OUCH! Lipiec 2020

Ransomware

Czym jest ransomware?

Ransomware jest rodzajem złośliwego oprogramowania, którego głównym celem jest szyfrowanie plików przechowywanych na komputerze wymagający zapłaty za odzyskanie dostępu do nich. Ransomware stał się w ostatnim czasie bardzo popularny wśród przestępców, głównie ze względu na jego dochodowość.

Jak większość złośliwego oprogramowania, ransomware najczęściej rozpowszechnia się poprzez wiadomości e-mail, w których to cyberprzestępcy nakłaniają odbiorcę do otwarcia złośliwego załącznika lub kliknięcia w link prowadzący do strony przestępcy. W momencie kiedy ransomware zainfekuje komputer, rozpoczyna szyfrowanie plików zapisanych na dysku twardym jak i również tych znajdujących się m.in. na dysku zewnętrznym aktualnie podłączonym do komputera. W rezultacie dostęp do ważnych plików, takich jak zdjęcia czy dokumenty zostaje zablokowany, a przestępcy żądają zapłacenia okupu w zamian za odszyfrowanie danych (ang. ransom - okup, ang. software - oprogramowanie, stąd nazwa ransomware). Zdarza się, że przestępcy grożą upublicznieniu dokumentów jeśli nie otrzymają okupu. Najczęściej haracz musi być wpłacony w postaci kryptowaluty, np. Bitcoin. Pamiętaj, że jeśli nawet zapłacisz okup nie masz gwarancji, że odzyskasz swoje dane. Bywa również tak, że przestępcy otrzymają pieniądze ale nie pomogą w odszyfrowaniu plików, a co gorsza będą próbowali uzyskać więcej pieniędzy.

Ochrona przed zainfekowaniem

Możesz zabezpieczyć się przed zainfekowaniem ransomware'm w taki sam sposób jak przed innymi rodzajami złośliwego oprogramowania. Przedstawiamy trzy kroki jak to uczynić:

- **Aktualizuj system operacyjny oraz oprogramowanie**: Cyberprzestępcy często infekują komputery lub urządzenia wykorzystując luki bezpieczeństwa w oprogramowaniu. Im bardziej aktualne oprogramowanie posiadasz, tym mniej jest w Twoim systemie luk bezpieczeństwa, a atakującemu jest trudniej zainfekować komputer. Dlatego upewnij się, że system operacyjny, zainstalowane aplikacje i pozostałe urządzenia, z których korzystasz mają włączoną opcje automatycznych aktualizacji.

- **Oprogramowanie antywirusowe**: Korzystaj z aktualnego oprogramowania antywirusowego dostarczonego od zaufanego dostawcy. Programy tego typu zostały zaprojektowane w celu wykrywania oraz powstrzymywania działania złośliwego oprogramowania. Pamiętaj jednak o tym, że program antywirusowy może nie być w stanie zablokować lub usunąć wszystkich

wirusów oraz zazwyczaj nie udaje mu się odzyskać zaszyfrowanych plików. Cyberprzestępcy nieustannie poszukują oraz opracowują nowe i coraz bardziej wyrafinowane taktyki infekcji złośliwym oprogramowaniem 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 przypomina to wyścig zbrojeń, w którym jedna strona próbuje przechytrzyć drugą.

- **Bądź czujny**: Cyberprzestępcy często oszukują ludzi i nakłaniają do zainstalowania oprogramowania, które potem okazuje się być złośliwym. Na przykład wysyłają wiadomości e-mail, które wyglądają wiarygodnie i zawierają załącznik lub link do strony internetowej. Wiadomości te mogą wyglądać tak, jakby zostały wysłane przez bank lub Twojego znajomego. Jednakże, po otwarciu załącznika lub kliknięciu w link instalowane jest złośliwe oprogramowanie. Jeśli treść wiadomości nakłania do pośpiechu w działaniu, bądź wydaję się być podejrzana np. zawiera błędy gramatyczne, może to być próba ataku. Bądź czujny i podejrzliwy. Atakujący często grają na emocjach. Zdrowy rozsądek jest często najlepszym sposobem obrony.

Tworzenie kopii zapasowych plików

Często błędnym założeniem jest twierdzenie, że zawsze będziesz w stanie zapobiec infekcji ransomware'm, dlatego najlepszą ochroną są kopie zapasowe. Jeśli posiadasz kopię zapasową ważnych dokumentów i plików, masz możliwość odzyskania ich bez płacenia okupu przestępcom. Warto skorzystać z programów do automatycznego tworzenie kopii zapasowych. Ponadto pamiętaj, aby regularnie sprawdzać działanie kopii zapasowych i być pewnym, że będziesz w stanie odzyskać pliki w razie potrzeby. Miej na uwadze, że jeśli backup jest przechowywany na komputerze, ransomware może zaszyfrować również i jego. Dlatego ważne jest, aby kopie zapasowe przechowywane były w "chmurach" lub na zewnętrznych dyskach, które nie są stale podłączone do komputera.

Redaktor gościnny

Lenny Zeltser zajmuje się bezpieczeństwem w firmie Axonius. Prowadzi wykłady poświęcone walce ze złośliwym oprogramowaniem w Instytucie SANS. Lenny jest dostępny na Twitterze jako @lennyzeltser oraz prowadzi blog poświęcony bezpieczeństwu zeltser.com.

Źródła

Czy robisz kopie zapasowe: https://www.sans.org/security-awareness-training/resources/got-backups
Powstrzymać phishing: https://www.sans.org/security-awareness-training/resources/stop-phish
The Power of Updating: https://www.sans.org/security-awareness-training/resources/power-updating
Kurs SANS FOR610 - Reverse Engineering Malware: https://sans.org/for610

Polski przekład CERT Polska: Bartłomiej Wnuk.