Płać lub płacz, bo nigdy nie zobaczysz swojego systemu

Wymuszenia, kradzieże danych, szantaże – to atmosfera, w której ekipa dochodzeniowa CHIP-a czuje się jak ryba w wodzie. Tym razem **WPADLIŚMY NA TROP NIEZWYKLE NIEBEZPIECZNEGO KONIA TROJAŃSKIEGO**, który już wkrótce może zaatakować także twój komputer. W artykule pokazujemy, jak sobie radzić w takiej sytuacji EDWARD KRZYWY

Warszawa, 13:00 czasu miejscowego, redakcja CHIP-a. Za oknem jesienny deszczowy dzień. Dzwoni telefon. W słuchawce zdenerwowany męski głos. To Janusz K. skarży się, że nieznany szantażysta zaszyfrował mu partycję systemową Windows:

– Nie wiem, co robić. Na dysku mam wszystkie kontakty firmowe. Jak uruchomiłem rano komputer, zobaczyłem ekran logowania po rosyjsku. Nie za bardzo rozumiem, ale chyba chodzi o to, że mam wysłać SMS-a pod wskazany numer. Wtedy przyślą mi kod do odszyfrowania. A jak nie, to to coś wykasuje mi dane na amen. Co mam robić?

– Po pierwsze nie panikować – odpowiada jeden z naszych redakcyjnych kolegów. – Po drugie nie dotykać komputera, podać swój adres i czekać. Po trzecie zgodzić się na opisanie całej sprawy w CHIP-ie – to cena naszej wizyty. – Zgodził się. A więc przed nami nowe zadanie.

Czy, wyjeżdżając w ten dżdżysty dzień w teren, byliśmy przekonani, że nam się powiedzie? Prawdę mówiąc, nie do końca. Wiedzieliśmy tylko, że czeka nas prawdziwe wyzwanie: wirus albo trojan zaszyfrował dysk. Trzeba ten kod złamać, odzyskać dane, usunąć szkodnika, a na koniec upewnić się, że komputer Janusza będzie odporny na kolejne ataki. Ale – jak to mówią – no risk no fun. A więc w drogę!

Wizja lokalna: To szantaż!

Warszawa, 13:30 czasu miejscowego, docieramy na miejsce przestępstwa – niewielkie biuro kserograficzne na Powiślu, gdzie stoi zainfekowana maszyna. Właściciel Janusz K. miota się przy komputerze. Włączamy go i zamiast ekranu powitalnego Windows widzimy komunikat w języku rosyjskim. Na szczęście jeden z nas zna jako tako cyrylicę. Tekst na monitorze brzmi: „Płać lub płacz, bo nigdy nie zobaczysz swojego systemu!". Ponadto znajdują się tam informacje, jak postępować, aby otrzymać kod odblokowujący. Sprawa jest jasna – to szantaż.

Żarty się skończyły! Dzwonimy do zaprzyjaźnionego z redakcją specjalisty. Igor Daniłow, znany lepiej jako Dr Web, po zapoznaniu się ze sprawą stwierdza, że to prawdopodobnie Trojan.Winlock.20 – zupełnie nowy rodzaj konia trojańskiego. Szkodnik ma tylko jeden cel: wymuszenie okupu. Na szczęście Dr Web nie pierwszy raz spotyka się z takim przypadkiem. – Do tej pory „dwudziestka" szalała głównie u Ruskich, ale widać do Polski miała niedaleko – śmieje się i wyjaśnia, co należy zrobić, żeby odblokować peceta.

Idziemy za radą Igora i na stronie news.drweb.com wypełniamy formularz, w którym podajemy numer, pod jaki mieliśmy wysłać SMS do szantażysty. Jakieś 3 minuty później bezpłatnie otrzymujemy kod, który odblokowuje system i partycję. Janusz K. odczuwa wyraźną ulgę. Jednak to nie znaczy, że zażegnaliśmy niebezpieczeństwo – trojan wciąż jest na dysku. Dzięki nieocenionej pomocy Dr. Weba i ten problem udaje się nam szybko rozwiązać.

