RANSOMWARE ISTNIEJE OD PONAD 30 LAT, CIĄGLE SIEJE SPUSTOSZENIE

Przychody z cyberprzestępczości z użyciem oprogramowania szyfrującego ransomware wzrosły w 2020 roku o 311 proc. w porównaniu z poprzednim rokiem i szacunkowo wyniosły 350 milionów dolarów.

Ransomware stanowi poważne zagrożenie dla funkcjonowania wielu gałęzi gospodarki. To złośliwe oprogramowanie blokujące dostęp do systemu, które umożliwia hakerowi żądanie okupu w zamian za przywrócenie sprzętu do stanu pierwotnego.

Według raportu Fortinet „Global Threat Landscape", w grudniu 2020 roku codziennie na świecie 17,2 tys. urządzeń stawało się celem ataków tego typu.

Natomiast przychody z cyberprzestępczości z użyciem szyfrującego oprogramowania wzrosły w tym samym okresie o 311 proc., w porównaniu z ubiegłym rokiem, osiągając szacunkową wartość 350 milionów dolarów.

Eksperci FortiGuard Labs przypominają, że ransomware w ciągu ostatnich 30 lat ewoluował - od ataków z użyciem dyskietek aż do usług działających w złożonych modelach biznesowych.

Pierwszy w historii atak ransomware

Trojan AIDS z 1989 roku był pierwszym w historii atakiem ransomware, który został wymierzony w branżę medyczną. W czasie konferencji Światowej Organizacji Zdrowia poświęconej tematyce AIDS rozdano 20 tys. zainfekowanych dyskietek, które zawierały program do analizy ryzyka zachorowania oraz złośliwe oprogramowanie. Uruchamiało się automatycznie, po włączeniu po raz 91. komputera. Wirus ukrywał katalogi i szyfrował nazwy wszystkich plików znajdujących się na dysku C, a następnie wyświetlał komunikat o żądaniu okupu.

Atak ten został nazwany trojanem AIDS, ale był również znany jako wirus PC Cyborg – od fikcyjnej nazwy firmy żądającej zapłaty: PC Cyborg Corporation. W kolejnych latach pojawiły się podobne ataki, ale oprogramowanie ransomware nadal pozostawało stosunkowo niewielkim zagrożeniem.

Era internetu i nowe możliwości: Archiveus i GPcode

Coraz powszechniejszy dostęp do internetu spowodował także wzrost cyberataków i nowe formy cyberprzestępczości. W 2006 roku pojawił się trojan Archiveus, który był pierwszym oprogramowaniem ransomware korzystającym z szyfrowania RSA. Blokował on wszystkie pliki w katalogu i wymagał od ofiar zakupu produktów w aptece internetowej, w celu uzyskania 30-cyfrowego kodu klucza, dającego możliwość odzyskania dostępu.

W tym samym roku złośliwe oprogramowanie GPcode infekowało komputery poprzez ataki typu spear-phishing. Wirus trojan był rozsyłany jako załącznik do wiadomości e-mail, wyglądających jak podania o pracę. GPcode, podobnie jak Archiveus, używał 660-bitowego klucza publicznego RSA do szyfrowania plików w katalogu „Dokumenty". Aby uzyskać kod dostępu, ofiary były zmuszone zapłacić okup.

Kryptowaluty coraz popularniejszą formą płatności

W 2008 roku stworzono bitcoina, zdecentralizowaną cyfrową kryptowalutę, której potencjał szybko wyczuli cyberprzestępcy, co wynika z braku powiązania transakcji z konkretną osobą. Liczba wykrywanych ataków typu ransomware zaczęła wzrastać, a w pierwszym i drugim kwartale 2011 roku zanotowano ich ok. 30 tys. W trzecim – liczba ta podwoiła się. Pod koniec 2012 roku ransomware osiągnęło na czarnym rynku wartość 5 milionów dolarów.

Jednym z głównych graczy w tej dziedzinie był wtedy trojan WinLock, który blokował całe systemy zamiast pojedynczych plików, atakował system operacyjny Windows i uniemożliwiał użytkownikom dostęp do wszystkich zasobów, aż do momentu zakupu klucza.

Ransomware jako usługa

Ostatnia dekada przyniosła intensywny rozwój cyberprzestępczości za sprawą modelu usługowego Ransomware-as-a-Service (RaaS), która umożliwia kupno gotowych narzędzi i daje możliwość przeprowadzania ataków bez konieczności posiadania zaawansowanej wiedzy technicznej.

Trojan Zeus, który został zidentyfikowany w 2007 roku, kilka lat później – w 2013-2014 roku służył do przeprowadzenia wielu ataków poprzez instalowanie ransomware o nazwie CryptoLocker.

Globalne ataki: WannaCry i Petya

W maju 2017 roku oprogramowanie WannaCry – wymierzone w systemy operacyjne Windows – zainfekowało ponad 200 tys. komputerów w 150 krajach, co spowodowało szkody sięgające miliardów dolarów.

Natomiast w czerwcu 2017 roku pojawił się nowy wariant znanego wcześniej oprogramowania Petya – nazwany NotPetya, który wywołał globalny cyberatak. Zarejestrowano go w Rosji, na Ukrainie, we Francji, Niemczech, Włoszech, Polsce, Wielkiej Brytanii i Stanach Zjednoczonych. W samej Ukrainie ucierpiało ponad 1500 osób fizycznych i prawnych, w tym instytucje finansowe.

Celem ataków korporacje

Współcześnie cyberprzestępcy działają głównie jako duże, rozproszone firmy, z centralami telefonicznymi do obsługi płatności okupu. Celem ich ataków są głównie korporacje lub znane osoby. Grupa znana jako Sodinokibi (lub REvil) wykorzystała koncepcję RaaS do budowy zaawansowanego modelu dystrybucji swojego oprogramowania. Udało im się pozyskać blisko terabajt danych dużej firmy prawniczej.

Niedawno przestępcy znani jako DarkSide uzyskali dostęp do sieci Colonial Pipeline, największego systemu rurociągów do transportu pochodnych ropy naftowej w USA.

Czytaj też: Amerykanie wyciągają wnioski po ataku na Colonial Pipeline