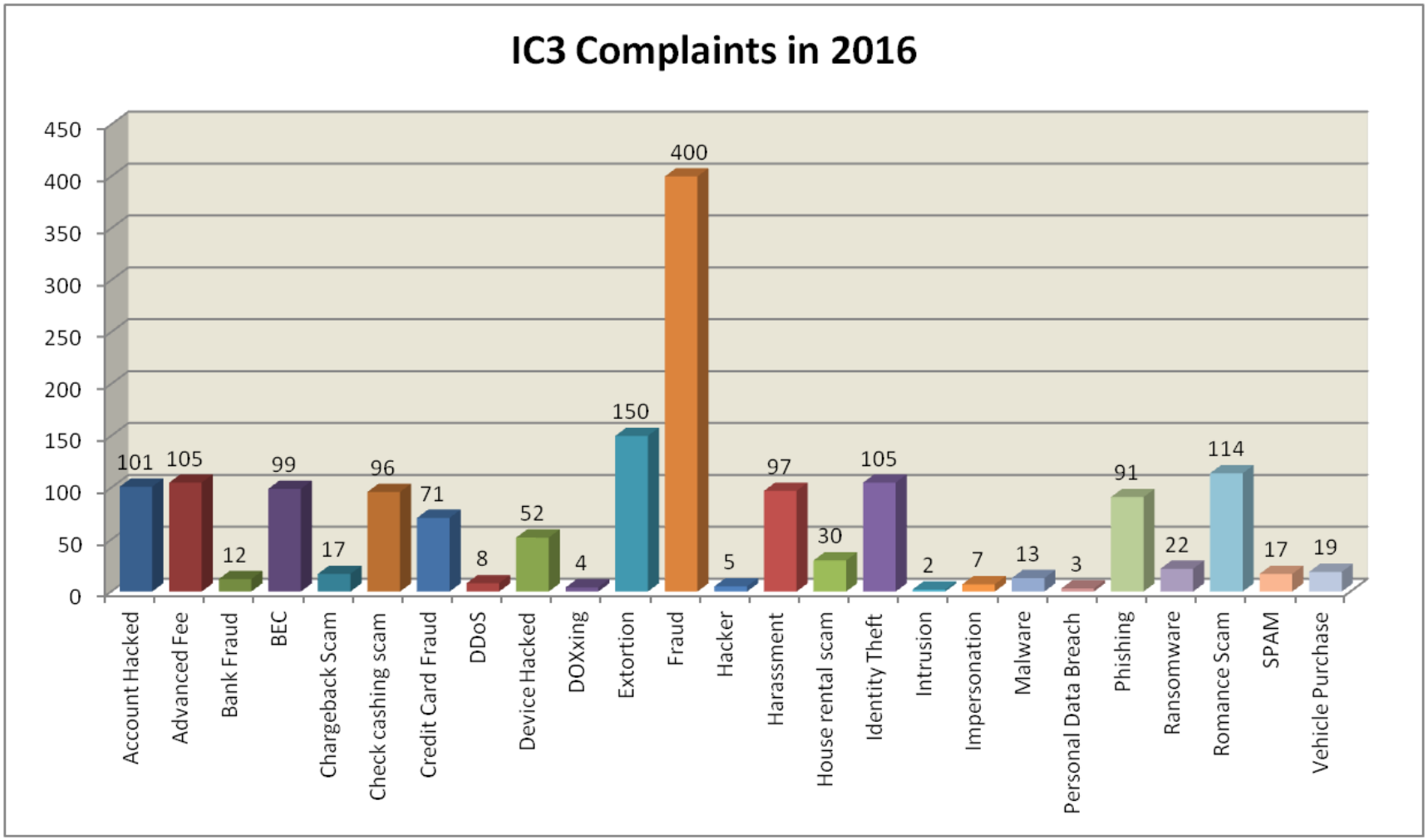
2015 Oregon Revised Statute 164.377

- Any person commits computer crime who **knowingly accesses, attempts to access or uses, or attempts to use**, any computer, computer system, computer network or any part thereof **for the purpose of**:
  - **(a)** Devising or executing any scheme or artifice to defraud;
  - **(b)** Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or
  - **(c)** Committing theft, including, but not limited to, theft of proprietary information or theft of an intimate image.

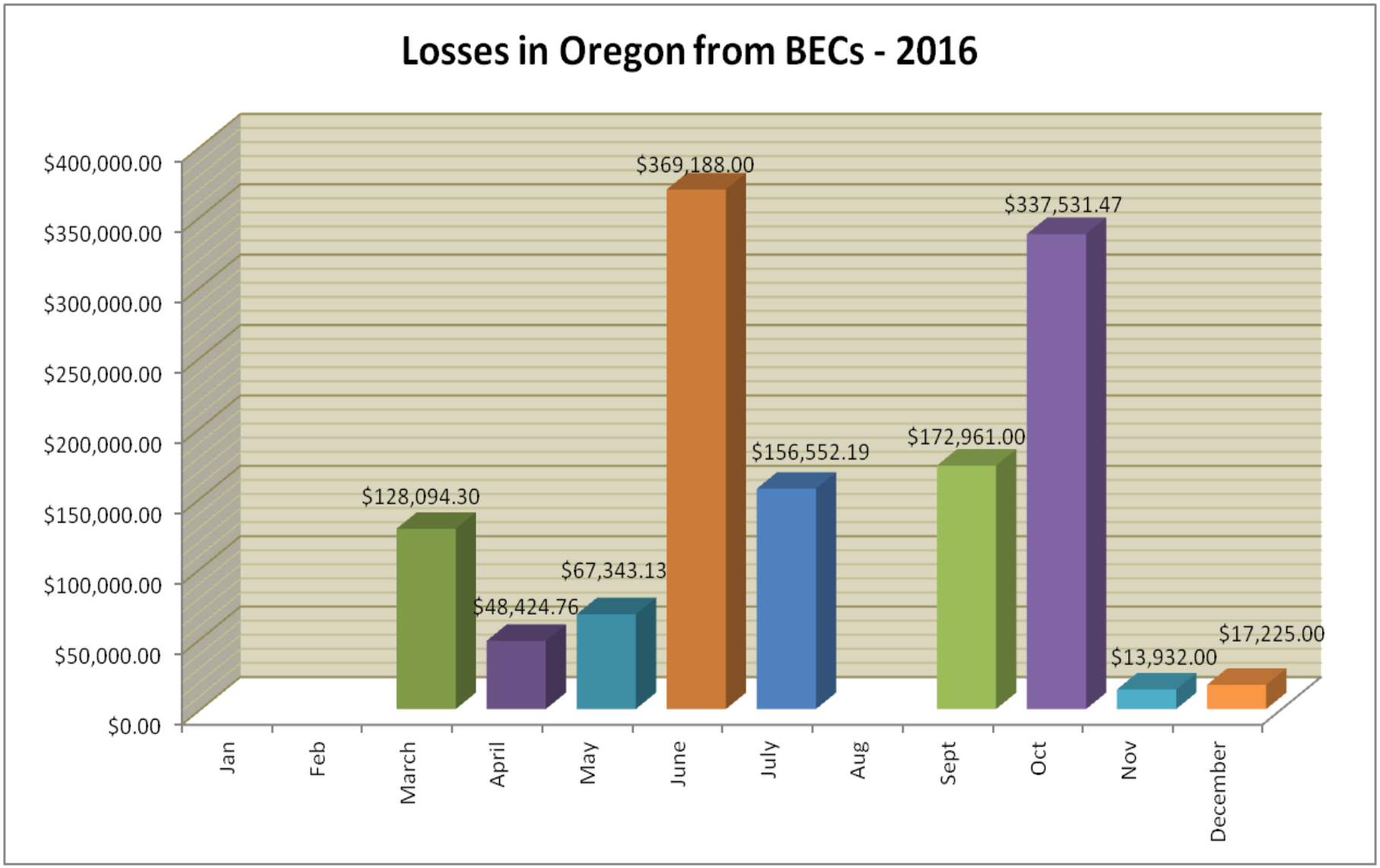
- Any person who knowingly and without authorization **alters, damages or destroys** any computer, computer system, computer network, or any computer software……, commits computer crime.

