Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Tak, Ty też jesteś celem

Wstęp

Powszechnym i zupełnie błędnym mniemaniem wielu ludzi jest to, że nie są oni celem działań cyberprzestępczych: że oni lub ich komputery nie mają dla nikogo żadnej wartości. Nic bardziej mylnego. Jeśli posiadasz komputer, urządzenie mobilne, konta internetowe, adresy e-mail, karty kredytowe, lub angażujesz się w inny rodzaj działalności online, stanowisz jakąś wartość dla cyberprzestępców. W tym biuletynie postaramy się wyjaśnić dlaczego jesteś celem, jak jesteś atakowany oraz to, co możesz zrobić, aby się przed atakami ochronić.

Redaktor gościnny

Eric Conrad jest prezesem i CTO Backshore Communications oraz autorem książek: CISSP Study Guide (drugie wydanie) i Eleventh Hour CISSP (drugie wydanie). Jest także współautorem sześciodniowego kursu SANS "Continuous Monitoring and Security Operations" (SEC511).

Dlaczego Ty też jesteś celem?

Takie przestępstwa jak oszustwa, kradzież tożsamości czy wymuszenia towarzyszą ludziom od kiedy zaczęły istnieć cywilizacje i niezależnie od wszystkiego są częścią naszego codziennego życia. Celem przestępców od zawsze było to samo: zarobić możliwie jak najwięcej przy minimalnym ryzyku. Próby dokonania tego w sposób tradycyjny były dosyć trudne, ponieważ przestępcy często byli ograniczeni do działań w danej lokalizacji i konieczna była fizyczna interakcja z ich potencjalnymi ofiarami. To nie tylko zawężało krąg osób, które przestępcy decydowali się zaatakować, ale także narażało ich na duże ryzyko. Jednakże przestępczość radykalnie zmieniła się wraz z pojawieniem się Internetu i nowych technologii komunikacji. Teraz cyberprzestępcy mogą z łatwością wziąć sobie za cel niemal każdego na świecie, w dodatku przy bardzo niskim lub zerowym koszcie i niewielkim ryzyku. Dodatkowo cyberprzestępcy stali się bardzo dobrze zorganizowani i efektywni, co pozwala im być bardziej skutecznymi niż kiedykolwiek.

Grupy przestępcze działające w sieci wiedzą, że im więcej haseł i danych kart kredytowych wykradną, na im więcej kont bankowych się włamią, tym więcej pieniędzy będą mogli sobie przywłaszczyć. Dlatego będą próbować włamać się dosłownie na każdy komputer podłączony do Internetu, w tym również Twój. Złamanie zabezpieczeń na komputerach milionów ludzi na całym świecie może się wydawać czymś niemożliwym lub wymagającym dużego wysiłku, a jednak jest zaskakująco proste przy użyciu zautomatyzowanych narzędzi, które wykonują całą pracę za przestępców. Na przykład mogą oni zbudować bazę danych składającą się z milionów adresów e-mail i wówczas użyć automatycznego narzędzia do wysyłania wiadomości na każdy z tych adresów, która zawiera próbę oszustwa. Wysłanie takich wiadomości e-mail nie kosztuje przestępców prawie nic: aby wykonywać swoją brudną robotę wykorzystują oni po prostu inne przejęte komputery, być może także i Twój.

Tak, Ty też jesteś celem

Jest to kolejny przykład, dlaczego Twoje urządzenia mają dla przestępców wartość, w najgorszym dla nich wypadku zawsze mogą zostać użyte, aby zaatakować urządzenia należące do kogoś innego. Przestępcy nie wiedzą, kto padnie ofiarą ich ataków w postaci wiadomości email, ale wiedzą, że im więcej e-maili zostanie wysłanych, tym więcej ich będzie. Może być też tak, że przestępcy będą dosłownie skanować każdy komputer w Internecie (i tym razem wykorzystując do tego inne przejęte komputery), szukając miejsc, na które mogą się włamać. Pamiętaj, nie zostałeś wybrany na cel ataku z jakiegoś szczególnego powodu. Wręcz przeciwnie, przestępcy celują w każdego w kogo tylko mogą, i tak się składa, że włącznie z tobą.

