Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

- Co to jest spear phishing
- Skuteczność spear phishingu
- Jak się chronić

Spear phishing

Co to jest spear phishing?

Możliwe że miałeś już do czynienia z phishingiem. Są to wiadomości e-mail wysyłane przez cyberprzestępców do milionów potencjalnych ofiar na całym świecie, które mają na celu je oszukać, nabrać lub zaatakować. Zazwyczaj wiadomości te wydają się pochodzić z zaufanego źródła, np. z banku lub od kogoś znajomego. E-maile często zawierają pilną wiadomość lub specjalną ofertę dla Ciebie, tak dobrą, że żal byłoby z niej nie skorzystać. Jeśli klikniesz na link w takiej wiadomości phishingowej, możesz zostać zabrany do złośliwej strony internetowej, która będzie próbowała włamać się do Twojego komputera albo pozyskać Twój login i hasło. Wiadomość e-mail z phishingiem może też posiadać zainfekowany załącznik, który po otwarciu będzie próbował zainfekować i przejąć kontrolę nad Twoim komputerem. Cyberprzestępcy wysyłają te wiadomości do możliwie największej liczby osób, wiedząc, że im więcej osób je otrzyma, tym więcej będzie ich potencjalną ofiarą.

Redaktor gościnny

Lenny Zeltser jest redaktorem gościnnym tego wydania OUCH! Zajmuje się zabezpieczaniem procesów IT w firmie NCR Corp oraz naucza sposobów walki ze złośliwym oprogramowaniem w Instytucie SANS. Lenny jest aktywnym użytkownikiem Twittera (**@lennyzeltser**) oraz prowadzi blog o bezpieczeństwie pod adresem **http://blog.zeltser.com**.

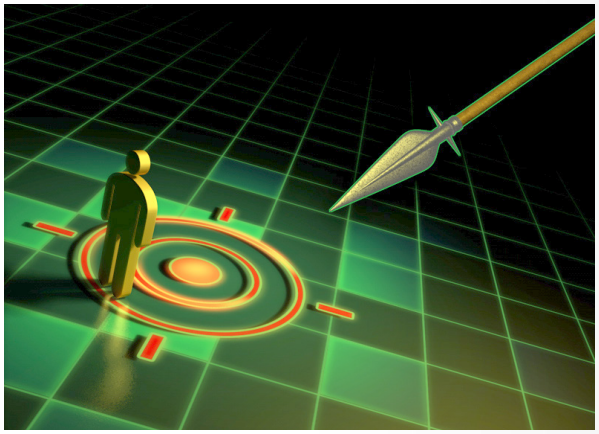
Chociaż zwykły phishing jest wciąż skuteczny, pojawił się nowy rodzaj ataku o nazwie spear phishing. Koncepcja jest taka sama: przestępcy wysyłają e-maile do swojej ofiary, udając znaną jej organizację lub zaufaną osobę. Jednak w przeciwieństwie do tradycyjnego phishingu, treść tych wiadomości jest wyraźnie ukierunkowana. Zamiast wysyłać e-maile do milionów potencjalnych ofiar, cyberprzestępcy wysyłają wiadomości spear phishingowe (czyli ukierunkowane od ang. sprear - włócznia) do nielicznych, wybranych osób. W przeciwieństwie do zwykłego phishingu, stosując phishing ukierunkowany atakujący przeprowadza wywiad środowiskowy potencjalnych ofiar. Zapoznaje się z treścią profilu na LinkedIn czy Facebooku lub wiadomościami jakie zostały zamieszczone na publicznych blogach albo forach. Na podstawie takiego rozpoznania, przestępcy tworzą spersonalizowaną wiadomość e-mail, której treść wydaje się być zupełnie sensowna dla potencjalnego celu ataku. Takie działanie sprawia, że odbiorcy wiadomości łatwiej stają się ofiarami ataku.

Skuteczność spear phishingu

Spear phishing jest wykorzystywany kiedy cyberprzestępca chce przeprowadzić atak konkretnie na Ciebie lub na Twoją organizację. Inaczej niż w przypadku zwykłych przestępców chcących ukraść pieniądze, osoba wykorzystująca spear phishing ma bardzo konkretne cele. Zazwyczaj jest to uzyskanie dostępu do poufnych informacji, takich jak tajemnice handlowe, projekty technologii, czy kanały informacyjne w instytucjach rządowych.

Spear phishing

Może się też zdarzyć tak, że próby włamania do Twojej organizacji są jednym z etapów uzyskania dostępu do innej organizacji. Przestępcy stosujący takie techniki grają o dużą stawkę i są w stanie poświęcić czas i energię aby przeprowadzić wyczerpujące śledztwo przed atakiem.



