Месечен бюлетин за Информационна Сигурност насочен към потребителите

OUCH!

В ТОЗИ БРОЙ...

- **Какво е социален инженеринг**
- **Разпознаване / Спиране на атаки чрез социален инженеринг**

Социален инженеринг

Преглед

Често срещано погрешно схващане, което имат повечето хора за кибер нападателите е, че те използват само силно напреднали инструменти и техники, за да проникнат в компютрите или сметките на хората. Това просто не е вярно. Кибер нападателите са се научили, че често най-лесните начини да откраднат информация от вас, да хакнат сметките ви или да заразят системите ви е, като просто ви подмамят да направите грешка. В този бюлетин ще се научите как работят тези атаки, наречени социален инженеринг, и какво можете да направите, за да се предпазите.

Гост-редактор

Джеймс Лайн (**@jameslyne**) е сертифициран SANS инструктор и глобален ръководител на проучванията в Sophos. Той разплита и извършва обратен инженеринг на последните и най-добри творения на кибер престъпниците. Той е автор и на курсовете Metasploit (SEC580) и Социално инженерство (SEC567) в SANS.

Какво е социален инженеринг

Социалният инженеринг е психологическа атака в която атакуващият ви подмамва да направите нещо, което не бива да правите. Концепцията за социалния инженеринг не е нова, тя съществува от хиляди години. Помислете за измамниците или мошениците, идеята е една и съща. Това, което прави модерните технологии толкова по-ефективни за кибер нападателите е, че не можете физически да ги видите, могат лесно да претендират, че са каквото или когото си поискат и да се целят в милиони хора по света, включително вас. В допълнение, атаките чрез социално инженерство могат да заобиколят много технологии за защита. Най лесният начин да разберете как работят тези атаки и да се предпазите от тях е да вземете два примера от истинския свят.

Получавате телефонно обаждане от някой, който твърди, че е от фирма за компютърна поддръжка, от вашия Интернет доставчик или може би дори техническа поддръжка на Microsoft. Обаждащият се ви обяснява, че компютърът ви сканира активно интернет, като според него е заразен и той е бил натоварен със задачата да ви помогне да защитите компютъра си. След това същият използва различни технически термини и ви превежда през объркващи стъпки, за да ви убеди, че компютърът ви е заразен. Например, човекът може да ви помоли да проверите дали имате някои файлове на компютъра си и да ви преведе през нужните стъпки, за да ги намерите. Когато намерите тези файлове, обаждащият се ви уверява, че тези файлове доказват, че компютърът ви е заразен, като в действителност тези файлове са общи системни файлове, които могат да се намерят на почти всеки компютър в света. След като ви е подмамил да вярвате, че компютърът ви е заразен, човекът ви притиска да купите техния софтуер за сигурност или да му дадете отдалечен достъп до компютъра ви, за да може да го оправи. Истината е, че софтуерът който

Социален инженеринг

ви се продава всъщност е злонамерена програма. Ако го купите и го инсталирате, не само са ви заблудили като са заразили компютъра ви, но сте си и платили, за да го направят. Ако им дадете отдалечен достъп до компютъра си, те ще го превземат, ще откраднат данните ви или ще го използват за наддаванията си.

Здравият разум е най-здравата защита в идентифицирането и спирането на повечето атаки чрез социален инженеринг.

Друг пример е имейл атака, наречена Измама Изпълнителен директор, която най-често става на работа. Това е случаят в който кибер нападателят проучва организацията ви онлайн и открива името на шефа ви или ваш колега. Атакуващият изготвя имейл, който претендира да е от този човек и ви изпраща имейла. Имейлът ви подканва да преприемете действие незабавно, като например да преведете пари веднага или да изпратите поверителна информация за друг служител. Доста често тези имейли претендират, че има спешен случай, който изисква да заобиколите стандартни практики на защита, например могат да се опитат да ви накарат да изпратите високо поверителна информация на личен акаунт в gmal.com. Онова, което прави целенасочени атаки като тези толкова опасни е, че кибер атакущите правят проучвания предварително. В допълнение на това, технологии за защита като антивирусни програми или защитни стени не могат да засекат или спрат тези атаки, тъй като няма намесени злонамерен софтуер или злонамерени хипервръзки.

Помнете, че атаките чрез социално инженерство като тези не са ограничени до телефон или имейл, а могат да се случат във всякаква форма включително текстови съобщения на телефона ви, в социалната мрежа или дори лице в лице. Ключът е в това да знаеш какво да търсиш, ние самите сме си най-добрата защита.

Разпознаване / Спиране на атаки чрез социален инженеринг

За щастие, спирането на подобни атаки е по-лесно отколкото може би си мислите – здравият разум е най-здравата защита. Ако усещате нещо подозрително или нередно, значи може би е атака. Най-често срещаните признаци на атака чрез социален инженеринг включват:

- Някой създава огромно усещане за спешност – опитват се да ви преметнат, за да направите грешка.
- Някой иска информация до която не би трябвало да има достъп или вече би трябвало да я знае, като например номера на акаунта ви.
- Някой ви пита за паролата ви, няма истинска организация, която някога би ви попитала за това.
- Някой ви притиска да заобиколите или да игнорирате процеси на защита или процедури, които се очаква да следвате на работа.

Социален инженеринг

- Нещо е твърде добро, за да е истина. Например, уведомяват ви, че сте спечелили от лотарията или сте спечелили iPad, въпреки че изобщо не сте участвали в лотария.
- Получавате странен имейл от приятел или колега, който е написан по начин, които не звучи свойствен за тях. Кибер нападател може да е влязъл в акаунта им и се опитва да ви измами. За да се предпазите, проверявайте подобни молби като се свържете с приятеля си по различен метод за комуникация, като лице в лице и по телефона.

Ако подозирате, че някой се опитва да ви измами или преметне, не комуникирайте с човека повече. Ако атаката е свързана с работа, постарайте се да докладвате на екипа по поддръжка или на екипа по информационна сигурност незабавно. Не забравяйте - здравият разум е най-здравата защита.

НАУЧЕТЕ ПОВЕЧЕ

Абонирайте се за месечния бюлетин за информационна сигурност OUCH!, разгледайте архивните броеве на OUCH! и научете повече за решенията за информационна сигурност на SANS като ни посетите на securingthehuman.sans.org/ouch/archives.

Радослава Несторова (лингвист) и Николай Дачев (технически експерт) са екип, доказал се в областта на техническите преводи. Повече за нас можете да научите на нашите страници в LinkedIn:
https://www.linkedin.com/pub/radoslava-nestorova/6/6a2/962
https://www.linkedin.com/pub/nikolay-dachev/7b/5bb/96b

Ресурси

Фишинг:	https://securingthehuman.sans.org/ouch/2015#december2015
Измама Изп. директор:	https://securingthehuman.sans.org/ouch/2016#july2016
Софтуер изискващ откуп:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH Архиви:	https://securingthehuman.sans.org/ouch/archives

Редакторски колектив: Бил Уайман, Уолт Скривенс, Фил Хофман, Боб Рудис
Превод: Николай Дачев и Радослава Несторова