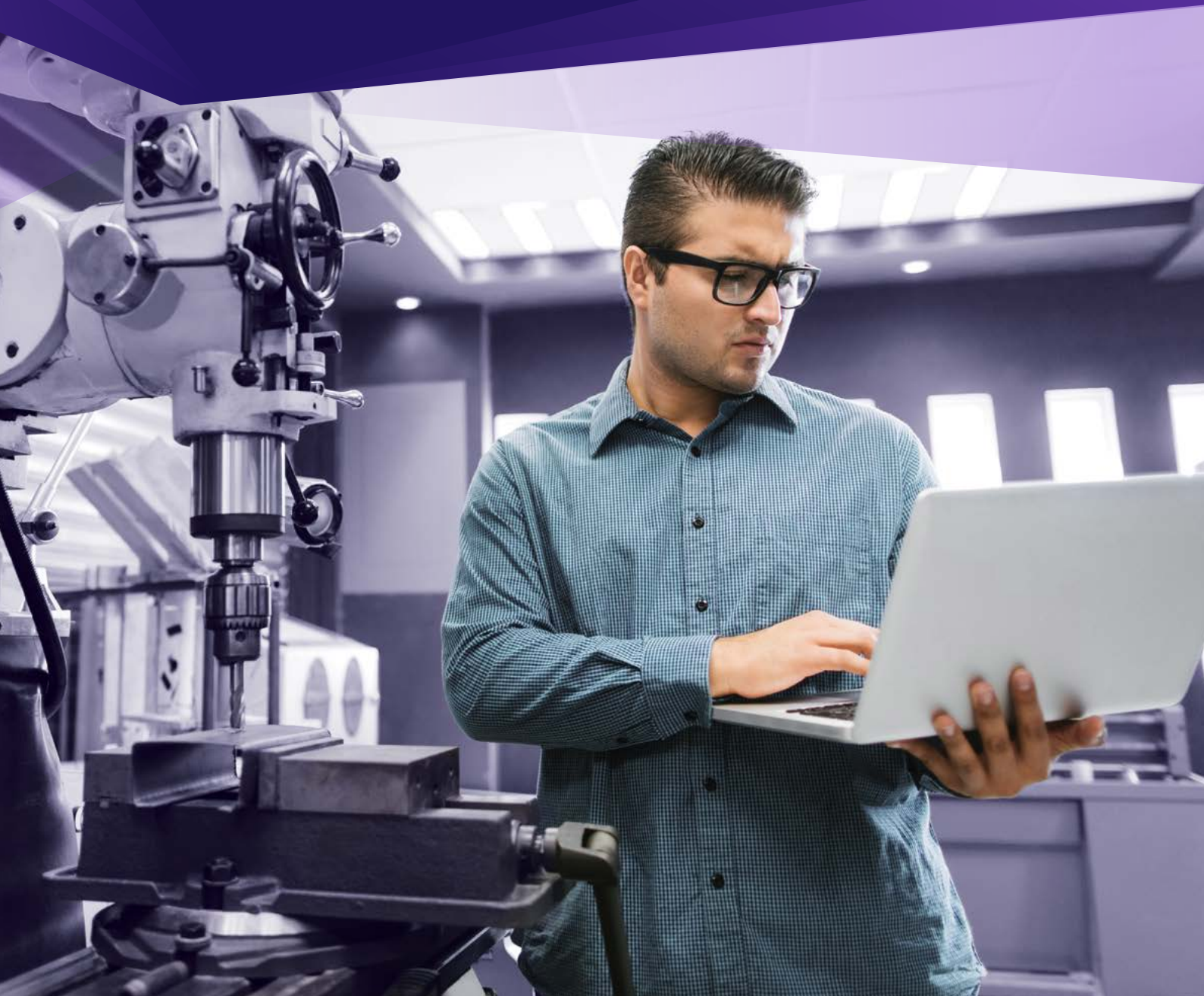
FORTINET

RAPORT

Raport firmy Fortinet o tendencjach w zakresie zabezpieczeń technologii operacyjnych w 2019 r.

Najnowsze informacje o zagrożeniach dotyczących systemów ICS i SCADA



Spis treści

Streszczenie 3

Infografika — najważniejsze wnioski 3

Wstęp 4

Tendencje w zakresie zabezpieczeń systemów OT 5

Ataki wykorzystujące infrastrukturę IT coraz częściej mają na celu systemy OT 5

Ataki na systemy OT nadal są prowadzone, a celem są teraz systemy zabezpieczeń . . 10

Ataki na systemy OT nie zależą od lokalizacji 12

Podsumowanie. 14

Źródła 15

Streszczenie

W miarę rosnącej sprawności działania przedsiębiorstw w odpowiedzi na szybko rozwijający się rynek wiele technologii operacyjnych (operational technology, OT) jest po raz pierwszy podłączana do sieci zewnętrznych. Zjawisko to jest potencjalnym źródłem dużych korzyści dla przedsiębiorstw, ale jednocześnie naraża te technologie na ataki APT (ang. Advanced Persistent Threats), czyli ataki, w ramach których sprawca uzyskuje nieautoryzowany dostęp do sieci przedsiębiorstwa i pozostaje tam niewykryty przez dłuższy okres czasu. Po podłączeniu do niezabezpieczonej sieci zewnętrznej dotychczasowy bufor polegający na braku takiego podłączenia (ang. air gap), który izolował technologie operacyjne przed hakerami i złośliwym oprogramowaniem, przestaje istnieć i w efekcie technologie te stają się coraz częściej przedmiotem ataków.

W raporcie firmy Fortinet dotyczącym tendencji w zakresie zabezpieczeń technologii operacyjnych w 2019 r. poddano analizie zagregowane dane otrzymane z FortiGuard Labs, aby na ich podstawie uzyskać informacje na temat stanu zabezpieczeń systemów nadzorowania procesów technologicznych w przemyśle (Supervisory Control And Data Acquisition, SCADA) i innych przemysłowych systemów sterowania (Industrial Control Systems, ICS). Wyniki tej analizy wskazują, że technologie operacyjne są coraz częściej celem ataków zarówno ukierunkowanych na infrastrukturę IT — często za pomocą starszego złośliwego oprogramowania, które nie czyni już szkód tej infrastrukturze — jak i celowych ataków ukierunkowanych konkretnie na technologie operacyjne. Ataki te uderzają, rzecz jasna, w najsłabsze ogniwa sieci OT i wykorzystują złożoność wynikającą z braku standaryzacji protokołów. Warto przy tym zauważyć, że atakujący nie dyskryminują swoich celów ze względu na branżę lub lokalizację geograficzną, ponieważ groźne ataki zostały odnotowane w każdej branży i w każdym regionie geograficznym.

W miarę jak technologie operacyjne są coraz częściej podłączane do sieci zewnętrznych wydaje się, że dokonywanych jest na nie coraz więcej ataków. To nowe zjawisko wymaga od przedsiębiorstw stosowania bardziej rygorystycznych zabezpieczeń i najlepszych praktyk w zakresie zarządzania cyklem eksploatacji, aby chronić się przed groźnymi zagrożeniami dla działalności podstawowej. W rezultacie działy OT i IT muszą ze sobą współpracować, aby kompleksowo reagować na to rosnące zagrożenie.

Infografika — najważniejsze wnioski



W 2018 r. **wzrosła liczba i częstość występowania ataków** na systemy ICS/SCADA niemal każdego dostawcy.



Atakujący regularnie **wykorzystują złośliwe oprogramowanie stosowane przeciwko systemom IT** do atakowania systemów OT.

Celem

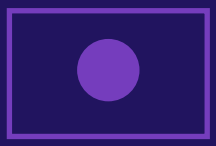
85%

wykrytych niepowtarzalnych zagrożeń były jednostki korzystające z protokołów:

OPC Classic
BACnet
Modbus



Ataki na protokół BACnet osiągnęły apogeum **w okresie od stycznia do kwietnia 2018 r**, co wiązało się z okresem aktywnością botneta Mirai.



