OUCH! | Kwiecień 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

Zhakowali mnie, co dalej?

Wstęp

Każdemu z nas zależy na tym, żeby komputer i urządzenia mobilne oraz informacje, które zawierają były bezpieczne i podejmujemy w tym celu odpowiednie kroki. Czasami jednak, nieważne jak dobrze i bezpiecznie posługujesz się nowymi technologiami, nadal możesz paść ofiarą ataku. W tym biuletynie znajdziesz informacje o tym jak wykryć taki atak i jakie kroki podjąć później. Najważniejszy w tym przypadku jest czas - im szybciej wykryjesz włamanie i podejmiesz odpowiednie kroki, tym mniej szkody wyrządzi atakujący.

Redaktor gościnny

Samantha Davison (**@sam_e_davison**) jest menedżerem programu dotyczącego edukacji i podnoszenia poziomu świadomości kwestii związanych z cyberbezpieczeństwem w firmie Uber. Jej program obejmuje wszystkich pracowników w ponad 350 miastach na całym świecie.

Co wskazuje na udany atak

To czy zostałeś zhakowany może czasem być trudne do określenia. Przestępcy mogą to zrobić na wiele sposobów i zwykle też pozostawiają jakieś ślady, które możesz znaleźć. Poniżej przedstawiamy zbiór wskazówek. Jeśli znajdziesz kombinację kilku z nich, możesz być pewien, że padłeś ofiarą włamania.

- Twój program antywirusowy zgłosił infekcję na komputerze. Szczególną uwagę należy zwrócić, gdy program nie był w stanie usunąć zainfekowanych plików bądź przenieść ich do kwarantanny.
- Strona domowa Twojej przeglądarki internetowej jest inna niż zwykle lub przeglądarka wchodzi na strony bez interakcji z Twojej strony.
- W systemie operacyjnym znajdują się konta użytkowników, których nie utworzyłeś lub zauważasz, że w systemie operacyjnym uruchomione są programy, których sam nie instalowałeś.
- Programy na Twoim komputerze często się zawieszają oraz co chwilę wyskakują dziwne okna aplikacji.
- Jakiś program domaga się uwierzytelnienia dla konta administratora w celu wykonania zmian w systemie operacyjnym, pomimo tego, że nie robisz w tym momencie żadnej aktualizacji i nie instalujesz nowych aplikacji.
- Hasło logowania do systemu lub kont online przestało działać pomimo, że masz 100% pewność, że jest poprawne.
- Znajomi zgłaszają Ci, że wysyłasz bardzo dużo spamu, chociaż wiesz, że nic takiego nie robiłeś.
- Twoje urządzenie mobilne samo wysyła SMSy na numery premium.
- Twoje urządzenie mobilne generuje dużo ruchu sieciowego oraz jego bateria znacznie szybciej się wyczerpuje niż uprzednio.

Zhakowali mnie, co dalej?

Zhakowali mnie - co robić, jak żyć?

Jeśli jesteś przekonany, że ktoś uzyskał nieautoryzowany dostęp do Twojego komputera, podejmij odpowiednie działania najszybciej jak tylko możesz. Jeśli komputer lub urządzenie mobilne należy do pracodawcy, bądź było wykorzystywane do pracy, nie staraj się naprawić problemu własnoręcznie. Nie tylko możesz pogorszyć stan infekcji, ale także zatrzeć cenne ślady, które mogą prowadzić do sprawcy. Zgłoś incydent do np. zespołu help-desk w dziale IT, specjalnego zespołu ds. bezpieczeństwa IT lub bezpośrednio do swojego przełożonego. Jeśli z jakichś powodów nie możesz tego zrobić, albo obawiasz się, że pracodawca nie zareaguje odpowiednio szybko, odłącz urządzenie mobilne lub komputer od sieci i przenieś je w stan uśpienia, hibernację lub tzw. tryb samolotowy (dla urządzeń mobilnych). Nawet jeśli nie jesteś do końca pewien czy atak rzeczywiście miał miejsce, lepiej zgłosić swoje podejrzenia. Twój pracodawca z pewnością jest przygotowany na taką sytuację i poradzi sobie z tym lepiej niż Ty sam. Jeśli jednak chodzi o Twój prywatny komputer, to poniżej znajduje się kilka podpowiedzi, które pomogą Ci walczyć z infekcjami.

