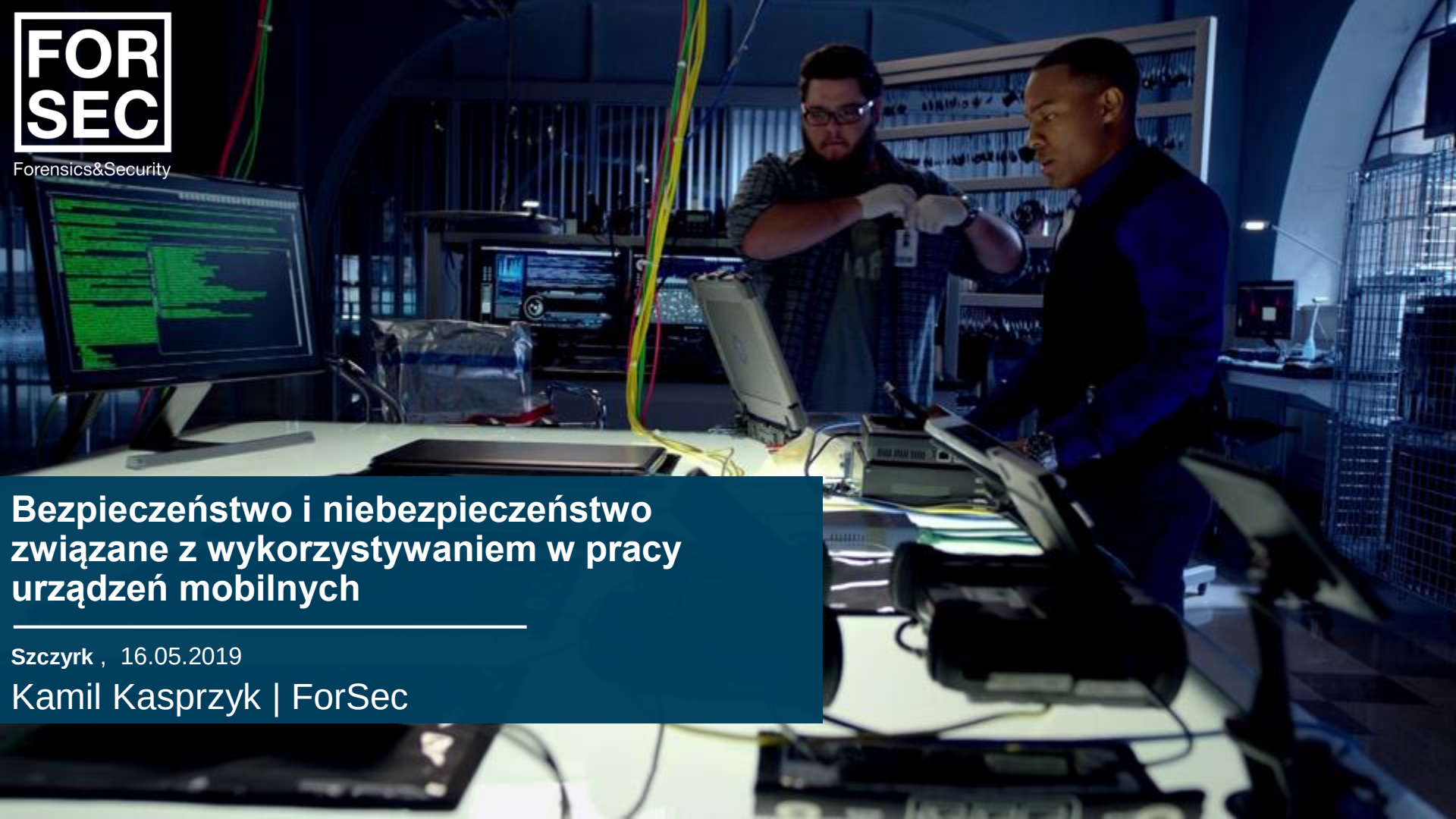


FORSEC
Forensics&Security

Bezpieczeństwo i niebezpieczeństwo związane z wykorzystywaniem w pracy urządzeń mobilnych

Szczyrk , 16.05.2019

Kamil Kasprzyk | ForSec

ForSec – kim jesteśmy

Audyty - Bezpieczeństwo IT - Ekspertyzy - Oprogramowanie -Szkolenia

- Instytucja specjalistyczna
- Zespół najlepszych specjalistów w Polsce
- Własne produkty
- Profesjonalne centrum szkoleniowe
- Laboratorium Odzyskiwania Danych
- Dział analiz kryminalnych
- Dział handlowy
- Dział audytu

FOR SEC
Forensics&Security

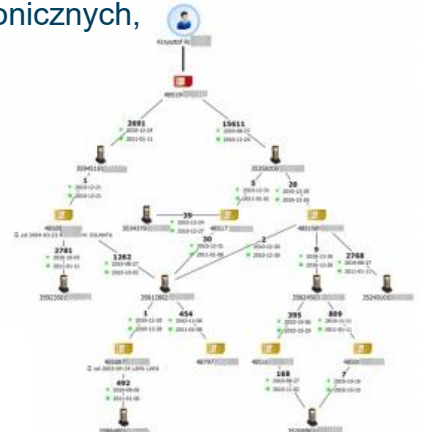
Laboratorium - Zakres Usług

- Odzyskiwanie danych z komputerów, dysków przenośnych, telefonów, serwerów itd.
  W skrócie - Wszelkich urządzeń przechowywujących dane.
- Analiza **uszkodzonych** urządzeń mobilnych oraz dronów. Jeśli trzeba wraz z naprawą urządzenia.
- **Zabezpieczanie danych w terenie**
- Analiza komputerów, telefonów i tabletów.
- Odblokowywanie komputerów i telefonów.
- Analiza nagrań video, monitoringu, poprawa jakości obrazu
- Analiza nagrań głosowych, stenogramy

Laboratorium - Zakres Usług

- **Odblokowywanie najnowszych telefonów i tabletów – iPhone , Samsung, Huawei - JAKO JEDYNI W POLSCE**

- Analizy ataków cyberprzestępczych, Analizy włamań sieciowych
- **Odszyfrowywanie danych**
- **Analizy kryminalne** (Analizy danych pochodzących z rachunków bankowych, faktur, z bilingów telefonicznych, oraz analizy grup przestępczych)



- Usługi hybrydowe – informatyka śledcza + analiza kryminalna

- **Ekspertyzy**
- **Audyty bezpieczeństwa i testy penetracyjne**
- **Outsourcing**

Centrum Szkoleniowe ForSec

- Prowadzimy szkolenia z zakresu:
  - Bezpieczeństwa IT
  - Informatyki Śledczej
  - Informatyki Śledczej – Mobile Forensics
  - Informatyki Śledczej – Wideo Forensics
  - Ścieżka Systemu Linux

Najpopularniejsze:

- Bezpieczny pracownik

- Techniki Hackingu i Cyberprzestępczości

Szkolenia Produktowe

(Xways, FTK, UFED, Amped5 i wiele innych)

Szkolenia, eventy, konferencje…

Konferencja ForSec – 09-10.X – KATOWICE

„Analizy kryminalne zorganizowanych grup przestępczych”

JESTEŚMY WYŁĄCZNYM DYSTRYBUTOREM WIELU KLUCZOWYCH ROZWIĄZAŃ

FOR SEC Forensics&Security

SUMURI Forensics Simplified

ACCESSDATA

Logicube®

Cellebrite Digital intelligence for a safer world

FOR SEC
Forensics&Security

Bezpieczeństwo danych twojego smartfona

1983

Analogowy telefon

Ledowy wyświetlacz

Pamięć na 30 numerów

2019

Pamięć nawet 1TB + karta pamięci

Wyświetlacz o rozdzielczości 3040×1440

GSM/UMTS/LTE/WIFI/BT/NFC

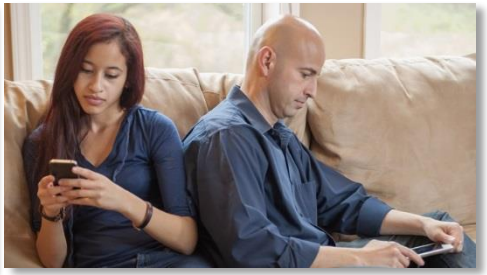
GPS, aparat, odblokowywanie palcem, twarzą, źrenicą..

2049

?

Jak wygląda nasze życie w 2019 ?

Z przyjaciółmi



W rodzinie

W miejscach publicznych

W pracy

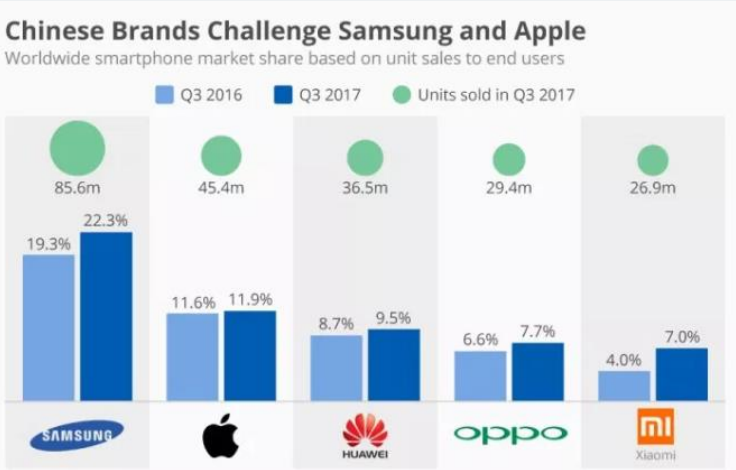
Akcesoria do smartfonów

Nasze życie jest non-stop rejestrowane

Bezpieczeństwo Twoich danych i danych przedsiębiorstwa

- **Wszystkie telefony** nowej generacji są podatne na ataki hackerskie, przez co jesteśmy narażeni na utratę naszych prywatnych danych oraz danych instytucji w której pracujemy

Top 5 Producentów Telefonów

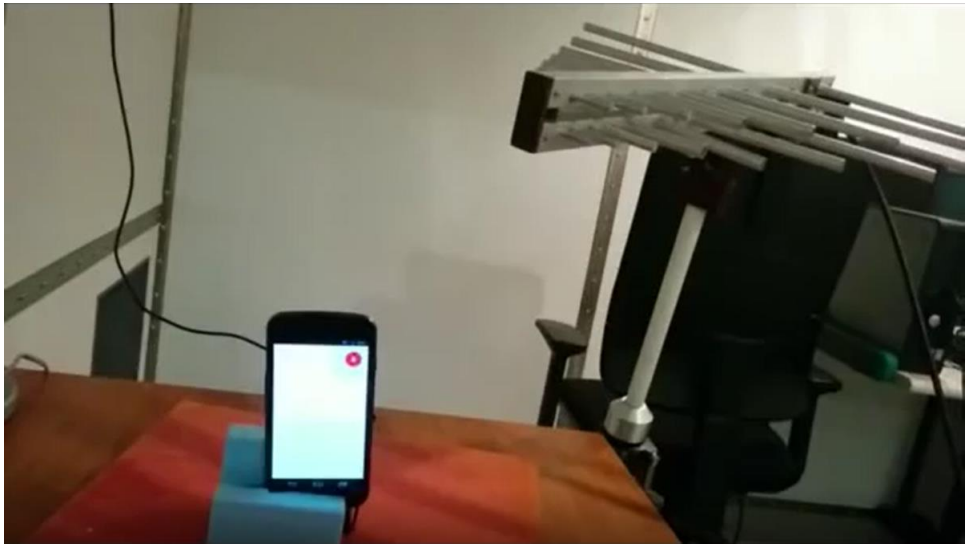


TOP 5 producentów smartfonów w 3 kwartale 2017 r. (według liczby sprzedanych urządzeń)

PRODUCENT	UDZIAŁ 3Q 2016	UDZIAŁ 3Q 2017	SPRZEDAŻ 3Q 2017 (MLN)
Samsung	19,3%	22,3%	85,6 mln
Apple	11,6%	11,9%	45,4 mln
Huawei	8,7%	9,5%	36,5 mln
Oppo	6,6%	7,7%	29,4 mln
Xiaomi	4,0%	7,0%	26,9 mln

Źródło: Statista – Chinese Brands Challenge Samsung and Apple

Co by było, gdyby Twój telefon sam, zaczął nagle dzwonić, wysyłać wiadomości, przeglądać strony internetowe?



Jak to możliwe?

Do przeprowadzenia tego ataku wystarczyło :

- iPhone z iOS 11.2 lub niższym lub telefon z Androidem 8
- W telefonie aplikacja wirtualnego asystenta
- Zestaw słuchawkowy z **podłączonymi do telefonu słuchawkami**
- Nadajnik radiowy

Jak to możliwe?

Jak wygląda taki atak?

- Nadajnik radiowy wysyła fale radiowe, które po cichu wydają polecenia głosowe do iPhona lub telefonu z Androidem, które mają włączone aplikacje Siri lub Google Now.
- Kable słuchawkowe działają jak antena radiowa i mogą być wykorzystane do swoistego oszukania telefonu, żeby uwierzył, że polecenia głosowe pochodzą z mikrofonu użytkownika.

Konsekwencje

Mając dostęp do telefonu i kontrolę nad nim, haker może przeprowadzić teraz wiele czynności np.:

- Zadzwonić do dowolnej osoby
- wysłać wiadomości SMS, MMS
- przekształcić telefon ofiary w urządzenie podsłuchowe,
- przeglądać strony zainfekowane złośliwym oprogramowaniem,
- rozsyłać spam za pomocą poczty firmowej wiadomości typu phishing przy użyciu e-maila,
- Przejąć kontrolę nad portalami społecznościowymi Facebooka czy Twittera
- Zainfekować znajomych złośliwym oprogramowaniem
- Popełniać przestępstwa, wyłudzenia

CIEKAWOSTKI

Zyski z cyberprzestępczości już dawno znacznie przekroczyły te spowodowane światową sprzedażą marihuany, kokainy i heroiny.

W ostatnim roku ofiarami cyberprzestępców padło 541 mln osób na całym świecie.

Około 73% procent dorosłych korzystających z Internetu było przynajmniej raz w życiu ofiarą ataku cyberprzestępczego, z czego w ponad 40% atakach brały udział urządzenia mobilne

Dwie trzecie (65%) użytkowników Internetu na całym świecie, w tym dwóch na pięciu (40%) polskich użytkowników stało się ofiarami cyberprzestępstw np. wirusów komputerowych, oszustw online, czy kradzieży numerów kart kredytowych i tożsamości.

Polska znajduje się na 6 miejscu pod względem największej liczby ofiar ataków. cyberprzestępczych.

Użytkownicy nie zawsze mają świadomość, że często jedno kliknięcie w link dzieli ich od stania się ofiarą ataku w Internecie.

JAK SIĘ BRONIĆ?

Nie ma skutecznej metody, która zagwarantuje nam pełną ochronę przed atakami hackerskimi.

- Jako użytkownicy smartfonów, komputerów i innych urządzeń mobilnych jesteśmy zobligowani do aktualizowania swoich urządzeń, ponieważ aktualizacje zwiększają szanse na obronę.
- Pamiętaj, w chwili odejścia od komputera zawsze blokuj swój komputer.
- Pamiętaj, jeśli nie używasz telefonu zawsze go blokuj minimum 6 znakowym kodem. **Ustaw szybkie włączenie blokady ekranu.**
- Unikaj haseł łatwych takich jak data urodzin lub 000000
- Nigdy nie podawaj haseł dostępowych, kodu blokady - NAWET WSPÓŁPRACOWNIKOWI.
- Nie zapisuj haseł w miejscach ogólnie dostępnych.
- Najlepiej nigdzie ich nie zapisuj.

JAK SIĘ BRONIĆ?

- **Korzystaj ze specjalnego adresu e-mail** w celu uwierzytelniania i zmian kodu PIN. Ten adres powinien się różnić od osobistego adresu, z którego korzystasz na co dzień i który może być powszechnie znany.
- **Nie instaluj aplikacji z nieznanych źródeł**, szczególnie darmowych wersji popularnych aplikacji.
- **Pobieraj wyłącznie aplikacje z App Store, Google Play** lub innych oficjalnych źródeł, ponieważ regularnie monitorują i usuwają podejrzane aplikacje.
- **Nie uzyskuj dostępu do poufnych informacji** (np. konta bankowego), korzystając z niezabezpieczonej publicznej sieci Wi-Fi.
- **Włącz funkcję automatycznego wymazywania zawartości** w przypadku przekroczenia określonej liczby nieprawidłowych prób zalogowania (i dbaj o tworzenie regularnej kopii zapasowej telefonu).
- **Wyłączaj funkcję Bluetooth**, kiedy z niej nie korzystasz.
- **Włącz funkcję „Znajdź mój telefon”**, aby szybko go zlokalizować, jeśli go zgubisz lub zostanie skradziony.
- **Zainstaluj w telefonie oprogramowania antywirusowe**, ale tylko zatwierdzonego i dobrze znanego (które zwykle nie jest darmowe).
- **Postaraj się zbyt długo nie przechowywać w telefonie osobistych informacji**. Dąż do utrzymywania telefonu w stanie jak największej „czystości”, przenosząc z niego dokumenty i zdjęcia do bezpieczniejszej lokalizacji.
- Jeśli to możliwe szyfruj swoje dane.

Dziękuję

FOR SEC
Forensics&Security