MAGAZYN

NR 29 / MARZEC 2016

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

UZYSKANIE DOSTĘPU DO SZYFROWANYCH DOWODÓW ELEKTRONICZNYCH: WYZWANIA I ROZWIĄZANIA

PROFILOWANIE HAKERÓW - CZĘŚĆ II

OS X: 7 METOD NA UKRYCIE SIĘ MALWARE

EMAIL JAKO NAJCZĘSTSZY WEKTOR CYBERATAKÓW W OKRESIE NOWEGO ROKU 2016

CSI SUITE MOŻE POGODZIĆ SKUTECZNE PROWADZENIE BIZNESU ZE SKUTECZNĄ OCHRONĄ INFRASTRUKTURY IT

CO W NUMERZE?

Magazyn w wersji PDF

Wszystkie Magazyny możesz bezpłatnie pobrać z Magazyn.mediarecovery.pl

Nowelizacja ustawy o Policji – pole do popisu dla informatyków śledczych?

Co takiego wprowadziła nowelizacja ustawy z dnia 6 kwietnia 1990 r. o Policji oraz niektórych innych ustaw, która weszła w życie 7 lutego br., nazywana ustawą inwigilacyjną, krytykowana przez praktycznie wszystkie środowiska opiniotwórcze? Jakie uprawnienia w ramach prowadzenia kontroli operacyjnej w cyberświecie uzyskały służby, czy (nadal) swobodnie będą mogły sięgać po bilingi i czy rzeczywiście wolność i prywatność internautów jest obecnie zagrożona?

Jarosław Góra

W wyroku z dnia 20 lipca 2014 r. (sygn. K 23/11) Trybunał Konstytucyjny, badając przygotowany w tamtym czasie projekt nowelizacji ustaw o służbach autorstwa senatorów PO orzekł, że celem zapewnienia stanu prawnego zgodnego z ustawą zasadniczą oraz prawem europejskim (kwestia tzw. retencji danych była wówczas „na tapecie" ze względu na orzeczenie Trybunału Sprawiedliwości UE w zakresie nieważności dyrektywy w tym przedmiocie), należy wprowadzić niezależną kontrolę udostępniania służbom danych od operatorów, uregulować przepisy gwarantujące niezwłoczne i komisyjne niszczenie materiałów pochodzących z inwigilacji, jeśli zawierały tajemnice zawodowe (np. dziennikarskie, adwokacką - jeśli sąd nie ich nie uchylił), zobowiązać sądy, aby te precyzyjnie określały w zezwoleniu na inwigilację, jakie dane i jakimi technikami mogą być zbierane, wprowadzić obowiązek informowania inwigilowanego (po zakończeniu inwigilacji) o tym fakcie oraz określić w ustawie maksymalny czas trwania tego rodzaju kontroli. Trybunał orzekł, iż niezbędne zmiany w ustawach powinny zostać wprowadzone w terminie 18 miesięcy.

Odpowiedniej nowelizacji nie zdążyli przygotować i wprowadzić rządzący poprzedniej kadencji, natomiast uchwalili ją obecnie sprawujący władzę. Nowelizacja krytykowana jest przez organizacje społeczne, Helsińską Fundację Praw Człowieka, Rzecznika Praw Obywatelskich, Naczelną Radę Adwokacką oraz Krajową Izbę Radców Prawnych. Również Biuro Analiz Sejmowych uznało projekt nowelizacji za niezgody z prawem Unii Europejskiej. Czy słusznie? Analiza wprowadzonych zmian rzeczywiście nie skłania do uznania, iż wdrożone zostały wszystkie zalecenia Trybunału Konstytucyjnego.

Zakres czynności możliwych do podjęcia w ramach kontroli operacyjnej, która do tej pory obejmowała przede wszystkim kontrolę korespondencji, przesyłek i treści rozmów telefonicznych oraz przy pomocy sieci telekomunikacyjnej został rozszerzony. Obecnie niejawna kontrola może polegać również

na uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne, uzyskiwaniu i utrwalaniu treści korespondencji prowadzonej za pomocą środków komunikacji elektronicznej, uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Wcześniej podmioty wykonujące działalność telekomunikacyjną oraz podmioty świadczące usługi pocztowe były obowiązane do zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej. Obecnie obowiązek taki ciąży na przedsiębiorcach telekomunikacyjnych, operatorach pocztowych oraz usługodawcach świadczących usługi drogą elektroniczną.

W zakresie tajemnicy obrończej nowelizacja uwzględnia uwagi TK, bowiem w przypadku, gdy materiały zgromadzone podczas kontroli zawierają informacje, o których mowa w art. 178 Kodeksu postępowania karnego, Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki Policji zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie. W przypadku tajemnicy dziennikarskiej natomiast materiały te są przekazywane prokuratorowi, który niezwłocznie po otrzymaniu materiałów kieruje je do sądu, który zarządził kontrolę operacyjną albo wyraził na nią zgodę, w celu stwierdzenia, które z przekazanych materiałów zawierają takie informacje oraz dopuszczenia (bądź nie) do wykorzystania w postępowaniu karnym materiałów zawierających informacje stanowiące tajemnice. Sąd ma natomiast dopuścić możliwość wykorzystania tych materiałów, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu, albo zarządzić niezwłoczne zniszczenie materiałów, których wykorzystanie w postę-

powaniu karnym jest niedopuszczalne.

Jeśli chodzi o uzyskiwanie i przetwarzanie przez służby danych telekomunikacyjnych, pocztowych i internetowych, to mogą je przetwarzać bez wiedzy i zgody osoby, której dotyczą, a wskazani wyżej dostawcy usług są obowiązani je przekazywać. Nowość dotyczy danych internetowych, określonych w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, a więc obejmuje bardzo szeroki zakres danych o internaucie. Jednak zgromadzone dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Trybunał Konstytucyjny wskazał, iż niezbędne jest wprowadzenie systemu nadzoru nad prowadzoną przez służby kontrolą operacyjną. Nowelizacja wprowadza obowiązek składania sprawozdań do sądu okręgowego, w okresach półrocznych, obejmujących liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych, rodzaj tych danych oraz kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o te dane albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych (takie bowiem są cele ich uzyskania). Wydaje się, że nie o taki system nadzoru chodziło Trybunałowi. Z punktu widzenia informatyków śledczych najciekawsze wydają się nowe uprawnienia służb polegające na możliwości uzyskiwania i utrwalaniu treści korespondencji prowadzonej za pomocą środków komunikacji elektronicznej, ale również danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Czy w ten sposób służby uzyskały uprawnienie do „zaglądania" do naszych komputerów zdalnie? Przekonamy się w praktyce. Z całą pewnością jednak informatycy śledczy będą mieli sporo pracy.

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

Email jako najczęstszy wektor cyberataków w okresie Nowego Roku 2016

Paweł Pietrzak

Okres świąteczno-noworoczny to również czas wytężonej pracy dla cyberprzestępców, którzy sprawdzają skuteczność nowych technik dla rozpoczęcia ataku, często losowo wybierając swoje ofiary. Historycznie ten intensywny okres roku zwiastował zawsze prawdziwy zalew zagrożeń przenoszonych drogą email, zwykle tematycznie związanych z zakupami lub dostawą zamawianych towarów. Pozwalało to na uśpienie czujności nawet użytkowników świadomych zagrożeń.

Według specjalistów z FireEye Labs, aktywność cyberprzestępców w końcówce 2015 roku możemy podzielić na trzy grupy:

1. Kampanie kradzieży tożsamości usług bankowych
2. Kampanie dla okupu (tzw. ransomware)
3. Nowe trendy złośliwego oprogramowania

Niekwestionowanym liderem pierwszej grupy jest Dridex - bardzo rozpowszechniona odmiana trojana, którego głównym celem jest kradzież bankowych danych uwierzytelniających oraz - w efekcie - pieniędzy z konta ofiary. Dotychczas znaliśmy Dridex w postaci złośliwych załączników MS Word lub odsyłaczy URL, dostarczanych w poczcie elektronicznej. Jednak wkrótce po aresztowaniu głównego operatora Dridex w połowie października 2015 roku, zaobserwowano nową metodę dystrybucji trojana przy użyciu złośliwych makr w plikach Excel oraz tzw. Exploit Kit-ów. Ponad dziesięciokrotne nasilenie tej kampanii przypadło na drugi tydzień listopada. Zapewne atakujący chcieli pokazać swoją moc i odzyskać kontrolę na utraconymi zasobami. Dridex próbował wtedy oszukać odbiorców podszywając się pod znane marki jak: Avis, Shell czy UK Mail.

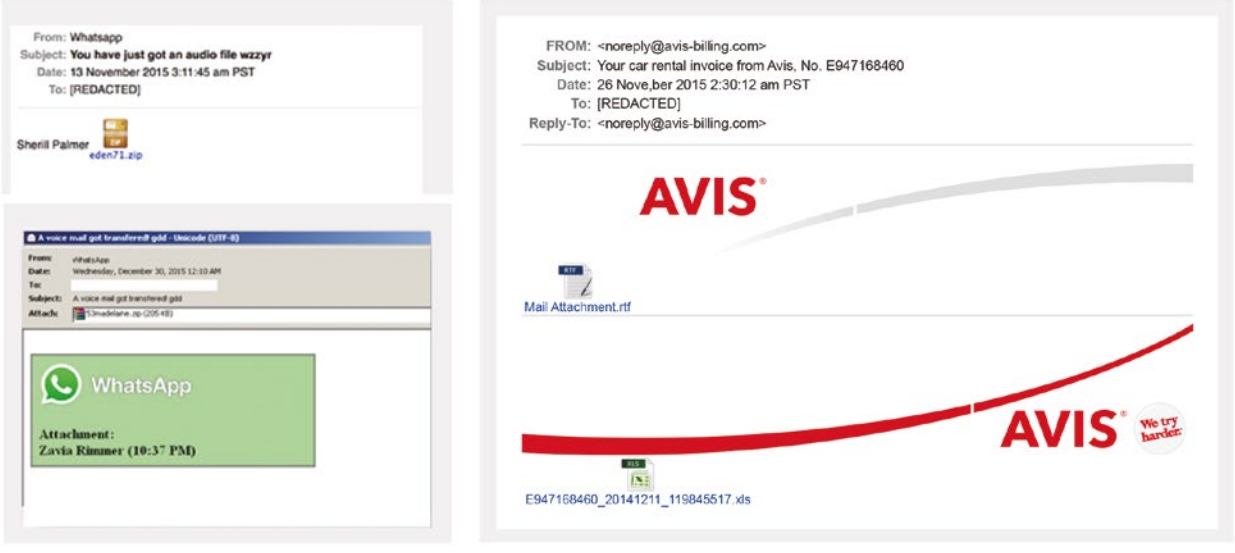
Kolejny z tej grupy zagrożeń to Fareit – znany również jako Pony Loader, którego celem jest kradzież danych z aplikacji FTP, pamięci podręcznej przeglądarki

lub popularnych kryptoportfeli: Bitcoin, Bytecoin, Litecoin. Fareit był zwykle instalowany jako tzw. downloader drugiego etapu np. dla Trojana Zbot. Ostatnie ataki dowodzą, że sprawdził się również jako główne źródło infekcji w phishingu. Bożonarodzeniowa kampania Fareit podszywała się głównie pod firmy sektora turystycznego jak American Airlines czy Abercrombie&Kent. Ostatni reprezentant tej rodziny malware to Ursnif. Relatywnie stary, bo wykryty już w 2007 roku, malware z grupy MITB (Man In The Browser), nastawiony na kradzież haseł dostępowych, certyfikatów i innych informacji transferowanych bez szyfrowania. Konstrukcja wiadomości email z ostatniej kampanii rozsyłającej złośliwy załącznik Ursnif była bardzo prosta, bez zawartości elementów graficznych, z użyciem aktualnych całorocznie tematów np. „wezwanie do zaplaty", „transaction", „wezwanie przedsądowe", „payment".

Drugą grupę otwiera Teslacrypt – pierwszy raz widziany w lutym 2015. W fazie infekcji wykorzystuje popularny Exploit Kit Angler. Szczyt aktywności Teslacrypt jako szkodliwego załącznika email nastąpił w połowie grudnia 2015, przy czym podobnie jak Ursnif, tylko okazjonalnie podszywano się pod znane marki, wykorzystując bardziej ogólne tematy wiadomości np. „invoice", czy „order". Cechą wyróżniającą ten atak od typowego spamu, były z pewnością złośliwe skrypty typu downloader, często unikalne pod względem sumy MD5. Innym przedstawicielem kategorii ransomware jest Nymaim stosujący zaawansowane zaciemnianie kodu oraz złożoność ataku: pierwszy plik wykonywalny po pomyślnym uruchomieniu pobiera drugi komponent. Należy podkreślić pomysłowość atakujących, którzy w spreparowanej wiadomości email zachęcali ofiarę do osobistego kontaktu z nadawcą, co służyło budowaniu dodatkowego zaufania do wiadomości.

W trzeciej grupie reprezentującej nowe trendy ataków korzystających z email jest Nivdort – dotychczas bardzo rzadko obserwowany, o działaniu podobnym do Trojana Spy. Dystrybuowany jako załącznik ZIP w kampaniach spam, po udanym ataku tworzy losowy katalog, po czym ustawia jego atrybut na ukryty i dopisuje się do regularnego autostartu, zapewniając sobie uruchomienie po każdym włączeniu lub restarcie komputera.

W najnowszej odsłonie Nivdort próbował podszywać się pod skrzynkę głosową komunikatora Whatsapp, w tytule wiadomości używając języka angielskiego, niemieckiego, francuskiego i rumuńskiego. "Phishing" pozostaje wciąż jednym z głównych wektorów infekcji, chętnie używanym przez cyberprzestępców dla dostarczenia malware do organizacji. Również wykrycie takich złośliwych kampanii email pozostaje wciąż wyzwaniem dla systemów ochrony opartych na sygnaturach (AV/AS), ze względu na ciągłe doskonalenie technik ataku, stosowanie socjotechniki i używanie modyfikacji wersji malware. Dowodzą tego zaprezentowane tutaj przykłady ewolucji znanych rodzin malware-u. Odmiana „phishingu" – tzw. "spear phising", była także skutecznie wykorzystywana w atakach APT (tzw. Advanced Persistent Threats) wykrytych przez urządzenia FireEye w roku 2015, związanych z działaniami takich grup jak APT29 czy APT30 . Dlatego tak ważne jest, aby brać pod uwagę wzrost znaczenia email we współczesnych atakach i odpowiednio wzmocnić ochronę tego kanału komunikacji, zarówno przez stosowanie rozwiązań do analizy i detekcji ataku bez opierania się na wcześniejszej znajomości próbki malware (bezsygnaturowych) jak i przez edukację i uświadamianie zagrożenia użytkownikom poczty elektronicznej.



