**Kwartalny raport Fortinet: wzmożona aktywność cyberprzestępców**

**Warszawa, 03.09.2019 Fortinet, globalny dostawca rozwiązań cyberochronnych, przedstawił wnioski ze swojego kwartalnego badania zagrożeń informatycznych. Wynika z niego, że cyberprzestępcy nieustannie szukają nowych okazji na ataki w przestrzeni cyfrowej i z coraz większą wprawą wykorzystują sposoby na unikanie wykrycia oraz techniki antyanalityczne. Z kolei indeks krajobrazu zagrożeń (Threat Landscape Index) jest wyższy o 4% w porównaniu z poprzednim rokiem. Za wzrost wskaźnika odpowiada przede wszystkim wzmożona aktywność eksploitów i innych rodzajów złośliwego oprogramowania.**

**Nowe standardy unikania wykrycia**

Wiele nowoczesnych narzędzi typu malware zawiera funkcje unikania interakcji z oprogramowaniem ochronnym i innymi środkami wykrywania zagrożeń. Cyberprzestępcy dążą jednak do jeszcze skuteczniejszych sposobów unikania detekcji, korzystając z technik tzw. zaciemniania kodu i antyanalizy.

Za przykład wykorzystywania tych praktyk może służyć kampania spamu w Japonii. W jej trakcie do e-maili phishingowych dodawany był załącznik z uzbrojonym plikiem Excel zawierającym złośliwe makra. Zaprojektowano je w taki sposób, aby wyłączało narzędzia zabezpieczające, wykonywało dowolne komendy, wywoływało problemy z pamięcią urządzenia i działało tylko na japońskich systemach.

Kolejny przykład to jedna z wersji trojana bankowego Dridex, który przy każdym logowaniu użytkownika zmieniał nazwy i hashe plików, utrudniając odnalezienie złośliwego oprogramowania w zainfekowanym systemie. – *Coraz powszechniejsze wykorzystywanie antyanalizy i praktyk unikania detekcji przypomina o potrzebie korzystania z ochrony wielowarstwowej i behawioralnego wykrywania zagrożeń* – mówi **Jolanta Malak, dyrektor polskiego oddziału firmy Fortinet**.

**Długoterminowa strategia ukrytych ataków**

Złośliwe oprogramowanie Zegost było zastosowane w kampanii *spearphishingowej*, która wykorzystywała kilka ciekawych technik. Tak jak w przypadku innych rodzajów oprogramowania typu *infostealer*, głównym celem Zegosta jest zbieranie i potajemne wydobywanie informacji o urządzeniu ofiary. Wyróżnia go jednak unikalna konfiguracja, która ma chronić przed wykryciem. Zegost wyposażony jest np. w funkcję czyszczenia zapisów zdarzeń, co nie jest zazwyczaj charakterystyczną cechą złośliwego oprogramowania. Kolejną ciekawą funkcją wyróżniającą Zegosta jest komenda, która utrzymywała go w uśpieniu przed 14 lutego 2019. Dopiero po tej dacie rozpoczął się cykl infekowania.

Osoby odpowiedzialne za rozpowszechnianie Zegosta wykorzystują cały arsenał eksploitów, a więc luk w zabezpieczeniach, aby nawiązać i utrzymać połączenie z ofiarą. Dlatego jest to o wiele bardziej długoterminowe zagrożenie w porównaniu z innymi odpowiednikami tego oprogramowania.

**Ukierunkowane ataki ransomware**

Popularność ransomware’u nie zanika – oprogramowanie to stanowi poważne zagrożenie, czego dowodzą liczne ataki na infrastruktury miejskie czy lokalne jednostki samorządowe. Przestępcy korzystający z ransomware odchodzą od strategii szeroko zakrojonych kampanii celujących w przypadkowe ofiary, a skupiają się na ukierunkowanych atakach na ofiary mające możliwości lub powody, aby zapłacić okup. W niektórych przypadkach cyberprzestępcy przeprowadzali dokładny rekonesans przed skierowaniem ransomware’u na starannie dobrane systemy, aby zwiększyć szansę powodzenia ataku.

Dla przykładu ransomware o nazwie *RobbinHood* zaprojektowano w taki sposób, aby atakował infrastrukturę sieci przedsiębiorstwa. Oprogramowanie było w stanie wyłączać usługi Windows chroniące przed szyfrowaniem danych oraz przerywać połączenie ze współużywanymi dyskami.

