Keyloggery — jak działają i jak się przed nimi bronić?

Kamil Breczko

kamil.breczko@gmail.com

1 Keylogger - Czym jest?

Keylogger jest to rodzaj oprogramowania lub urządzenia, którego głównym działaniem jest rejestrowanie klawiszy naciskanych przez użytkownika. Keylogger najczęściej przebywa pomiędzy klawiaturą a systemem operacyjnym, przechwytując klawisze w ukryciu, aby osoba, która korzysta aktualnie z klawiatury nie była świadoma, że jest monitorowana. Istnieje wiele różnych rodzajów keyloggerów opartych na różnych metodach. Należą do nich keyloggery sprzętowe i programowe. Obecnie istnieją bardziej zaawansowane programy monitorujące urządzania, posiadające funkcje: pobieranie informacji o aktywnych programach, wysyłanie zebranych danych poprzez e-mail, zapisywanie zawartości schowka czy też przechwytywanie dzwięku z mikrofonu, aparatu i co najgorsze z ekranu. W tym artykule poznamy szczegóły jak działają tego typu metody oraz odpowiemy sobie na pytanie, czy da się zabezpieczyć przed keyloggerem oraz czy wszystkie keyloggery są szkodliwym oprogramowaniem?

2 Legalne użycie keyloggera

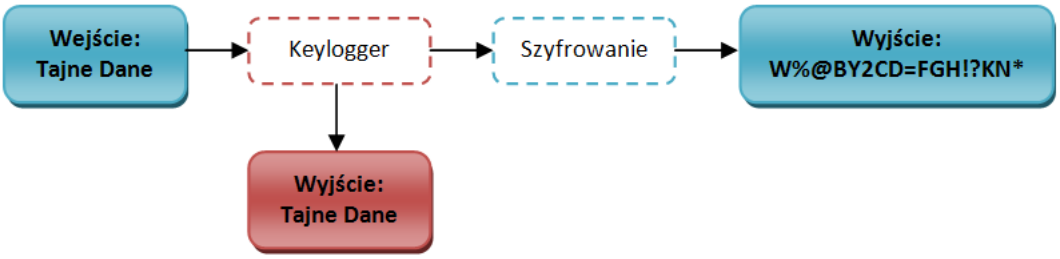
Użytkownicy korzystający z oprogramowania Windows 10 przy ustawieniach domyślnych są monitorowani. Microsoft włącza ustawienia do rejestrowania i śledzenia każdego słowa, które jest wpisywane na klawiaturze lub ekranie dotykowym, a następnie zebrane dane okresowo wysyła na swoje serwery. Jak pisze firma, to nie jest keylogger rozumiany jako złośliwe oprogramowanie, ale zbiór danych do tworzenia bazy użytkowników, w celu dopasowania reklam. Co jeśli użytkownik nie chce reklam? Microsoft w Windows 10 umożliwia wyłączenie tej opcji w menu ustawień. [**?**]

Czy po wyłączeniu podanej opcji mamy pewność, że Microsoft nie zbiera danych bez wiedzy użytkownika? A co z wbudowanymi aparatami lub mikrofonami? To nie jest pierwszy przypadek, kiedy firma Microsoft narusza prywatność użytkowników. W takim razie, w jakim celu Windows 10 podsłuchuje użytkowników i gdzie te dane zostaną użyte? [**?**]

Keyloggery są różnież używane przez organy ściagania. Najgłośniejszym przypadkiem było wykorzystanie keyloggera przez FBI w 1999 roku, który przyczynił się do ujęcia szefa mafii z Filadelfii Nicodemo Scarfo Juniora. Początkowo agenci FBI mieli problem z schwytaniem gangstera i przechwyceniem jego wiadomości, ponieważ korzystał z PGP (Pretty Good Privacy), a to oznacza, żeby odczytać treść wiadomości trzeba posiadać klucz odszyfrujący. Kryptografia komputerowa osiągnęła poziom, w którym jest praktycznie nie do złamania. Jedynym wyjściem było użycie keyloggera, ponieważ przechwytuje dane wejściowe, a nie dane wyjściowe komputera.

