MADE IN GERMANY

G DATA TechPaper

Ransomware

Spis treści

Wprowadzenie

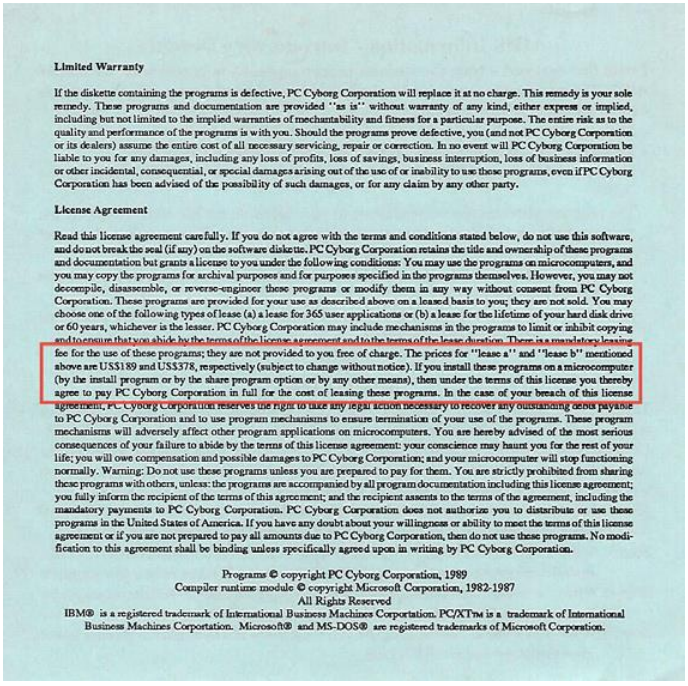
Ransomware ewoluowało stając się jednym z największych zagrożeń zarówno dla użytkowników domowych, jak i biznesowych. Oczekuje się, że w 2017 r. liczba ataków ransomware wzrośnie dwukrotnie o ponad 4 000 w ciągu dnia, a ryzyko utraty plików osobistych, planów biznesowych lub informacji o klientach będzie coraz większe. Ten artykuł wyjaśnia czym jest ransomware i jak zapobiegać infekcjom.

1. Co to jest Ransomware?

Technicznie rzecz biorąc, ransomware jest tylko kolejną formą złośliwego oprogramowania. Odróżnia się ona od innego złośliwego oprogramowania jedną kluczową własnością. Podczas gdy regularne złośliwe oprogramowanie zaraża urządzenia do używania ich jako części botnetu lub kradzieży wrażliwych informacji, twórcy oprogramowania ransomware próbują zarabiać pieniądze wymuszając je bezpośrednio od użytkownika. W celu wymuszania okupu, ransomware blokuje urządzenie lub nawet szyfruje dane do czasu, aż ofiara zapłaci wymaganą kwotę.

1.1. Historia

W ostatnich latach ransomware stał się głównym hasłem w niektórych głośnych sprawach. Użytkownicy domowi, właściciele małych firm, duże przedsiębiorstwa - wszyscy padli ofiarą ataków ransomware. Nie jest to jednak zjawisko nowe: jego historia sięga późnych lat osiemdziesiątych. Zimą 1989 r. ponad 10.000 dyskietek zawierających oprogramowanie ransomware trafiło do placówek medycznych, badaczy oraz osób prywatnych. Dyskietka zawierała oprogramowanie, które miało dostarczyć informacje nt. AIDS, jak reklamowano, jednak w zamian aplikacja stosowała nielegalne metody w celu wyegzekwowania umowy licencyjnej. Blokując komputer i szyfrując pliki, autor próbował nakłonić użytkowników do zapłaty 189 dolarów, które miały zostać wysłane na skrytkę pocztową twórcy.



Limited Warranty

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

License Agreement

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corporation. PC/XT™ is a trademark of International Business Machines Corporation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

Źródło: United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS); BBR Services.

Oprogramowanie nie było zbyt skomplikowane. Pliki i programy można było przywrócić za pomocą specjalnie opracowanego antidotum. Dopiero w 1996 roku naukowcy opisali pojęcie przestępczej kryptografii: wykorzystywanie klucza publicznego w sposób złośliwy. Potem potrzeba było około dziesięciu lat, aby pojawiło się pierwsze oprogramowanie ransomware dystrybuowane masowo z faktycznym szyfrowaniem, jak PGPCoder w 2005 roku czy Archiveus w 2006 roku. Podczas, gdy niektóre rodzaje ransomware nadal tylko blokowały komputer, niekiedy podając się za organy ścigania, ransomware z szyfrowaniem szybko przyjął się jako najbardziej rozpowszechniony typ.

