The Role of People in Security

Chapter 4

News

- https://it.slashdot.org/story/23/09/14/0120204/hackers-claim-it-only-took-a-10-minute-phone-call-to-shut-down-mgm-resorts?utm_source=feedly1.0mainlinkanon&utm_medium=feed

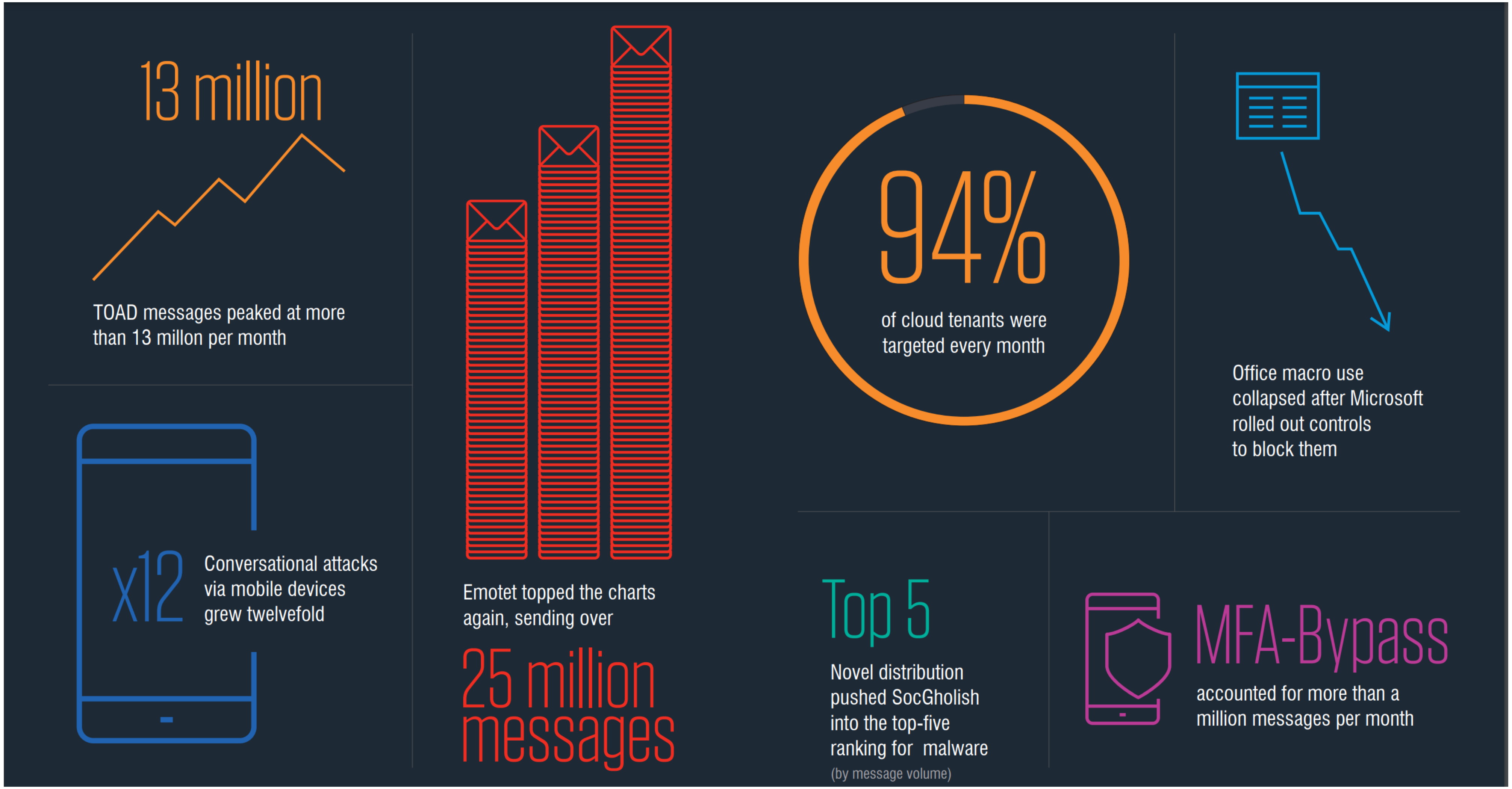
Objectives

- Define basic terminology associated with social engineering
- Describe steps organizations can take to improve their security
- Describe common user actions that may put an organization's information at risk
- Recognize methods attackers may use to gain information about an organization
- Determine ways in which users can aid instead of detract from security
- Recognize the roles training and awareness play in assisting the people side of security