Przykładowe wiadomości z kampanii Nivdort WhatsApp oraz Dridex Avis

Pełna wersja raportu FireEye, która zawiera również dane ataków w postaci IoC (Indicators of Compromise) dla opisanych powyżej przykładów zagrożeń, jest dostępna pod adresem: https://www2.fireeye.com/holiday-email-campaigns-fireeyelabs.html

Autor jest inżynierem systemowym w firmie FireEye.

Profilowanie hakerów

część 2

Od czasu opublikowania pierwszej części artykułu miałem możliwość przemyślenia i przedyskutowania moich poglądów na temat profilowania hakerów. W związku z tym i obecnie wykonywaną pracą chciałbym zastrzec, że prezentowane poniżej uwagi są wyłącznie moją opinią i nie powinny być łączone z jakąkolwiek instytucją.

Maciej Gajewski

Pozostaje aktualnym stwierdzenie, że w Polsce w dalszym ciągu profilowanie jest zagadnieniem, o którym można poczytać w literaturze popularnej, np. Katarzyna Bonda w cyklu Cztery Żywioły profilerkę Saszę Załuską uczyniła swoją bohaterką, ale z takim prawdziwym żywym exemplum ciężko się zetknąć na co dzień.

Osobiście zainteresowany jestem profilowaniem hakerów, a pozostałe kwestie związane z profilowaniem, jakkolwiek bardzo ciekawe pozostawiam poza polem rozważań. Miałem przyjemność uczestniczyć w ciekawej konferencji policyjnej, gdzie zaprezentowany został referat nawiązujący do profilowania cyberprzestępców, ale według mojej wiedzy wciąż jest to bardzo rzadką praktyką. Nie chciałbym być też źle zrozumiany i uznany za osobę, która uważa profilowanie hakerów za jedyne lekarstwo. Po prostu uważam to narzędzie za bardzo ciekawe i mogące przynieść wiele przydatnych odpowiedzi. Tych, którzy chcą poznać wszystkie minusy, wady profilowania, odsyłam do ciekawej publikacji Karoliny Olszak-Haubler „Czy profilowanie kryminalne ma podstawy naukowe". Zastanawiające dla mnie jest to, że wydaje się stosunkowo duże środki - nawet w sektorze publicznym - na bezpieczeństwo teleinformatyczne, a nie bada drugiej strony, tej atakującej. I nie chodzi mi o aspekt jak?, kiedy?, gdzie? kto? (to jest robione) tylko o aspekt dlaczego? I przy okazji dlaczego ten ktoś, to robi, lub zrobił, bądź ewentualnie może zrobić. Na chwilę odbiegając od głównego wątku chciałbym dodać, że nie istnieje żaden system, który pokazywałby zbiorczo w skali całego kraju ilość incydentów i analizował sposób postępowania (modus operandi) ewentualnych sprawców. Jakieś tam elementy wiedzy są obecne w poszczególnych instytucjach, ale są one ze sobą nie połączone. Kiedyś na tych samych łamach pisałem o braku systemu zarządzania incydentami teleinformatycznymi w całym kraju. Takiego systemu w dalszym ciągu nie ma, są pewne zalążki, które można by oprzeć np. o zbudowaną przez MAC sieć pełnomocników ds. cyberbezpieczeństwa. Nie jest tajemnicą, że poważne służby państwowe przygotowują analizy ryzyka nie mając twardych danych o zjawiskach z cyberprzestrzeni. Nie prowadzi się akcji informacyjnych, bo nie ma danych i analiz grup cyberprzestępczych. Na konferencji SECURE w tym roku była przedstawiona prezentacja CERT-u NASK-u: „Cyberprzestępczość w Polsce". Jednym z proponowanych działań na przyszłość było badanie przyczyn źródłowych cyberprzestępczości. Bardzo mnie to cieszy i będę temu kibicował. Ładnie wydane raporty za 2014 rok Cert Orange Polska i CERT.GOV.PL nie mówią o tym, dlaczego ktoś dopuszcza się działań związanych z naruszeniem cyberbezpieczeństwa innych podmiotów. Słynna służba na trzy litery jest tak zajęta wypełnianiem swoich obowiązków, że nie jest w stanie przygotować jawnych materiałów, które można by upubliczniać i poszerzyć wiedzę społeczeństwa.

Wbrew pozorom, wszystko to, co wyżej napisałem ściśle łączy się z zagadnieniem profilowania, gdyż nie mając bazy do analizy, trudno mówić o wynikających z niej wnioskach. Jak z powyższych słów wynika, profilowaniem mogą się zajmować ewentualnie jacyś zwariowani pasjonaci, którzy nie mają nic do roboty. Może i by się ich udało gdzieś razem zagonić do wspólnej pracy, ale w dalszym ciągu wracamy do punktu wyjścia. Nie ma w naszym kraju instytucji badawczej, która zajęłaby się takimi sprawami, bo nawet gdyby istniała jakaś fundacja, która byłaby zainteresowana pozyskaniem tego typu wiedzy, to w efekcie ktoś musiałby za to zapłacić. I znowu mamy problem. Najłatwiej jest straszyć hakerami, cybeprzestępcami i innymi złymi ludźmi, bo tak łatwo jest powiedzieć w mediach. Ja osobiście, jak przypuszczam większość osób zajmujących się bezpieczeństwem chcielibyśmy wiedzieć nie tylko przed czym i przed kim mamy się bronić, ale chcielibyśmy również wiedzieć coś więcej o atakującym, o sposobie jego myślenia, motywacji. Interesuję się profilowaniem, bo powinienem wiedzieć, czy np. ktoś, kto jest właśnie przyjmowany do pracy, ma takie cechy, że może stwarzać problemy, a może już zatrudnieni mają skłonności, które należałoby przeanalizować. Szukam narzędzi i wiedzy, która może mi pomóc.

Norma „PN-ISO/IEC 27005:2014 Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji" zaleca zwrócenie szczególnej uwagi na źródła zagrożeń osobowych. Dzieli je na 5 grup. (Rys. 1)

Do każdych z tych grup norma przypisuje motywację. Przy hakerach, crackerach są to: wyzwanie, ego, rebelia, status, pieniądze. Pytanie do czytelnika: skąd autorzy taką wiedzę na temat motywacji mają? Moim zdaniem odpowiedź jest jedna: kogoś, gdzieś na świecie to interesuje i ktoś to bada, skoro wyniki

Rys. 1 - Grupy zagrożeń osobowych

tych badań znalazły się w międzynarodowej normie. Szkoda, że nie w Polsce.

Jak napisałem na początku, miałem możliwość zrewidowania swoich poglądów na temat profilowania hakerów. Instytucja będąca jednym z pionierów w zakresie profilowania, czyli FBI, w zakresie profilowania hakerów nie podejmuje badań, idzie bardziej w kierunku profilowania przestępstw tzw. białych kołnierzyków. W tym obszarze mieszczą się często cyberprzestępstwa. Inne organizacje również bardziej zwracają uwagę na zagrożenie ze strony własnych pracowników, tzw insiderów. National Cybersecurity and Communications Integration Center w 2014 r. opublikował „Combating the Insider Threat". Na gruncie polskim chętnych odsyłam do publikacji Małgorzaty Nyc „Profilowanie w polityce bezpieczeństwa korporacyjnego". Nie jest nowością, że więcej ataków generalnie pochodzi ze środka niż z zewnątrz organizacji. Pamiętam wypowiedź Ricka Fergussona (chyba z tamtego roku), który twierdził, że obecnie atakujący jest już w środku organizacji i przed tym musimy się bronić. Całkowicie się z tym zgadzam, bo uważam, że nasza praca – osób odpowiedzialnych za bezpieczeństwo informacji – polega głównie na budowaniu security awareness, jak niektórzy mówią tworzeniu tzw. kultury bezpieczeństwa informacji. Raport Trend Micro o głównych przyczynach wycieków oraz celu pozyskiwania danych osobowych mówi że np. rozczarowani pracownicy upubliczniają dane z własnej woli. I nie trzeba ich przełamywać (komentarz MG). Można powiedzieć, że dowodzi to też innej tezy. Cyberprzestępczość ewoluuje i w zasadzie prawdziwych hakerów w rozumieniu lat 80 już nie ma. Obecnie mamy do czynienia ze zorganizowanymi organizacjami, grupami, czy nawet jednostkami państwowymi, które wykorzystują narzędzia i metody hakerskie. Nasuwa się więc pytanie, cóż skomplikowanego jest w tym, aby odpowiednio wyedukować potencjalnego kandydata do pracy, wyposażyć go w umiejętności kojarzone z umiejętnościami hakerskimi i umieścić go w interesującej nas instytucji? Narzędzia pracy dostanie gotowe od swoich mocodawców.

Przed takimi zagrożeniami powinniśmy się bronić i do tego można wykorzystać profilowanie hakerów. Jak pisałem w I części artykułu w przypadku hakerów stworzony profil ma pomóc stworzyć zespół cech osobowościowych, czyli skłonności, upodobań wskazujących, że taka osoba może ewentualnie stanowić bazę, podbudowę do stania się hakerem. Istnieje duże prawdopodobieństwo, że tak się stanie. I znowu muszę nawiązać do tego, co pisałem wcześniej. Brak wsparcia, brak dużej bazy danych, notującej szereg dokładnie opisanych incydentów utrudnia takie działania.