W styczniu 1999r FBI otrzymało nakaz przeszukania domu i zainstalowano keylogger na komputerze Scarfo. Agenci FBI używając keyloggera już byli w stanie przedstawić dowody,

Instytut Informatyki Uniwersytetu Wrocławskiego, 2017–2018
Esej przygotowany w ramach zajęć *Kultura bezpieczeństwa komputerowego*



Rysunek 1: Keylogger a szyfrowanie danych

które pozwoliły na oskarżenie Scarfo w czerwcu 2000 roku. [?]

W większości twórcy keyloggerów sprzedają swoje produkty jako legalne oprogromowanie. Rejestratory mogą mieć wiele pozytywnych działań, takich jak nadzór rodzicielski czy też odzyskiwanie danych osobowych i haseł. Tego rodzaju metody używane są także przez pracodawców do monitorowania działania komputera pracowników. Ale, czy używanie takich oprogramować są zgodne z prawem? Według art. 267 § 1 ustawy z dnia 2 sierpnia 1997 r. kodeksu karnego (Dz.U. 1998 nr 21 poz. 94 -tekst jednolity) osoba, która zamierza podsłuchiwać wpisywane znaki na komputerze powinna poinformować użytkownika i otrzymać zgode na założenie keyloggera. W przypadku monitorowania działań komputera bez zgody użytkownika jest karalne. *"Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2."*

3 Keylogger programowy

Keylogger programowy może działać na różnych poziomach w systemie operacyjnym komputera. Najczęśniej dzieli się na: metody trybu użytkownika i metody trybu jądra.

Metoda oparta na trybie użytkownika jest najłatwiejszą metodą do przechwytywania wciśniętych klawiszy. Tym samym jest podatny na ujawnienie się i wykrycie przez antywirus. Polega na przechwytywaniu interfejsu API klawiatury w oprogramowaniu, nastepnie współdziałaniu z nim oraz rejestrowaniu naciśniętych klawiszy. Przykładowo w systemie Windows, najczęściej stosowaną techniką w keyloggerach jest użycie systemu hook, który przechowywuje powiadomienia o naciśnięciu klawiszy. Atak polega na użyciu funkcji API *SetWindowsHookEx*, ustawiając globalny uchwyt dla wszystkich zdarzeń klawiatury w wszystkich wątkach, w taki sposób, że każde naciśnięcie klawisza zostanie przechwycone przez keylogger. Inną dość powszechną metodą jest okresowe sprawdzenie stanu klawiatury, używając funkcji WinAPI, takich jak *GetAsyncnKeyState* i *GetKeyState*. Atak polega na analizowaniu otrzymanej przez podane funkcje tablicy z stanem wszystkich klawiszy. [?]

Metoda oparta na trybie jądra w porównaniu do metody trybu użytkownika jest bardziej zaawansowana. Polega na uzyskaniu dostępu administratora do ukrycia się w systemie operacyjnym i przechwytywaniu naciśniętych klawiszy przechodzące przez jądro. Keyloggery pracujące w tym trybie, mogą być praktycznie nie do wykrycia. Obecnie szkodliwe oprogramowanie z funkcją keyloggera są implementowane z wykorzsytaniem technologii rootkit, aby unikąć wykrycia ręcznego lub przez antywirus. Po uzyskaniu dostępu do sprzętu, może działać jako sterownik klawiatury przechwytując wszystkie wpisywane znaki na klawiaturze. Przykładowo w systemie Windows, powszechną metodą jest korzystanie z sterownika filtra funkcjonalnego i8042prt oraz

sterownika klawiatury Kbdclass, który jest sterownikiem filtru wysokiego poziomu. Atak z użyciem powyższych sterowników polega na przechwytywaniu żądania klawiatur, instalując filtr nad odpowiednim urządzeniem stworzonym przez sterownik. Aktualnie coraz rządziej używa się i8042prt w keyloggerach, ponieważ kontroluje tylko klawiatury z wejściem typu PS/2. [**?**]