- Any person who knowingly and without authorization uses, **accesses or attempts to access** any computer, computer system, computer network, or any computer software……, commits computer crime.

OCTF Threat Intelligence Overview



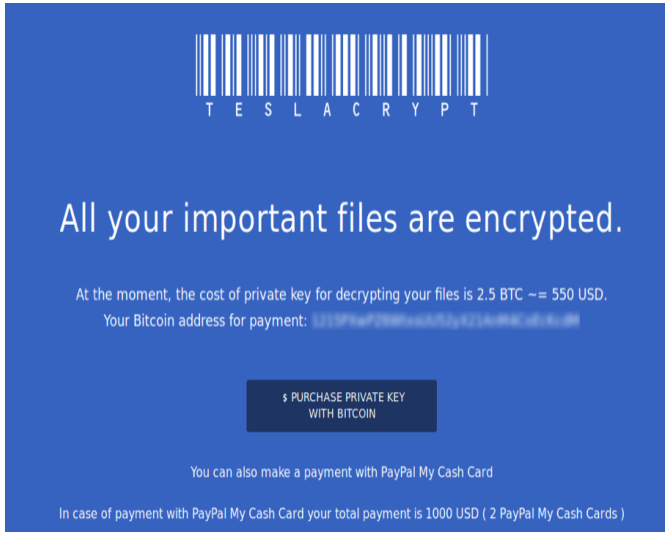
Losses From Business Email Compromise



Ransomware

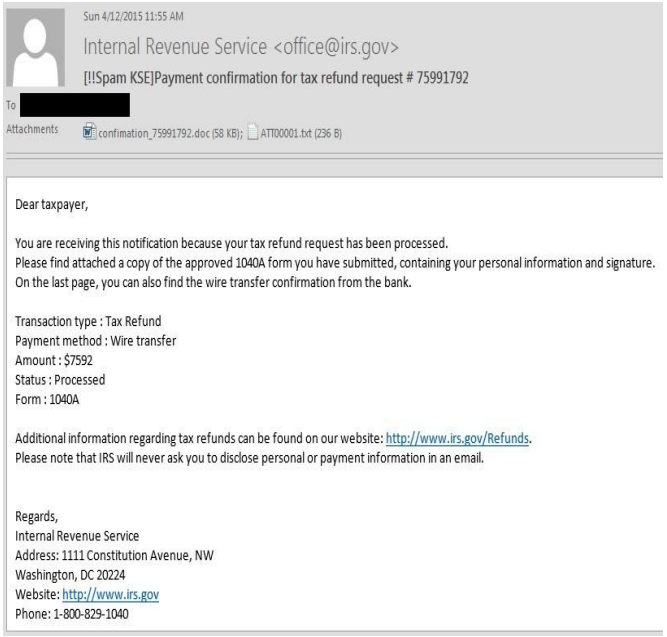
A Short(ish) Primer

- Ransomware is a kind of malware that removes your ability to access your files.
- Recovering your files generally requires you to pay a ransom to get the password or key to unlock the files.



A Short(ish) Primer

- Ransomware infections are most commonly delivered via malicious email or malicious website. Sometimes they combine the two methods.
- Email attacks generally come in the form of a malicious attachment or will attempt to lure victims to malicious websites.
- Malicious websites leverage software vulnerabilities in your browser or browser extensions (Java and Flash)



Sun 4/12/2015 11:55 AM

Internal Revenue Service <office@irs.gov>

[!!Spam KSE]Payment confirmation for tax refund request # 75991792

To [redacted]

Attachments confimation_75991792.doc (58 KB); ATT00001.txt (236 B)

Dear taxpayer,

You are receiving this notification because your tax refund request has been processed.
Please find attached a copy of the approved 1040A form you have submitted, containing your personal information and signature.
On the last page, you can also find the wire transfer confirmation from the bank.

Transaction type : Tax Refund
Payment method : Wire transfer
Amount : $7592
Status : Processed
Form : 1040A

Additional information regarding tax refunds can be found on our website: http://www.irs.gov/Refunds.
Please note that IRS will never ask you to disclose personal or payment information in an email.

Regards,
Internal Revenue Service
Address: 1111 Constitution Avenue, NW
Washington, DC 20224
Website: http://www.irs.gov
Phone: 1-800-829-1040

A Short(ish) Primer

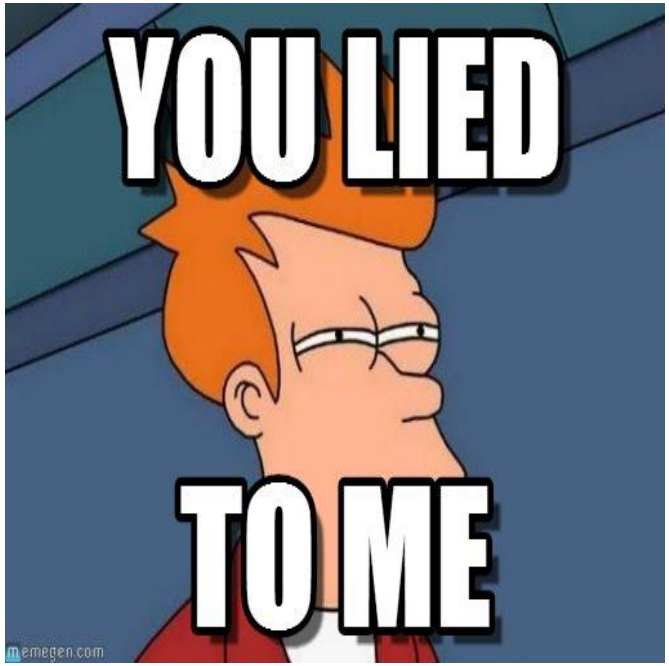
- Recovering your files generally requires you to pay a ransom to get the password or key to unlock the files.
- Payment is usually done via Bitcoin which is trivial to transfer online but hard to trace.

A Short(ish) Primer

- Obtaining and using Bitcoin can be difficult if you are not familiar with it.
- Most Ransomware variants require that payment must be made within a short timeframe.
- Ransomware payments range from $500 - $35,000

A Short(ish) Primer

- Paying the ransom does not guarantee you will get your files back.
- Recently several Ransomware variants have appeared that delete your files instead of encrypting them.



A Short(ish) Primer

- 2016 saw both Mac and Android variants.
- There is a variant that can encrypt your Smart TV.

