СЪВЕТ ПО
ИНОВАЦИИ
ПРИ БТПП

1895
БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Д О К Л А Д НА ТЕМА:

„Кибер-рискове в Интернет“

гл. ас. д-р Филип Андонов

СЪВЕТ ПО
ИНОВАЦИИ
ПРИ БТПП

1895
БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Съдържание

- Атаки от тип “човек по средата”
- Phishing атаки
- Социално инженерство
- Ransomware

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Кой – кого?

Кой?

- Хакери
- Активисти
- Измамници
- Криминални организации
- Правителствени служби

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Кой – кого?

Кого?

- Случайни граждани
- Организации
- Публични личности
- Хора, работещи в организация, взета на прицел
- Компании
- Правителства

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

Man In The Middle (MITM) е вид атака, при която нападателят прихваща и подменя информация, обменяна между две страни.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

Цели на този вид атаки са били:

- Google
- Френското външно министерство
- SWIFT (обединението на хиляди банки, което по „сигурен“ начин управлява финансови транзакции в над 200 държави)
- Компютърните мрежи на саудитската банка Riyad Bank
- Китайският технологичен гигант Huawei

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

Според изтекли документи, агенция на голяма държава е атакувала бразилската държавна петролна компания Petrobras въпреки изявленията, че „не участва в никакъв вид икономически шпионаж“

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

Изтеклите документи показват, че държавни агенции са атакували HTTPS протокола чрез man-in-the-middle атаки за да заобиколят шифроването като фалшифицират цифрови сертификати за да прихванат данните.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

- Преди масовото въвеждане на SSL, правителствените шпиони можеха да прихващат електронни писма и други данни в нешифрован вид директно от Интернет кабелите.
- SSL шифроването ги затруднява и агенции започват събирането на данни директно от Интернет компаниите.

Man-in-the-middle

- Но в някои случаи се предприемат по-агресивни мерки – заобикалят Google директно като извършват man-in-the-middle атака за да имперсонират Google сертификат за сигурност.
- Хакват се маршрутизатори на жертвата и пренасочват целия трафик, използвайки фалшиви сертификати, така че да могат да прихванат и дешифрират информационния поток.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

Wi-Fi и LAN man-in-the-middle атаки

- Това са атаки, при които злонамерено лице прихваща мрежовия трафик и ако той не е шифрован директно го чете, а ако е шифрован използва допълнителни техники за преодоляване на шифроването.

Man-in-the-middle

- Известна от миналото атака бе firesheep, но има много подобни и с по-голям обхват.
- В безжичния вариант работи ако атакуващия и жертвата са физически близо и компютърът на жертвата бива излъган да мисли, че компютъра на атакуващия е всъщност маршрутизатора
- В жичния вариант атакуващия трябва да бъде част от физическата вътрешна мрежа

Man-in-the-middle

Съществуват инструменти, които автоматизират такива атаки:

- Модифициране на iptables
- ARP cache poisoning
- SSL stripping
- Парсване на логовете в реално време

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

Има две неща, които да направите, за да се предпазите:

- Използвате програми за защита
- Да използвате главата си

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

- Никога, при никакви обстоятелства не въвеждайте важни удостоверителни данни (потребителски имена и пароли) през несигурни връзки, отворени wifi.
- Проверявайте дали сертификатите изглеждат добре
- Дали се използва шифрована връзка (SSL версия 3)
- Следете за необичайно поведение – презареждане на страницата, странно изглеждаща страница, прекалено дълго време за зареждане, излизане (logoff) без да го очаквате

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Man-in-the-middle

- Никога не ползвайте Wi-fi ако можете да използвате кабел.
- Никога не се включвайте към неизвестни Wi-fi мрежи по летища, молове и гари, тъй като всеки може да кръсти wi-fi рутера си както поиска.
- Не използвайте служебни компютри на такива места

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Фишинг (Phishing)

Опит да се получи поверителна информация – потребителски имена, пароли, данни за кредитни карти и т.н. с лоши намерения чрез маскиране като надежден участник в електронната комуникация.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Spear phishing

Когато атаката е насочената към специфични лица или компании, фишинг атаката се нарича spear phishing. Нападателите могат да съберат лична информация за целите си, за да увеличат шансовете си за успех.

