**FortiGuard Labs: cyberzagrożenia przechodzą znaczną przemianę**

*Skala cyberataków i ewolucja sposobów ich przeprowadzania wpływają na bezpieczeństwo przedsiębiorstw w każdym aspekcie, także na brzegu sieci i w cyfrowym łańcuchu dostaw*

**[Warszawa, 02.03.2021] Fortinet, światowy lider w dziedzinie zintegrowanych i zautomatyzowanych rozwiązań cyberochronnych, przedstawił wyniki najnowszego półrocznego raportu *Global Threat Landscape Report* opracowanego przez FortiGuard Labs. Dane o zagrożeniach z drugiej połowy 2020 roku ilustrują bezprecedensowy rozwój skali zagrożeń na całym świecie. Według raportu hakerzy wykazali się wysoką zdolnością dostosowania do okoliczności, poprzez tworzenie kampanii destrukcyjnych i wyrafinowanych ataków. Ich celem była duża liczba osób pracujących lub uczących się zdalnie. Wykazali się również nowymi umiejętnościami w próbach ataków na cyfrowe łańcuchy dostaw, a nawet na rdzenie sieci.**

**Najważniejsze wnioski z raportu dotyczącego drugiego półrocza 2020 roku:**

**Nie ustają ataki ransomware** – Według danych FortiGuard Labs, w porównaniu z pierwszą połową 2020 roku nastąpił siedmiokrotny wzrost całkowitej liczby ataków z użyciem oprogramowania ransomware. Wpływ na to miało wiele czynników: ewolucja i dostępność oprogramowania w modelu usługowym *Ransomware-as-a-Service* (RaaS), próby uzyskiwania wysokich okupów od ofiar o dużej skali działalności czy też groźba ujawnienia skradzionych danych w przypadku niespełnienia żądań. Spośród analizowanych rodzajów ransomware’u najbardziej aktywnymi były, występujące w różnym stopniu rozpowszechnienia: Egregor, Ryuk, Conti, Thanos, Ragnar, WastedLocker, Phobos/EKING i BazarLoader. Z kolei najczęściej atakowanymi podmiotami z różnych obszarów gospodarki były: ochrona zdrowia, firmy świadczące usługi dla biznesu oraz społeczeństwa, organizacje sektora publicznego i przedsiębiorstwa z branży finansowej. Aby skutecznie radzić sobie ze zmieniającym się ryzykiem związanym z ransomware’em, firmy będą musiały systematycznie wykonywać kompletne i odpowiednio zabezpieczone kopie zapasowe danych przechowywane poza siedzibą firmy lub przynajmniej na nośnikach odłączonych od sieci. Powinny także wdrażać strategię Zero Trust Network Access oraz segmentację sieci.

**Ataki na cyfrowe łańcuchy dostaw (*supply chain*)w centrum uwagi**: – Próby zmanipulowania dostarczanych w ramach jakiegoś procesu informacji mają długą historię, ale dopiero udany atak na firmę SolarWinds przeniósł dyskusję o nich na nowe tory. W miarę jego rozwoju, od ofiar wyciekło wiele informacji. FortiGuard Labs uważnie monitorował te doniesienia i wykorzystywał je do zdefiniowania tzw. wskaźnika ataku (Indicator of Compromise) w celu wykrycia innych, powiązanych z nim działań. Ruch w internecie, związany z dystrybuowanym w ramach tego ataku w grudniu 2020 r. backdoorem SUNBURST pokazuje, że kampania miała prawdziwie globalny charakter, zaś stowarzyszenie *Five Eyes* wskazało na szczególnie duży ruch, którego charakter odpowiadał zdefiniowanym wcześniej wskaźnikom ataku. Istnieją również dowody na to, że cyberprzestępcy wybrali także inne instytucje jako cel swoich ataków prowadzonych w podobny sposób, co ukazuje ich zwiększone zainteresowanie cyfrowymi łańcuchami dostaw, a więc konieczność zintensyfikowania prac nad ich zabezpieczeniem oraz zarządzaniem ryzykiem ich zakłócenia.

