Hacker-Lexikon: Was ist Phishing?

Originalveröffentlichung : www.wired.com |

-
-

Dann 1/kabelgebunden

Ihre IT-Abteilung hat ohne Zweifel gewarnt, Sie nicht, klicken auf verdächtige Links in E-mails, auch wenn die Sendschreiben ein vergnügtes Video verspricht oder aus einer scheinbar vertrauenswürdigen Quelle stammt. Wenn der Link verdächtig aussieht: tun. Nicht. Klicken Sie auf.

Und zwar deshalb, weil diese e-Mails oft Phishing-Betrügereien entwickelt, um Sie zu verleiten zu einer schädlichen Anhang anklicken oder Besuch einer manipulierten Website sind. Im letzteren Fall die Website scheinbar eine legitime Bank Website oder e-Mail Website entworfen, um den Benutzer zu betrügen, vertraulichen Informationen preiszugeben – beispielsweise ein Benutzername und ein Kennwort oder Bankkonto – oder einfach heimlich Malware auf den Computer des Opfers herunterladen kann.

Fragen Sie einfach den weißen Haus-Mitarbeiter, die offenbar auf eine Phishing-Mail, die angeblich aus dem State Department kommen geklickt und erlaubt Hackern in mehreren Regierung Netzwerke.

TL; DR: Phishing bezieht sich auf bösartige e-Mails, die entworfen sind, um den Empfänger in einen bösartigen Anhang anklicken oder Besuch einer manipulierten Website trick. Spear-Phishing ist eine gezieltere Form von Phishing, die von einem vertrauenswürdigen bekannten zu kommen scheint.

Spear-Phishing ist eine gezieltere Form des Phishing. Während gewöhnliche Phishing schädlichen e-Mails geschickt, um eine zufällige e-Mail-Konto handelt, Spear-Phishing-Mails sind entworfen, um scheinbar von jemandem stammen, der Empfänger kennt und vertraut – wie ein Kollege, Geschäftsführer oder Personalabteilung – und können eine Betreffzeile oder Inhalte, die speziell für das Opfer bekannten Interessen oder Industrie. Für wirklich wertvolle Opfer können Angreifer studieren, ihre Facebook, LinkedIn und andere social-Networking-Konten, um Erkenntnisse über ein Opfer und wählen die Namen von vertrauenswürdigen Personen in ihrem Kreis zu imitieren oder ein Thema von Interesse, um das Opfer zu locken und ihr Vertrauen gewinnen.

Mit Phishing oder Spear-Phishing e-Mail beginnen schätzungsweise 91 - Prozent von Hacker-Angriffen. Obwohl Firewalls und andere Sicherheitsprodukte auf dem Perimeter Netzwerk eines Unternehmens helfen können verhindern, dass andere Arten von bösartigen Datenverkehr in das Netzwerk gelangen – zum Beispiel durch gefährdete Ports – e-Mail gilt allgemein als legitime und vertrauenswürdige Verkehr und ist deshalb in das Netzwerk erlaubt. E-Mail-Filter Systeme kann einige Phishing-Versuche zu fangen, aber sie nicht alle von ihnen fangen. Phishing-Angriffe sind so erfolgreich, weil Mitarbeiter klicken Sie darauf mit einer alarmierenden Geschwindigkeit, auch wenn e-Mails natürlich misstrauisch sind.

Eines der berühmtesten Beispiele von Spear-Phishing-Attacke, die trotz ihrer verdächtige Natur gelang es, gezielt das RSA Security-Unternehmen im Jahr 2011.

Die Angreifer zwei verschiedene gezielte Phishing e-Mails geschickt vier Arbeiter bei RSA Muttergesellschaft EMC. Die e-Mails enthalten eine schädliche Bindung mit der Datei Name "2011 Recruitment plan.xls," enthielt einen Zero-Day-Exploit.

Wenn einer der vier Empfänger auf den Anhang geklickt, angegriffen das ausnutzen eine Sicherheitslücke in Adobe Flash, eine backdoor auf den Computer des Opfers zu installieren.

"Die e-Mail wurde gefertigt, gut genug zum Stich einer der Mitarbeiter aus ihren Junk-Mailordner abrufen, und öffnen Sie die beigefügten Excel-Datei" schrieb RSA in einem Blogpost über den Angriff.

Die Hintertür gab der Angreifer einen Fuß aus dem Aufklärung betreiben und einen Weg zu mehr wertvolle Anlagen auf das Netzwerk des Unternehmens abbilden. Es gelang ihm schließlich, Informationen in Bezug auf die Produkte des Unternehmens SecurID zwei-Faktor-Authentifizierung zu stehlen. Der Angriff war überraschend, weil jeder davon ausgegangen, dass ein Top-Security-Unternehmen wie RSA Mitarbeiter haben würde, die wissen besser als verdächtige e-Mails öffnen. Aber einer ihrer Angestellten nicht nur öffnete eines der verdächtige e-Mails aus seinem Junk-Ordner abgerufen – nach seiner e-Mail-Filter es verdächtig erachtet hatte – um ihn zu öffnen.

Eine weitere überraschende Opfer eine Spear-Phishing-Attacke war das Oak Ridge National Laboratory in Tennessee. Labor, auch im Jahr 2011 gehackt habe mit eine Phishing-Mail, die von der Personalabteilung kommen erschienen, getroffen und enthalten einen Link zu einer Webseite, wo Malware Opfer Maschinen heruntergeladen. Die Angreifer e-Mail die bis 530 des Labors 5.000 Arbeiter und siebenundfünfzig Menschen auf den bösartigen Link in der e-Mail geklickt haben. Nur zwei Maschinen wurden mit Malware infiziert, aber das war genug, um die Angreifer in das Netzwerk. Entdeckt wurden sie erst als Administratoren Megabyte an Daten aus dem Labor Netzwerk abgeschöpft wird bemerkt.

Der Hack war so überraschend, weil die Hochsicherheits-Bundes Lab eingestufte Energie und Staatssicherheit Arbeit für die Regierung, einschließlich Arbeit über nukleare Nichtverbreitung und Isotopen-Produktion führt. Jedoch das Lab, ironischerweise auch Cyber-Forschung – Arbeit, die konzentriert sich auf, unter anderem die Erforschung von Phishing-Attacken.

Zurück nach oben. Skip To: Start des Artikels.

https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/