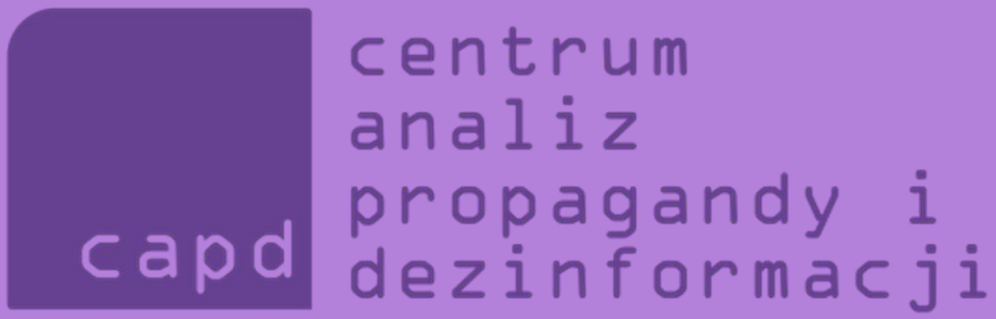
2017

ANALIZA: Wanna Cry Ransomware jako potencjalne narzędzie propagandy i dezinformacji



AUTOR ARTYKUŁU:
Maciej Ostasz

FUNDACJA CENTRUM ANALIZ PROPAGANDY I DEZINFORMACJI | MAJ 2017

W drugi weekend maja br. byliśmy świadkami największego w historii cyfrowego świata globalnego ataku hakerskiego wymierzonego bezpośrednio w serwery i urządzenia końcowe. Ilość zainfekowanych maszyn oraz straty jakie wygenerował przestój związany z cyberatakiem liczony jest w setkach tysięcy dolarów.

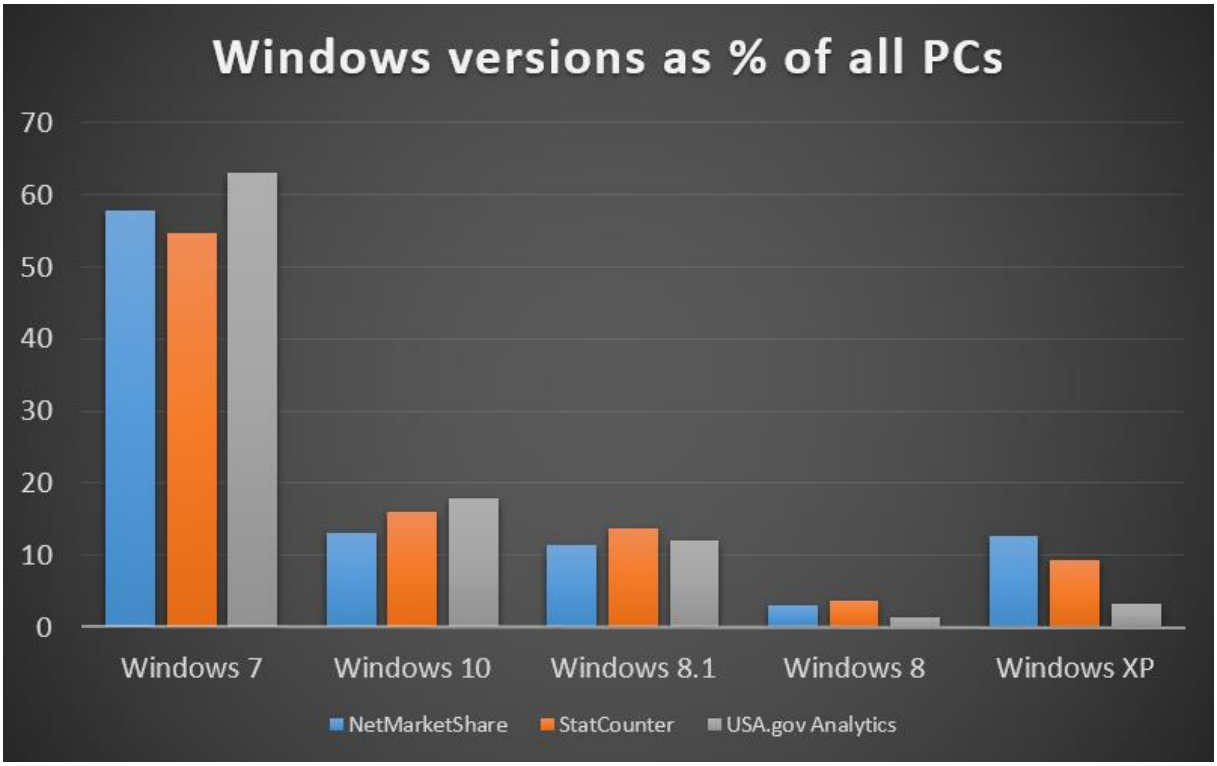
Atak był wymierzony głównie w sektor przemysłowy i instytucje publiczne, ale jak wynika z licznych informacji pojawiających się od tego czasu, w jego wyniku ucierpiało również wiele osób prywatnych. Oczywistym jest, że można było go uniknąć lub co najmniej zminimalizować skalę ataku. Nie miałby on bowiem tak dużego zasięgu, gdyby wszystkie komputery i serwery na świecie miały zainstalowane systemy z aktualnym wsparciem i poprawkami bezpieczeństwa oraz były odpowiednio zabezpieczone. Kolejnymi ważnymi aspektami ataku jest to, kto za niego odpowiada oraz na ile uda się zmodyfikować narzędzia wykradzione z NSA, a także jak bardzo może to wpłynąć na zarządzanie informacją w przestrzeni publicznej.