1.2. Ransomware dzisiaj

Wraz z rozwojem badań nad kryptografią przestępcy także rozwijali swoje metody. Podczas gdy oprogramowanie ransomware, które blokuje komputer nie pozostawia żadnych trwałych uszkodzeń po jego usunięciu, dodanie funkcji szyfrowania plików do kodu oznacza, że nawet po usunięciu szkodnika pliki nadal nie są dostępne. Obecnie twórcy ransomware bazują na silnych kluczach szyfrujących, przez co zaszyfrowane pliki można odzyskać tylko wtedy, gdy przestępcy popełnili jakiekolwiek błędy w implementacji. Dlatego infekcjom ransomware należy zapobiegać, a użytkownicy i administratorzy muszą upewnić się, że mogą odzyskać swoje dane po infekcji ransomware.

Pod koniec 2013 roku Cryptolocker ugruntował swoją pozycję jako jednego z najbardziej niesławnych rodzajów ransomware. Od tego czasu to oprogramowanie rozwinęło się w rodzinę podobnych typów ransomware. Wszystkie mają wspólną cechę, szyfrują dane na dysku twardym ofiary i wysyłają klucz do atakującego. Aby odzyskać dostęp do plików firmowych lub prywatnych, takich jak zdjęcia, ofiary muszą zapłacić okup w celu otrzymania klucza deszyfrującego. Inne przykłady ransomware, takie jak Locky, WannaCry czy Spora, różnią się między sobą pod względem realizacji, ale podstawowa koncepcja i działanie pozostaje niezmienione. Wzrost wyrafinowania przestępców internetowych można zaobserwować patrząc na wysiłek włożony w rozwijanie ransomware. Niektórzy przestępcy po prostu szyfrują pliki i pokazują komunikat o zapłaceniu okupu, inni budują kompletną infrastrukturę, w tym portal internetowy, system czatów i wiele opcji płatności, w tym pełne odszyfrowanie, odporność lub usunięcie.

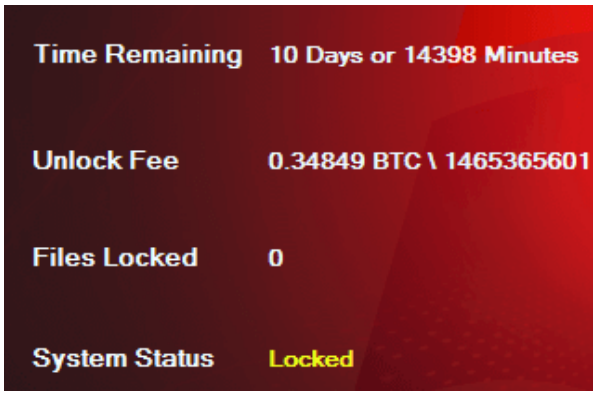
1.3. Dystrybucja i ofiary

Ransomware jest zazwyczaj dystrybuowane jak każdy inny rodzaj złośliwego oprogramowania. Obejmuje to metody takie jak:

- Spam z załącznikiem lub linkiem do pobrania
- Skompromitowana strona internetowa
- Zainfekowana sieć reklamowa

Mimo że specjaliści ds. bezpieczeństwa i administratorzy systemów od lat mówią użytkownikom końcowym, aby nie klikali w jakiekolwiek podejrzane linki lub załączniki, spam pozostaje głównym wektorem infekcji.

Ransomware często ukrywa się w dokumentach tekstowych z obsługą makr, ale pliki wykonywalne mogą teoretycznie zostać załączone do każdego wrażliwego typu załącznika. Oprócz spamu, często wykorzystywane są również zainfekowane strony internetowe do dystrybucji oprogramowania ransomware. A nawet strony, które nie zostały zaatakowane, mogą rozprzestrzeniać ransomware, jeśli zawierają kod z sieci reklamowych, które nie są wystarczająco kontrolowane.



Źródło:: https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/.

Przestępcy często nie adresują wirusa do konkretnych firm lub użytkowników domowych, ale zamiast tego decydują się na dystrybucję ransomware w możliwie jak największej liczbie kanałów. Ponieważ metody dystrybucji obejmują dużą liczbę metod, istnieje duże ryzyko infekcji wśród użytkowników. Nie ma znaczenia, czy ofiara jest przedsiębiorcą czy użytkownikiem końcowym, ponieważ obaj najprawdopodobniej zapłacą okup, jeśli zaszyfrowane zostaną dostatecznie ważne dane. Mimo to, dla niektórych przedsiębiorstw skutki mogą być większe niż dla innych. Na przykład szpitale były w dużym stopniu dotknięte ransomware.

Prawdopodobnie powodem jest relatywnie stara infrastruktura IT, krytyczny czas dostępu do wrażliwych danych oraz liczba podłączonych urządzeń.

Ransomware nie tylko wykorzystuje najnowsze technologie, aby zmaksymalizować swoją efektywność. Przestępcy stosują również sztuczki behawioralne, aby zachęcić użytkowników do płacenia. Jak gdyby samo szyfrowanie ważnych danych nie wystarczyło, presja na ofiary jest zwiększana poprzez wyświetlanie limitu czasowego. Wiele rodzajów oprogramowania ransomware grozi usuwaniem plików lub kluczy deszyfrujących, jeśli ich żądania nie zostaną spełnione w określonym czasie. Jedna z rodzin ransomware pozwala użytkownikom na bezpłatne odszyfrowanie plików, jeśli rozpowszechniają złośliwe oprogramowanie wśród swoich znajomych lub innych użytkowników.

1.4. Model biznesowy

Oczywistym powodem wzrostu dystrybucji oprogramowania ransomware jest bezpośredni zysk finansowy przestępców internetowych. Istnieje jednak wiele czynników, które przede wszystkim przyczyniły się do tego wzrostu i doprowadziły do powstania rzeczywistych modeli biznesowych stojących za oprogramowaniem ransomware. Po pierwsze, wzrost liczby kryptowalut pozwolił przestępcom żądać pieniędzy, pozostając jednocześnie anonimowymi. Wiele typów okupu przyjmuje płatności w Bitcoin, która jest kryptowalutą i nie wymaga tradycyjnego rachunku bankowego. Inni wykorzystują bony płatnicze lub przekazują płatności za pośrednictwem wielu usług, aby ukryć swoją tożsamość. Po drugie, sama technologia ransomware stała się towarem.

Przestępcy nie muszą już opracowywać własnych metod szyfrowania - mogą korzystać z oferty ransomware-as-a-service, które są łatwo dostępne na podziemnych rynkach. Oznacza to, że prawie żadna inwestycja nie jest wymagana do zbudowania ransomware. Wreszcie, infrastruktura ransomware jest bardzo elastyczna, co komplikuje starania funkcjonariuszy organów ścigania mające na celu zlokalizowanie serwerów dystrybucyjnych lub płatniczych. Szansa wpadki jest zatem stosunkowo niewielka. Czynniki te umożliwiają stworzenie modelu biznesowego, który pozwala przestępcom szybko zorganizować kampanię ransomware, skierowaną do dużej liczby użytkowników przy relatywnie niskich kosztach własnych.

2. Ochrona przed ransomware

W wielu przypadkach zainfekowani użytkownicy decydują się na wniesienie okupu, licząc na odzyskanie zaszyfrowanych plików. Niestety uiszczenie opłaty nie zawsze jest jednoznaczne z odzyskaniem danych. Serwery z kluczami szyfrującymi mogą w międzyczasie zostać wyłączone lub zablokowane. Dokonanej płatności nie można wyśledzić, a więc nie można jej wycofać. Nawet po odzyskaniu danych złośliwe oprogramowanie może nadal pozostawać w zarażonym systemie. Nie ma pewności, że oprogramowanie ponownie nie zaszyfruje danych. Płacenie przestępcom samo w sobie nie jest najlepszym możliwym wyborem, gdyż zachęca ich do kontynuowania swojego przestępczego procederu.

2.1. AntiRansomware

Najlepsza ochrona przed szkodnikami wymuszającymi opłaty za dostęp do danych to oczywiście zablokowanie możliwości uruchomienia ransomware w systemach operacyjnych. Zaleca się stosowanie rozwiązań dedykowanych do wykrywania i blokowania aktywności ransomware. Oprogramowanie zabezpieczające, poza standardowym wykrywaniem zagrożeń w oparciu o sygnatury, powinno być wyposażone w szereg mechanizmów do wykrywania i blokowania aktywności typowej dla najnowszych jeszcze nieznanych zagrożeń.

2.2. Aktualizacje

Ochrona przed ransomware to również polityka regularnego aktualizowania oprogramowania oraz samych systemów operacyjnych. Oznacza to w praktyce możliwie jak najczęstsze weryfikowanie dostępności poprawek

i ich aplikowanie. W sieciach z większą ilością stanowisk przydatne może być wdrożenie specjalnego, centralnego rozwiązania do zarządzania aktualizacjami do systemów operacyjnych i zainstalowanych na stacjach aplikacji.

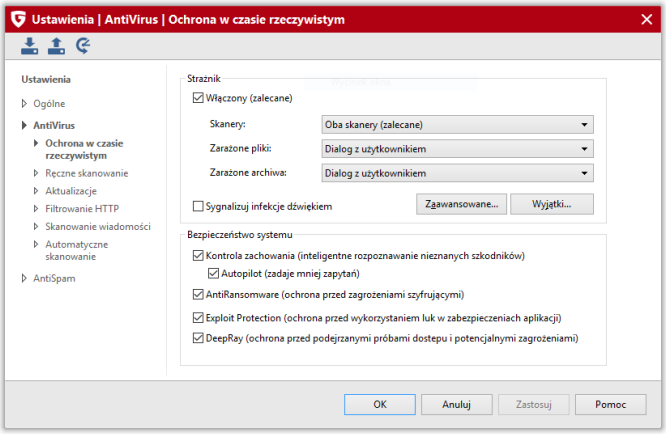
2.3. Backup

Jako że oprogramowanie ransomware bazuje na szyfrowaniu zasobów ważnych dla użytkowników, jedną z metod ochrony przed tym zagrożeniem jest regularne tworzenie kopii zapasowych najważniejszych plików i folderów. Kopie powinny być przechowywane na nośnikach poza lokalnymi stacjami roboczymi, aby zapobiec zaszyfrowaniu kopii w przypadku infekcji ransomware naszej sieci. Użytkownicy domowi mogą skorzystać z opcji przechowywania danych w chmurze lub na zewnętrznym dysku twardym. Administratorzy sieci mogą wdrożyć rozwiązanie przechowujące ważne dokumenty z wszystkich końcówek w firmie w centralnej lokalizacji.

2.4. Świadomość zagrożenia

Niezwykle ważnym czynnikiem zapobiegawczym jest ustawiczne wpływanie na świadomość użytkowników poprzez informowanie i szkolenia wewnętrzne w firmach. Uwrażliwienie użytkowników na otwieranie załączników poczty od nieznanych adresatów, a także rozsądne podejście do linków przesyłanych pocztą lub poprzez media społecznościowe może w wielu przypadkach uchronić istotne dane przed zaszyfrowaniem lub wyciekiem.

3. Jak G DATA chroni przed ransomware?



Rozwiązania G DATA oferują kompleksową ochronę przed ransomware dla użytkowników domowych oraz biznesowych. Nasze rozwiązania wyposażone są w dedykowany moduł AntiRansomware chroniący przed zagrożeniami mającymi za zadanie szyfrować pliki. W wersji biznesowej moduł jest centralnie sterowany za pomocą konsoli G DATA Administrator. W sieciach firmowych istotne jest wdrożenie kompleksowej polityki aktualizacji oprogramowania w czym zdecydowanie może pomóc opcjonalny składnik oprogramowania G DATA o nazwie Patch Management.

Użytkownicy domowi mogą dodatkowo skorzystać z opcji regularnego sporządzania kopii zapasowych dostępnej w aplikacjach G DATA Internet Security oraz G DATA Total Security. Więcej informacji na temat rozwiązań G DATA dla domu i dla firm znajdziesz na stronie www.gdata.pl.

Moduł G DATA AntiRansomware

Moduł funkcjonuje niezależnie od sygnatur zagrożeń i wykorzystuje heurystyczne metody detekcji wspomagając ochronę proaktywną. Dzięki zastosowaniu tej technologii możliwe jest wczesne wykrywanie również nieznanych dotąd zagrożeń szyfrujących na podstawie typowych zachowań i cech charakterystycznych. Przykłady typowego zachowania dla zagrożeń z rodziny ransomware:

- Nawiązanie kontaktu z serwerem kontrolującym. Niektóre rodziny zagrożeń szyfrujących uaktywniają się dopiero po nawiązaniu łączności i otrzymaniu niezbędnych danych od
- serwerów C&C
- Wyłączenie mechanizmów tworzących kopie zapasowe i usunięcie kopii zapasowych z systemu
- Stosowanie procedur do bezpowrotnego usunięcia danych z dysku. Zwykłe usunięcie danych umożliwia ich przywrócenie, ponieważ nadal znajdują się na dyskach twardych
- Szyfrowanie wielu plików w krótkim czasie

- Po zapisaniu danych modyfikowany jest rodzaj plików oraz entropia
- Zmiana rozszerzeń plików (np. z .docx na .locky)

Po wykryciu w systemie działań charakterystycznych dla zagrożeń szyfrujących, moduł AntiRansomware zatrzymuje wszystkie procesy biorące udział w takich działaniach oraz wstrzymuje proces szyfrowania. Jednocześnie przenosi szkodliwe oprogramowanie do folderu kwarantanny.