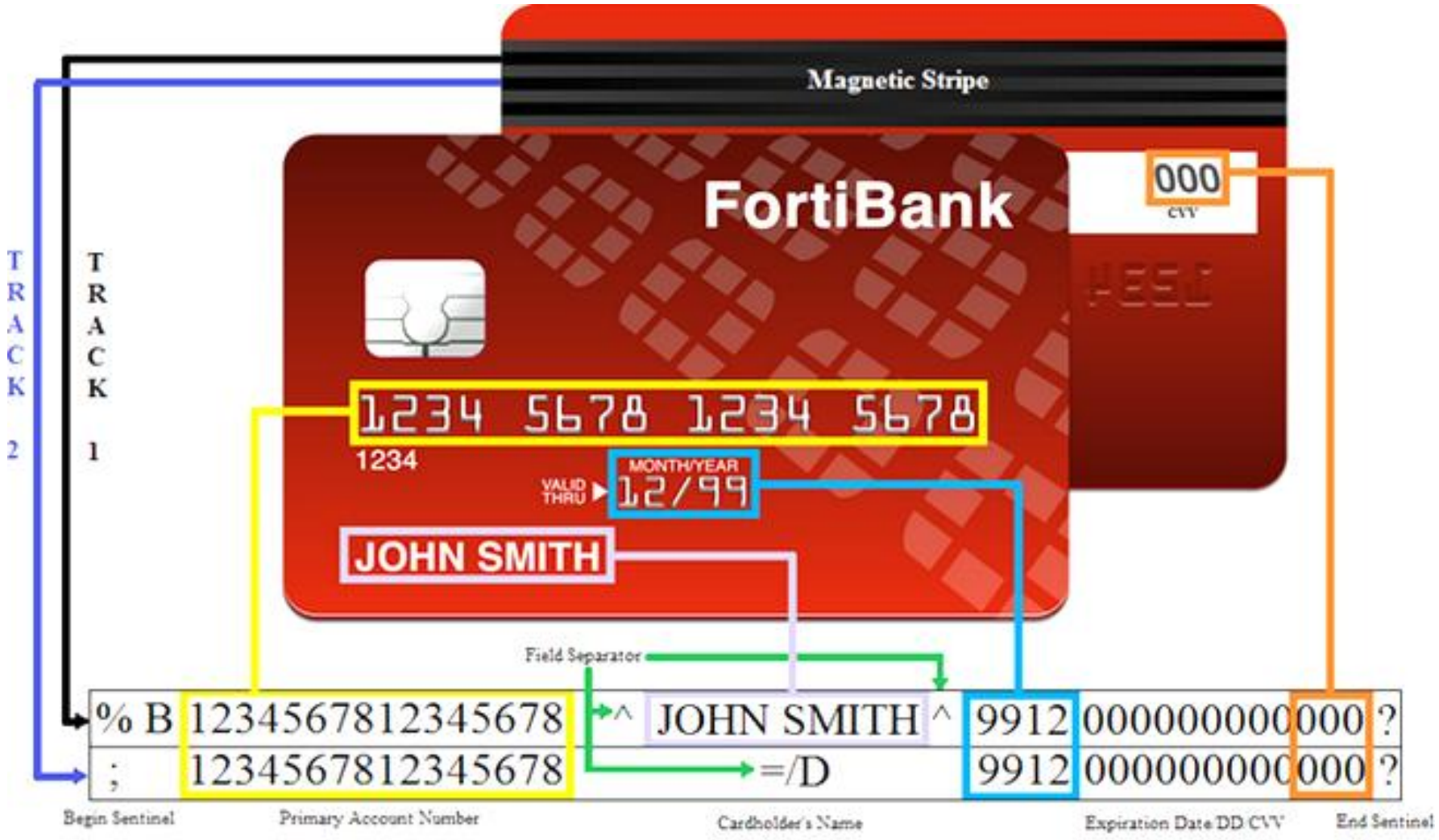
Prevention

- Update your software.
  - Attacks leverage vulnerabilities in software to deliver malicious payloads.
  - “0-Day” or unknown vulnerabilities are very rare. Most attacks use well known vulnerabilities that have patches available.
- Use caution when opening attachments, especially from unknown senders.
- Backups
  - Backups are the only guaranteed way to recover your sensitive files.
  - Backups need to be stored on separate systems that cannot be directly accessed by victim computers.

PoS Malware: In a nutshell

- Typical PoS intrusion –
  - RAM-scraping malware is installed on POS
  - Data is securely encrypted in STORAGE and TRANSIT.
  - BUT…… When the data is actively in use by the terminal, at the point the transaction is taking place, the processing in RAM in done in clear text.
  - Malware captures the clear text from RAM. Stores for later exfiltration by hackers.
    - Names, Account #'s, Expiration dates, CVV are exposed!

PoS Malware: In a nutshell



How PoS Malware Attack Occur

Trend Micro researchers noted five main POS attack themes:

1) **Phishing and social engineering:**

   – When hackers takes advantage of unsuspecting computer users, worming their way into company networks via legitimate-looking emails or surprising convincing phone calls.

How PoS Malware Attack Occur

2) **Employee on the inside:**

- An employee who willingly serves as an ingress point for malicious activity. This can result in both the installation of skimmers or PoS Malware.

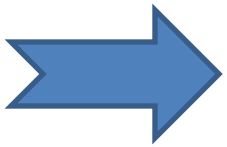
3) **Exploitation:**

- When malware infiltrates a system that hasn't been updated with the latest security patch.

How PoS Malware Attack Occur

4) **Non-compliance with PCI DSS guidelines:**

- Failure to abide by the industry's regulations concerning security, which evolved last year to include EMV chip usage.

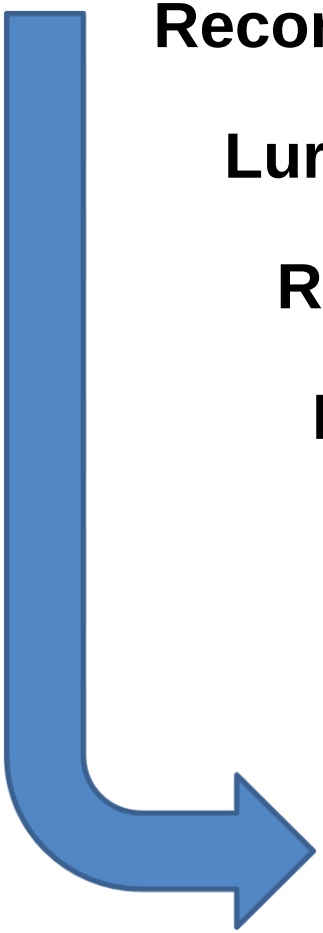


How PoS Malware Attack Occur

5) Sophisticated targeted attacks:

– When hackers get on the network using advanced techniques.

PoS Malware Stages (POSRAM)



Recon: *Type of PoS vendor, system architecture*

Lure: *Spear phishing email or web attack*

Redirect: *Redirect victim to attacker's website*

Exploit Kit: *Run exploit kit on victim's computer*

Dropper File: *Install custom malware*

Call Home: *Capture and send CC data offsite*

Data Theft: *Cyber criminals sell or use PII*

EMV Chips

- EMV smartcards –
  - Designed to reduce fraud occurring in magnetic stripe.
  - Face-to-face transaction protection.
  - Uses integrated-circuit (IC) based cards, use keys to generate authentication and authorization data (tokens).
  - The dynamic code gets reorganized with each purchase..

- However, EMV alone does not protect
  - The confidentiality of or inappropriate access to sensitive data and/or cardholder data.

PoS Malware Trends

- Attack the PoS Vendor:
  - In 2016 criminals targeted the support portal for MICROS PoS terminals allowing them to steal customer usernames and passwords.