W Japonii intensywnie wykorzystywana była luka **Moxa 313**.

Wstęp

Dotychczas odizolowane od niezabezpieczonych sieci zewnętrznych systemy OT są coraz częściej do takich sieci podłączane, czasami w zakresie szerszym niż zdaje sobie z tego sprawę kierownictwo zakładów lub zespół inżynierów obsługujący te systemy. Według wyników jednego z ostatnich badań do sieci zewnętrznej podłączonych jest niemal dwie trzecie urządzeń operacyjnych, z czego 32% bezpośrednio do Internetu, a kolejne 32% — przez bramę przedsiębiorstwa[1]. Bramę taką stanowi czasami zwykły komputer PC podłączony oddzielnie zarówno z daną technologią operacyjną, jak i z Internetem.

Zintegrowanie systemów OT i IT to dla wielu przedsiębiorstw dobra decyzja biznesowa, z której płyną następujące korzyści:

- **Skuteczniejsze i efektywniejsze monitorowanie procesów** z możliwością dokonywania na bieżąco istotnych zmian
- **Zdolność do użycia danych pochodzących z urządzeń związanych z Internetem rzeczy** w celu podejmowania świadomych decyzji, które to dane stanowią dodatkową warstwę wiedzy o klientach, produktach i procesach
- **Dostęp do danych rynkowych w czasie rzeczywistym** w celu zapewnienia optymalnego czasu dostawy i płynniejszych interakcji w ramach łańcucha dostaw
- **Istotne oszczędności** związane z ograniczeniem zużycia energii, zmniejszeniem ilości odpadów surowcowych i poprawą wydajności pracowników

Integracja systemów OT w kontekście bezpieczeństwa.

Mimo tych wyraźnych korzyści podłączenie systemów OT do niezabezpieczonych sieci zewnętrznych naraża te systemy na takie same zagrożenia, na które narażone są systemy IT, oraz ułatwia rozprzestrzenianie się zagrożeń ukierunkowanych specjalnie na systemy OT. Co gorsza systemy ICS i SCADA od zawsze działają w ramach znacznie dłuższego cyklu aktualizacji i wymiany niż systemy informatyczne, co oznacza, że wiele bardzo starych systemów ICS i SCADA jest obecnie po raz pierwszy narażonych na ataki APT. Kolejnym problemem jest brak widoczności: w jednym z badań 82% respondentów przyznało, że nie są w stanie zidentyfikować wszystkich urządzeń podłączonych do obsługiwanych przez nich sieci OT i IT[2].

W wielu przedsiębiorstwach problemy te doprowadziły do niedopuszczalnie wysokiej liczby incydentów związanych z bezpieczeństwem. W niedawnym badaniu przeprowadzonym wśród specjalistów ds. OT 77% respondentów stwierdziło, że w ciągu ostatniego roku doświadczyło włamania przy użyciu złośliwego oprogramowania, przy czym połowa z nich miała do czynienia z takimi zdarzeniami w liczbie od trzech do dziesięciu[3]. Charakter takich włamań jest niepokojący: 43% z nich negatywnie wpłynęło na produktywność, 36% — na przychody, 30% — na świadomość marki, 28% — na utratę danych, a 23% — na bezpieczeństwo fizyczne człowieka.

Zabezpieczenie systemów OT niesie ze sobą istotne zagrożenia.

Wiele zachęt skłania do atakowania systemów ICS i SCADA. Na przykład szantażyści mogą żądać okupu po zatrzymaniu linii produkcyjnych, wyłączeniu systemu kontroli dostępu lub przejęciu kontroli nad krytycznym elementem infrastruktury. Konkurenci — często jednostki państwowe działające w imieniu przedsiębiorstw państwowych — mogą infiltrować systemy w celach związanych ze szpiegostwem przemysłowym. Osoby kierujące się pobudkami politycznymi mogą natomiast atakować przedsiębiorstwo postrzegane za przeszkodę w realizacji ich celów i wywoływać w nich chaos i zamęt.

Osoba odpowiedzialna za zabezpieczenie systemu OT stoi zatem w obliczu poważnych problemów w przypadku podłączenia go do niezabezpieczonych sieci zewnętrznych:

- **Zwiększona powierzchnia ataku** wskutek wspomnianego podłączenia do sieci zewnętrznej
- **Nieadekwatność zabezpieczeń starszych systemów**, które były projektowane dla infrastruktury niepodłączonej do wspomnianych sieci zewnętrznych
- **Słaba widoczność** systemów, często z urządzeniami związanymi z Internetem rzeczy podłączonymi w sposób nieuporządkowany
- **Starsze urządzenia telemetryczne**, naruszenie bezpieczeństwa których może skończyć się katastrofalnie
- **Słaba segmentacja sieci**, gdzie 45% użytkowników systemu ICS/SCADA nie korzysta z funkcji zarządzania tożsamościami uprzywilejowanymi[4]

Przygotowany przez firmę Fortinet raport o tendencjach w zakresie zabezpieczeń technologii operacyjnych w 2019 r. jest oparty na wynikach analizy danych zebranych z milionów urządzeń Fortinet mającej na celu rozpoznanie stanu cyberbezpieczeństwa systemów ICS i SCADA. Wnioski płynące z tej analizy mogą pomóc osobom odpowiedzialnym za bezpieczeństwo tych systemów w zrozumieniu pojawiających się zagrożeń i nadanie odpowiednich priorytetów reakcjom na takie zagrożenia.

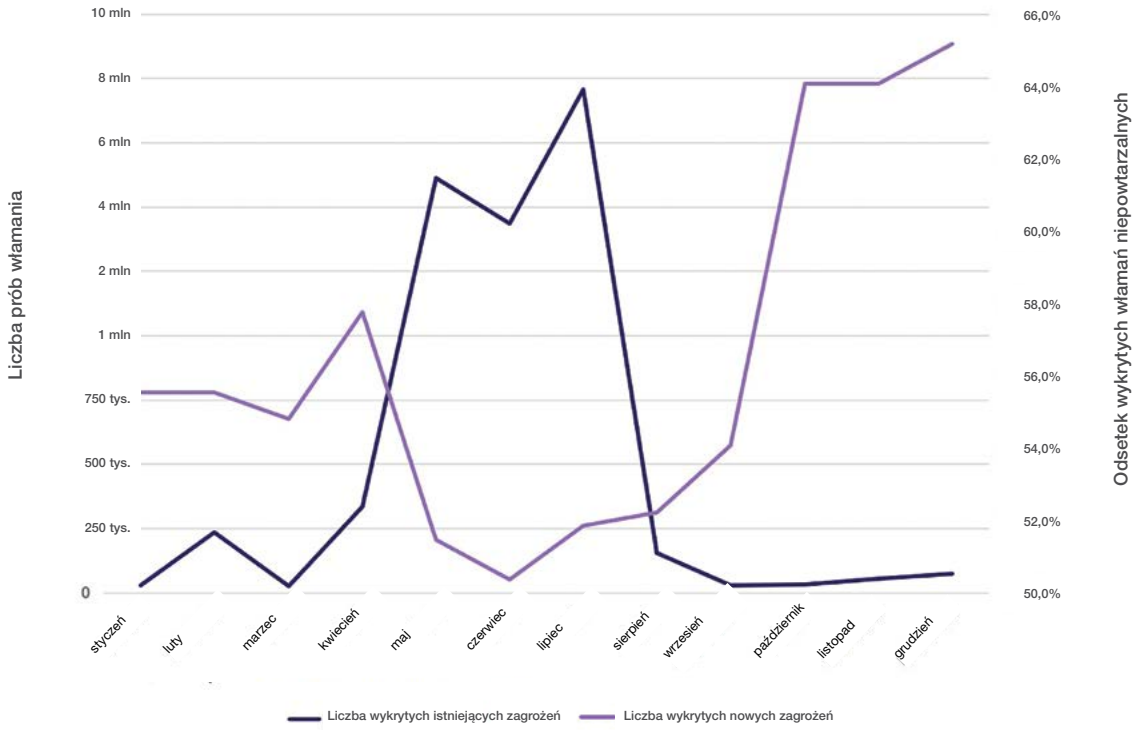
Tendencje w zakresie zabezpieczeń systemów OT

Tendencja — ataki wykorzystujące infrastrukturę IT coraz częściej mają na celu systemy OT

Systemy OT podłączone do sieci IT są często najsłabszym ogniwem w łańcuchu zabezpieczeń. Dane z FortiGuard Labs wskazują, że celem ataków wykorzystujących infrastrukturę IT są właśnie technologie operacyjne. W typowym scenariuszu za pomocą jednego typu złośliwego oprogramowania atak jest prowadzony jednocześnie na używane w przedsiębiorstwie systemy IT i OT. Systemy OT często korzystają ze starszych rozwiązań technicznych i mają słabiej rozwinięte zabezpieczenia, co sprawia, że atakujący mają tutaj większą szansę na sukces.

