CYBER SECURITY SUMMIT 2016

Anatomy of an Attack: Hack Stories and How You are Being Infiltrated

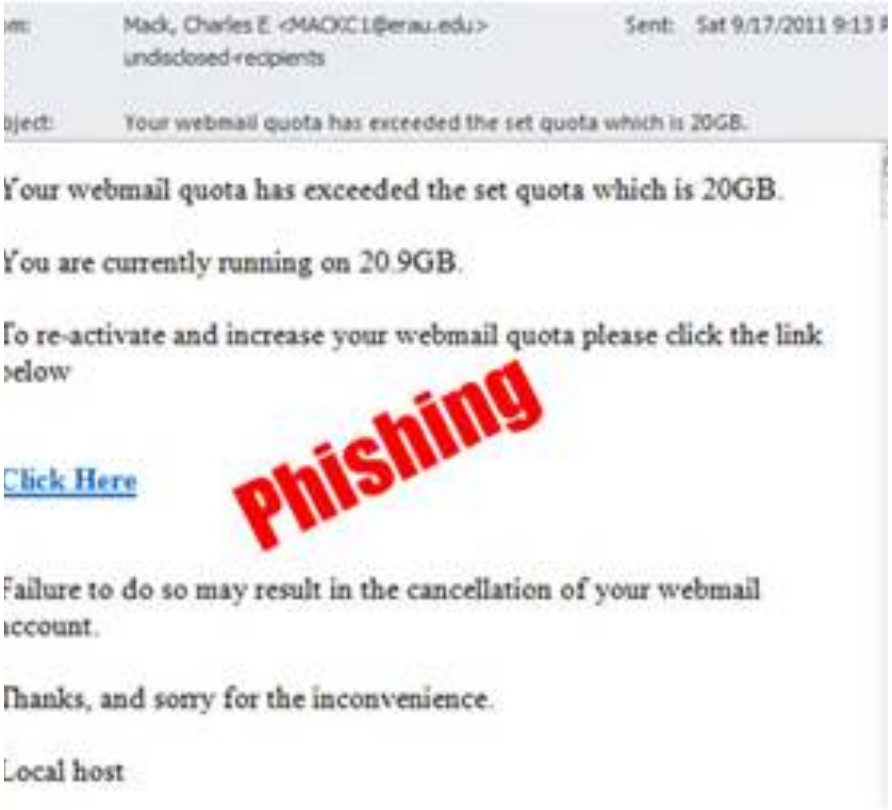
Optum, Kevin Charest, VP IT Cyber Defense Operations

Phishing

- Phishing - social engineering and technical mechanisms
- Social Engineering – weakness of human element
  - Early phishing through IM
  - AOL
  - Evolved into email
  - Use of malicious links
    - Typo - Paypals.com
    - Character replacement- Paypa1.com
    - Subdomains - Paypal.payments.com
    - TLD - Paypal.om

Phishing

- Technical component – weakness of system
  - Screenloggers / keyloggers
  - Corrupt browser navigation
  - Malware delivery
- All take advantage of human component



Common Phishing Types/Campaigns

- Business Email Compromise (BEC)
- Wire Transfer Fraud
- Recent News events (Olympics themed subjects, Political news, etc.)
- Spear Phishing
- Whaling

Credentials

- Credential harvesting
  - Not just financial
  - social networking, gaming, email, multimedia services
- Portal Data Theft
  - More able criminal actors
  - Most bang for buck
  - Passwords stored in various forms
    - plaintext, hash, salted hash

Credentials

- What are criminals doing with credentials
  - Profitable
    - Fraud
    - Selling to those who will use for fraud
      - Plaintext and hash are more profitable than salted hash
  - Just releasing them

Credential Reuse

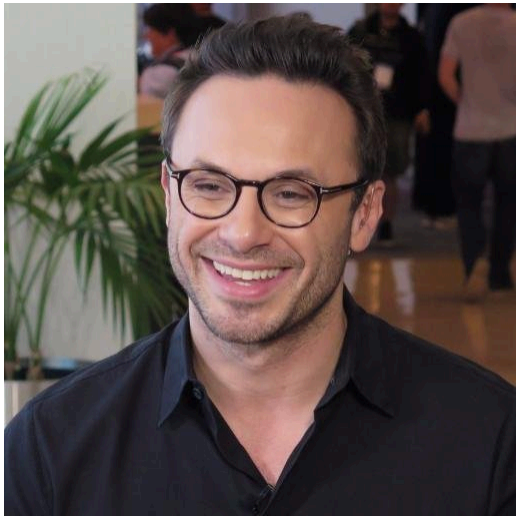
- Why concern?
  - Just reset password on breached account
- Password Reuse across accounts
- Telesign poll
  - 2000 people in US and UK
  - 21% passwords 10+ years old
  - 47% passwords 5 years old
  - 73% duplicate password used on other online accounts
  - average 6 unique passwords 24 online accounts

