JAK NIE STAĆ SIĘ OFIARĄ RANSOMWARE?

Ransomware jest formą szkodliwego oprogramowania komputerowego, które poprzez zaszyfrowanie danych uniemożliwia dostęp do komputera i informacji w nim zawartych. Następnie domaga się zapłacenia okupu, w zamian za który obiecuje przesłać klucz do deszyfrowania plików, a co za tym idzie, odzyskanie dostępu.

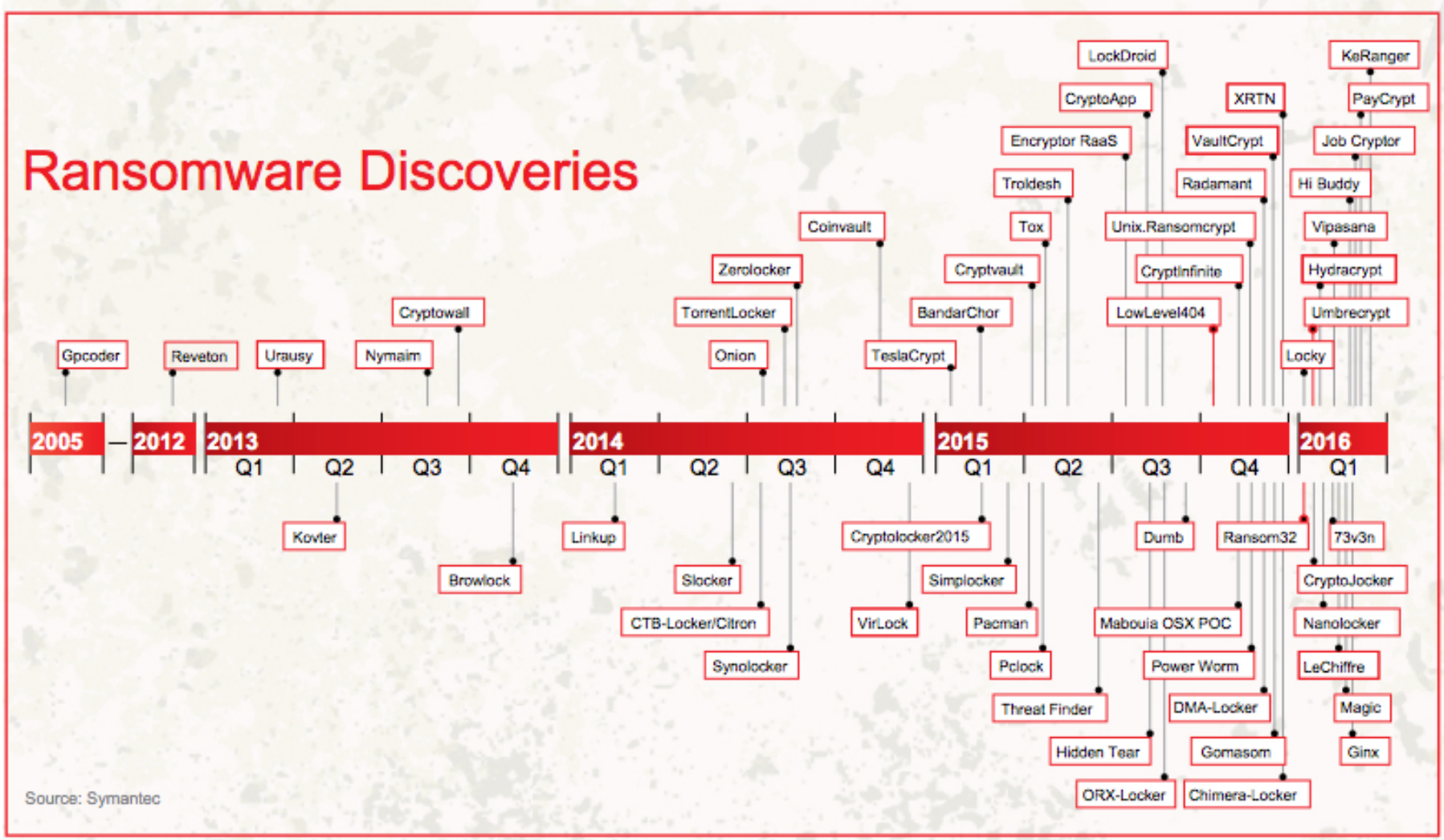
Dlaczego to ma znaczenie dla mnie ?

Raporty wskazują, że 42% małych i średnich przedsiębiorstw (MSP) uważa krypto-malware (taki jak ransomware) za jedno z najpoważniejszych zagrożeń, które napotyka - i nie bez powodu! Ataki ransomware coraz bardziej koncentrują się na małych i średnich firmach oraz rozproszonych przedsiębiorstwach, wśród których można znaleźć dużą liczbę takich organizacji, w których ochrona sieci nie wystarcza by wykryć i zapobiec działaniu zaawansowanego szkodliwego oprogramowania.

Cyberprzestępcy często postrzegają małe i średnie firmy oraz rozproszone przedsiębiorstwa jako „owoce, po które łatwo sięgnąć”. Niestety można się tutaj obłowić. Podczas gdy pojedyncze żądanie okupu to zwykle około 300 $, badania pokazują, że jeden atak ransomware może kosztować małe i średnie firmy nawet do 99,0001 $.

Jakie są kluczowe trendy, jakie obserwujemy w zagrożeniu Ransomware - i jaką zapewnić strategię i działania w celu obrony przed tymi atakami??

Ransomware jest coraz częściej stosowaną przez hakerów metodą ataku na małe/ średnie firmy i przedsiębiorstwa rozproszone. Podczas gdy pierwsze przypadki szkodnika zostały odkryte w już w 2005 roku, dopiero ostatnie trzy lata obrazują eksplozję popularności tego typu zagrożenia i kompromitację milionów komputerów i urządzeń mobilnych na całym świecie.



Przebiegłość ransomware

W bezpieczeństwie często mówimy o potrzebie ochrony danych, który są wrażliwe i utrzymaniu ich z dala od rąk napastników, którzy mogliby wykorzystać je dla własnego zysku. Widzieliśmy niedawno masowe naruszenia w organizacjach publicznych i prywatnych, które doprowadziły do ogromnych strat finansowych w wyniku przedostania się w ręce przestępców danych osobowych i numerów kart kredytowych, wykorzystywanych do popełniania kolejnych przestępstw. Na te naruszenia nakładają się efekty boczne, które są często trudne do oszacowania, takie jak utrata reputacji firmy i zaufania swoich klientów.

Recepta na te ataki w dużej mierze pozostała taka sama: zidentyfikowanie poufnych danych, zbudowanie zabezpieczenia tam, gdzie dane są przechowywane i wykorzystywane, a tam gdzie to możliwe, trzymanie dane zaszyfrowanych.
Ponieważ dane są przechowywane dla okupu, wartość dla napastnika nie zawiera się w samych danych, ale w wartości, jaką stanowią dla użytkownika (lub organizacji). To znaczy, mimo że dane mogą nie posiadać wrażliwej treści, ich brak może okazać się krytyczny dla działalności organizacji w perspektywie krótko- i długoterminowej.

Dostępność. Ransomware-as-a-service

Ciemna strona internetu to prawdziwa mekka dla cyberprzestępców, gdzie niewykwalifikowany haker - lub nawet zwykły cywil - może kupić narzędzia potrzebne do przeprowadzania zaawansowanych ataków malware. To upowszechnianie próbek złośliwego oprogramowania i narzędzi ułatwia napastnikowi uzyskanie konkretnego typu złośliwego oprogramowania dla małych i średnich firm, potrzebnego do przeprowadzenia ukierunkowanego ataku, bez marnowania czasu i energii. A ponieważ wiele z tych firm nie posiada niezbędnego zabezpieczenia, wiele z nich pada ofiarą ataku ransomware.

Jak się łapie ransomware

Ataki RansomWare zazwyczaj realizowane są przez phishing ze złośliwym linkiem, wykonywany metodą tzw. „spray attacks” [pol. atak natryskowy]. Hakerzy masowo wysyłają e-maile, próbując zarazić tak wielu ludzi, jak to tylko możliwe. Tysiące takich e-maili wysyłanych jest każdego dnia, a napastnicy manewrują jedynie liczbami i mają nadzieję, że ktoś będzie na tyle naiwny, aby kliknąć link lub pobrać plik od kogoś, kogo nie zna. Smutnym faktem jest to, że nadal wiele osób będzie się zarażać tą metodą, świadczy o tym fakt, że 85% organizacji ucierpiało w wyniku ataku phishing’u w 2015 roku.