**Przestępcy śledzą aktywność w sieci** – Badanie najpowszechniejszych rodzajów złośliwego oprogramowania pomogło ujawnić najpopularniejsze techniki cyberprzestępców umożliwiające zdobycie „przyczółka” w przedsiębiorstwach. Ich głównym celem były platformy firmy Microsoft i dokumenty, z których większość ludzi korzysta podczas przeciętnego dnia pracy. Kolejnym polem walki z hakerami są przeglądarki internetowe. Kategoria zagrożeń HTML obejmuje strony phishingowe zawierające złośliwe oprogramowanie oraz skrypty wstrzykujące złośliwy kod lub przekierowujące użytkowników do zainfekowanych witryn. Tego typu zagrożenia nieuchronnie nasilają się w czasach kryzysów o globalnym zasięgu lub w okresach wzmożonego handlu online. Natomiast pracownicy, którzy zazwyczaj korzystają z usług filtrowania stron internetowych podczas przeglądania ich w sieci firmowej, są bardziej narażeni na niebezpieczeństwo, gdy robią to bez wykorzystania ochronnych filtrów.

**Domowe biuro pozostaje celem hakerów**: – W 2020 roku granice między domem a biurem uległy znacznemu zatarciu. Oznacza to, że skuteczne zaatakowanie domowej sieci przybliża przestępców do infrastruktury korporacyjnej. W drugiej połowie 2020 roku na szczycie listy zagrożeń znalazły się złośliwe narzędzia wykorzystujące luki w urządzeniach Internetu Rzeczy (IoT), które znajdują się w wielu domach. Każde z nich wprowadza do sieci nową „przestrzeń”, która musi być chroniona. Wymaga to monitorowania każdego tego typu sprzętu i dbania o jego bezpieczeństwo.

**Duzi gracze na globalnej scenie** – Cyberprzestępcze grupy, specjalizujące się w zaawansowanych uporczywych atakach APT (*Advanced Persistent Threat*), nadal wykorzystują pandemię COVID-19 na wiele różnych sposobów. Do najczęstszych należą kradzieże dużych baz danych osobowych lub zawierających własność intelektualną oraz pozyskiwanie informacji wywiadowczych, zgodnie z aktualnymi priorytetami, charakterystycznymi dla kraju, z którego pochodzi dana grupa prowadząca ataki APT. Pod koniec 2020 r. nastąpił wzrost aktywności takich cyberprzestępców wobec instytucji zaangażowanych w prace związane z COVID-19, w tym badania nad szczepionkami czy też opracowanie krajowej lub międzynarodowej polityki zdrowotnej dotyczącej pandemii. Wśród zaatakowanych organizacji były np. agencje rządowe, firmy farmaceutyczne, uniwersytety i medyczne ośrodki badawcze.

**Spłaszczanie krzywej wykorzystania podatności** – Łatanie luk bezpieczeństwa w sprzęcie i oprogramowaniu powinno być priorytetem dla przedsiębiorstw i instytucji, ponieważ cyberprzestępcy wciąż aktywnie z nich korzystają. Śledzenie rozwoju 1500 eksploitów „na wolności” w ciągu ostatnich dwóch lat uwidacznia, w jakim tempie i jak daleko mogą się one rozprzestrzenić. Wydaje się, że większość z nich nie rozpowszechnia się bardzo szybko. Spośród wszystkich eksploitów prześledzonych w ciągu ostatnich dwóch lat tylko 5% zostało wykrytych przez więcej niż 10% firm. Losowy wybór przy równomiernym rozkładzie daje około 1 na 1000 szans, że przedsiębiorstwo zostanie zaatakowane. Około 6% eksploitów trafia do więcej niż 1% firm w ciągu pierwszego miesiąca, a 91% nie przekroczyło progu 1% nawet po roku. Niezależnie od tego, rozsądne jest koncentrowanie się na łataniu znanych luk i priorytetowe traktowanie tych najszybciej rozprzestrzeniających się.

