MAGAZYN

NR 28 / GRUDZIEŃ 2015

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Jak skutecznie obsługiwać zaawansowane ataki APT

Mobile Forensic nie zawsze prosty i przyjemny

Ekstrakcja danych z kont Google

Co w numerze?

Nowy zakaz dowodowy, czyli coś na kształt doktryny owoców zatrutego drzewa

Jarosław Góra

Na mocy tzw. wielkiej nowelizacji, która weszła w życie 1 lipca br., do polskiego procesu karnego wprowadzono nowy zakaz dowodowy, zbliżony nieco do amerykańskiej doktryny „owoców zatrutego drzewa". Potencjalnie nowy przepis może bardzo mocno wpłynąć na informatyków śledczych oraz kwestie wykorzystywania elektronicznego materiału dowodowego w sprawach karnych.

Przede wszystkim wskazać należy, że na skutek nowelizacji zdecydowanie rozszerzono możliwość wprowadzania do procesu karnego tzw. dowodów prywatnych. Od lat podnoszono, że należy w jakiś sposób ograniczyć organy ścigania, aby nie naginały przepisów podczas gromadzenia materiału dowodowego. Aby zniechęcić uczestników procesu, zarówno będących po stronie oskarżenia, jak i obrony, do podejmowania prób uzyskiwania dowodów w sposób sprzeczny z prawem, ustawodawca zdecydował się na nowy zakaz dowodowy.

Mając na uwadze powyższe, wprowadzenie tego zakazu wydaje się słuszne. Czy jednak ustawodawca nie popełnił kilku błędów? Jak nowy przepis wpłynie na pracę informatyków śledczych, zarówno tych zaangażowanych przez organy ścigania, jak i tych pomagających obronie zidentyfikować i zabezpieczyć dowody?

Wprowadzony do kodeksu postępowania karnego w art. 168a zakaz polega na tym, iż niedopuszczalne jest przeprowadzenie i wykorzystanie dowodu uzyskanego do celów postępowania karnego za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego. Jeden krótki przepis i szereg wątpliwości.

Czy zakazane jest uzyskiwanie dowodów jedynie za pomocą przestępstwa? Przepis odwołuje się jedynie do § 1 artykułu pierwszego Kodeksu karnego, zatem czy kwestia stopnia społecznej szkodliwości (§2) oraz zawinienia (§3) nie ma znaczenia? Czy popełnienie czynu zabronionego powinno zostać udowodnione, czy wystarczy prawdopodobieństwo? Jak powinien procedować sąd, kiedy kwestia „zatrutych dowodów" pojawi się w trakcie postępowania? Czy powinien sam dokonać karnoprawnej oceny zachowania, dzięki któremu uzyskano dowód, czy też

powinien postępowanie zawiesić i zawiadomić organy ścigania o podejrzeniu popełnienia przestępstwa? Jeśli sam dokona oceny, np. uznając, że zakaz powinien znaleźć zastosowanie i wnioskowany dowód nie zostanie dopuszczony, a później na skutek odrębnego postępowania okaże się, że przestępstwa jednak nie popełniono, czy proces powinien zostać wznowiony? Kto miałby dopuścić się czynu zabronionego: wnioskujący o dopuszczenie dowodu, osoba działająca na jego zlecenie, ktokolwiek inny? Podobnych pytań można zadać zdecydowanie więcej.

Jak się natomiast ma nowy zakaz dowodowy do pracy informatyków śledczych?

Z całą pewnością podczas prac polegających na identyfikacji, zabezpieczaniu oraz analizie danych cyfrowych może dojść do realizacji znamion kilku czynów zabronionych. Wystarczy wskazać choćby art. 267 kodeksu karnego. Informatyk musi czasem przełamać lub ominąć zabezpieczenia, celem uzyskania dostępu do informacji (§1). Analiza danych znajdujących się na urządzeniu oskarżonego lub świadka, wbrew ich woli, to nic innego jak uzyskanie dostępu do systemu bez uprawnienia (§2), a monitoring sieci bez wiedzy użytkowników, za pomocą odpowiedniego oprogramowania, można uznać za posługiwanie się oprogramowaniem do podsłuchu (§3). Jeśli działania te są dokonywane na zlecenie organów ścigania, w oparciu o odpowiednie przepisy prawa, uznać należy, iż informatyk działa w ramach kontratypu wyłączającego bezprawność działania. Obrona z całą pewnością baczniej będzie się teraz przyglądać, czy organ ścigania dopełnił wszelkich procedur przy zatrzymaniu i przeszukaniu sprzętu elektronicznego. Można bowiem forsować stanowisko, iż działanie sprzeczne z procedurą powoduje, iż organ wykracza poza kontratyp, co przy realizacji znamion czynu zabronionego może spowodować wykluczenie dowodu z procesu. Czy w takiej sytuacji informatyk śledczy dokonujący czynności może „dostać rykoszetem", bowiem to jemu będzie zarzucać się popełnienie czynu zabronionego?

Co w sytuacji, gdy na zlecenie prywatnej osoby informatyk śledczy dokona analizy sprzętu i zgromadzi materiał dowodowy wskazujący na popełnienie przestępstwa, po czym okaże się, że sprzęt nie był własnością tej osoby, a został skradziony? Znamiona czynu zabronionego zrealizuje zarówno zlecająca analizę osoba, jak i informatyk, który uzyskał dostęp do systemu, wbrew woli rzeczywistego właściciela urządzenia. Czy wiedza informatyka o tym w jakim celu zlecającemu potrzebne są zabezpieczane informacje, np. na potrzeby postępowania karnego, ma znaczenie?

Jak nowy zakaz dowodowy będzie funkcjonował w praktyce, będziemy mogli się dopiero przekonać. Wprowadzony przepis z całą pewnością powinien jednak skłonić informatyków śledczych do większej czujności i ostrożności, zarówno przy przyjmowaniu zleceń, jak i ich realizacji.

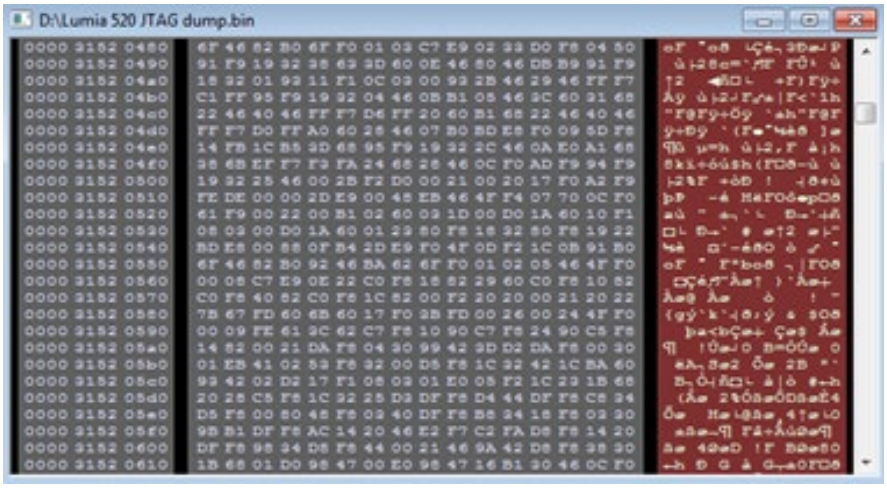
Autor jest adwokatem, szefem zespołu prawa własności intelektualnej i nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy. Trener w Akademii Informatyki Śledczej.

Mobile Forensic nie zawsze prosty i przyjemny

Michał Tatar

Dawno, dawno temu w odległej galaktyce... Takimi słowami chciałbym zacząć ten tekst zważywszy na to, o czym będzie traktował. Nie, to nie wstęp do następnej części Gwiezdnych Wojen, a Lord Vader nie zabierze Was na Ciemną Stronę. Wstęp odnosi się do czeluści kodu binarnego, który często jest odległy, ogromny i niezrozumiały, a który bardzo często dostarcza informatykom śledczym ciekawą historię z niestety nie zawsze dostępnym happy endem. Kod binarny, który kryje za sobą tajemnice w postaci danych, w świecie Mobile Forensic jest spotykany często natomiast rzadko prawidłowo interpretowany i analizowany. Z pewnością dlatego, że badanie jego zawartości nie jest proste i przyjemne. Pozwolę sobie zatem zabrać Was na Dobrą Stronę mocy...

Wyobraźmy sobie sytuację, w której do analizy otrzymujemy telefon bez interfejsu kablowego. Połączenie za pomocą radia Bluetooth jest niedostępne i jedyną możliwą drogą do ekstrakcji danych jest interfejs JTAG. Sytuacja spotykana często i jestem pewny, iż osoby mające do czynienia na co dzień z analizą urządzeń mobilnych skiną głową zgadzając się ze mną.

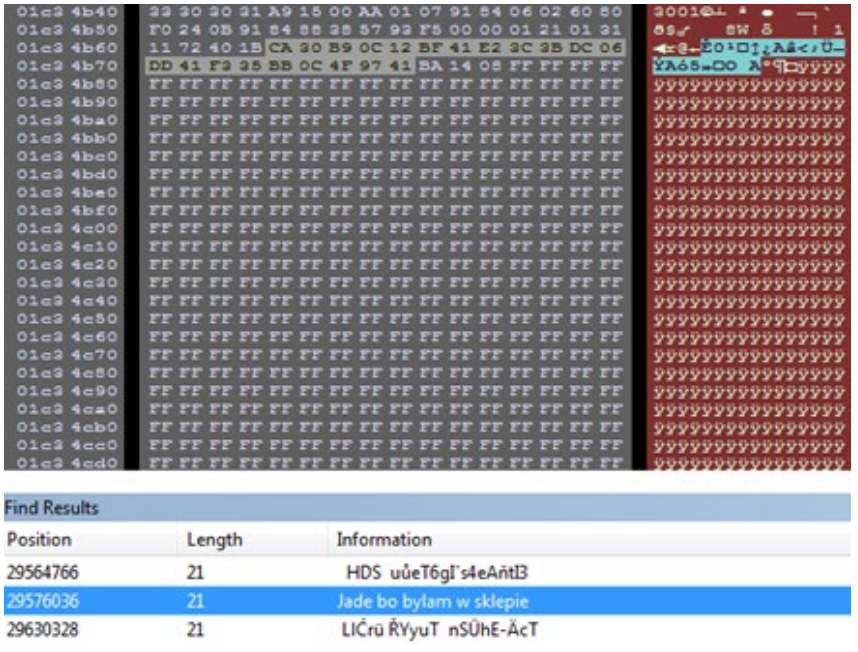


Rys. 1 Kod heksadecymalny.

Sprawa jest skomplikowana już na etapie samej ekstrakcji, gdyż odczyt danych przez złącze JTAG do łatwych nie należy i potrzeba odpowiedniego sprzętu i wiedzy by wyodrębnić dane w odpowiedni sposób.

Nie będę się jednak w tym artykule rozpisywał nad takim modelem ekstrakcji danych, gdyż owy tekst traktuje o analizie, a nie o sposobach odczytu. Idąc dalej, zakładamy sytuację, w której odczyt ląduje na naszym dysku twardym w postaci pliku BIN (pliku binarnego), który w dowolnej aplikacji wygląda tak jak na Rys 1. Na pierwszy rzut oka nie wygląda to w żaden sposób zachęcająco. Wręcz przeciwnie. Kod heksadecymalny dla człowieka nie jest w żaden sposób czytelny bez użycia odpowiednich narzędzi. Osobiście nie znam nikogo poza bohaterami filmu Matrix, którzy czytają biegle w HEXie.

Idealną sytuacją, w której przychodzi nam się zmierzyć z plikiem binarnym jest zastosowanie mechanizmów automatycznego dekodowania, dostępnego np. w oprogramowaniu XRY. Wówczas sprawa jest bardzo prosta – wystarczy zaimportować w odpowiedni sposób plik binarny do XRY, a on dzięki odpowiednio zaimplementowanym mechanizmom



Find Results

Position	Length	Information
29564766	21	HDS uůeT6gl˙s4eAńtl3
29576036	21	Jade bo bylam w sklepie
29630328	21	LIĆrü ŘYyuT nSÚhE-ÄcT

Rys. 2
7-bitowy ciąg przetłumaczony przez rozwiązanie XACT firmy MSAB.

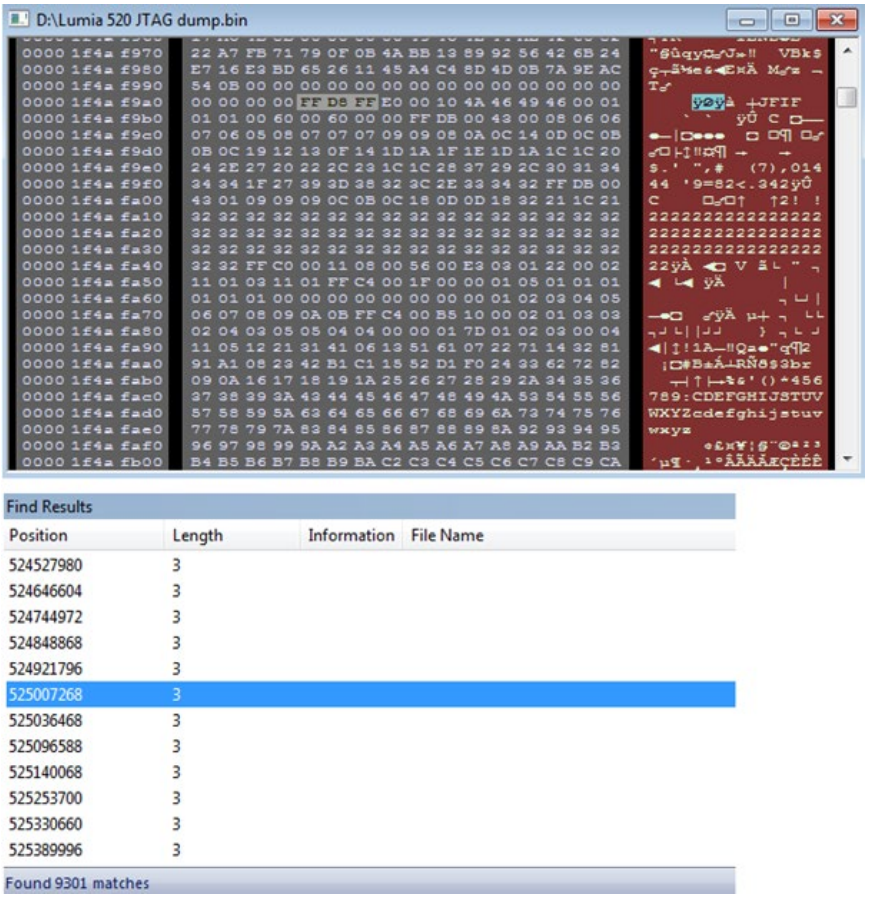
'przeczyta' plik BIN i pokaże w prosty sposób znalezione informacje, takie jak wiadomości SMS, MMS, e-mail, spis kontaktów, spis połączeń czy też różnego rodzaju pliki multimedialne. Jednakże złośliwość (świadoma bądź nie) producentów urządzeń mobilnych oraz systemów operacyjnych, pod kontrolą których pracują te urządzenia często stawiają nas w sytuacji, w której wykorzystanie metod automatycznego dekodowania nie jest dostępne. W takiej sytuacji musimy skorzystać z metod alternatywnych.

Zaawansowane metody analizy danych wymagają specjalistycznej wiedzy, ale przede wszystkim równie zaawansowanych narzędzi - na przykład XACT firmy MicroSystemation. Z pozoru prosty program, jednak przy odpowiednich umiejętnościach daje bardzo szerokie spektrum analizy plików binarnych. Jak to wygląda w praktyce? Sprawdzamy!

Przy analizie pliku binarnego przede wszystkim musimy być świadomi metod zapisu informacji przez systemy urządzeń mobilnych. Na początku przyjrzyjmy się wiadomościom SMS, ciągle lubianemu formatowi przekazywania informacji przez Polaków.

Międzynarodowym standardem wiadomości SMS jest alfabet GSM, który domyślnie zapisuje treści wiadomości w ciągach 7-bitowych. Tak, to nie pomyłka – 7 bitów, które nie dość, że są oczywiście zapisane w heksadecymalnym formacie, to jeszcze w kodowaniu 7 bitowym. Z pomocą przychodzi wspomniany wcześniej XACT, który wyposażony w różne metody przeszukiwania plików binarnych jest w stanie znaleźć ciągi wiadomości 7-bit oraz od razu przetłumaczyć je w przystępny dla każdego sposób. To, co widzimy po lewej (Rys. 2) to efekt końcowy. XACT odnalazł ciąg w formie ciągu 7-bitowego CA 30 B9 0C 12 BF 41 E2 3C 3B DC 06 DD 41 F3 35 BB 0C 4F 97 41 i automatycznie zdekodował go na prostą wiadomość „Jade bo bylam w sklepie". Prawda, że treść jest przystępna? Wiadomości SMS jak to zostało pokazane, są możliwe do wyodrębnienia z plików binarnych. Co zatem z plikami, na przykład graficznymi? Dzisiaj prawie wszystkie urządzenia mobilne wyposażone są w cyfrowe aparaty fotograficzne. Za statystykami – w kończącym się 2015 roku zostało wykonanych na świecie ponad tryllion zdjęć. Idąc dalej tym tropem, ponad 78% wszystkich tych zdjęć zostało wykonanych za pomocą urządzeń mobilnych.

Na zdjęciach odnalezionych w urządzeniach mobilnych znajdziemy wszystko

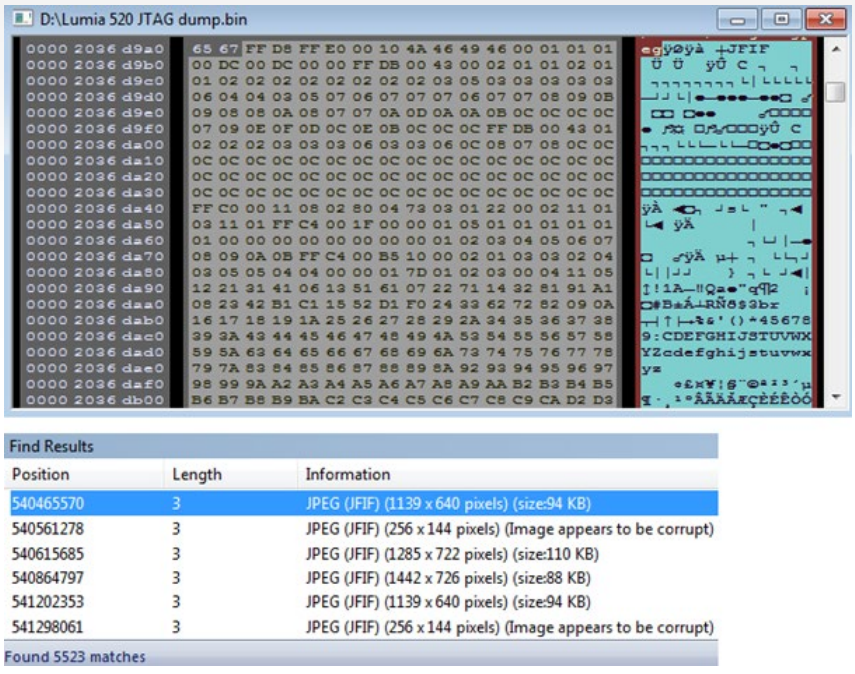


Rys. 3 Przeszukiwanie plików binarnych pod kątem występowania sygnatury pliku JPEG za pomocą XACT.

co możemy sobie wyobrazić, a nawet więcej. W analizie urządzeń mobilnych, pliki multimedialne, a zwłaszcza zdjęcia są bardzo często wykorzystywane jako dowody w sprawie. Przyjrzyjmy się zatem możliwościom ekstrakcji plików graficznych bezpośrednio z pliku binarnego. Tutaj również warto wspomnieć o zapisie plików graficznych - dla przykładu plik z rozszerzeniem JPEG, który najczęściej znajduje się w pamięci urządzenia mobilnego po wykonaniu zdjęcia przez użytkownika. Każdy plik posiada tzw. sygnaturę pliku, czyli ciąg bajtów określający typ pliku. Dla plików z rozszerzeniem JPEG sygnatura to pierwsze trzy bajty, na którą składają się „FF D8 FF" (w zapisie heksadecymalnym). Spróbujmy za pomocą XACT przeszukać plik binarny pod względem występowania sygnatury pliku JPEG (Rys. 3).

Jak widać na rysunku nr 3, w całym pliku binarnym wartość HEX „FF D8 FF" została odnaleziona 9301 razy. Nie oznacza to jednak, że wszystkie wartości heksadecymalne stanowią sygnaturę plików. W takim razie zastosujmy dodatkowy mechanizm dostępny w XACT, który dostarczy nam wszystkie pliki graficzne już poddane analizie pod kątem sygnatur plików. Wyszukiwarka odnalazła ponad 5000 plików graficznych JPEG (Rys. 4).

Naszym oczom we wskazanym wcześniej folderze ukazują się pliki graficzne i co więcej, również te skasowane i odzyskane.



Rys. 4 Przeszukiwanie plików binarnych pod kątem występowania sygnatury pliku JPEG za pomocą XACT.

Alternatywne metody pozyskiwania danych do łatwych i przyjemnych nie należą jednak warto znać mechanizmy, dzięki którym jest to możliwe. Na przykładzie treści wiadomości SMS oraz plików graficznych starałem się pokazać takie możliwości oraz zachęcić wszystkich, którzy pracują z urządzeniami mobilnymi by praktykować takie działania. Pokażcie swoją moc i stójcie zawsze po jej Dobrej Stronie. I jak to mówią – Niech moc będzie z Wami!

Autor jest specjalistą w zakresie analizy urządzeń mobilnych (Mobile Forensics) w Laboratorium Informatyki Śledczej Mediarecovery. Zajmuje się również implementacją rozwiązań mobilnych zarówno w sektorze prywatnym jak i publicznym (m.in. Mobile Device Management). Trener w ramach Akademii Informatyki Śledczej.

Ekstrakcja danych z kont Google - badanie firmy Elcomsoft

Andrey Malyshev

Firma Google zbiera i przechowuje ogromne ilości danych na temat każdego użytkownika korzystającego z ich usług. Uzyskanie do nich dostępu jest często niezbędne przy prowadzeniu wielu śledztw. Wiedza o tym co Google wie o podejrzanym ma kolosalne znaczenie dla służb i biegłych sądowych z zakresu informatyki śledczej.

Niestety, standardowe podejście uniemożliwia dostęp do tych informacji. Z tego powodu rozpoczęliśmy analizę kont Google na niższym poziomie niż pozwalają na to narzędzia Google.

Jakie to rodzaje danych? Obecnie prawie wszyscy posiadają konto Google. Według serwisu Site Point, udział Google Chrome przekracza 50% wśród wszystkich przeglądarek. Część użytkowników korzysta z możliwości synchronizacji przeglądarki Chrome, a co za tym idzie udostępnia swoje zakładki, historię wyszukiwania, nawigacji wraz z przechowywaniem formularzy i haseł na stronach www. Google Drive oferuje bardzo konkurencyjne rozwiązanie typu cloud pozwalając na przechowywanie prawie wszystkiego od zdjęć i filmów, przez dokumenty, e-maile na kopiach zapasowych systemu operacyjnego Android kończąc.

Android, jest najbardziej popularną platformą mobilną na świecie. Podaje się, że nawet 82% urządzeń mobilnych pracuje na Android OS. Łączna liczba aktywnych urządzeń z Androidem to około 1,4 mld (choć nie wszystkie z nich są urządzeniami Google). Od Androida 5.0 Lollipop, Google oferuje opcję tworzenia kopii zapasowej danych aplikacji do usługi w chmurze. Wiedza o tym co Google wie o nas i jakie rodzaje danych przechowuje jest bardzo ważna.

Badanie

Na początku użyliśmy Google Takeout czyli domyślnego narzędzia od Google do eksportu danych. Korzystając z niego staraliśmy się wyeksportować wszystko co Google przechowuje w chmurze.

Odkryliśmy, że Google Takeout nie dostarcza wszystkich ważnych danych. Informatycy śledczy i organa ścigania muszą korzystać z Google Takeout z ostrożnością ponieważ jego użycie pozostawia ślady na koncie użytkownika. Dodatkowo zostaje on powiadomiony, że jego dane zostały wyeksportowane przy użyciu Google Takeout. Ponadto plik wynikowy generowany przez Google Takeout nie jest gotowy do natychmiastowej analizy, jeśli dane zapisywane są w kilku różnych formatach. Przez to nie można go użyć do szybkiej analizy i weryfikacji danych.

Po analizie Google Takout rozpoczęliśmy badania żądań HTTPS i odpowiedzi przychodzących z urządzeń opartych na Androidzie z Google Chrome i innych aplikacji. Okazało się, że Google przechowuje przede wszystkim następujące informacje:

- Profil użytkownika
- Wszystkie podłączone urządzenia
- Urządzenia, przeglądarki i aplikacje, które ubiegają się o dostęp
- Ustawienia Google Advertising (w tym wiek, zainteresowania itp.)
- Kontakty
- Kalendarze
- Notatki (Google Keep)
- Wiadomości e-mail (Gmail)
- Albumy (zdjęcia, obrazki, filmy)
- Rozmowy Hangout
- Kompleksową historię lokalizacji
- Dane z Google Fit (śledzenie aktywności sportowej)

Google Chrome przechowuje następujące informacje:

- Historię przeglądania
- Zakładki
- Zapisane hasła
- Dane autouzupełniania
- Zakładki
- Historia wyszukiwania w wyszukiwarce Google i YouTube

Wyszukiwanie i historia przeglądania zawiera wiele ważnych informacji, z punktu widzenia śledczych. Każdy rekord ma następujące atrybuty:

- Informacje o przeglądarce lub aplikacji mobilnej
- Działania wyników wyszukiwania (otwarte lub nie)
- Interakcje z reklamami (kliknięcia i zakupy)
- Adres IP
- Informacje o przeglądarce

Wyszukiwanie i historia przeglądania nie są eksportowane przez Google Takeout.

W kopiach zapasowych systemu operacyjnego Android Google zapisuje następujące dane:

- Ustawienia kalendarza Google
- Sieci Wi-Fi i hasła
- Tapety ekranu głównego
- Ustawienia Gmail
- Listę aplikacji zainstalowanych przez Google Play
- Ustawienia wyświetlania
- Język i wprowadzanie ustawień
- Datę i godzinę
- Dane aplikacji innych producentów

Automatyczne tworzenie kopii zapasowych dla aplikacji innych producentów zostało ogłoszone dopiero dla Androida 6.0 „Marshmallow". Wersje wstępne Androida 6.0 wykorzystują opcję „opt-out", jako sposób obsługi kopii zapasowych danych dla aplikacji innych firm, co oznacza, że dane te zostaną zapisane i przywrócone zaocznie chyba, że deweloper zrezygnował z tej funkcji w pliku manifestu w aplikacji.

Docelowa wersja Androida 6 odwróci ten problem, korzystając z metody „opt-in". W celu automatycznego przywrócenia zapasowych kopii danych programiści muszą zezwolić na to w manifeście aplikacji. Do tej pory tylko kilka aplikacji korzysta z tego więc zapasowe kopie danych firm trzecich nie zdarzają się jeszcze zbyt często.

Więcej informacji na ten temat dostępnych jest w doskonale napisanym artykule zamieszczonym na Ars Technica: Android 6.0 ma świetny system tworzenia automatycznych kopii zapasowych, których nikt nie używa (jeszcze). Oczywiście, wszystkie zdjęcia (czyli Google Picasa, znana też jako Google+ Photos) również są przechowywane w chmurze. Takie informacje przechowuje:

- Albumy i wydarzenia
- Komentarze
- Tagi Geo
- Subskrypcje
- Licznik wyświetleń
- Ludzie oznaczeni na zdjęciach

Podczas badań okazało się, że do niektórych fragmentów danych (na przykład historia lokalizacji, elementy dashboardu czy rozmowy Hangout) można uzyskać dostęp bez wywoływania powiadomienia użytkownika lub bez pozostawiania śladów na koncie Google. Pozwala na to na przeprowadzenie analizy nie alarmując użytkownika.

Jeszcze w tym roku, mamy plany na udostępnienie narzędzia do pozyskiwania i analizowania danych z kont Google. Elcomsoft Cloud eXplorer umożliwi śledczym na dostęp do kont Google i zdobycie wszystkich dostępnych informacji. Proszę śledzić wiadomości na https://www.elcomsoft.com

Autor jest praktykiem, stale angażującym się w rozwój rozwiązań służących do analiz śledczych urządzeń mobilnych i odzyskiwania haseł. CTO w Elcomsoft.

Wyzwania w pozyskiwaniu i analizie danych z urządzeń mobilnych

Tatiana Pankova

W dzisiejszych czasach ludzie częściej używają urządzeń mobilnych niż komputerów - czatują przez komunikatory, udostępniają wydarzania życiowe w sieciach społecznościowych, korzystają z mobilnych przeglądarek internetowych, planują wycieczki i spotkania za pośrednictwem aplikacji itp. To dlatego pozyskiwanie danych z urządzeń mobilnych jest tak istotne dla specjalistów informatyki śledczej. W artykule chciałabym opisać wyzwania w analizach mobile forensics.

Urządzenia chronione hasłem

Z ostatnich badań wynika, że aż 2/3 wszystkich użytkowników w USA stosuje na swoich urządzeniach mobilnych blokadę w postaci hasła. Istnieje kilka chińskich rozwiązań łamiących blokady ekranu, takie jak IP Box i MFC Dongle, ale nie obsługują one najnowszej wersji iOS i mają słabe wsparcie dla urządzeń opartych na systemie Android. W naszym oprogramowaniu, Oxygen Forensic Detective, proponujemy metodę omijania blokady ekranu iOS z wykorzystaniem pliku z komputera użytkownika lockdown.plist. Ponadto wiemy, jak w skuteczny sposób ominąć blokadę ekranu z urządzeń Android OS. Jeśli to nie pomoże zawsze można próbować JTAG lub metody Chip-off. Obrazy utworzone za pomocą tych metod mogą być analizowane w Oxygen Forensic Detective.

Zaszyfrowane kopie zapasowe

Użytkownik może ustawić hasło, nie tylko na ekranie urządzenia, ale również do tworzenia kopii zapasowych urządzeń lub obrazu. Na przykład może zaszyfrować kopię zapasową iTunes. Nie ma sposobu, aby ją ominąć, trzeba poznać hasło inaczej żadne dane nie zostaną wyodrębnione. W Oxygen Forensic Detective wbudowane jest narzędzie autorstwa Passware, które rozpoznaje hasła za pomocą różnych ataków, w tym brute-force.

Zdobądź tyle danych ile to możliwe

Wyobraźmy sobie, że nie masz urządzenia lub jest ono doszczętnie zniszczone. W tym przypadku trzeba poszukać innych źródeł akwizycji danych. Można poszukać pliku kopii zapasowej urządzenia na komputerze użytkownika, zwrócić się do providera po CDR (Call Data Records) celem analizy komunikacji lub zdobyć dane z chmury. W Oxygen Forensic Detective wszystkie te metody są obsługiwane i wszystkie ekstrakcje danych mogą być połączone w jedną celem kompleksowej analizy.

Odzyskiwanie usuniętych danych

Nie wystarczy wyodrębnić istniejących rekordów, informatycy śledczy potrzebują również dostępu do usuniętych danych. Prawie wszystkie dane użytkownika przechowywane są w bazie danych SQLite i nie ważne jakie jest to urządzenie - iOS, Android, BlackBerry 10, Windows Phone 8. Usunięte dane takie jak kontakty, czaty, rozmowy mogą być pozyskane z bazy danych SQLite przez prawie wszystkie oprogramowania do analiz mobile forensic.

Analiza danych

Wyobraźmy sobie, że udało się przezwyciężyć wszystkie dotychczasowe wyzwania, więc masz gigabajty zdjęć, tysiące wiadomości i połączeń, setki kontaktów. Ręczna analiza tych danych zajmie dużo czasu. Istnieje kilka narzędzi analitycznych, takich jak „i2" ale należy pamiętać, że nie wszystkie formaty są ze sobą kompatybilne. W każdym przypadku lepiej mieć oprogramowanie śledcze z wbudowaną opcją analityczną. W Oxygen Forensic Detective można analizować wszystkie eventy w porządku chronologicznym, znaleźć właściciela urządzenia, wskazać najbliższy krąg komunikacji, sprawdzić wspólne kontakty i wspólną lokalizację różnych urządzeń, a poprzez słowa kluczowe znaleźć interesujące nas dane w kilka sekund. Osoby chcące wypróbować nasze rozwiązanie zapraszam do przesłania prośby o wersję trailową za pośrednictwem naszej oficjalnej strony www.oxygen-forensic.com

Autorka jest ekspertem z zakresu data mining. Posiada ponad 9-letnie doświadczenie w tzw. głębokiej analizie danych zapisanych w chmurze i urządzeniach mobilnych.

Jak skutecznie obsługiwać zaawansowane ataki APT (tzw. Advanced Persistent Threats)

Paweł Pietrzak

Pomimo setek milionów złotych wydawanych rocznie na systemy bezpieczeństwa większość organizacji jest ciągle narażona na ataki APT (tzw. Advanced Persistent Threats), które pozostają niewykryte przez wiele miesięcy, i które przynoszą wymierne straty dla działalności i wizerunku rynkowego. Rozwój „security" nie może oznaczać tylko dążenia do perfekcji systemów prewencyjnych, które przestały być już skutecznym gwarantem obrony.

Sytuacja może ulec poprawie poprzez zmianę podejścia działów IT w firmach do obsługi incydentów i postawienie na: szybkość, trafność i powtarzalność procesu odpowiedzi (tzw. Incident Response Workflow - IRW). Planując reakcję na incydent APT nie należy jednak jej sprowadzać tylko do reinstalacji zainfekowanej stacji. Należy wziąć pod uwagę także problem wskazania celowanego ataku wśród wielu alertów związanych z tzw. „commodity malware" oraz dostępność narzędzi dla efektywnego kontynuowania analizy zdarzenia przez SOC.

FireEye od dłuższego czasu promuje wdrażanie procesu IRW. Tej strategii podporządkowany jest rozwój produktów i usług firmy. W czasie prezentacji na konferencji URDI 2015 zostało w praktyczny sposób zaprezentowane rozwiązanie endpoint – FireEye HX – które pomaga w sprawnej realizacji czterech najważniejszych etapów procesu IRW:

1. Wykrycie incydentu (detection)
2. Zapobieganie/ograniczenie wpływu incydentu na działalność organizacji (prevention)
3. Analiza incydentu i gromadzenie danych na temat ataku (analysis)
4. Wdrożenie działań remediacyjnych – naprawczych (response)

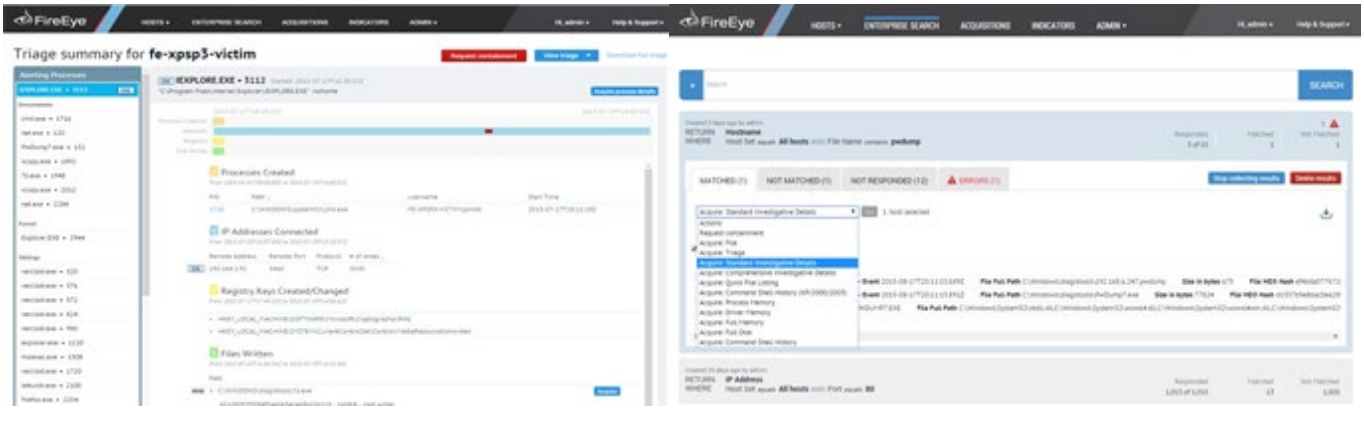
Dzięki automatycznej integracji między urządzeniami sieciowymi FireEye wykrywającymi ataki APT w procesie dynamicznej analizy w środowisku MVX, a agentami endpoint, HX umożliwia płynne przejście z etapu „Wykrycia incydentu" do „Zapobiegania" i „Analizy Incydentu" – czyli domeny HX.

FireEye HX umożliwia automatyczne potwierdzenie infekcji hosta na podstawie definicji ataku (tzw. IoC - Indicator of Compromise). Tuż po stwierdzeniu zagrożenia operator systemu może przystąpić do jego wstępnej oceny – agent HX automatycznie przekazuje mu logi opisujące najważniejsze zmiany w systemie wykonane przez malware i przedstawia je w formie graficznej upraszczającej analizę.

Ślady wskazujące na zaawansowany atak, szczególnie, jeśli istnieje zagrożenie zdalnego dostępu do stacji, pozwalają operatorowi podjąć decyzję o przekazaniu incydentu do szczegółowej analizy oraz wykonać izolację (tzw. Containment) hosta od reszty sieci.

Od tego momentu jedynie uprawnione komputery mogą się komunikować z zainfekowaną stacją. Inne połączenia są blokowane, co ogranicza wpływ ataku na organizację. Izolacja może dotyczyć zarówno komputera w sieci LAN jak i tego znajdującego się poza siedzibą firmy. Specjalista przystępujący do szczegółowej analizy ataku ma również do dyspozycji tzw. Enterprise Search, umożliwiający tworzenie zapytań o prawie każdy parametr systemu, w celu potwierdzenia potencjalnych zmian i wykluczenia tzw. False Positives.

Po zawężeniu analizy do wybranych komputerów możliwe jest zebranie dowodów i dalsza analiza narzędzi i metod użytych podczas ataku. FireEye HX umożliwia pobieranie podejrzanych plików, historii wykonywanych komend, pamięci RAM

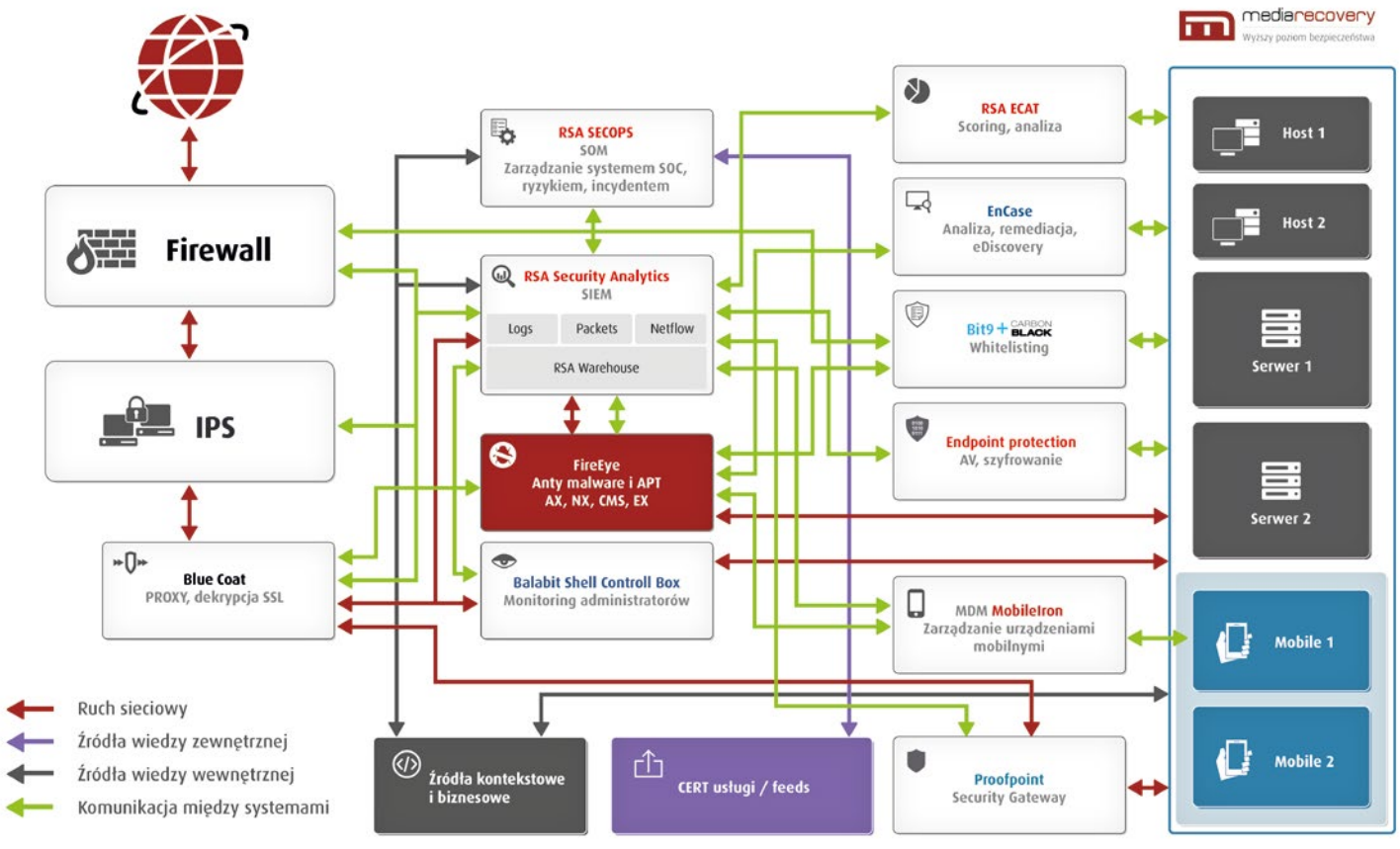


Po lewej widok tzw. Triage Viewer w konsoli HX podsumowującego najważniejsze zdarzenia związane z wykrytym atakiem Po prawej przykład tzw. Enterprise Search w GUI HX.

czy nawet obrazów dysków z hostów. Warto podkreślić, że wszystkie funkcjonalności HX zostały opracowane i są nadal rozwijane na podstawie doświadczeń specjalistów działu Mandiant w FireEye, którzy realizują usługi Incident Response w najbardziej skomplikowanych i największych przypadkach włamań na świecie. Powiązanie techniki i doświadczenia z jej stosowania, pozwoliło uzyskać sprawdzone narzędzie dla obsługi najbardziej skomplikowanych incydentów.

Autor jest inżynierem systemowym w firmie FireEye.

FireEye w przykładowej strukturze Security Operations Center



Usługi Mediarecovery w obszarze Security Operations Center

Projektowanie

Opracowywanie procesów i określanie zasobów

Integracja systemów

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: magazyn@mediarecovery.pl
www.magazyn.mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Mariusz Ruski
Reklama: Damian Kowalczyk

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl
www.mediarecovery.pl

mediarecovery
Lider informatyki śledczej