Istnieje też nowszy ransomware, *Sodinokibi*, który pod względem funkcjonalności nie różni się znacznie od innych dostępnych narzędzi. Stwarza jednak problem, ponieważ wykorzystuje nową podatność – umożliwia uruchamianie dowolnych skryptów bez konieczności interakcji z użytkownikiem, w porównaniu np. z ransomware’em dostarczanym przez e-maile phishingowe.

Należy więc pamiętać o tym, jak ważne są regularne aktualizacje i szkolenia na temat bezpieczeństwa. Co więcej, podatności typu RDP (Remote Desktop Protocol), takie jak BlueKeep, wskazują, że zdalny dostęp do usług może stanowić okazję dla cyberprzestępców i być wykorzystany jako wektor ataku do rozpowszechniania ransomware’u.

**Nowe możliwości w przestrzeni cyfrowej**

Jednak domowe drukarki i infrastruktura krytyczna w przedsiębiorstwach to niejedyne cele cyberprzestępców. Pomiędzy nimi „wyrosła” nowa kategoria produktów odpowiedzialnych za kontrolowanie rozwiązań IT w gospodarstwach domowych oraz małych firmach. Tego typu inteligentne systemy nie przyciągają dużej uwagi cyberprzestępców w porównaniu z systemami przemysłowymi, ale wkrótce może się to zmienić. W wyniku niedawnych obserwacji zanotowano zwiększoną liczbę przypadków, gdzie celem ataków były urządzenia kontrolujące środowisko, kamery i systemy bezpieczeństwa. Co prawda tylko 1% podmiotów zanotował wykrycie złośliwego oprogramowania atakującego rozwiązania do zarządzania budynkami, ale jest to większy odsetek niż zauważa się zazwyczaj w przypadku rozwiązań typu ICS lub SCADA.

Cyberprzestępcy szukają też nowych sposobów na przejęcie kontroli nad urządzeniami w domach i przedsiębiorstwach. Niekiedy są to urządzenia, na które nie zwraca się uwagi przy tradycyjnym zarządzaniu środowiskiem IT. Należy przykładać szczególną uwagę do ich bezpieczeństwa, zwłaszcza że uzyskanie do nich dostępu przez cyberprzestępców może nieść poważne konsekwencje. Jest to szczególnie ważne w środowisku pracy zdalnej, gdzie bezpieczny dostęp odgrywa kluczową rolę.

**Jak chronić swoją firmę: rozległe, zintegrowane i zautomatyzowane zabezpieczenia**

Dynamiczna, proaktywna i dostępna w czasie rzeczywistym analiza zagrożeń może pomóc w przedstawieniu ewolucji metod cyberataków, a także rozpoznawaniu trendów i wskazywaniu priorytetów higieny cyberbezpieczeństwa,. Reagowanie na informacje o zagrożeniach traci na wartości, jeśli takie działania nie odbywają się w czasie rzeczywistym na każdym urządzeniu. Tylko działające w szerokiej skali, zautomatyzowane i zintegrowane rozwiązania zabezpieczające mogą zapewnić szybką i rozległą ochronę całemu środowisku sieci, od IoT po brzeg sieci, jej rdzeń oraz systemy wielochmurowe.

**Informacje o raporcie i indeksie**

[Najnowszy „Threat Landscape Report” firmy Fortinet](https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf) to regularny przegląd informacji zebranych w drugim kwartale 2019 r. przez FortiGuard Labs dzięki sieci sensorów rozlokowanych na całym świecie. Raport obejmuje również indeks krajobrazu zagrożeń (Threat Landscape Index) złożony ze wskaźników dotyczących jego trzech głównych obszarów (exploitów, złośliwego oprogramowania i botnetów) oraz prezentujący ich rozpowszechnienie i częstotliwość występowania w danym kwartale.

**Informacja o firmie Fortinet**

Fortinet (NASDAQ: FTNT) chroni największe przedsiębiorstwa, dostawców usług i podmioty administracji publicznej na całym świecie. Klienci Fortinet objęci są pełną i inteligentną ochroną w dobie zwiększającej się sfery zagrożeń i stale rosnących oczekiwań wobec wydajności rozszerzających się sieci. Architektura Fortinet Security Fabric zapewnia skuteczne zabezpieczenia, odpowiadające na kluczowe wyzwania bezpieczeństwa środowisk sieciowych, aplikacji, chmury oraz urządzeń mobilnych. Fortinet jest liderem pod względem liczby urządzeń zabezpieczających sprzedanych na całym świecie. Rozwiązania firmy chronią działalność już ponad 415 tys. klientów.

Więcej informacji na [www.fortinet.com](http://www.fortinet.com/), [Fortinet Blog](https://blog.fortinet.com/) oraz [FortiGuardLabs](http://www.fortiguard.com/" \t "_blank).