People—A Security Problem

- Operational model of computer security acknowledges that prevention technologies are not sufficient to protect our computer systems and networks
    - The biggest reason is that every network and computer system has at least one human user
        - Humans are prone to make mistakes and are often easily misled or fooled

ProofPoint - The Human Factor 2023



13 million

TOAD messages peaked at more than 13 millon per month

x12 Conversational attacks via mobile devices grew twelvefold

Emotet topped the charts again, sending over

25 million messages

94%

of cloud tenants were targeted every month

Office macro use collapsed after Microsoft rolled out controls to block them

Top 5

Novel distribution pushed SocGholish into the top-five ranking for malware

(by message volume)

MFA-Bypass

accounted for more than a million messages per month

Current Top Malware

- Emotet - https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a
- SocGholish - https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

OSINT – The Prequel to SE

http://e-mate2.s3-website-us-east-1.amazonaws.com/OSINT/OSINT.html

OSINT Challenge

http://e-mate2.s3-website-us-east-1.amazonaws.com/osint-pd/OSINT_PD_Challenge.html

What is the person’s name?

What is the person’s address?

What is the spouse’s name?

What are the children’s names?

OSINT Framework

- https://osintframework.com/

Other Tools For OSINT

https://ncr-remote.cse.unr.edu/accounts/login/

- theHarvester
- Maltego

Some Other OSINT Tools

- Google Dorking
  - https://www.stationx.net/google-dorks-cheat-sheet/
  - Filetype: This is used to find filetypes
  - Ext: This is used to identify files with specific extensions. Think of using it for finding such files like .log, which are not supposed to be indexed

Social Engineering

Social Engineering

- Social engineering is the process of convincing an authorized individual to provide confidential information or access to an unauthorized individual
- Various deceptive practices are used to convince the targeted person to:
  - Divulge information they normally would not divulge
  - Do something they normally wouldn't do

Why does social engineering work?

- One idea: Cialdini's Social Influence Theory
  - Reciprocity
  - Consistency and commitment
  - Social proof
  - Liking
  - Authority
  - Scarcity
- Another idea: Truth Default Theory
  - Assume that communication is honest until proven otherwise
  - Fits with the state of the world, where most communication is honest
  - Can usually detect deception based on whether the lie serves the potential liar's interests

Defenses

- Awareness and training
- In all the cases of impersonation, the best defense is to have processes in place that require employees to ask to see a person's ID before engaging with them if the employees do not personally know them
- Strong defenses including MFA and monitoring

Social Engineering Toolkit

- Several tools to launch SE attacks.

Example Defense Tools

- Netcraft anti-phishing
  - http://toolbar.netcraft.com/

Module 3 Assignments

- Phishing Quizzes
- Graduate Final Project Topic

Definitions

These slides are not presented in class, they are here for your reference

Tools

- Principles (reasons for effectiveness)
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

Attacks

- Social engineering attacks target the people portion of your computing environment
  - Using psychology and technical means, the social engineer attempts to get a user to perform specific actions on a system—actions they normally would not do
  - These include clicking a link and going to a web page, running a program, saving information, and opening a file

Impersonation

- Impersonation is a common social engineering technique that can be employed in many ways
  - Third-party authorization
  - Contractors/outside parties
  - Help desk/tech support
  - Online attacks

Phishing

- Phishing is social engineering in which an attacker attempts to obtain sensitive information from a user
  - It masquerades as a trusted entity in an e-mail or instant message sent to a large group of often random users
  - Attacker attempts to obtain usernames, passwords, credit card numbers, and details about the user's bank accounts
  - Attacker points users to fake, non-reputable websites or sends bulk e-mails instructing users to click a fake link to verify that their account has not been tampered with
  - Phishing with open redirects: https://www.microsoft.com/security/blog/2021/08/26/widespread-credential-phishing-campaign-abuses-open-redirector-links/

Smishing

- Smishing is a version of a phishing attack using the Short Message Service (SMS) on victims' cell phones
  - It begins with an SMS message directing a user to a URL from which the attacker then can serve up a variety of attack vectors, including forms of malware
  - This attack works primarily because of the principles of urgency and intimidation