Атаката е особено успешна в Интернет, като статистиката сочи, че 91% от атаките са от този вид.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Атака 1

Атаката в реално време се опитва да разкрие както паролата, така и еднократния код на двуфакторната автентикация (2FA). Нападателят постига това като показва фалшива страница която симулира Gmail 2-стъпковия процес на влизане в системата. Нападателят едновременно получава входа на потребителя и влиза в истинската Gmail страница. Опитът за вход в системата кара Google да прати валиден 2FA код на жертвата, който атакуващият ползва и въвежда.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

- Стъпка 1: SMS от “Google” внушава страх от компрометиране на акаунта
- Атаката започва сутринта с SMS-и към целта.
- Съобщенията имитират стила на SMS-ите от Google, които уведомяват целта, че е имало неочакван опит за влизане в акаунта. Изпращащият номер е неизвестен на жертвата.

Phishing

- Стъпка 2: Веднага след това се получава известие за „Опит за влизане“
- По-малко от 10 минути след получаване на първия SMS, жертвата получава писмо, изглеждащо като известие от Gmail за опит за влизане в акаунта. Важно е да се отбележи, че e-mail-ът съдържа лична информация за жертвата, включваща име, профилна снимка и e-mail адрес.
- Друго забележително нещо е, че „неочакваният опит за влизане“ (“Unexpected sign-in attempt”) индикира че опитът е „от Иран“. За човек, който се притеснява да не е хакнат от ирански групи е нормално да се притесни от такава информация.

From: "Google Warning" <no-reply@support.googlemail.com>
Date: [redacted]
Subject: Unexpected sign-in attempt, secure account with this message
To: [redacted]
Cc:

Google [redacted]@gmail.com [redacted]

Hi [redacted]

We recently prevented several Log-in attempts to your Account: [redacted]

Log-in attempt info:
Location: The Iran
IP Address: 95.79.35.17

If this wasn't you
Please review your Account Activity page at Account Security to see if anything looks suspicious. Whoever tried to Log-in to your account knows your credentials information; we recommend that you change them right away.

If you do not recognize this Log-in attempt, someone else might be trying to access your account. You should reset your credentials information immediately.

Reset password

Sincerely,
The Google Accounts team

This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Адресът на изпращача е направен да изглежда като Gmail домейн.

no-reply@support.qooqlemail.com

Същият домейн е използван и при други атаки.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