Innym rodzajem keyloggera programowego mający dużą popularność jest motoda wstrzykiwania skryptu napisanego w języku *javascript* na strony www lub pdf. Technika polega na wprowadzeniu funkcji na stronie, która nadsłuchuje wciśnięte klawisze oraz wysyła dane na zewnątrz. Przykładowy kod napisany w języku *javascript*, służący do wyświetlenia na ekranie wpisywanych znaków z klawiatury:

```
document.addEventListener('keypress', function(e)
    alert(e.keyCode);
);
```

Przykładem, w którym użyto keyloggera programowego i przestrogą, gdzie powinniśmy zabezpieczać się przed keyloggerami jest przypadek Joe Lopeza, który został okradziony z sumy wysokosci 90,348 $. *"Do zdarzenia doszło 6 kwietnia 2005 roku, gdzie ofiara odkryła nieautoryzowany przelew."* Za oszustwem stał trojan zwany coreflood, który został później wykryty przez tajne służny amerykańskie. Coreflood posiada funkcje keyloggera i poprzez internet wysyła zebrane informacje użytkownikom. Lopez często wykorzystywał internet do zarządzania swoim kontem w Bank of America, *" obecnie przestał używać przelewów bankowych"*.

Głównymi środkami zaradczym przed keyloggerami typu programowego są antywirusy i anty-keyloggery. Każde z nich są w stanie wykryć zainstalowanego keyloggera, ale tylko typu programowanego. Pierwszy z nich wykrywa w oparciu o heurystyke oraz wzorce w wykonywalnym kodzie. Antywirusy także analizują miejsca w systemie podatne na atak, przykładem jest system hook. Zaś anty-keyloggery szukają podobieństwa porównując wszystkie pliki w komputerze z bazą danych keyloggerów. Obie metody nie dają nam całkowitego bezpieczeństwa, ponieważ mogą wykryć co najwyżej szkodliwe oprogramowania z trybu użytkownika. Za najbezpieczniejszy środek zaradczy przed keyloggerami programowymi uważa się uruchomienie komputera przy użyciu Live CD, czystego od wirusów. [**?**]

Innym środkiem zabezpieczającym przed przechwyceniem danych przez keylogger programowy jest stosowanie monitorów sieciowych analizujące połączenia sieciowe. Podana metoda wymaga od użytkownika ciągłego wglądu na stan połączenia, a w przypadku każdej próby wysłania danych użytkownik zostaje poinformowany o zdarzeniu.

Popularnym i wprowadzającym dodatkowe zabezpieczenie przy logowaniu na stronę internetową, nie tylko przed keyloggerami programowymi, a także sprzętowymi jest użycie weryfikacji dwuetapowej lub hasła jednorazowego. Taka technika pozwala na zabezpieczeniu profilu na stronie przed przejęciem kontroli przez nieuprawnioną osobę. Podana metoda polega na wprowadzeniu do formularza dodatkowego hasła, które należy wcześniej wygenerować. Wygenerowane hasło jest jednorazowe i ważne przez krótki odstęp czasu, najczęściej przez 15s. Do generowania hasła jednorazowego zalecane jest użycie urządzenia zewnętrznego. Przykładowym urządzeniem może być smartfon z aplikacją do generowania kodów. Jeśli komputer ofiary znajduję się pod zdalną kontrolą jest możlwiość wykorzystania aktywnej sesji w celu kradzieży danych.

4 Keylogger sprzętowy

Keyloggery sprzętowe są rządziej używane, ze względu na fizyczne zamontowanie urzadzenia przy komputerze. Większość keyloggerów sprzętowych służy jako złącze lub przejściówka między klawiaturą komputera i komputerem, ale istnieją także urządzenia które przyjmują postać modułu zainstalowanego wewnątrz klawiatury. Tego typu keyloggery mogą przechowywać zebrane dane w swojej pamięci lub wysyłać drogą radiową. W pierwszym przypadku osoba, musi fizycznie zainstalować i usunąć keyloggera, aby uzyskać zebrane informacje, zaś w przypadku

drugim istnieją specjalne urządzenia, które mogą przechwycić wysyłane pakiety narażając osobe, która podłączyła keylogger na ujawnienie. Sposobem sprawdzającym się w klawiaturach bezprzewodowych są bezprzewodowe sniffery typu keylogger [**?**], które mogą przechwycić dane wysyłane między klawiaturą a komputerem. Oprócz przechwytywania danych, za pomocą sniffera atakujący jest w stanie wprowadzić dane do komputera co zwiększa zagrożenie. Innym rodzajem keyloggerem sprzętowym są nakładki na klawiaturę, które są najczęściej stosowane do przechwytywania kodu PIN w bankomatach.

Do rzadziej stosowanych sposobów, można zaklasyfikować kryptoanalize akustyczną i czujniki smatfonów. Na podstawie wykonanych próbek dźwiękowych istnieje możliwość odwzorowania dźwięku na litery, rozpoznawając co użytkownik wpisuje na klawiaturze. Metoda analizuje takie parametry jak częstość wciskania danego klawisza lub grupe klawiszy oraz odległość dźwieku od urządzenia nagrywającego, określając tym samym prawdopodobne położenie znaków na klawiaturze. Przykładem zastosowania podobnej metody jest eksperyment Patricka Traynora, adiunkta w Wyższej Szkole Informatyki w Atlancie stanie Georgia. Patrick i jego koledzy *" zaprogramowali smartfony, w taki sposób aby odczytywać wciśnięte klawisze w pobliskich klawiaturach"*. Do rozpoznania klawiszy użyli akcelerometr wbudowany w smartfony, otrzymując podobne wyniki jak przy użyciu mikrofonu, który jest bardziej czułym czujnikiem niż akcelerometr ale lepiej zabezpieczony. Według Patricka, zastosowana technika polega na scharakteryzowaniu pary klawiszy położeniem względem siebie, a dokłanie odległość oraz kierunek położenia. W tym przypadku czujnik powinien znajdować się na tym samym podłożu co klawiatura. Następnie zebrane dane są porównywane ze specjalnie przygotowanym słownikiem, gdzie znajdują sie słowa podzielone w podobny sposób. W celu zabezpieczenia się przed daną metodą należy schować telefon lub odsunąć od komputera. [**?**]

Keyloggery sprzętowe są wykorzystywane, jeżeli sprawcy zależy na niewykrywalności przez antywirus i ma dostęp do naszego komputera. Bez fizycznego badania wykrycie keyloggera jest praktycznie niemożliwe, ponieważ dane są przechwytywane, zanim dotrą do docelowej aplikacji. Bezpieczną praktyką radzenia sobie z keyloggerami jest używanie programu do automatycznego wypełniania formularzy, gdzie obecnie oferuje to większość przeglądarek i niezależnych firm. Dane, które użytkownik uzna za wrażliwe będą przechowywane na serwerach w postaci zaszyfrowanych ciągów, co zmiejsza ryzyko przechwycenia. Aby samemu odszyfrować dane, potrzebna jest znajomość głównego hasła. W przypadku wykrycia strony z formularzem, będą one automatycznie wypełniane, a co najważniejsze bez użycia schowka systemowego oraz klawiatury. Kradzież danych może nastąpić w innym miejscu systemu operacyjnego, na przykład za pomocą snifferów sieciowych i narzędzi proxy. Dlatego dodatkowym środkiem ostrożności jest korzystanie z TLS (ang. Transport Layer Security). TLS jest to rozwinięcie protokołu SSL (ang. Secure Socket Layer), który zapewnia poufność i integralność transmisji danych opierając się na szyfrowaniu asymetrycznym oraz certyfikatach X.509. Innymi zabezpieczeniami przed keyloggerem sprzętowym, a raczej przed przechwyceniem danych wpisywanych za pomocą klawiatury, są klawiatury ekranowe. Podobnie jak w przypadku rozpoznawania pisma ręcznego lub gesty myszy, oprogramowanie do keyloggera może posiadać dodatkowe funkcje, takie jak przechwytywanie obrazu z ekranu, a to oznacza, że podane metody mogą być niewystarczające aby chronić nasze dane. Innym sposobem zabezpieczenia się przed keyloggerem jest oprogramowanie konwersji dźwieku na tekst. W tym przypadku istnieje większe bezpieczeństwo, ponieważ nie wprowadzamy tekstu przez klawiaturę ani nie wykonujemy żadnych ruchów myszą. Jednak dane można przechwycić zapisując dźwięk lub przechwytując tekst wysyłany do oprogramowania docelowego.