EternalBlue alias WannaCrypt 2.0

Zagrożenie, które w połowie maja pojawiło się w sieci to zmodyfikowane narzędzia NSA wykradzione co najmniej miesiąc temu z serwerów amerykańskiej agencji. Kod wirusa, który prawdopodobnie powstał do celów inwigilacyjnych systemów z rodziny Microsoft Windows, został zmodyfikowany przez hakerów w taki sposób, by można było w pełni kontrolować zainfekowane urządzenie. Czym jest ransomware można przeczytać w wielu publikacjach dostępnych na ten temat w sieci, lecz warto w tym miejscu zwrócić uwagę na jeden ważny aspekt tego zagrożenia, a mianowicie, co zostało zaatakowane w początkowej fazie.

Atak nie był wymierzony w konkretne instytucje czy przedsiębiorstwa. Został skierowany globalnie we wszystkich w taki sposób, aby dotknął firmy, instytucje i organizacje państwowe oraz osoby prywatne, które zbagatelizowały ważność aktualizacji, zabezpieczeń sieci, sprzętu i własnej infrastruktury. Można powiedzieć, że był to globalny sprawdzian z zakresu bezpieczeństwa. Atak najbardziej dotkliwy okazał się dla firm korzystających z systemów serwerowych Windows Server 2003, Windows Vista i XP, które zostały pozbawione wsparcia ze strony producenta w normalnym cyklu życia oprogramowania. Koniec wsparcia dla tych systemów, choć kilkukrotnie przesuwany, stał się faktem 8 kwietnia 2014 r., a dla systemu Windows Vista z zainstalowanym Service Pack 2 nastąpił niespełna miesiąc temu – 11 kwietnia bez wsparcia pozostała wersja Visty bez SP2, podobnie jak XP.