Ataki na systemy OT prowadzone za pomocą złośliwego oprogramowania „z recyklingu”.

W innym scenariuszu ataki na systemy OT są prowadzone za pomocą starszych pakietów złośliwego oprogramowania, które były kiedyś używane do ataków na sieci IT, ale obecnie są już neutralizowane przez każdy system zabezpieczeń sieci IT oparty na rozpoznawaniu sygnatur. Na rys. 1 przedstawiono odsetek istniejących zagrożeń wykrytych przez rozwiązania Fortinet w poszczególnych miesiącach w roku w zestawieniu z liczbą zaatakowanych w tych miesiącach urządzeń z protokołami OT. Widać tu wyraźną cykliczność — im więcej wykrytych zagrożeń, tym mniej zaatakowanych urządzeń i vice versa.



Rys. 1: Liczba wykrytych włamań a liczba wykrytych włamań niepowtarzalnych w 2018 r.

Cykl ten sugeruje, że atakujący intensywnie szukają nowych luk w zabezpieczeniach w nowo podłączonych do sieci systemach OT. W takiej fazie rozpoznania na stosunkowo niewielkiej liczbie komputerów testowana jest szersza gama starego złośliwego oprogramowania. Potem następuje faza ataku, podczas której większa liczba komputerów staje się przedmiotem ataku złośliwego oprogramowania, które okazało się skuteczne w pierwszej fazie. W tym przypadku celem jest maksymalne wykorzystanie potencjału istniejącego złośliwego oprogramowania, zanim zainwestuje się w nowe, lepiej ukierunkowane ataki.

Na wspomniane sezonowe wahania dotyczące użycia nowego i starego złośliwego oprogramowania wpływać może kolejny czynnik. Wydaje się bowiem, że ataki na systemy COWIG (ciepłownictwo, ogrzewnictwo, wentylacja i gazownictwo) i sieci elektryczne mogą zdarzać się częściej wtedy, gdy systemy te działają najbardziej intensywnie, zazwyczaj podczas miesięcy letnich na półkuli północnej. Istotnym czynnikiem jest również wiek tych technologii, ponieważ ataki na starsze systemy OT zdarzają się częściej niż ataki na nowe, lepiej zabezpieczone systemy OT.

Atakowane są urządzenia używające różnych protokołów OT.

O ile systemy IT od wielu lat korzystają ze standardowego protokołu TCP/IP, systemy OT używają wielu różnych protokołów, z których wiele jest specyficznych dla danej funkcji, branży lub lokalizacji geograficznej. W celu standaryzacji protokołów używanych w branży powołano do życia w latach 90-tych XX w. organizację OPC Foundation, która opracowała protokół OPC UA — rozwiązanie mające potencjał do ujednolicenia protokołów stosowanych we wszystkich systemach przemysłowych. Niestety taka konsolidacja raczej szybko nie nastąpi ze względu na częstość występowania starszych protokołów oraz dłuższe cykle wymiany systemów OT.

Cyberprzestępcy aktywnie starali się wykorzystać ten brak standaryzacji, atakując słabe ogniwa poszczególnych protokołów. Te problemy strukturalne pogłębia brak standardowych zabezpieczeń i słaba higiena zabezpieczeń obecna w przypadku wielu systemów OT (wynik lat braku połączenia z niezabezpieczonymi sieciami zewnętrznymi).

W kategoriach ilościowych dominują trzy protokoły.

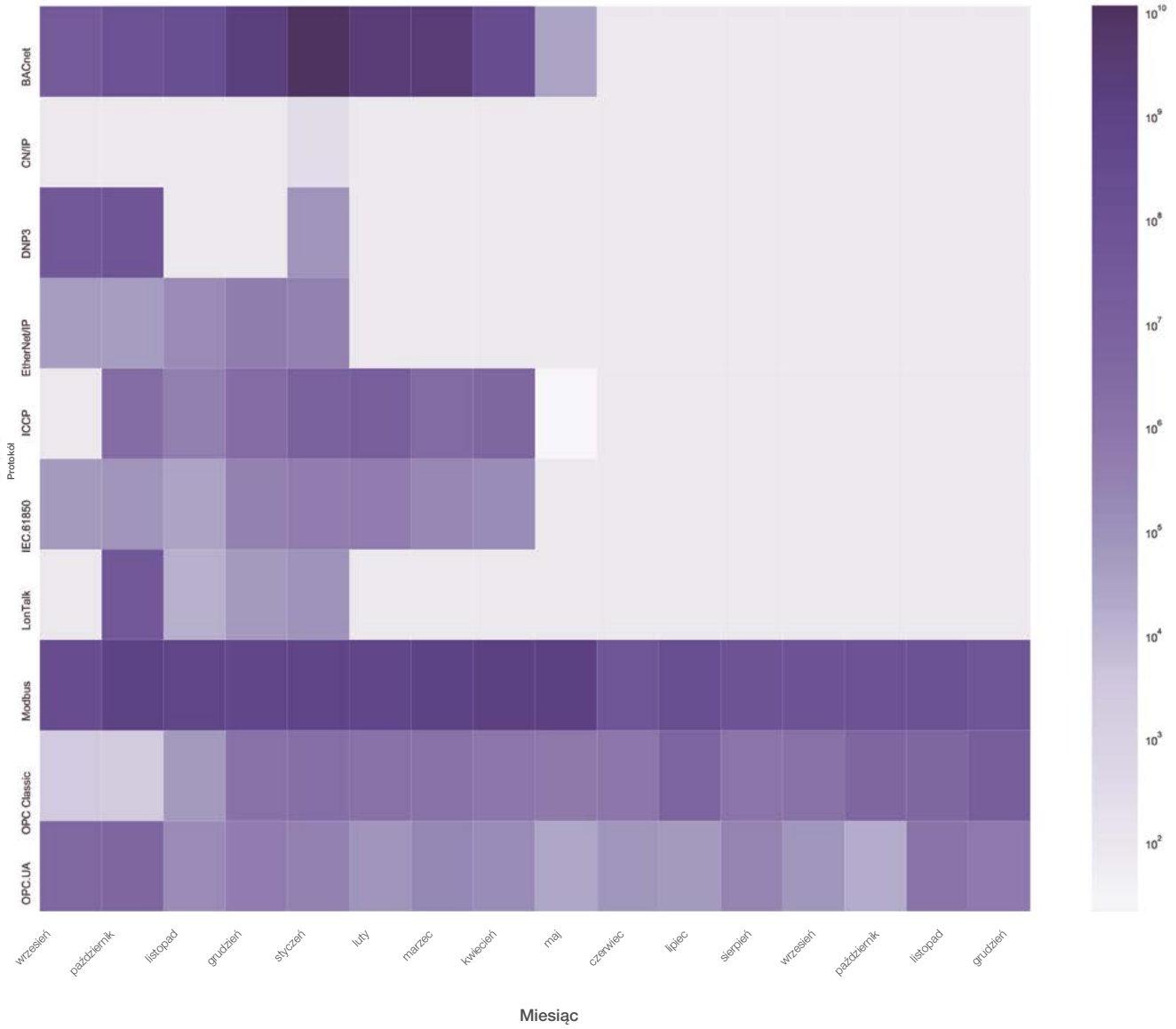
Wydaje się, że to, które protokoły są najczęściej celami ataku w kategoriach natężenia ruchu, zależy od dwóch czynników: powszechności użycia i podatności na zagrożenia. Protokoły OPC Classic, BACnet i Modbus odpowiadają łącznie za 85% sygnatur wykrywanych przez mechanizm kontroli aplikacji w kontekście systemów OT.

Zdecydowanie najczęściej atakowanym protokołem w kontekście ruchu sieciowego jest **OPC Classic** — poprzednik protokołu OPC UA, ale obecnie nadal znacznie bardziej od niego powszechny. Protokół ten korzysta z nowszej technologii niż niektóre inne protokoły (jego znaczna część została opracowana na przełomie XX i XXI w.), ale jego częstość występowania i „silosowy" sposób opracowania różnych elementów czyni z niego kuszący cel dla cyberprzestępców.

Automatyzacja budynków jest jednym z obszarów OT, w którym w większości przypadków korzysta się z jednego protokołu **BACnet**. Protokół ten jest stosowany w prawie każdym dużym przedsiębiorstwie niezależnie od branży, częściowo dlatego, że jest używany przez dużych dostawców systemów COWIG takich jak Johnson Controls i Carrier. W rezultacie BACnet jest drugim najczęściej stosowanym protokołem w kontekście systemów OT. Co więcej protokół BACnet jest oparty na bardzo starej technologii z 1987 r. Trzy z czterech największych zagrożeń w 2018 r. pod względem liczby zaatakowanych urządzeń były związane z protokołem BACnet (rys. 2). Liczba wykrytych ataków na komputery z protokołem BACnet szybko wzrosła w pierwszej połowie roku (rys. 3) wskutek działania botneta Mirai, którego ataki typu DDoS na systemy BACnet odnotowano na całym świecie[5]. Fakt, że botnet Mirai działał od października do grudnia 2018 r., a w tym czasie nie odnotowano ataków na urządzenia z protokołem BACnet wskazuje, że Mirai, „botnet do wynajęcia", nie był już używany do przeprowadzania ataków na urządzenia z protokołem BACnet, lecz raczej innych ataków na systemy OT.



Rys. 2. Cztery najczęściej wykrywane programy wykorzystujące luki w zabezpieczeniach protokołów według liczby urządzeń w 2018 r.

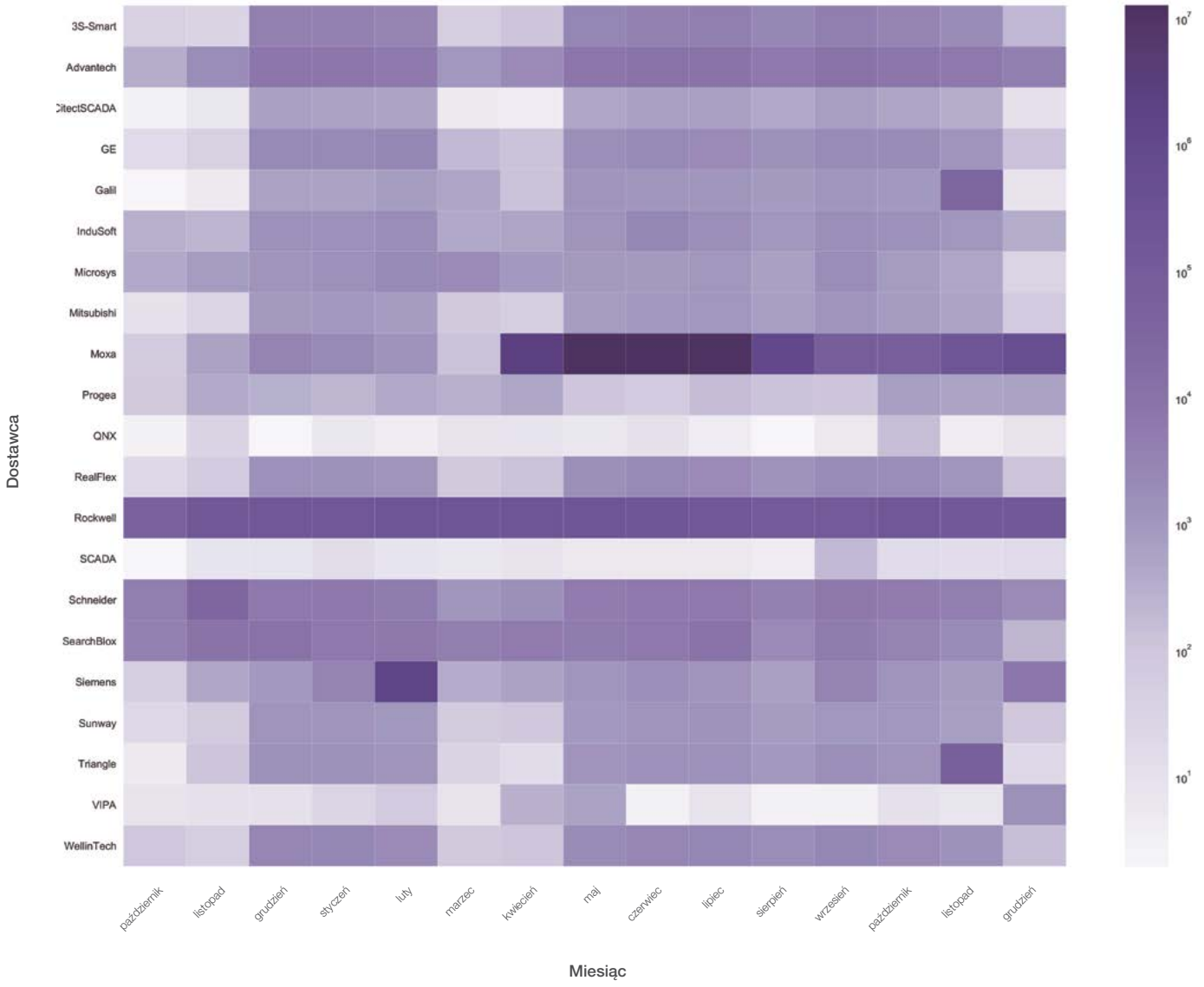


Rys. 3: Liczba wykrytych zagrożeń dla protokołów (wrzesień 2017 r. – grudzień 2018 r.).

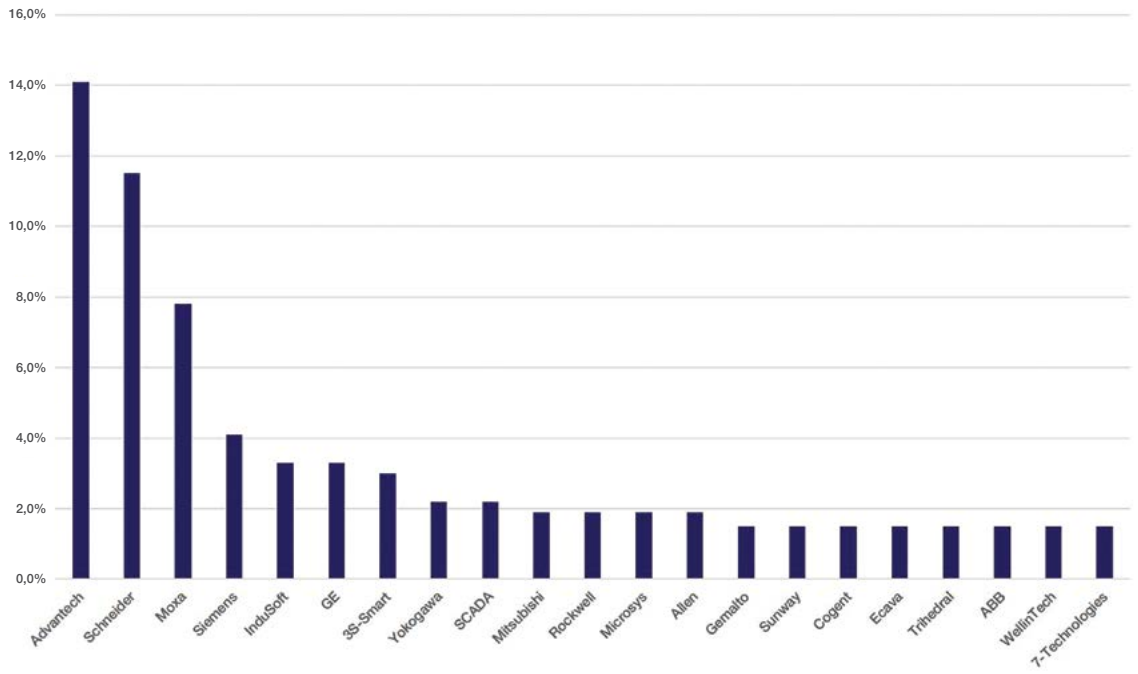
Trzeci najczęściej używany protokół, **Modbus**, to protokół komunikacyjny, który pomaga różnym składnikom systemów OT efektywnie ze sobą współdziałać. Protokół ten został opracowany w 1979 r. na potrzeby systemu zamkniętego (niepodłączonego do niezabezpieczonych sieci zewnętrznych). Modbus ma dziesiątki różnych wersji utworzonych przez różnych dostawców, co utrudnia zespołom ds. OT śledzenie jego podatności na zagrożenia.

Żaden dostawca systemów ICS/SCADA nie jest bezpieczny.

Ataki na każdego z 70 badanych przez firmę Fortinet dostawców OT zostały wykryte w 2018 r. i oprócz kilku specyficznych ataków, których celem były firmy Schneider i Moxa, ataki te były wykrywane konsekwentnie przez cały rok (rys. 4). Oznacza to, że najczęstszymi celami ataków pod względem unikatowych zagrożeń są jedne z największych firm na świecie takie jak Advantech, Schneider, Moxa i Siemens (rys 5). Ogólnie rzecz biorąc, starsze, bardziej złożone oferty dostawców mają więcej luk w zabezpieczeniach niż nowsze, bardziej usprawnione produkty.



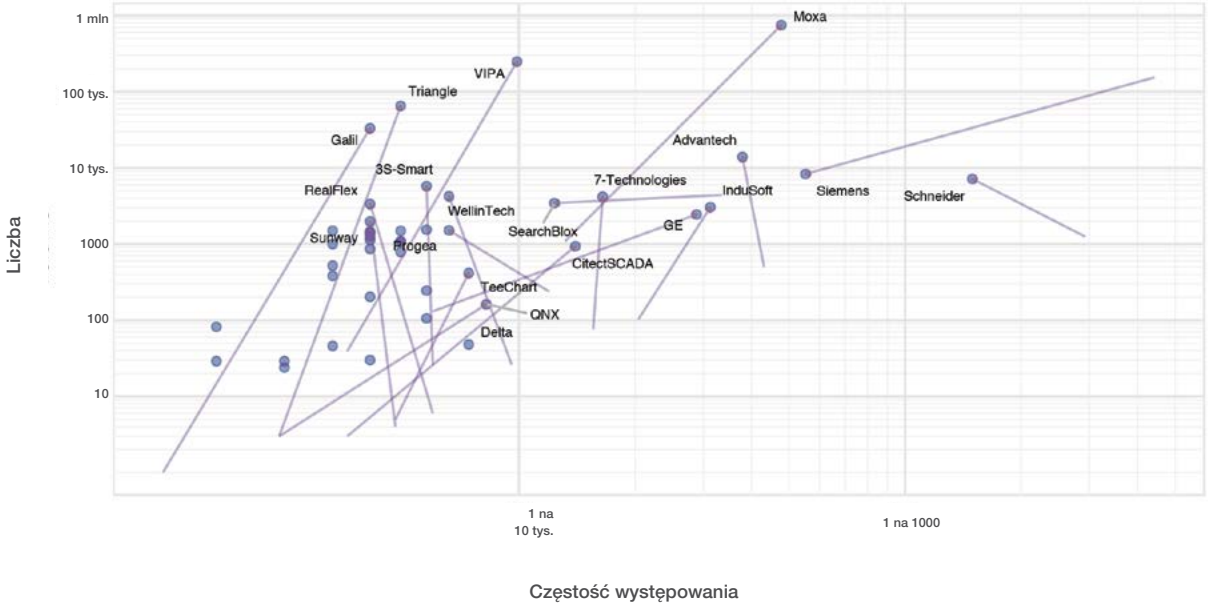
Rys. 4. Liczba wykrytych zagrożeń atakujących systemy ICS/SCADA (październik 2017 r. – grudzień 2018 r.).



Rys. 5. Najwięksi dostawcy systemów ICS/SCADA według liczby wykrytych niepowtarzalnych zagrożeń.

Ogólnie rzecz biorąc, ataki wykorzystujące infrastrukturę IT nasilają się.

Mimo sezonowych wahań i dużej różnorodności celów, w jednej kwestii dane są jednoznaczne: ataki na systemy OT wykorzystujące infrastrukturę IT nasilają się. Na przykład wykres 1 wskazuje, że liczba wykrytych nowych zagrożeń jest znacznie wyższa pod koniec roku niż na początku roku. Rys. 6 wskazuje natomiast, że w 2018 r. wzrosła zarówno liczba, jak i powszechność ataków na przemysłowe systemy sterowania niemal wszystkich dostawców. Nie ma podstaw, aby oczekiwać, że tendencja ta zmieni się w 2019 r. Liczba jest miarą ogólnej częstotliwości lub proporcji i przedstawia całkowitą liczbę lub odsetek obserwacji danego zagrożenia. Częstość występowania jest miarą obecności lub dominacji w poszczególnych grupach, ze wskazaniem odsetka przedsiębiorstw, które zgłosiły zagrożenie przynajmniej raz.



Rys. 6. Zmiany dotyczące częstości występowania i liczby programów wykorzystujących luki w zabezpieczeniach atakujących systemy ICS największych dostawców (Q1 – Q4 2018 r.).

Tendencja — ataki na systemy OT nadal są prowadzone, a celem są teraz systemy zabezpieczeń

Złośliwe oprogramowanie specyficzne dla systemów ICS i SCADA jest tworzone od co najmniej dekady, ale nie ma licznych jego przykładów (wymienić tu można w sumie oprogramowanie **Stuxnet, Havex i Industroyer** oraz ostatnio **Triton/Trisis**).

Przypuszcza się, że oprogramowanie Industroyer i Havex było początkowo używane przez siły zbrojne Rosji jako cyberbroń służąca do atakowania ukraińskich sieci energetycznych podczas rosyjskiej inwazji na ten kraj w 2016 r. Następnie oprogramowanie to wyciekło i było ponownie używane do ataków na sieci korzystające z tej samej co na Ukrainie infrastruktury Schneider Electric[11].

Nowe i niebezpieczne ataki na systemy bezpieczeństwa.

Celem złośliwego oprogramowania Triton/Trisis są kontrolery powszechnie stosowanego w branży energetycznej systemu bezpieczeństwa Triconex sprzedawanego również przez Schneider Electric. Pierwszą jego ofiarą padł zakład petrochemiczny w Arabii Saudyjskiej, który w 2017 r. został całkowicie zamknięty[12]. Biorąc pod uwagę fakt, że oprogramowanie to było wymierzone w system bezpieczeństwa, mogło być jednak jeszcze bardziej „złośliwe", niszcząc maszyny i stwarzając zagrożenie dla życia[13]. W kwietniu 2019 r. ogłoszono, że Triton/Trisis ma kolejną ofiarę — nienazwane przedsiębiorstwo na Bliskim Wschodzie[14]. Istnienie oprogramowania Triton/Trisis zaalarmowało specjalistów, ponieważ pod wieloma względami było ono sprawcą pierwszego prawdziwego cyberfizycznego ataku na systemy OT.



Oprogramowanie szyfrujące w celu wymuszenia okupu nadal atakuje systemy OT

Na początku 2018 r. laboratoria FortiGuard Labs odnotowały w środowiskach IT ogromny wzrost liczby ataków realizowanych za pomocą oprogramowania szyfrującego w celu wymuszenia okupu (ransomware) oraz przenoszących to oprogramowanie robaków[6]. Nastąpiło to tuż po szeroko zakrojonym i wysoce skutecznym ataku oprogramowania ransomware NotPetya, który w 2017 r. rzucił na kolana systemy IT i OT na całym świecie. Wśród zaatakowanych systemów OT znalazły się systemy:

- **Merck** — oprogramowanie NotPetya spowodowało zamknięcie systemów OT w większej części oddziałów tego giganta z branży farmaceutycznej. W efekcie zatrzymana została produkcja, a samo przedsiębiorstwo zostało zmuszone do pożyczenia z zapasów amerykańskiej agencji CDC (Centers for Disease Control) dawek szczepionki Gardasil o wartości 240 mln USD[7]. Łącznie poniesione przez Merck koszty ataku wyniosły niemal 1 mld USD.

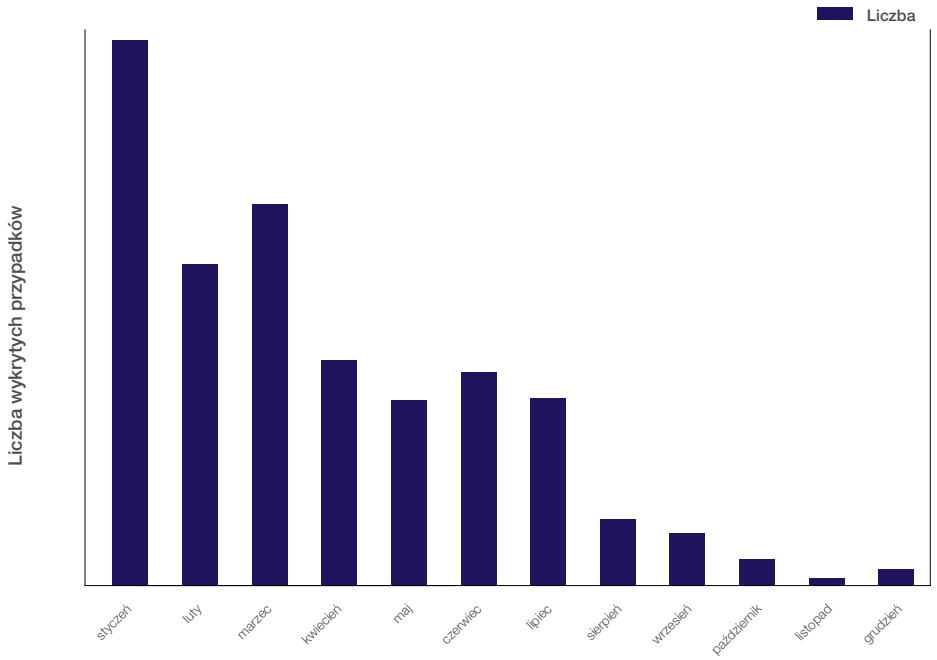
- **A.P. Møller – Maersk —** w wyniku działania oprogramowania NotPetya największa na świecie firma zajmująca się transportem kontenerowym odnotowała 20% spadek sprzedaży. Wartość ta byłaby znacznie większa, gdyby nie oddani pracownicy, którzy zaczęli ręcznie zarządzać działalnością globalną i w ciągu 10 dni odbudowali całą infrastrukturę elektroniczną[8]. Szacuje się, że poniesione przez A.P. Møller – Maersk koszty ataku wyniosły co najmniej 200 mln USD.

Pod koniec 2018 r. liczba ataków na systemy IT przy użyciu oprogramowania szyfrującego w celu wymuszenia okupu spadła, a wielu atakujących „przerzuciło się" na inne typy ataków takich jak na przykład złośliwe wydobywanie kryptowalut (cryptojacking)[9]. Niektórzy cyberprzestępcy wykorzystują jednak istniejące złośliwe oprogramowanie do ataków na systemy OT, z których wiele nie jest tak dobrze zabezpieczonych jak systemy IT. Może to sugerować, że w najbliższej przyszłości oprogramowanie szyfrujące w celu wymuszenia okupu będzie większym zagrożeniem dla systemów OT niż dla systemów IT. Stacje główne systemu SCADA są często obsługiwane przez system Microsoft Windows i sprzęt oparty na Linuksie, jeśli zatem nie zostaną wdrożone odpowiednie zabezpieczenia, może się tam pojawić oprogramowanie ransomware.

Możliwość wystąpienia takiego scenariusza została potwierdzona przeprowadzonym w marcu 2019 r. atakiem na koncern **Norsk Hydro**, giganta w produkcji aluminium, który został zmuszony do zamknięcia kilku zakładów, co w pierwszym tygodniu kosztowało go 40 mln USD. O ile związane z tym atakiem złośliwe oprogramowanie **LockerGoga** zostało najwyraźniej dopracowane i poprawione, jego pierwsze wcielenie było stosunkowo proste i powstało na bazie wcześniejszego złośliwego oprogramowania[10].

Trwają ataki na systemy OT przy użyciu starszych rozwiązań.

Dane z FortiGuard Labs wskazują, że złośliwe oprogramowanie ukierunkowane na systemy OT nadal atakuje urządzenia na całym świecie. Na przykład na rys. 7 przedstawiono odnotowane w 2018 r. próby ataku za pomocą oprogramowania Industroyer, szczególnie intensywne w pierwszej połowie tego roku. Złożone złośliwe oprogramowanie takie jak Industroyer zazwyczaj ma dużą „żywotność", nawet po jego wykryciu i umieszczeniu w odpowiednich miejscach jego sygnatur.



Rys. 7. Liczba wykrytych przypadków złośliwego oprogramowania Industroyer w 2018 r.

EternalBlue — zagrożenie dla starszych systemów Windows

Autorem oprogramowania EternalBlue jest Agencja Bezpieczeństwa Narodowego (NSA), co wynika z zeznań jej byłych pracowników. 24 kwietnia 2017 r. oprogramowanie to zostało wykradzione przez grupę hakerską Shadow Brokers i użyte podczas przeprowadzonych w tym samym roku za pomocą oprogramowania WannaCry i NotPetya ataków mających na celu wymuszenie okupu. Uważa się również, że EternalBlue wchodzi w skład używanego do ataków na banki trojana Retefe. EternalBlue wykorzystuje lukę w zabezpieczeniach protokołu Microsoft Server Message Block (SMB).

Microsoft zaktualizował protokół SMB do nowego protokołu CIFS (Common Internet File Sharing), aby w systemach IT z uaktualnioną infrastrukturą Microsoft Windows po prostu wystarczyło skonfigurować protokół CIFS tak, aby nie akceptował żądań używających starszego protokołu SMB. Niestety wiele systemów ICS/SCADA bazuje na starszych wersjach systemu Windows, które nie obsługują protokołu CIFS. W rezultacie konieczne jest wdrożenie zewnętrznych mechanizmów kontroli w zaporze następnej generacji (NGFW), które obsłużą określone rodzaje ruchu SMB i odrzucą inne typy.