5 Wniosek

Mimo że człowiek stara się robić wszystko, by zabezpieczyć swój komputer przed innymi, to nie wiadomo, czy kiedykolwiek tak naprawdę mu się to uda. Keyloggery wykorzystują różne techniki

i metody do kradzieży danych. Środki zaradcze najczęściej są przystosowane do konkretnego typu keyloggera, gdzie z jednej strony chronią nasze dane, a z drugiej strony bardziej narażają nas na niebezpieczeństwo. Wraz z rozwojem nowych technologii, programy szpiegujące rozwijają się oraz pojawiają się nowe techniki monitorowania, *"broniąc"* się przed zabezpieczaniem informacji. Za rozwojem i produkcją keyloggerów, odpowiada nie tylko strona przestępcza, ale także i firmy, które wytwarzają zgodne z prawem oprogramowanie, nacześniej w celu zebrania jak najwięcej informacji i dopasowania produktu pod daną osobę, tylko wtedy gdy użytkownik jest o tym poinformowany. Dlatego użytkownik korzystający z komputera powinien być czujny na każdym kroku. Aby zmniejszyć poziom ryzyka zostania ofiarą keyloggera należy zacząć się samemu zabezpieczać, nikt nie zrobi tego za nas. Jak mówi przysłowie - przezorny zawsze ubezpieczony.

Literatura

[1] Lincoln Spector, *How to turn off Windows 10's keylogger (yes, it still has one)*, url: `https://www.pcworld.com/article/2974057/windows/how-to-turn-off-windows-10s-keylogger-yes-it-still-has-one.html` (term. wiz. 11. 11. 2017)

[2] Caleb Chen, *Microsoft Windows 10 has a keylogger enabled by default – here's how to disable it*, url: `https://www.privateinternetaccess.com/blog/2017/03/microsoft-windows-10-keylogger-enabled-default-heres-disable/` (term. wiz. 11. 11. 2017)

[3] John Leyden, *Florida man sues bank over $90K wire fraud*, url: `https://www.theregister.co.uk/2005/02/08/e-banking-trojan-lawsuit/` (term. wiz. 11. 11. 2017)

[4] *Keyloggers: How They Work and More*, url: `https://www.resources.infosecinstitute.com/keyloggers-how-they-work-and-more/` (term. wiz. 11. 11. 2017)

[5] Nikolay Grebennikov, *Keyloggers: Implementing keyloggers in Windows. Part Two*, url: `https://www.securelist.com/keyloggers-implementing-keyloggers-in-windows-part-two/36358/` (term. wiz. 11. 11. 2017)

[6] Nikolay Grebennikov, *Keyloggers: How they work and how to detect them (Part 1)*, url: `https://www.securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/` (term. wiz. 11. 11. 2017)

[7] Michael Terrazas, *Georgia Tech Turns iPhone Into spiPhone*, url: `https://www.news.gatech.edu/2011/10/17/georgia-tech-turns-iphone-spiphone` (term. wiz. 11. 11. 2017)

[8] *MouseJack Technical Details*, url: `https://www.news.gatech.edu/2011/10/17/georgia-tech-turns-iphone-spiphone` (term. wiz. 12. 11. 2017)