**Walka z cyberprzestępcami wymaga zintegrowanej strategii i szerokiej świadomości**

Przedsiębiorstwa i instytucje stoją w obliczu cyberzagrożeń na wszystkich możliwych frontach. Wykrywanie ataku pozostaje kluczowym czynnikiem dla jego zrozumienia oraz doboru właściwych sposobów obrony. Krytycznego znaczenia nabiera także widoczność środowiska IT, szczególnie gdy znaczna liczba użytkowników znajduje się poza tradycyjnym środowiskiem pracy. Każde urządzenie otwiera nową przestrzeń, która musi być monitorowana i zabezpieczona. Wykorzystanie sztucznej inteligencji (AI) oraz zautomatyzowanego wykrywania zagrożeń w każdym zakątku infrastruktury sieciowej umożliwia firmom natychmiastową reakcję na ataki i jest niezbędne do łagodzenia ich skutków z odpowiednią szybkością i na właściwą skalę. Priorytetem powinno być również prowadzenie regularnych szkoleń dla całego personelu z zasad cyberhigieny, ponieważ zachowanie bezpieczeństwa leży w gestii nie tylko zespołów IT.

## Derek Manky, Chief, Security Insights & Global Threat Alliances, FortiGuard Labs

„Przez cały rok 2020 byliśmy świadkami dramatycznego rozwoju krajobrazu cyberzagrożeń. Pandemia odegrała w tym główną rolę, a w miarę upływu roku cyberprzestępcy udoskonalali ataki, które miały coraz bardziej destrukcyjne skutki. Zmaksymalizowali oni zakres podejmowanych działań – w tej chwili uderzają nie tylko w rdzeń sieci, ale także środowisko zdalnej nauki i pracy, a także cyfrowe łańcuchy dostaw. Ryzyko związane z cyberbezpieczeństwem nigdy nie było większe niż obecnie, ponieważ w rozszerzającym się środowisku cyfrowym wszystko jest ze sobą połączone. Zintegrowane i bazujące na sztucznej inteligencji podejście platformowe do bezpieczeństwa, powiązane ze skutecznymi mechanizmami wykrywania niebezpieczeństw, są niezbędne do obrony na całym brzegu sieci oraz do identyfikowania i usuwania w czasie rzeczywistym zagrożeń, przed którymi stoją dziś przedsiębiorstwa.”

**Informacje o raporcie**

Najnowszy raport *Global Threat Landscape Report* zawiera zbiorczą analizę FortiGuard Labs, sporządzoną na podstawie danych z drugiej połowy 2020 roku, pochodzących z należącej do Fortinetu rozległej sieci czujników, gromadzących miliardy informacji o zagrożeniach obserwowanych na całym świecie. W podobny sposób, jak ramy MITRE ATT&CK klasyfikują taktykę i techniki cyberprzestępców w trzech grupach obejmujących rozpoznanie, przygotowanie i próba uzyskania dostępu, tak FortiGuard Labs wykorzystuje ten model do opisania w dokumencie *Global Threat Landscape Report,* w jaki sposób hakerzy znajdują luki, budują złośliwą infrastrukturę i eksplorują środowisko ofiary. Raport uwzględnia również perspektywę globalną i regionalną.