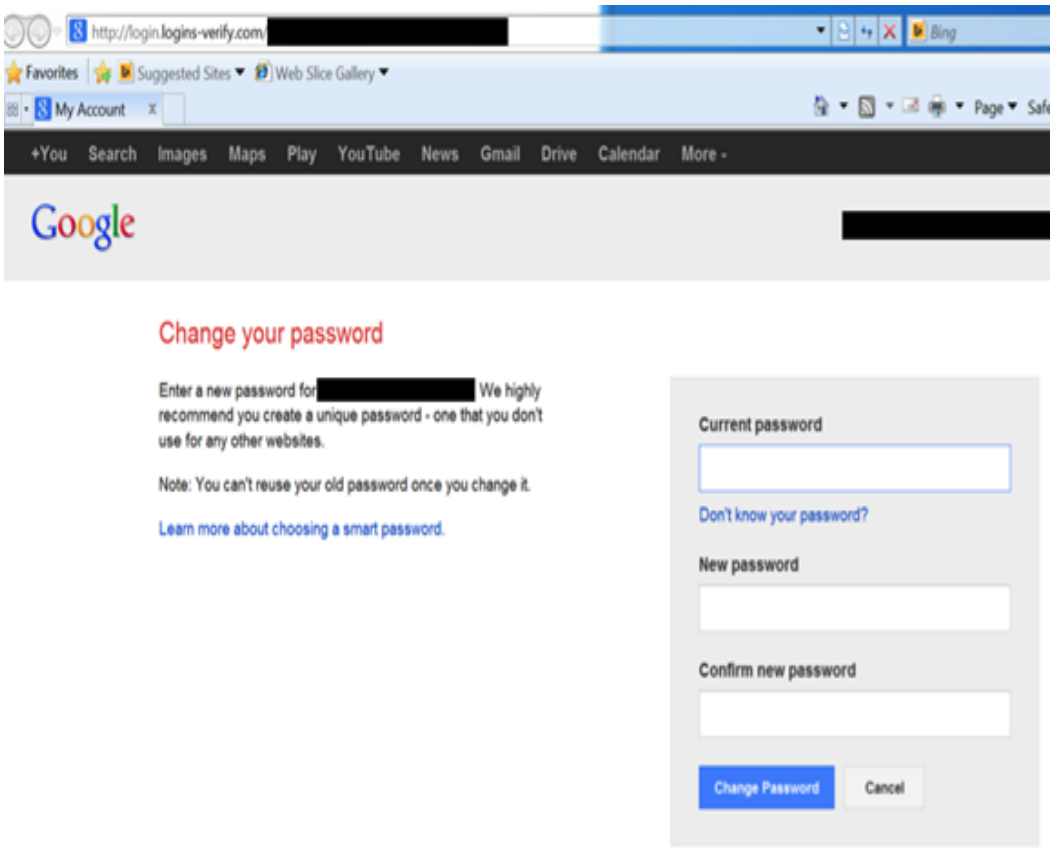
Phishing

- Стъпка 3: Жертвата бива подлъгана да въведе паролата си и да чака за 2FA код
- Щракането върху хипервръзката “Reset Password” води до внимателно създадена phishing страница.
- Страницата отново съдържа лична информация на целта и включва пощенския адрес и име. Съдържа и допълнителен код, взет от Google, за да изглежда сякаш това е истинска страница на Google.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