Vishing

- Vishing is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking
  - Takes advantage of the trust people place in the telephone network
  - Attackers can spoof (simulate) calls from legitimate entities using Voice over IP (VoIP) technology
  - Voice messaging can also be compromised
  - Attackers are after credit card numbers or other information that can be used in identity theft

Spam

- Spam is bulk unsolicited e-mail
  - It is not generally considered a social engineering issue
  - Spam can be a security concern
  - Legitimate spam is sent by a company advertising a product or service
  - Malicious spam includes an attachment containing malicious software designed to harm your system, or a link to a malicious website that may attempt to obtain personal information from you

Spam over Internet Messaging (SPIM)

- SPIM is spam delivered via an instant messaging application
  - The purpose of hostile SPIM is the same as that of spam—the delivery of malicious content or links and getting an unsuspecting user to click them, thus initiating the attack

Spear Phishing

- Spear phishing is the term used for a phishing attack that targets a specific group of people or businesses with something in common
  - Because a specific group is being targeted, such as senior executives, the ratio of successful attacks (that is, the number of responses received) to the total number of e-mails or messages sent usually increases
    - A targeted attack will seem more plausible than a message sent to users randomly

Whaling

- A whaling attack is one where the target is a high-value person, such as a CEO or CFO
    - Whaling attacks are not performed by attacking multiple targets and hoping for a reply, but rather are custom-built to increase the odds of success

Pharming

- Pharming consists of misdirecting users to fake websites made to look official
  - Using phishing, individuals are targeted one by one by sending out e-mails
  - To become a victim, the recipient must take an action

Dumpster Diving

- Dumpster diving is the process of going through a target's trash in hopes of finding valuable information that might be used in a penetration attempt
  - One common place to find information, if the attacker is in the vicinity of the target, is in the target's trash

Shoulder Surfing

- Shoulder surfing does not require direct contact
  - The attacker may simply look over the shoulder of the user at work, for example, or may set up a camera or use binoculars to view the user entering sensitive data
  - Example of information desired: PINs or gate codes
- Shoulder surfing prevention techniques
  - Small shield surrounding keypad or scramble location of the numbers on keypad
  - Best defense is user awareness of surroundings
  - Be aware of attacker starting conversation with target

Tailgating/Piggybacking

- Tailgating (or piggybacking) is the simple tactic of following closely behind a person who has just used his own access card or PIN to gain physical access to a room or building
  - An attacker can gain access to the facility without having to know the access code or acquire an access card
  - Prevent tailgating by using procedures ensuring nobody follows too closely or is in a position to observe actions
  - Can use a mantrap, which utilizes two doors to gain access to the facility

Eliciting Information

- Calls to or from help desk and tech support units can be used to elicit information
  - A skilled social engineer can use a wide range of psychological techniques to convince people whose main job is to help others to perform tasks resulting in security compromises

Prepending

- Prepending is defined as the act of adding something else to the beginning of an item
  - When used in a social engineering context, prepending is the act of supplying information that another will act upon, frequently before they ask for it, in an attempt to legitimize the actual request, which comes later

Identity Fraud

- Identity fraud is the use of fake credentials to achieve an end
  - This can be a high-risk endeavor, such as pretending to be an official representative of a government agency or a regulator, or it can be lower risk, such as showing up as the person who waters the plants

Invoice Scams

- Invoice scams are just that—a scam using a fake invoice in an attempt to get a company to pay for things it has not ordered
  - The premise is simple: send a fake invoice and then get paid

Credential Harvesting

- Credential harvesting is the collection of credential information, such as user IDs, passwords, and so on, thus allowing an attacker a series of passes to the system
  - The objective of a credential harvest is just that—credentials

Reverse Social Engineering

- Reverse social engineering occurs when the attacker hopes to convince the target to initiate the contact
  - Attack is successful since target is initiating the contact
    - Attacker may not have to convince target of their authenticity
    - The tricky part of this attack is convincing the target to make that initial contact
  - Methods to accomplish an attack
    - Send out a spoofed e-mail with contact information
    - Target an organization undergoing organizational change

Reconnaissance

- Reconnaissance is a military term used to describe the actions of surveying a battlefield to gain information prior to hostilities
  - In the field of cybersecurity, the concept is the same—an adversary will examine the systems they intend to attack, using a wide range of methods

Hoax

- A hoax can be very damaging if it causes users to take some sort of action that weakens security
  - Training and awareness are the best and first line of defense for both users and administrators
  - Users should be trained to be suspicious of unusual e-mails and stories and should know who to contact in the organization to verify their validity when received
  - Hoaxes often also advise the user to send it to their friends so they know about the issue as well—and by doing so, they help spread the hoax

