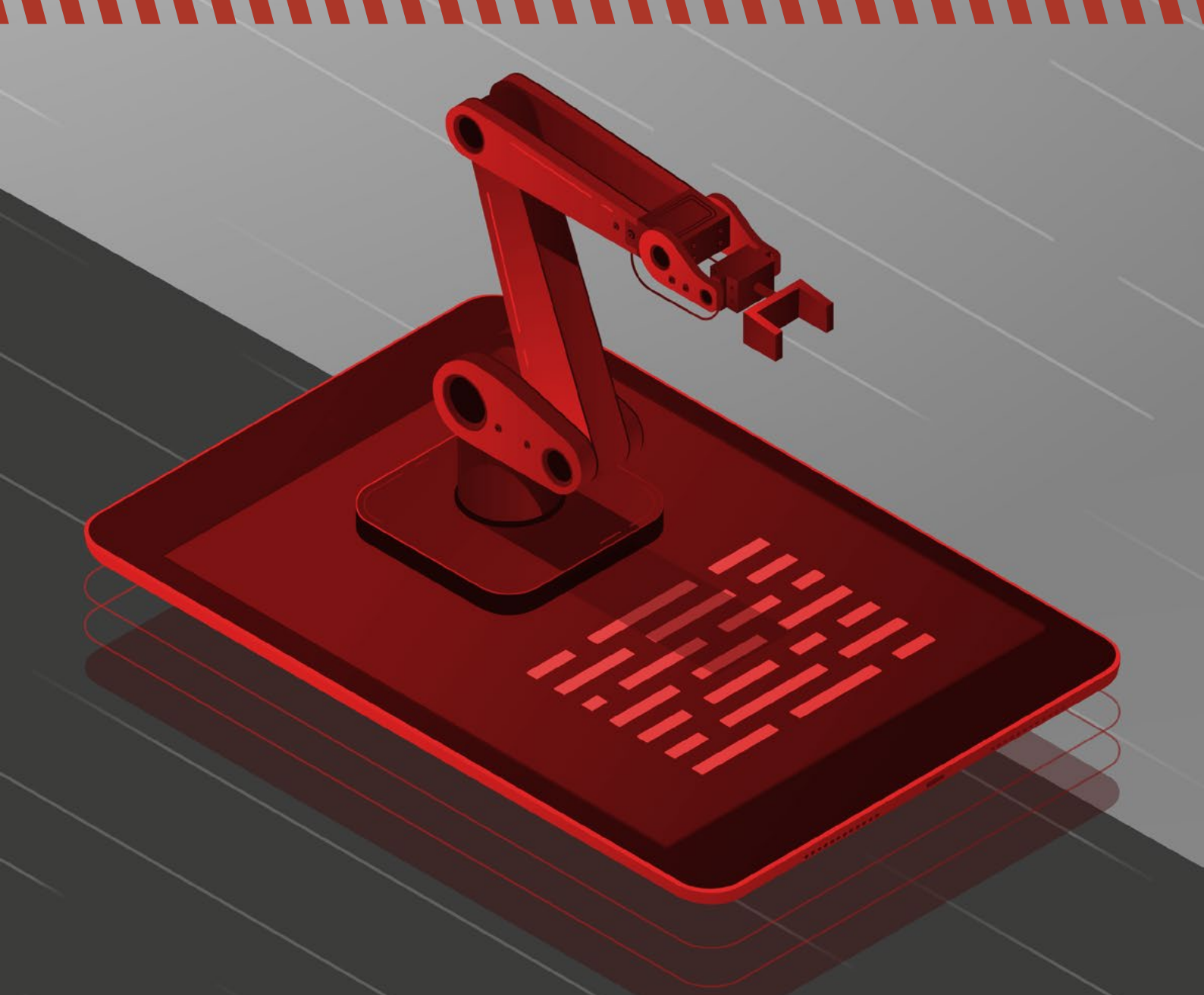


Fabryka-pułapka

sposobem na przeanalizowanie zagrożeń wymierzonych w systemy automatyki przemysłowej

Zbudowana przez ekspertów zespołu Threat Research w Trend Micro infrastruktura, symulująca funkcjonowanie realnego środowiska IT w małym zakładzie produkcyjnym, pomogła w ocenie sposobów działania cyberprzestępców podejmujących działania wymierzone w sektor przemysłowy. Opisujemy jakimi pobudkami kierowały się osoby stojące za atakami przeprowadzonymi na środowisko badawcze Trend Micro.

iTWIZ

TREND MICRO™

O szczegółach projektu badawczego, mającego na celu ocenę zagrożeń wymierzonych w firmy z sektora produkcyjnego, założeniach budowy systemu honeypot – fabryki-pułapki, wykorzystanych rozwiązaniach, wykrytych zagrożeniach i interakcjach z hakerami, a także zaleceniach w zakresie zapewnienia bezpieczeństwa IT na przykładzie niewielkiej firmy produkcyjnej, mówi Rainer Vosseler, członek zespołu Threat Research w Trend Micro.

Eksperyment Trend Micro pokazał, jak duże ryzyko występuje w obszarze bezpieczeństwa systemów przemysłowych

Na potrzeby analizy ataków ukierunkowanych na sektor przemysłowy w 2019 roku zastawili Państwo pułapkę na hakerów…

To prawda. Wyniki naszych analiz opierają się na fikcyjnym środowisku, które zostało zbudowane tak, aby symulowało działanie faktycznych systemów IT, typowych dla stosunkowo małego przedsiębiorstwa produkcyjnego. Wykorzystaliśmy wiele narzędzi pozwalających nam obserwować poczynania intruzów w naszym środowisku. Celowo popełniliśmy też błędy w zakresie konfiguracji systemów IT. W pewnym sensie rzeczywiście zastawiliśmy pułapkę na osoby próbujące podejmować działania o charakterze cyberprzestępczym.

Nie był to nasz pierwszy tego rodzaju projekt. Kilka lat temu uruchomiliśmy podobne środowisko na potrzeby analizy zagrożeń wymierzonych w organizacje z sektora użyteczności publicznej, konkretnie przedsiębiorstwa wodno-kanalizacyjne. W roku 2015 przeprowadziliśmy – także oparte na symulowanym środowisku typu honeypot – analizy ataków ukierunkowanych na podmioty zarządzające zbiornikami gazowymi. W odróżnieniu od najnowszego badania, poprzednie analizy opierały się głównie na rozwiązaniach aplikacyjnych. Zbudowaliśmy zwirtualizowane środowiska, symulujące systemy zarządzania infrastrukturą gazową i wodno-kanalizacyjną. Wówczas wpadliśmy na pomysł stworzenia bardziej rozbudowanego systemu, wykorzystującego również wyspecjalizowane rozwiązania sprzętowe, który zrealizowaliśmy w 2019 roku.

Z jakich rozwiązań sprzętowych i aplikacyjnych zbudowali Państwo środowisko symulujące systemy zakładu produkcyjnego?

Fizycznie nie były to bardzo zaawansowane rozwiązania, choć wykorzystaliśmy sprzęt rzeczywiście spotykany w firmach produkcyjnych. Były to sterowniki PLC trzech różnych dostawców, odpowiednio skonfigurowane rozwiązania sieciowe, a także maszyny wirtualne związane z obsługą systemu sterowania produkcją czy z oprogramowaniem ABB RobotStudio.

Więcej pracy z naszej strony wymagało za to przygotowanie całościowej, fikcyjnej tożsamości organizacji, którą nazwaliśmy MeTech. Miała to być stosunkowo niewielka firma, świadcząca usługi związane z prototypowaniem dla większych podmiotów przemy-

słowych, m.in. z sektora motoryzacyjnego. Zależało nam na tym, aby haker, który włamie się do naszej infrastruktury, widział aplikacje i procesy systemowe spotykane w rzeczywistych środowiskach IT. Co więcej, chcieliśmy, aby te procesy funkcjonowały podobnie do tego, jak dzieje się to w praktyce. Dlatego też opracowaliśmy m.in. skrypty symulujące zachowanie rozwiązań robotyki przemysłowej wykonujących pewne operacje, zarówno w warstwie zarządzania, jak i bieżącego sterowania. Tym samym daliśmy cyberprzestępcom szerokie możliwości działania w ramach naszego środowiska. Mogli oni np. przeprogramować system automatyki produkcyjnej, choć oczywiście żadnym robotem faktycznie nie dysponowaliśmy. Podobne symulatory opracowaliśmy również dla sterowników PLC i innych specjalistycznych rozwiązań imitujących w naszym środowisku prawdziwe przedsiębiorstwo. Opracowanie logiki oraz współzależności pomiędzy poszczególnymi elementami naszej fikcyjnej fabryki było niezwykle czasochłonne, ale i opłacalne ze względu na uzyskany efekt.

