Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

Skracanie adresów URL / Kody QR

Wstęp

Uniform Resource Locator (lub URL) nie jest niczym więcej niż inną nazwą adresu strony internetowej, na przykład dobrze znanej http://www.google.pl. URL to nazwa którą wpisujesz, kiedy chcesz odwiedzić stronę internetową. Po wpisaniu URLa w pasek adresu w przeglądarce jest on tłumaczony na adres IP, czyli rzeczywiste miejsce, gdzie strona znajduje się w Internecie. Twoja przeglądarka łączy się ze stroną internetową, a następnie pobiera całą jej zawartość, którą potem możesz przeglądać. Problemem jest to, że cyberprzestępcy mogą próbować różnych sztuczek z adresami URL. Mogą na przykład sprawić, że będzie Ci się wydawać, że odwiedzasz prawdziwą witrynę, podczas gdy naprawdę jesteś na zupełnie innej stronie, kontrolowanej przez nich i przeznaczonej do kradzieży informacji, ataku na przeglądarkę albo zainfekowania komputera. To gdzie Ci się wydaje, że się łączysz, a to, gdzie się rzeczywiście łączysz, mogą być dwoma różnymi miejscami w sieci. Przyjrzyjmy się, jak działa URL, poznajmy kilka popularnych ataków związanych z adresami URL oraz zobaczmy jak można się przed nimi zabezpieczyć.

Redaktor gościnny

Dr Eric Cole jest uznanym ekspertem w branży bezpieczeństwa. Jest autorem wielu książek, w tym Advanced Persistent Threat, Hackers Beware i Network Security Bible. Dr Cole jest również założycielem Secure Anchor Consulting, wykładowcą i autorem kursów na wydziale SANS.

Zrozumieć URL

URL to nic więcej niż miejsce przeznaczenia składające się z trzech części. Pierwszą z nich jest protokół, czyli określenie w jaki sposób łączysz się ze stroną internetową. Zwykle jest to HTTP (tekst jawny, tzw. clear text) lub HTTPS (połączenie szyfrowane). Druga część adresu URL to domena, czyli nazwa serwisu internetowego który chcesz odwiedzić. Trzecią częścią jest strona docelowa w tym konkretnym serwisie. Spójrzmy na przykład URLa:

https://www.securingthehuman.org/ouch

Ten adres zaczyna się od HTTPS, co oznacza połączenie szyfrowane. Druga część, www.securingthehuman.org, to strona internetowa, którą się odwiedzi jeśli się kliknie na link. Trzecia część zaczyna się od '/' i wszystko po ukośniku oznacza, jaką dokładnie część wybranego serwisu internetowego chcesz odwiedzić. W tym przykładzie przeszło by się do strony Securing The Human, a następnie zostałoby się przekierowanym do najnowszych stron OUCH. Najważniejszym elementem do zbadania jest druga część adresu URL, czyli domena. Czy to

Skracanie adresów URL / Kody QR

jest naprawdę strona którą zamierzałeś odwiedzić? Zobaczmy jakie triki mogą stosować przestępcy aby wysłać Cię do witryn, które są kontrolowane przez nich.

Skracanie adresów internetowych

Najprawdopodobniej widziałeś już kiedyś skrócony adres URL. Skracanie adresów to usługa, która bierze bardzo długi i złożony adres URL, a następnie skraca go do krótkiej i prostej formy. To ułatwia przesyłanie linków za pomocą różnych kanałów komunikacji, jak e-mail czy różne komunikatory. Taka usługa jest również przydatna, gdy liczba znaków w jakimś miejscu jest ograniczona, tak jak np. na Twitterze lub w wiadomości tekstowej. Przykładami usług skracania adresów URL są m.in. tinyurl.com, bit.ly lub goo.gl. Ryzykiem jakie płynie z korzystania z nich jest to, że po kliknięciu takiego skróconego adresu URL, nie można zobaczyć prawdziwego celu do jakiego on prowadzi. Wtedy przestępcy internetowi mogą zamieszczać skrócony adres URL, który ostatecznie przeniesie Cię do stron internetowych, które są przez nich kontrolowane.

Dla swojego bezpieczeństwa, zanim klikniesz, najpierw sprawdź prawdziwy cel skróconego adresu URL albo kodu QR.

Jednym ze sposobów w jaki można się zabezpieczyć jest sprawdzenie, gdzie skrócony link Cię zaprowadzi, zanim na niego klikniesz. Wiele stron internetowych oferuje usługi, które pozwalają wkleić skrócony adres URL i podejrzeć jego prawdziwe miejsce przeznaczenia (poszukaj przykładów w podrozdziale “Zasoby”). Ponadto niektóre usługi skracające adresy URL dają możliwość podglądu prawdziwego celu. Na przykład, jeśli masz adres z serwisu bit.ly, wystarczy dodać “+” na końcu tego adresu URL, aby podejrzeć prawdziwy cel, tak jak na przykładzie:

http://bit.ly/10hVtvV+

Kody QR

Koncepcja QR kodów jest podobna do koncepcji skracania adresów URL, ale są one przeznaczone dla smartfonów. W tym wypadku adres URL jest przekształcany do obrazu cyfrowego. Przy użyciu specjalnej aplikacji na telefonie komórkowym, można zrobić zdjęcie kodu QR, który następnie otwiera przeglądarkę w Twoim telefonie i zabiera Cię na stronę zakodowaną w kodzie QR. Jednak wiąże się to z tym samym ryzykiem jak w przypadku skróconych adresów URL - pozostajesz zależny od zaufania jakim darzysz konkretny QR kod i nie wiesz dokąd on prowadzi. Powiedzmy, że jesteś na stacji kolejowej lub lotnisku i widzisz plakat reklamujący nowy film. Plakat obiecuje, że jeśli użyjesz smartfona do odczytania kodu QR zostaniesz zabrany do strony

Skracanie adresów URL / Kody QR

ze zwiastunem filmu. Choć plakat jest najprawdopodobniej prawdziwy, każdy przestępca może łatwo podejść do plakatu i przykleić na niego własną naklejkę z kodem QR w miejsce istniejącego. Od tego momentu każde urządzenie, które odczyta kod QR zostanie przekierowane nie na zwiastun filmu, ale na stronę internetową kontrolowaną przez atakującego.

Podobnie jak w przypadku skracania adresów URL, najpierw zawsze sprawdź miejsce docelowe odnośnika. Upewnij się, że Twoja aplikacja czytająca kody QR obsługuje możliwość podejrzenia, gdzie dany skrócony link ma Cię zabrać i daje możliwość zadecydowania, czy rzeczywiście chcesz odwiedzić daną stronę internetową, czy też nie. Jeśli czytnik kodów QR nie daje możliwości podglądu celu znajdź inną aplikację, ponieważ na rynku istnieje wiele darmowych opcji.

Dowiedz się więcej

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Źródła

Skracanie adresów internetowych:	http://pl.wikipedia.org/wiki/Skracanie_adres%C3%B3w_internetowych
Unfurlur:	http://unfurlr.com/
URL X-ray:	http://urlxray.com/
Słownik pojęć bezpieczeństwa (ang.):	http://preview.tinyurl.com/6wkpae5
Porada dnia SANS (ang.):	http://preview.tinyurl.com/6s2wrkp

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz