OUCH! | sierpień 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- Czym jest Ransomware
- Czy płacić okup?
- Kopie zapasowe
- Dalsze sposoby ochrony

Ransomware

Czym jest Ransomware?

Ransomware jest specjalnym rodzajem złośliwego oprogramowania, które aktywnie rozprzestrzenia się w Internecie, grożąc zniszczeniem dokumentów i innych plików należących do ofiary. Złośliwe oprogramowanie, zwane też malware, to program komputerowy napisany w celu wykonywania szkodliwych działań. Ransomware jest jednym z rodzajów malware'u, który stał się w ostatnim czasie bardzo popularny ze względu na dochodowość, jaką przynosi przestępcom. Ransomware, po zainfekowaniu Twojego komputera, szyfruje wybrane pliki, a w niektórych przypadkach nawet cały dysk. W rezultacie Twój komputer lub dostęp do ważnych plików, takich jak dokumenty lub zdjęcia, zostaje zablokowany, a ransomware żąda zapłacenia okupu przestępcom w zamian za odszyfrowanie danych i odzyskanie dostępu do komputera (ang. ransom - okup, ang. software - oprogramowanie, stąd nazwa ransomware). Najczęściej, okup musi być wpłacony w postaci kryptowaluty, np. Bitcoin. Ransomware rozprzestrzenia się tak jak wiele innych rodzajów złośliwego oprogramowania. Najpopularniejszą metodą dystrybucji ransomware jest wysyłka złośliwych maili, w których cyberprzestępcy nakłaniają odbiorcę do otwarcia złośliwego załącznika lub kliknięcia w link prowadzący do strony przestępcy.

Redaktor gościnny

Lenny Zeltser zajmuje się zabezpieczeniami IT w firmie NCR Corp. oraz prowadzi wykłady poświęcone walce ze złośliwym oprogramowaniem w Instytucie SANS. Jest aktywnym użytkownikiem Twittera (**@lennyzeltser**) oraz prowadzi blog poświęcony bezpieczeństwu - **zeltser.com**.

Czy płacić okup?

Jest to trudne pytanie. Problemem jest, że im częściej ludzie będą płacić okup przestępcom, tym bardziej będą oni zmotywowani do infekowania kolejnych użytkowników. Z drugiej strony możesz nie mieć innej możliwości odzyskania swoich plików. Bądź jednak ostrożny. Jeśli nawet zapłacisz okup nie masz gwarancji, że odzyszkasz swoje dane. Masz w końcu do czynienia z przestępcami, którzy mogą nie odszyfrować Twoich plików, lub nawet jeśli dostaniesz w zamian za okup narzędzia do odszyfrowania, coś może pójść nie tak w trakcie procesu deszyfrowania. Niewykluczone, że Twój komputer może być zainfekowany dodatkowym złośliwym oprogramowaniem.

Rób kopie zapasowe swoich plików

Być może najlepszym sposobem na odzyskanie sprawnego systemu, bez płacenia okupu, po infekcji ransomware'm byłoby przywrócenie plików z kopii zapasowych. W tym przypadku, nawet jeśli zostałeś ofiarą złośliwego oprogramowania, masz mozliwość odzyskania plików po wyczyszczeniu komputera. Miej jednak na uwadze, że jeśli Twoja kopia zapasowa była

Ransomware

dostępna z zainfekowanego komputera, ransomware mógł skasować lub zaszyfrować pliki kopii zapasowej. Dlatego ważne jest, aby backup tworzony był w “chmurach” lub na zewnętrznych dyskach, które nie są na stałe podłączone do systemu. Ponadto, częstym błędem popełnianym przez osoby tworzące kopie zapasowe jest przekonanie, że uda im się przywrócić dane bez faktycznego sprawdzenia, czy są one poprawne. Pamiętaj, aby regularnie sprawdzać działanie kopii zapasowych i być pewnym, że będziesz w stanie odzyskać pliki w przypadku zainfekowania oprogramowaniem szyfrującym. Kopie zapasowe są ważne ponieważ pozwalają odzyskać pliki skasowane przez przypadek lub w wyniku awarii dysku twardego.

