OUCH! | Styczeń 2017

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Czym jest socjotechnika
- Wykrywanie / powstrzymywanie ataku socjotechnicznego

Socjotechnika

Wstęp

W powszechnym, błędnym mniemaniu wielu osób, cyberprzestępcy używają bardzo zaawansowanych narzędzi oraz technik aby włamać się do komputerów czy kont internetowych ofiar. To nie jest prawdą. Przestępcy nauczyli się, że jednym z najprostszych sposobów aby zainfekować twój komputer, wykraść z niego informację oraz przejąć dostępy do konta jest zwyczajne oszukanie Ciebie. W tym biuletynie dowiesz się jak działają ataki określane socjotechniką, oraz co można zrobić, aby się przed nimi ochronić.

Redaktor gościnny

James Lyne (**@jameslyne**) jest certyfikowanym instruktorem SANS oraz Globalnym Szefem Badań w firmie Sophos. Uruchamia oraz analizuje najnowsze 'produkty' cyberprzestępców. Ponadto jest autorem Metasploit (SEC580) oraz Social Engineering (SEC567) wykładanych w SANS.

Czym jest Socjotechnika

Socjotechnika jest rodzajem ataku psychologicznego, której celem jest nakłonienie ofiary do wykonania szkodliwej czynności. Socjotechnika istnieje od tysięcy lat – oszustwa i naciągacze to przecież nic nowego. Dzisiejsza technologia sprawia jednak, że atakujący staje się anonimowy, mogąc podawać się przy tym za kogokolwiek oraz kierując atak na miliony użytkowników, także na Ciebie. Ponadto współczesne ataki są w stanie pokonać wiele zabezpieczeń. Najprostszym sposobem, aby zrozumieć jak działa inżynieria społeczna, jest przyjrzenie się przykładom z życia.

Odbierasz telefon od kogoś podającego się za pracownika serwisu komputerowego, dostawcę usług internetowych albo wsparcie techniczne Microsoft. Rozmówca wyjaśnia, że Twój komputer aktywnie skanuje sieć, co może mieć związek z działaniem szkodliwego oprogramowania. Następnie w celu przekonania, używa niezrozumiałych dla Ciebie pojęć. Zaleca sprawdzenie plików w systemie, tłumacząc jak to zrobić. Odnalezione pliki to dowód na to, że komputer jest zainfekowany, w rzeczywistości są to zwyczajne pliki systemowe. Kiedy atakującemu uda się przekonać Cię, że Twój komputer jest zainfekowany, będzie nakłaniać do odwiedzenia ich strony i zakupu oprogramowania zabezpieczającego lub poprosi o zdalne nadanie dostępu do komputera w celu usunięcia problemu. Sprzedawany program to w rzeczywistości wirus. Jeżeli dałeś namówić się na zakup to nie dość, że zainfekowałeś swój komputer, ale nawet za to zapłaciłeś! Jeśli pozwoliłeś na zdalny dostęp do komputera, przestępca zainfekuje go samodzielnie a potem przejmie nad nim kontrolę.

Socjotechnika

Kolejnym przykładem jest atak określany jako ‘atak na dyrektora’, zdarza się on często w miejscu pracy. Atakujący analizuje Twoją firmę w sieci ustalając nazwiska Twoich współpracowników oraz przełożonych. Sporządzane są adresy e mail imitujące osoby z Twojego środowiska. Z nich otrzymujesz wiadomość w której jesteś pilnie proszony o podjęcie działania: zlecenie przelewu lub przekazanie poufnych informacji. Bardzo często wiadomość ze względu na stan wyjątkowy informuje o konieczności odstępstw od zwyczajnego trybu, np. jesteś proszony o wysłanie poufnych danych na prywatną skrzynkę @gmail.com. Niebezpieczeństwem w tego typu atakach jest wcześniejsze rozpoznanie firmy przez przestępców. Zabezpieczenia w firmach często nie wykrywają takich ataków ponieważ nie wykorzystują one złośliwego oprogramowania czy linków.

W przypadku socjotechniki Twój trzeźwy osąd sytuacji jest w stanie zidentyfikować a także powstrzymać większość ataków.

Miej na uwadze, że ataki socjotechniczne nie ograniczają się tylko do telefonów lub maili; mogą wykorzystywać także wiadomości sms, media społecznościowe czy nawet osoby. Kluczem do skutecznej obrony jest zrozumienie intencji atakującego.

Wykrywanie/powstrzymywanie ataku socjotechnicznego

Na szczęście powstrzymanie tego typu ataków jest prostsze niż myślisz – przytomne myślenie jest Twoim najlepszym sposobem obrony. Jeśli coś jest wydaje Ci się podejrzane, lub jest inne niż zazwyczaj, to może być atak. Najczęściej spotykane elementy socjotechniki to:

- Ktoś próbuje stworzyć poczucie sytuacji wyjątkowej, przestępcy liczą na to, że popełnisz wtedy błąd.
- Ktoś próbuje uzyskać informacje do których nie powinien mieć dostępu lub które powinien znać, np. numery kont.
- Ktoś prosi o Twoje hasła dostępu, żadna organizacja nigdy tego nie robi.
- Ktoś nakłania Cię do zignorowania procedur lub procesów bezpieczeństwa w organizacji.
- Coś jest zbyt piękne żeby było prawdziwe. Na przykład wygrałeś iPada na loterii w której nie brałeś udziału.
- Odebrałeś wiadomość od przyjaciela bądź kolegi z pracy, zawierający wyrażenia, których zwykle nie używa. Przestępcy mogli przejąć jego konto i próbują Cię zwieść. W przypadku podejrzeń spróbuj skontaktować się z nim inną drogą np. przez telefon.

Socjotechnika

Jeśli podejrzewasz, że ktoś próbuję Cię atakować, nie komunikuj się więcej z tą osobą. Jeśli atak ma związek z Twoją pracą, upewnij się, że poinformowałeś o tym odpowiednie osoby w organizacji. Pamiętaj, zdrowy rozsądek jest Twoją najlepszą obroną.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego.

Odwiedź securingthehuman.sans.org/ouch/archives i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: http://www.cert.pl

Twitter: @CERT_Polska

Facebook: http://facebook.com/CERT.Polska

Źródła

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
CEO Fraud:	https://securingthehuman.sans.org/ouch/2016#july2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Archives:	https://securingthehuman.sans.org/ouch/archives

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Małgorzata Dębska, Przemysław Zielony, Sebastian Kondraszuk