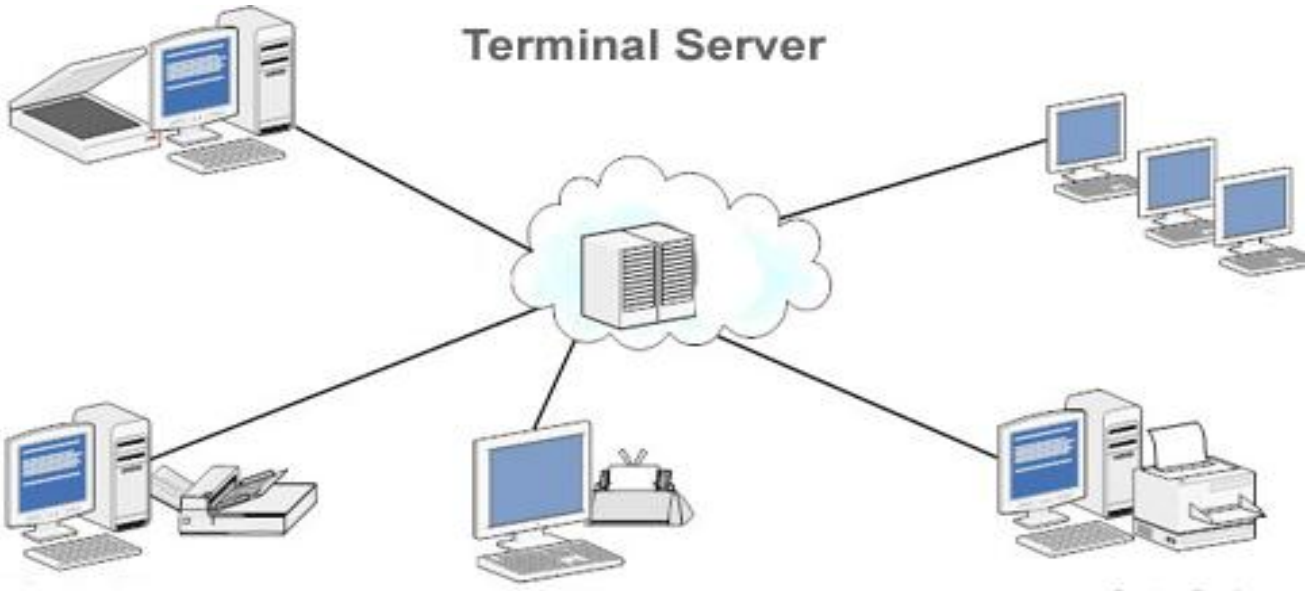
- PunkeyPOS / POSCardReader:
  - In 2016 hackers took advantage of weak **user logins** and obtained valid account credentials for LogMeIn, a program retailers use to manage remote systems.

PoS Malware Trends

- Multigrain:
  - PoS Malware that uses DNS Tunnelling (Encapsulating) in order to exfiltrate stolen information in what appears to be routine DNS queries.
  - In 2016 this PoS malware was used to infect hundreds of restaurants in the United States.

PoS Malware Trends

- In late 2016 another wave of attacks occurred across multiple industry sectors
- Common among victims was a Terminal Server facing the Internet.
  - A Terminal Server is a server or network device that enables multiple client systems (terminals) to connect to a LAN network without using a modem or a network interface card (NIC).



Ways to Reduce the Risk

- Train employees to detect social engineering and phishing attempts. Attackers need to know the target's OS platforms, will also seek to determine network topology and architecture.

- Know how your system works, conduct a baseline analysis of network communications for internal, external and remote office connections. This can help identify outliers in outbound and inbound communications.

- Consider Data Loss Prevention (DLP) solutions, specifically design your data security system to protect highly sensitive information, such as credit cards and social security numbers. Focus on your most important assets first.

- Ensure only authorized applications run within your POS environment (whitelisting).

Ways to Reduce the Risk

- Fully deploy EMV (chip-card) enabled POS terminals
- Provide end-to-end or point-to-point encryption (E3 or P2PE) hardware-encrypting data, starting from the POI (Point of Interaction) device. This can be a costly, but is also highly effective.
- Keep an eye on your employees and remain alert for suspicious behavior to identify potential insider threats. The number of breaches due to employee negligence and error continue to increase.
- This vigilance should extend to 3rd-Party vendors with whom you may out-source some of your business support functions.

Ways to Reduce the Risk

- Or just go back to this!

Oregon Reporting Requirements

- https://justice.oregon.gov/consumer/databreach
- Oregon Revised Statutes 646A.600-646A.628

DDoS Extortion

: FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

Your will be DDoS-ed starting Tuesday (April 26) if you don't pay protection fee - 20 Bitcoins @ 1QF$k1Z$xrPntSMjcpSyjD3iTQxX

When we say all, we mean all - users will not be able to access sites host with you at all.

If you don't pay by Tuesday, attack will start, yours network going down permanently price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. And we pass CloudFlare and others remote protections!

So, no cheap protection will help.

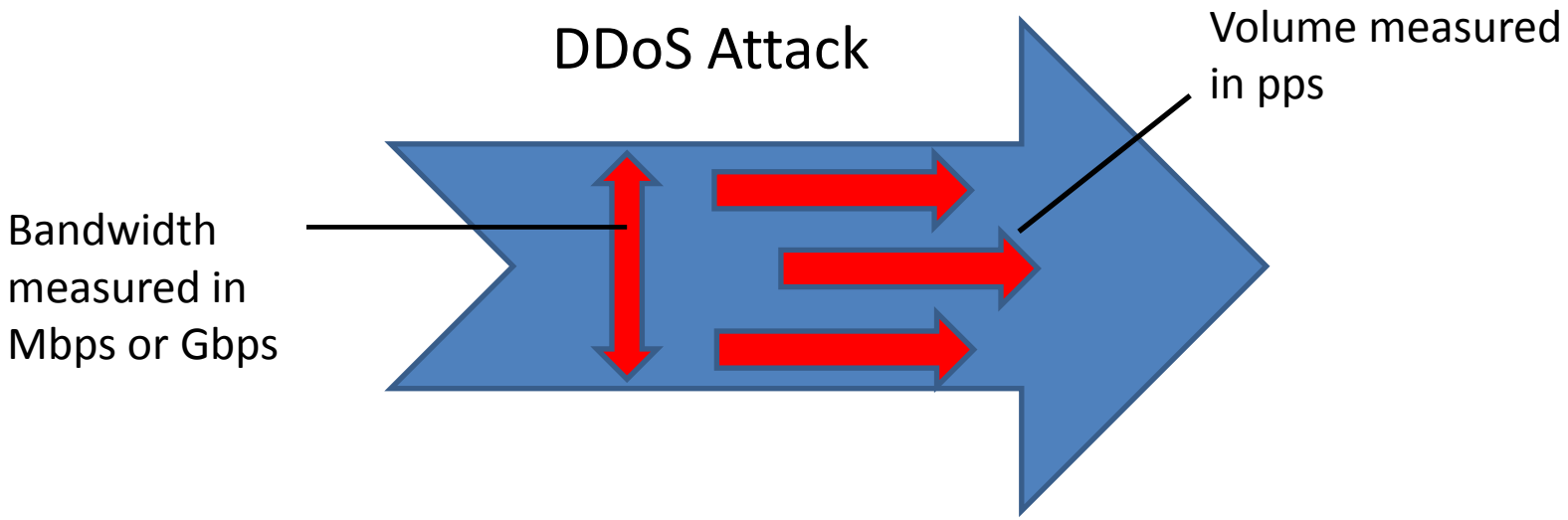
Prevent it all with just 20 BTC @ 1QF$k1Z$xrPntSMjcpSyjD3iTQxX

