**Ransomware Ryuk: Precyzyjnie wymierzone ataki złośliwego oprogramowania**

**W ciągu dwóch ostatnich tygodni precyzyjnie wymierzone i zaplanowane ransomware o nazwie Ryuk zaatakowało wiele organizacji na świecie. Jak dotąd ofiarami było kilka firm, którym zaszyfrowano setki komputerów znajdujących się w wielu różnych centrach danych – informuje na swoim blogu firma Check Point Software Technologies.**

Pomimo, że techniczne możliwości Ryuk są stosunkowo niewielkie, przynajmniej trzy firmy z różnych stron świata zostały poważnie dotknięte atakiem. Co gorsza, część organizacji zapłaciła ogromne kwoty okupu w celu odzyskania swoich plików. Cena okupu poszczególnych ofiar waha się od 15 do 50 BTC, w sumie ponad 640 000 dolarów.

Co ciekawe, badania Check Pointa wykazały, że sposób działania oprogramowania Ryuk jest zbliżony do ransomware HERMES, którego autorstwo przypisuje się północnokoreańskiej grupie hakerskiej APT Lazarus Group. HERMES również został użyty do ataków na wielką skalę, dlatego podejrzewamy, że aktualna fala ataków może być sterowana przez twórców HERMES albo przez kogoś, kto uzyskał jego kod źródłowy.

W poniższej analizie Check Point opisuje precyzyjnie zaplanowane ataki za pomocą aplikacji Ryuk oraz porównuje je z atakami przeprowadzanymi przy użyciu oprogramowania HERMES. Eksperci Check Pointa analizują także finansowe aspekty ataków i przedstawiamy w jaki sposób autorzy Ryuka chcą ukryć swoją tożsamość poprzez podział i przekazywanie wpłat do różnych portfeli.

**Ogólne spojrzenie na Ryuk**

W przeciwieństwie do zwykłego ransomware, regularnie rozpowszechnianego poprzez kampanie spamowe i exploity, Ryuk jest wykorzystywany tylko w atakach na ściśle określone cele. Szyfrowane są jedynie kluczowe zasoby w każdej z zainfekowanych sieci, a atakujący ręcznie rozpowszechniają złośliwe oprogramowanie.

Oznacza to, że przed każdym atakiem każda sieć jest mapowana, a w wyniku ataków hakerskich zbierane są dane logowania. Wynika z tego, że atakujący posiadają spore doświadczenie w tego typu atakach, co było widoczne np. we włamaniu do Sony Pictures w 2014 roku.

**Żądanie okupu Ryuk**

Check Point wykrył dwie wersje wiadomości wysyłanej do ofiar: dłuższa, lepiej napisana notatka, która spowodowała wypłacenie okupu 50 BTC (około 320 000 dolarów) oraz krótsza, bardziej bezpośrednia, która została wysłana do wielu innych organizacji, żądająca wypłaty okupów w wysokości 15-35 BTC (do 224 000 dolarów). Może to świadczyć o tym, że przeprowadzono dwie fazy ataków.

**Ryuk kontra HERMES**

Ransomware HERMES wykryto w październiku 2017, kiedy zostało użyte w ataku na Far Eastern International Bank (FEIB) na Tajwanie. W tym ataku, który powszechnie przypisano grupie Lazarus, skradziono 60 milionów dolarów w wyrafinowanym ataku SWIFT. Na szczęście później udało się odzyskać tę sumę. W tym przypadku bank zainfekowano HERMESem w formie dywersji.

W przypadku Ryuk jednak nie ma wątpliwości, że ataki typu ransomware, które przeprowadzono w ciągu dwóch ostatnich tygodni, są gwoździem programu, a nie zasłoną dymną. Po sumie już zapłaconych okupów widać, że Ryuk zdecydowanie skutecznie oddziaływuje na ofiary ataków.

Poniższe porównanie techniczne programów Ryuk i HERMES wykazuje, że ktokolwiek napisał pierwszy z nich musiał mieć albo kod źródłowy HERMES-a albo jest to ta sama osoba wykorzystująca kod źródłowy do kolejnej fali ataków.

**Porównanie złośliwego oprogramowania**

Ciekawy faktem dostrzeżonym przez firmę [Malwarebytes](https://blog.malwarebytes.com/threat-analysis/2018/03/hermes-ransomware-distributed-to-south-koreans-via-recent-flash-zero-day/) jest podobieństwo algorytmów kodujących programów Ryuk i HERMES. Jeżeli porównamy funkcje szyfrującą poszczególne pliki, widzimy dużo podobieństw w strukturze, co widać na poniższych diagramach:

Wygląda na to, że autor Ryuka nie zadał sobie nawet trudu żeby zmienić generowany przez program w zaszyfrowanych plikach znacznik, który służy do określenia, czy plik został już zaszyfrowany - jest on identyczny w obu plikach:

Ponadto, funkcja, która wywołuje powyższy kod, wykonuje bardzo podobne kroki w obu przypadkach. Przykładowo, na białej liście znajdują się te same foldery (m. in. “Ahnlab”, “Microsoft”, “$Recycle.Bin” itp.) w celu uniknięcia szyfrowania zawartych w nich plików. Oba programy generują skrypt o nazwie “window.bat” w tej samej ścieżce, podobny skrypt wykorzystywany jest do usunięcia plików tymczasowych. Podobnie w obu przypadkach tworzone są pliki “PUBLIC” oraz “UNIQUE\_ID\_DO\_NOT\_REMOVE”.

Ta sama logika wykorzystywana jest w 32 i 64 bitowych wersjach Ryuka. Takie podobieństwa mogą wskazywać na to, że zostały one wygenerowane z identycznego kodu źródłowego.

Zarówno natura ataku, jak i wewnętrzne działanie złośliwego oprogramowania wiążą Ryuka z ransomware HERMES i wzbudzają ciekawość co do tożsamości grupy stojącej za nim i związku z Grupą Lazarus. Po tym jak udało się zainfekować a w efekcie wyłudzić około 640 000 dolarów, Check Point uważa, że to nie koniec kampanii i że kolejne organizacje mogą stać się ofiarą Ryuka.

Dalsza część analizy dostępna na [blogu firmy Check Point](https://research.checkpoint.com/ryuk-ransomware-targeted-campaign-break/)