EUIPO
URZĄD UNII EUROPEJSKIEJ DS. WŁASNOŚCI INTELEKTUALNEJ

IDENTYFIKACJA I ANALIZA ZŁOŚLIWEGO OPROGRAMOWANIA NA WYBRANYCH STRONACH INTERNETOWYCH PODEJRZEWANYCH O NARUSZANIE PRAW AUTORSKICH

STRESZCZENIE

Wrzesień 2018 r.

Abstrakt

Treści podejrzewane o naruszanie praw autorskich stanowią poważne naruszenie praw własności intelektualnej. Istnieją strony internetowe, które udostępniają takie treści publicznie, czasami nawet nieodpłatnie i bez żadnej rejestracji. Wraz z takimi treściami strony internetowe często rozpowszechniają różnego rodzaju złośliwe oprogramowanie oraz potencjalnie niepożądane programy (z ang. tzw. PUP-y), wabiąc użytkowników do pobierania i uruchamiania tych plików. Badanie zawiera przegląd najnowszych przykładów złośliwego oprogramowania i PUP-ów znalezionych na stronach internetowych podejrzewanych o naruszanie praw autorskich. Programy te wykorzystują zwodnicze techniki i inżynierię społeczną, jak np. puste instalacje gier i pozornie „użyteczne" oprogramowanie w celu nakłonienia użytkowników końcowych do ujawnienia informacji szczególnie chronionych. W trakcie badania odkryto różne PUP-y, takie jak „użyteczne" oprogramowanie, fałszywe instalatory gier czy fałszywi klienci platform do strumieniowej transmisji wideo. Oprogramowanie to niekoniecznie stanowi bezpośrednie zagrożenie dla oprogramowania lub sprzętu komputerowego użytkownika. Jednak dzięki sztuczkom inżynierii społecznej można przekonać użytkownika do ujawnienia szczególnie chronionych danych osobowych lub danych kart płatniczych. Ponadto informacje o samym komputerze mogą zostać ujawnione innym stronom bez wyraźnej zgody użytkownika.

Zespół badawczy

W skład zespołu badawczego weszli: Francesca Bosco, urzędnik ds. programów UNICRI, oraz Andrii Shalaginov, doktorant w dziedzinie bezpieczeństwa informacji w Departamencie Bezpieczeństwa Informacji i Technologii Komunikacyjnych (grupa ds. kryminalistyki cyfrowej) na Wydziale Technologii Informacyjnej i Inżynierii Elektrycznej Norweskiego Uniwersytetu Nauk i Technologii.

Zastrzeżenie prawne

W tym kontekście należy podkreślić, że jedynym celem badania było określenie właściwości technicznych złośliwego oprogramowania i PUP-ów, na które natknięto się podczas badania i na które mogli natknąć się użytkownicy internetu poszukujący treści podejrzewanych o naruszanie praw autorskich. Udokumentowanych przykładów złośliwego oprogramowania i PUP-ów nie można uznać za wyczerpujące, a celem badania (lub jego wyników) nie było przedstawienie oceny ogólnego prawdopodobieństwa lub ryzyka wystąpienia złośliwego oprogramowania oraz infekcji PUP-ami, z którymi zetknąłby się użytkownik internetu poszukujący materiału podejrzewanego o naruszanie praw autorskich.

Przedmowa

Działania w internecie podejrzewane o naruszanie praw autorskich mogą być finansowane na różne sposoby, w tym poprzez pobieranie opłat abonamentowych, darowizny, płatności za usługi pomocnicze oraz przychody z reklam wyświetlanych w internecie.

Nie wszystkie środki finansowania są jednak tak niegroźne, jak te w powyższych przykładach. Przez lata rozpowszechnianie złośliwego oprogramowania oraz innego rodzaju potencjalnie niepożądanych programów (PUP-ów) miało kluczowe znaczenie dla finansowania działań podejrzewanych o naruszanie praw autorskich w internecie.

Zwykli użytkownicy internetu powoli zaczynają zdawać sobie sprawę z zagrożeń związanych z infekcją takim oprogramowaniem, która może nastąpić podczas wchodzenia na strony internetowe lub aplikacje mobilne podejrzewane o naruszanie praw autorskich.

Tabela wskaźników EUIPO w zakresie własności intelektualnej młodzieży z 2015 r. pokazała, że 52% młodych ludzi uznaje bezpieczeństwo na stronie internetowej za ważną kwestię przy uzyskiwaniu dostępu do treści online. Ogółem 78% młodych ludzi stwierdziło, że zastanowiliby się dwa razy, gdyby byli świadomi ryzyka, że komputer lub urządzenie mogą zostać zainfekowane wirusami lub złośliwym oprogramowaniem. Ogółem 84% respondentów uznało, że zastanowiliby się dwa razy, gdyby byli świadomi ryzyka możliwości kradzieży danych kart kredytowych.

W badaniach przeprowadzonych na potrzeby niniejszego opracowania Urząd podjął się bardzo trudnego technicznie zadania polegającego na wykryciu i udokumentowaniu przykładów złośliwego oprogramowania i PUP-ów, z którymi użytkownik internetu mógłby się zetknąć podczas próby uzyskania dostępu do popularnych pirackich filmów, muzyki, gier wideo i produkcji telewizyjnych.

W tym kontekście należy podkreślić, że jedynym celem badania było określenie właściwości technicznych złośliwego oprogramowania i PUP-ów, na które natknięto się podczas badania i na które mogli natknąć się użytkownicy internetu poszukujący treści podejrzewanych o naruszanie praw autorskich. Udokumentowanych przykładów złośliwego oprogramowania i PUP-ów nie można uznawać za wyczerpujące, a celem badania (lub jego wyników) nie było przedstawienie oceny ogólnego prawdopodobieństwa lub ryzyka wystąpienia złośliwego oprogramowania oraz infekcji PUP-ami, z którymi zetknąłby się użytkownik internetu poszukujący materiału podejrzewanego o naruszanie praw autorskich.

Badanie przeprowadzono w kilku etapach, w ścisłej współpracy z Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu.

Wyniki wskazują na szereg różnych zagrożeń związanych ze złośliwym oprogramowaniem i PUP-ami, z którymi użytkownik internetu może się zetknąć podczas poszukiwania treści podejrzewanych o naruszanie praw autorskich. Większość udokumentowanego złośliwego oprogramowania i PUP-ów można zaklasyfikować jako trojany lub inne niechciane oprogramowanie, które jest w stanie uzyskać nieuprawniony dostęp do danych osobowych użytkowników internetu. Przykłady te będą istotne i interesujące nie tylko dla społeczności uprawnionej z tytułu prawa własności intelektualnej, ale również dla organów ścigania, a także — co nie mniej istotne — dla konsumentów, którzy obawiają się udostępniania ich danych osobowych bez ich zgody.

Streszczenie

Badanie zawiera przegląd najnowszych przykładów złośliwego oprogramowania i potencjalnie niepożądanych programów (PUP-ów) znalezionych na stronach internetowych podejrzewanych o naruszanie praw autorskich. Programy te wykorzystują zwodnicze techniki i inżynierię społeczną, jak np. puste instalacje gier i pozornie „użyteczne" oprogramowanie w celu nakłonienia użytkowników końcowych do ujawnienia informacji szczególnie chronionych.

Celem tego badania jest wykrycie i udokumentowanie złośliwego lub w inny sposób niechcianego oprogramowania rozpowszechnianego na wybranych stronach internetowych podejrzewanych o naruszanie praw autorskich, jak również sklasyfikowanie wykrytych próbek według różnych taksonomii złośliwego oprogramowania. W tym kontekście należy podkreślić, że jedynym celem badania było określenie właściwości technicznych złośliwego oprogramowania i PUP-ów, na które natknięto się podczas badania i na które mogli natknąć się użytkownicy internetu poszukujący treści podejrzewanych o naruszanie praw autorskich. Udokumentowanych przykładów złośliwego oprogramowania i PUP-ów nie można uznać za wyczerpujące, a celem badania (lub jego wyników) nie było przedstawienie oceny ogólnego prawdopodobieństwa lub ryzyka wystąpienia złośliwego oprogramowania oraz infekcji PUP-ami, z którymi zetknąłby się użytkownik internetu poszukujący materiału podejrzewanego o naruszanie praw autorskich. Do celów niniejszego badania programy telewizyjne, filmy, muzyka oraz gry wideo uznawane są za treści chronione prawami autorskimi.

Wyniki badania

Treści podejrzewane o naruszanie praw autorskich stanowią poważne naruszenie praw własności intelektualnej. Istnieją strony internetowe, które udostępniają takie treści publicznie, czasami nawet nieodpłatnie i bez żadnej rejestracji. Wraz z taką treścią strony internetowe często rozpowszechniają różnego rodzaju złośliwe oprogramowanie oraz PUP-y, wabiąc użytkowników do pobierania i uruchamiania tych plików. Podczas identyfikacji stron internetowych na podstawie rankingu Alexa Top 500 — oprócz symulacji wyszukiwań przeciętnych użytkowników przy użyciu znanych wyszukiwarek, takich jak Google, Yahoo i Bing — stwierdzono, że wykaz stron internetowych zmienił się między dwiema turami badania. Zmiana ta jest prawdopodobnie wynikiem prób wyszukiwarek w kwestii usuwania linków do stron podejrzewanych o naruszanie praw autorskich, przy równoczesnym pojawianiu się nowych stron podejrzewanych o takie samo naruszenie. Co się tyczy identyfikacji stron internetowych, jednym z interesujących ustaleń był fakt, że przeważająca większość stron internetowych jest utrzymywana w Stanach Zjednoczonych lub posiada nazwy domen powiązane z utrzymywanymi tam stronami. Zalewie kilka ze stron znajduje się natomiast na serwerach w UE. Ponadto domeny .com i .net są najczęstszymi nazwami domen najwyższego poziomu, których używa się na stronach internetowych podejrzewanych o naruszanie praw autorskich. Może to być spowodowane faktem, że — w przeciwieństwie do domen specyficznych dla danego kraju — nie mogą one wymagać identyfikacji użytkownika za pomocą paszportu lub innego dokumentu tożsamości. Średnio dodano 20% nowych stron internetowych, a 20% starych stron usunięto pomiędzy dwiema turami identyfikacji. Ponadto prawie 8% stron internetowych zidentyfikowanych w obu turach platforma VirusTotal uznała za złośliwe. Dzięki różnym systemom zarządzania treścią proste stało się obecnie tworzenie strony internetowej i dostarczanie użytkownikom nie tylko treści, lecz również złośliwych aplikacji.

Przed zebraniem złośliwego oprogramowania w 2017 r. przeprowadzono przegląd zagrożeń związanych ze złośliwym oprogramowaniem oraz klasyfikację najnowocześniejszych rozwiązań. Zdobyty zasób wiedzy wykorzystano następnie podczas analizy złośliwego oprogramowania w ramach przestrzegania przyjętych przez społeczność zasad dotyczących złośliwego oprogramowania i identyfikacji rodziny. W trakcie obu tur gromadzenia danych zgromadzono łącznie 106 plików. Obejmowały one zarówno pliki pobrane bezpośrednio ze stron internetowych

podejrzewanych o naruszanie praw autorskich, jak i te utworzone podczas uruchamiania pobranych plików. Podczas badania odkryto różne PUP-y, takie jak „użyteczne" oprogramowanie, fałszywe instalatory gier czy fałszywi klienci platform do strumieniowej transmisji wideo. Oprogramowanie to niekoniecznie stanowi bezpośrednie zagrożenie dla oprogramowania lub sprzętu komputerowego użytkownika. Jednak dzięki sztuczkom inżynierii społecznej można przekonać użytkownika do ujawnienia szczególnie chronionych danych osobowych lub danych kart płatniczych. Ponadto informacje o samym komputerze mogą zostać ujawnione innym stronom bez wyraźnej zgody użytkownika.

Zebrane złośliwe oprogramowanie przeanalizowano najpierw przy użyciu narzędzi open source w celu zrozumienia wewnętrznej logiki, wykrycia możliwych złośliwych działań oraz oceny ich znaczenia dla niniejszego badania dotyczącego złośliwego oprogramowania. Oprócz wstępnej analizy przy użyciu narzędzi open source, stworzona przez Europol platforma rozwiązań do analizy złośliwego oprogramowania (EMAS) przeanalizowała zebrane próbki złośliwego oprogramowania. W rezultacie wykryła ona wiele różnych przedmiotów i złośliwych działań. Raporty EMAS zawierają kompleksową analizę plików przy użyciu czterech wersji systemu MS Windows, w ramach której — w celu dalszej analizy — dokładnie rejestruje się ruch sieciowy, wywołanie funkcji i działania związane z dyskami. Ponadto platforma podświetla wszelkie podejrzane działania wykryte podczas uruchamiania plików. Po przeanalizowaniu wszystkich raportów EMAS odnotował 35 rodzajów złośliwych działań, które sklasyfikowano w 17 klasach złośliwych zdarzeń. Zdarzenia te obejmowały zarówno ogólne anomalie (takie jak uruchamianie procesów systemowych lub przeglądanie procesów w pamięci), jak i jednoznacznie złośliwe działania (takie jak manipulowanie keyloggerem, rootkitem i ruchem sieciowym).