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

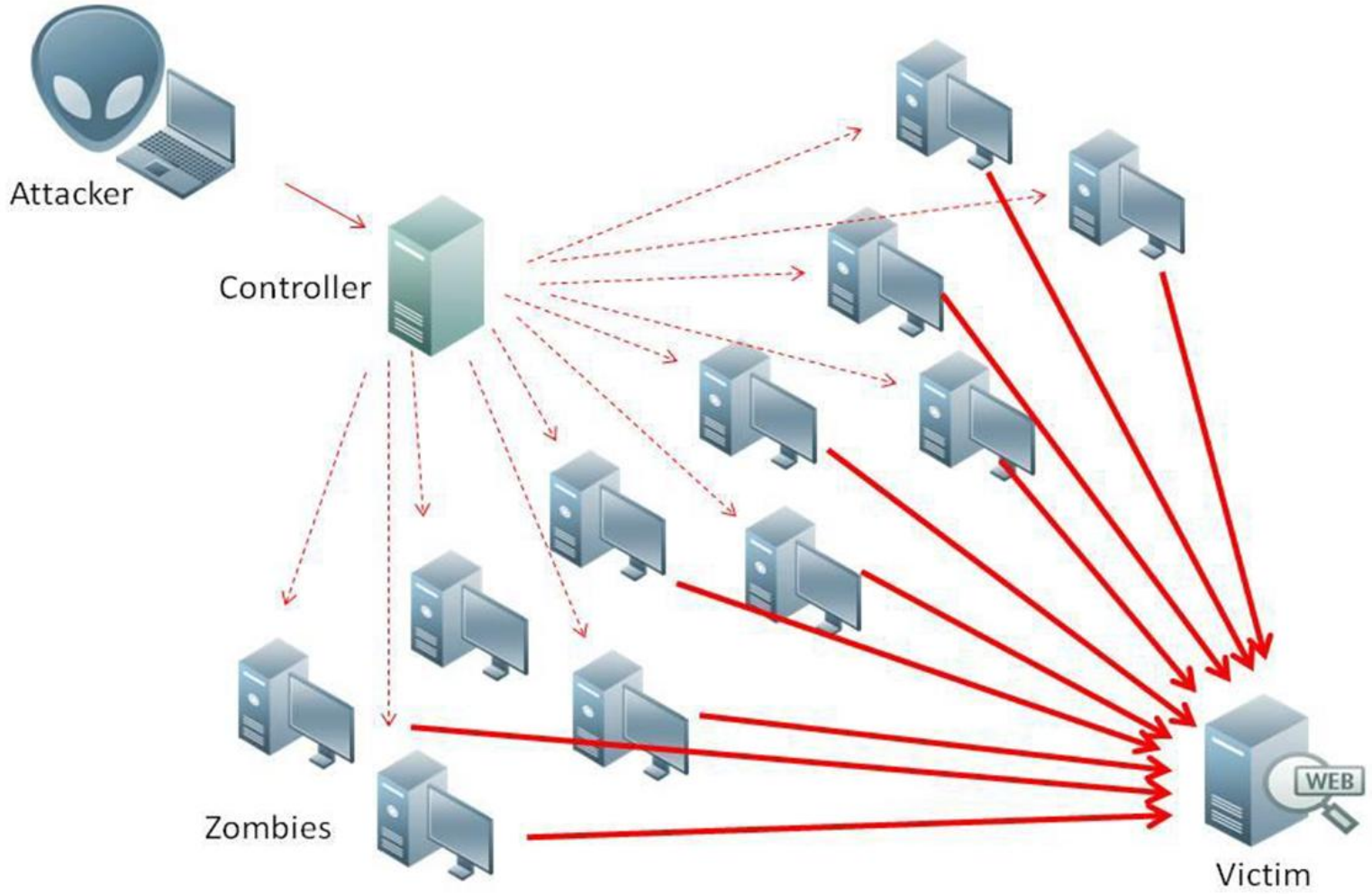
Bitcoin is anonymous, nobody will ever know you cooperated.

DDoS 101

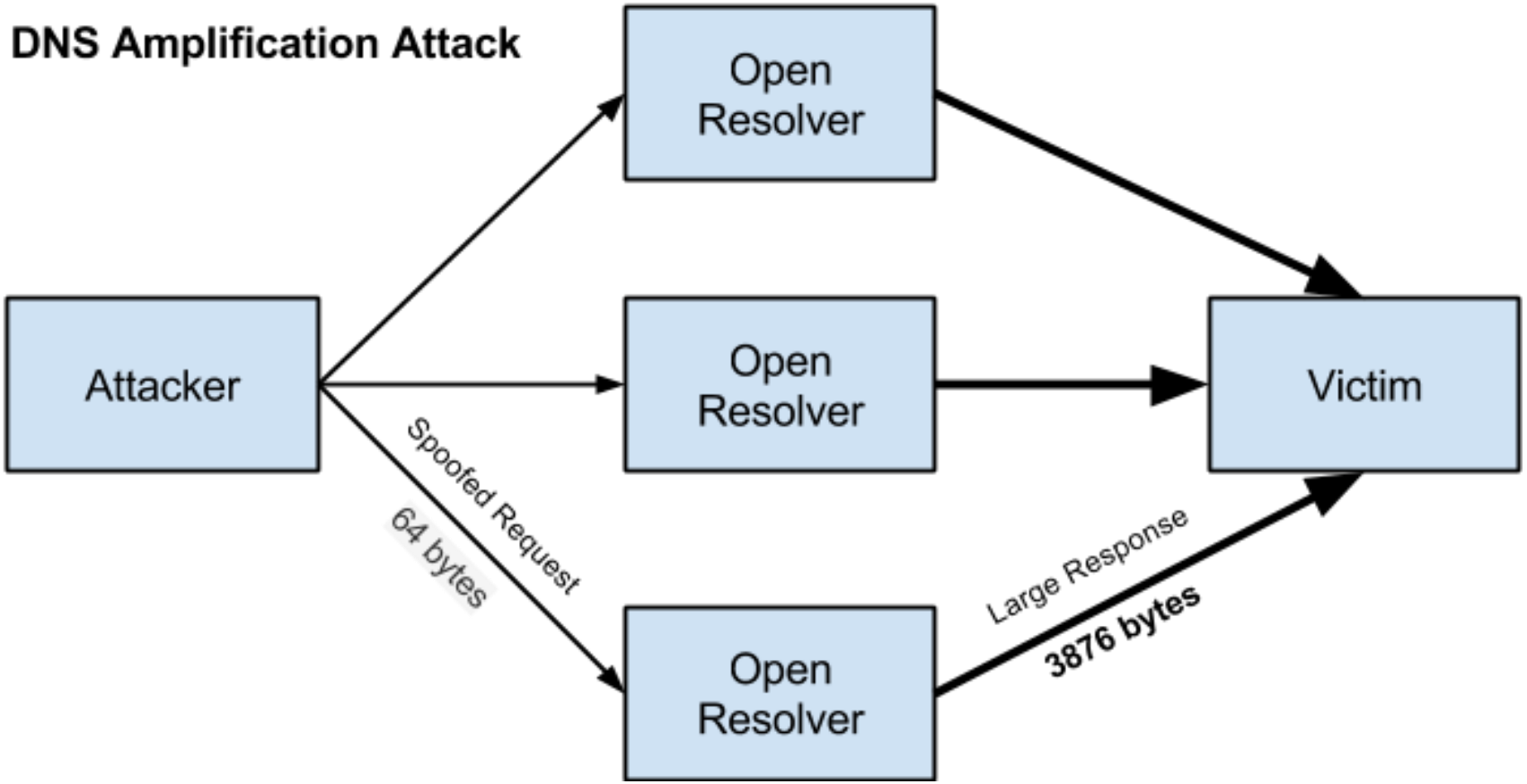
The bandwidth is calculated in megabits or gigabits per second (Mbps or Gbps) and volume is calculated in packets per second (pps). A high number in either of these attributes can lead to overloading of a targeted server or application, leaving it unable to respond to legitimate requests.



Traditional DDoS Using a Botnet



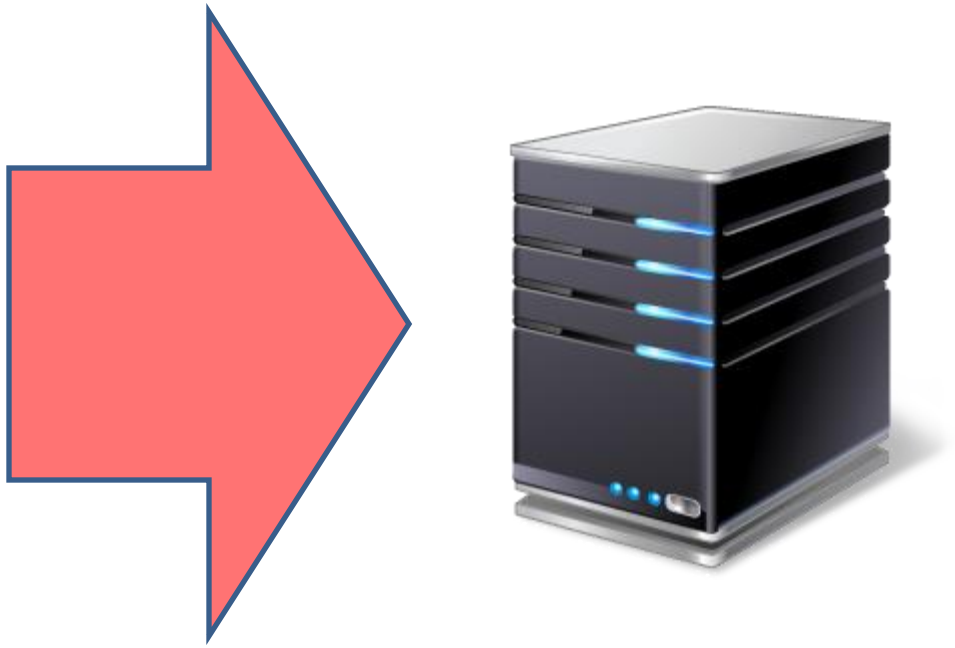
DDoS Using DNS Amplification Attack



DDoS Trends

- A recent attack against Krebs Security was notable for not only its size (600-700Gbps), but also its depth and complexity.

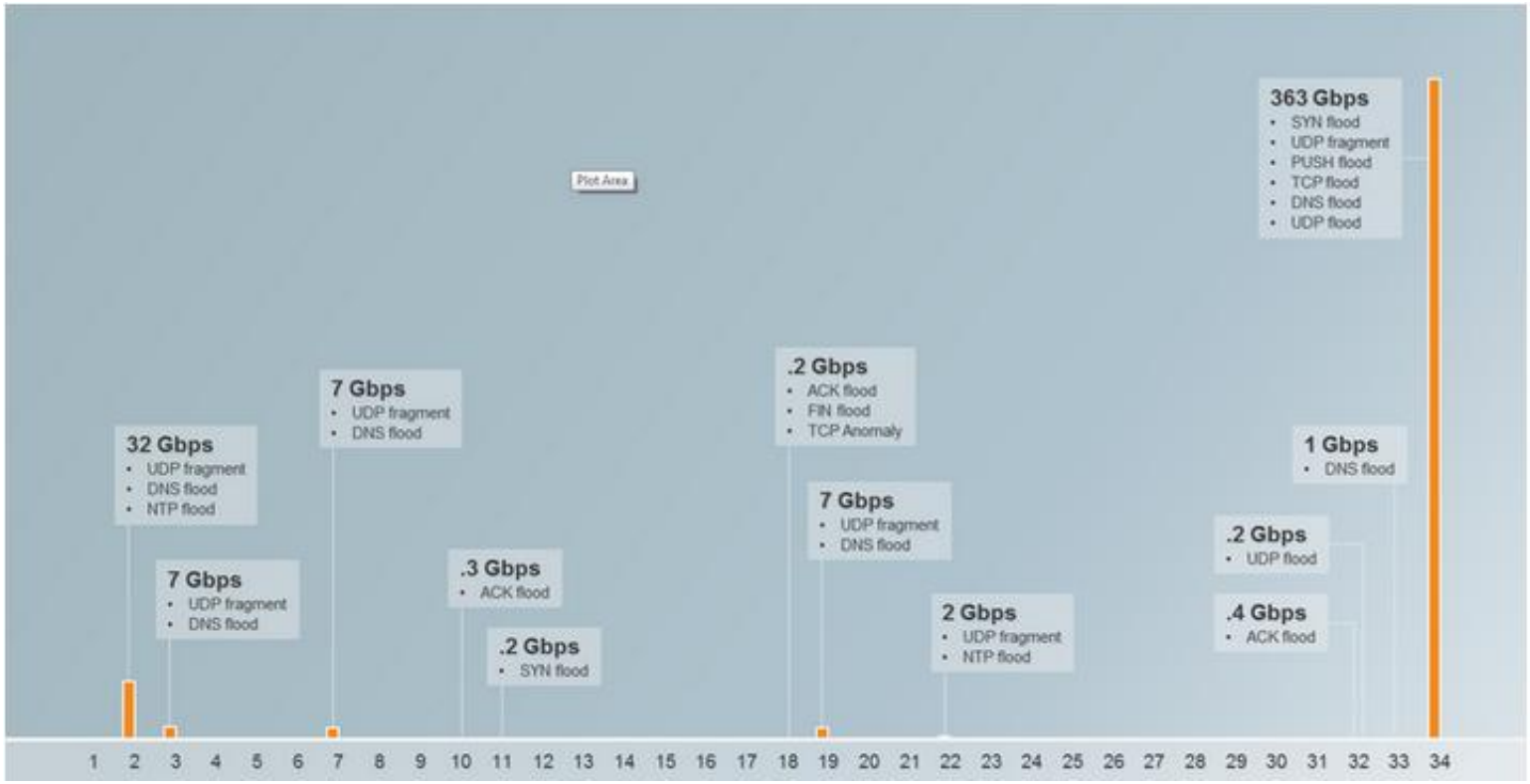
- SYN Flooding
- UDP Flooding
- VSE Query Flooding
- GRE Flooding
- ACK Flooding
- HTTP GET
- HTTP POST
- HTTP HEAD



Reference: John Dunn, 09/26/16, ComputerWorldUK

DDoS Trends

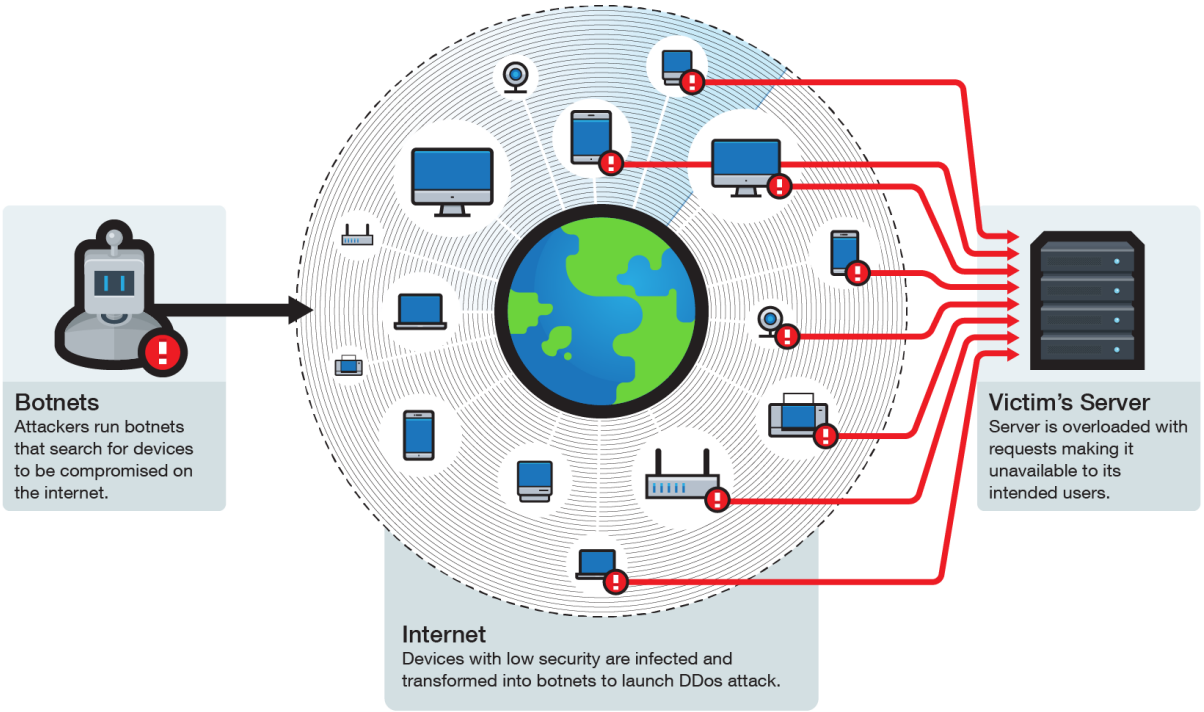
Based upon the latest massive DDoS attacks and the experiences of victim companies, criminals may be moving towards campaigns consisting of repeated attacks which bundle extreme size with the use of multiple attack types.



Reference: John Dunn, 07/21/16, ComputerWorldUK

DDoS Trends

Internet of Things (IoT) – The Mirai Botnet-based attack against Dyn Managed DNS Infrastructure likely involved over 100,000 malicious endpoints.



Reference: Dyn statement 10/26/2016

Points to Consider in a DDoS Extortion

- Payment of the ransom does not mean a victim will not be attacked or ransomed again;
- Not all groups can follow through on their threat, in fact many cannot;
- Inform your upstream provider and data center;
- Extortion emails will usually be sent to a publicly accessible email listed on a company webpage;
- Conduct research, consult with experts and law enforcement to determine if the threat is credible.

Contacting Law Enforcement

- Contact law enforcement if you believe a crime is being committed.
- Be prepared to provide as much information as possible:
  - Start/End of attack, is it repeated, patterns?
  - Were there communications from the attacker?
  - Detailed traffic information, type, source, IP's, port numbers, packet rate, bandwidth
  - Is the attack targeting a particular virtual host or domain?
  - ID changes observed in the attack over time
  - Provide an impact assessment

Business Email Compromise

A Short Primer

- BEC (Business Email Compromise) are scams that compromise business accounts in order to transfer money out of victim's accounts.
  - Also known as CEO Fraud
- Considered one of the biggest threats to organizations today.
- Attackers use social engineering techniques combined with extensive research to spoof scam organizations into transferring money to the criminals.

Red Flags

- New Requests
- Non-Standard Requests
- Abnormal Times
- Large Amounts
- Requests for Secrecy
- Requestor is sending from a non-standard account
- Requestor is on vacation so can’t do it themselves

Prevention

- Document and train staff on Wire Transfer policies and procedures.
- Consider requiring verbal authorization in addition to email for large Wire Transfer amounts, especially on one-time or new transfers.
- Tighten SPAM filters.
- Update software frequently.
- TWO FACTOR AUTHORIZATION

The Insider Threat

- A malicious insider is defined as a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access.

- The insider threat can also be a current or former employee, contractor, or business partner who unwittingly, or through negligence, negatively affects the confidentiality, integrity, or availability of the organization's information or information systems.

Insider Threat Study

Carnegie Mellon University (CERT) Insider Threat Center has analyzed over 600 cases of crimes committed against organizations by insiders. One of their key findings was that insiders who steal intellectual property (IP) stole at least some of their organization's IP within 30 days of their termination.

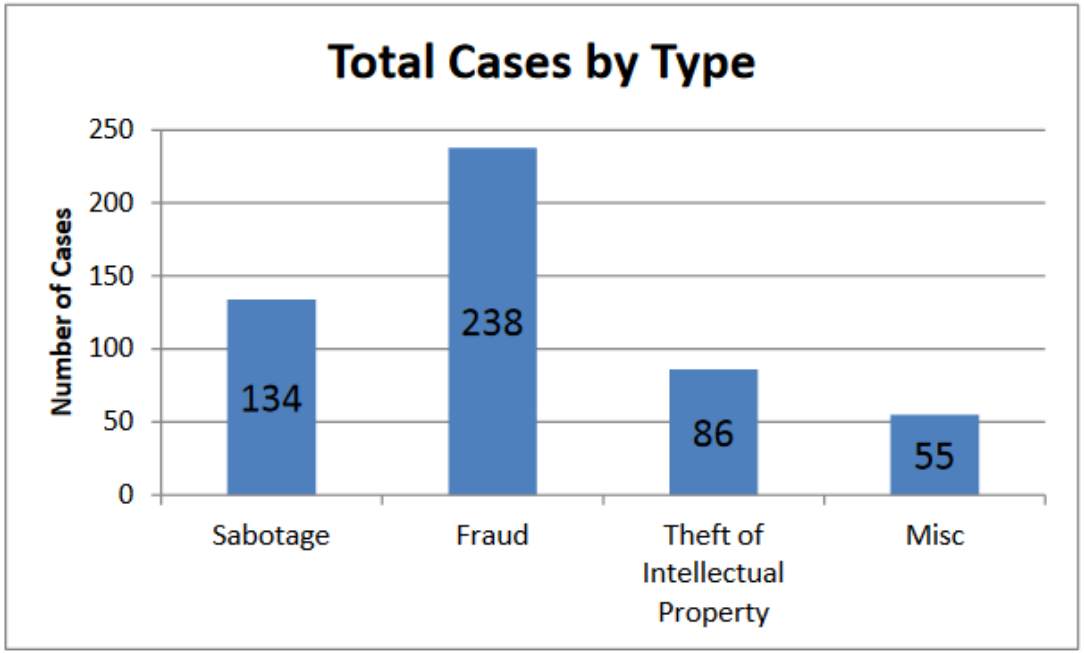


Figure 1: Number of Cases in the CERT Insider Threat Database by High-Level Category (Excluding National Security Espionage Cases)

Insider Threat

- Personal Factors
  - A variety of motives or personal situations may increase the likelihood an individual may engage in criminal activity against their employer.

- Organizational Factors
  - Organizational situations may increase the ease for thievery

- Behavioral Indicators
  - Some behaviors may be a clue that an employee is “spying” and/or methodically stealing from an organization

Personal Factors

- Greed or Financial Need
- Anger or Revenge
- Compulsive and Destructive Behavior
- Ego/Self-Image
- Family Problems
- Ingratiation
- Adventure/Thrill
- Problems at Work

Organizational Factors

- The ease with which someone might exit the facility with proprietary or other protected company information;
- Proprietary or protected information is not labeled as such, or is labeled incorrectly;
- Undefined or poorly written security policies, or no policy at all;

Organizational Factors

- Employees are not trained on how to protect proprietary or sensitive information;
- Time pressure; employees are rushed and may not recognize the consequences of their actions.
- Access privileges are provided to those who do not need it;

Behavioral Indicators

- Interest in matters outside the scope of their duties;
- Remotely accesses the computer network while on vacation, sick leave or other odd times

Behavioral Indicators

- Regularly disregards company computer security polices related to installing personal software or hardware, accessing restricted websites or downloading confidential/sensitive data.

- Engages in suspicious personal contacts, i.e. with competitors, business partners or other individuals;

- Overwhelmed by life crises or career disappointments;

Behavioral Indicators

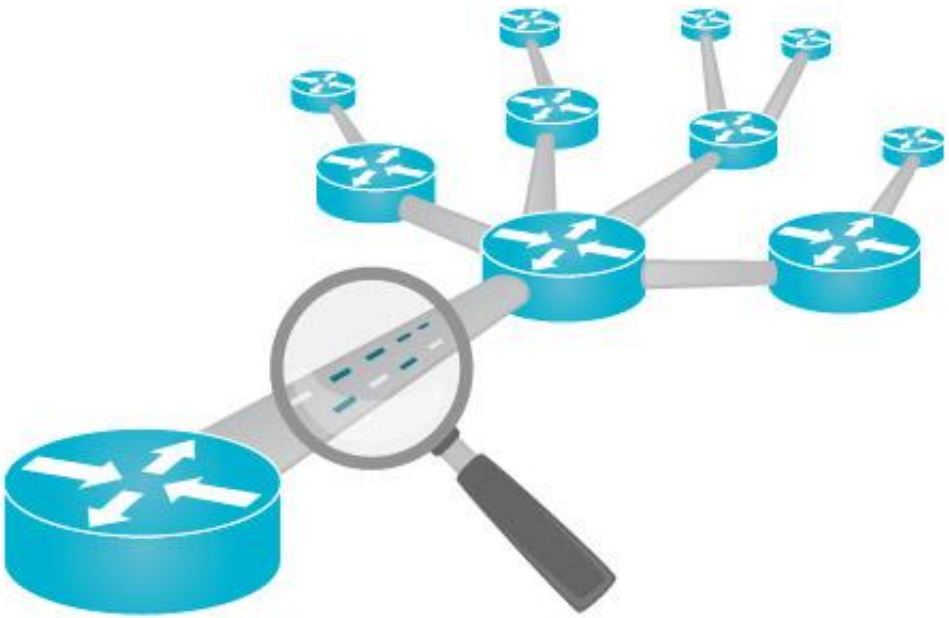
- Works odd hours without authorization;
- Unexplained affluence;
- Concerns they are being investigated, leave traps to detect searches of their home and work areas.