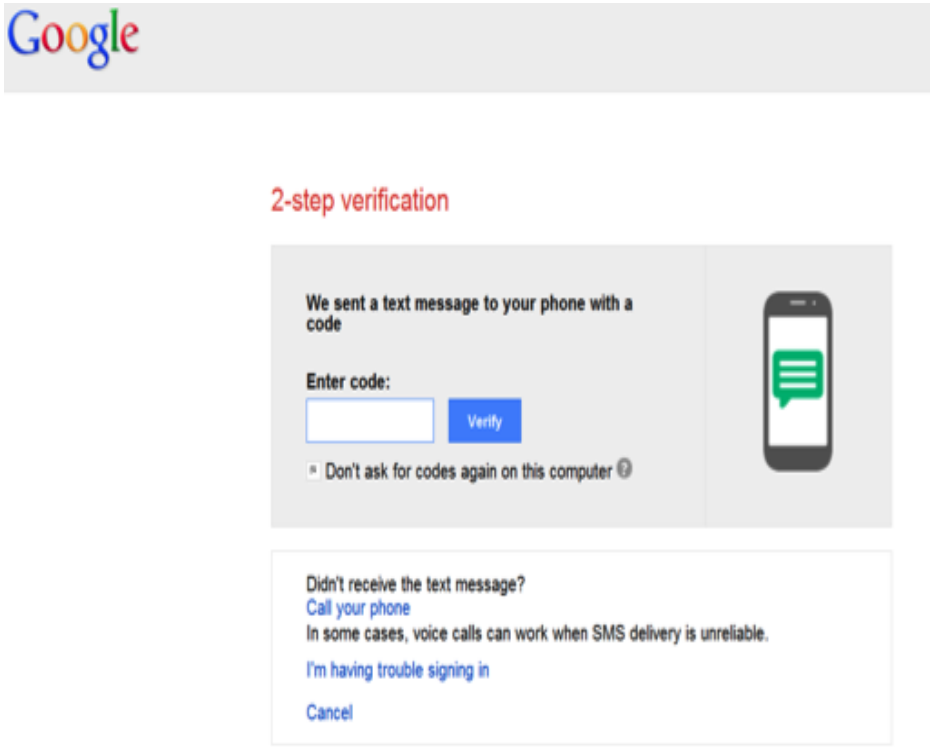
Phishing



СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing



Phishing

- За да работи тази атака, нападателят трябва активно да наблюдава фишинг страницата. След като целта въведе своята парола във фишинг сайта атакуващият използва тези данни за да влезне в gmail. Опитът на нападателя да влезне активира изпращането на 2FA код от истинският Google към целта. Нападателят изчаква целта да въведе кода на фишинг сайта и след това той го въвежда в истинската страница на Google.
- Веднъж след като целта въведе кода, акаунтът му е в контрола на нападателя и може да прави каквото си поиска.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Инструмент за събиране на информация за организация

Интегрира се с корпоративни директории и социални мрежи за да създаде карта на връзките между служителите, както и важни външни контакти.

Това е „реалната организационна структура“.

Хакерите използват такава информация за да изберат хора, за които да се представят.

Въоръжени с тази информация злонамерени лица могат да се създават специфични фишинг кампании, чрез мейл и туитър и да видят как ще реагират потребителите.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Как всъщност атакуващите успяват да съберат толкова много лична информация за жертвите?

- Социални мрежи
  - Google Plus
  - LinkedIn
  - Facebook
  - Twitter

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Phishing

Как всъщност атакуващите успяват да съберат толкова много лична информация за жертвите?

- Социално инженерство
  - „Здравейте, аз съм журналист“
  - „Здравейте, пише ви новият системен администратор“
- Публично достъпна информация:
  - сайт на учреждението
  - сайт на университета

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Социалното инженерство е техника, при която нападателят убеждава жертвата си да направи нещо в негова изгода.

Атаката може да е:

- Лично
- По телефон
- През Интернет

Целта може да е:

- Действие
- информация

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Просто питай

Кевин Митник

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Пример 1.

- Здравейте, аз съм Жана Герганова от Здравната Каса. Обаждам се да ви съобщя, че не сте попълнили номер на сметката си в документите в болницата и болничните ви не могат да бъдат изплатени.
- Какво? Какви болнични, станала е някаква грешка.
- С Иван Петров ли говоря?
- Да!?
- Иван Петров с работодател Министерство на Транспорта?
- Да, но не зная за никакви болнични!

Social Engineering

- Е, ами това е добре, щом не боледувате.
- Е, грипът през зимата е неизбежен, ама не влизаме в болница за него.
- Сигурно е някаква грешка. В нашата система данните на държавните служители се въвеждат по служебен номер. Сигурно някой е въвел номера грешно. Случва се често. А какъв е вашият?

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Пример 2

По Коледа един човек получава писмо от PayPal, в което пише, че към акаунта му е добавен нов пощенски адрес.

Той влиза в PayPal и сменя паролата си и превключва пощенския адрес обратно на неговия, изтривайки непознатия.

След това се обажда в PayPal и пита как нападателят е успял да влезе и може ли да направи нещо друго, за да се защити.

Получава отговор, че нападателят е използвал неговото име и парола и че човекът е направил всичко, което трябва и няма нужда да се безпокои.

Social Engineering

Двадесет минути по-късно проверява отново пощата си и има ново писмо, в което се казва че към акаунта му е добавен нов адрес.

Реагирайки както и предходния път той се опитва да влезне отново в PayPal, но този път от акаунта му е махнат неговия личен пощенски адрес и паролата му е сменена.

PayPal заключва акаунта, когато нападателят се опитва да прати пари на известен терорист. Целта явно е била да усложни живота на жертвата.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Човекът се обажда отново в PayPal и настоява да говори с някой от по-високо ниво.

От разговора той разбира, че неговата много сложна парола никога не е била компрометирана. Нападателят просто се е обадил на отдела за обслужване на клиенти в PayPal и се е представил за него, успявайки да reset-не паролата като предостави просто четирите последни цифри от социално-осигурителния номер на жертвата и четирите последни цифри от стара кредитна карта.

Човекът се нарича Брайън Кребс и неговите данни са били публикувани много пъти онлайн.

Проблемът е, че компанията разчита на статични данни за автентикация.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Пример 3

Използвайки собствения си Tinder профил, хакерът търси всички мъже, живеещи в радиус от два километра (атаката няма да е достатъчно бърза ако градът е голям и радиусът е по-голям)

Първата ни жертва е мъж, атаката няма да успее, ако започнем с жена. Мъжете гонят, жените бягат.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Избираме си жертва – привлекателен млад мъж, ще го наречем Боби.

Правим снимка профилната снимка на екрана и записваме биографията му.

Създаваме фалшив Facebook профил на Боби. Ще използваме същото първо име и възраст.

Регистрираме фалшивия Боби в Tinder.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Супер-харесваме всички жени в радиус от 2 километра. Използва се специален плъгин, за да може да се автоматизира тази инак непосилна задача.

Изчакваме отговор от привлекателна жена. Ще я наречем Анна.

Създаваме фалшив неин профил във Facebook и оттам в Tinder.

Ограничаваме търсенето до 2 километра и намираме оригиналния Боби.

Супер-харесваме Боби от фалшивия акаунт на Анна и чакаме за отговор.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Боби “Здрасти :)”

Успех! Захапа кукичката.

Това се нарича атака „човек по средата“ (man in the middle)

Боби “Как си?” => Fake Alice => Фалшив Боби => **Анна**

Анна “Супер! А ти?” => Фалшив Боби => Фалшива Анна => **Боби**

Боби “Винаги съм добре :) Къде си?” => Фалшива Анна => Фалшив Боби => **Анна**

Анна “Центъра, а ти?” => Фалшив Боби => Фалшива Анна => **Боби**

Боби “Аз съм в Изток. Имаш ли планове за довечера?” => Фалшива Анна => Фалшив Боби => **Анна**

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

В момента подслушваме личен разговор на двама непознати. Можем обаче и да им променяме реалността.

Нека да променим къде ще се срещнат.

Боби “Да пийнем по едно довечера?” => Fake Alice => Fake Bob “Да пийнем по едно довечера? Била ли си във Фрапе?” =>

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Анна “Не съм, сега го видях в Google. Изглежда супер!” => Fake Bob => Fake Alice “Да, нека се видим на пилоните на НДК ” => **Боби**

Сега ще го направим по-пикантно.

Анна “До довечера! ” => Fake Bob => Fake Alice “Предизвиквам те в момента в който ме видиш да ми пуснеш език в ухото! Или те е шубе?” => **Боби**

В някакъв момент обменят телефонни номера и спират да говорят по Tinder.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Можем да продължим атаката върху всякаква друга комуникация, защото ние подменяме съобщенията и на двамата. Можем да дадем фалшив номер на всеки един от тях. Или Viber, Skype, …

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Пример

Привлекателни млади жени се наемат от собственици на скъпи ресторанти

Жените се свързват с мъже в сайтове за запознанства, уговаряйки си срещи във въпросните ресторанти, в които естествено мъжът ще плати

Те никога не си правят повторна среща, а мъжът си мисли, че просто „не се е получило“.

Жертвата никога така и не разбира, че е бил измамен.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Social Engineering

Изводи

- Познаването на жаргона, имена на отдели, хора, процедури, системи НЕ удостоверява искащия информация
- Не разчитайте на сигурност, основана на непрозрачност.
- Обаждане от вътрешен номер или от писмо от служебен адрес НЕ удостоверява насрещния човек

Ransomware

- Ransomware е зловреден компютърен софтуер, който се инсталира незабележимо на компютъра на жертвата, ограничава достъпа до софтуер, данни или хардуер и изисква откуп за да възстанови нормалното функциониране.
- В по-опростения си вариант ransomware може да заключи системата по начин, който специалист може сравнително лесно да преодолее.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

- По-сериозна заплаха представлява софтуера, който шифрова файловете на жертвата, правейки ги недостъпни и изисквайки откуп, за ключа за дешифриране.
- Някои ransomware шифрират файловата таблица или целия диск.
- На практика това е атака от типа отказ на достъп
- Най-честият вектор на атака за първоначално инсталиране на ransomware е троянски кон.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

- Цели на ransomware-а са както клиентски компютри, така и сървъри
- Вторият вариант има по-сериозни последствия, защото възпрепятстването на работата на организация или основната ѝ търговска дейност може да доведе дори до фалит
- При вторият вариант жертвите обикновено се въздържат да оповестят, че са подложени на такава атака, защото ще загубят доверие на клиенти и партньори и се опитват да решат проблема си самостоятелно

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

WannaCry

- от пролетта на 2017-а година.
- Известен с бързото си разпространение и атакуването на множество организации и фирми – включително:
  - болници
  - FedEx
  - здравната служба на Великобритания
  - Руското външно министерство

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

- За дни се разпростира в повече от 100 държави.
- Най-засегнати са:
  - Русия
  - Украйна
  - Индия
  - Тайван

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

- Както и при други атаки от този тип мащабите не могат да се определят, защото жертвите не правят публичен факта за плащането на откуп,
- Специалисти смятат, че хакерите може да са взели над **1 милиард долара.**

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

- Разпространява се по електронната поща, използвайки фишинг, подобен на използвания при атаката срещу Демократическата партия в САЩ. Изисква откуп от 300 долара в bitcoins.
- Базира се на уязвимост, открита и използвана от NSA.
- Група хакери, наречени ShadowBrokers откраднаха и разпространиха кибер-оръжия, използвани от агенцията. Сред тях е и уязвимостта с кодово име EternalBlue, известна на NSA от преди 2014-а.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

- Уязвимостта не е поправена, а е експлоатирана от щатските служби в продължение на 5 години.
- Когато обаче инструментите за хакване са откраднати, NSA най-накрая съобщава на MS за уязвимостта и тя е закърпена. За съжаление не всички инсталират „кръпката“, а и тя не е налична за стари версии на Windows, което способства за разпространението на Wanna Cry.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

Herbalife

- През септември 2017 се наблюдава разпространението на агресивен ransomware, като най-голям обем на писма идва от Виетнам
- Други големи източници на атаката са Индия, Колумбия, Турция и Гърция.
- Обемът е необичайно голям – около 20 милиона писма за 24 часа, като бройката расте.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

Първоначално писмото е един от два вида – Herbalife брандирано или обикновено, което се представя за доставка на ‘copier' file. По-късно се появява трети вариант на писмото, а по-късно още два нови. Единият се представя за съобщение от гласова поща, а другият – за фактура от marketplace.amazon.uk.

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

Изводи

- Както при другите видове зловреден софтуер, ransomware-а може да не бъде открит от софтуера отговарящ за сигурността
- Шифроването отнема доста време, така че ако атаката е открита в ранен етап, премахването на зловредния софтуер ще спаси данните, които още не са били шифровани

СЪВЕТ ПО ИНОВАЦИИ ПРИ БТПП

1895 БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

Ransomware

Изводи

- Антивирусен софтуер ще открива известни ransomware-и, но едва ли нови такива
- Съхраняването на резервни копия на офлайн носители е най-добрата защита
- Наличието на нешифровано копие на даден файл може да спомогне за дешифрирането на други, които нямат резервно (нешифровано) копие

СЪВЕТ ПО
ИНОВАЦИИ
ПРИ БТПП

1895
БЪЛГАРСКА ТЪРГОВСКО-ПРОМИШЛЕНА ПАЛАТА
BULGARIAN CHAMBER OF COMMERCE AND INDUSTRY

БЛАГОДАРЯ ВИ ЗА ВНИМАНИЕТО!

гл. ас. ФИЛИП АНДОНОВ, доктор по информатика

E-mail: fandonov@nbu.bg;

моб.тел.: 0898 392 007