Najlepszym sposobem ochrony przed spear phishingiem jest świadomość, że Ty też możesz stać się jego celem, rozważne publikowanie informacji o sobie oraz zgłaszanie podejrzanych wiadomości.

Na przykład zagraniczny rząd może dojść do wniosku, że Twoja firma opracowuje produkt lub technologię, która jest kluczem do ich sukcesu gospodarczego i zacząć się Tobą interesować. Sprawdzają dokładnie stronę internetową Twojej organizacji i wybierają sobie trzy kluczowe osoby. Następnie wnikliwe badają strony tych osób na LinkedIn, Twitterze i Facebooku aby stworzyć jak najobszerniejszy zbiór informacji o nich. Po przeanalizowaniu wszystkich zebranych informacji o tych wybranych osobach, atakujący przygotowują wiadomość e-mail podając się za dostawcę, z którym organizacja rzeczywiście współpracuje. E-mail zawiera załącznik udający fakturę, który w rzeczywistości jest zainfekowanym plikiem. Dwie z trzech osób, na które był ukierunkowany atak, dają się oszukać przez spear phishingowy e-mail i otwierają zainfekowany załącznik, dając tym samym obcemu rządowi całkowity dostęp do swoich komputerów, a ostatecznie do wszystkich sekretów produktów Twojej organizacji, które teraz będą sami produkować.

Ataki typu spear phishing są znacznie bardziej niebezpiecznym zagrożeniem niż proste ataki typu phishing, ponieważ atakujący przeprowadzają atak ukierunkowany konkretnie na Ciebie i Twoją organizację. To znacznie zwiększa szanse na sukces atakujących. Te ataki są także o wiele trudniejsze do wykrycia.

Jak się chronić

Pierwszym krokiem do ochrony siebie przed atakami ukierunkowanymi jest zrozumienie, że Ty też możesz stać się jego celem. Prawdopodobnie zarówno Ty, jak i Twoja organizacja jesteście w posiadaniu poufnych informacji, na których mogłoby komuś zależeć albo takich, które mogłyby być wykorzystane do dostępu do innej organizacji, która mogłaby być ostatecznym celem ataku. Kiedy zdasz sobie sprawę, że Ty sam też możesz być celem, podejmij następujące środki ostrożności w celu ochrony siebie i swojej organizacji:

- Ogranicz informacje jakie o sobie umieszczasz w takich miejscach jak fora, Facebook czy LinkedIn. Im większą ilością danych się dzielisz, tym łatwiej atakującemu przygotować spear phishingowy e-mail, który będzie wydawał się sensowny i prawdziwy.

Spear phishing

- Jeśli otrzymasz podejrzaną wiadomość e-mail, w której ktoś prosi aby otworzyć załącznik, kliknąć w link albo żąda podania poufnych informacji, dobrze sprawdź wiadomość zanim wykonasz te czynności. Jeśli e-mail wydaje się pochodzić od firmy lub osoby którą znasz, skorzystaj ze swojej własnej książki adresowej aby skontaktować się z nadawcą i sprawdzić czy to na pewno on wysłał tą wiadomość.
- Wesprzyj swoją organizację w działaniach mających na celu zwiększenie bezpieczeństwa. Stosuj się do obowiązującej polityki bezpieczeństwa i korzystaj z dostępnych narzędzi zabezpieczających, takich jak programy antywirusowe, szyfrowanie i aktualizacje.
- Pamiętaj, że technologia nie jest w stanie wyłapać i zapobiec wszystkim atakom wykorzystującym e-mail, a zwłaszcza ukierunkowanym wiadomościom spear phishingowym. Jeśli na pierwszy rzut oka e-mail wydaje Ci się nieco dziwny, przeczytaj go bardzo uważnie. Jeśli masz najmniejszą obawę, że otrzymałeś właśnie e-mail z phishingiem lub jeśli padłeś ofiarą phishingu ukierunkowanego, natychmiast skontaktuj się z działem help desk lub zespołem bezpieczeństwa w swojej organizacji.

Dowiedz się więcej

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org 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

Ataki typu „spear phishing” (pl): http://pl.norton.com/spear-phishing-scam-not-sport/article

OUCH! Email i ataki typu phishing (pl): http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_po.pdf

Zalecenia dot. ataków ukierunkowanych (pl): http://www.cert.gov.pl/portal/cer/8/118

Jak nie zostać ofiarą spear phishingu (ang): http://www.theatlanticwire.com/technology/2013/02/spear-phishing-security-advice/62304/

Unikanie ataków z wykorzystaniem socjotechniki i phishingu (ang): http://www.us-cert.gov/ncas/tips/st04-014

Słownik pojęcia bezpieczeństwa SANS (ang): http://www.securingthehuman.org/resources/security-terms

Porada dnia SANS (ang.): https://www.sans.org/tip_of_the_day.php

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski