Zagrożenia w Policji wynikające z uruchomienia niezidentyfikowanych plików

MALWARE

kom. Sławomir Sobolewski
Wydział Ochrony Systemów Informatycznych
Biuro Łączności i Informatyki
Komenda Główna Policji

podkom. Kamil Jurczyk
Wydział Ochrony Systemów Informatycznych
Biuro Łączności i Informatyki
Komenda Główna Policji

Współczesny policjant, niezależnie od rodzaju wykonywanych zadań, korzysta na co dzień z systemów teleinformatycznych Policji. Niniejszy artykuł ma na celu zwrócenie uwagi na kilka kluczowych elementów przekładających się na bezpieczeństwo użytkowników policyjnych sieci teleinformatycznych.

Policja jako jedna z formacji podlegających MSWiA realizuje swoje zadania na podstawie ustawy o Policji[1]. Codzienna służba policjantów jest trudna oraz wymaga ogromnego poświęcenia w różnych aspektach. Do tych aspektów możemy zaliczyć specyfikę zadań realizowanych przez funkcjonariuszy prewencji, ruchu drogowego, kryminalnych, walczących z przestępczością gospodarczą, techniki operacyjnej, szkół Policji oraz pozostałych. Mocno zróżnicowane zadania przekładają się na wysoki poziom podziału kompetencji pomiędzy funkcjonariuszami. Służba polegająca na patrolach pieszych i zmotoryzowanych, udziale w zabezpieczeniach, prowadzeniu dochodzeń w sprawach przestępstw i wykroczeń czy analizie danych zebranych przy użyciu sprzętu technicznego wymaga w obecnych czasach dostępu do systemów teleinformatycznych Policji. Najważniejsze systemy przetwarzające dane przechowywane są w ramach redundantnych ośrodków przetwarzania danych, obsługiwanych przez Biuro Łączności i Informatyki Komendy Głównej Policji. Celem istnienia Biura jest m.in. wspomaganie funkcjonowania oraz cyfryzacja określonych obszarów znajdujących się w naszej formacji. Same działania są ukierunkowane na daleko idące usprawnienia oraz innowacje technologiczne. Zdecydowana większość zadań Biura Łączności i Informatyki KGP odbywa się poza zasięgiem poszczególnych jednostek, a proces udostępniania usług jest w pełni przezroczysty dla ich odbiorców.

W zależności od rodzaju realizowanych zadań do podstawowych policyjnych sieci zalicza się Policyjną Sieć Transmisji Danych (PSTD) oraz Centralny Węzeł Internetu (CWI). Każda z wymienionych sieci posiada swoje zastosowanie. Zależy to od rodzaju przetwarzanych danych oraz udostępnianych narzędzi, które są wykorzystywane w służbie. Do głównych różnic należy zaliczyć stopień otwartości na publiczną sieć Internet. Sieć PSTD jest z założenia zamknięta, co sprawia, że przetwarzanie danych odbywa się bez dostępu do sieci Internet. Techniczne uwarunkowania mają za zadanie zminimalizować możliwe próby przeprowadzenia bezpośredniego, bezprawnego ataku na urządzenia, systemy, aplikacje oraz dane znajdujące się wewnątrz naszej formacji. Do tych danych należy zaliczyć przede wszystkim dane osobowe, szczegóły dotyczące prowadzonych śledztw, wykroczeń drogowych, dokumenty służbowe i wiele innych. Ponadto prowadzona jest wymiana danych z innymi służbami krajowymi (np. Strażą Graniczną), w tym służbami specjalnymi oraz międzynarodowymi, jak np. Europol i Interpol. Sieć PSTD zawiera wiele systemów i aplikacji, które są krytyczne dla sprawnego funkcjonowania naszej formacji,

jak np. KSIP, SWD, SWOP itp. Z drugiej strony – część istotnych informacji możliwa jest do uzyskania wyłącznie z sieci Internet. Dlatego też obecnie rolę „pośrednika" pełni sieć CWI. Z uwagi na skalę działań oraz wagę przetwarzanych informacji zdecydowano o wykorzystywaniu niezależnych i oddzielnych stanowisk komputerowych dla każdej z tych sieci.

Podstawową i najważniejszą siecią policyjną jest zamknięta sieć PSTD, która daje możliwość między innymi sprawdzenia w trakcie legitymowania (za pośrednictwem stacji komputerowych oraz mobilnych terminali noszonych), czy wprowadzone dane należą do osoby poszukiwanej. Możliwość uzyskania nieautoryzowanego dostępu do centralnych zasobów sieci PSTD mogłaby prowadzić do odczytu, modyfikacji lub usunięcia informacji decydujących o postępowaniu lub śledztwie. Są to kluczowe informacje z punktu widzenia nie tylko Policji, ale również całego państwa. Dlatego też kwestie bezpieczeństwa, a dokładniej mówiąc cyberbezpieczeństwa, wewnątrz naszej formacji stanowią ważny element, który ma wpływ na bezpieczne i dobre funkcjonowanie państwa prawa.

Komórką kształtującą oraz odgrywającą wiodącą rolę związaną z szeroko rozumianym cyberbezpieczeństwem w sieci PSTD jest Wydział Ochrony Systemów Informatycznych, znajdujący się w Biurze Łączności i Informatyki Komendy Głównej Policji. Wydział ten odpowiada między innymi za dostęp do centralnych zasobów, autoryzację użytkowników oraz bezpieczne przetwarzanie danych, z wykorzystaniem najnowszych technologii (w tym projektowanie infrastruktury teleinformatycznej). Istotnym elementem zabezpieczania połączenia jest zestawianie tuneli kryptograficznych i wymiana danych z innymi podmiotami odgrywającymi ważne role w strukturach państwa. Jednocześnie należy zauważyć, że niezależnie od prowadzonych działań inżynieryjnych, rozwiązań technologicznych oraz kampanii informacyjnych, również użytkownik jest odpowiedzialny za bezpieczeństwo danych, z których korzysta. Poniżej zostaną omówione podstawowe, stosowane przez cyberprzestępców oraz twórców szkodliwego oprogramowania, techniki ataku na stacje końcowe.

Jedną z podstawowych technik wykorzystywanych przez cyberprzestępców wobec użytkowników każdej sieci jest użycie szkodliwego oprogramowania (malware) do przeprowadzania infekcji na stacjach końcowych (należących do ich użytkowników). Jest to zazwyczaj pierwszy krok i nazywany jest „kampanią malware". Kampanie mają swoje cele i kierunki ataków, np. państwa, regiony, konkretne firmy lub instytucje. Głównym celem kampanii jest uruchomienie w systemie operacyjnym szkodliwego pliku i umożliwienie infekcji, która może prowadzić do np. eskalacji uprawnień, szyfrowania danych lub wykorzystania systemu jako botnet. Cyberprzestępcy wykorzystują wiele technik, aby nakłonić użytkownika do uruchomienia pliku na jego komputerze.

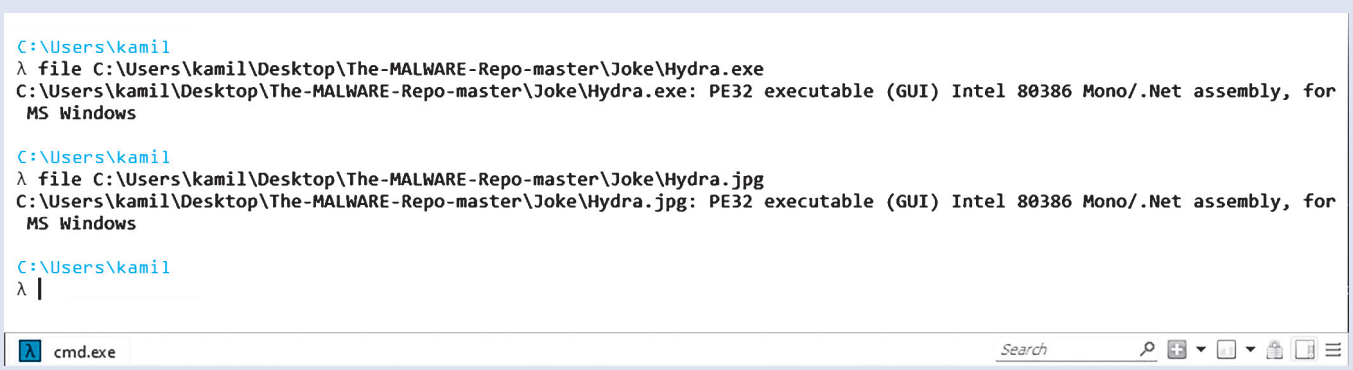
Pierwsza z omawianych technik polega na ukryciu pliku wykonywalnego .exe (ang. *executable*) w innym rozszerzeniu, co może minimalizować czujność użytkownika, np. fotografia .jpg (ang. *Joint Photographic Experts Group*) zamiast fotografia.exe. Technika ta jest prosta w wykonaniu i może dotyczyć również innych rozszerzeń (doc, pdf, xml itp.). Analiza wymaga podstawowego wglądu w strukturę binarną samego pliku.

Zrzut ekranu znajdujący się poniżej (rys. 1) przedstawia jeden i ten sam plik malware pod nazwą „Hydra" zawierający szkodliwe oprogramowanie, zapisany w dwóch różnych formatach .exe oraz .jpg. Pomimo iż sam system operacyjny wyświetla każdy z tych plików z innym rozszerzeniem, to podstawowa analiza wskazuje, że mamy do czynienia z programem graficznym (GUI) przygotowanym na platformę MS Windows w formacie PE32 (ang. *Portable Executable*).

Dodatkowo, pewność w ręcznej analizie co do faktycznego rozszerzenia dają nam tak zwane ang. *magic number* znajdujące się wewnątrz pliku. To za ich sprawą system interpretuje zachowanie pliku i podejmuje decyzję, jakie narzędzie będzie w stanie go obsłużyć (np. plik muzyczny = Windows Media Player). Dla każdego pliku wykonywalnego „magicznymi numerami" będą *4D 5A*, które w łańcuchach znaków posiadają oznaczenie *MZ*.

Kolejnym elementem jest sama informacja *This program cannot be run in DOS mode*, która oznacza brak możliwości uruchomienia pliku w trybie DOS. Jest to element pozostałości z przeszłości. Nagłówek *MZ* został zachowany dla zgodności wstecznej, co pozwala starszym systemom DOS rozpoznać plik jako wykonywalny.

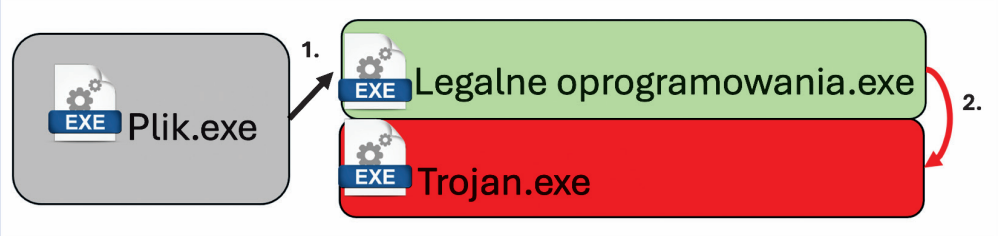
Kolejną próbą ukrycia malware może być technika wykorzystywana w tzw. trojanach, czyli plikach udających prawdziwe, „legalne" oprogramowanie. Pliki te charakteryzują się zazwyczaj dwutorowym działaniem. Jedną ze ścieżek może być faktyczne uruchomienie np. instalatora programu ALLPlayer.exe, jednocześnie drugą ścieżką



Ryc. 1. Porównanie pliku wykonywalnego .exe ze sfabrykowanym plikiem .jpg.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Tekst zdekodowany
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00	.....È...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..º..´.Í!¸.LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.....
00000080	AD	31	38	81	E9	50	56	D2	E9	50	56	D2	E9	50	56	D2	.18.éPVÒéPVÒéPVÒ
00000090	2A	5F	09	D2	EB	50	56	D2	E9	50	57	D2	4D	50	56	D2	*_.ÒëPVÒéPWÒMPVÒ

Ryc. 2. „Magiczne numery” pliku wykonywalnego.

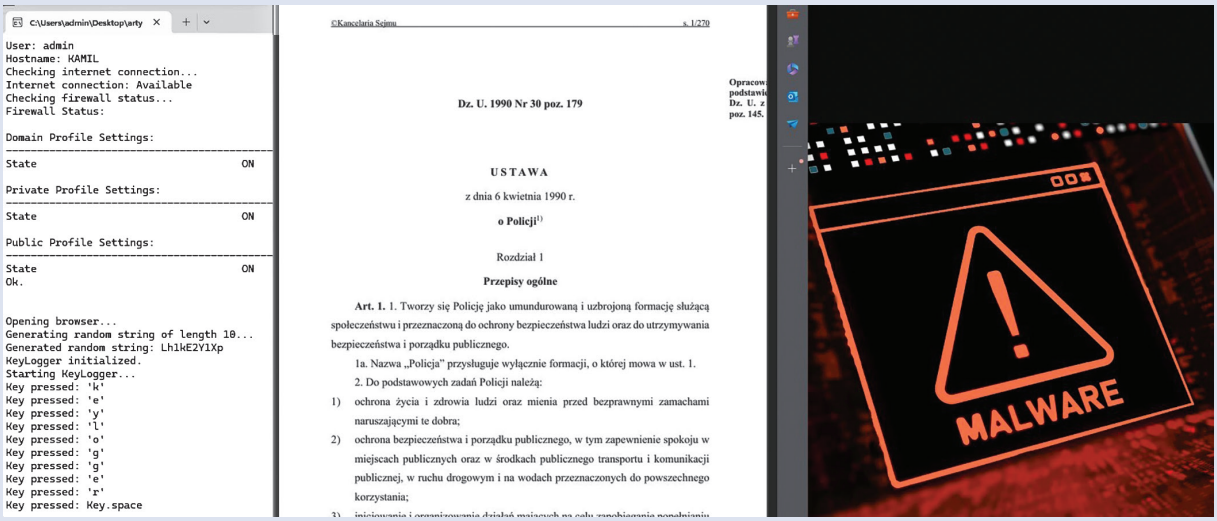


Ryc. 3. Jeden z wariantów uruchomienia zainfekowanego pliku trojan.

może być uruchomienie kawałka szkodliwego kodu wymierzonego w użytkowników i ich systemy.
Cała procedura zapewnia pełne ukrycie obecności oraz działania szkodliwego oprogramowania. Skutkiem takiej infekcji może być uzyskanie dostępu do danych, przejęcie kontroli nad systemem operacyjnym, zakłócenie działania systemu (spowolnienie, błędy, awarie) oraz wiele innych. W trakcie niskopoziomowej analizy można zwrócić uwagę na elementy związane z tworzeniem nowych procesów w systemie operacyjnym, uruchomianiem innych programów, otwieraniem plików lub nazw URL. Jednym z działań może być zapisywanie danych w przestrzeni adresowej innego procesu, co często zdarza się we „wstrzykiwaniu” złośliwego kodu. Ponadto wykorzystuje się tzw. instalacje haków (ang. *hooks*) za sprawą funkcji *SetWindowsHookEx* do przechwytywania i monitorowania wiadomości pochodzących z systemu operacyjnego.
W celu zapewnienia ciągłości działania szkodliwego oprogramowania w systemie operacyjnym po jego kontrolowanym lub niekontrolowanym zamknięciu stosuje się specjalne modyfikacje systemu. Zazwyczaj odpowiada za to właściwy wpis w rejestrze systemu Windows. Modyfikacja odbywa się za sprawą otwarcia klucza rejestru (*RegOpenKeyEx*) z uprawnieniami do zapisu (*KEY_WRITE*). Proces konfiguracji rejestru (*RegSetValueEx*) polega na wykorzystaniu nazwy oraz ścieżki do złośliwego kodu malware (MyTrojan). Działanie to zapewnia automatyczne uruchamianie przy każdym starcie systemu Windows szkodliwego oprogramowania (zapewniając trwałość i unikanie wykrycia).
Odpowiedzią na pytanie, dlaczego użytkownik zazwyczaj nie widzi wszystkich modyfikacji w swoim systemie, jak np. uruchomionego Wiersza Polecenia lub PowerShell, jest fakt wykorzystania kolejnej techniki ukrywania. Za pomocą dodatkowych modyfikacji w funkcji wShowWindow (*=SW_HIDE*) oraz nShow (*=SW_HIDE*) użytkownikowi nie „wyskakują” okienka na poziomie GUI (wszystko wykonuje się w tle).
W celu zobrazowania potencjalnych działań pliku malware na stacji użytkownika w środowisku laboratoryjnym przygotowano próbkę testową (bez funkcji ukrywania) symulującą szkodliwe oprogramowanie. Utworzony program posiada podstawowe funkcjonalności inwigilujące (keylogger).
Po uruchomieniu pliku użytkownik w pierwszej kolejności otrzymuje widok okna realizującego wyświetlenie pliku ustawa.pdf (to, czego użytkownik oczekiwał). Następnie uruchamiany jest kolejny moduł (to, czego użytkownik nie oczekuje) wyświetlający informacje o systemie i zalogowanym użytkowniku oraz sprawdzane jest połączenie z siecią Internet. To właśnie za sprawą dostępu do sieci Internet pobierane są kolejne wersje szkodliwego oprogramowania (i aktualizowane jego

```
void InstallTrojan() {
    char szPath[MAX_PATH];
    GetModuleFileName(NULL, szPath, MAX_PATH);
    HKEY hKey;
    RegOpenKeyEx(HKEY_CURRENT_USER, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", 0, KEY_WRITE, &hKey);
    RegSetValueEx(hKey, "MyTrojan", 0, REG_SZ, (const BYTE*)szPath, strlen(szPath) + 1);
    RegCloseKey(hKey);
```

Ryc. 4. Pseudokod odpowiadający za wprowadzenie zmian w rejestrze systemu Windows.



Ryc. 5. Uruchomiony keylogger w systemie bez funkcji ukrywania.

funkcjonalności) lub przesyłane są dane zainfekowanej stacji użytkownika na serwer cyberprzestępcy. Przy wykorzystaniu luki w oprogramowaniu możliwe jest dostosowanie ustawień zapory systemu (wyłączenie zapory). Nasza próbka zawiera wyłącznie funkcję sprawdzenia, czy wszystkie elementy zapory są obecnie aktywne. Kolejnym etapem działania jest uruchomienie przeglądarki internetowej i wyświetlenie informacji o zainfekowaniu. Zazwyczaj informacja o zainfekowaniu jest starannie ukrywana przed użytkownikiem. Ostatnim z etapów jest uruchomienie modułu keyloggera, który zbiera i zapisuje do pliku *.txt aktywność użytkownika systemu Windows. Te informacje łatwo mogą zostać przesłane do dowolnego miejsca na świecie.

Podsumowanie

Każdy z użytkowników ma wpływ, pośrednio i bezpośrednio, na bezpieczeństwo danych w policyjnych sieciach teleinformatycznych. Zaleca się, aby stacje robocze były wykorzystywane zgodnie z ich przeznaczeniem i polityką bezpieczeństwa. Odradza się pobierania i instalacji oprogramowania z niezidentyfikowanych źródeł. Zaleca się ostrożność w otwieraniu załączników lub linków od nieznajomych nadawców. Wymaga się, aby każda ze stacji służbowych miała uruchomioną zaporę systemową i zainstalowany policyjny system antywirusowy. Ponadto skonfigurowane do pracy stacje robocze nie mogą być celowo modyfikowane w nieuprawniony sposób do własnych celów użytkownika (własna reinstalacja lub konfiguracja systemu). Zabrania się przepinania stacji roboczych lub innych urządzeń służbowych pomiędzy siecią PSTD i CWI.
Pamiętajmy, że cyberbezpieczeństwo formacji to również nasze bezpieczeństwo. Wszyscy jesteśmy za nie odpowiedzialni.

[1] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145).

Bibliografia:

Fortinet, *What Is A Keylogger? Definition and Types*, https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers [dostęp: 17 czerwca 2024 r.].
McGowan E., *Trojan viruses: Detecting and removing*, https://us.norton.com/blog/malware/what-is-a-trojan [dostęp: 17 czerwca 2024 r.].
Microsoft, *RegOpenKeyExA function (winreg.h)*, https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regopenkeyexa [dostęp: 17 czerwca 2024 r.].
Microsoft, *SetWindowsHookExA function (winuser.h)*, https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-setwindowshookexa [dostęp: 17 czerwca 2024 r.].
Microsoft, *ShowWindow function (winuser.h)*, https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-showwindow [dostęp: 17 czerwca 2024 r.].
Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145).
Wikipedia, *DOS MZ executable*, https://en.wikipedia.org/wiki/DOS_MZ_executable [dostęp: 17 czerwca 2024 r.].

Summary

Threats in the Police resulting from running unidentified files (malware)

The Polish Police performs almost all of its tasks based on ICT systems, which are located in an internal network structure called the Police Data Transmission Network (Policyjna Sieć Transmisji Danych). Personal data and other information must be well guarded by both hardware, software and the human factor, which can be provided in this case through the education process. This article will describe the basic techniques that enable cyber criminals to get a user to run malware. The goal is to raise awareness among police officers and employees about cyber security threats caused by social engineering and other factors.

Tłumaczenie: autorzy