**Rok później: WannaCry, czyli początek nowej generacji ataków cybernetycznych**

**W ciągu jednego weekendu, słynny atak ransomware, znany powszechnie znany jako WannaCry zainfekował ponad 200.000 maszyn na całym świecie, powodując miliardy dolarów szkód. Ataki ransomware zdarzają się cały czas, ale szybkość i skala tego konkretnego ataku – jakiej nigdy wcześniej nie było – sprawiła, że nagłówki gazet na całym świecie skupiły się właśnie na tym incydencie. Zaledwie kilka miesięcy później byliśmy świadkami śladów WannaCry w kolejnym ransomware, który sparaliżował Atlantę.**

WannaCry zmienił zasady gry bezpieczeństwa cybernetycznego nie tylko poprzez jego szerokie oddziaływanie, ale również poprzez jej wyjątkowy wpływ na krajobraz zagrożeń cybernetycznych. Określając punkt zwrotny w środowisku cyberbezpieczeństwa, mieliśmy do czynienia z pierwszą globalnie skalowaną, wielopoziomową kampanią zasilaną narzędziami sponsorowanymi przez państwo. WannaCry zainicjował nową, piątą generację cyberataków.

Z pewnością nie był to ostatni atak tzw. generacji V. Nadszedł czas, aby organizacje dostosowały się do nowych realiów cyberataków, które obejmują…

**…(wykradzione) narzędzia sponsorowane przez państwa:**

Na około miesiąc przed atakiem WannaCry, grupa hakerów o nazwie Bracia Mroku wykradła tzw. eksploit rozwinięty przez Narodową Agencję Bezpieczeństwa (NSA). Ten eksploit, oznaczony jako EternalBlue, zostanie później użyty jako część ataku WannaCry.

W przeszłości cyberprzestępcy tradycyjnie wykorzystywali do działań hakerskich uproszczone, własne narzędzia. WannaCry zaznaczył przejście w kierunku stosowania broni wojskowej, narzędzi hakerskich, które są na tyle potężne, że narodowa agencja obrony cybernetycznej może wykorzystywać je w międzynarodowej walce cybernetycznej. Zaledwie sześć tygodni po WannaCry, NotPetya użyła tego samego eksploitu w swoim ataku na ukraińskie systemy infrastruktury krytycznej. Niedawny atak ransomware SamSam, który sparaliżował Atlantę, opierał się na DoublePulsar - kolejnym eksploicie opracowanym przez NSA. Cyberprzestępcy zwiększają swoją siłę ognia i ustawiają swoje celowniki wyżej niż kiedykolwiek wcześniej.

**Narzędzia skalowane globalnie:**

W 2015 r. ataki ransomware spowodowały straty na kwotę 325 mln dolarów. Do 2017 r. wartość ataków wzrosła piętnastokrotnie do 5 mld dolarów, ponieważ firmy traciły zarówno produktywność, jak i reputację w wyniku przestojów w pracy systemów własnych. Wraz z uderzeniem, WannaCry zrodziła setki wariantów ransomware. Co więcej, przed WannaCry, pod koniec stycznia 2017 roku, ilość wariantów złośliwego oprogramowania oscylowała wokół 635. W lutym 2018 wykryto już 1 105 różnych wariantów złośliwego oprogramowania, co oznaczało 74 procentowy wzrost!

Ta globalna ambicja jest decydującym elementem ataków cybernetycznych nowej generacji - hakerzy generacji V-tej myślą o skalach większych niż kiedykolwiek wcześniej, a coraz więcej organizacji przestępczych rozwija nowe strategie lukratywnych operacji hakerskich.

**Oraz narzędzia wielowektorowe:**

Ataki cybernetyczne są uważane za "haki na komputery", które zarażają Twój komputer osobisty.

Rozprzestrzeniając się przez sieci chmur obliczeniowych, zdalne serwery biurowe i sieciowe punkty końcowe, WannaCry była w stanie "dzielić i podbijać", ponieważ do zainfekowania całego systemu potrzebował tylko jednego punktu wejściowego. To wielopoziomowe podejście pozwoliło WannaCry z łatwością przytłoczyć te firmy, które stosowały zwykłą strategię bezpieczeństwa polegającą na wybieraniu swoich ulubionych produktów od różnych dostawców dla każdego punktu wejścia.

Strategia „najlepszy w swojej klasie” oznacza, że firmy wybierają jeden konkretny produkt dla swoich urządzeń mobilnych, inny dla swoich sieci chmur obliczeniowych, a inny dla swoich sieci bezpieczeństwa sieciowego.

Nie jest to nielogiczna strategia, sama w sobie, ale tego właśnie oczekuje WannaCry (i inne ataki Gen V): rozbieżnej, rozłącznej obrony, która nie działa w jednorodny sposób, aby pokryć wszystkie bazy.

**Wnioski:**

W miarę jak przyzwyczajamy się do nowych realiów, organizacje po prostu nie mają innego wyboru, jak się do nich dostosować.

Daleko nam do tego, aby firmy mogły dotrzymać kroku hakerom dzięki swojej infrastrukturze bezpieczeństwa cybernetycznego. Ostatnie badanie firmy Check Point pokazało, że tylko trzy procent firm jest dziś przygotowanych do odparcia ataku V generacji, podobnego do WannaCry.

Atak taki jak WannaCry wymaga bezpieczeństwa cybernetycznego, które może aktywnie zapobiegać zagrożeniom (w przeciwieństwie do reaktywnego wykrywania ich po zadaniu obrażeń). Aby walczyć z wielosektorowym podejściem ataków Gen V, organizacje muszą również zabezpieczyć swoją chmurę obliczeniową i system mobilny. Przed tymi nowoczesnymi, innowacyjnymi atakami mogą bronić się jedynie ujednolicone systemy zapobiegania zagrożeniom, które zabezpieczają wszystkie wektory.

Dziś jednak zdecydowana większość organizacji jest tak samo podatna na WannaCry, jak dokładnie rok temu…