Możesz nie zdawać sobie z tego sprawy ale Twoje urządzenia i informacje o Tobie mają ogromną wartość dla cyberprzestępców na całym świecie.

Jak się chronić?

Gdy cyberprzestępcy próbują przejąć komputery ludzi na całym świecie, zazwyczaj robią to za pomocą stosunkowo prostych metod. Na szczęście, wykonując kilka prostych kroków, możesz znacznie poprawić swoje bezpieczeństwo. Oto nasze zalecenia:

- **Ty**: Jakkolwiek na to nie spojrzeć, jesteś pierwszą linią ochrony przed wszelkimi cyberatakami. Wiele z nich zaczyna się zwykłą próbą oszustwa czy nabrania cię, jak na przykład próba nakłonienia do otwarcia zainfekowanego załącznika w wiadomości e-mail lub podania jakiegoś hasła przez telefon. Zdrowy rozsądek jest najlepszą obroną: jeśli coś wydaje się być dziwne, podejrzane lub zbyt piękne, aby mogło być prawdziwe, to najprawdopodobniej to właśnie jest próba ataku na ciebie.

- **Aktualizacje** : Upewnij się, że każdy komputer lub urządzenie mobilne z którego korzystasz jest w pełni zaktualizowane i zawiera wszystkie najnowsze poprawki. Jest to ważne nie tylko w przypadku systemu operacyjnego, ale dla każdej aplikacji lub wtyczki których używasz. Mając swoje systemy i aplikacje zawsze zaktualizowane chronisz się przed najbardziej typowymi atakami.

- **Hasła**: Używaj silnych i różnych haseł dla każdego z kont. W ten sposób, nawet gdy dana strona internetowa zostanie przejęta przez cyberprzestępców i wszystkie hasła do niej również (w tym Twoje), reszta Twoich kont pozostanie bezpieczna. Upewnij się też, że wszystkie Twoje urządzenia są chronione przez silne, unikalne hasło, PIN lub innego rodzaju mechanizm blokujący. Aby bezpiecznie przechowywać różne hasła zalecamy korzystanie z menedżera haseł.

- **Karty kredytowe**: Sprawdzaj swój wyciąg z karty często, zalecamy robić to co najmniej raz w tygodniu (co miesiąc to zdecydowanie za mało). Jak tylko zauważysz jakąś nieautoryzowaną transakcję na karcie kredytowej,

Tak, Ty też jesteś celem

niezwłocznie zgłoś się do wystawcy karty. Jeśli Twój bank pozwala ustawić powiadomienia e-mail lub SMS dla dużych lub dziwnych transakcji, korzystaj z nich dla jeszcze szybszego dowiedzenia się o podejrzanych działaniach.

- **Sieć**: Zabezpiecz swój domowy punkt dostępu Wi-Fi silnym hasłem administratora i upewnij się że Twoja sieć Wi-Fi wymaga hasła, aby ktoś mógł się do niej przyłączyć. Zawsze bądź świadomy jakie urządzenia zostały podłączone do Twojej sieci domowej i pamiętaj aby były one zaktualizowane.

- **Media społecznościowe**: Im więcej informacji zamieszcza się o sobie w Internecie tym częściej można wystawić się na ryzyko. Dzięki nim cyberprzestępcom jest nie tylko łatwiej oszukać cię, ale wszelkie informacje które zamieszczasz mogą potencjalnie zidentyfikować Cię jako bardziej wartościowy cel.

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 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

Źródła

OUCH! Manadżer haseł:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Zabezpiecz swoją domową sieć:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Ataki Phishingowe:	http://www.securingthehuman.org/ouch/2013#february2013
Plakat: Jesteś Celem:	http://www.securingthehuman.org/resources/posters

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