Prędzej czy później ktoś zainfekuje Twój komputer. Im szybciej wykryjesz taki incydent i zareagujesz, tym mniejszą przewagę ma cyberprzestępca.

- **Zmiana haseł**. Pamiętaj, żeby zmienić wszystkie swoje hasła. Nie tylko hasła, których używasz do logowania na komputerze czy innych urządzeniach, ale także te do serwisów internetowych. Pamiętaj, aby robić to z innego komputera, o którym wiesz, że jest bezpieczny.
- **Program antywirusowy**. Jeśli program antywirusowy powiadomił Cię o infekcji, najlepiej jest wykonać kroki, które doradza. Zwykle program zaleci kwarantannę podejrzanego pliku, usunięcie infekcji z pliku lub usunięcie całego pliku. Większość programów antywirusowych również udostępnia link do strony, gdzie znajdziesz informacje na temat wykrytego zagrożenia. Jeśli nie wiesz co robić, najlepiej przenieś plik do kwarantanny. Jeśli nie jest to możliwe, usuń go.
- **Powtórna instalacja**. Jeśli program antywirusowy nie jest w stanie usunąć infekcji, najbezpieczniejszym działaniem, które możesz podjąć jest powtórna instalacja systemu operacyjnego. Po pierwsze, odłącz komputer od sieci. Następnie postępuj zgodnie z instrukcjami producenta, co najczęściej oznacza zainstalowanie systemu z partycji odzyskiwania (“recovery”). Jeśli nie masz takiej partycji, jest ona zainfekowana albo nie masz do niej dostępu, skontaktuj się z producentem, aby otrzymać płytę DVD z systemem operacyjnym. Nie instaluj systemu operacyjnego z kopii bezpieczeństwa. Mogą one zawierać te same błędy, które pomogły atakującemu uzyskać dostęp do Twojego komputera. Z kopii bezpieczeństwa powinieneś tylko odzyskiwać swoje prywatne dane. W przypadku urządzeń mobilnych, często jedyną metodą jest przywrócenie ustawień fabrycznych i całkowity reset urządzenia. Jeśli nie czujesz się komfortowo wykonując te procedury, zastanów się czy nie poprosić o pomoc profesjonalisty. Jeśli

Zhakowali mnie, co dalej?

Twój komputer jest już stary, to często prostszym, a nawet czasem tańszym, rozwiązaniem jest kupno nowego niż spędzenie kilkunastu godzin na próbie ponownej instalacji systemu operacyjnego.

- **Kopie bezpieczeństwa**. Najważniejszym z kroków, które pomogą Ci się przygotować na wypadek włamania są właściwie robione kopie bezpieczeństwa. Muszą być robione regularnie oraz trzeba sprawdzać czy zostały wykonane poprawnie i czy da się przywrócić dane w nich zawarte. Dosyć często okazuje się, że po infekcji trzeba usunąć wszystkie dane z komputera i zainstalować system operacyjny na nowo. W takiej sytuacji kopie bezpieczeństwa pomogą Ci przywrócić Twoje osobiste dane.
- **Policja**. Jeżeli uważasz, że padłeś ofiarą cyberprzestępców, zgłoś zawiadomienie o popełnieniu przestępstwa w jednostce Policji lub w prokuraturze, najlepiej najbliższej Twojego miejsca zamieszkania lub miejsca, w którym w danym momencie się znajdujesz.

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

Źródła

Backup i odzyskiwanie danych:	https://securingthehuman.sans.org/ouch/2015#august2015
Nowe oblicze hasła:	https://securingthehuman.sans.org/ouch/2015#april2015
Czym jest złośliwe oprogramowanie:	https://securingthehuman.sans.org/ouch/2016#march2016
Zabezpiecz swój nowy tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

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