Ogólnie rzecz biorąc, zebrane próbki binarne złośliwego oprogramowania i PUP-ów ujawniły kilka różnych ogólnych modeli biznesowych: „użyteczne" oprogramowania rzekomo usuwające stare pliki na komputerze użytkownika po opłaceniu abonamentu, symulatory instalacji gier wymagające danych osobowych użytkownika oraz darmowe oprogramowania oferujące dostęp do platform dystrybuujących pirackie treści, np. za pośrednictwem trackera BitTorrent. Dwie tury identyfikacji stron internetowych i gromadzenia złośliwego oprogramowania dały obiecujące wyniki w zakresie zrozumienia metod rozpowszechniania złośliwego oprogramowania i inżynierii społecznej w pozyskiwaniu szczególnie chronionych informacji osobowych i identyfikowalnych. Ponadto rosnąca popularność urządzeń mobilnych w ostatnich latach jest widoczna w świetle wykrycia wielu PUP-ów dla systemu Android OS, dostępnych za pośrednictwem platform dystrybucyjnych podejrzewanych o naruszanie praw autorskich. W wyniku zestawienia analiz wyciągnięto wniosek, że krajobraz zagrożeń złośliwego oprogramowania rozpowszechnianego za pośrednictwem stron internetowych naruszających prawa autorskie jest bardziej złożony niż mogłoby się to wydawać na pierwszy rzut oka. Wśród odkrytego oprogramowania niektóre można dodatkowo sklasyfikować jako trojana, adware'a, backdoora czy agenta. Sytuację pogarsza fakt, że znaleziono również wiele szczególnych rodzin złośliwego oprogramowania, takich jak WisdomEyes, DealPly, czy też FileRepMalware. Co więcej, taka kompleksowa klasyfikacja w równym stopniu dotyczy platformy Android, nie tylko Microsoft Windows. Istnieje wiele zagrożeń dla zasobów użytkowników, w tym między innymi kradzież danych uwierzytelniających i danych osobowych szczególnie chronionych, informacji o konfiguracji sprzętu oraz modyfikacja ruchu sieciowego. W związku z tym nawet jeśli zidentyfikowane oprogramowanie okazuje się PUP-em, może mieć ono wpływ na użytkowników, szczególnie w przypadkach, w których dotyczy ono przeciętnego użytkownika niebędącego w pełni świadomym podstawowych praktyk i środków bezpieczeństwa online.

Poniżej przedstawiono przykład wyników badania.

Strona internetowa 03	Strona internetowa 09	
Strona internetowa nakłania użytkowników do korzystania z fałszywych instalatorów gier; cały proces pozyskiwania szczególnie chronionych informacji o użytkowniku uległ zmianie pomiędzy pierwszą a drugą turą pobierania złośliwego oprogramowania. Użytkownik tego serwisu pobiera archiwum zawierające treści zamaskowane w formie plików związanych z grami, a nie wyraźnie binarny plik wykonywalny, który dowolny antywirus może rozpoznać jako złośliwy. Zaszyfrowane archiwum umożliwia dostęp tylko do nazw plików, ale nie do zawartości merytorycznej plików.	Strona internetowa oferuje dostęp do wszelkiego rodzaju treści wideo dostępnych za pośrednictwem tzw. torrent trackerów za pomocą narzędzia programowego. Narzędzie to wymaga mniejszej liczby interakcji użytkownika w porównaniu z innymi trackerami BitTorrent. Do pobrania treści z nieznanych źródeł potrzeba zaledwie kilku kliknięć, a użytkownik nie jest ani chroniony, ani nie ma kontroli nad tym, co jest pobierane.	(Android) Strona internetowa zapewnia dostęp do wielu darmowych aplikacji mobilnych bez konieczności rejestracji. Jedna aplikacja zapewnia nieograniczony dostęp do strumieniowej transmisji programów telewizyjnych i filmów. Nie ma wyraźnej prośby o podanie szczególnie chronionych informacji o użytkowniku lub szczegółów płatności za zakup dostępu do filmów chronionych prawem autorskim. Użytkownik musi jednak wyłączyć ustawienia bezpieczeństwa, co z kolei pozwoli na instalację aplikacji innych niż te pochodzące z oficjalnego rynku aplikacji.

Metodyka

W celu przeprowadzenia badania konieczne było przyjęcie solidnej metodyki dotyczącej wyboru tytułów i stron internetowych, jak również podjęcie się trudnego technicznie zadania polegającego na wykryciu i udokumentowaniu przykładów znalezionego złośliwego oprogramowania i PUP-ów. Poniżej znajduje się krótki przegląd metodyki:

1. W I fazie badania UNICRI, we współpracy z europejskim obserwatorium do spraw naruszeń praw własności intelektualnej (obserwatorium), powołano ekspercką grupę wsparcia, której zadaniem było doradzanie w zakresie metodyki badań, wyboru stron internetowych wykorzystywanych do analizy oraz oceny badań podejmowanych na każdym etapie realizacji projektu. Ekspercka grupa wsparcia składała się z przedstawicieli zainteresowanych stron obserwatorium, organizacji zrzeszających właścicieli praw, środowisk akademickich, organów ścigania oraz agencji UE.

