Marek Piotr Stolarski

Obrona przed atakami nuklearnymi przy wykorzystaniu robaków komputerowych na przykładzie irańskiej infrastruktury jądrowej

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 1, 193-202

2012

AUTOR

mgr Marek Piotr Stolarski

RECENZENT

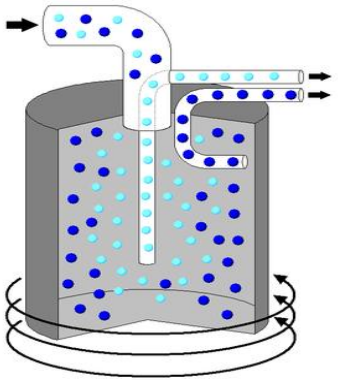
płk dr hab. Marek Wrzosek

OBRONA PRZED ATAKAMI NUKLEARNYMI PRZY WYKORZYSTANIU ROBAKÓW KOMPUTEROWYCH NA PRZYKŁADZIE IRAŃSKIEJ INFRASTRUKTURY JĄDROWEJ

Wprowadzenie

W latach 50. XX wieku, w ramach programu "Atom dla pokoju", Stany Zjednoczone pomogły Iranowi rozpocząć budowę własnego programu atomowego[315]. Pomoc ta trwała aż do roku 1979, kiedy to została przerwana przez wybuch irańskiej rewolucji islamskiej i obalenie szacha Rezy Pahlaviego.

W styczniu 2010 śledczy z Międzynarodowej Agencji Energii Atomowej, w trakcie inspekcji irańskiego ośrodka wzbogacania uranu w Natanz, zwrócili uwagę na wyjątkową anomalię w procesie wymiany wirówek wzbogacających. Urządzenie takie jest szybkoobrotową wirówką, w której pod wpływem sił odśrodkowych następuje rozdzielenie gazowych związków izotopów uranu. Wzbogacanie uranu odbywa się w sposób następujący: uran wzbogacony jako lżejszy pozostaje w komorze środkowej, podczas gdy uran zubożony przemieszcza się ku ścianom wirówki[316].



Źródło: Wikipedia: *Wirówka wzbogacająca*

Rysunek 1. Schemat działania wirówki wzbogacającej

[315] S. Roe, *An atomic threat made in America,* Chicago Tribune, Chicago, 28.01. 2007

[316] Definicja: za wikipedią: *Wirówka wzbogacająca*,

W warunkach typowej eksploatacji wirówki ulegają zużyciu na poziomie do 10% w skali roku. Obecnie w Natanz zainstalowanych jest 8700 wirówek, co daje średnio 870 wymienianych egzemplarzy każdego roku. W trakcie kontroli zapisów kamer przemysłowych ujawniono, że w obrębie kilku miesięcy zostało ich wymienionych od 1000 do 2000, co znacznie przewyższa typowe zużycie[317].

Iran nie był zobligowany do wyjaśniania powodów, dla których wirówki były wymieniane tak często, ale oczywiste wydawało się, że uszkodzenie musiała spowodować niewłaściwa eksploatacja. Okazało się, że błędne użytkowanie nie było dziełem irańskich inżynierów, lecz niezwykle dopracowanego i bardzo szkodliwego w obszarach działania wirusa – komputerowego robaka, którego później nazwano Stuxnetem.

Incydent

W lipcu 2009 roku wiele irańskich komputerów zostało zainfekowanych skomplikowanym wirusem komputerowym, którego jedynym celem był sabotaż irańskiego programu wzbogacania uranu i tym samym spowolnienie procesu uzyskania przez Iran broni jądrowej. W celu przeprowadzenia ataku skierowanego wykorzystano tzw. robaka sieciowego, czyli szkodliwy kod zdolny do replikacji i rozprzestrzeniania się przez sieć. Punktem wejścia (sposobem, w jaki wirus infekował komputery) były liczne, nieznane wcześniej luki bezpieczeństwa (tzw. luki 0-day) znalezione w systemie operacyjnym Windows. Szkodliwy program wyposażono też w możliwości przenoszenia się z użyciem napędów pamięci wymiennych USB, a także aktualizowania własnego kodu przez współtworzone z innymi zarażonymi systemami sieci Peer-to-Peer (P2P).

Cel ataku

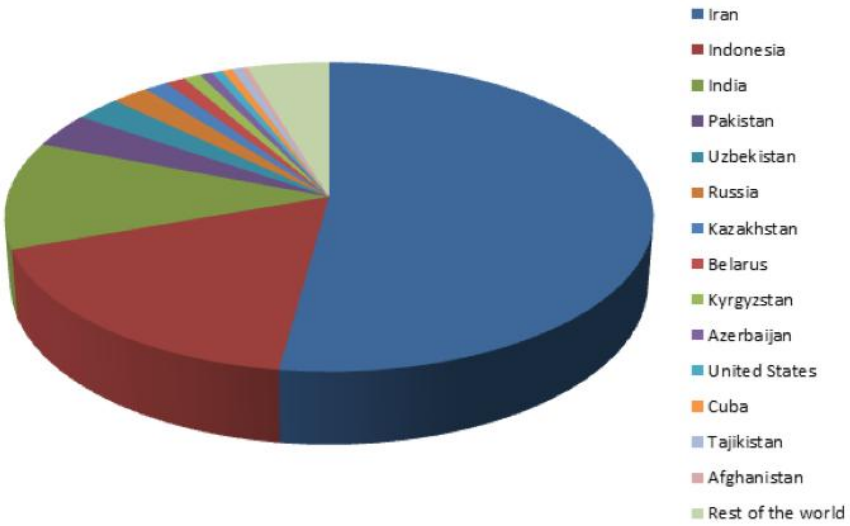
Przyjmuje się, że głównym celem wirusa Stuxnet był irański program wzbogacania uranu, a w szczególności jego spowolnienie[318]. Wskazują na to nie tylko opinie ekspertów[319], lecz także dane statystyczne[320].

[317] J. Warrick, *Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack*, Washington Post, 16.02. 2011 r.

[318] J. Fildes *Stuxnet Virus Targets and Spread Revealed,* BBC News, 15 .02. 2011 r.

[319] S. Cherry wywiad z R. Langnerem *How Stuxnet Is Rewriting the Cyberterrorism Playbook,* IEEE Spectrum, 13 .10.2010 r.

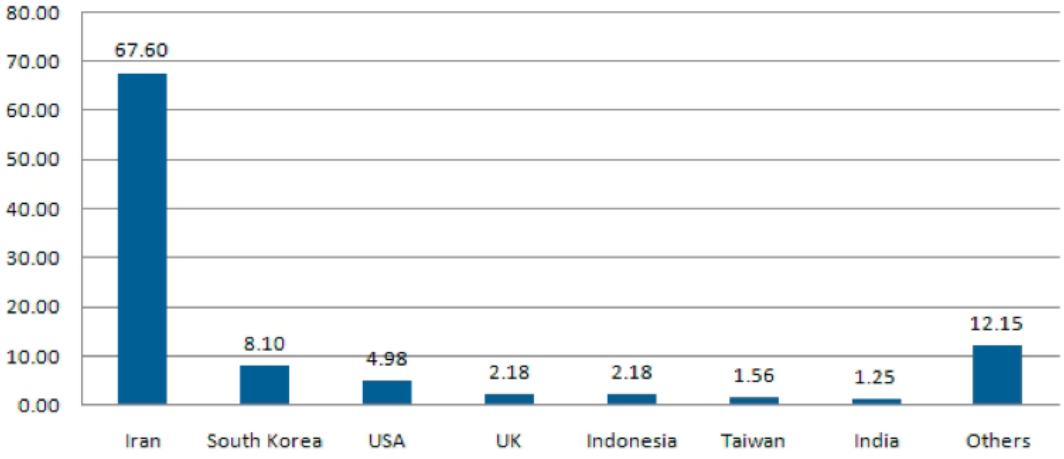
[320] A. Matrosov, E. Rodionov, D. Harley, J. Malcho, *Stuxnet Under the Microscope,* wrzesień 2010 r.



Źródło: A. Matrosov, E. Rodionov, D. Harley, J. Malcho, *Stuxnet Under the Microscope,* wrzesień 2010 r.

Rysunek 2. Geograficzny rozkład infekowanych systemów

Zgodnie z powyższym rozkładem 60% wszystkich infekcji dotyczyło komputerów ulokowanych w Iranie. Dużym odsetkiem, ale nie tak istotnym jak irański, charakteryzowały się również Malezja i Indie. Podobnie ma się rozkład infekcji na komputerach, na których było zainstalowane oprogramowanie firmy Siemens.



Źródło: Symantec: *W32.Stuxnet Dossier*, luty 2011.

Rysunek 3. Geograficzny rozkład infekowanych systemów z zainstalowanym oprogramowaniem firmy Siemens

Duża liczba infekcji w Iranie może świadczyć o tym, że właśnie tam mieliśmy do czynienia z pierwszymi infekcjami. Najprawdopodobniej dokonano ich zanim wirus pojawił się w krajach rozwiniętych, gdzie wykryły go systemy pułapki firm produkujących oprogramowanie antywirusowe. Dzięki temu mógł on namnożyć się, nie będąc powstrzymywany przez zwalczające oprogramowanie „szkodniki", które zwyczajnie nie były wyćwiczone, aby go zwalczać (brakowało im odpowiednich sygnatur pozwalających wykrywać kod Stuxneta).

Zakładając, że Stuxnet był bronią wymierzoną w konkretne cele, daje się zauważyć, jak priorytetowa musiała być to operacja, skoro w celu osiągnięcia wysokiej skuteczności ataku, dopuszczono do powstania wielu punktów infekcji i w rezultacie pozwolono na rozprzestrzenienie się wirusa po całym świecie. Ewentualne usterki w funkcjonowaniu niektórych systemów operacyjnych związane z obecnością „szkodnika" i aktywizacje alarmów w urządzeniach analizujących anomalie ruchu sieciowego, można w tym wypadku zakwalifikować do strat ubocznych – na szczęście związanych z niezabezpieczonymi środowiskami komputerowymi, a nie bezpośrednio z ludnością cywilną.