Zainfekowany komputer działał pod kontrolą systemu Windows XP Home PL. Uruchamiamy Wiersz polecenia, wybierając »Start | Uruchom«, i wpisujemy »regedit«. W edytorze Rejestru przechodzimy do gałęzi »HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer«, gdzie tworzymy nowy klucz typu »Wartość DWORD« o nazwie »NoControlPanel« i ustawiamy jego wartość na »1«. Ponownie uruchamiamy komputer. W trakcie restartu wciskamy [F8] i wybieramy tryb awaryjny. Znów otwieramy Rejestr – zgodnie z informacjami, jakie otrzymaliśmy od Dr. Weba, wirus utworzył w nim nowy klucz, który musimy usunąć ręcznie. Przechodzimy do gałęzi »HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\"Userinit"« i kasujemy wszystkie wpisy typu »%Temp%\don[*].tmp«, gdzie etykieta [*] oznacza dowolny łańcuch znakowy. Na koniec uruchamiamy Windows w normalnym trybie. Trojan na dobre zniknął z komputera Janusza K., ale to jeszcze nie koniec naszego zadania.

Śledztwo: Jak zainfekowano peceta

Szkodniki, które znajdujemy na naszych dyskach, z reguły pochodzą z zainfekowanych stron w Sieci albo pobranych plików. Spytaliśmy Janusza, czy odwiedzał witryny ze scrakowanymi programami, np. www.cracks.am, lub używał aplikacji typu Azerus. Zaprzeczył. Nie odwiedzał także niebezpiecznych stron ani nie pobierał plików z Sieci. Twierdził również, że ma zainstalowanego antywirusa, firewalla, a system operacyjny jest na bieżąco aktualizowany.

Postanowiliśmy zweryfikować te informacje za pomocą aplikacji BTF Sniffer (na naszej płycie), która może być uruchamiana wprost z pamięci flash. Aby otrzymać jak najbardziej jasny obraz działalności Janusza na pececie, aktywowaliśmy najbardziej dokładne wyszukiwanie i nakazaliśmy programowi sporządzenie raportu w pliku tekstowym. Po chwili mieliśmy już przed oczami szczegółowe zestawienie: jakie pliki były otwierane, jakie zmieniane, jakie aplikacje były instalowane i które strony w Sieci odwiedził Janusz.

Po krótkiej analizie dochodzimy do wniosku, że wszystkie ślady prowadzą do pendrive'a firmy Imation. Jednak Janusz twierdzi, że nie ma takiego urządzenia. Idziemy dalej tym tropem: dzięki narzędziu USBDeview (również na naszej płycie) mamy zamiar się dowiedzieć, kiedy i jak często wspomniany pendrive był podłączany do komputera. Program informuje nas, że urządzenie zostało podłączone do peceta Janusza o godzinie 10:26:22 w dniu poprzedzającym atak trojana. Janusz K. sprawdził tę datę w terminarzu. Okazało się, że przebywał wtedy poza firmą. Wniosek albo hipoteza? Groźnego trojana musiał w tym czasie skopiować na jego komputer ktoś inny. Tylko kto? Nie wiedzieliśmy wtedy, że od rozwiązania zagadki dzieli nas dosłownie krok.

