RAPORT TYGODNIOWY NC CYBER

29 Listopada – 5 Grudnia 2017 | Numer 1/12/17

NCCYBER.034.RT1-12.2017.WLA

Spis treści

NASK NC CYBER CERT.PL dyżurnet.pl

Aktualności

Rozwiązanie konkursu Capture The Flag w ramach ECSM 2017

CERT Polska opublikował wyniki zorganizowanego w ramach Europejskiego Miesiąca Cyberbezpieczeństwa[1] konkursu typu Capture The Flag. Szczegóły konkursu, lista laureatów oraz zadania realizowane w ramach konkursu dostępne są na stronie: Rozwiązania zadań z konkursu Capture The Flag w ramach ECSM 2017

W tym roku odbył się piąty Europejski Miesiąc Cyberbezpieczeństwa. Z tej okazji, w całej Europie zorganizowano ponad 300 wydarzeń w celu promowania bezpieczeństwa w Internecie. W 2017 roku kampania obejmowała głównie zagadnienia bezpieczeństwa cybernetycznego w miejscu pracy, regulacje, ochronę prywatności i danych oraz bezpieczeństwa cybernetycznego w domu. Koordynatorem inicjatywy w Polsce był NASK. Więcej informacji można znaleźć na stronie na stronie aktualności NASK: Październik miesiącem cyberbezpieczeństwa.

Kolejne ostrzeżenia NC Cyber w Regionalnym Systemie Ostrzegania

W minionym tygodniu NC Cyber opublikowało komunikat RSO ostrzegający przed fałszywymi sklepami internetowymi. W treści komunikatu zwrócono uwagę na spodziewany w okresie świątecznym wzrost liczby powstających fałszywych sklepów oraz zagrożenia, jakie mogą spotkać konsumentów. Komunikat ten zawierał także wskazówki na co zwracać uwagę, aby nie zostać oszukanym, m.in. weryfikacja, czy cena nie jest podejrzanie niska względem konkurencji, oraz czy sklep posiada pozytywne, aktualne opinie w serwisach opinii konsumenckich.

Pełna treść komunikatu dostępna jest na stronie Regionalnego Systemu Ostrzegania: Komunikat NC Cyber.

[1] Europejski Miesiąc Cyberbezpieczeństwa (European Cyber Security Month – ECSM) powstał z inicjatywy agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz Komisji Europejskiej DG CONNECT (Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii). W trakcie kampanii prezentowane są projekty oraz inicjatywy realizowane w krajach europejskich, związane zarówno z propagowaniem wiedzy na temat bezpiecznego korzystania z Internetu jak i rozwojem nowoczesnych technologii teleinformatycznych.

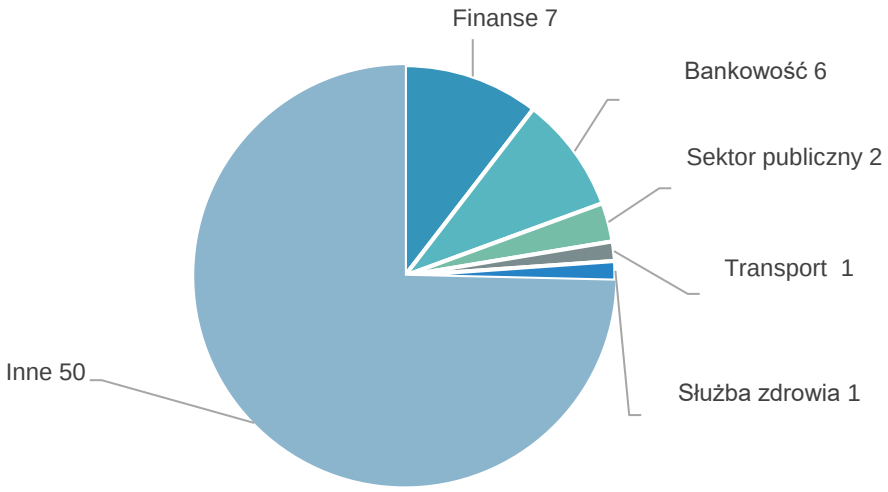
Statystyki zarejestrowanych zagrożeń

Statystyki zawarte w niniejszym rozdziale obejmują dane o ilości zarejestrowanych zgłoszeń[2] oraz liczbie obsłużonych przez NC Cyber incydentów[3] w analizowanym tygodniu. Oddzielną grupę stanowią incydenty związane z potencjalnie nielegalnymi treściami w Internecie, obsługiwane przez specjalnie do tego dedykowany zespół – Dyżurnet.pl.

Zarejestrowane zgłoszenia i incydenty cyberbezpieczeństwa

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	302
w tym zarejestrowane incydenty	67

Zarejestrowane incydenty w podziale na sektory występowania



[2] Zgłoszenia przesłane są za pośrednictwem formularza dostępnego na stronie www.cert.pl lub są wysłane na adres zgłoszeniowy cert@cert.pl. Centrum Operacyjne NC Cyber rejestruje także powiadomienia otrzymywane bezpośrednio od przedstawicieli sektora publicznego oraz prywatnego. Otrzymane informacje o zagrożeniach cyberbezpieczeństwa stanowią podstawę rejestracji nowych zgłoszeń, incydentów lub są rejestrowane wyłącznie do celów statystycznych, jako zgłoszenia nie mające charakteru realnego zagrożenia.

[3] Incydenty dotyczą konkretnej kategorii zagrożenia np. phishingu, spamu czy ataku z użyciem złośliwego oprogramowania.

Str. 3 Statystyki zarejestrowanych zagrożeń

Rodzaje zagrożeń w podziale na sektory występowania

Rodzaj incydentu	Liczba	Sektor[4]
Phishing	1	Sektor publiczny
	4	Bankowość
	7	Infrastruktura rynków finansowych
	17	Inne[5]
Złośliwe oprogramowanie	1	Transport
	2	Bankowość
	20	Inne
Spam	4	Inne
Skanowanie	6	Inne
DDoS	2	Inne
Włamanie	1	Sektor publiczny
	1	Inne
Inne	1	Służba zdrowia

Pochodzenie atakującego według lokalizacji adresu IP

Pochodzenie atakującego	Liczba
Polska	18
Zagranica	12
Nieznane	36

[4] Sektor określany jest na podstawie załącznika nr II Dyrektywy NIS (Dyrektywa Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii).

[5] Sektor „Inne" obejmuje sektory różne od: bankowość; energetyka; infrastruktura rynków finansowych; infrastruktura cyfrowa; telekomunikacja; transport; służba zdrowia; zaopatrzenie w wodę, odprowadzanie i oczyszczanie ścieków; sektor publiczny.

Str. 4 Statystyki zarejestrowanych zagrożeń

Typ poszkodowanego według lokalizacji adresu IP

Typ poszkodowanego	Liczba
Osoba prywatna	18
Instytucja komercyjna	20
Instytucja badawcza lub akademicka	1
Inna niekomercyjna instytucja	1
Nieznany	20

Pochodzenie poszkodowanego według lokalizacji adresu IP

Pochodzenie poszkodowanego	Liczba
Polska	26
Zagranica	29
Nieznane	11

Zgłoszenia dotyczące nielegalnych treści oraz podjęte działania

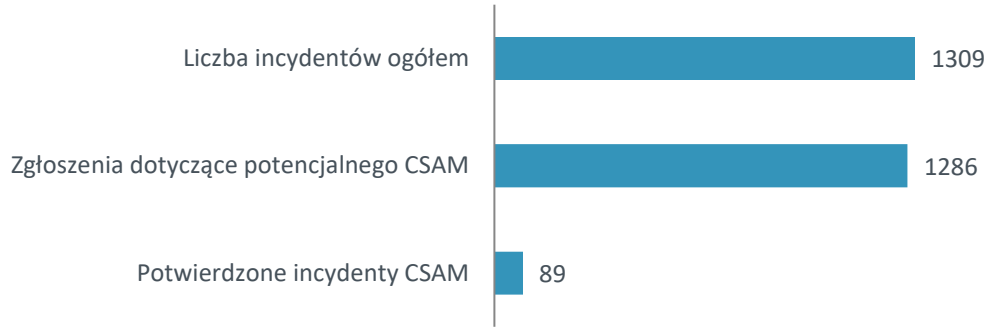
Zgłoszeniami dotyczącymi potencjalnie nielegalnych treści, w tym materiałami przedstawiającymi seksualne wykorzystywanie dziecka (CSAM – child sexual abuse material), zajmuje się zespół Dyżurnet.pl (www.dyzurnet.pl).

W listopadzie 2017 roku zespół Dyżurnet.pl otrzymał blisko 1300 zgłoszeń dotyczących potencjalnych treści pornograficznych z udziałem osób małoletnich, z czego około 400 zgłoszeń zostało zaklasyfikowanych jako „treści nie znalezione". Zgłaszane treści miały znajdować się na serwisach hostingowych zlokalizowanych w Holandii, jednak nie były dostępne w momencie analizy.

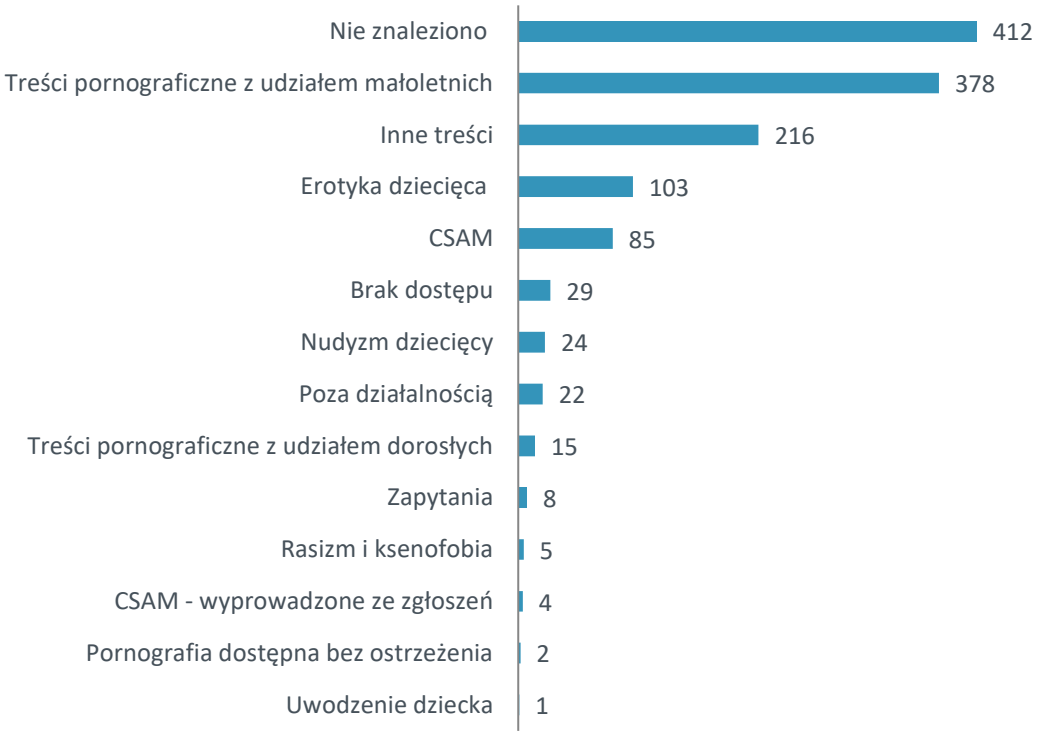
Zespół Dyżurnet.pl w kontekście statystyk za listopad zwraca uwagę, że eksperci jedynie w 7% przypadków potwierdzili CSAM (treści pornograficzne z udziałem dzieci). Stanowi to znaczny spadek w porównaniu do 21-22% w ostatnich dwóch latach. Wynika to ze stosunkowo dużej liczby treści nie znalezionych w związku z dynamicznością i ulotnością treści internetowych. Kolejną przyczyną jest niezmiennie duża liczba incydentów klasyfikowanych, jako treści pornograficzne z udziałem osób pełnoletnich, które np. są stylizowane na osoby niepełnoletnie. Dlatego też Dyżurnet.pl podkreśla wagę każdego zgłoszenia przesłanego przez zaniepokojonego internautę, które może zostać potwierdzone przez ekspertów i wobec których mogą podjąć dalsze działania.

Str. 5 Statystyki zarejestrowanych zagrożeń

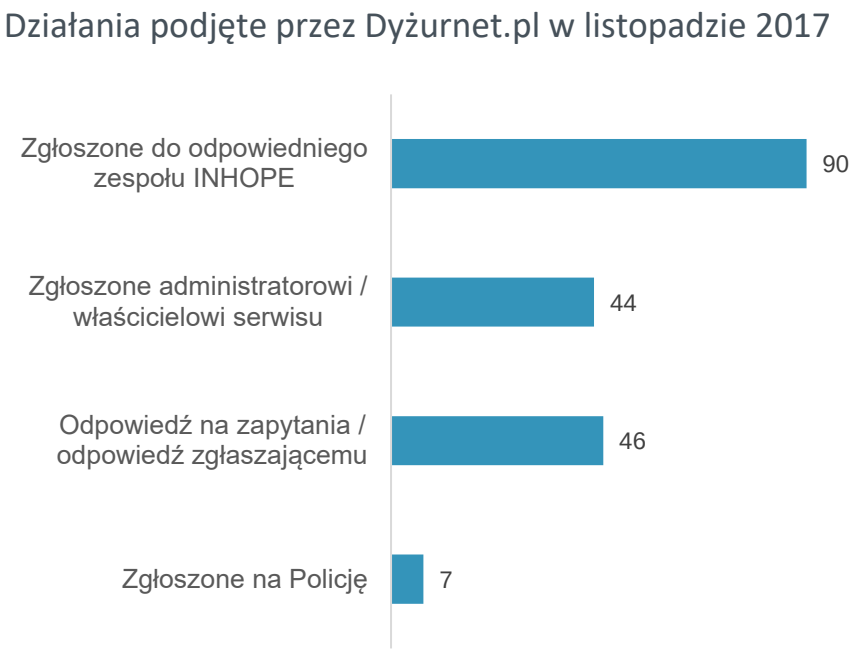
Zgłoszenia i incydenty zarejestrowane w listopadzie 2017 roku



Klasyfikacja incydentów zarejestrowanych w listopadzie 2017 roku



Statystyki zarejestrowanych zagrożeń



Analiza zaobserwowanych zagrożeń

Największy udział w zarejestrowanych przez NC Cyber zagrożeniach minionego tygodnia mają incydenty phishingu oraz kampanii z użyciem złośliwego oprogramowania. Następnie, na podobnym poziomie ilościowym obsłużono incydenty rozsyłania spamu oraz skanowania sieci komputerowych. Zarejestrowano także pojedyncze incydenty prób włamania oraz ataku DDoS.

Wybrane incydenty minionego tygodnia

Trojan bankowy Gozi ISFB

Zespół NC Cyber zarejestrował kampanię dystrybucji szkodliwego pliku, którego uruchomienie skutkowało pobraniem trojana bankowego Gozi ISFB. W wiadomościach e-mail rozsyłany był załącznik o nazwie „Faktura 00504201712 (1).zip". W spakowanym załączniku znajdował się plik javascript, którego otwarcie aktywowało pobieranie trojana ISFB. Wirus ten ma za zadanie wykraść loginy i hasła do serwisów bankowości elektronicznej.

Wektorem ataku była spreparowana wiadomość e-mail, mająca na celu wykorzystanie ciekawości odbiorcy i pozornego poczucia bezpieczeństwa. Autor kampanii celowo umieszczał w polu nadawcy nazwę firmy lub imię i nazwisko osoby licząc, iż odbiorca tylko pobieżnie sprawdzi nadawcę. Kiedy brak pewności co do wiarygodności przesłanej wiadomości, najlepiej jej nie otwierać lub dokonać weryfikacji nadawcy, np. przez kontakt z osobą lub organizacją rzekomo wysyłającą wiadomość.

> Fakt, że po otwarciu załącznika nie pojawia się żadne okno lub nie zaobserwowano niczego nietypowego, nie oznacza, że nie doszło do infekcji urządzenia. Nie należy bagatelizować żadnej podejrzanej sytuacji, a każdy potencjalny incydent powinien zostać zgłoszony osobom odpowiedzialnym za systemy informatyczne.

Inny incydent związany z trojanem Gozi dotyczył braku odpowiedniego zabezpieczenia biuletynu koreańskiego CERTu – Korea Internet Security Center (KrCERT/CC). Przestępcy umieścili w biuletynie złośliwe oprogramowanie, które informowało użytkowników o wystąpieniu w znanym programie luki i konieczności zainstalowania poprawki. Otwarcie pakietu działało odwrotnie do oczekiwań użytkownika – pobierało trojana bankowego Gozi.

> Dobrą praktyką w przypadku dystrybucji istotnych dokumentów powinno być podpisywanie wiadomości oraz samych dokumentów ważnym certyfikatem bezpieczeństwa. Autentyczność dokumentu można weryfikować również na podstawie publikowanych sum kontrolnych pliku.

Szczegóły omawianego ataku zostały opisane w artykule: Banking Trojan Dropped Through Spoofed Korean CERT Bulletin

Nieuprawnione przekierowanie na stronę internetową

Właściciel strony internetowej zgłosił przekierowanie z obcej strony na jego witrynę internetową. Ustawienie przekierowania bez zgody właściciela strony do jednej z podstron mogło prowadzić do mylnego odbioru treści przez osoby odwiedzające daną stronę. W tego typu przypadkach sugerowany jest kontakt z osobą odpowiedzialną za witrynę, na której zostało ustawione przekierowanie lub bezpośrednio do firmy świadczącej hosting.

Podatność w aplikacji mobilnej obsługującej płatności elektroniczne

W minionym tygodniu poinformowano NC Cyber o podatności wykrytej w aplikacji mobilnej jednej z firm obsługującej płatności elektroniczne. Osoba zgłaszająca podatność wykazała, że dostępna publicznie aplikacja mobilna posiada lukę, umożliwiającą przejęcie danych dostępowych użytkowników aplikacji. Sytuacja dotyczyła użytkowników, którzy włączyli w aplikacji automatyczne zapamiętywanie i uzupełnianie loginu oraz hasła do banku. Podatność wynikała z nadużycia nieudokumentowanych metod biblioteki, wykorzystywanych przez oprogramowanie. Badacz, któremu udało się odkryć podatność skontaktował się również z producentem oprogramowania udostępniając pełną dokumentację oraz scenariusz przykładowego ataku (proof-of-concept). Sam producent potwierdził prawidłowość zaprezentowanego scenariusza ataku i zapowiedział wydanie poprawek łatających podatność podczas najbliższej aktualizacji.

Podatności narzędzi deweloperskich oraz inżynierii wstecznej aplikacji Android

W bieżącym tygodniu pojawiła się informacja o krytycznej podatności narzędzi deweloperskich oraz inżynierii wstecznej aplikacji Android. Podatność otrzymała nazwę ParseDroid i została opisana m.in. przez badaczy Check Point Research Team wraz z przedstawieniem proof-of-concept. Opisana podatność ma miejsce w narzędziach korzystających z popularnej biblioteki parsującej XML "DocumentBuilderFactory" używanej w wielu narzędziach takich jak Google's Android Studio, JetBrains' IntelliJ IDEA, Eclipse czy narzędzi do Reverse Engineeringu - APKTool, Cuckoo-Droid. Podatność może być wykorzystana podczas załadowania do środowiska deweloperskiego Android aplikacji APK, zdekodowania jej oraz parsowania przygotowanego przez atakującego pliku "AndroidManifest.xml". Wykorzystanie luki może prowadzić między innymi do zdalnego wykonania kodu na podatnej maszynie. Większość producentów podatnego oprogramowania udostępniła już aktualizacje swojego oprogramowania.

Szczegóły podatności dostępne są w artykule: ParseDroid: Targeting The Android Development & Research Community

Rekomendacje

Bezpieczeństwo korzystania z aplikacji mobilnych

Ponieważ urządzenia mobilne, takie jak smartfony i tablety stały się jedną z podstawowych technologii wykorzystywanych w życiu codziennym, coraz częściej dochodzi do naruszeń zasad bezpieczeństwa i związanych z tym wycieków wrażliwych informacji. Zgłoszona do NC Cyber podatność wykryta w aplikacji mobilnej służącej do obsługi płatności online jest przykładem, jak ważne jest wczesne wykrywanie podatności i ich szybkie aktualizowanie. Na bezpieczeństwo korzystania z aplikacji internetowych mają wpływ także sami użytkownicy.

Dobre praktyki użytkowania urządzeń mobilnych

- Instalacja aplikacji z bezpiecznego i zaufanego źródła

  Aplikacje należy instalować tylko z oficjalnych źródeł, z rozwagą pobierać nowe aplikacje oraz takie, które mają niską reputację. Uruchamianie w androidzie opcji instalacji aplikacji z nieznanego źródła zawsze wiąże się potencjalnym zagrożeniem.

- Systematyczne usuwanie zbędnych aplikacji

  Każda zainstalowana aplikacja może posiadać luki bezpieczeństwa, które następnie mogą zostać wykorzystane przez przestępców. Regularne usuwanie nieużywanych aplikacji zabezpiecza urządzenie przed nieuprawnionym dostępem, kradzieżą danych czy infekcją złośliwym oprogramowaniem.

- Regularne aktualizowanie oprogramowania

  Podobnie jak w przypadku komputerów, aktualizacje oprogramowania na telefonie czy tablecie stanowią podstawę bezpiecznego systemu. Dotyczy to zarówno oprogramowania samego urządzenia, jak i zainstalowanych na nim aplikacji. Jeśli jest taka możliwość, należy włączyć opcję automatycznych aktualizacji lub regularnie sprawdzać dostępność i pobierać aktualizacje.

- Weryfikacja uprawnień aplikacji

  Warto sprawdzić czy oprogramowanie zostało poprawnie zainstalowane i czy aplikacja nie posiada nadmiarowych uprawnień. Jeśli nie chcemy udostępniać danych, do których oprogramowanie ma mieć dostęp, najlepiej zainstalować inną aplikację.

Str. 10 Rekomendacje

- Bezpieczeństwo w miejscach publicznych

  Należy wystrzegać się takich czynności: jak wpisywanie haseł, korzystanie z aplikacji bankowych oraz czytanie korespondencji służbowej w miejscach publicznych, gdzie nieznane nam osoby mogą podejrzeć wrażliwe dane. Warto pamiętać o tym, że miejsca publiczne objęte są bardzo często monitoringiem, zatem dane wrażliwe narażone są na ujawnienie również za pomocą „oka" kamery. Ponieważ urządzenia mobilne łatwo jest fizycznie ukraść, zgubić lub pozostawić bez nadzoru, trzeba pamiętać o stosowaniu blokady ekranu, zabezpieczeniu dostępu do aplikacji np. hasłem lub zaszyfrowaniu zawartości telefonu.

Kluczowe poprawki bezpieczeństwa

Aktualizacje czołowych dostawców oprogramowania

Dostawca	Data	Produkt	Aktualizacja
UBUNTU	05.12.17.	Ubuntu	Firma Ubuntu opublikowała aktualizacje dla zidentyfikowanych podatności w swoich produktach. Szczegóły: Ubuntu security notices
GOOGLE	04.12.17.	Android	Firma Google opublikowała aktualizację dla systemu Android. Aktualizacja zwiera poprawki do 6 krytycznych podatności. Szczegóły: Android Security Bulletin — December 2017
MOZILLA	04.12.17.	Firefox 57.0.1.	Firma Mozilla opublikowała aktualizację dla zidentyfikowanych podatności w przeglądarce Mozilla Firefox. Podatność oznaczona jako krytyczna. Szczegóły: Security vulnerabilities fixed in Firefox 57.0.1
APACHE	04.12.17.	Apache Struts	Firma Apache Software Foundation opublikowała aktualizacje oprogramowania Apache Struts. Szczegóły: S2-054, S2-055
CISCO	29.11.17.	Cisco WebEx	Firma Cisco opublikowała aktualizacje zabezpieczeń dotyczące luki w produktach Cisco WebEx ARF Player oraz Cisco WebEx WRF Player. Aktualizacja oznaczona jako krytyczna. Szczegóły: Multiple Vulnerabilities in Cisco WebEx Recording Format and Advanced Recording Format Players
APPLE	29.11.17.	Apple MacOS High Sierra 10.13	Firma Apple opublikowała uzupełniającą aktualizację zabezpieczeń dotyczącą luki w systemie macOS High Sierra 10.13. Szczegóły: Zawartość związana z zabezpieczeniami w uaktualnieniu zabezpieczeń 2017-001

Wybrane wiadomości minionego tygodnia

Popularność Bitcoina spowodowała wzrost ilości złośliwego oprogramowania o tematyce kryptowalutowej.

Artykuł: Cyber-thieves seek to cash in on Bitcoin boom

Google ogłosił, że blokuje możliwość wprowadzania kodu innych aplikacji do przeglądarki Chrome oraz przedstawił plan działań na najbliższe 14 miesięcy.

Artykuł: Google Chrome will block code injection from third-party software within 14 months

Analiza dotycząca wdrażania strategii bezpiecznego Internetu Rzeczy (IoT) oraz napotykane przeszkody – kwestie bezpieczeństwa, koszty wdrożenia i zaangażowanie ze strony kierownictwa firmy.

Artykuł: Security and costs holding back those looking to implement IoT projects

Analiza zarejestrowanych ataków DDoS za Q3 2017 roku.

Artykuł: Global DDoS Threat Landscape Q3 2017

Zalecenia i ostrzeżenia National Cyber Security Center w kwestii stosowanego w Wielkiej Brytanii rosyjskiego oprogramowania antywirusowego.

Artykuł: U.K. cyber agency tells government to handle Russian anti-virus software with caution

Wspólne działania grup do walki z cyberprzestępczością doprowadziły do likwidacji jednej z najdłużej działających grup przestępczych – Andromedy, znanej również jako Gamarue.

Artykuł: Andromeda botnet dismantled in international cyber operation

Opracowanie:
NASK – Państwowy Instytut Badawczy
Dział Centrum Operacyjne
ul. Kolska 12, 01-045 Warszawa