What You Can Do

- Educate and regularly train employees on security and other protocols, have a clear security policy;
- Ensure security, (to include computer network security) personnel have the tools they need;
- Ensure that proprietary or sensitive information is adequately protected;

What You Can Do

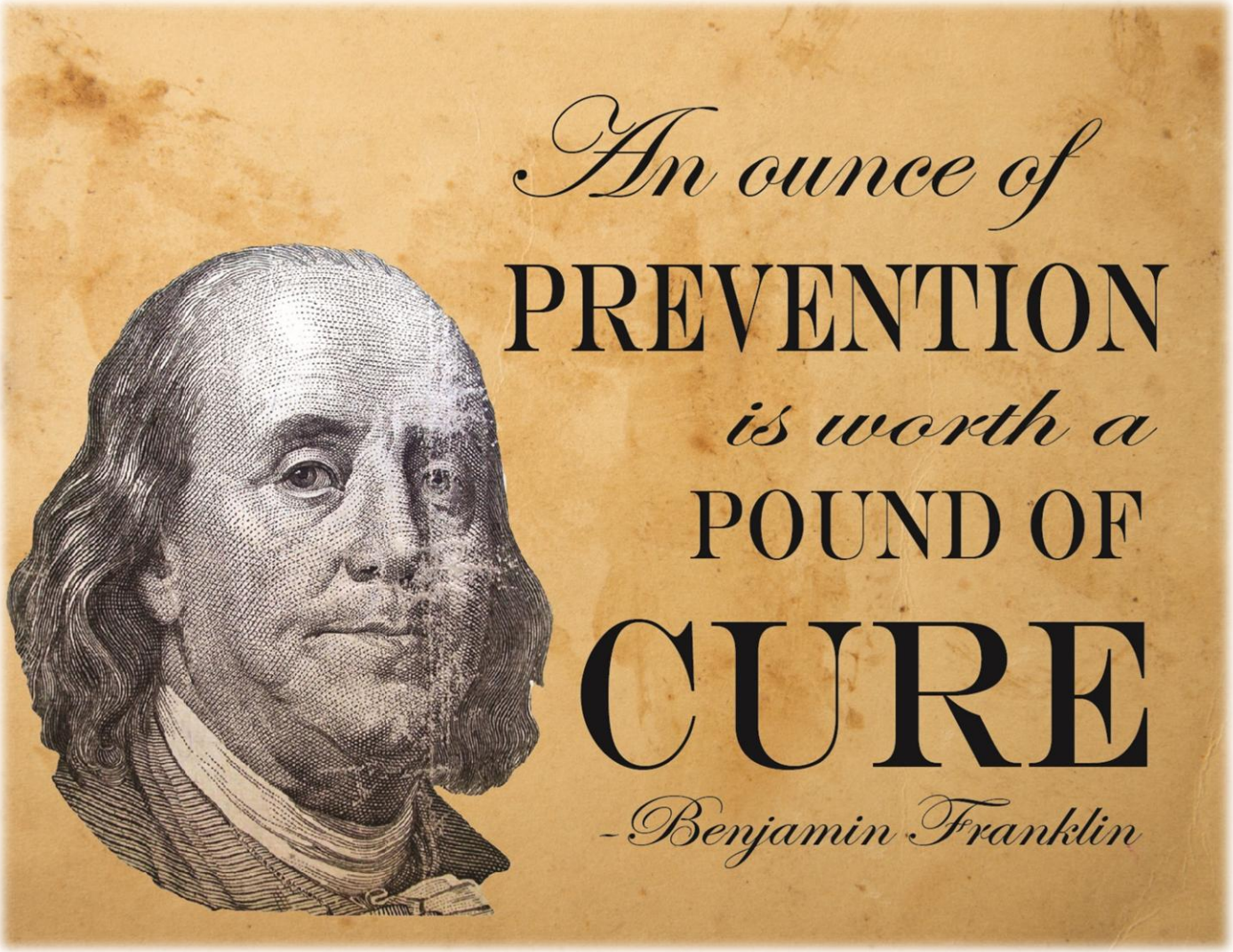
- Provide non-threatening, convenient ways for employees to report suspicions;
- Routinely monitor computer networks for suspicious activity;



What You Can Do

- Hire Good People
  - Use appropriate screening processes and criteria to select and hire new employees;

Preparation and Prevention



Steps to Take Before an Incident Occurs

- Identify Your “Crown Jewels”, that which you simply cannot afford to lose;
- Have an actionable plan in place;

- Have appropriate Technology and Services in place;
- Ensure legal counsel is familiar with technology and Cyber Incident Management to reduce response time during an incident;

Steps to Take Before an Incident Occurs

- Ensure organization policies align with your incident response plan;
- Control Access;
- Establish relationships with Cyber Information Sharing Organizations (ISACs);
- Engage with law enforcement;

Authorization for Network Monitoring

- Have Appropriate Authorization in Place to Permit Network Monitoring;
- Real-time monitoring of an organization's own network is typically lawful if prior consent for such monitoring is obtained from network users;
  - Computer User Agreements
  - Workplace Policies and Personnel Training, written acknowledgement of receiving such training should be obtained
  - Network Banners

Network Banners

In other cases, network providers may wish to establish a more limited policy. Here are three examples of relatively narrow banners that will generate consent to access in some situations but not others.

This computer network belongs to the Grommie Corporation and may be used only by Grommie Corporation employees and only for work-related purposes. The Grommie Corporation reserves the right to monitor use of this network to ensure network security and to respond to specific allegations of employee misuse. Use of this network shall constitute consent to monitoring for such purposes. In addition, the Grommie Corporation reserves the right to consent to a valid law enforcement request to search the network for evidence of a crime stored within the network.

Network Banners

Warning: Patrons of the Cyber-Fun Internet Café may not use its computers to access, view, or obtain obscene materials. To ensure compliance with this policy, the Cyber-Fun Internet Café reserves the right to record the names and addresses of World Wide Web sites that patrons visit using Cyber-Fun Internet Café computers.

It is the policy of the law firm of Rowley & Yzaguirre to monitor the Internet access of its employees to ensure compliance with law firm policies. Accordingly, your use of the Internet may be monitored. The firm reserves the right to disclose the fruits of any monitoring to law enforcement if it deems such disclosure to be appropriate.

Creating a Company Security Policy

- Policy Statement
  - S.M.A.R.T

- State the Issue
- Identify the players
- Find Relevant Documentatio
- Define the Policy
- Identify Penalties
- Make Sure the Policy is Enforceable

Technical Prevention

- Use Multi-Factor Authentication Measures;
- Enforce Periodic Password Changes;
- Implement Minimum Privileges;

Technical Prevention

- Restrict Administrator Account Access;
- Implement Automated Patching Tools;
- Segregate Your Network;

Technical Prevention

- Establish a baseline of applications and security measures installed on all network machines across your enterprise. This baseline can be a starting point for distinguishing malicious and benign activity.

Things you can do today!

- Update your software
  - ISP supplied router firmware.
- Change your passwords
  - Change default passwords.
  - Make sure you use different passwords for different applications.
  - Use a password manager.
  - Passphrase vs. password
  - Wifi passwords
- Install /Run/ Update protection software
- Limit Internet access