Identyfikacja: Sprawca zostaje zdemaskowany

Zasadnicza trudność polegała na tym, że nie mieliśmy narzędzia zbrodni. Wtedy pomógł nam przypadek – jeden z pracowników Janusza, słysząc naszą rozmowę, przypomniał sobie, że niedawno sprzątaczka znalazła w koszu na śmieci przy jednym z biurek klucz USB. Mężczyzna wyszedł, by po chwili wrócić z pendrive'em, który – jak mówił – schował na wszelki wypadek. Już pierwszy rzut oka wystarczył, żeby stwierdzić, że producentem urządzenia jest firma Imation. Poczuliśmy się jak psy, które zwęszyły świeżą krew. Szybko ustaliliśmy, że wcześniej przy tym biurku pracował Konrad L., którego Janusz niedawno zwolnił. Pojawił się więc prawdopodobny motyw – zemsta. Czy rozgoryczony Konrad L. faktycznie popełnił ten czyn? Mogliśmy to łatwo ustalić – jego komputer ciągle stał na biurku. Gdyby okazało się, że tak, dostalibyśmy nowe zadanie – zebrać dowody winy, które można zaprezentować przed sądem.

ZABEZPIECZENIE DOWODÓW Uruchamiamy komputer Konrada L., bootując go z płyty CD ze specjalistyczną dystrybucją Linuksa – Deft Linux Live (do pobrania z www.deftlinux.net), której przeznaczeniem jest informatyka śledcza. W tym celu musimy wcześniej w ustawieniach BIOS-u zdefiniować napęd CD/DVD jako »First Boot Device«. Po załadowaniu systemu zostaniemy poproszeni o ustawienie języka menu. Wybieramy »Polski«. Aby system uruchomił się w trybie graficznym, w konsoli wpisujemy komendę »deft-gui«. Na Pulpicie odnajdujemy i uruchamiamy narzędzie Partition Editor, aby ustalić, jaki identyfikator Linux przypisał do dysku sprawcy. Ustalamy, że »sda1«. Mamy zamiar sporządzić z niego kopię kryminalistyczną. Jest ona niezbędna do dalszej pracy, ponieważ dysk oryginalny musi pozostać nienaruszony, jeśli ma być dowodem w sądzie.

Podczas sporządzania kopii kryminalistycznej kopiuje się nośnik wraz z pustymi obszarami tak, aby suma kontrolna oraz znacznik czasowy istniejących na nim danych były takie same jak na oryginale. Dane utrwalimy na wymiennym dysku USB, wystarczająco dużym, żeby pomieścić zawartość jednej partycji. Podłączamy go, uruchamiamy Terminal – linuksową wersję Wiersza poleceń – i instalujemy w systemie, wpisując komendę:

```
mount•/dev/sdb1•/mnt
```

Następnie korzystając z polecenia:

```
dcfldd•if=/dev/sda1•of=/mnt/image.dd•
bs=4096•conv=noerror,sync
```

kopiujemy wszystkie dane z analizowanej partycji na nasz dysk wymienny. Dzięki →

NA PŁYCIE

avast4 Home ▶ skuteczny, niezawodny, a przy tym darmowy program antywirusowy
BTF Sniffer ▶ wykrywa ślady używania ponad 370 aplikacji w systemie Windows
F-Secure Internet Security ▶ efektywnie chroni peceta przed zagrożeniami z Sieci
KeePass ▶ bezpiecznie przechowuje hasła
McAfeeAvert Stinger ▶ wprawnie wykrywa i usuwa szkodniki gniezdzące się w systemie
MUICacheView ▶ tworzy listę programów zostawiających ślady w Rejestrze systemowym
Password Safe ▶ zarządza listami haseł
PC Security Test ▶ symuluje ataki hakerskie
PeerGuardian ▶ blokuje niebezpieczne IP
Powerbullet Presenter ▶ nadaje się do tworzenia prezentacji z materiału dowodowego
Secunia PSI ▶ zamyka luki w programach
Spybot Search and Destroy ▶ wyszukuje i eliminuje reklamowe szkodniki systemowe
TrueCrypt ▶ szyfruje cały dysk twardy
USBDeview ▶ wyświetla urządzenia podłączone w przeszłości do portów USB