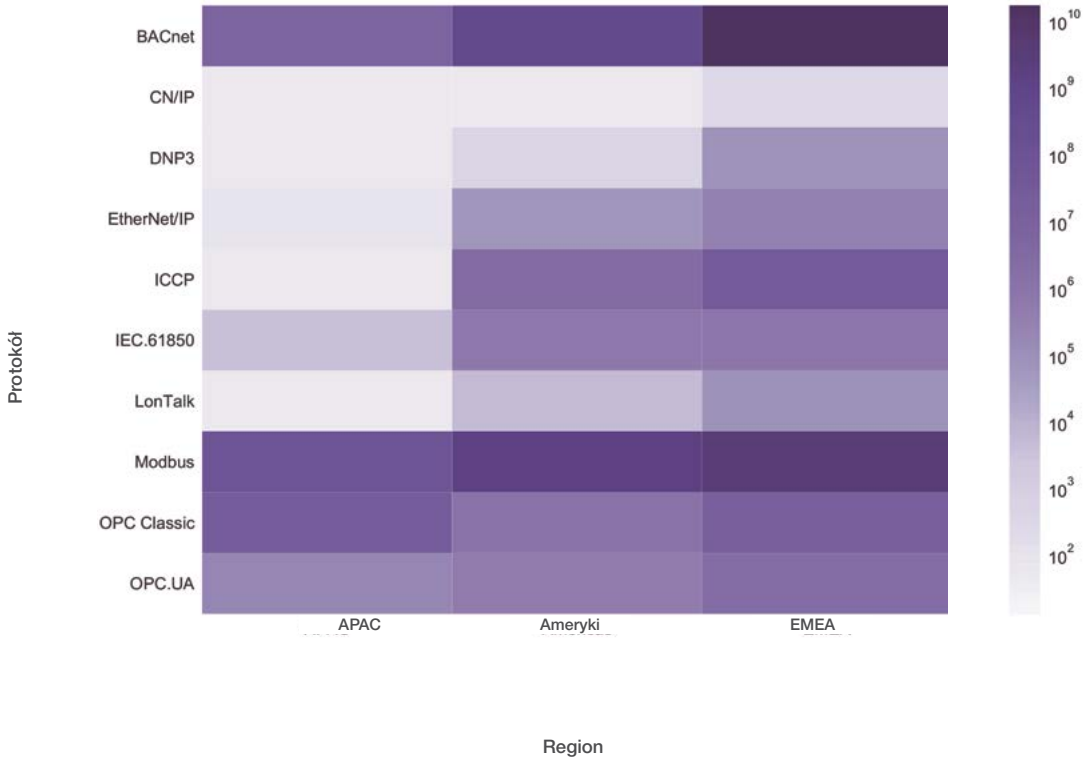
Tendencja — ataki na systemy OT nie zależą od lokalizacji geograficznej

W światowej gospodarce zdominowanej w wielu sektorach przemysłu przez podmioty globalne i cechującej się bardzo wysokim stopniem powiązań sieciowych bariery geograficzne mogą być już bez trudu pokonywane przez podmioty działające zarówno legalnie, jak i nielegalnie. Na rys. 8 pokazano, że o ile ataki na systemy większości dostawców były stosunkowo równo rozłożone w poszczególnych regionach, o tyle ataki na systemy Rockwell i Schneider w nieproporcjonalnie dużym stopniu miały miejsce w Ameryce Północnej i Południowej, gdzie udział tych systemów w rynku jest największy. Powszechnie stosowane systemy Moxa były natomiast silnie atakowane na całym świecie, mimo że największy atak na ten system miał miejsce w Japonii (zob. „Ukierunkowany atak na lukę Moxa 313" na stronie 13).



Rys. 8. Rozkład regionalny przypadków wykrycia ataków na konkretnych dostawców systemów ICS/SCADA w 2018 r.

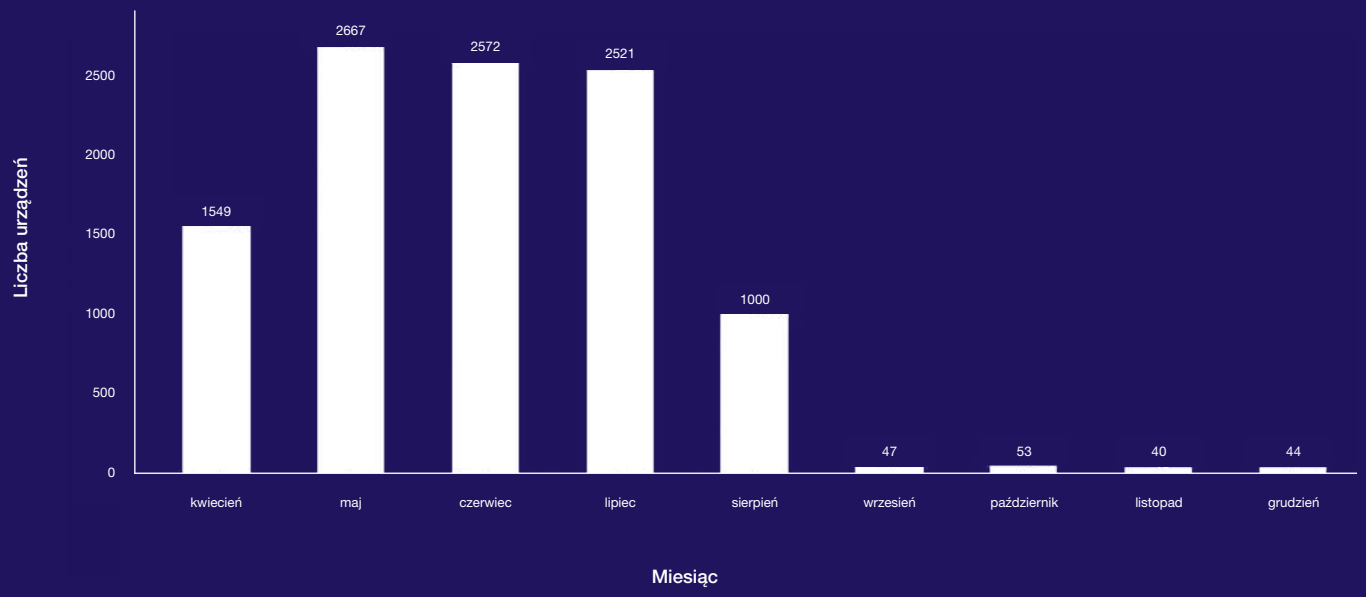
Na rys. 9 pokazano, że protokoły BACnet i Modbus są powszechnie stosowane na całym świecie, ale najbardziej intensywnie w regionie EMEA. Liczba wykrytych protokołów była albo dość równomiernie rozłożona w poszczególnych regionach geograficznych, albo bardziej skupiona w obszarach, w których są one najczęściej używane. Na przykład protokół ICCP jest używany głównie przez dostawców takich jak Siemens i Honeywell, którzy są w mniejszym stopniu obecni w Azji.



Rys. 9. Rozkład regionalny przypadków wykrycia ataków na konkretne protokoły w 2018 r.