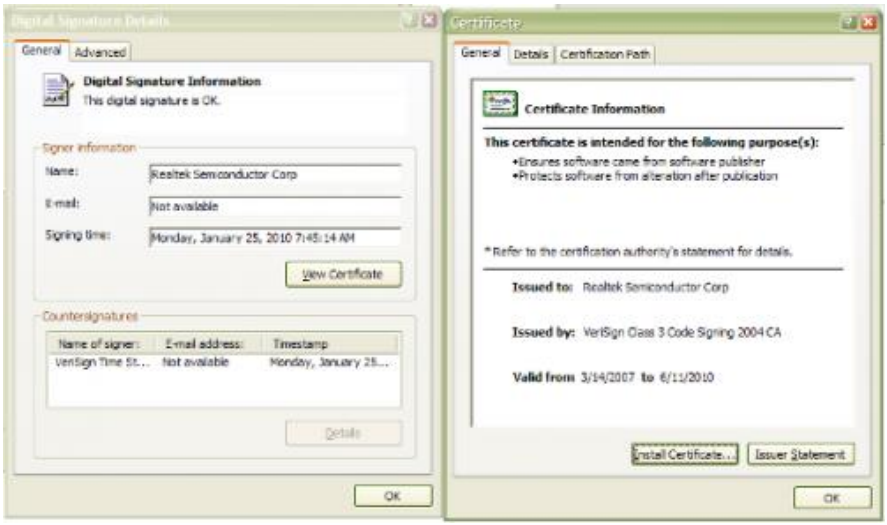
Metoda działania

Po zainfekowaniu systemu docelowego wirus nie wykazuje żadnej aktywności przez kilkanaście dni. Poszukuje za to konkretnego modelu sterownika PLC firmy Siemens, który wraz z oprogramowaniem rodziny SCADA (Step7 i SIMATIC PCS 7) służy do kontrolowania pracy linii przemysłowych. Jeśli odpowiedni driver nie zostanie wykryty przez potencjalnie niebezpieczny podprogram, to nie wyrządza on żadnych szkód, poza próbami replikacji w celu infekowania innych komputerów. Jeżeli jednak właściwy komponent oprogramowania zostanie znaleziony, to uruchomione zostają procedury niszczące, które zostały skonstruowane w taki sposób, aby nie zostawiać wyraźnych śladów, przynajmniej w początkowym okresie aktywności.

Robak sieciowy zagnieżdżony w irańskiej infrastrukturze programu wzbogacania uranu modyfikował ustawienia rejestrów konfiguracyjnych PLC w celu zwiększenia częstotliwości wirówek do 1.51 kHz. Po 15 minutach nakazywał systemowi sterowania linią przemysłową powrót do normalnej częstotliwości pracy wirówek wynoszącej 1.064 kHz. Częstotliwość była utrzymana na tym poziomie przez kolejne 27 dni, by następnie obniżyć ją do zaledwie 2Hz na czas 50 minut. Po tym okresie następował okres jałowy, charakteryzujący się brakiem jakiejkolwiek aktywności przez kolejne 27 dni i wirus ponawiał atak wedle tej samej sekwencji. Takie zachowanie

okazało się destrukcyjne dla tak wrażliwego urządzenia jak wirówka wzbogacająca[321].

Podczas badań ujawniono, że kod wirusa został rozpowszechniony nie wcześniej niż rok przed jego wykryciem, najprawdopodobniej w lipcu 2009. Od tego czasu jego twórca aktualizował go i udoskonalał, wypuszczając 3 kolejne wersje. Co więcej, odkryto, że wirus używał zaufanych podpisów cyfrowych, które zostały złożone z użyciem certyfikowanych kluczy kryptograficznych uprzednio wykradzionych z firmy RealTek Semiconductors – tajwańskiego twórcy podzespołów elektronicznych – tym samym doprowadzając do sytuacji, w której systemy traktowały go jako autoryzowany program firmy RealTek.



Rysunek nr 4. Przykład okien dialogowych systemu Windows prezentujących właściwości cyfrowo podpisanych sterowników firmy RealTek

Certyfikaty cyfrowe to element Infrastruktury Klucza Publicznego (IKP), czyli powszechnie stosowanego systemu kryptograficznego, wykorzystującego powiązaną matematycznie parę kluczy. Dane zaszyfrowane jednym z nich, mogą być odszyfrowane wyłącznie drugim i vice versa. Jeden z sekretów, zwany umownie kluczem publicznym, przeznaczony jest do wolnej dystrybucji, a jeśli opatrzony jest dodatkowo podpisem cyfrowym zaufanej instytucji, to nazywamy go certyfikatem. Właściciel pasującego do niego klucza tajnego może deszyfrować przeznaczone dla niego wiadomości zabezpieczone częścią publiczną. Może również używać kluczy w odwrotnym kierunku, szyfrując kluczem prywatnym sumę kontrolną pewnego tek-

[321] *A worm in the centrifuge: An unusually sophisticated cyber-weapon is mysterious but important*. The Economist. 30.09. 2010 r.

stu lub danych – w ten sposób powstaje podpis cyfrowy. Każdy, kto posiada klucz publiczny, jest potem w stanie odszyfrować sumę kontrolną i porównać ją z sumą samodzielnie wyliczoną dla otrzymanych danych. Jeśli wyniki będą zgodne, to integralność komunikatu lub innego obiektu binarnego zostanie poświadczona przez nadawcę. Dzieje się tak dlatego, że podpis mogła złożyć wyłącznie osoba lub instytucja z dostępem do klucza prywatnego.

