OUCH! | maj 2014

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Co zrobić po włamaniu?

Informacje ogólne

Każdemu z nas zależy na tym, żeby komputer, jak i informacje, które zawiera, były bezpieczne i podejmujemy w tym celu odpowiednie kroki. Jednak, analogicznie jak w przypadku jazdy samochodem, nieważne jak dobrze prowadzisz i tak możesz być ofiarą wypadku. W tym biuletynie znajdziesz informacje na temat dowodów, które pozwolą Ci odkryć włamanie i informacje co zrobić później. Najważniejszy w tym przypadku jest czas - im szybciej wykryjesz włamanie i podejmiesz odpowiednie kroki, tym mniej szkody wyrządzi atakujący.

Redaktor gościnny

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) jest Głównym Naukowcem w CSRgroup Computer Security Consultants. Jest również współautorem dwóch kursów instytutu SANS: Memory Forensic (FOR526) oraz Malware Reverse Engineering (FOR610).

Dowody włamania (IoC)

Musisz zrozumieć, że nie istnieje jedna złota reguła, która powie Ci, że Twój komputer został skompromitowany. Za każdym razem jest to kilka dowodów, które możesz znaleźć. Jeśli znajdziesz kombinację z nich, możesz być pewien, że padłeś ofiarą włamania. Poniżej znajduje się kilka przykładów takich dowodów.

- Twój program antywirusowy zgłosił infekcję na komputerze. Szczególnie należy zwrócić na to uwagę, gdy program nie był w stanie usunąć infekcji bądź przenieść jej 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.
- Zauważasz, że w systemie operacyjnym zainstalowane są programy, których sam nie instalowałeś.
- Komputer znacząco spowolnił, albo wręcz zaczyna się zacinać.
- Program prosi Ciebie o dostęp do komputera z prawami administratora pomimo, że nic nie instalujesz ani nie aktualizujesz.
- Twoja zapora sieciowa ostrzega cię, że nowy program próbuje uzyskać dostęp do sieci.

Co zrobić?

Jeśli jesteś przekonany, że ktoś uzyskał nieautoryzowany dostęp do Twojego komputera, podejmij odpowiednie działania najszybciej jak możesz. Jeśli komputer należy do pracodawcy, bądź był wykorzystywany do pracy, nie staraj

Co zrobić po włamaniu?

się naprawić problemu samemu i nie wyłączaj komputera. Nie tylko możesz pogorszyć stan infekcji, ale także możesz zatrzeć cenne ślady, które mogą prowadzić do sprawcy. Skontaktuj się natychmiast z pracodawcą, na przykład za pomocą help desku w dziale IT lub swojego przełożonego. Jeśli z jakiś powodów nie możesz tego zrobić, albo obawiasz się, że pracodawca nie zareaguje odpowiednio szybko, odłącz komputer od sieci i przenieś go w stan uśpienia bądź w hibernację. Nawet jeśli nie jesteś do końca pewien swoich wniosków, 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 atakujący.

- **Kopie bezpieczeństwa**. Najważniejszym z kroków, które pomogą Ci się przygotować na wypadek włamania są właściwie robione kopie bezpieczeństwa. Muszą one być robione regularnie oraz trzeba sprawdzać czy zostały wykonane poprawnie i 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 lub wręcz trzeba kupić nowy komputer. W takiej sytuacji kopie bezpieczeństwa pomogą Ci przywrócić Twoje osobiste dane.
- **Zmiana haseł**. Pamiętaj, żeby zmienić wszystkie swoje hasła. Nie tylko hasła, które używasz do logowania się na komputer czy inne urządzenia, ale także wszystkie hasła 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 to nie jest możliwe, usuń go.
- **Powtórna instalacja**. Jeśli program antywirusowy nie jest w stanie usunąć infekcji, najbezpieczeniejszym działniem, 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

Co zrobić po włamaniu?

atakującemu uzyskać dostęp do Twojego komputera. Z kopii bezpieczeństwa powinieneś tylko odzyskiwać swoje prywatne dane. Jeśli komputer jest stary, to często prostszym, a nawet czasem tańszym, rozwiązaniem jest kupno nowego niż spędzenie kilkunastu godzin na próbie ponownej instalacji systemu opracyjnego.

- **Profesjonalna pomoc**. Jeśli podejrzewasz, że przejęto kontrolę nad Twoim komputerem, a nie masz odpowiednich umiejętności, aby naprawić infekcję, oddaj swój komputer w ręce profesjonalisty. Może się też okazać, że Twoje kopie bezpieczeństwa są w stanie, który nie pozwala na ich przywrócenie. W takiej sytuacji możesz chcieć przegrać pliki takie jak zdjęcia, dokumenty czy filmy pomiędzy zainfekowaną maszyną a nowym komputerem. Jednak wtedy grozi Ci również to, że razem z plikami przeniesiesz także infekcję. Zdecydowanie bezpieczniej jest oddać komputer w ręce profesjonalisty, który przeniesie pliki bez ryzyka przeniesienia infekcji.

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

OUCH! Backup i przywracanie osobistych danych:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#september2013
OUCH! Hasła:
http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Czym jest złośliwe oprogramowanie:
http://www.securingthehuman.org/ouch/2014#february2014

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