Upewniliśmy się też, że nikt nie będzie w stanie zidentyfikować naszego środowiska jako systemu honeypot. Wymagało to od nas szczegółowej analizy konfiguracji oraz usunięcia narzędzi powszechnie wykorzystywanych do budowy takich środowisk. Zbudowaliśmy również rozbudowane mechanizmy, pozwalające monitorować działania podejmowane przez potencjalnych włamywaczy w naszym środowisku w czasie rzeczywistym. Dotyczy to także m.in. nagrywania ekranu każdego użytkownika naszej infrastruktury. Mogliśmy więc na bieżąco obserwować działania hakerów.

Od maja do grudnia 2019 roku - czyli w okresie, kiedy odbywał się eksperyment - zaobserwowaliśmy bardzo zróżnicowane ataki wymierzone w nasze środowisko. Były to zarówno próby wykorzystania go do dalszych nadużyć - tzn. kradzieży danych, podglądania operacji wykonywanych przez poszczególne systemy, modyfikacji konfiguracji systemów przemysłowych - a nawet wandalizmu, czyli zatrzymywania newralgicznych procesów, w celu wygenerowania niedostępności kluczowych systemów biznesowych. Najbardziej powszechne były jednak ataki ransomware, a także te związane z wykorzystaniem zasobów naszej infrastruktury na potrzeby „kopania" kryptowalut. Co ciekawe, niektóre ataki pokrywały się ze sobą i wchodziły sobie w drogę. Przykładowo, jedna próba kradzieży danych została zablokowana atakiem ransomware.

Stworzyli Państwo również całą fikcyjną organizację biznesową…

Staraliśmy się zbudować realistyczne środowisko MeTech zarówno w wymiarze IT, jak i wizerunkowym. Na stronie internetowej naszej fałszywej firmy zamieściliśmy właściwie wszystkie elementy spotykane na witrynach rzeczywistych organizacji z tego sektora. Wykorzystaliśmy wizerunki rzekomych pracowników, które zostały wygenerowane przez algorytmy sztucznej inteligencji. Uruchomiliśmy również dedykowane numery telefonów. Przygotowali-

Zapewnienie bezpieczeństwa IT we wszystkich organizacjach biznesowych powinno być postrzegane w kategorii ciągłego, powtarzalnego procesu. Przede wszystkim należy zinwentaryzować posiadane rozwiązania i systemy IT oraz ocenić ich realną wrażliwość na zagrożenia i faktyczne znaczenie biznesowe. W pierwszej kolejności warto jednak sięgnąć po dobre praktyki, aby zminimalizować ryzyko zagrożeń opartych na prostych, powtarzalnych błędach. Oczywiście konieczne jest też zapewnienie fundamentalnych rozwiązań bezpieczeństwa, takich jak zapory firewall czy systemy klasy IPS. Ogromne znaczenie ma również monitoring działania środowiska IT.

śmy też techniczne i marketingowe treści, opisujące działalność fikcyjnej organizacji.

Staraliśmy się także przywiązywać dużą wagę do detali. Udając małą firmę, niejako start-up, co jakiś czas wyłączaliśmy całość infrastruktury produkcyjnej, symulując faktyczne zachowania małych zakładów produkcyjnych w okresach świąt czy wakacji. Wszystko po to, aby zapewnić jak najwyższą wiarygodność naszego środowiska-pułapki. Nasze działania się opłaciły, ponieważ w stosunkowo krótkim czasie tak stworzone środowisko, czy raczej błędy, które umyślnie popełniliśmy w jego konfiguracji, zostały zgłoszone do zespołu Industrial Control Systems Cyber Emergency Response Team – ICS-CERT, który zajmuje się monitorowaniem bezpieczeństwa oraz podatności w systemach automatyki przemysłowej. Z pewnością był to pewnego rodzaju sukces, z którego jednak musieliśmy tłumaczyć się przed ICS-CERT.

Jak to się stało, że Państwa środowisko-pułapka znalazło się w obszarze zainteresowań cyberprzestępców?

Upewniliśmy się, że odszukanie naszego środowiska nie będzie trudne, inaczej cały projekt nie miałby większego sensu. Postaraliśmy się więc o to, aby było ono zaindeksowane w wyszukiwarce Shodan, która pozwala odszukać określone rodzaje urządzeń podłączonych do internetu. Jest dość często używana przez osoby, które chcą zaatakować systemy konkretnych producentów. Zamieściliśmy też kilka wpisów sugerujących występowanie podatności w naszym środowisku w serwisie Pastebin.

Umyślnie pozostawiliśmy w naszym środowisku wiele otwartych portów, standardowo wykorzystywanych przez niektóre rozwiązania, narażając się na ataki rozpoczynające się od skanowania podatności infrastruktury. Zadbaliśmy również o ustawienie stosunkowo prostych haseł do niektórych jej elementów oraz aby nasze zasymulowane systemy specjalistyczne były osiągalne z internetu. Brak separacji był tu bardzo istotnym czynnikiem, obniżającym poziom bezpieczeństwa naszego środowiska. Zachowaliśmy tu jednak umiar, aby nie wzbudzać podejrzeń ze strony atakujących i otwierać na świat tylko te rozwiązania, w przypadku których miało to jakiś sens dla naszych rzekomych pracowników. W skrócie, skumulowaliśmy w ramach jednej infrastruktury dużo błędów, dość powszechnie popełnianych w mniejszych organizacjach, a również w odniesieniu do systemów przemysłowych. Nasz eksperyment pokazał, jak duże jest ryzyko w obszarze bezpieczeństwa IT małych i średnich firm.

Jakiego rodzaju ataki i zagrożenia udało się Państwu zaobserwować?

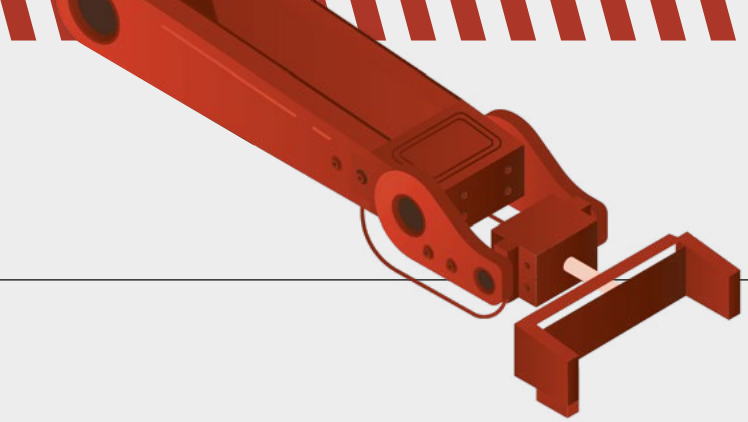
Od maja do grudnia 2019 roku – czyli w okresie, kiedy odbywał się eksperyment – zaobserwowaliśmy bardzo zróżnicowane ataki wymierzone w nasze środowisko. Były to zarówno próby wykorzystania go do dalszych nadużyć – tzn. kradzieży danych, podglądania operacji wykonywanych przez poszczególne systemy, modyfikacji konfiguracji systemów przemysłowych – a nawet wandalizmu, czyli zatrzymywania newralgicznych procesów, w celu wygenerowania niedostępności kluczowych systemów biznesowych. Najbardziej powszechne były jednak ataki ransomware, a także te związane z wykorzystaniem zasobów naszej infrastruktury na potrzeby „kopania" kryptowalut.

Co ciekawe, niektóre ataki pokrywały się ze sobą i wchodziły sobie w drogę. Przykładowo, jedna próba kradzieży danych została zablokowana atakiem ransomware skutecznie przeprowadzonym przez inną osobę. Zaobserwowaliśmy m.in. aplikację przesyłającą nieznanym odbiorcom małe paczki danych. Zanim jednak udało nam się pozyskać więcej informacji, została ona zaszyfrowana wraz z całym środowiskiem podczas równolegle prowadzonego ataku ransomware. Warto tutaj zaznaczyć, że mieliśmy też do czynienia z hakerami o dobrych intencjach. Jedna z takich osób pozostawiła nam wiadomość z rekomendacjami wdrożenia zmian konfiguracji, które pozwolą podnieść bezpieczeństwo naszych systemów.

Przeraża fakt, że po kilku miesiącach negocjowali Państwo z cyberprzestępcami wysokość okupu…

Rzeczywiście, negocjacje potraktowaliśmy jako część projektu badawczego. Udało nam się utargować kwotę okupu z 10 000 do 6 000 USD. Oczywiście ostatecznie żadnych środków nie zapłaciliśmy, a jedynie przywróciliśmy nasze środowisko z przygotowanej wcześniej kopii. W rzeczywistych sytuacjach niestety nie zawsze jest taka możliwość. Tymczasem, zwłaszcza w przypadku małych i średnich firm, ryzyko ataku ransomware jest stosunkowo wysokie.

Które z zaobserwowanych w symulowanym środowisku ataków stanowiły potencjalnie największe zagrożenie dla działalności Państwa fikcyjnej firmy?