NA PŁYCIE Wszystkie narzędzia znajdziesz, wpisując kod: **SZANTAZ**

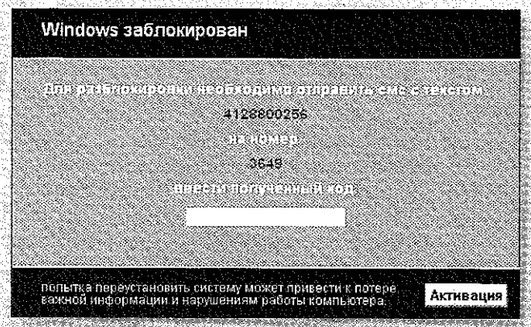
zastosowaniu opcji »bs=4096« Linux czyta i zapisuje bloki o wielkości 4096 bajtów – w efekcie backup zostanie wykonany szybciej. Ostatni parametr sprawia, że procedura zostanie przerwana w przypadku wystąpienia jakichkolwiek błędów.

ANALIZA W utworzonej kopii kryminalistycznej będziemy teraz szukać dowodów. Aby się upewnić, że oryginalny dysk sprawcy nie jest używany w systemie (to mogłoby zmienić jego sumę kontrolną i tym samym zdyskwalifikować jako dowód sądowy) wpisujemy w Terminal instrukcję:

```
mount
```

która wyświetla wszystkie podłączone napędy. Teraz uruchamiamy widoczne na Pulpicie narzędzie Autopsy i, wybierając »New Case«, zakładamy nową sprawę. Nadajemy jej nazwę i zatwierdzamy, ponownie klikając »New Case«. Na kolejnym ekranie nic nie zmieniamy, tylko dwukrotnie klikamy przycisk »Add Host«. Za pomocą »Add image | Add image file« ładujemy naszą kopię kryminalistyczną (/mnt/image.dd) i wybieramy opcje »Disk«, »Simlink« oraz »Volume Image«. Autopsy może, używając sumy kontrolnej (algorytm MD5), przetestować jej integralność. W tym celu aktywujemy »Calculate the hash value for this image«. Zaznaczamy również opcję »Verify hash after importing?«, ponieważ zgodność sum kontrolnych jest w sądzie dowodem na to, że podczas sporządzania kopii kryminalistycznej nie doszło do przekłamań. Klikając przycisk »Add«, rozpoczniemy ładowanie danych z kopii. Ze względu na weryfikację musi to chwilę potrwać.

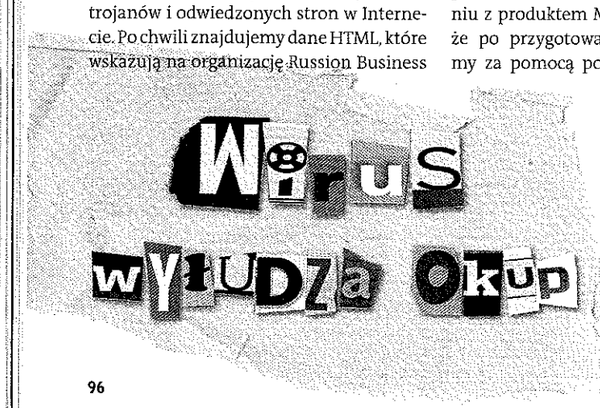
Gdy proces dobiega końca, wciskamy »OK«, po czym wybierając »Analize«, uruchamiamy kolekcjonowanie dowodów. Sposób, w jaki to przebiega, zależy od rodzaju popełnionego przestępstwa. W naszym przypadku podejrzewamy sprawcę o załadowanie z Sieci trojana. Za pomocą polecenia »File Analysis« szukamy śladów trojanów i odwiedzonych stron w Internecie. Po chwili znajdujemy dane HTML, które wskazują na organizację Russion Business Network oraz hakerski serwis aukcyjny WSLabi – to właśnie w nim sprawca nabył wirusa. Zapisujemy nasze ustalenia w pliku tekstowym za pomocą polecenia »Gedit« – entuzjaści Excela mogą utrwalić je w formacie popularnego w środowisku Linuksa arkusza kalkulacyjnego Gnumeric. Daty i godziny popełnionych czynów otrzymujemy w Autopsy dzięki poleceniu »File Activity Timelines | Create Data File«. Po wybraniu naszej kopii kryminalistycznej, »image.dd«, posiłkując się informacjami uzyskanymi od Janusza K., ustalamy startowy i końcowy punkt obserwacji. Autopsy tworzy oś czasu, na której zaznacza dla każdego z przetwarzanych w tym okresie plików takie szczegóły, jak jego nazwa i wielkość, nazwa użytkownika (User ID), nazwa grupy (Group ID) oraz typowy dla Uniksa znacznik »macb« – jest to skrót, w którym kolejne litery oznaczają atrybuty pliku: (m) – modyfikowany, (a) – otwierany, (c) – zmieniany i (b) – nowo utworzony. Wszystkie te informacje Autopsy zapisuje w pliku tekstowym.



INTERNETOWY SZANTAŻYSTA Rosyjski trojan Winlock.20 zaszyfrował partycję systemową Windows i zażądał okupu.

W ten sposób zebraliśmy mocne dowody – wiemy, kiedy podejrzany Konrad L. skopiował plik wirusa na komputer szefa, wiemy też, skąd trojan wziął się na pececie. Aby Janusz K. mógł przedstawić dokładny przebieg przestępstwa przed sądem, utworzymy teraz ze zdobytych dowodów prezentację.

PRZYGOTOWANIE Niestety, ani Autopsy, ani Deft Linux nie oferują narzędzi do zaprezentowania wyciągniętych wniosków w przejrzystej formie. Użyjemy zatem do tego celu programu Powerbullet Presenter (na naszej płycie). Aplikacja działa bardzo podobnie do PowerPointa, ale w porównaniu z produktem Microsoftu ma tę zaletę, że po przygotowaniu prezentacji możemy za pomocą polecenia »File | Export« zapisać ją jako plik EXE, dzięki czemu uruchomimy ją na dowolnym komputerze z systemem operacyjnym Windows, bez konieczności posiadania na nim oryginalnego programu. Tak utworzony plik Powerbullet Presenter domyślnie zapisuje w katalogu »Moje dokumenty\Powerbullet«. Nie musimy zatem robić już nic więcej oprócz skopiowania pliku na pendrive i przekazania go Januszowi K.

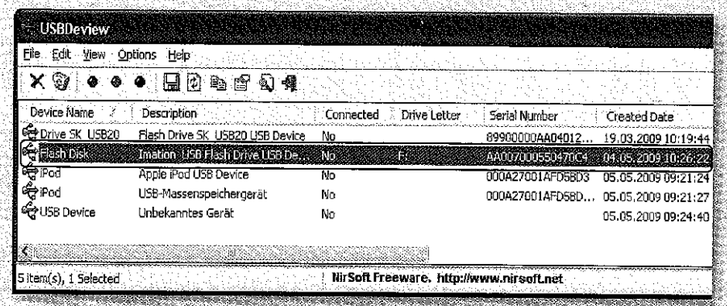


Pełna ochrona:
Pecet odporny na włamania

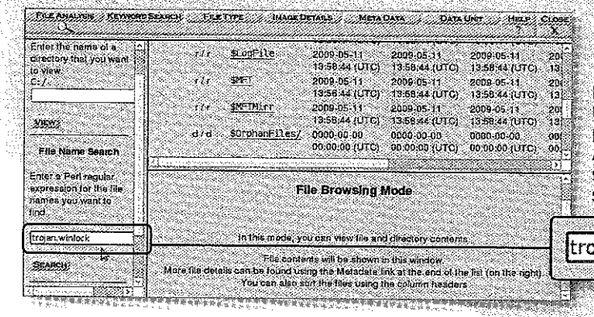
Godzina 16:10, Warszawa-Powiśle. Usunęliśmy trojana, ustaliliśmy sprawcę, udowodniliśmy mu winę i przygotowaliśmy wszystkie dowody w takiej formie, aby zrozumiał je nawet słabo orientujący się w technice adwokat czy sędzia. Co więcej, na oryginalnym dysku przestępcy – dzięki sporządzeniu z niego kopii kryminalistycznej – nie zmienił się nawet pojedynczy bit. Pozostało więc tylko jedno: zabezpieczenie komputera Janusza K., aby w przyszłości nie stał się ofiarą podobnego ataku.