Credential Reuse

- GotomyPC – Carbonite – Logmein
  - mandatory password reset
- Escalation of privileges
  - reused passwords are enough for a foot in the door

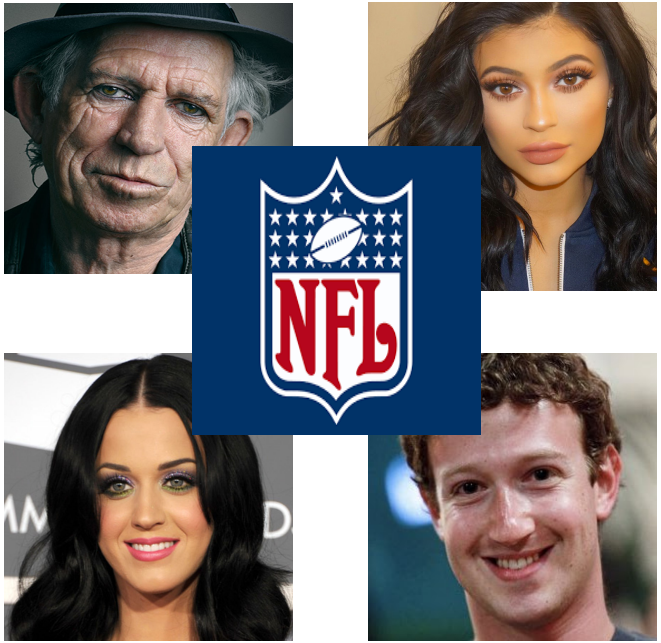
Credential Reuse

- Remote Desktop Services
  - Teamviewer and GoToMyPC customers
  - Reused credentials from other breaches
  - Personal financial data - Installed malware
  - Used Internet browser
    - Autofill – saved passwords feature
- Oculus CEO Brendan Iribe
  - Twitter account
  - MySpace password reused



Credential Reuse

- Celebrities
  - Mark Zuckerberg
    - Twitter and Pinterest
    - Reused from LinkIn – dadada
  - Katy Perry
  - Keith Richards
  - Kylie Jenner
  - Official NFL Twitter



Credential Reuse

- Dropbox
  - 68,648,009 – 5GB
  - Salted hash
  - Breach in 2012
  - Evidence attacker used breached third party site username/password combinations
  - One was a Dropbox employee which gave attacker access

Breaches

Latest credential releases 'mega breeches"

- Tessa88 and Peace-of-Mind
- Majority seen for sale in last months
- 2012 – 2013
- Plaintext and hashed (no salt) passwords
  - No salt hash determined with ease

Myspace

- 360 million
- Thomas White published
- unsalted SHA-1 hashes

Breaches

VK – (formerly VKontakte) Russian version of the most popular Facebook

- 100 million– a vast majority Russian speaking users
- plaintext

LinkedIn

- 117 million
- unsalted SHA-1 hashes

Last.FM

- 43 million
- unsalted MD-5 hashes

Breaches

- Rambler – Russian answer to Yahoo! In terms of functionality
  - 98 million
  - Plaintext
- Twitter
  - 32 million
  - Plaintext
  - Evidence end-user infected not Twitter breach
  - Mostly Russian speaking victims
- Total 750 million set of credentials
  - Unsalted and plaintext

Password analysis

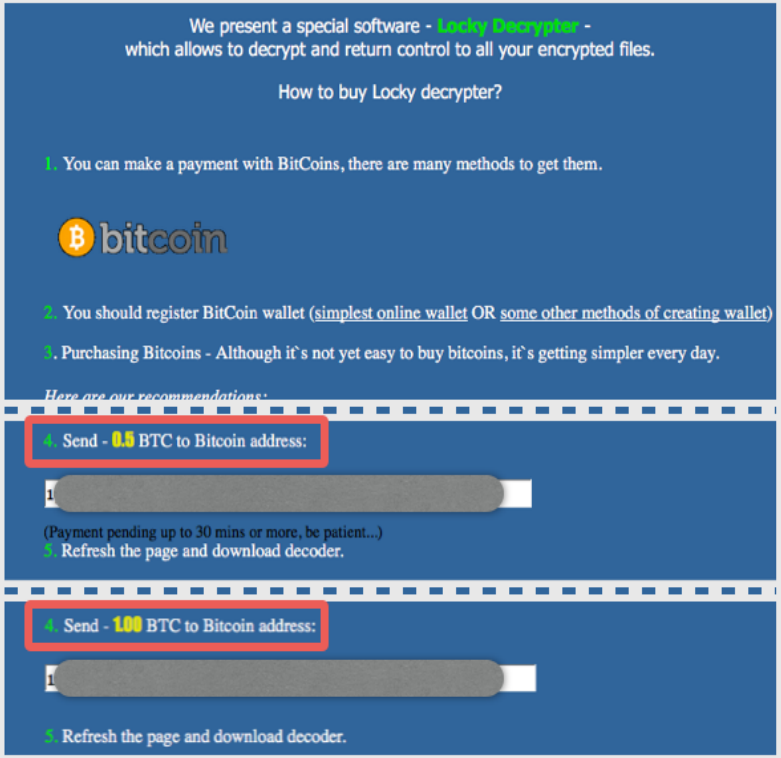
MySpace	VK	LinkedIn	LastFM	Rambler.ru	Twitter
	123456	123456	123456		123456
	123456789				123456789
				123456	
123456	111111	123456789	123456789	0	
	1234567890	12345678		666666	1234567
	1234567	111111		654321	1234567890
123456789	12345678	1234567			12345678
	123321		12345	123321	123321
	0		1234	555555	111111
	123123	654321		123123	12345