Rysunek nr 5. Okno systemu Windows ostrzegające przed próbą instalacji komponentu nieopatrzonego podpisem cyfrowym

Opisany wyżej mechanizm wykorzystywany jest do cyfrowego poświadczania autentyczności sterowników w Windows. System ten posiada wbudowane klucze publiczne skojarzone bezpośrednio lub przez cyfrowe pełnomocnictwa z kluczami prywatnymi zaufanych producentów oprogramowania. Gdy taki producent wydaje nową wersję, to używa własnego klucza prywatnego do złożenia na niej podpisu. Jeśli użytkownik lub procedura automatycznej aktualizacji zainstaluje tak podpisany komponent, to przed wczytaniem go system sprawdzi, czy złożony na nim podpis cyfrowy pochodzi od zaufanego wydawcy oprogramowania.

W przypadku Stuxnetu doszło do kradzieży klucza tajnego, używanego do podpisywania sterowników, a więc część kodu wirusa była ładowana przez systemy bez zgłaszania ostrzeżenia. Na tym jednak nie koniec, ponieważ wirus wykorzystywał jeszcze jeden klucz, należący do firmy Jmicron Technology, który też został skradziony. Oba wymienione przedsiębiorstwa mieszczą się w Tajwańskim Parku Naukowym Hsinchu, co może sugerować bezpośrednie i fizyczne włamanie do ich siedzib w celu uzyskania kluczy tajnych, a nie zdalne włamanie do ich systemów komputerowych.

Za każdym razem, gdy Stuxnet infekował system, łączył się z komputerami wskazywanymi przez jedną z dwóch nazw domenowych, utrzymywanych na duńskich i malezyjskich serwerach systemu nazw domenowych (DNS): www.mypremierfutbol.com i www.todaysfutbol.com. „Szkodnik" przekazywał tam raport o dopiero co zainfekowanym środowisku. Raportowane były następujące dane: nazwa komputera, rodzaj systemu operacyjnego i jego wersja, używane adresy IP (zarówno z puli prywatnej, jak i zewnętrzne), a także odpowiedź na pytanie, czy w środowisku zostało zainstalowane oprogramowanie, w którego skład wchodzi komponent Siemens Simatic WinCC. Będąc w stałej komunikacji z w/w serwerami Stuxnet mógł zostać rozszerzony o nowe funkcje.

Odpowiednie organy wystąpiły do rejestratorów nazw domenowych o przejęcie wspomnianych stref DNS, dzięki czemu możliwe stało się obserwowanie napływającego ruchu sieciowego pochodzącego z zarażonych systemów. Zrealizowano to w ten sposób, że z nazwami domenowymi skojarzono odpowiednie systemy pułapki, które imitowały serwery komend i kontroli (C&C) Stuxneta. We wskazanym środowisku badawczym w ciągu pierwszego tygodnia obserwacji ujawniono 38000 potwierdzonych infekcji, z których 22000 dotyczyło Iranu.

Oprogramowanie SIMATIC PCS 7 posiada możliwość programowania i monitorowania PLC przez specjalnie zaprojektowany interfejs komunikacyjny, pozwalający na wysyłanie i odbieranie komend. Stuxnet potrafił przechwytywać te komendy i zastępować je własnymi. Jednocześnie wyłączał on wszelkiego rodzaju ostrzeżenia systemowe oraz ukrywał własne komendy w taki sposób, aby żadne działanie wirusa nie zostało przypadkowo wykryte i zaraportowane przez system, a pracownicy monitorujący działanie urządzeń byli informowani wyłącznie o standardowych, typowych i niezmienionych warunkach. Jest to pierwszy przypadek w historii robaków sieciowych, w którym głównym zadaniem szkodliwego oprogramowania jest rzeczywiste działanie na szkodę przez fizyczne uszkadzanie urządzeń spowodowane wymuszaniem ich nieprawidłowej pracy.