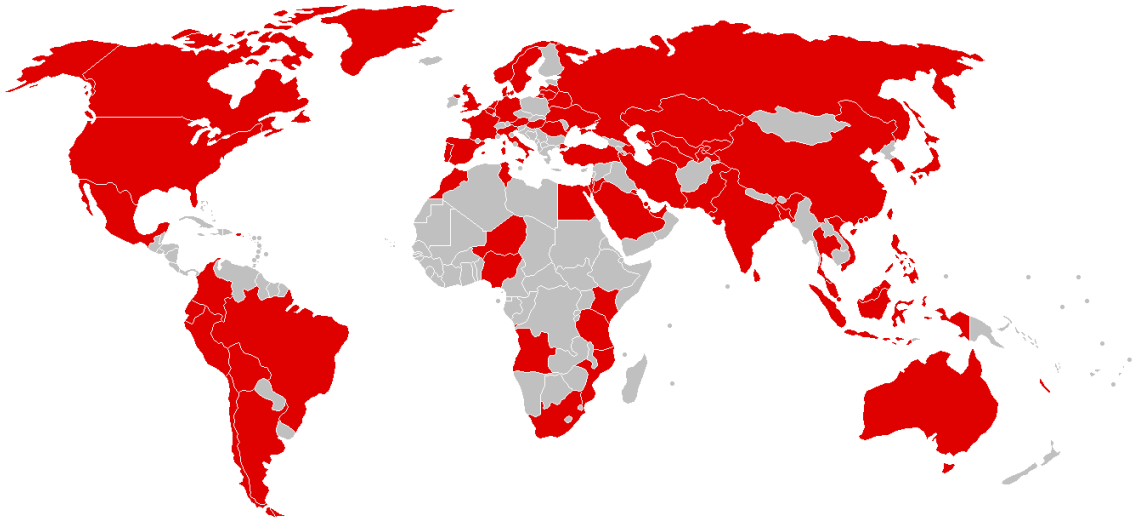
Możliwość przeprowadzenia podobnego ataku była do przewidzenia, gdyż liczne statystyki popularności systemów operacyjnych nie pozostawiają złudzeń jak wiele maszyn opartych o starsze wersje oprogramowania nadal pracuje w sieci Internet.



Popularność systemów operacyjnych rodziny Windows. Stan na styczeń 2016 | Źródło: zdnet.com

Z danych opublikowanych na portalu Zdnet.com wynika, że liczba komputerów klasy PC z zainstalowanym jednym z systemów rodziny Windows to 1,5 miliarda sztuk. Dane te pochodzą z początku 2016 roku i pokazują jak silnym graczem na rynku oprogramowania jest firma Microsoft. Warto zwrócić uwagę na ilość komputerów opartych o system Windows XP. Z przedstawionych danych szacunkowych średnia to 9,4% wszystkich komputerów opartych o produkty Microsoftu. Na podstawie ogólnej ilości wiadomo, że na całym świecie aktywnych maszyn opartych o ten system jest ok. 140 milionów sztuk. Komputery z zainstalowanym Windowsem XP użytkowane są głównie w firmach i instytucjach, gdzie problemem jest przejście na nowe architektury systemów z powodu oprogramowania, które nie jest kompatybilne z nowszymi wersjami Windowsa. Najlepszym dowodem na to są bankomaty, które w większości oparte są właśnie o system Windows XP. O skali problemu może świadczyć chociażby fakt, iż Microsoft z własnej inicjatywy wydał aktualizacje bezpieczeństwa dla niewspieranych już systemów. Firma z Redmond najlepiej zdaje sobie sprawę z powagi sytuacji, gdyż posiada najdokładniejsze dane na temat ilości używanych komputerów z zainstalowanym systemem Windows i Windows Server.

Atak ten pokazał również na jak niskim poziomie znajduje się infrastruktura teleinformatyczna firm i instytucji publicznych. Brak modernizacji kluczowych elementów sieci, jakimi są węzły i serwery, spowodowała rozprzestrzenienie się wirusa na wiele maszyn i infekcję samych serwerów. Regionalne oddziały ministerstwa spraw wewnętrznych Rosji, policja w Chinach czy hiszpański operator Telefonica – to zaledwie kilka krytycznych przykładów przeprowadzonego ataku.



Mapa ataku WannaCrypt 2.0 |Źródło: Wikipedia |Autor: Roke | Licencja CC0

Wpływ funduszy unijnych

W Internecie pojawiło się wiele znaków zapytania odnośnie tego, dlaczego do ataku nie doszło w Polsce a infekcja aplikacją WanaCrypt0r 2.0 nie spowodowała w naszym kraju zastojów i problemów komunikacyjnych. Aby odpowiedzieć na pytanie dlaczego Polska, podobnie jak i kilka innych krajów Europy nie zostały objęte zagrożeniem, należy zwrócić uwagę na jeszcze jeden kraj, który również nie został zainfekowany, a jest mocnym wykładnikiem cyberbezpieczeństwa w całej Wspólnocie. Mowa o Estonii, która po wydarzeniach z 17 maja 2007 r. całkowicie zmodernizowała swoją infrastrukturę teleinformatyczną, uszczelniła systemy i postawiła na innowacje, tak bardzo promowane w całej UE oraz mocny CERT (ang. Computer Emergency Response Team).

W przypadku Polski ta innowacyjność była rozwijana latami wraz z uczestnictwem w projektach Unii Europejskiej. W wielu przypadkach modernizacji infrastruktury lub przy realizacji nowych projektów publicznych i komercyjnych, pojawiały się pomówienia o niegospodarność i nieprawidłowe użytkowanie funduszy unijnych na technologie, które są drogie i nie będą w pełni wykorzystywane, przez co nie będą spełniać swojej funkcji. Zapewne nikt nie spodziewał się, że rzekomy „przerost formy nad treścią", czyli potencjalnie przeinwestowana infrastruktura teleinformatyczna, okaże się funkcjonalnym zabezpieczeniem na poziomie państwowym i prywatnym, co przyczyniło się do zauważalnego, niskiego stopnia zagrożeń zewnętrznych.

Postawienie na częste modernizacje i aktualność krytycznej części infrastruktury teleinformatycznej w Polsce i Estonii pokazuje, zwłaszcza na tle reszty świata, jak ważne jest dbanie o aktualne, a zarazem bardzo dynamiczne standardy, które w bezpieczeństwie technologii informacyjnych odgrywają kluczową rolę. Patrząc na mapę infekcji udostępnioną przez Wikipedię, doskonale widać, że wspomniane wcześniej programy innowacyjności oferowane przez UE przyniosły podobne korzyści także innym państwom, które dołączyły do Unii po 2004 roku.

Windows Server 2003 a nowi członkowie UE z 2004 roku i Rosja

Okazuje się, że istnieje oczywista zależność pomiędzy serwerowym systemem Microsoftu a członkostwem w Unii Europejskiej, która miała decydujący wpływ na to czy dane państwo unijne zostało zainfekowane podczas omawianego ataku. Polska, podobnie jak pozostałe kraje, które dołączyły do UE w 2004 roku, rozpoczęła pobieranie dotacji.

Należy podkreślić, że rozwój technologiczny krajów byłego Układu Warszawskiego nie byłby możliwy bez finansowego wsparcia ze strony Unii. Polska, Czechy i Słowacja to kraje, które dosyć prężnie walczą o względy zagranicznych firm i inwestorów, co też wpływa na jakość krajowych usług oferowanych m.in. przez dostawców rozwiązań teleinformatycznych. Większość środków przeznaczonych na budowę i modernizację infrastruktury teleinformatycznej na terenie RP, pochodziła z dotacji przewidzianych na lata 2007-2013 i zostały wydzielone z programów Infrastruktura i Środowisko, Innowacyjna Gospodarka i Rozwój Polski Wschodniej. Plany i wnioski składane w 2007 r. były realizowane w kolejnych latach, a co za tym idzie budowa i modernizacja krytycznej i niekrytycznej infrastruktury teleinformatycznej była realizowana od roku 2008. W tym samym roku pojawiła się kolejna odsłona systemu Windows Serwer, oznaczona jako 2008. Warto nadmienić, że starzy

członkowie Unii najprawdopodobniej nie skorzystali z dotacji na kolejne modernizacje infrastruktury teleinformatycznej i pominęli ten krok, bagatelizując zagrożenia z powodu stabilności działania wcześniej wdrożonych procesów. To samo dotyczy podmiotów komercyjnych, ale w ich przypadku należy wziąć pod uwagę fakt, że rozprzestrzenienie się robaka jakim jest WanaCrypt0r 2.0 w znacznej mierze zależało od stanu zabezpieczeń i aktualizacji infrastruktury krytycznej, w tym węzłów komunikacyjnych. Kraje, które podniosły poziom zabezpieczeń i postawiły na modernizację, nie odczuły konsekwencji tego ataku i najprawdopodobniej uchroni je to lub przynajmniej zminimalizuje skutki przyszłych zagrożeń.

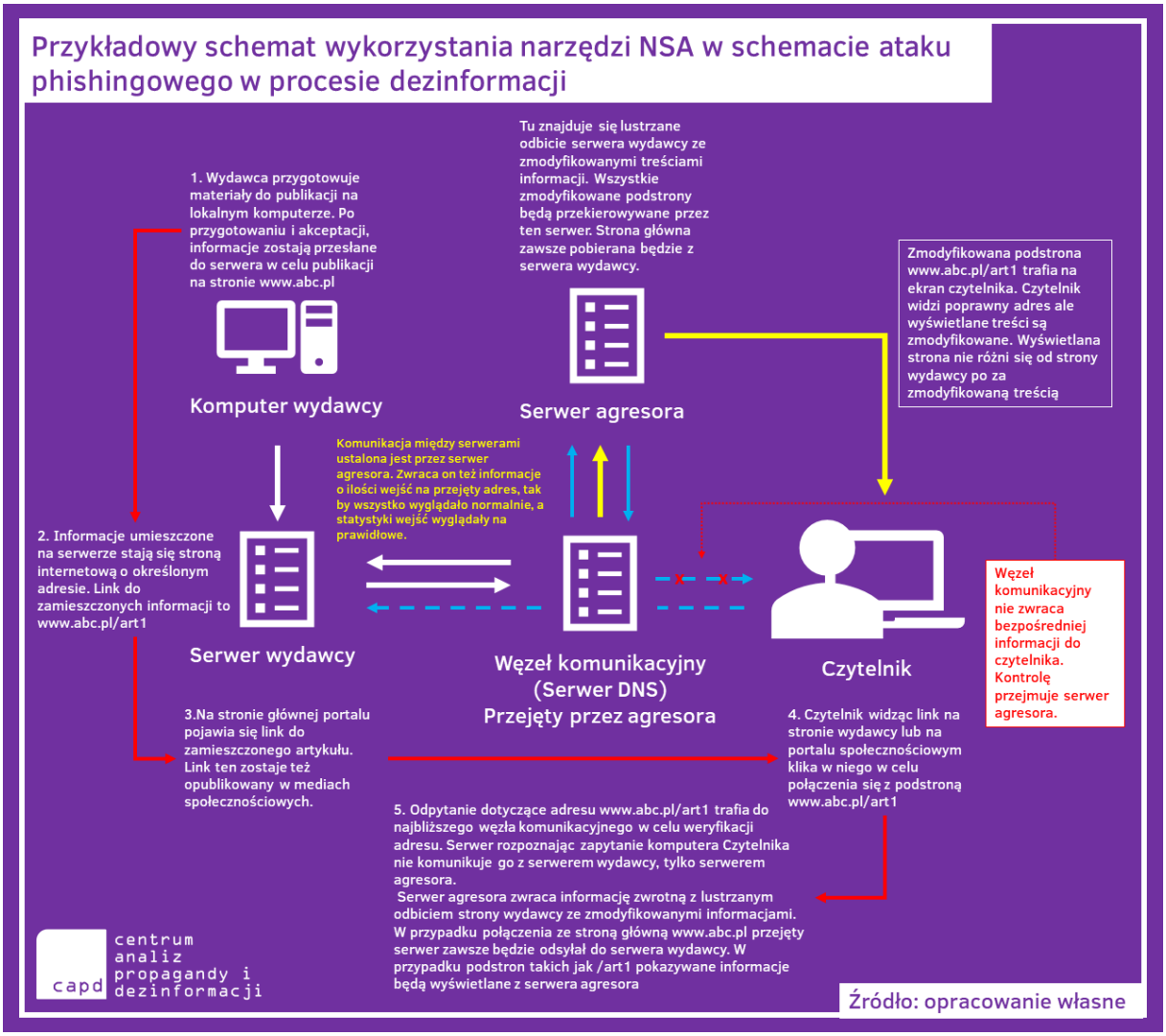
Inną ważną obserwacją po przeprowadzonym ataku jest stan infrastruktury informacyjnej Federacji Rosyjskiej. Rosyjskie ministerstwo spraw wewnętrznych zostało zaatakowane infekcją, która w jakiś sposób musiała przeniknąć do intranetu resortu. Ten fakt świadczy o tym, że serwery zarządzające ruchem sieciowym oparte są o przestarzałą i niemodernizowaną strukturę, a cały urząd pracuje głównie na komputerach opartych o Windows XP. Pomimo iż sam system operacyjny jest podatny na ataki, jego infekcja zależy w dużej mierze od sieci do jakiej jest podłączona dana maszyna.

Problemem, który pośrednio przyczynił się do tak dużej skali infekcji, jest szeroko rozumiany proces technologiczny. Na proces ten składa się wiele czynników, które muszą ze sobą współgrać, by założony łańcuch zdarzeń działał prawidłowo. Wspomniane wcześniej bankomaty nadal oparte są o Windowsa XP z powodu mechanizmów współpracujących z serwerami bankowymi. Ze względu na zmianę architektury późniejszych wersji Windowsa, migracja do kolejnych wersji systemów była niemożliwa, a instytucje i firmy czekały do końca obowiązywania wsparcia tego systemu bez pracy nad nowym procesami czy systemami integracji. Współdzielone mechanizmy przetwarzania informacji, czyli proces technologiczny komunikacji klient-serwer dla systemów bankowych nie były również modernizowane z powodu dużej stabilności działania. To również przyczyna, dlaczego aktualizacja procesów przetwarzania informacji nie była realizowana, przez co kluczowy element infrastruktury banków został złamany. Przykład ataku na bankomaty to tylko pewien schemat, który można odwzorować w każdej firmie i każdej instytucji, która korzysta z przestarzałych technologii. Ten sam schemat procesu technologicznego przetwarzania informacji można podpiąć dla hiszpańskiego telekomu Telefonica, niemieckich kolei Deutsche Bahn czy brytyjskiej służby zdrowia. Dawno temu wdrożone standardy nie były modernizowane, co przyniosło fatalny efekt.

Teraz ransomware potem mirroring – nowe narzędzie dezinformacji

Przeprowadzony atak to tylko jedna z części potencjalnie znacznie większego problemu. Tak naprawdę oficjalnie do końca nie wiadomo jakie są możliwości wykradzionych narzędzi stworzonych przez NSA. Z informacji które dostępne są obecnie w sieci wiadomo, że za ich pomocą można przejąć kontrolę nad danym urządzeniem. Istnieje możliwość, że oprogramowanie to może zostać wykorzystane jako narzędzie dezinformacyjne, które mogłoby działać według następującego schematu. Udział w nim brałyby 3 strony: wydawca informacji, czytelnik i agresor. W momencie, gdy wydawca opublikowałby informację, którą agresor chciałby zatuszować lub zmanipulować zamieszczony tekst, mógłby za pomocą tych samych narzędzi, które zostały użyte do stworzenia WannaCrypt 2.0 zmienić serwer docelowy i przekierować wszystkie połączenia z witryny wydawcy do lustrzanego odbicia strony, gdzie zamieszczone informacje byłyby zmodyfikowane. Czytelnik ze swojej strony nie zauważyłby różnicy, a wydawca nie byłby świadomy takiego zajścia do momentu, kiedy ktoś nie poinformowałby

za pomocą np. mediów społecznościowych, że odczytana informacja jest podejrzana. Jak dokładnie miałby działać mechanizm oparty o kod NSA przedstawia poniższy schemat.



Przedstawiony schemat w dużej mierze bazuje na schemacie ataku phishingowego, polegającego na podszywaniu się pod konkretną stronę internetową w taki sposób, aby osoba zaatakowana nie zauważyła różnic pomiędzy stroną oryginalną a wyłudzającą informacje. Metoda ta jest obecnie stosowana do pozyskiwania informacji dotyczących dostępu do kont bankowych. W przypadku przedstawionego schematu ofiarą jest potencjalny czytelnik, który zostałby przekierowany do lustrzanego odbicia strony z kompletnie inną treścią.

Istnieje bardzo duże prawdopodobieństwo wykorzystania tych narzędzi do wojny hybrydowej. Przeprowadzony atak z całą pewnością stał się punktem zapalnym pokazującym niedoskonałości świata cyfrowego. Nie wiemy co i w jaki sposób można zmodyfikować wykradzione narzędzia NSA oraz jak wiele luk bezpieczeństwa jest w oprogramowaniu i systemach operacyjnych, o których wiedzą tylko pracownicy agencji oraz hakerzy mający dostęp do tajemnicy agencji. Aby zapewnić najwyższy poziom bezpieczeństwa instytucjom państwowym, podmiotom prywatnym oraz całej krytycznej

infrastrukturze organizacja bezpieczeństwa powinna być złożona, skoordynowana i składać się z następujących elementów:

- modernizacja lub wymiana urządzeń na nowe, współpracujące z systemami operacyjnymi posiadającymi pełne wsparcie producenta i twórców oprogramowania dodatkowego;
- modernizacja serwerów i całej krytycznej infrastruktury publicznej i prywatnej, poprzez usuwanie urządzeń niespełniających standardy bezpieczeństwa oraz posiadające krytyczne luki bezpieczeństwa;
- w przypadku braku możliwości wymiany lub modernizacji urządzeń końcowych należy zadbać o bezpieczeństwo na głównych węzłach komunikacyjnych oraz o aktualizacje na serwerach, szczególnie tych odpowiedzialnych za zarządzanie siecią;
- kooperacja i współpraca ze służbami bezpieczeństwa, zgłaszanie incydentów do NASK, CERT oraz Ministerstwa Cyfryzacji w przypadku dużych i masowych incydentów.

Wnioski

W wielu mediach cyfrowych i analogowych można było przeczytać nagłówki mówiące o ogromnej skali przeprowadzonego ataku i nadaniu mu miana największego w historii rewolucji cyfrowej. Większość autorów publikowanych informacji najprawdopodobniej nie posiada wiedzy o tym, że przeprowadzony atak w skali globalnych infekcji jest jednym z mniejszych pod względem zasięgu, nie mniej jednak z całą pewnością najpoważniejszym w historii. Najbardziej globalne infekcje zostały wykryte w latach 2008, 2011 i na czas ich działalności mogły stanowić dużo większe zagrożenie niż zmodyfikowane narzędzia NSA. Botnety Metulji i Mariposa, które po słoweńsku i hiszpańsku oznaczają motyla, zainfekowały ponad 10 milionów komputerów każdy, co pokazuje jak nisko w globalnym rankingu stoi WannaCrypt 2.0.

Botnet to wrusowy mechanizm łączący komputery w grupy w taki sposób, aby użytkownicy nie byli świadomi wykorzystania ich maszyn do niepożądanych operacji. O sprzęcie, który został zainfekowany wirusem łączącym go z botnetem mówi się, że to komputer-zombie. Głównym zadaniem zainfekowanych maszyn, było spamowanie skrzynek mailowych, a w grupach służyły do ataków DDoS. Atak ten polega na jednoczesnym wysłaniu dużej ilości zapytań, np. adresu strony internetowej, co powoduje zablokowanie dostępu do serwera z powodu zbyt dużej ilości operacji do wykonania przez serwer. Wiele publikacji nawiązujących do ataku na Estonię opublikowanych w latach 2009-2013 odnosi się do wykorzystana zasobów botnetu Metulji i przyczynienia się do stagnacji krytycznej infrastruktury kraju.

Opisane wcześniej wpływy efektów unijnych dotacji na państwa, które dołączyły w 2004 roku do Unii Europejskiej, mają ogromne znaczenie i widać to do chwili obecnej, chociażby na przykładzie infrastruktury sieci telefonii komórkowej. Polska jako jeden z nielicznych krajów Unii posiada ponad 90% pokrycia kraju zasięgiem, dostęp do mobilnego Internetu oscyluje w graniach 75%, co na tle starych członków UE jest miażdżącym osiągnięciem. Przykład Włoch, w których powiedzenie „im dalej na południe, tym gorzej" doskonale pokazuje podejście do odpowiedniego gospodarowania i rozwoju technologicznego. Problem z działaniem telefonów, niski transfer danych czy widoczny niski poziom rozwoju technologicznego wzdłuż autostrady A1 (tzw. „autostrady słońca" czyli najpopularniejszego, lecz i najbardziej obciążonego ciągu komunikacyjnego w tym kraju), wyraźnie pokazuje podejście starych członków Unii. Pomimo tego, że Włochy są jedną z technologicznych potęg, to mają poważny problem z rozwijaniem bezpiecznej infrastruktury teleinformatycznej.

Wracając do ataku, warto przyjrzeć się temu co wydarzyło się w Niemczech. Atak na Deutsche Bahn doskonale obrazuje problem modernizacji procesu technologicznego zarządzania informacją. Mechanizmy zarządzania infrastrukturą kolejową, stworzone lub zmodernizowane w latach 2000-2005, nie przeszły konstruktywnej modernizacji w późniejszym okresie, co doprowadziło do patowej sytuacji, w której system zarządzania został złamany.

Biorąc pod uwagę skalę komputerów z przestarzałym oprogramowaniem działających w instytucjach państwowych, podmiotach komercyjnych i prywatnych, należy liczyć się z kolejnymi atakami. System Windows XP został wydany 15 lat temu. Otrzymał w tym czasie 3 duże aktualizacje Service Pack, ale dalej jest oprogramowaniem niedoskonałym, które dodatkowo utraciło wsparcie ze względu na rozwój nowych rozwiązań. Kurczowe trzymanie się go może oznaczać w przyszłości zmasowany atak na struktury organizacyjne za pomocą nieznanych luk bezpieczeństwa.

Jeszcze jednym ważnym globalnym problemem związanym z działaniami zapobiegającymi masowym atakom są przepisy prawa. Bardzo często nie są one dostosowane do danego poziomu rozwoju technologicznego, przez co w wielu przypadkach okazuje się, że wprowadzane ustawy i rozporządzenia nie są już aktualne w stosunku do technologii. Rynek urządzeń cyfrowych zmienia się z kwartału na kwartał. Ze względu na obecne uwarunkowania społeczno-ekonomiczno oraz dynamiczne zmiany na rynku urządzeń i oprogramowania władze wszystkich krajów świata powinny stworzyć uniwersalne, globalne regulacje dotyczące standaryzacji i zasad bezpieczeństwa globalnej sieci Internet. Regulacje te powinny ogólnikowo określać w jaki sposób powinny być przeprowadzane modernizacje krytycznej infrastruktury i narzucać okresy obligatoryjnych modernizacji. Zapewnienie najnowszych rozwiązań w sektorze teleinformatycznym na poziomie globalnym, pozwoliłoby na ograniczenie ryzyka ataków skierowanych na cały świat do minimum.