2. Równolegle wybrano zespół badawczy. W ramach tego raportu nie było technicznie możliwe[1] przeprowadzenie badań we wszystkich państwach członkowskich UE, w związku z czym w fazie II spośród 28 państw członkowskich UE wybrano losowo 10 państw.

3. W III fazie zidentyfikowano popularne filmy, programy telewizyjne, piosenki i gry wideo. Popularność obejmowała zarówno ogólnoświatową popularność, jak i popularność zaledwie w jednym lub kilku z 10 krajów objętych próbką na początku okresu gromadzenia danych, tj. w dniu 23 czerwca 2017 r. W kolejnych fazach badania te przykładowe tytuły były systematycznie wykorzystywane w internetowych wyszukiwaniach w celu znalezienia stron

[1] Liczba wybranych krajów będzie miała bezpośredni wpływ (wzrost) na liczbę wybranych stron internetowych podejrzewanych o naruszanie praw autorskich oraz na liczbę odpowiadających tym stronom plików binarnych poddawanych analizie. W związku z tym w celu pomyślnego przeprowadzenia części praktycznej badania w określonym czasie zdecydowano się skoncentrować wyłącznie na wybranych krajach.

internetowych i aplikacji mobilnych naruszających prawa autorskie. Każdy z tytułów spełniał dwa lub więcej z poniższych kryteriów:

- cieszył się popularnością w czasie gromadzenia danych w państwach członkowskich UE;
- cieszył się popularnością w czasie gromadzenia danych w skali globalnej;
- cieszył się popularnością historycznie w skali globalnej; oraz
- został zaklasyfikowany jako film, program telewizyjny, piosenka lub gra wideo.

Wybrano pięć tytułów filmowych, pięć tytułów telewizyjnych, pięć tytułów muzycznych oraz pięć tytułów gier wideo, co dało w sumie 20 przykładowych tytułów. Zwrócono szczególną uwagę na źródła wykorzystane do określenia popularności danego tytułu, co oznaczało systematyczne przeprowadzanie procesu selekcji w celu zapewnienia dostępności danych źródłowych dla wszystkich lub większości państw członkowskich.

4. W IV fazie zidentyfikowano strony internetowe podejrzewane o udzielenie nielegalnego dostępu do materiałów chronionych prawem autorskim, które na dzień 26 czerwca 2017 r. cieszyły się popularnością na całym świecie lub w 10 wybranych krajach (pierwsza tura gromadzenia złośliwego oprogramowania). W późniejszej fazie badania strony te analizowano pod kątem obecności złośliwego oprogramowania i potencjalnie niepożądanych programów.

   Metodykę identyfikacji stron internetowych podejrzewanych o naruszanie praw autorskich opracowano przy udziale eksperckiej grupy wsparcia określonej w fazie I oraz po dokonaniu przez UNICRI przeglądu istniejącej literatury. Metodykę stworzono specjalnie w celu wygenerowania próbki stron internetowych, które:

   - cieszą się popularnością w różnych państwach członkowskich UE, zapewniając szeroki zasięg geograficzny;
   - reprezentują różne rodzaje stron internetowych podejrzewanych o naruszanie praw autorskich, w tym strony z transmisją strumieniową, strony z linkami, strony z usługami hostingowymi, strony z cyfrowymi zasobami osobistych plików (tzw. cyberlockery) oraz strony z torrentami;
   - reprezentują szeroki zakres treści podejrzewanych o naruszanie praw autorskich, w tym filmy, tytuły telewizyjne, muzykę i gry wideo; oraz
   - reprezentują strony internetowe, z którymi zetknąłby się przeciętny użytkownik internetu przy próbie uzyskania dostępu do materiałów podejrzewanych o naruszanie praw autorskich.

   Wyboru stron internetowych podejrzewanych o naruszanie praw autorskich dokonano w pięciu etapach. Pierwsze trzy etapy miały na celu zidentyfikowanie najpopularniejszych stron internetowych podejrzewanych o naruszanie praw autorskich w państwach członkowskich UE. Metoda ta imitowała scenariusze, w których przeciętny użytkownik wyszukuje strony internetowe podejrzewane o naruszanie praw autorskich bez podania np. tytułu filmu lub piosenki. Ostatnie dwa etapy miały na celu zidentyfikowanie stron internetowych podejrzewanych o naruszanie praw autorskich, na które przeciętny użytkownik może się natknąć podczas wyszukiwania sposobów na pobranie określonego popularnego tytułu bez podawania strony internetowej. Etap ten był szczególnie istotny ze względu na obecność podejrzanych złośliwych stron internetowych odpowiedzialnych za zatruwanie wyników wyszukiwania, które poprzez optymalizację dla wyszukiwarek internetowych wykorzystywały popularne w danym momencie treści. Oba podejścia obejmowały różne sposoby, w jakie przeciętny użytkownik próbuje znaleźć w internecie materiały podejrzewane o naruszanie praw autorskich.

   Nacisk położono na równoczesną analizę złośliwego oprogramowania i PUP-ów charakterystycznych dla aplikacji mobilnych na urządzeniach, takich jak smartfony i tablety, uznając je za główne zagrożenia związane z cyberprzestępczością. Analiza ograniczała się do urządzeń opartych o system Android ze względu na wskazania w istniejącej literaturze co do większej obecności złośliwego oprogramowania w sklepach z aplikacjami Android (np.

Google Play) niż w sklepie Apple iTunes. Metodykę opracowano w celu wygenerowania próbki aplikacji mobilnych, które:

- cieszą się popularnością w czasie gromadzenia danych w skali globalnej;
- reprezentują różne typy aplikacji (w tym aplikacje z transmisją strumieniową, torrentami i usługami hostingowymi);
- zawierają lub zapewniają dostęp do szerokiej gamy treści podejrzewanych o naruszanie praw autorskich (w tym filmy, tytuły telewizyjne, muzyka i gry mobilne); oraz
- przedstawiają, na co natknie się przeciętny użytkownik urządzenia mobilnego podczas próby pobrania lub korzystania z aplikacji ułatwiającej dostęp do treści prawdopodobnie chronionej prawami autorskimi.

5. Faza V polegała na pobraniu — oprócz aplikacji mobilnych — złośliwego oprogramowania i PUP-ów ze zidentyfikowanych stron internetowych w celu ich późniejszego zbadania i prawidłowego sklasyfikowania. Faza pozyskiwania danych obejmowała dwie tury pobierania i analizy złośliwego oprogramowania wykonanych latem 2017 r. W wyniku pierwszej tury pobierania złośliwego oprogramowania zebrano 1 054 unikalnych nazw domen, a druga tura doprowadziła do zebrania 1 057 unikalnych nazw domen w 10 wybranych państwach członkowskich UE. Złośliwe oprogramowanie pobrano zarówno w trybie ręcznym i automatycznym w celu stworzenia symulacji doświadczeń przeciętnego użytkownika.

Pobieranie ręczne. Metoda ta polegała na ręcznym przeglądzie domen zidentyfikowanych w poprzedniej fazie. Korzystając z ręcznego pobierania danych, ekspert był w stanie stworzyć symulację doświadczeń przeciętnego użytkownika internetu poprzez klikanie reklam oraz interakcję ze stronami internetowymi wymagającymi podpowiedzi.

Pobieranie automatyczne. W tej metodzie wykorzystano automatycznego robota internetowego zaprojektowanego przez eksperta w celu śledzenia wszystkich dostępnych linków na wskazanej stronie internetowej podejrzewanej o naruszanie praw autorskich. W pierwszej kolejności na danej stronie internetowej robot zbierał informacje pochodzące z linków na stronie głównej. W drugim etapie robot podążał za każdym z tych linków do drugorzędnych stron internetowych. W trzeciej kolejności robot podążał za każdym z tych linków do trzeciorzędnych stron internetowych. Na każdym etapie robot pobierał pliki binarne, które mogły okazać się interesujące dla późniejszej analizy ręcznej, w tym potencjalne lub podejrzane złośliwe oprogramowanie oraz potencjalnie niepożądane programy. Proces ten trwał do 1 000 linków na stronę internetową.

6. Po zebraniu plików binarnych zostały one przeanalizowane w bezpiecznym środowisku komputerowym w celu zrozumienia ich wewnętrznej funkcjonalności oraz prawidłowej ich klasyfikacji. Wstępną analizę przeprowadzono przy użyciu narzędzi open source, tak aby umożliwić zestawienie ustaleń ze sprawozdaniami dotyczącymi zagrożeń cybernetycznych. Zebrane próbki oprogramowania zostały następnie dostarczone do EMAS w celu analizy, a następnie analizę EMAS porównano ze wstępnymi wynikami.

Przegląd metodyki

Wykryte próbki złośliwego oprogramowania i PUP-ów

Na dzień 28 lipca 2017 r. w trakcie pierwszej tury pobierania danych automatycznie sprawdzono 5 240 stron internetowych (1 054 unikalnych), z których pobrano 617 odpowiednich plików (muzycznych, filmowych, plików torrentowych i oprogramowania) o łącznej objętości 47 GB. Ta niesortowana partia plików wymagała dalszej analizy w celu ustalenia, które z pobranych plików były istotne dla badania. Próbki stron internetowych naruszających prawa autorskie były podobne we wszystkich wybranych 10 krajach dla każdego z rodzajów mediów (programów telewizyjnych, filmów, muzyki i gier wideo). W rezultacie spośród krajów objętych próbką losowo wybrano Belgię, a wszystkie strony internetowe określone jako naruszające prawa autorskie w Belgii zweryfikowano ręcznie pod kątem obecności złośliwego lub w inny sposób niepożądanego oprogramowania. W dniu 10 sierpnia 2017 r., po drugiej turze, automatycznie pobrano 3 665 plików ze stron internetowych we wszystkich krajach o łącznej objętości 167 GB. Łączna liczba unikalnych adresów URL wyodrębnionych dla wszystkich krajów wyniosła 1 057 z 5 606 stron internetowych, co uniemożliwiło ich ręczną weryfikację.

Po wstępnej analizie zebranych plików, w wyniku obu tur pobierania złośliwego oprogramowania, wyodrębniono 106 unikalnych plików binarnych dla systemów MS Windows, Android i Mac OS. W pierwszej turze wybrano 41 plików, a w drugiej 65 — a dokładnie: 2 dla systemu Mac, 15 dla systemu Android i 89 dla systemu MS Windows. Spośród tych plików 21 można uznać za dobrze znane złośliwe programy, które wielu dostawców antywirusów wskazuje jako dodane przez platformę VirusTotal. Należą do nich pliki pobierane bezpośrednio z wybranych stron internetowych podejrzewanych o naruszanie praw autorskich, a także pliki powstałe w trakcie uruchamiania pobranych plików. Następnie zebrane próbki oprogramowania przeanalizowano w środowisku tzw. piaskownicy (ang. sandbox) i dostarczono do EMAS w celu przeprowadzenia bardziej zaawansowanej analizy możliwych złośliwych działań. W sumie w czterech raportach EMAS (Windows 7 SP1, 64-bitowy Windows 7 SP1, 64-bitowy Windows 10, Windows XP SP3)

wykryto 821 odrębnych złośliwych zdarzeń dla wszystkich plików binarnych. Niektóre raporty nie zawierały żadnych podejrzanych działań, a niektóre z nich zawierały nawet 10 znanych wcześniej złośliwych działań. W końcowej fazie badania zestawiono wyniki wstępnej analizy z raportami EMAS. Ilościowe podsumowanie wyników przedstawiono w poniższej tabeli.

	Tura 1	Tura 2
Data	28 lipca 2017 r.	10 sierpnia 2017 r.
Odkryte strony internetowe w 10 krajach UE	5 240	5 606
Unikalne strony internetowe	1 054	1 057
Odpowiednie pliki	617	3 665[2]
Całkowity rozmiar plików w GB	47	167
Dostarczone do EMAS		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Całkowity rozmiar, bajty	175 600 117	522 991 095

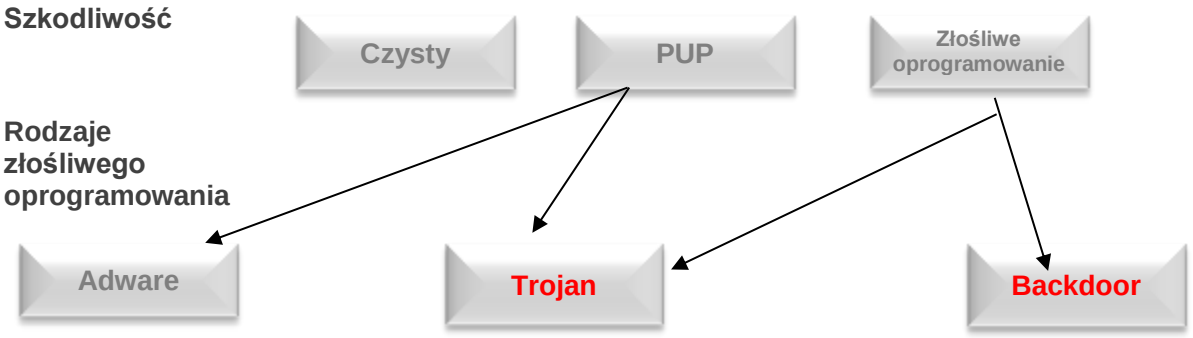
Rozwiązanie do analizy złośliwego oprogramowania stworzone przez Europol (EMAS)

Rozwiązanie do analizy złośliwego oprogramowania stworzone przez Europol (EMAS) jest dynamicznym, zautomatyzowanym rozwiązaniem do analizy złośliwego oprogramowania dostarczanym państwom członkowskim UE przez Europol. EMAS oferuje możliwość tworzenia raportów analitycznych, jednak jego najbardziej rewolucyjną cechą jest tworzenie danych wywiadowczych dla policjantów służb dochodzeniowych. Zautomatyzowane kontrole krzyżowe mogą wykazać powiązania między atakami dokonywanymi w różnych krajach z wykorzystaniem tego samego złośliwego oprogramowania lub tej samej rodziny złośliwego oprogramowania używanej przez tę samą organizację przestępczą, które łączą te same domeny i są powiązane z różnymi dochodzeniami w UE lub poza jej granicami. W 2015 r. EMAS stał się w pełni zautomatyzowany, aby umożliwić bezpośredni dostęp do organów ścigania, z którymi Europol zawarł porozumienia operacyjne. W 2015 r.: w EMAS przeanalizowano 525 108 plików, z czego 356 863 zidentyfikowano jako złośliwe.

Jak pokazano na poniższym schemacie, zebrane pliki binarne można generalnie sklasyfikować według szkodliwości jako łagodne (pliki, które nie wyrządzają żadnej szkody), PUP-y i szkodliwe złośliwe oprogramowanie. Co więcej, PUP-y zostały odkryte nie tylko dla systemu Microsoft Windows, ale także dla systemu Android i Mac OS, co sugeruje, że twórcy złośliwego oprogramowania próbują wpłynąć na jak największą liczbę użytkowników, korzystając z różnych platform. PUP-y i złośliwe oprogramowanie można dodatkowo rozróżnić w zależności od głównych typów złośliwego oprogramowania, tj. trojana, adware'a i backdoora. Większość znalezionego oprogramowania należała do kategorii PUP. Funkcjonowanie PUP-ów można powiązać z jednym z następujących modeli biznesowych: fałszywy instalator gier wymagający podania danych osobowych i danych konta bankowego, pobranie „użytecznych" programów, które zmuszają użytkowników do zakupu abonamentu na płatną wersję, czy też instalacja darmowych programów

[2] W celu wyjaśnienia różnicy w liczbach pochodzących z tury 1 i tury 2 należy podkreślić, że podczas tury 2 automatycznego pobierania istniały strony internetowe, które publikowały wiele zestawów plików na każdej ze swoich stron internetowych.

w celu uzyskania dostępu do platform naruszających prawa autorskie. Aplikacje te mogą stanowić zagrożenie dla danych osobowych użytkowników i konfiguracji komputera. Dzięki sztuczkom inżynierii społecznej można również ujawniać różnego rodzaju dane prywatne, takie jak dane kart płatniczych, dane osobowe i dane uwierzytelniające kont w mediach społecznościowych. W podobny sposób w badaniu zidentyfikowano 15 aplikacji Android pochodzących z rynków aplikacji innych firm, a po wstępnej analizie stwierdzono, że takie aplikacje mogą być zaangażowane w dystrybucję treści naruszających prawa autorskie oraz w ujawnianie danych osobowych.



Zagrożenia dla użytkowników końcowych

Podczas dwóch tur identyfikacji stron internetowych i analizy złośliwego oprogramowania nie znaleziono żadnego binarnego oprogramowania typu ransomware. Ogólnie większość pobranego złośliwego oprogramowania można określić jako trojany, co oznacza, że może być ono przedstawiane na stronach internetowych jako łagodne, powszechnie używane lub popularne oprogramowanie, podczas gdy w rzeczywistości jest ono w stanie wykradać lub ujawniać informacje prywatne. Niedoświadczony użytkownik może mieć wysokie zaufanie do oprogramowania i może przeoczyć nieprawidłowości. Ponadto analiza statyczna i dynamiczne obserwacje behawioralne takiego oprogramowania mogą nie ujawnić pełnej funkcjonalności bez posiadania kodu źródłowego. Po wstępnej analizie złośliwego oprogramowania analiza EMAS wykazała bardziej konkretne złośliwe działania. Zainstalowanie takiego oprogramowania może mieć znaczny wpływ na komputer użytkownika końcowego, powodując nie tylko straty finansowe, ale również kradzież danych osobowych i inne zagrożenia związane z niepożądanymi dostępem i kontrolą. W wyniku tych działań dane osobowe mogą być gromadzone i przekazywane osobom trzecim w zaszyfrowanym lub otwartym formacie tekstowym. Takie dane mogą obejmować na przykład dane uwierzytelniające konta bankowego z przeglądarki, szczegóły konfiguracji sprzętu komputerowego/oprogramowania lub zasadniczo wszystko to, co zostało wpisane na klawiaturze.

IDENTYFIKACJA I ANALIZA ZŁOŚLIWEGO OPROGRAMOWANIA NA WYBRANYCH STRONACH INTERNETOWYCH PODEJRZEWANYCH O NARUSZANIE PRAW AUTORSKICH

STRESZCZENIE

Wrzesień 2018 r.