**Nowy rok, nowe warianty ransomware – Monti, BlackHunt i Putin**

**Analitycy z FortiGuard Labs, podmiotu firmy Fortinet zajmującego się badaniem i analizą zagrożeń, nieustannie zbierają dane na temat najpoważniejszych niebezpieczeństw w cyfrowym świecie. Na początku 2023 roku wykryli trzy warianty złośliwego oprogramowania, które dotknęły użytkowników systemów Windows i Linux.**

Każda zidentyfikowana odmiana ataku ransomware szyfrowała dane na zainfekowanym urządzeniu i żądała okupu od ofiary w zamian za odszyfrowanie informacji. Poniżej przedstawiono mechanizm działania wykrytych wariantów.

**Oprogramowanie Monti prowadzi tzw. ścianę wstydu**

Monti to stosunkowo nowy wariant ataku ransomware, zaprojektowany do szyfrowania plików w systemach Linux. Pliki zaatakowane przez Monti mają rozszerzenie „.puuuk”. Zespół FortiGuard Labs wykrył także warianty tego złośliwego oprogramowania, które działają na systemach Windows.



Grafika 1. Pliki zaszyfrowane przez Monti

Na zainfekowanym urządzeniu Monti zostawia notatkę o konieczności zapłaty okupu zatytułowaną „README.txt”. Ponadto, pokazuje ofierze, ile plików zostało zaszyfrowanych. W przeciwieństwie do typowego ataku ransomware, Monti obsługuje dwie oddzielne strony w sieci TOR: jedną do hostowania danych skradzionych ofiarom i drugą, do negocjowania okupu. W momencie opracowywania tego materiału druga witryna nie była dostępna.

Strona wycieku danych zawiera tzw. ścianę wstydu (Wall of Shame) z założeniem, że pokazywała będzie dane ofiar, które nie zapłaciły okupu. Obecnie ściana jest pusta, ale zawiera prowokacyjną wiadomość, która może wskazywać, że wiele ofiar dotkniętych Monti było „chętnych do współpracy” i zapłaciło okup (z wyjątkiem jednej ofiary w Argentynie).



Grafika 2. Tzw. ściana wstydu oprogramowania Monti.

**BlackHunt atakuje także kopie plików**

Analitycy FortiGuard Labs zidentyfikowali nowe warianty złośliwego oprogramowania BlackHunt. Dostęp do sieci ofiar uzyskują poprzez niepoprawnie skonfigurowany protokół zdalnego dostępu Remote Desktop Protocol (RDP).

Pliki zaszyfrowane przez ransomware BlackHunt można zidentyfikować za pomocą następującego wzorca nazwy pliku: [unikalny identyfikator przypisany do każdej zagrożonej maszyny].[kontaktowy adres e-mail].Black. BlackHunt usuwa również kopie plików, co znacznie utrudnia ich odzyskanie. Oprogramowanie zostawia na zainfekowanym urządzeniu dwie notatki na temat okupu: jedna nosi tytuł „#BlackHunt\_ReadMe.hta”, a druga „#BlackHunt\_ReadMe.txt”.



Grafika 3. Pliki zaszyfrowane przez BlackHunt.

Chociaż obie noty dotyczą ataku BlackHunt, zawierają różne adresy e-mail, za pośrednictwem których ofiara powinna skontaktować się z przestępcami, a także odmienne identyfikatory przypisane do każdej ofiary. Notatka o okupie w formacie HTA zawiera link do strony sieci TOR, która nie była już dostępna w czasie dochodzenia prowadzonego przez FortiGuard Labs.



Grafika 4. Notatka w formacie HTA, mówiąca o ataku BlackHunt i konieczności zapłacenia okupu.

**Ransomware Putin publikuje dane na Telegramie**

Putin to najnowszy wariant złośliwego oprogramowania szyfrującego pliki. Ta odmiana ataku ransomware próbuje wyłudzić pieniądze za odszyfrowanie danych i ich nieupublicznianie. Pliki zaszyfrowane przez ransomware Putin mają rozszerzenie „.PUTIN”.

Podobnie jak Monti i BlackHunt, oprogramowanie Putin zostawia na zaatakowanym urządzeniu notatkę zatytułowaną „README.txt”, która informuje ofiarę, że ma dwa dni na zapłacenie okupu, a w przeciwnym razie skradzione dane nie zostaną odzyskane. Jest to powszechna taktyka stosowana przez atakujących, która ma wywrzeć presję na ofiarach, aby jak najszybciej zapłaciły okup.



Grafika 5. Wiadomość od oprogramowania Putin mówiąca o konieczności zapłaty okupu w ciągu dwóch dni.

Notatka mówiąca o konieczności zapłacenia okupu zawiera linki do dwóch kanałów na platformie Telegram: jeden służy negocjowaniu płatności okupu z przestępcami, a drugi publikowaniu danych skradzionych ofiarom. W momencie prowadzenia śledztwa przez FortiGuard Labs na kanale wykorzystywanym do gromadzenia danych wymienione są dwie firmy – z Singapuru i Hiszpanii. Jednak daty postów na kanale sięgają tylko końca listopada 2022 r., wskazując, że ransomware Putin prawdopodobnie nie jest jeszcze rozpowszechniony na szeroką skalę.



Grafika 6. Kanał ransomware Putin na platformie Telegram.

W obliczu ciągle pojawiających się nowych wariantów ataków ransomware, przedsiębiorstwa powinny dostosować swoje działania obronne do taktyk cyberprzestępców. Tworzenie kopii zapasowych danych, korzystanie z wielopoziomowego podejścia do zabezpieczania cyfrowych zasobów, a także identyfikowanie ścieżek, którymi przestępcy mogą dostać się do systemu, to podstawowe sposoby na minimalizowanie negatywnych skutków cyberataku.

\*\*\*