OCHRONA INTERFEJSÓW W pierwszej kolejności postanowiliśmy zabezpieczyć wejścia USB, gdyż to one okazały się najsłabszym punktem obrony. Wiele komputerów umożliwia blokowanie wejść USB z poziomu BIOS-u, ale w przypadku peceta Janusza K. to się nie udało. Wobec tego ściągnęliśmy ze strony www.devicelock.pl 30-dniowe demo programu DeviceLock, który chroni firmę przed wyciekami danych na urządzenia mobilne. Pełna wersja programu kosztuje 130 zł netto, ale wziąwszy pod uwagę możliwe straty, Janusz postanowił ją kupić.

Konfiguracja jest prosta. Podczas instalacji wskazujemy wszystkie wejścia, w przypadku których aplikacja ma regulować prawa dostępu. W zakładce »Lock Automatically« zaznaczamy: »Floppy Drives«, »Removable Devices«, »CD-ROMs«, »Windows Mobile Devices«, »DVDROMs«, »USB-Ports« i »FireWire Ports«. Dzięki temu będziemy decydować o tym, jakie urządzenia i o jakiej porze mogą być podłączane do komputera, a jakich ma on nie akceptować.



ZDEMASKOWANIE Na dysku Janusza K. znaleźliśmy ślady prowadzące do pendrive'a sprawcy.



DOCHODZENIE Używając programu Autopsy, szukaliśmy śladów trojana.

Aby jeszcze bardziej uszczegółowić nadzór, klikamy ikonę »Device Lock Service Settings Control« na Pulpicie. W nowym oknie wybieramy »Device Lock Service | Devices | Permissions | Removable« i określamy użytkowników, którzy mogą podłączyć do komputera zewnętrzny dysk twardy, oraz czas, kiedy mogą tego dokonać. Co więcej, decydujemy, czy urządzenie ma pracować w trybie tylko do odczytu, czy dane na nim mogą być modyfikowane, a dysk sformatowany, a także czy będzie można je ponownie podłączyć. Na koniec za pomocą w polecenia »USB Devices White List« dodajemy do listy urządzeń w pełni zaufanych osobisty pendrive Janusza K.

BLOKOWANIE HAKERSKICH PŁYT CD Narzędzie DeviceLock monitoruje urządzenia wyłącznie wtedy, gdy uruchomiony jest system Windows. By uniemożliwić nieupoważnionej osobie dostęp do komputera za pośrednictwem bootowalnej płyty, takiej jak np. Ophcrack, ustawiamy w BIOS-ie dysk twardy jako pierwsze urządzenie rozruchowe, prosząc Janusza o zabezpieczenie BIOS-u hasłem użytkownika i administratora. W efekcie tylko Janusz K. będzie mógł uruchomić tego peceta.

KOMPLETNA OCHRONA Janusz K. instalował w przeszłości różne narzędzia, by się ochronić przed spamem i złośliwym oprogramowaniem. Zasugerowaliśmy mu zastąpienie ich jedną aplikacją: pakietem typu Internet Security. Większość z nich kosztuje 100–200 zł netto i skutecznie chroni przed wirusami, malware'em, spamem, oferuje także funkcje firewalla i pełnej ochrony rodzicielskiej. Wybór jest bardzo duży: Kaspersky, G Data, F-Secure czy Panda to tylko niektóre z firm, które zajmują się profesjonalną i kompleksową ochroną peceta przed zagrożeniami z Sieci. Nie wiemy, na co ostatecznie zdecydował się Janusz K. (chciał porównać oferty), ale poradziliśmy mu, żeby po instalacji pakietu natychmiast przeprowadził pełne skanowanie komputera – tylko wtedy będzie miał stuprocentową pewność, że jego dysk jest czysty.

