protiviti®
Face the Future with Confidence

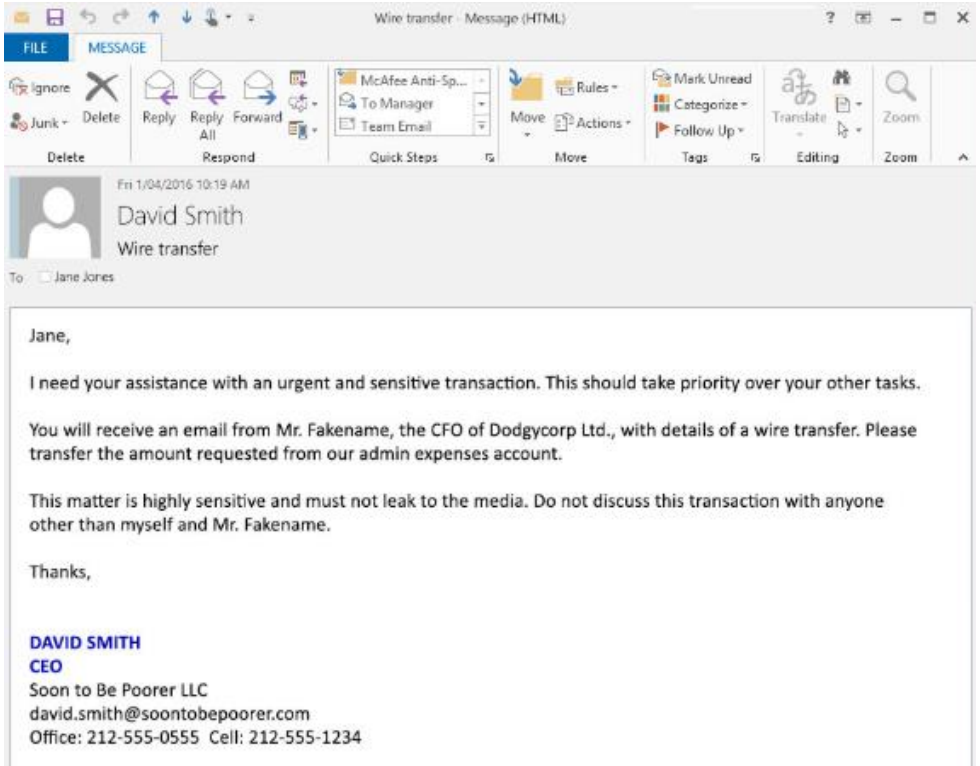
DID YOUR BOSS REALLY REQUEST THAT WIRE?

Protiviti Presentation for the Space City Cash Conference

September, 2018

Protiviti Perspective provided by Michael K., New York

IMAGINE THIS SCENARIO



protiviti

SOCIAL ENGINEERING

How the attack plays out

Attacker Research

- Target specific C-Suite employee.
- Leverage open source intel; social media, corporate websites.

Typo Squatting

- Register similar domain name to company e.g. “conpany.com”.
- Or, another top-level-domain.

Send Phishing Email

- Craft message to target employee impersonating CEO or CFO.
- Typically initiates an urgent contact.

Staff “Hooked”

- Employee responds and communication established.
- Payload deployed (wire transfer request).

