Biuletyn Bezpieczeństwa Komputerowego

Spersonalizowane oszustwa

Wprowadzenie

Cyberprzestępcy w dalszym ciągu poszukują nowych, kreatywnych sposobów oszukiwania ludzi. Na popularności zyskuje nowy rodzaj tzw. spersonalizowanego oszustwa. Przestępcy wyszukują lub nabywają informacje o milionach osób, wykorzystując zdobyte dane do przeprowadzenia ataku. Poniżej przedstawimy mechanizm tego rodzaju działań, ilustrując go jednym z popularnych przykładów. Jego zrozumienie pomoże Ci w wychwyceniu i powstrzymaniu oszustów.

Jak to działa?

Oszustwa przy użyciu wiadomości email, czy rozmowy telefonicznej to żadna nowość. Cyberprzestępcy próbują oszukiwać ludzi w ten sposób od wielu lat. Najlepsze przykłady stanowią wiadomości w stylu "Wygrałeś nagrodę!", czy wciąż popularny tzw. nigeryjski przekręt. Przy tego rodzaju tradycyjnych oszustwach atakujący nie wiedzą do kogo kierują swoją wiadomość. Tworzą prostą, generowaną masowo treść i wysyłają ją do milionów osób. Takie wiadomości są z reguły łatwe do wychwycenia ze względu na swój ogólnikowy charakter. Inaczej jest przy spersonalizowanych atakach. W tym wypadku oszuści najpierw zdobywają informacje o osobach, by następnie dostosować wiadomość do każdej z ofiar. Odbywa się to dzięki znalezionej lub kupionej bazie danych. Może ona zawierać imiona i nazwiska osób, ich hasła, numery telefonów, a także inne wrażliwe informacje. Powyższe dane są dostępne za pośrednictwem wielu skompromitowanych serwisów internetowych. Mogą być także powszechnie dostępne w mediach społecznościowych czy rządowych archiwach. Po uzyskaniu poszukiwanych informacji przestępcy przygotowują spersonalizowane oszustwo.

Jedną z popularnych sztuczek stosowanych przez cyberprzestępców jest zastraszanie lub wymuszanie zapłaty. Atak przebiega w następujący sposób: oszuści pozyskują bazy danych z loginami i hasłami pochodzącymi ze skompromitowanych stron internetowych. Następnie przesyłają (z reguły wszystkim osobom odnalezionym w bazie) wiadomość email z osobistymi informacjami o Tobie, włącznie z hasłem którego używałeś w trakcie logowania do skompromitowanej witryny. Przestępcy starają się w ten sposób udowodnić, że przejęli kontrolę nad Twoim komputerem, co oczywiście nie jest prawdą. Następnie informują, że mając do niego dostęp, przyłapali Cię na oglądaniu pornografii. Oszuści grożą, że opublikują i przekażą Twojej rodzinie i znajomym wstydliwe materiały, jeśli nie zapłacisz im określonej kwoty okupu.

Haczyk polega na tym, że w niemal w każdym przypadku przestępcy nie przełamali zabezpieczeń Twojego systemu i nie są w posiadaniu kompromitujących Cię materiałów. Nie wiedzą nawet kim jesteś i jakie strony odwiedzasz. Oszust po prostu próbuje użyć paru osobistych informacji, które znalazł na Twój temat, aby nakłonić Cię do zapłaty. Pamiętaj, że podobna metoda ataku może zostać wykorzystana przy oszustwach telefonicznych.

Co powinniśmy zrobić?

Miej na uwadze, że takie wiadomości email czy połączenia telefoniczne to zwykłe oszustwa. To normalne, że jesteśmy przestraszeni, kiedy ktoś używa osobistych informacji o nas. Pamiętajmy jednak, że oszuści kłamią. Każdy atak jest częścią zmasowanej i zautomatyzowanej kampanii, która nie jest skierowana wyłącznie do nas. Ze względu na coraz łatwiejsze pozyskiwanie informacji, powinniśmy spodziewać się wzmożonej liczby tego rodzaju ataków w przyszłości. Poniżej podajemy kilka wskazówek, które mogą świadczyć o próbie ataku:

- **Gdy dostajesz dziwnego email-a, wiadomość SMS czy połączenie telefoniczne, bądź czujny. Ktoś, kto próbuje wykorzystać emocje, takie jak strach lub nakłania Cię do podjęcia nagłej decyzji, prawdopodobnie chce, abyś w pośpiechu popełnił błąd.**
- **Kiedy ktoś żąda zapłaty w kryptowalucie Bitcoin, kartach podarunkowych lub innej trudnej do wyśledzenia metodzie płatności.**
- **Gdy otrzymujesz podejrzaną wiadomość email, skorzystaj z wyszukiwarki Google. Sprawdź, czy ktoś nie informował o podobnym rodzaju ataku.**

Ostatecznie, najlepszą obroną jest zachowanie zdrowego rozsądku. Ponadto zachęcamy Cię do używania niepowtarzalnych, odpowiednio silnych haseł do Twoich kont. Masz problem z ich zapamiętaniem? Skorzystaj z menedżera haseł. Tam gdzie to możliwe, użyj dwuskładnikowego uwierzytelniania.

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

Redaktor Gościnny

Lenny Zeltser *to weteran w dziedzinie cyberbezpieczeństwa. Tworzy rozwiązania przeciwdziałające złośliwemu oprogramowaniu w Minerva Labs, a także prowadzi wykłady w ramach zajęć w SANS Institute. Posiada doświadczenie w zakresie doradzania i zarządzania usługami bezpieczeństwa. Śledź go na zeltser.com/blog oraz jego koncie Twitter @lennyzeltser.*

Źródła

Socjotechnika:	https://www.sans.org/u/MUU
Powstrzymać phishing:	https://www.sans.org/u/MUZ
Odszukaj siebie w sieci:	https://www.sans.org/u/MV4
Menedżer haseł:	https://www.sans.org/u/MV9