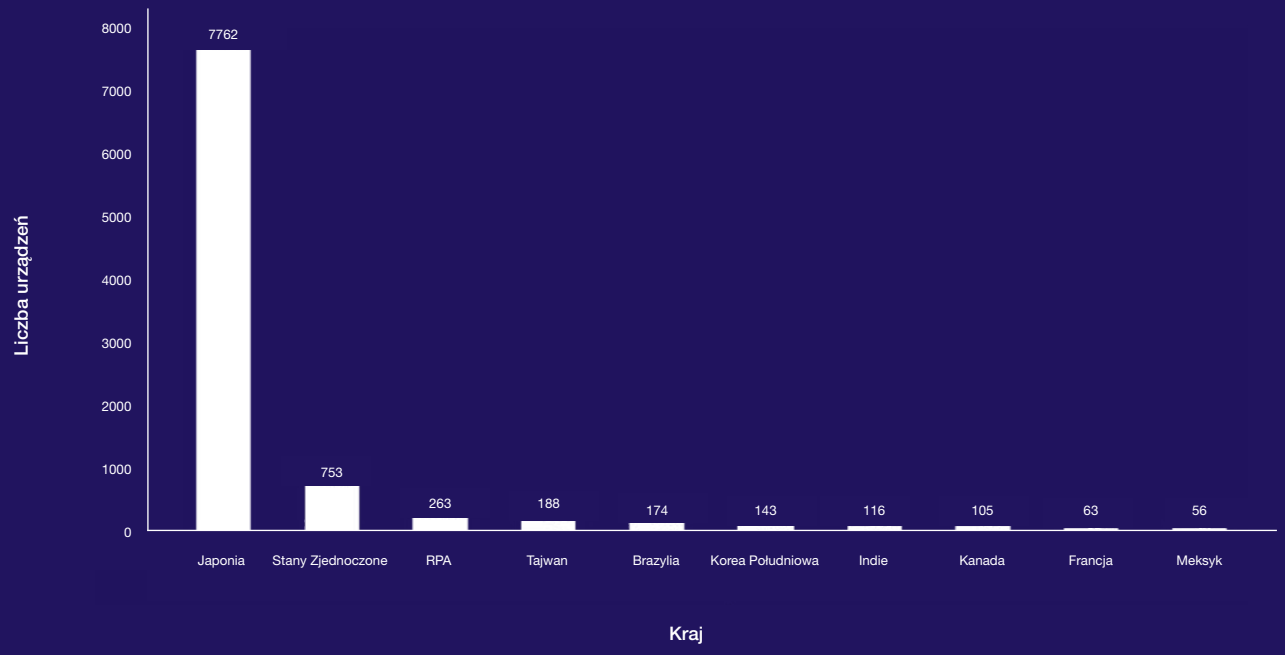
Ukierunkowany atak na lukę Moxa 313

Ten ujawniony w kwietniu 2018 r. atak wykorzystał lukę w zabezpieczeniach urządzeń Moxa związaną z wykonywaniem poleceń systemu operacyjnego. Istotą tej luki był brak weryfikacji przez system danych wejściowych podczas przetwarzania złośliwych żądań Telnet. Atak dotknął jedna za drugą tysiące zapór NGFW w kwietniu, maju i czerwcu, a potem do września niemal całkowicie wygasł (rys. 10), prawdopodobnie ze względu na wdrożenie odpowiednich aktualizacji zabezpieczeń.



Rys. 10: Liczba przypadków wykrycia ataków na lukę Moxa 313 według miesięcy w 2018 r.

Analiza geograficzna tego przypadku ujawniła, że atak był terytorialnie niemal całkowicie ograniczony do Japonii (rys. 11), w której technologie Moxa są szeroko stosowane w produktach automatyki domowej i biznesowej. Technologie Moxa są jednak również powszechnie stosowane w innych krajach świata. Fakt, że ten atak rozwinął się tak szybko, nawet w odizolowanej przestrzeni geograficznej, potwierdza, że atakujący skłaniają się do brania na cel najmniejszych i najprostszych elementów infrastruktury OT: mostów i konwerterów szeregowych.



Rys. 11: Liczba przypadków wykrycia ataków na lukę Moxa 313 według krajów w 2018 r.

Podsumowanie

Przygotowany przez firmę Fortinet raport o tendencjach w zakresie zabezpieczeń technologii operacyjnych w 2019 r. przedstawia zagrożenia, które powinny być brane na poważnie przez przedsiębiorstwa, których systemy ICS/SCADA są podłączone do niezabezpieczonych sieci zewnętrznych. Atakujący myślą strategicznie i do granic możliwości wykorzystują każde opracowane przez siebie nowe zagrożenie, atakując niechronione systemy i luki w zabezpieczeniach starszych i nowszych technologii. Szczególne wyzwania wynikające z dłuższych cykli wymiany i korzystania przez to ze starszych technologii będą nadal aktualne przez kolejne lata.

W reakcji na te nowe zagrożenia, zwłaszcza w odniesieniu do infrastruktury krytycznej, gdzie ryzyko jest bardzo duże i obejmuje nawet pojawienie się globalnego załamania gospodarczego, rządy poszczególnych krajów opracowały wytyczne, które mają pomóc przemysłowi w ochronie kluczowych zasobów. Na przykład w odpowiedzi na awarię sieci energetycznej w 2003 r., do której doszło w północno-wschodniej części Stanów Zjednoczonych, przyjęto normy NERC (North American Electric Reliability Corporation). Fakt, że normy takie jak NERC i NIST (National Institute of Standards and Technology) stają się coraz bardziej rygorystyczne, to kolejny dowód na to, że zagrożenie jest realne.

W wielu przedsiębiorstwach systemy ICS i SCADA przez dekady nie były poddawane istotnym uaktualnieniom. W obliczu ataków APT potrzebne jest jednak bardziej strategiczne podejście i wdrożenie wszystkich potrzebnych zabezpieczeń, od zwykłych poprawek, po mechanizmy segmentacji i kontroli dostępu. Systemy te po prostu muszą podlegać temu samemu poziomowi zabezpieczeń, tym samym normom higieny zabezpieczeń, temu samemu poziomowi ochrony bezpieczeństwa, tym samym standardom higieny bezpieczeństwa i tym samym procesom śledzenia i raportowania co sieci IT. W przeciwnym razie sieć OT okaże się słabym ogniwem, za pośrednictwem którego złośliwe oprogramowanie przedostanie się do sieci wewnętrznej i uzyska dostęp do krytycznych systemów i danych, zarówno OT, jak i IT.

Aby nie dopuścić do takiej sytuacji, osoby odpowiedzialne w przedsiębiorstwach za systemy IT i OT muszą przezwyciężyć kulturowe wyzwania związane z dotychczasową izolacją tych systemów i zrozumieć swoje wzajemne potrzeby, aby wypracować na przyszłość obopólnie korzystne relacje. Zagrożenia są realne i coraz większe. Najlepszym sposobem, aby im przeciwdziałać, jest wdrożenie kompleksowej strategii obejmującej całe przedsiębiorstwo.

Źródła

[1] Barbara Filkins, „The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns", SANS Analyst Program, lipiec 2018 r.

[2] Jeff Goldman, „IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices", eSecurity Planet, 8 listopada 2017 r.

[3] „State of Operational Technology and Cybersecurity Report", Fortinet, marzec 2019 r.

[4] „Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks", Fortinet, 7 maja 2018 r.

[5] Oliver Gasser, et al., „Security Implications of Publicly Reachable Building Automation Systems", Technical University of Munich, dostęp z dnia 18 kwietnia 2019 r.

[6] „Quarterly Threat Landscape Report, Q4 2018" Fortinet, dostęp z dnia 9 kwietnia 2019 r.

[7] Eric Palmer, „Merck has hardened its defenses against cyberattacks like the one last year that cost it nearly $1B", FiercePharma, 28 czerwca 2018 r.

[8] Richard Chirgwin, „IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz", The Register, 25 stycznia 2018 r.

[9] „Quarterly Threat Landscape Report, Q4 2018" Fortinet, dostęp z dnia 9 kwietnia 2019 r.

[10] Lindsey O'Donnell, „Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities", Threatpost, 27 marca 2019 r.

[11] Charlie Osborne, „Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout", ZDNet, 30 kwietnia 2018 r.

[12] Lily Hay Newman, „Menacing Malware Shows the Dangers of Industrial System Sabotage", WIRED, 18 stycznia 2018 r.

[13] „FortiGuard Threat Intelligence Brief", Fortinet, 2 lutego 2018 r.

[14] Tara Seals, „SAS 2019: Triton ICS Malware Hits A Second Victim", Threatpost, 10 kwietnia 2019 r.

FORTINET

www.fortinet.com

Copyright © 2019 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare®, FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmie, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).

czerwca 27, 2019 12:03 PM

D:\ARGOS\2019\06_2019\Assignment A-344888-940697\Work\PAKIET\OT\General\Report-security trends-A4_PL\Report-security trends-A4_PL

352048-0-1-PL