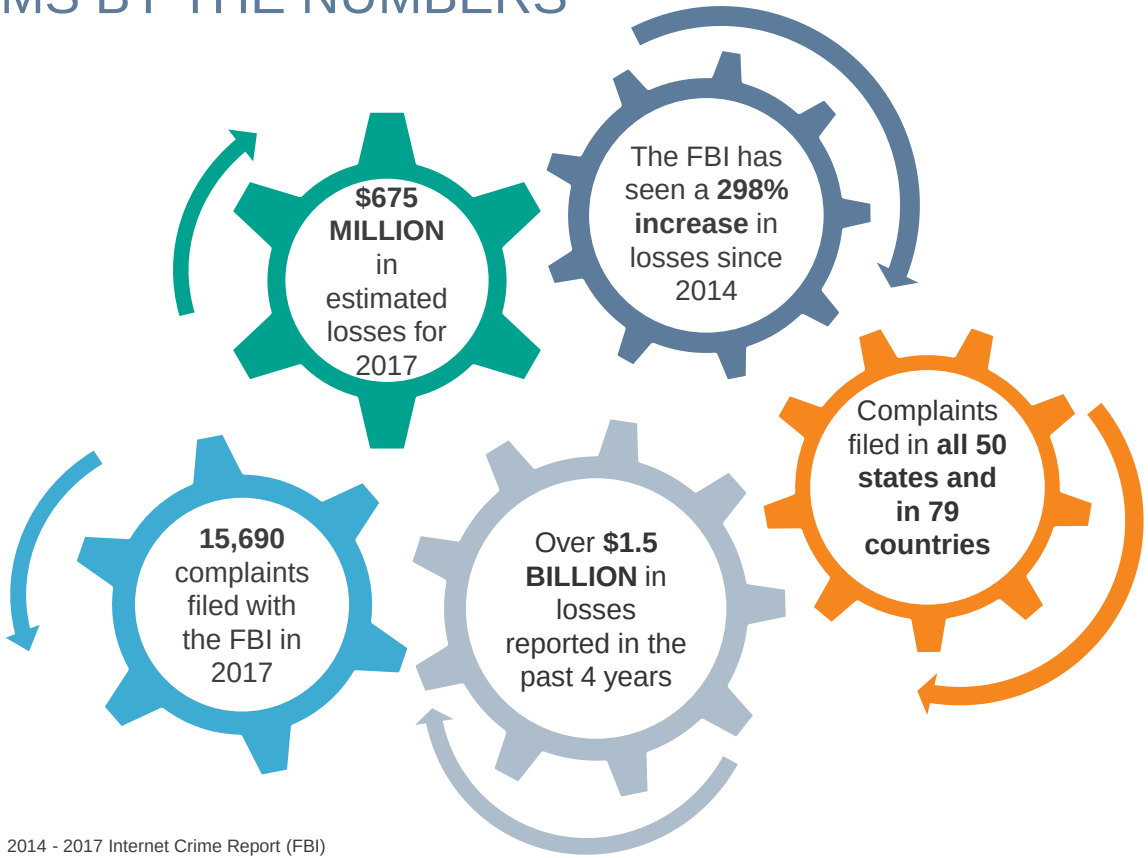
Money Wired

- Finance duped into sending wire, bank or BACS transfer to attacker account.

protiviti

THE HUMAN FACTOR IN SECURITY

CEO SCAMS BY THE NUMBERS



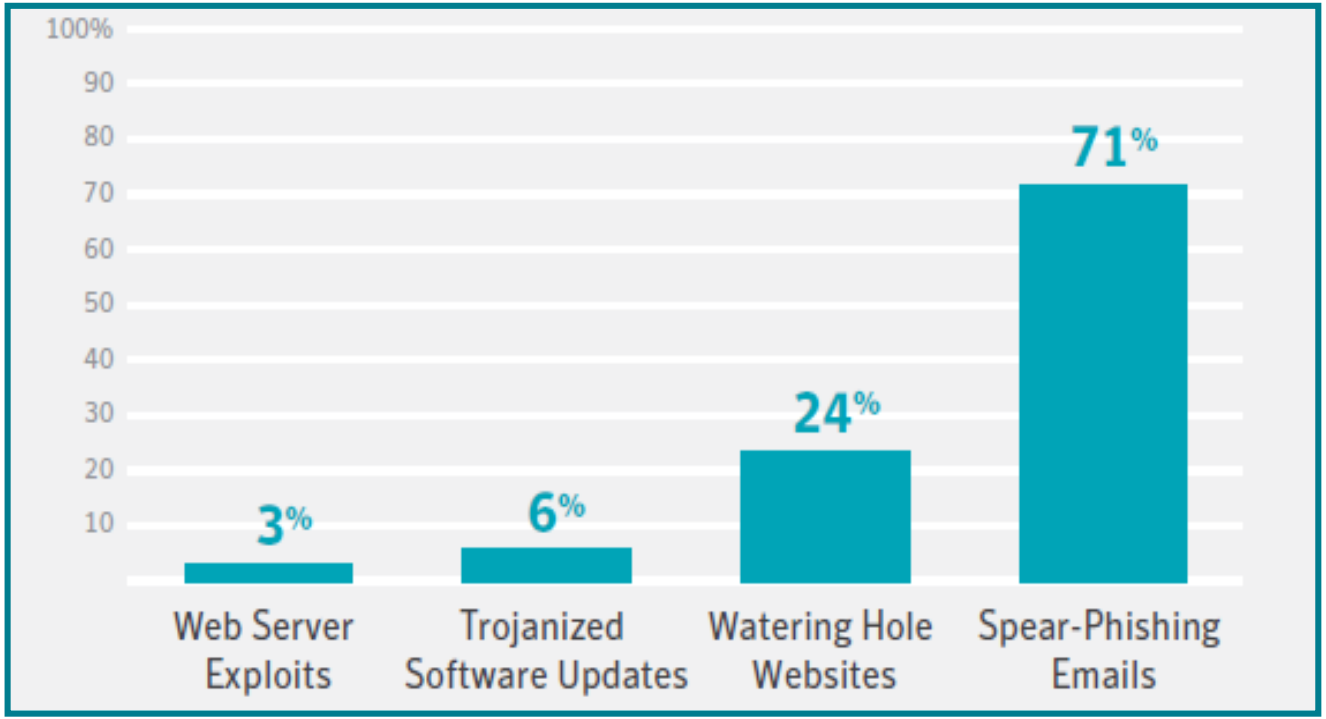
Source = KrebsOnSecurity, 2014 - 2017 Internet Crime Report (FBI)

protiviti

THE CYBERSECURITY CLIMATE

HOW DO ATTACKERS GET IN?

Spear-phishing emails emerged as by far the most widely used infection vector, employed by 71 percent of groups.

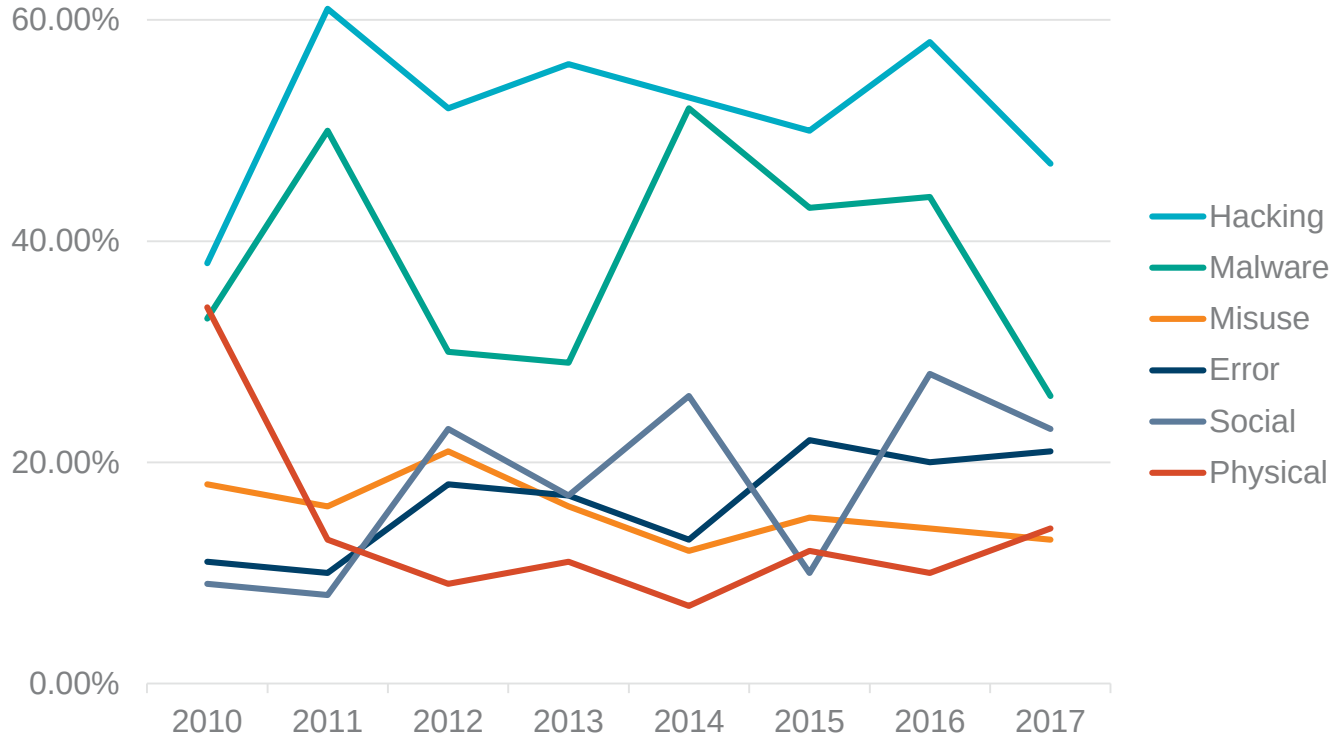


Source: 2017 Symantec Internet Security Report

protiviti

WHAT ARE THEY DOING?

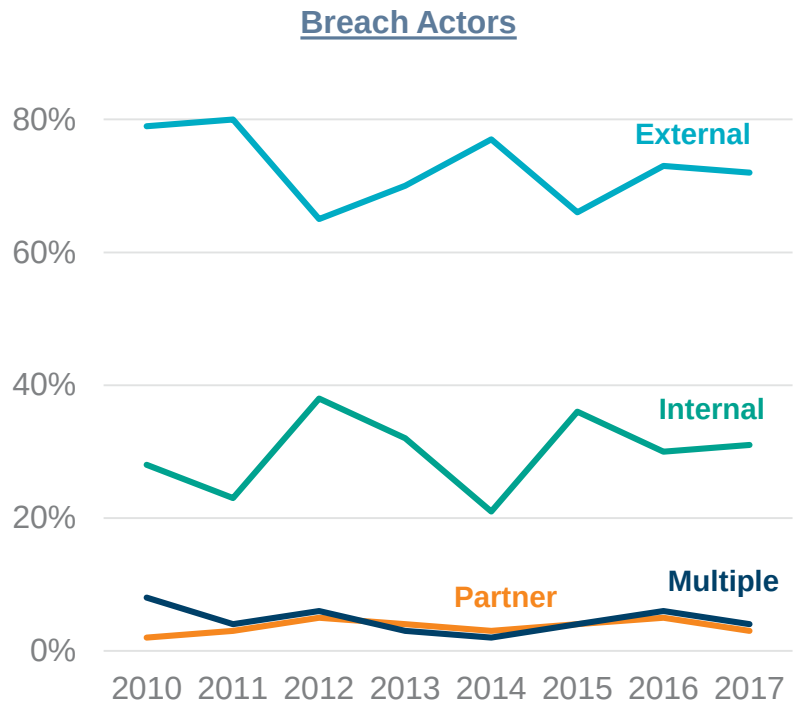
Hacker Activities in Breaches

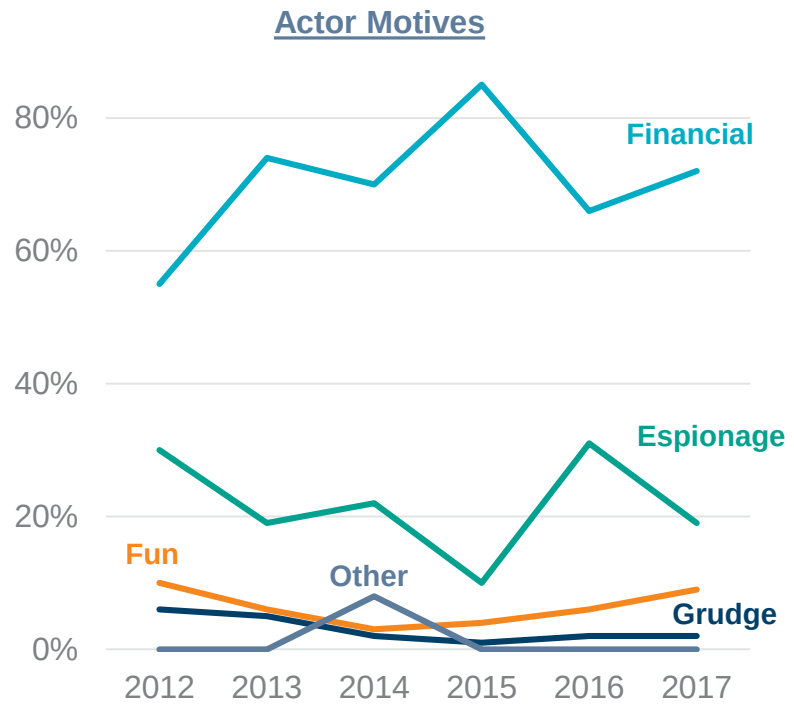


Source: 2018 Verizon Data Breach Investigation Report

protiviti

WHO'S DOING THIS AND WHY?





Source: 2018 Verizon Data Breach Investigation Report

protiviti

WHO ARE THE BAD GUYS?

Who are the external Bad Actors, their victims, methods and target data?

	Organized crime	State-affiliated	Activists
Victim Industry	• Finance • Retail • Food	• Manufacturing • Professional • Transportation	• Information • Public • Other Services
Desired Data	• Payment cards • Credentials • Bank account info	• Credentials • Trade secrets • System info	• Personal info • Credentials • Internal data
Targeted Assets	• ATM • POS controller/terminal • Database • Desktop	• Laptop/desktop • File server • Mail server • Directory server	• Web application • Database • Mail server
Region	• Eastern Europe • North America	• East Asia (China)	• Western Europe • North America
Common Actions	• Tampering (Physical) • Brute force (Hacking) • Spyware (Malware) • Capture data (Malware) • Adminware (Malware) • RAM Scraper (Malware)	• Backdoor (Malware) • Phishing (Social) • Export data (Malware) • Password dumper (Malware) • Downloader (Malware) • Stolen creds (Hacking)	• SQLi (Hacking) • Stolen creds (Hacking) • Brute force (Hacking) • RFI (Hacking) • Backdoor (Malware)

THE COST OF A BREACH

Results of the 2018 Cost of a Data Breach Study

$3.86 Million
Average total cost of a breach

$148
Average cost per record breached

197 Days
Average time from breach until discovery

Source: 2018 Cost of a Data Breach, Ponemon Institute

SOCIAL ENGINEERING

SOCIAL ENGINEERING EXPLOSION

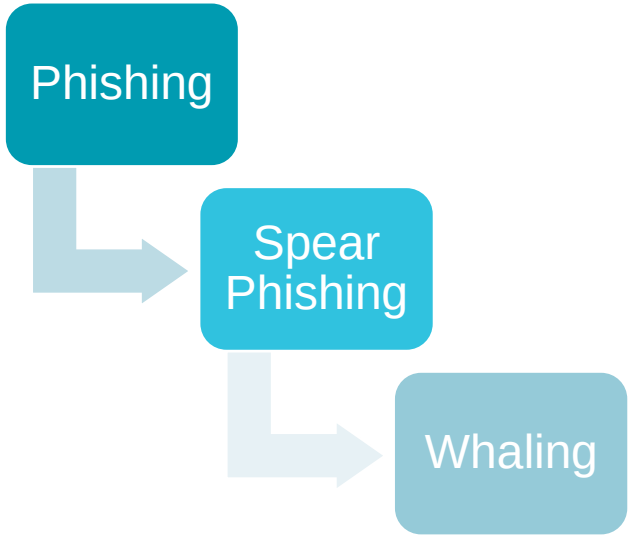
Social Engineering Methods Have Grown Up

Social engineering has moved beyond the well-known spam email campaigns and developed into a variety of mature techniques.

Source: Russell A Jackson - “Pulling Strings”, Internal Auditor Magazine, August 2018

protiviti

LET’S JUST FOCUS ON PHISHING



- **Phishing** – Sending fake emails, often impersonating a trusted source (e.g., major banks, technology companies)
- **Spear Phishing** – Precision phishing, tailored to a specific individual or organization
- **Whaling** – Targeted phishing of specific, high-ranking members of an organization

CHARACTERISTICS OF A SCAM

Look for these common techniques scammers use:

protiviti

WHAT CAN WE DO?

Stick to the Process

- Don’t give in to pressure or scare tactics in phishing attempts
- Follow established procedures and controls

Keep Your Passwords Secret

- IT departments and third parties will never ask for your passwords
- Use a different password across websites

Ask For Help

- When in doubt, reach out to the requestor via established means of communication
- Ask your IT department for support

Stay Vigilant

- Social engineering attacks rely on victims dropping their guard
- Inspect wire and information requests carefully

TAKEAWAYS

KEY POINTS TO REMEMBER

Cyber threats are on the rise across organizations.

Breaches are hard to detect and expensive to respond to.

It only takes one security failure for a breach to occur.

You have a part in preventing breaches.

QUESTIONS

Face the Future with Confidence

protiviti®