Przez wiele lat badałem wizerunek medialny hakerów, różnice między stereotypem funkcjonującym w świadomości medialnej, społeczeństwie a rzeczywistością. Nie miałem takich możliwości jak Raoul Chiesa i nie prowadziłem badań kwestionariuszowych nie przeprowadzałem wywiadów z byłymi hakerami. W każdym razie na podstawie własnych doświadczeń studiowanej literatury przedmiotu mogę powiedzieć, że można przygotować kwestionariusz, który będzie weryfikował i badał skłonności badanego. Jak przy każdym profilowaniu bardzo ważną rolę odgrywa tu doświadczenie badającego, sposób prowadzenia rozmowy, znajomość rzeczy. Myślę, że na potrzeby polityki bezpieczeństwa takie profilowanie byłoby już przydatne. Takie działania uznałem za niewystarczające i dlatego szukałem dalej. Czytając publikacje poświęcone badaniom gier komputerowych, środowiskom ich twórców i producentów znalazłem pewne cechy wspólne dla hakerów, twórców gier oraz graczy. Na podstawie takiej analizy można przygotować oprogramowanie / grę, która będzie doskonale weryfikować skłonności badanych do hakingu.

Brak tu miejsca na dokładny opis takiego oprogramowania / gry, ale z moich analiz wynika jednoznacznie, że właśnie mechanizm gry potrafi pokazać, ujawnić cechy typowe lub kluczowe dla osób w jakiś sposób zarażonych ideą hakingu. Wszystkie inne media gubią istotne elementy obrazowania hakera i hakingu, gra zaś jest całością, jest syntezą.

Autor jest specjalistą w zakresie ochrony informacji w sektorze publicznym z 15 letnim doświadczeniem. W wolnym czasie realizuje się jako niezależny badacz „ciemnej strony" cyberkultury i pasjonat security awareness.

Dowody elektroniczne odgrywają ważną rolę w wielu dochodzeniach lecz zdarza się, że ich istotna część jest zaszyfrowana. W wielu przypadkach szyfrowanie może uniemożliwić prowadzone śledztwo oraz pozyskanie i analizę dowodów.

Uzyskanie dostępu do **szyfrowanych dowodów elektronicznych**: Wyzwania i rozwiązania

Dmitry Sumin

Obecnie są setki aplikacji wspierających szyfrowanie. Działają zarówno na urządzeniach mobilnych, jak i komputerach stacjonarnych. To pozostawia informatyka śledczego z wieloma typami plików zaszyfrowanych: dokumentów biurowych i archiwów. Hasła i loginy do stron internetowych mogą znajdować się w pamięci komputera lub plikach hibernacji. Full Disc Encryption jest dostępny dla wszystkich głównych systemów operacyjnych na rynku.

Metody deszyfrowania są bardzo zróżnicowane dla różnych typów plików. Choć słabe szyfrowanie pozwala znaleźć hasło lub klucz szyfrujący pliki niemal natychmiast, najbardziej nowoczesne formaty szyfrowania są naprawdę solidne. Atak brute-force (sprawdzanie wszystkich haseł), atak słownikowy lub kombinacje tych metod to w niektórych przypadkach jedyna opcja.

Informatykom śledczym zapewniamy bezpłatne narzędzie, które skanuje system plików i wykrywa te zaszyfrowane. Narzędzie wykorzystuje tę samą technologię wykrywania szyfrowania, która jest używana przez Passware Kit Forensic i EnCase od Guidance Software. Raportuje typy szyfrowania i określa jak trudny może być atak na dany plik.

Szyfrowanie jest coraz bardziej popularne wśród użytkowników. Zarówno system Windows 10, jak i Mac OS X Yosemite mają pełne szyfrowanie dysków (odpowiednio BitLocker i FileVault2) włączoną domyślnie. Użytkownicy są też coraz bardziej świadomi w zakresie tworzenia silnych haseł. Większość najnowszych aplikacji używa standardowych, bezpiecznych algorytmów szyfrujących. To sprawia, że uzyskanie dostępu do zaszyfrowanych dowodów elektronicznych staje się dużym wyzwaniem. Ataki brute-force są czasochłonne, mogą trwać od kilku tygodni do ponad roku, zanim hasło zostanie znalezione lub atak zostaje po prostu przerwany. Zalecane jest stosowanie dedykowanych urządzeń w celu przyspieszenia odzyskiwania haseł. Zamiast opierać się o GPU stosuje się akceleratory. Niezwykle trudny do przewidzenia jest wskaźnik sukcesu ataków typu brute-force.

Jednym ze sposobów przezwyciężenia tych wyzwań to analiza „live" pamięci. Passware Kit Forensic jest zdolny do skanowania obrazów pamięci, tworzenia listy wykrytych kluczy szyfrowania wraz z tekstową prezentacją hasła oraz haseł do kont użytkowników i tokenów uwierzytelniania umożliwiających dostęp do danych w chmurze.

Istnieje wiele rodzajów obrazów zawierających, z punktu widzenia informatyków śledczych, bezcenne informacje: zrzut pamięci fizycznej RAM, dumpy, hiberfil.sys (plik hibernacji Windows) czy pagefile. Wykonanie obrazu z pamięci zablokowanego komputera z pewnością nie należy do trywialnych. „Warm boot attack" to praktyczny sposób prowadzenia akwizycji pamięci „live" w takich przypadkach. Bootowalny pendrive lub nośnik CD-ROM jest używany do uruchamiana ba-

Passware Encryption Analyzer można pobrać pod adresem:
http://www.lostpassword.com/encryption-analyzer.htm

danego komputera poprzez użycie bardzo małej wersji systemu operacyjnego Linux, która wykonuje zrzut pamięci RAM na zewnętrzny dysk twardy lub pendrive. W ten sposób można wykonać akwizycję większości zawartości pamięci, z wyjątkiem obszarów, które zostały użyte w celu załadowania pamięci samego narzędzia.

Technika ta jest bardzo skuteczna w poszukiwaniu kluczy szyfrowania dla oprogramowania pełnego szyfrowania dysku, takiego jak BitLocker, FileVault2 lub TrueCrypt. Obrazy „live" pamięci mogą wskazać hasła używane przez przeglądarki komputerowe pracujące w trybach „Incognito" lub „InPrivate".

Główną korzyścią wynikającą z analizy pamięci „live" jest wysoki wskaźnik sukcesu i przewidywalny czas potrzebny do zbadania obrazów. Przetwarzanie obrazu pamięci 16GB jest zazwyczaj wykonywane w niecałe 30 minut, w porównaniu do dni, tygodni lub miesięcy poświęconych na ataki brute-force.

Wykonywanie tego typu akwizycji ma znaczenie krytyczne. W wielu sprawach ważne jest by uchwycić jak najwięcej dowodów, jak to możliwe, w tym obrazy „live" pamięci.

Więcej informacji o Passware Kit Forensics i metod dekrypcji danych jest dostępnych na stronie internetowej www.passware.com

Założyciel i prezes Passware Inc. Specjalista kryptografii i kryptoanalizy z 17-letnim doświadczeniem.

OS X: 7 metod na ukrycie się malware

Michał Ferdyniok

Twierdzenie, że urządzenia pracujące na OS X są bezpieczne jest już od dłuższego czasu nieaktualne. Wraz ze wzrostem popularności rozwiązań Apple znalazły się one w polu zainteresowań cyberprzestępców. Problem jest na tyle dojrzały, że zainteresował analityków z Bit9+Carbon Black Threat Research Team, amerykańskiej firmy zajmującej się ochroną korporacji przed malware.

To właśnie zaawansowany malware jest obecnie największym zagrożeniem bezpieczeństwa IT. Chodzi tu o skalę i powszechność użycia szkodliwego oprogramowania przez cyberprzestępców. Trojany, wirusy, spyware i inne są równie zaawansowane technicznie, jak profesjonalne oprogramowanie tworzone przez firmy.

Przez długi czas cyberprzestępcy nie interesowali się urządzeniami produkowanymi przez Apple, skupiając się na komputerach pracujących pod Windows. Zwyczajnie nie opłacało się im angażować wysiłków w tworzenie złośliwego oprogramowania dla stosunkowo niewielkiej liczby urządzeń. Na koniec 2001 roku udział rynkowy Apple wynosił niecałe 3%, na koniec 2014 roku już ponad 16%. Zauważyli to również cyberprzestępcy i zaczęli działać.

Na podstawie ponad 1400 próbek złośliwego oprogramowania, analitykom z Bit9+Carbon Black Threat Research Team udało się wyróżnić 7 najczęstszych metod ukrywania się malware w OS X. Oto one:

1. LaunchAgents - proces w systemie operacyjnym uruchamiany z uprawnieniami użytkownika. W tym wypadku malware zaczyna działać w momencie logowania się użytkownika do systemu i zostaje aktywny do momentu jego wyłączenia. 2. LaunchDaemons - proces w systemie operacyjnym umożliwiający uruchomienie programów w tle. Jeśli zostanie wykorzystana ta technika to malware uruchomi się zaraz po włączeniu komputera przed zalogowaniem się użytkownika. 3. Cron job – jest to sposób na uruchomienie malware przy pomocy procesu systemowego cyklicznie uruchamiającego zadania zdefiniowane w plikach konfiguracyjnych. W takim wypadku skrypt cyklicznie uruchamia złośliwe oprogramowanie. 4. Login items – wykorzystuje ustawienia użytkownika w celu uruchomienia malware w komputerze po zalogowaniu się użytkownika do systemu. Twórcy złośliwego oprogramowania wykorzystują możliwość definiowania programów uruchamianych automatycznie przy starcie systemu. 5. Wtyczki do przeglądarki – nie w każdym przypadku malware dokonuje infekcji samego systemu operacyjnego, zdarza się iż celem ataków są poszczególne programy np. przeglądarki internetowe. Infekcja zostaje wykonana poprzez instalację wtyczki do przeglądarki. Wtyczka taka może zbierać informacje o użytkowniku np. loginy i hasła 6. StartupItems – podobnie jak w przypadku LaunchDaemons – jest to lista programów i usług które uruchamiane są podczas startu systemu operacyjnego. Oprogramowanie takie może zostać uru-

chomione raz lub działać jako usługa w tle. 7. Infekcja binarna – modyfikuje oryginalny plik wykonywalny dodając do niego szkodliwy kod. W takim przypadku użytkownikowi wydaje się, że uruchamia poprawną i sprawdzoną aplikację np. program do poczty e-mail jednak dodatkowo uruchamia się też złośliwy kod. Omawiane badanie wskazuje wyraźnie, że również w komputerach Apple należy używać oprogramowania zabezpieczającego. W przypadku użytkowników domowych może być to program antywirusowy, w przypadku firm najlepiej żeby było to rozwiązanie oparte na whitelistingu. Infrastruktura firm jest narażona na większą ilość i różnorodność cyberzagrożeń. Zatem i ochrona przed malware wymaga bardziej zaawansowanych i skutecznych środków zaradczych.

Autor jest kierownikiem laboratorium informatyki śledczej Mediarecovery

CSI Suite może pogodzić skuteczne prowadzenie biznesu ze skuteczną ochroną infrastruktury IT

„Biznes hamowany jest przez procedury bezpieczeństwa IT. W odpowiedzi na rosnące ataki, organizacje przyjmują strategie obronne, które opierają się na cyklu coraz mocniejszych predefiniowanych kontroli bezpieczeństwa. Powoduje to, że biznes jest nadmiernie ograniczany, jego produktywność zmniejsza się, a zespoły bezpieczeństwa są przytłoczone alertami i ciągle zmienianymi poleceniami. W wielu organizacjach takie podejście w rzeczywistości osłabia bezpieczeństwo, gdyż kontrole są pomijane a potencjalne zagrożenia bezpieczeństwa niezauważone.” – *komentuje Zoltán Györkő, CEO firmy Balabit.*

Rośnie obawa firm przed wyrafinowanymi cyberatakami. Obecnie napastnicy są inteligentni, dobrze przygotowani, a atakujący mogą swobodnie poruszać się wewnątrz środowiska IT ofiar. Działanie z wewnątrz organizacji ma przewagę nad infrastrukturą bezpieczeństwa firmy, ponieważ narzędzia te zostały stworzone do ochrony przed zewnętrznymi zagrożeniami, a nie przed własnymi, zaufanymi pracownikami. W ukierunkowanych atakach wykorzystuje się kombinacje luk systemowych, inżynierię społeczną i zwykłe przestępstwa, aby pozyskać nieautoryzowany dostęp do wewnętrznej sieci firmowej. Ostatnie badania opinii specjalistów IT wykazują, że pomimo obawy o bezpieczeństwo, w obliczu znaczącej okazji biznesowej i zysku, rośnie chęć do ryzyka i omijania zabezpieczeń. Ponad 2/3 profesjonalistów IT byłaby skłonna do podjęcia ryzyka potencjalnego zagrożenia bezpieczeństwa w celu osiągnięcia największej transakcji swojego życia. Jest tak mimo, że wcześniej prawie ¾ z nich twierdziło, że bezpieczeństwo jest równie ważne, jak nie ważniejsze od elastyczności biznesowej, (według ankiety przeprowadzonej przez Balabit pośród blisko 400 profesjonalistów IT, również z Polski).

„Te wyniki ukazują, że organizacje muszą jeszcze dużo zrobić, aby zbalansować wymogi bezpieczeństwa i elastyczność biznesu. Wykazują, że nadmierne bezpieczeństwo może być tolerowane podczas normalnych zadań biznesowych, jednakże gdy przychodzi wielki „deal” respondenci nie wahaliby się ominąć zabezpieczenia w celu osiągnięcia sukcesu biznesowego. To ważne, aby rozpoznać i odpowiednio rozpatrywać ten problem.” – komentuje Zoltán Györkő.

Jednym ze skutecznych rozwiązań może być zintegrowany Contextual Security Intelligence Suite firmy Balabit, który łączy zarządzanie rejestrami zdarzeń (Log Management), monitoring uprzywilejowanych użytkowników (Privileged User Monitoring) oraz narzędzia analizy ich zachowania (User Behavior Analytics). Takie podejście usprawnia bezpieczeństwo IT poprzez koncentrowanie się na aktywności użytkownika. Przy czym zamiast ograniczać uprzywilejowanych użytkowników poprzez coraz bardziej skomplikowane i uciążliwe zasady uwierzytelniania, rozwiązanie CSI Suite działa na zasadzie zaufania, ale ze sprawdzaniem. Stale monitoruje aktywność uprzywilejowanych użytkowników i zbiera w czasie rzeczywistym dane z całego przedsiębiorstwa o okolicznościach powiązanych z tą aktywnością.

Technologia uczących się maszyn i zawansowane algorytmy są wykorzystywane do stworzenia profilu normalnych zachowań użytkownika i do identyfikacji anomalii, które są potencjalnymi zagrożeniami bezpieczeństwa. W ten sposób wcześniej nieznane zagrożenia mogą być traktowane priorytetowo i zbadane wraz z szeroką wiedzą o okolicznościach z nimi związanymi.

CSI Suite zawiera zaawansowany interfejs użytkownika, który pozwala zespołowi bezpieczeństwa szybko zobaczyć przegląd zagrożeń i wybrać najbardziej ryzykowne aktywności. Dostarczony też jest poziom śledczy, zawierający pełny przegląd i wideo powtórki wszystkich aktywności uprzywilejowanych użytkowników.

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

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