Ransomware

- 2016-"The Year of Ransomware"
- Ransomware has existed since 1989…so why now?
- Usage of Personal Computers
- Dependence on the Internet
- Cryptowall/Cryptolocker Code was released for sale in 2014.
- Ransomware is cheap, adaptable and effective (spray and pay)
- Often uses standard phishing techniques for delivery

Locky

- Most Prevalent of the New Wave of Ransomware
- Many, many variants
- Recently adapted to utilize 'Autopilot" functions, no longer needs to communicate with a Command and Control Server to Encrypt files



Different ransom demands by "Locky" at different times

Protections against Ransomware

- Backup regularly and keep a recent physical backup copy off-site.
- Don’t enable macros in document attachments received via email.
- Be cautious about unsolicited attachments.
- Be Stingy with Admin Access
- Keep Patches up to Date
- Airgap devices

Ransom DDoS Extortion

- New method to extort money from corporations
- Similar motives with different methods
- Multiple malicious actors using ransom DDoS
  - Kadyrovtsy (new group)
  - Lizard Squad
  - DD4BC (DDoS for Bit Coin)
  - Armada Collective
- Payment in Bitcoins
- Some actors will conduct a 'Demo" DDoS to demonstrate their capabilities
- Mixed results and follow through by actors.
  - Some never execute the DDoS even if they don't get paid.

DDoS Ransom Motives

- Economics
  - Very inexpensive to attack websites
  - Low Risk/High Reward
  - Some organizations just pay the ransom
- Most small businesses lack the technical support to fend off these attacks.
- A DDoS attack can cost an Ecommerce business significant losses if the web site is down for an extended amount of time.
- Even with a low success rate the attackers will come out ahead
- Attackers tailor the amount of demanded money to the business.
  - Large companies would receive a larger demand than that of a smaller business.

Fake Ransom DDoS Scams

- Recent incidents with fake actors purporting to be legitimate known adversaries
  - Armada Collective
  - Lizard Squad
- No intention or no ability to execute an actual DDoS attack
- The emails, although similar to legitimate adversaries have distinct differences
  - Contain technical inaccuracies
  - Use the same bitcoin address with each email
  - Poor or broken English
  - Low bitcoin amount (1 BTC)
- Organizations without technical expertise appear to be paying the ransom demand
- Actors will continue as long as they are successful

User Education and Training

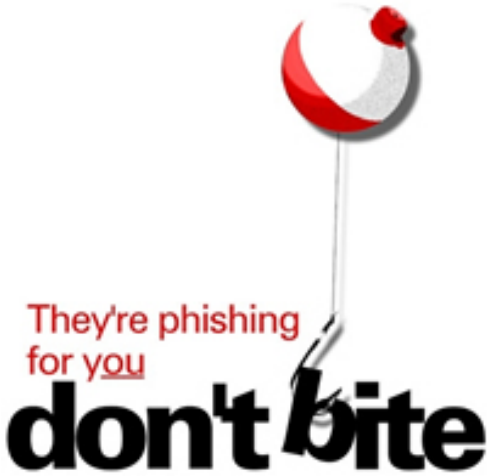
- Majority of attacks start with Social Engineering
- High success rate
- Data everywhere—easy to begin individual targeting
  - Social Media
  - Developer websites such as GitHub (Developers have great access)
  - Use of company e-mails on sites
- Use of gathered information to specifically target an employee
  - Socially engineered e-mail topics

User Education and Training

Education is the key to thwart this threat

Training Topics

- How to spot social engineering
  - E-mails
  - Web pages
- How to minimize exposure on internet and social media



Conclusion

It is clear from this discussion that end-users remain our biggest asset in the fight against cyber-criminals and cyber-crime in general.

It is equally clear that they remain the single biggest vulnerability and risk to your enterprise.

Reminders…

- Continuous security awareness for end-users
- Continuous security monitoring and visibility within your environment
- Proactive password resetting whenever possible as proper cyber hygiene