Choć szerokie [natryskowe] ataki nadal odnoszą sukcesy, ukierunkowane ataki czyli tzw. „spear-phishing” są dziś bardziej powszechne niż kiedykolwiek. Badania wykazały wzrost o 22% w atakach typu „spear-phishing” od 2014 do 2015. Dzięki poświęceniu odrobiny czasu na poszukiwaniu odpowiedniego celu, utworzeniu przekonującego e-mail (może nawet podszywanie współpracownika lub przyjaciela) i zaprojektowania złośliwego oprogramowania, wykwalifikowani napastnicy są w stanie zapewnić atakowi większą szansę sukcesu. Małe i średnie przedsiębiorstwa są często poddawane kampaniom spear-phishingowym, a 43% ataków ukierunkowanych było skierowanych do przedsiębiorstw z 250 lub mniejszą ilością pracowników.

Pracownicy najsłabszym ogniwem

Socjotechnika jest od dawna stosowana przez przestępców jako sposób na zmanipulowanie swojej ofiary. Od stosowania taktyki zastraszania, przez podszywanie się pod agencje federalne czy policję, do dostarczania szkodliwego oprogramowania za pośrednictwem starannie spreparowanych e-maili, ukierunkowanych do konkretnej osoby, inżynieria społeczna jest często integralną częścią ataku ransomware. Stawia to Twoich pracowników w pierwszej linii frontu walki ze szkodnikiem.
Jedno kliknięcie w wiadomość phishingową przez pracownika z działu rachunkowości i system jest posiekany, urządzenia zablokowane, biznes staje. W przypadku ataków ukierunkowanych jest bardzo ważne jest, żeby pracownicy wiedzieli, co to jest phishing, jak wygląda i czym jest.

Zmniejszenie zagrożenia zarażeniem ransomware

Liczba incydentów RansomWare eksplodowała w ciągu ostatnich kilku lat, zarażając setki tysięcy systemów na całym świecie. Dostępność narzędzi RansomWare i pojawienie się Ransomware-as-a-service oznacza, że napastnicy nie muszą być technicznie doświadczeni. Podczas gdy dostępność tych narzędzi zwiększa liczbę ataków ransomware, wielu z nich można by zapobiec.
WatchGuard Total Security Suite to pierwsza usługa dostępna w UTM, które przynosi korporacyjnej klasy narzędzia do ochrony przed ransomware - małym i średnim firmom. Z zaawansowanymi rozwiązania bezpieczeństwa, jak WebBlocker, APT Blocker i Host RansomWare Prevention, WatchGuard Total Security Suite jest najlepszym rozwiązaniem dla ochrony działalności jakichkolwiek organizacji, przed atakami szkodnika.

- **WEBBLOCKER**

WebBlocker to w pełni zintegrowany moduł bezpieczeństwa dla urządzeń WatchGuard, który pozwala administratorom IT zarządzać dostępem do sieci i treściach ściślejszej kontroli bezpieczeństwa i surfowania po Internecie. Moduł ten blokuje złośliwe strony, które mogą zawierać ransomware, zapobiegając pobraniu go.

- **APT BLOCKER**

APT Blocker jest dynamicznym rozwiązaniem sandboxowym zapewniającym widoczność i szczegółową analizę złośliwego oprogramowania. Jeśli plik nie został rozpoznany, zostanie zdetonowany w środowisku wirtualnym, które przeanalizuje jego zachowanie i określi poziom zagrożenia, zapewniając ochronę przed zaawansowanymi zagrożeniami malware i zero-day.

- **HOST RANSOMWARE PREVENTION**

Host Ransomware Prevention (HRP) wykrywa i zapobiega atakom RansomWare w punkcie końcowym. HRP jest zbudowany na silniku behawioralnym, który monitoruje szeroki wachlarz zachowań punktu końcowego w celu określenia, czy dane działanie jest związane z szkodnikiem. Kiedy rozpoznanie się powiedzie, HRP blokuje działanie pliku, zanim dojdzie do szyfrowania.