Z pewnością były to ataki ransomware, które mogą narazić firmę na poważne koszty, a jednocześnie uniemożliwić bieżące funkcjonowanie. Bardzo bolesne w skutkach mogą być również ataki ukierunkowane na kradzież własności intelektualnej. Trudno jednak uogólniać, ponieważ w zależności od sytuacji i specyfiki każdej organizacji, nawet chwilowe zatrzymanie normalnego przebiegu procesu produkcyjnego może generować ogromne straty. Praktyka pokazuje więc, że problematyczne są także ataki phishingowe związane z kradzieżą danych uwierzytelniających, których z oczywistych powodów w naszym środowisku nie zanotowaliśmy. Nie zaobserwowaliśmy też ataków nietypowych czy wymierzonych specyficznie w infrastrukturę przemysłową, choć pojawiały się próby podglądania lub ingerowania w konfigurację sterowników PLC. Być może wynikało to z faktu, że symulowaliśmy środowisko stosunkowo małej organizacji. Większość atakujących nastawiła się bowiem na działania zmierzające do stosunkowo szybkiego osiągnięcia korzyści finansowych – czy to w formie okupu, czy też wygenerowanych kryptowalut.

Wyniki naszych analiz opierają się na fikcyjnym środowisku, które zostało zbudowane tak, aby symulowało działanie faktycznych systemów IT, typowych dla stosunkowo małego przedsiębiorstwa produkcyjnego. Wykorzystaliśmy wiele narzędzi, pozwalających obserwować poczynania intruzów w naszym środowisku. Celowo popełniliśmy też błędy w zakresie konfiguracji systemów IT. W pewnym sensie rzeczywiście zastawiliśmy pułapkę na osoby próbujące podejmować działania o charakterze cyberprzestępczym.

Jakich zasad należy przestrzegać, aby uniknąć choć części incydentów, które wykryli Państwo w swoim środowisku?

Należy postępować według dobrych praktyk związanych choćby z generowaniem haseł. Gdyby nasze środowisko było skonfigurowane w sposób zgodny z nimi, to z pewnością zaobserwowalibyśmy dużo mniej przypadków naruszenia bezpieczeństwa. Należy jednak pamiętać, że mamy do czynienia z dość powszechnym dążeniem do podłączania systemów OT do internetu, a także integracji świata OT ze światem IT. Oznacza to, że w wielu firmach pojawia się konieczność zabezpieczenia dostępu do urządzeń, które często nie były projektowane z myślą o takiej właśnie integracji. Kluczowego znaczenia nabierają tu więc zarówno kwestie właściwej organizacji obszaru bezpieczeństwa IT, jak i posiadania odpowiednich narzędzi, w tym rozwiązań pozwalających na bieżący monitoring zdarzeń zachodzących w całym środowisku.

W jaki sposób firmy produkcyjne powinny podejść do kwestii zapewnienia bezpieczeństwa środowiska, na które obok typowych systemów IT składają się rozwiązania klasy OT?

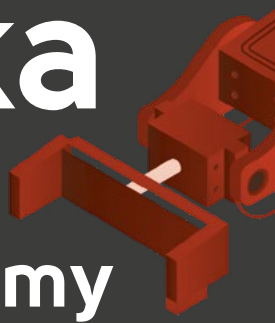
Zapewnienie bezpieczeństwa IT we wszystkich organizacjach biznesowych powinno być postrzegane w kategorii ciągłego, powtarzalnego procesu. Przede wszystkim należy zinwentaryzować posiadane rozwiązania i systemy IT oraz ocenić ich realną wrażliwość na zagrożenia i faktyczne znaczenie biznesowe. W pierwszej kolejności warto jednak sięgnąć po dobre praktyki, aby zminimalizować ryzyko zagrożeń opartych na prostych, powtarzalnych błędach. Oczywiście konieczne jest też zapewnienie fundamentalnych rozwiązań bezpieczeństwa, takich jak zapory firewall czy systemy klasy IPS. Ogromne znaczenie ma również monitoring działania środowiska IT. Tylko dzięki temu będziemy w stanie ocenić efektywność wdrożonych rozwiązań bezpieczeństwa i podejmować racjonalne decyzje związane z przeciwdziałaniem incydentom.

W tego rodzaju potrzeby świetnie wpisują się rozwiązania Trend Micro, choćby – chroniące przed konkretnymi zagrożeniami – urządzenia z linii TippingPoint czy – wspierająca wykrywanie ataków ukierunkowanych i potencjalnych zagrożeń – platforma Deep Discovery. Naszą ofertę systematycznie rozwijamy na podstawie wniosków z analiz prowadzonych przez zespół Trend Micro Threat Research. Przykładowo, oferujemy proste do użycia rozwiązania, pozwalające na łatwe przeprowadzenie oceny bezpieczeństwa systemów, które nie są podłączone do internetu. Jest to np. infrastruktura OT w firmach produkcyjnych. W ofercie Trend Micro dostępne są też rozwiązania EdgeIPS i EdgeFirewall przeznaczone do ochrony systemów automatyki przemysłowej, związanych m.in. z internetem rzeczy.

Najpopularniejsze były ataki ransomware, które mogą narazić firmę na poważne koszty, a jednocześnie uniemożliwić bieżące funkcjonowanie. Bardzo bolesne w skutkach mogą być również ataki ukierunkowane na kradzież własności intelektualnej. Trudno jednak uogólniać, ponieważ w zależności od sytuacji i specyfiki każdej organizacji, nawet chwilowe zatrzymanie normalnego przebiegu procesu produkcyjnego może generować ogromne straty. Praktyka pokazuje więc, że problematyczne są także ataki phishingowe związane z kradzieżą danych uwierzytelniających, których z oczywistych powodów w naszym środowisku nie zanotowaliśmy.

Fabryka-pułapka

sposobem na przeanalizowanie zagrożeń wymierzonych w systemy automatyki przemysłowej



Zbudowana przez ekspertów zespołu Threat Research w Trend Micro infrastruktura, symulująca funkcjonowanie realnego środowiska IT w małym zakładzie produkcyjnym, pomogła w ocenie sposobów działania cyberprzestępców podejmujących działania wymierzone w sektor przemysłowy. Jakimi pobudkami kierowały się osoby stojące za atakami przeprowadzonymi na środowisko badawcze Trend Micro?

Realizowany w ramach zespołu Threat Research projekt badawczy zakładał uruchomienie środowiska honeypot, imitującego działanie infrastruktury wykorzystywanej w zakładach produkcyjnych. Co ważne – w ramach środowiska IT zbudowanego na potrzeby analizy – zastosowano m.in. powszechnie spotykane sterowniki PLC, przemysłowe systemy sterowania, a także oprogramowanie inżynierskie. Zdaniem autorów badania, jego wyniki mogą okazać się pomocne w planowaniu strategii bezpieczeństwa firm produkcyjnych.

Zaobserwowane incydenty związane bezpośrednio z działaniami cyberprzestępców były przede wszystkim ukierunkowane na pozyskanie realnych korzyści finansowych. Ponadto badanie pokazało, że większość zaobserwowanych ataków nie była wymierzona konkretnie w instytucję przemysłową, a opierała się na zasadzie poszukiwania łatwego celu. Oznacza to, że środowiska IT/OT wykorzystywane w sektorze produkcyjnym są narażone na działania cyberprzestępcze o dość uniwersalnym charakterze. W szczególności dotyczy to mniejszych zakładów produkcyjnych.

Główna motywacja cyberprzestępców: pieniądze

Zaobserwowane incydenty związane bezpośrednio z działaniami cyberprzestępców były przede wszystkim ukierunkowane na pozyskanie realnych korzyści finansowych. Ponadto badanie pokazało, że większość zaobserwowanych ataków nie była wymierzona konkretnie w instytucję przemysłową, a opierała się na zasadzie poszukiwania łatwego celu. Oznacza to, że środowiska IT/OT wykorzystywane w sektorze produkcyjnym są narażone na działania przestępcze o dość uniwersalnym charakterze. W szczególności dotyczy to mniejszych zakładów produkcyjnych.

Taki właśnie zakład został zasymulowany w ramach projektu badawczego Trend Micro. Ze względu na skalę i charakter prowadzonej działalności, małe zakłady produkcyjne nie są narażone na precyzyjnie ukierunkowane ataki, z jakimi mają do czynienia największe, globalne firmy. „Dyskusje na temat cyberzagrożeń wymierzonych w przemysłowe systemy sterowania ICS zbyt często ograniczają się do zaawansowanych ataków ze strony wrogich państw, mających na celu sabotaż kluczowych procesów. Tymczasem nasze badanie pokazuje, że co prawda stanowią one zagrożenie dla Przemysłu 4.0, ale istnieje duże prawdopodobieństwo, że padnie on ofiarą bardziej przyziemnych ataków" – komentuje wyniki badania Greg Young, wiceprezes ds. cyberbezpieczeństwa w firmie Trend Micro.

Brak choćby podstawowych zabezpieczeń naraża przedsiębiorstwa produkcyjne na wiele banalnych, ale potencjalnie bardzo kosztownych w skutkach zagrożeń. Mowa tu m.in. o – zaobserwowanych w ramach projektu badawczego Trend Micro – atakach typu ransomware, próbach kradzieży danych oraz incydentach związanych z wykorzystaniem mocy obliczeniowej firmowej infrastruktury na potrzeby generowania kryptowalut.

Proste, ale niebezpieczne ataki

Niezależnie od motywacji atakujących, zagrożenia o dość powszechnym charakterze mogą okazać się wyjątkowo groźne dla przedsiębiorstw produkcyjnych. Korzystają one bowiem zarówno z typowej infrastruktury IT, jak i ze specjalistycznych technologii operacyjnych oraz rozwiązań przemysłowych OT, które często nie były projektowane z myślą o otwarciu firmowych środowisk na świat.

Autorzy analizy zwracają uwagę na przypadki włamania do zasymulowanego środowiska, podczas których atakujący skupili się na specjalizowanych rozwiązaniach przemysłowych. **Zanotowano przykłady działań** - choć być może były to próby rozeznania się w możliwościach ingerencji w funkcjonowanie środowiska OT - **skutkujących m.in. zatrzymaniem działania symulowanej linii produkcyjnej. W realnych warunkach taka sytuacja mogłaby prowadzić do znaczących strat biznesowych związanych, przykładowo, z utratą surowców, opóźnieniami w realizacji zamówień czy koniecznością utylizacji niedokończonej serii wyrobów.**

Co więcej, jak pokazuje praktyka, dla wielu, ciągle użytkowanych rozwiązań przemysłowych nie są oferowane aktualizacje usuwające stale wykrywane luki lub podatności.

Autorzy analizy zwracają uwagę na przypadki włamania do zasymulowanego środowiska, podczas których atakujący skupili się na specjalizowanych rozwiązaniach przemysłowych. Większość z nich nie miała szczególnie negatywnych skutków, ale możliwe, że zaobserwowane działania były jedynie elementem oceny czy symulowane środowisko produkcyjne jest wartościowym celem. Zanotowano jednak przykłady działań – choć być może były to próby rozeznania się w możliwościach ingerencji w funkcjonowanie środowiska OT – skutkujących m.in. zatrzymaniem działania symulowanej linii produkcyjnej. W realnych warunkach taka sytuacja mogłaby prowadzić do znaczących strat biznesowych związanych, przykładowo, z utratą surowców, opóźnieniami w realizacji zamówień czy koniecznością utylizacji niedokończonej serii wyrobów.

Jak zadbać o bezpieczeństwo?

Projekt badawczy Trend Micro pokazał, że wielu z zaobserwowanych incydentów można było uniknąć dzięki zastosowaniu stosunkowo prostych środków. Dotyczy to zarówno dbałości o właściwą konfigurację środowiska IT, w tym ograniczenie liczby osiągalnych z zewnątrz portów sieciowych, jak i wykorzystanie dobrych praktyk w zakresie kontroli dostępu oraz tworzenia haseł uwierzytelniających. Niezbędne jest także użycie podstawowych rozwiązań bezpieczeństwa oraz monitoringu funkcjonowania środowiska IT. Wraz z postępującą specjalizacją działań cyberprzestępców oraz wzrostem skali ataków coraz częściej niezbędne stają się też bardziej zaawansowane, wielowarstwowe rozwiązania wyspecjalizowane pod kątem ochrony specyficznych rozwiązań biznesowych i wykorzystujące analitykę obserwowanych w środowisku zdarzeń.

W ofercie Trend Micro przykładem takich rozwiązań są narzędzia zaprojektowane z myślą o ochronie środowisk IT wykorzystywanych w przedsiębiorstwach wdrażających koncepcję Przemysłu 4.0. I tak, w ochronie rozproszonych środowisk brzegowych pomocne są rozwiązania, takie jak zapora firewall Trend Micro EdgeFire oraz platforma zapobiegania włamaniom Trend Micro EdgeIPS, oferowane wraz z centralnym rozwiązaniem Trend Micro OT Defense Control ułatwiającym zarządzanie bezpieczeństwem przemysłowego sprzętu operacyjnego.

Zalecenia te w szczególnym stopniu dotyczą tych organizacji, które na szeroką skalę korzystają z nowoczesnych technologii produkcyjnych. Wraz ze wzrostem zależności organizacji od technologii cyfrowych rośnie zarówno skala podatności na zagrożenia ze strony cyberprzestępców, jak i skala potencjalnych strat związanych z różnego rodzaju incydentami. „Podczas budowy środowisk bazujących na idei Przemysłu 4.0 powstają luki, z którymi nie radzą sobie ani informatycy, ani zespoły odpowiedzialne za technologie operacyjne. Rosnące ryzyko obrazuje liczba zgłoszonych luk w zabezpieczeniach systemów ICS, która w 2018 roku wzrosła o ponad 224% w porównaniu z rokiem 2017" – podkreśla Greg Young. Według niego, we wszystkich organizacjach biznesowych korzystających z nowoczesnych rozwiązań IT, w tym z rozwiązań oferowanych w modelu chmury obliczeniowej, niezbędne stają się również systemy przeznaczone do zabezpieczenia środowisk cloud, a także warstwy integracji między infrastrukturą lokalną a chmurą.

Dyskusje na temat cyberzagrożeń wymierzonych w przemysłowe systemy sterowania ICS zbyt często ograniczają się do zaawansowanych ataków ze strony wrogich państw, mających na celu sabotaż kluczowych procesów. Tymczasem brak choćby podstawowych zabezpieczeń naraża przedsiębiorstwa produkcyjne na wiele banalnych, ale potencjalnie bardzo kosztownych w skutkach zagrożeń. Mowa tu m.in. o - zaobserwowanych w ramach projektu badawczego Trend Micro - **atakach typu ransomware, próbach kradzieży danych oraz incydentach związanych z wykorzystaniem mocy obliczeniowej firmowej infrastruktury** na potrzeby generowania kryptowalut.

Piotr Waszczuk

Szczegóły projektu badawczego

fabryka-pułapka

przeprowadzonego przez zespół Threat Research firmy Trend Micro

Najważniejsze zdarzenia zaobserwowane podczas działania środowiska symulującego realną infrastrukturę IT/OT w firmie produkcyjnej

06.05.2019
uruchomienie środowiska badawczego

24.06.2019
atak ukierunkowany na kopanie kryptowalut

30.06.2019
kolejny atak ukierunkowany na kopanie kryptowalut

01.08.2019
zdalna zmiana konfiguracji zapory firewall

22.09.2019
atak ransomware

16.09.2019
nieudana próba ataku ukierunkowanego na kopanie kryptowalut

02.09.2019
próba wykorzystania infrastruktury do przeprowadzenia nadużyć finansowych

25.08.2019
nieuprawnione zatrzymanie oprogramowania operatorskiego systemu produkcyjnego

Udostępnione publicznie porty sieciowe na zewnętrznym ruterze sieciowym symulowanego środowiska sieciowego

102 Siemens S7	3 389 RDP	5 900 VNC
5 901 VNC	9 600 Omron FINS	44 818 EtherNet/IP

9452

adresów IP nawiązywało komunikację ze symulowanym środowiskiem w czasie trwania analizy przez zespół Threat Research firmy Trend Micro

6,45%

spośród wszystkich ataków na symulowane środowisko fabryki-pułapki odpowiadało za skanowanie podatności oraz portów

10 000 USD

to wysokość pierwotnego okupu oczekiwanego przez osoby odpowiedzialne za atak ransomware z 22 września 2019 roku, ostatecznie udało się wynegocjować 6000 USD

01.10.2019
próba przeprowadzenia ataku przy użyciu modułu Meterpreter w środowisku Metasploit

15.10.2019
kolejny atak ukierunkowany na kopanie kryptowalut

16.10.2019
próba przeprowadzenia ataku mającego na celu kradzież danych

22.10.2019
atak ransomware

31.10.2019
włamanie do stacji roboczej symulującej system sterowania robotyką przemysłową (paletyzatorem)

01.11.2019
ostrzeżenie od hakera whitehat z informacją o sugerowanych lukach bezpieczeństwa do załatania

12.11.2019
prosty atak pozorujący działanie ransomware

10.12.2019
zdalne uruchomienie środowiska produkcyjnego i wywołanie operacji sterowania produkcją, a następnie zatrzymanie całego procesu produkcyjnego

31.12.2019
wyłączenie środowiska badawczego

Maszyny wykorzystane na potrzeby zasymulowania infrastruktury IT zakładu produkcyjnego:

3x maszyny wirtualne pełniące odpowiednio rolę:

- panelu sterowniczego HMI
- stacji roboczej symulującej system sterowania paletyzatorem
- stacji roboczej nadzorującej pracę sterowników PLC

1x komputer przenośny pełniący rolę serwera plików

1x Raspberry Pi 3 jako platforma pozwalająca na monitorowanie ruchu sieciowego w cyklach 24-godzinnych

1x zapora firewall Cisco ASA 5505

Źródło: Trend Micro