**Dodatkowe zasoby**

* Więcej informacja na [blogu Fortinet](https://www.fortinet.com/blog/industry-trends/fortiguard-labs-global-threat-landscape-report-2021?utm_source=pr&utm_campaign=2021-q1-fortiguard-labs-global-threat-landscape-report-2021) lub w [pełnej wersji raportu](https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/Global-TLR-2021-2H.pdf).
* Więcej informacji o tym jak platforma [Fortinet Security Fabric](https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html?utm_source=blog&utm_campaign=2018-security-fabric) zapewnia szeroką, zintegrowaną i zautomatyzowaną ochronę w cyfrowej infrastrukturze przedsiębiorstwa.
* Więcej informacji o laboratoriach [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs.html?utm_source=blog&utm_medium=campaign&utm_campaign=FortiGuardLabs) oraz [portfolio](https://www.fortinet.com/support-and-training/support-services/fortiguard-security-subscriptions.html?utm_source=blog&utm_campaign=2018-blog-security-services) usług ochronnych FortiGuard.
* Więcej o [darmowej inicjatywie edukacyjnej](https://www.fortinet.com/blog/business-and-technology/why-cybersecurity-training-is-more-important-than-ever.html) oraz koordynowanych przez Fortinet programach: [Network Security Expert](https://training.fortinet.com/?utm_source=blog&utm_campaign=2019-q3-nse-institute), [Network Security Academy](https://training.fortinet.com/local/staticpage/view.php?page=fnsa&utm_source=blog&utm_campaign=2019-q3-fnsa) i [FortiVet](https://www.fortinet.com/corporate/careers/vets.html?utm_source=blog&utm_campaign=2018-q2-fortivet).
* Więcej informacji o tym jak [klienci zabezpieczają swoje przedsiębiorstwa](https://www.fortinet.com/customers.html?utm_source=pr&utm_campaign=2019-q3-telecommunications) z wykorzystaniem rozwiązań firmy Fortinet.
* Uzyskanie dodatkowych informacji o produktach i technologiach oraz udział w dyskusjach z ekspertami z branży możliwe są na [forum użytkowników rozwiązań Fortinet (Fuse)](https://fusecommunity.fortinet.com/home?utm_source=blog&utm_medium=campaign&utm_campaign=2020-fusecommunity).
* Profile firmy Fortinet w mediach społecznościowych: [Twitter](https://twitter.com/Fortinet), [LinkedIn](https://www.linkedin.com/company/fortinet), [Facebook](https://www.facebook.com/fortinet/), [YouTube](https://www.youtube.com/fortinet) oraz [Instagram](https://www.instagram.com/behindthefirewall/).

**Informacja o firmie Fortinet**

Fortinet zabezpiecza infrastrukturę IT największych przedsiębiorstw, dostawców usług i instytucji rządowych na całym świecie. Swoim klientom zapewnia pełen wgląd w stan ich środowiska oraz ochronę przed atakami pochodzącymi z różnych źródeł – wszystko przy uwzględnieniu wymogów dotyczących wydajności, zarówno tych obowiązujących dziś, jak i w przyszłości. Tylko stworzona przez Fortinet platforma Security Fabric jest w stanie poradzić sobie z najtrudniejszymi wyzwaniami związanymi z bezpieczeństwem oraz ochroną całej cyfrowej infrastruktury, zarówno w sieciowych, aplikacyjnych, wielochmurowych, jak też brzegowych środowiskach. Fortinet uplasował się na pierwszym miejscu w rankingu sprzedaży urządzeń ochronnych na całym świecie – do ochrony własnej infrastruktury wykorzystuje je ponad 480 tys. klientów. Zarówno Fortinet, jak też należący do tego producenta instytut szkoleniowy [Fortinet Network Security Expert (NSE)](https://training.fortinet.com/?utm_source=blog&utm_campaign=2019-q3-nse-institute), mają jedne z najbardziej zaawansowanych programów szkoleniowych w branży. Więcej informacji na stronie [www.fortinet.com](http://www.fortinet.com), na [blogu producenta](https://blog.fortinet.com) oraz w serwisie laboratorium [FortiGuard Labs](https://www.fortinet.com/fortiguard/labs.html?utm_source=blog&utm_medium=campaign&utm_campaign=FortiGuardLabs).