Możliwy scenariusz ataku z użyciem wirusa Stuxnet[322] rozpoczyna się od umieszczenia w kilku komputerach z systemem Windows zainfekowanej pamięci USB. Jeśli system operacyjny nie został przez producenta uaktualniony poprawką MS10-046, to jest podatny na atak z użyciem odpowiednio spreparowanych plików skrótów (rozszerzenie .LNK). Wadliwy komponent systemowy (Windows File Explorer) pozwoli na wykonanie dowolnego kodu, którym będzie pierwsza część wirusa. Jej zadaniem jest szybkie zamaskowanie się w systemie i ukrycie niebezpiecznych zbiorów umieszczonych na podłączonej pamięci przenośnej. Z użyciem podpro-

[322] Opracowano na podstawie dokumentu *W32.Stuxnet Dossier* firmy Symantec, luty 2011 r.

gramu umieszczonego w przestrzeni użytkownika ukrywane są pliki, których nazwy kończą się rozszerzeniami .LNK, .TMP lub rozpoczynają sekwencją „~ WTR".

Kolejnym etapem jest instalacja szkodliwego kodu w przestrzeni pamięci należącej do jądra systemu operacyjnego. W tym celu robak instaluje podpisane wykradzionymi kluczami sterowniki mrxcls.sys i mrxnet.sys. Dodatkowo, instaluje też automatycznie uruchamiany podprogram działający w przestrzeni użytkownika. Zaraz potem uruchamiane są dwie usługi systemowe (MRXCLS i MRXNET), które pozostają ukryte (nie można ich zauważyć, korzystając z narzędzi do analizy działających procesów). Na tym kończy się faza zarażania systemu. Jedynym sposobem na wykrycie wczesnych wersji „szkodnika" jest sprawdzenie, czy w systemie plików nie rezydują pliki system32/drivers/mrxcls.sys, system32/drivers/mrxnet.sys, infoem6c.pnf i infoem7a.pnf.

Zaraz po udanym zarażeniu Stuxnet łączy się z Internetem i próbuje zgłaszać gotowość do przyjmowania poleceń. Używa w tym celu wspomnianych wcześniej nazw domenowych. Zdalny operator może ręcznie nakazać robakowi wykonanie następujących poleceń: odczyt plików, zapis plików, usuwanie plików, pobranie z sieci Internet dodatkowych bibliotek i programów w celu ich uruchomienia. Dzięki temu robak staje się tylnym wejściem do zainfekowanego komputera, czyli tzw. backdoorem. Teoretycznie systemy sterowania liniami przemysłowymi powinny być odseparowane od Internetu, lecz praktyka pokazuje, że na wielu z nich usunięto zalecane ograniczenia dla wygody pracowników obsługi.

Następną fazą ataku jest uruchomienie kodu odpowiedzialnego za przejęcie kontroli nad komponentem WinCC, działającym w środowisku sterowania liniami produkcyjnymi PCS 7. Na początku uważano, że na ataki narażone są też wydania oprogramowania Step7, jednak specjaliści z firmy Siemens wydali oświadczenie, w którym stwierdzają, że podatne są wyłącznie systemy automatyki SIMATIC PCS 7. Poza tym późniejsza analiza kodu wirusa ujawniła, że zawiera on również procedury pozwalające pobierać zawartość baz danych Microsoft SQL, z których korzysta WinCC. Stuxnet używa wpisanego na stałe hasła do bazy danych, aby połączyć się z serwerem SQL, lecz nie wysyła nigdzie tak zebranych informacji. Najprawdopodobniej połączenie z bazą jest mu potrzebne do ustalenia najbliższych celów ataku, czyli innych systemów korzystających z PCS 7. Właściwa procedura niszcząca aktywowana jest w chwili znalezienia przez „szkodnika" plików konfiguracyjnych o rozszerzeniach .S7P i .MCP, których obecność świadczy o działającym systemie sterowania automatyką. W celu przejęcia kontroli nad PLC i tym samym częstotliwością pracy wirówek, Stuxnet przejmuje komunikację z wywołaniami funkcji bibliotecznych obec-

nymi w pliku s7otbxdx.dll. W ten sposób, niezależnie od poleceń operatora czy skryptu, do urządzeń trafiają komendy nakazujące inny przebieg pracy.

Końcową fazą działania wirusa jest infekowanie nośników podłączanych do komputera. Krok ten podejmowany jest również wtedy, gdy w systemie nie wykryto oprogramowania sterującego linią przemysłową. Dodatkowo wirus próbuje dyskredytować zabezpieczenia systemów Windows znajdujące się w sieci lokalnej, wykorzystując w tym celu kilka usterek, z których jedna była w czasie jego aktywności wcześniej nieznaną luką typu 0-day. Poza przyjmowaniem poleceń od operatorów, Stuxnet tworzy też sieci P2P, aby kodowi infekującemu nie zagroził pojedynczy punkt awarii.

Podsumowanie

Fakt, że Stuxnet znał i potrafił wykorzystać przynajmniej 4 podatności typu 0-day, świadczy o jego sile. Luki tego typu to usterki bezpieczeństwa, które są w danym czasie nieznane nie tylko specjalistom z zakresu bezpieczeństwa, lecz także producentom oprogramowania. Za odnalezienie błędu zabezpieczeń, który nie został dotąd opublikowany, firmy zajmujące się bezpieczeństwem płacą wysokie honoraria. Nie tylko one są zainteresowane zakupem takich podatności, chęć wyrażają również organizacje przestępcze, których działanie opiera się o technologie informacyjne, np. RBN[323].

Stworzenie Stuxneta to również koszty, na które domorosły twórca szkodliwego oprogramowania nie mógłby sobie pozwolić. Autor lub autorzy wirusa musieli zbudować analogiczną do infekowanych linię produkcyjną i odseparowaną od publicznych podsieci infrastrukturę komputerową, aby przeprowadzać serie testów. Wspomnieć należy też o kosztach operacyjnych polegających na kradzieży kluczy z siedzib popularnych firm zajmujących się tworzeniem oprogramowania.

Łącząc wszystkie fakty, trudno oprzeć się wrażeniu, że Stuxnet wyprodukowała organizacja, której zasoby pozwalają na prowadzenie międzynarodowych operacji i tworzenie ćwiczebnych laboratoriów eksperymentalnych. Organizacja ta musiała również posiadać dostęp do zamkniętej wiedzy inżynierskiej firmy Siemens, aby na jej podstawie wyposażyć „szkodnika" w odpowiednie procedury niszczące. Biorąc pod uwagę efekty działań robaka, który z powodzeniem zakłócił prace wybranych instalacji w Iranie, należy stwierdzić, że jego przypadkowe wytworzenie przez pasjonatów czy pospolitych cyberprzestępców jest wysoce nieprawdopodobne. Z drugiej strony koszty ewentualnej interwencji wojskowej, której celem byłoby uszkodzenie irańskich wirówek do wzbogacania uranu, byłyby –

[323] RBN (skrót od Russian Business Network) – organizacja o charakterze przestępczym specjalizująca się w wytwarzaniu złośliwego oprogramowania, kradzieży tożsamości, atakach DDoS, itp.

uwzględniając sytuację geopolityczną – znacznie większe niż te związane z wywiadem i stworzeniem komputerowego programu, który sam się powiela.

Protection against Nuclear Attacks Using Computer Worms on the Example of Iranian Nuclear Infrastructure

Abstract: In July 2009, the IT system controlling the uranium enrichment process in Iranian nuclear facility at Natanz was infected by a computer worm called Stuxnet. It is estimated that the losses inflicted by the worm, mainly consisting in intelligent modification of configuration parameters of enrichment centrifuges, could have slowed down the Iranian nuclear programme for even two years.

Therefore it is justifiable to make a thesis that the defence of the state in the computerized and constantly technologically developing world will not be exclusively based on conventional armed forces but it will more often depend on the IT base of the state and the cyber army taking advantage of it.