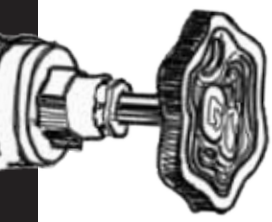
2/2016

FUNDACJA bezpieczna cyberprzestrzeń



zawór bezpieczeństwa 2/2016

Czy twoje hasło jest na tej liście?

Firma SplashData wydała piąty raport z „listą najgorszych haseł". Lektura ma zachęcić użytkowników do większej refleksji nad bezpieczeństwem dostępu do różnych serwisów, z których korzystają. Raport powstał na bazie ponad 2 milionów haseł, które wyciekły w ciągu ostatniego roku.

Raport pokazuje jak bardzo użytkownicy ryzykują. Choć z roku na rok na liście debiutują coraz dłuższe hasła, niekoniecznie oznacza to, że są bezpieczniejsze. Od lat prym wiodą hasła numeryczne, najłatwiejsze do zgadnięcia przez przestępców – w pierwszej dziesiątce jest ich aż sześć. Na miejscu pierwszym i drugim nie ma niespodzianki – od 2011 roku królują hasła „123456" oraz „password".

Wśród pozostałych najczęstszym tematem haseł jest sport: na 7 miejscu mamy football, a na 10 baseball. Przebiły się też „starwars", „princess", „solo". Hasła, które debiutują to „welcome", „login", „passw0rd". Chcecie poznać cały ranking? Czy odważycie się sprawdzić swoje hasło z listą? Od razu podpowiemy, że na listę nie załapał się polski klasyk „admin".

Ranking haseł:

1	123456	8	1234
2	password	9	1234567
3	12345678	10	baseball
4	qwerty	11	welcome
5	12345	12	1234567890
6	123456789	13	abc123
7	football	14	111111
15	1qaz2wsx		
16	dragon		
17	master		
18	monkey		
19	letmein		
20	login		
21	princess		
22	qwertyuiop		
23	solo		
24	passw0rd		
25	starwars [1]		

Nie dla selfie w pracy!

Rządy wielu państw są zatroskane bezpieczeństwem swojej infrastruktury krytycznej, zwłaszcza po ostatnim cyberataku, który odciął od prądu prawie 80 tysięcy gospodarstw domowych na Ukrainie.

Tymczasem eksperci ds. cyberbezpieczeństwa ostrzegają, że zarządzający obiektami o kluczowym znaczeniu, jak elektrownie, stacje uzdatniania wody czy obiekty przemysłowe, powinni równie mocno martwić się poczynaniami swoich pracowników na Instagramie czy Facebooku.

Eksperci przestrzegają, że zdjęcia selfie z różnych miejsc pracy mogą być rajem dla hakerów. Nierzadko bowiem dostarczają szczegółowych informacji nt. infrastruktury krytycznej. Sean McBride, starszy analityk z firmy iSight Partner badał temat, wśród zdjęć, które znalazł w mediach społecznościowych

były na przykład selfie w tle z infrastrukturą nadzoru i systemami SCADA (systemy oprzyrządowania, automatyki i kontroli).
„Dość selfies ze SCADA!", apelował McBride na konferencji w Miami. „Nie ułatwiajcie zadania przeciwnikom."
W sieci znaleźć można wiele zdjęć z miejsc, które raczej wypadałoby trzymać poza wzrokiem osób postronnych jak np. zdjęcia panoramiczne pokojów kontroli i filmiki z różnych obiektów z infrastrukturą krytyczną. Obrazu pomagają dopełnić informacje ze stron korporacyjnych, takie jak diagramy organizacji, listy pracowników czy kontakty. Historie ataków, przy których wykorzystano tego typu informacje, wcale nie są wyssane z palca. Fotografie opublikowane w 2008 roku przez biuro prasowe byłego prezydenta Iranu Mahmouda Ahmadinejada dostarczyły zachodnim analitykom nuklearnym szczegółów na temat wnętrz ośrodka nuklearnego Natanz oraz operacji wzbogacania uranu. W 2011 roku jeden z ekspertów wykorzystał zdjęcie monitora kontroli systemu SCADA aby zaatakować obiekt złośliwym oprogramowaniem. McBride sugeruje, aby zarządzający infrastrukturą krytyczną zanim upublicznią cokolwiek spróbowali pomyśleć jak hakerzy: „Zapytaj siebie. Co moi przeciwnicy wiedzą o mnie i organizacji, którą wspieram?".
Póki co James Bond zaciera ręce, nie będzie musiał już podróżować, swoje misje zrealizuje z sukcesem przeczesując Internet. [2]

Kamera na straży bezpieczeństwa? Nic bardziej mylnego!

Myślałeś, że zamontowanie w domu kamery gwarantuje bezpieczeństwo? Możesz być w błędzie. Paradoksalnie – kamera może wręcz narazić cię na dodatkowe zagrożenia. Jak to możliwe? Urządzenia typu IoT (czyli Internet przedmiotów) są łatwym celem dla hakerów. Już jakiś czas temu rynek zdobyły kamery, z których obraz można podglądać za pomocą aplikacji mobilnej. Eksperci z firmy NowSecure wzięli pod lupę kilka typów takich urządzeń, m.in. Vimtag Fujikam 361 HD, Zmodo PKD-DK4216, LaView LV-KDV0804B6S, Best Vision Systems SK-DVR-DIY. Ich wnioski nie pozostawiają cienia wątpliwości: w temacie bezpieczeństwa producenci kamer mają jeszcze wiele do nauczenia się. „Każde połączenie kamery z aplikacją, które testowałem miało co najmniej jedną lukę bezpieczeństwa, która mnie zaniepokoiła. Jest wiele modeli kamer, niemożliwe było przetestowanie wszystkich" – napisał Jake Van Dyke z NowSecure. Najczęściej występującym błędem było przesyłanie i przechowywanie wrażliwych danych w zwykłych plikach tekstowych. „Byłem zszokowany i rozczarowany jednocześnie jak łatwo włamać się komuś do konta" – dodaje. Aplikacje komunikują się z serwerami za pomocą nieszyfrowanych kanałów: hasła, adresy mailowe, tokeny są w zwykłych plikach XML. Ekspert wykazał, że hakerzy mogą w łatwy sposób manewrować przy różnych funkcjach kamery, takich jak nagrywanie audio i video, zmieniać ustawienia, sformatować kartę SD oraz uzyskać dostęp do zapisanych nagrań. Dodatkowo, okazało się, że klucz WPA2 jest archiwizowany na serwerze i łatwo dostępny dla wszystkich atakujących.
Póki co pozostaje czekać aż producenci wprowadzą usprawnienia i liczyć na to, że streaming z naszej posiadłości nie trafił jeszcze do sieci. [3]

Rozpal ogień

W oddalonym od osad ludzkich miejscu w regionie Neuenkirchen w Niemczech leży głaz. Z zewnątrz wygląda jak zwykła skała. Jednak tylko z pozoru. Tak naprawdę to zaawansowany projekt artystyczny o nazwie „Keepalive", jego twórcą jest artysta Aram Bartholl, który w 2015 roku wykonał pracę na zlecenie Centrum Kultury Cyfrowej uniwersytetu w Lüneburgu, w ramach jednego z projektów europejskich.
W głazie Bartholl zamontował termoelektryczny generator, który zmienia ciepło w prąd oraz router.

Po rozpaleniu przy skale ognia oba urządzenia aktywują się, umożliwiając odwiedzającym instalację, dostęp do pokaźnej cyfrowej biblioteki – poradników survivalowych w pdfach, które są przechowywane na USB podłączonym do skały. Goście mogą też wrzucać swoje pliki. Router nie jest podłączony do internetu, jest włączony tak długo jak długo ogień dostarcza wystarczającą ilość ciepła. Sam kamień jest przekaźnikiem danych, ale „bez ognia projekt staje się bezużyteczny. Potrzeba ognia. O to w tym wszystkim chodzi", wyjaśnia Bartholl.
Artysta tworzy prace z pogranicza internetu, rzeczywistości i kultury. Jeden z jego wcześniejszych projektów z 2010 roku to publiczne punkty dzielenia się danymi – seria pod nazwą „Dead drops", w ramach której artysta zainstalował porty USB w ścianach budynków w centrum Nowego Jorku, zapraszając ludzi do ściągania plików.
Dla odmiany wizyta przy głazie „Keepalive" wymaga wiele motywacji i wysiłku, ale można się podczas niej dowiedzieć jak to robiono w czasach kamienia łupanego. Ci którzy wybiorą Bartholla na swojego dostawcę Internetu, będą musieli dodatkowo zadbać o szczególne zabezpieczenia przeciwpożarowe. [4]

Cybermorderstwa? To nie science fiction!

Marie Moe to norweska badaczka, pracowała dla tamtejszego CERTu, obecnie dla niezależnej organizacji badawczej Sintef. Podczas gdy kraje debatują o zabezpieczaniu infrastruktury krytycznej przed cyberatakami, ona zastanawia się na ile bezpieczny jest zainstalowany w jej ciele mały komputerek, utrzymujący ją przy życiu.
Hakerzy nie ustają w poszukiwaniu nowych metod ataku, stąd temat bezpieczeństwa rozruszników serca jest jak najbardziej na czasie. Przy pierwszym rozruszniku Moe ściągnęła z sieci manual, po przeczytaniu którego zorientowała się, że ma on nie jeden, ale dwa bezprzewodowe interfejsy. Pierwszy umożliwia lekarzowi dostosowanie ustawień rozrusznika, a drugi pozwala urządzeniu dzielić się dziennikami danych przez internet. Wtedy też dobitnie do niej dotarło, że niektóre serca stały się częścią Internetu przedmiotów.
Pierwsze doniesienia o możliwych atakach na rozruszniki pojawiły się w 2008 roku po eksperymencie naukowców z Uniwersytetu w Michigan. W 2012 roku Barnaby Jack zademonstrował jak zniszczyć rozrusznik przy pomocy 830-voltowych wstrząsów. Eksperymenty przeprowadzano też na pompach insulinowych. Obawy wśród opinii publicznej zostały zasiane. Były wice prezydent USA, Dick Cheney ogłosił, że z obawy o bezpieczeństwo zdecydował się wyłączyć w rozruszniku funkcje wifi.
Marie Moe bardziej niż hakowania obawia się błędów programistycznych. Krótko po wszczepieniu jej rozrusznika, wchodząc pewnego dnia po schodach w londyńskim metrze, poczuła niewytłumaczalne zmęczenie. Okazało się, że wystąpił problem z maszyną, która sterowała jej ustawieniami w rozruszniku. Moe chciałaby, aby tak wrażliwe urządzenia były poddawane większej ilości testów przez strony trzecie. Trudno jednak znaleźć kompromis między producentami chcącymi chronić swoją własność intelektualną a ambicjami badaczy. „To komputer, który zarządza moim sercem, więc naprawdę musze mu ufać", mówi. Cybermorderstwa to istotnie przerażająca wizja eliminacji przeciwników. Wydaje się, że producenci nie mają na co czekać i powinni ruszać z firewall'ami specjalnie skrojonymi na rozruszniki. [5]

Banan rozdziela hasła wifi

W większości biur przychodząc na spotkanie służbowe po hasło do wifi udajesz się na recepcję. Zapisujesz je lub dostajesz od recepcjonistki gotową karteczkę z kodem. W tym po prostu naciskasz banana

później przez 8 godzin możesz spokojnie surfować. Nie, to nie żart. Duński inżynier sieciowy Stefan Milo zbudował swój owocowy system generacji kodów do wifi podłączając banana do tablicy sterowniczej Makey Makey i platformy komputerowej Raspberry Pi. Wszystko kosztowało mniej niż 100 dolarów i ma być alternatywą do voucherów-karteczek z indywidualnym kodem dla każdego gościa, po który z reguły zgłaszamy się na recepcję.

„Nawet jeśli masz małą drukarkę do voucherów, nadal potrzebna jest recepcjonistka, instalacja drukarki, wsparcie techniczne do sterowników, etc. I nadal potrzebny jest papier. Co to jest? 1999?", pyta Milo.

Działanie projektu jest proste. Duńczyk wygenerował pulę 5 tysięcy haseł, które są przechowywane w Raspberry Pi, połączonym przez USB z tablicą Makey Makey. Ta z kolei jest połączona z bananem. Gość dotyka banana, co powoduje spadek napięcia w owocu, Makey Makey interpretuje to jako naciśnięcie klawisza, następnie wysyła sygnał do Raspberry Pi, co powoduje generowanie vouchera z kodem. Każde hasło starcza na 8 godzin surfowania.

Milo zapewnia, że jego system ma potencjał działać przez lata i obsłużyć tysiące gości.

I w ten sposób banan wkroczył do świata hi-tech. Może to i koniec z drukowaniem voucherów z hasłem, jednak banana od czasu do czasu trzeba będzie wymienić. [6]

[1] http://bit.ly/1RiaM0p
[2] http://bit.ly/1SZFmvl
[3] http://bit.ly/1nY2tLU
[4] http://bit.ly/1QQw6bc
[5] http://bbc.in/1SE8IRT
[6] http://bit.ly/1Sbg2ny

Kolejne numery można śledzić również na serwisie społecznościowym LinkedIn

Zapraszamy do zapoznania się z Raportem Fundacji Bezpieczna Cyberprzestrzeń „Największe Zagrożenia Dla Bezpieczeństwa w Internecie w 2016 Roku".

Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet.

www: https://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo