ISSUE 01 | THREATS ON THE RISE

HOW TO COMBAT Spear Phishing
What is Spear Phishing?

Spear Phishing is one of the most common and most effective cyberattack vectors used today. Delivered through email, spear phishing campaigns aim either to infect devices with malware, or to steal important information like credentials and bank numbers. Unlike phishing, spear phishing is targeted at specific groups or individuals within an organization. Oftentimes, a spear phishing email will appear to come from someone trusted inside the company—like a boss or the head of a department—and will contain personalized content and a believable request to sound genuine. It is this characteristic that makes spear phishing so worrisome to security professionals.
How Does It Work?

Spear phishing relies on an attacker’s ability to make an email seem genuine—meaning attackers do their research before attempting a campaign. A quick Google search can reveal enough information about a person (job title, who they report to, what their role is) to craft a message that will prompt an employee to follow the directions inside.

These directions can request the user take a variety of actions—it might ask for a direct reply with information, it may include a link or attachment that prompts malware to be installed on an endpoint, or it could direct the user to a website where they are prompted to enter sensitive information such as a username and password.

Ultimately, it is much easier to deliver an attack that relies on human “error” than it is to hack into a system. For this reason, it’s important to have protections in place that gives visibility into and alerts on suspicious behavior.
How Carbon Black Combats Spear Phishing

VMware Carbon Black’s cloud-native endpoint protection platform (EPP) constantly monitors and records what is happening on your endpoints—offering total visibility into malicious activities. If any suspicious behavior is occurring (i.e. an application is attempting to open another application it normally wouldn’t), the Carbon Black Cloud will alert on it. If clearly malicious actions are being taken (i.e. malware is attempting to run), they will be blocked. Additionally, quick and easy attack chain visualizations help you understand the path an attacker has taken and prevent similar actions in the future.
Above is an example of how VMware Carbon Black provides this visibility into a spear phishing attack. The attack kill chain began with Outlook, which invoked Excel, which then invoked Powershell. Prevention was applied to Powershell due to the attempted invocation of malware, which is clear when looking at the associated TTPs (tactics, techniques, and procedures).
This is a prime example of how attackers are constantly innovating their spear phishing campaigns. This attack not only embedded malware, but also weaponized known-good pieces of software—like Excel documents—in an attempt to evade any signature prevention. The Carbon Black Cloud’s continuous, centralized recording saw all of this activity in real time, applied prevention when the suspicious activity became inherently malicious, and escalated the alert to administrators accordingly. This allowed them to take continued remediation steps from the console, if desired.

Alternatively, consider a situation in which an attacker sends a spear phishing email prompting the end user to visit a website that they’ve doctored to look legitimate and input their credentials. If an attacker is able to successfully harvest user credentials, the PSC is there to monitor, alert on, and prevent any malicious activity that then occurs—even when it is under the guise of a legitimate login.

Say the attacker, after successfully logging into the endpoint, tries to pull malicious code from online and run it locally—it would be blocked. Or, suppose they attempt to set up a
scheduled task that automatically makes outbound network connections to the attacker’s home IP address—this would be alerted on, allowing administrators to immediately see and evaluate the malicious nature of that activity, and launch a full scale investigation.

TO LEARN MORE AND SEE HOW YOU CAN COMBAT THREATS IN YOUR ENVIRONMENT, VISIT CARBONBLACK.COM/PSC-DEMO