SZYFROWANIE DYSKU TWARDEGO Nawet jeśli mimo naszych starań wirus lub haker w przyszłości włamie się do komputera Janusza K., stanie przed kolejnym problemem. Namówiliśmy bowiem Janusza do zaszyfrowania całego dysku za pomocą aplikacji TrueCrypt (na naszej płycie). Szyfrowanie uruchamiamy, wybierając z menu programu »System | Szyfruj Partycję /Dysk systemowy«. W kreatorze wskazujemy »Zaszyfruj partycję systemową Windows | Jeden system«. Jako algorytm polecamy AES – bardzo mocny i bardzo szybki.

Po kliknięciu przez nas przycisku »Dalej« na jednym z kolejnych ekranów program przystępuje do tworzenia dysku ratunkowego: najpierw zapisuje obraz płyty w formacie ISO, a później zmusza nas do jej wypalenia. Gdy to uczynimy, czeka nas jeszcze jej weryfikacja. Ta drobiazgowość jest jak najbardziej uzasadniona – zahaszowane hasło do odszyfrowania dysku twardego przetrzymywane jest w sektorze rozruchowym nośnika. Jeśli zostałby on uszkodzony, nie byłoby możliwe odzyskanie danych. Dysk ratunkowy stanowi skuteczne rozwiązanie tego problemu. Po weryfikacji program przystępuje do szyfrowania dysku, co może zająć dłuższą chwilę.

ŁATANIE DZIUR Na koniec załatamy dziury, które mogą być wykorzystane do zainfekowania peceta przez tak zwane Zero Day-Exploits. Są to szkodniki na tyle nowe, że musi upłynąć trochę czasu, zanim firmy zajmujące się bezpieczeństwem, takie jak G Data, Kaspersky czy Symantec, opracują stosowne szczepionki. Panaceum na to okazuje się Secunia Personal Software Inspector (PSI) – narzędzie, które uaktualnia wszystkie zainstalowane na naszym pececie aplikacje (do najnowszej wersji), minimalizując tym samym ryzyko istnienia potencjalnych luk w bezpieczeństwie.

Warszawa, 18:00 czasu lokalnego. Misja zespołu dochodzeniowego CHIP-a zakończyła się sukcesem – Janusz K. przedstawi dowody wraz z prezentacją swojemu prawnikowi i dalszy ciąg tej historii będzie miał finał w sądzie. A dzięki zastosowaniu polecanych przez nas aplikacji Janusz nie musi się już obawiać kolejnych wymuszeń. ■

Uwaga, ransomware

Trojany, przejmujące kontrolę nad systemem, które szyfrują twardy dysk i żądają pieniędzy za usunięcie tej blokady, określane są jako ransomware (z ang. ransom, czyli okup). Te bardziej znane to AIDS.trojan, Troj_PGPCoder.A oraz wymieniony w artykule Trojan.Winlock.

NIE KONTAKTUJ SIĘ Z SZANTAŻYSTĄ Jeśli twój dysk został zaszyfrowany, do odzyskania kontroli nad pecetem wystarczy płyta ratunkowa z przeglądarką lub drugi komputer. Odwiedź stronę dużego producenta oprogramowania antywirusowego, gdzie zazwyczaj znajdują się kody deszyfrujące wraz z instrukcją obsługi – możesz to wykorzystać do odzyskania danych, bez konieczności układania się z szantażystą. Następnie zabezpiecz swój komputer za pomocą narzędzi z naszej płyty i zaszyfruj partycję z Windows.