SecurityAwarenessNews

the security awareness newsletter for security aware people

MALWARE, PHISHING, AND OTHER LURKING THREATS

The How, Why, and What About Enterprise Threat Detection

BEC

Ransomware Roundup

The **How**, **Why**, and **What** About Enterprise Threat Detection

Security threats come from everywhere–all over the globe, 24 hours a day, 7 days a week, 365 days a year, banging on 'cyber-doors' incessantly. Detecting those threats before they cause damage is paramount to our success as an organization. From the enterprise and security viewpoints, threat detection takes many forms, and requires some reasonable technical skills and management. Here are a few examples from the more technical side:

1. **Endpoint detection and response (EDR)** monitors detailed endpoint (PC, Tablet, Phone, etc.) behavior, such as internal processes, registry settings, file activity, and network activity.
2. **Network traffic analysis (NTA)** monitors network traffic, looking for anomalous, suspicious, and malicious activity.
3. **Cyber threat intelligence (CTI)** looks at internal security incidents and cyber adversary tactics, techniques, and procedures.

These tools help organizations detect threats and neutralize them. But not all threat detection requires technical skills. In fact, the best form of threat detection is you, the *human firewall*. The human firewall uses non-technical skills to:

Spot and prevent physical threats such as a secured door left ajar, or an unknown person accessing secured areas.

Identify phishing attacks and other forms of social engineering.

Report all security incidents immediately, thereby reducing their impact.

Guard possessions and use caution when working remotely or traveling.

Follow policy no matter what.

In short, human firewalls are the ultimate threat detectors. You know how to scan your environment to notice odd things and behavior. You detect social engineering attempts and other potentially hostile threats. You never make assumptions and always think before you click. These *simple awareness behaviors* on your part improve our culture and help protect our organization from the many threats we face every day.

BEC

What is it? BEC stands for **business email compromise** and is defined by the FBI as a *"sophisticated scam targeting organizations working with foreign suppliers and organizations that regularly perform wire transfer payments."*

Types of BEC Attacks

CEO Fraud

Attackers impersonate a C-level member of an organization to send requests for sensitive info or wire transfers.

EAC

Email account compromise, also known as account hijacking, occurs when someone gains unauthorized access to an employee email account.

Invoice Scams

Attackers often issue fraudulent invoices by impersonating partners and foreign suppliers.

How does a BEC attack work?

The goal of a scammer is to gain and abuse your trust. Trust is how BEC attackers managed to compromise organizations in over 100 countries, racking up billions in financial losses in just a few years' time.

How is this possible? Imagine receiving an email from your boss asking you to wire money to someone or requesting highly sensitive information. How likely are you to engage and comply with the request? The same is true in your personal life. If you get an email from a close friend or family member claiming they are stuck in a foreign country and need money, what do you do?

The following steps outline how business email compromise works:

STEP 1: Gather Intel
The attackers spend weeks or even months gathering info about their targets, such as full names, email addresses, home addresses, hobbies, family members, close friends, and social status.

STEP 2: Hijack Email
By hijacking email accounts, the attacker can impersonate the owner of the email account and target that person's contact list.

STEP 3: Phish Employees
By impersonating the CEO, for example, the attacker can send a request to the financial department for a wire transfer payment to an unauthorized account. Since the email appears to come from someone the employee knows (the boss), the employee is much more likely to comply with the request, often without a second thought.

How to prevent this from happening to you.

Always verify the source. Requests for money or sensitive information should be handled cautiously, and with a degree of skepticism.

Vocally confirm those requests. Even if you're 99% sure the request is legitimate, there's no harm in confirming it and avoiding that 1% chance that you are wrong.

Be cautious on social media. Limit the amount of information you share and consider maxing out privacy settings. Cybercriminals use social media for data mining their targets.

Learn to spot phishing emails. Common signs of phishing attacks include bad grammar, poor spelling, awkward phrasing, and threatening language.

Participate in awareness training. Every employee, from C-level to reception, benefits from awareness training!

Remember that high-level access creates high-level risk. C-suites, managers, and executives need to be extra cautious in every aspect of their work and personal lives, since they are the number one target.

Think before you click. Many of these attacks are made possible by someone clicking on something they shouldn't have.

Always follow policy. No matter what, follow our organization's policy at all times, and if you're not sure about something, please ask!

RANSOMWARE ROUNDUP

Alive and well, ransomware continues to terrorize organizations and entities all over the world. Attackers have spread their campaigns from large corporations to schools, city governments, small businesses, and even individuals.

What is ransomware?

As the name suggests, ransomware is a form of malware that encrypts files or locks computers until a specified ransom is paid in full. Cybercriminals threaten to destroy the encrypted data if the ransom isn't met by a predetermined date.

How do ransomware infections happen?

Someone clicked on something! In almost every case, ransomware was made possible by malicious links or attachments sent via email. In a small percentage of attacks, cybercriminals successfully manipulated security holes to inject the malware into a network without human interaction, but that is rare.

Why is ransomware so popular?

Unlike traditional data breaches, which result in stolen information, attackers use ransomware to lock up crucial systems. They know that most entities will pay to have those systems restored. For example, a city in Florida paid a steep price to regain control of their systems, which included emergency dispatch services. Ransomware provides a quick and healthy payday in a way that even the largest data breaches can't.

Preventing Ransomware in 3 Easy Steps

First things first–preventing ransomware and other cyber-attacks begins and ends with following our organization's policies. They are designed to protect all of us, and circumventing policies, for any reason, puts us at risk. With that in mind, follow these three steps to prevent ransomware in your personal life, and if you have any questions about our policies here at work, please ask!

1. **Stay alert for phishing attacks.** Some are easy to spot thanks to obvious indicators like poor grammar, bad spelling, and threatening language (like claiming your account has been suspended or that you owe a delinquent tax payment). Other attacks use more sophisticated techniques, such as sending an unpaid invoice to someone. No matter what, think before you click, and stay alert!

2. **Keep systems up to date.** Even if ransomware rarely spreads via security vulnerabilities, outdated systems are begging to get hacked. Enable auto-update on all of your devices and apps so you never miss an important security patch.

3. **Back up your data.** Security researchers recommend that you keep at least two redundant copies of your data and store one of those copies at a second location (such as the Cloud). There are plenty of free programs that will manage your backups and run automatically. But to fully shield yourself from ransomware, consider storing a backup offline so it doesn't get impacted should you run into ransomware.