Executive Summary

Hacking the Human Operating System

Raj Samani, EMEA CTO

Charles McFarland, Senior MTIS Research Engineer

intel Security

Many cyberattacks involve an element of social engineering, which attempts to persuade a targeted individual to perform an action that causes an infection or the disclosure of valuable information.

Although the focus of attack remediation is a technical fix, the human angle of the attack results in blame placed on the target and a demand for further security awareness. Yet the truth is that most organizations do little to understand why the target was exploited and, more important, what to do beyond raising awareness to reduce the risk of further attacks.

The term social engineering can be defined as:

> *The deliberate application of deceitful techniques designed to manipulate someone into divulging information or performing actions that may result in the release of that information.*

During a social engineering attack, the victim is not consciously aware that his or her actions are harmful. The social engineer exploits the target's innocent instincts, not any criminal instincts. An attack can be divided into two categories:

- Hunting aims to extract information using minimal interaction with the target. This approach typically involves a single encounter, with the attacker ending communication once information has been acquired.
- Farming aims to establish a relationship with the target, and to "milk" them for information over a longer period.

Social engineering attacks that leverage email as the communication channel generally use hunting as the primary form of attack. There are exceptions to this such as the "Nigerian 419 scams," which attempt to extend the attack over a long duration so they can extract additional funds. Hunting and farming social engineering attacks typically consist of four phases:

1. Research: This optional phase aims to gather information about the target. The attacker seeks information that will help build a successful hook such as identifying the target's hobbies, place of work, or financial service provider.
2. Hook: The hook aims to set up a successful "play" by engaging the target and providing a pretext for an interaction. Psychologist Robert Cialdini cites six influencing levers, which aim to leverage the target's subconscious;
   - Reciprocation: People are provided with something for which they feel obligated and subsequently aim to repay the favor.
   - Scarcity: People tend to comply when they believe something is in short supply.
   - Consistency: Once targets have promised to do something, they will stick to their promises because they do not wish to appear untrustworthy.
   - Liking: Targets are more likely to comply when the social engineer is someone they like.
   - Authority: Exploits the human tendency to comply when a request comes from a figure of authority.
   - Social validation: The tendency to comply when others are doing the same thing.

3. Play: Carrying out the main part of the attack. This may be the disclosure of information, clicking on a link, transferring funds, etc.
4. Exit: The interaction is closed down. Although it may be beneficial to exit without suspicion for many farming attacks, this may not be necessary. For example, when attackers manipulate targets into the disclosure of payment card information, the former generally don't want to raise suspicion lest the victims report their cards as lost or stolen and then cancel them. However, if attackers successfully steal source code or other personal information, then even if the targets become suspicious they will be unable to recover the stolen data.

Social engineering attempts are not necessarily linear; a single attack may be part of a much larger campaign to gather multiple bits of related information. For example, attackers may perform one attack, retrieve the information, and disappear. Alternatively, they may perform numerous hunting attacks and with that collected information initiate a farming attack.

Channels of attack

Social engineers can use several avenues for their attacks.

- Websites: Social engineering attacks often leverage malicious websites as a channel of attack. According to the *2014 Verizon Data Breach Investigations Report,* "20% of espionage-motivated attacks use a strategic web compromise to deliver malware."
- Email: The most common forms of social engineering through email are phishing and the more targeted spear phishing. Email is an effective method for cybercriminals because "18% of users will visit a link in a phishing email," according to the Verizon report.
- Telephone: This is a popular channel for information brokers.
- Face to face: An employee can be approached and tricked or coerced into providing information.
- Postal service: Although this channel appears less prevalent than others, there are still reports of social engineering attacks via postal mail.
- Fax: Examples include emails posing as messages from online payment services.

Defending against social engineering

The following controls can be used to mitigate the risk of social engineering. These are divided into three categories: people, process, and technology. These controls are not exhaustive, and may not be applicable to all organizations.

People

- Provide clear boundaries: All staff should be keenly aware of the policies regarding the release of information and have clear escalation paths should a request fall outside of their boundaries.
- Ongoing education: Implement a security awareness program to consistently educate employees over time. Use tools such as the McAfee Phishing Quiz to highlight specific tactics commonly used in attacks.
- Permission to verify: Provide staff with the confidence to challenge even seemingly innocuous requests. An example of this is to challenge people when attempting to tailgate into offices.

- Teach the importance of information: Even seemingly innocuous information such as telephone numbers (enabling information) can be used to stage an attack.
- Create a no-blame culture: The targets of social engineers are victims. Punishing specific employees who have been deceived will make all staff less likely to admit to releasing information. Once conned, they could come under the control of the social engineer, who can then use blackmail.

Process

- Bogus call reports: When a suspicious activity has occurred, staff should complete a report that details the interaction. This assists investigations.
- Informative block pages: When employees reach a malicious web page, use a block page to inform them why they cannot proceed. This will cause them to reflect on their prior action and can help identify sources of attack.
- Customer notification: When callers are denied information, the organization should notify them and verify whether the caller was entitled to the information. Organizations should also consider how they communicate with customers. For example, PayPal includes guidance for users that helps identify if emails they receive are genuine; "A real email from us will never ask for your bank account number, debit, or credit card number etc. Also we'll never ask for your full name, your account password, or the answers to your PayPal security questions in an email."
- Escalation route: A clear reporting line for front-line staff to escalate any doubts they may have about interacting with potentially fraudulent messages.
- Tiger testing: Routinely test staff for their susceptibility to social engineering attacks over the use of multiple communication channels. This provides a tool to measure the effectiveness of training programs.

Technology

- Call recording: Routinely record incoming telephone calls to assist investigations.
- Bogus lines: Route calls that are believed to be suspicious to a monitored number.
- Email filtering: Remove fraudulent emails containing known and never-before seen malware.
- Web filtering: Block access to malicious websites and detect malware inline with access to the Internet.
- Strong authentication: Although leveraging multifactor authentication will not eliminate the risk of users being socially engineered into giving up their authentication credentials, it will make the task more difficult for would-be attackers.

Follow McAfee Labs

Summary

The threat of social engineering is very real. Cybercriminals use it to unlawfully extract information for various malicious uses. To best counter the problem, we must understand the nature of social engineering attacks. This means defining the likely threat actors, their attack methods, and their resources—and applying the relevant controls to reduce the risk of a successful attack.

A copy of the full report can be found at **www.mcafee.com/hacking-human-os.**

Twitter@Raj_Samani

Twitter@CGMcFarland

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com