Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Personliga bedrägerier

Inledning

Cyberkriminella fortsätter att komma på nya och kreativa sätt att lura människor. En ny typ av bedrägeri ökar i popularitet – bluffar riktade mot enskilda personer. Cyberkriminella hittar eller köper information om miljontals människor, sedan använder de informationen till anpassade attacker. Nedan visar vi dig hur dessa bedrägerier fungerar och går igenom ett vanligt exempel. Ju mer du vet om dessa bedrägerier, desto lättare är det för dig att upptäcka och stoppa dem.

Hur fungerar det?

E-post eller telefonsamtalsbluffar är inget nytt, cyberkriminella har försökt att lura människor i åratal. Exempel som "du vann lotteriet" eller de ökända nigeriabreven. Men i dessa traditionella bluffar vet cyberkriminella inte vem de angriper. De skapar helt enkelt ett generiskt meddelande och skickar ut det till miljontals människor. Eftersom dessa bluffar är så generiska, är de oftast lätta att upptäcka. En personlig bluff är annorlunda, cyberkriminella gör först en undersökning och skapar sedan ett anpassat meddelande för varje offer. De gör detta genom att samla eller köpa en databas med personers namn, lösenord, telefonnummer eller annan information. Den här typen av information är lättillgänglig på grund av alla webbplatser som har hackats. Den är också allmänt tillgänglig på sociala medier och i offentliga myndighetsregister. De kriminella angriper sedan alla de har information om.

Ett vanligt knep som cyberkriminella använder är rädsla eller utpressning för att tvinga dig till att betala dem pengar. Attacken fungerar så här. De samlar eller köper information om människors användarnamn och lösenord som erhållits från hackade webbplatser. De hittar dina kontouppgifter som ingår i en sådan databas och skickar ett e-postmeddelande till dig (och till alla andra i databasen) som innehåller en del personliga uppgifter om dig, inklusive det ursprungliga lösenordet du använde på den hackade webbsidan. De kriminella hänvisar till ditt lösenord som "bevis" för att ha hackat din dator eller enhet, vilket givetvis inte är sant. De kriminella hävdar sedan att medan de hackade din dator såg de också att du tittar på pornografi. E-postmeddelandet hotar att om du inte betalar en summa kommer de att dela bevis om pinsamma online-aktiviteter med din familj och vänner.

Tricket är, i nästan alla situationer som denna har cyberkriminella aldrig hackat ditt system. De vet inte ens vem du är eller vilka webbplatser du har besökt. Bedragaren försöker helt enkelt använda den lilla personliga informationen de har om dig för att

skrämma dig till att tro att de hackade din dator eller enhet och att lura dig att betala dem pengar. Kom ihåg, bedragarna kan även använda samma tekniker för telefonsamtalsbluffar.

Vad ska jag göra?

Inse att e-post eller telefonsamtal som dessa är en bluff. Det är naturligt att känna rädsla när någon har personlig information om dig men kom ihåg att avsändaren ljuger. Attacken är en del av en automatiserad storskalig kampanj, inte ett direkt angrepp mot dig. Det är mycket lättare för cyberkriminella idag att hitta eller köpa personliginformation, så förvänta dig mer bedrägerier riktade mot enskilda personer som dessa i framtiden. Några ledtrådar att söka efter.

- **När du får ett mycket brådskande e-post, meddelande eller telefonsamtal var mycket misstänksam. Om någon använder känslor som rädsla eller att det är brådskande, försöker de stressa dig till att göra ett misstag.**
- **När någon kräver betalning i BitCoin, presentkort eller andra metoder som inte kan spåras.**
- **När du får ett misstänkt e-postmeddelande, kan du söka på Google för att se om andra personer har rapporterat liknande attacker.**

Slutligen sunt förnuft är ditt bästa försvar. Vi rekommenderar dock att du alltid använder ett unikt, långt lösenord för var och en av dina online-konton. Kan du inte komma ihåg alla dina lösenord? Använd en lösenordshanterare. Som tillägg aktivera alltid multifaktor-autentisering när det är möjligt.

Visolit är nordens ledande specialist på molntjänster. Visolit har för närvarande Europas största och mest moderna driftsplattform för SMB-marknaden. Vi levererar allt från komplett IT-drift till enklare IT-tjänster som anpassas och integreras utifrån kundens existerande behov och infrastruktur. Med våra tjänster får små och medelstora företag tillgång till IT med en kvalitet och säkerhet som normalt är undantaget stora internationella företag. www.visolit.se eller följ oss på LinkedIn https://www.linkedin.com/company/visolit

Gästskribent

Lenny Zeltser *är en cybersecurity veteran. Han bygger anti-malware lösningar på Minerva Labs och undervisar säkerhetsklasser SANS Institute. Hans erfarenhet omfattar också managed security services och konsulttjänster. Följ honom på* zeltser.com/blog *och på Twitter* @lennyzeltser.

Källor

Social Engineering: https://www.sans.org/u/MUU
Stop That Phish: https://www.sans.org/u/MUZ
Search Yourself Online: https://www.sans.org/u/MV4
Password Manager: https://www.sans.org/u/MV9

OUCH! Publiceras av SANS Security Awareness och distribueras under Creative Commons BY-NC-ND 4.0-licens. *Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta* www.sans.org/security-awareness/ouch-newsletter. *Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Översatt av: Erik Täfvander & Johan Ahlberg*

SANS SECURITY AWARENESS
© SANS Institute 2019

Visolit