Ransomware jest rodzajem złośliwego oprogramowania, które infekując Twój komputer szyfruje wszystkie pliki uniemożliwiając dostęp do nich.

Dalsze sposoby ochrony

Co więcej, możesz zabezpieczyć się przed zainfekowaniem ransomware’m w taki sam sposób jak przed innymi rodzajami złośliwego oprogramowania. Zacznij od upewnienia się, że posiadasz aktualne oprogramowanie antywirusowe. Programy tego typu zostały zaprojektowane w celu wykrycia i powstrzymania działania złośliwego oprogramowania. Pamiętaj jednak o tym, że program antywirusowy może nie być w stanie zablokować lub usunąć wszystkich wirusów. Cybeprzestępcy nieustannie poszukują i wprowadzają do złośliwego oprogramowania coraz bardziej wyrafinowane rozwiązania pozwalające uniknąć wykrycia przez oprogramowanie antywirusowe. Z kolei producenci antywirusów stale aktualizują swoje produkty pozwalając im na wykrycie kolejnych rodzin złośliwego oprogramowania. Pod wieloma względami mamy swoisty wyścig zbrojeń, w którym jedna strona próbuje przechytrzyć drugą. Niestety, przestępcy są zazwyczaj o krok do przodu więc warto zadbać o kopie zapasowe i wykonać poniższe kroki dla zapewnienia ochrony swojego komputera:

- Przestępcy często infekują komputer i inne urządzenia wykorzystując luki bezpieczeństwa w oprogramowaniu. Im bardziej aktualne oprogramowanie posiadasz, tym mniej jest w Twoim systemie luk bezpieczeństwa, a atakującemu jest trudniej zainfekować Twój komputer. Dlatego upewnij się, że Twój system operacyjny, zainstalowane aplikacje i pozostałe urządzenia mają włączone automatyczne aktualizacje.
- Korzystając z komputera używaj konta o niższych uprawnieniach niż Administrator albo “root”. Zapewnisz w ten sposób dodatkową ochronę przed wieloma rodzajami złośliwego oprogramowania.
- Cyber przestępcy często nakłaniają ludzi to zainstalowania złośliwego oprogramowania. Na przykład wysyłają maile wyglądające zupełnie wiarygodnie i zawierające załącznik lub link. Maile te mogą wyglądać tak, jakby zostały wysłane przez bank lub Twojego znajomego. Jednakże, po otwarciu załącznika lub kliknięciu w link instalowane jest złośliwe

Ransomware

oprogramowanie. Jeśli wyświetlona wiadomość stwarza poczucie pośpiechu, albo informuje Cię o czymś co jest zbyt piękne by mogło być prawdziwe, zawiera błędy gramatyczne lub po prostu wydaje Ci się dziwna, może to być próba ataku. Bądź ostrożny i podejrzliwy! Zdrowy rozsądek jest często najlepszym sposobem obrony.

Uchroń się przed ransomwarem pozostając czujnym, gdy otwierasz załączniki z maili lub klikasz w linki. Upewnij się, że posiadasz zaktualizowanego antywirusa, a kopie zapasowe są regularnie tworzone i będziesz w stanie odzyskać z nich pliki.

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

Socjotechnika:	https://securingthehuman.sans.org/ouch/2014#november2014
Czym jest złośliwe oprogramowanie:	https://securingthehuman.sans.org/ouch/2016#march2016
Szyfrowanie:	https://securingthehuman.sans.org/ouch/2016#june2016
Backup i odzyskiwanie danych:	https://securingthehuman.sans.org/ouch/2015#august2015
Artykuł Microsoft:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
Kurs analizy wstecznej złośliwego oprogramowania SANS FOR610:	https://sans.org/for610

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