Watering Hole Attack

- A watering hole attack involves the infecting of a target website with malware
  - In some of the cases detected, the infection was constrained to a specific geographical area
  - These are not simple attacks, yet they can be very effective at delivering malware to a specific groups of end users
  - Watering hole attacks are complex to achieve and appear to be backed by nation-states and other high-resource attackers

Typo Squatting

- Typo squatting is an attack form that involves capitalizing on common typographical errors
    - If a user mistypes a URL, then the result should be a 404 error, or “resource not found”
        - But if an attacker has registered the mistyped URL, then the user would land on the attacker’s page
    - This attack pattern is also referred to as URL hijacking, using a fake URL, or brandjacking if the objective is to deceive based on branding

Influence Campaigns

- Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people's minds on a topic
    - One can engage in an influence campaign against a single person, but the effect is limited
    - Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation

Poor Security Practices (1 of 7)

- A significant portion of human-created security problems results from poor security practices
  - These poor practices may be:
    - Due to an individual user who is not following established security policies or processes
    - Caused by a lack of security policies, procedures, or training within the user's organization

Poor Security Practices (2 of 7)

- Password selection
  - Users tend to pick passwords that are easy to remember
    - Names of family members, pets, sports teams
  - The more the attacker knows about the user, the better the chance of discovering the user’s password
    - Organizations have encouraged users to mix upper- and lowercase characters and to include numbers and special characters in their password

Poor Security Practices (3 of 7)

- Shoulder surfing
  - Involves the attacker directly observing the target entering sensitive information on a form, keypad, or keyboard
- Piggybacking
  - Happens because the person is not paying attention to the context of their situation
- Dumpster diving
  - Process of going through a target's trash in hopes of finding valuable information that can be used in a penetration attempt

Poor Security Practices (4 of 7)

- Installing unauthorized hardware and software
    - Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems
    - A backdoor is an avenue used to access a system while circumventing normal security mechanisms and can often be used to install additional executable files that can lead to more ways to access the compromised system
    - Common examples include unauthorized communication software and a modem; a wireless access point; and games

Poor Security Practices (5 of 7)

- Data handling
  - Understanding the responsibilities of proper data handling associated with one's job is an important training topic
  - Include a training clause for certain data elements requiring special handling because of contracts, laws, or regulations
  - The spirit of the training clause is you get what you train; if security over specific data types is a requirement, it should be trained

Poor Security Practices (6 of 7)

- Physical access by non-employees
  - Significant deterrent to unauthorized individuals is to require employees to wear identification badges at work
    - Method to quickly spot who has permission to have physical access to the organization and who does not
    - Requires employees to actively challenge individuals who are not wearing the required identification badge
  - Personnel with legitimate access may have an intent to steal intellectual property or exploit the organization
    - Contractors, consultants, partners, custodial staff

Poor Security Practices (7 of 7)

- Clean desk policies
  - Specify that sensitive information must not be left unsecured in the work area when the worker is not present to act as custodian
    - Example: leaving the desk area and going to the bathroom can leave information exposed and subject to compromise
  - Policy should identify and prohibit things that are not obvious upon first glance, such as passwords on sticky notes under keyboards and mouse pads or in unsecured desk drawers

People as a Security Tool

- Social engineering paradox
  - People are the biggest problem and security risk, but also the best tool in defending against a social engineering attack
- To fight social engineering attacks, create policies and procedures that establish roles and responsibilities for security administrators and all users
  - Management expectations, security-wise, from employees
  - Description of items the organization is trying to protect, and mechanisms important for that protection

Security Awareness (1 of 2)

- Active security awareness program
  - Single most effective method to counter potential social engineering attacks
  - The extent of the training will vary depending on the organization’s environment and the level of threat
  - Training should stress the type of information that the organization considers sensitive and that may be the target of a social engineering attack
  - Employees should be aware of attack indicators
  - Employees should be taught to be cautious about revealing personal information

Security Awareness (2 of 2)

- Social networking and P2P
  - Confusing sharing information with friends and sharing business information with those who don’t need to know it is a line people are crossing on a regular basis
    - Be careful not to mix social and business communications
  - Users also need to understand the importance of not using common programs such as torrents and other peer-to-peer (P2P) file-sharing communication programs in the workplace