ENCRYPT 4.0

Съвместна инициатива за развитие на работна сила за подпомагане на европейската индустрия в преодоляването на недостига на професионалисти по киберсигурност

№ 2020-1-RO01-KA202-079983

О3: Документален архив за кибер атаки

Съфинансиран от програма „Еразъм+“ на Европейския съюз

СЪДЪРЖАНИЕ

ВЪВЕДЕНИЕ

С навлизането на информационните технологии и с възхода на четвъртата индустриална революция, бизнесът е изправен пред нови предизвикателства, свързани с киберсигурността и защитата на данните. Това е особено валидно за производствените МСП, които често нямат вътрешни ресурси и капацитет за ефективна оценка на рисковете по отношение на киберсигурността, съответстващи на нововнедрените технологии, базирани на Индустрия 4.0. В същото време МСП все по-често стават жертви на различни киберпрестъпления. Според последния доклад на Verizon за разследване на нарушения на данните за 2021 г. *(Verizon, 2021 г.)*, МСП са жертви и са много по-уязвими на кибератаки в сравнение с големите предприятия, тъй като им липсват ресурси, хора, информация и общ капацитет за предотвратяване на рисковете от кибератаки.

Междувременно киберзаплахите имат различни източници и стават все по-сложни, например и ако екипите не са имали подобни уязвимости и им липсват ясни насоки как да реагират на тях, може да отнеме дни и дори седмици, за да реагират правилно, което може да бъде фатално за някои производствени процеси. Според доклада за МСП за 2021 г. относно ИТ сигурността, за най-голяма пречка пред киберсигурността се считат служителите, които не следват указанията и тази тенденция се влошава с увеличаването на работата от разстояние поради пандемията COVID-19 *(Untangle, 2021 г.).* Въпреки това, когато има пробив в киберсигурността, той не засяга само хората, може също така да причини финансови загуби, загуба на доверието на клиентите и накърнена репутация *(Acronis, 2021 г*.).

Вземайки предвид гореспоменатото, консорциумът Encrypt 4.0 разработи настоящия документ, за да послужи като ноу-хау инструмент, даващ достъп до критичен анализ на реални кибератаки и извлечени уроци, както и пътни карти за това как да ги предотвратите, идентифицирате, справите и възстановите от тях.

Документалният архив Encrypt 4.0 за кибер атаки е специално пригоден за нуждите на производствените МСП в ЕС, работещи в контекста на Индустрия 4.0, и представлява компилация от казуси за кибер атаки, които са насочени към подкрепа на МСП за повишаване на тяхната киберсигурност и предотвратяване на кибер атаки.

СТРУКТУРА & МЕТОДОЛОГИЯ

Документалният архив Encrypt 4.0 съдържа общо **18 казуса**. Всеки от партньорите на ENCRYPT 4.0 е разработил 3 реални казуса за кибератаки, въз основа на документално проучване, личен опит и наблюдения и задълбочени интервюта с изпълнителни директори, специалисти по киберсигурност и ИТ специалисти, които обхващат различни видове кибер атаки и предоставят критичен анализ за причините за нарушенията на сигурността, как са били преодолени и какви са били последствията.

Консорциумът ENCRYPT 4.0 изгради специфичен модел „ПРЕВЕНЦИЯ-ИДЕНТИФИЦИРАНЕ-РЕАКЦИЯ-ВЪЗСТАНОВЯВАНЕ“ (PIRR), базиран на модела „Идентифициране, защита, откриване, реагиране и възстановяване“ на Националния институт за стандарти и технологии (NIST). Типът на кибер атаките е въз основа на модела STRIDE, както и на рамката MITER ATT&CK. Анализът на модела PIRR съдържа 4 основни категории/раздела, базирани на

основните стъпки за борба с проблем с киберсигурността, както и раздели с извлечени поуки (вижте Фиг. 1.).

Фиг. 1. Категории на модела „Превенция – Идентифициране – Реакция – Възстановяване“(PIRR)

ПРЕВЕНЦИЯ

Настоящият раздел е фокусиран върху намаляване на риска от излагане на кибер атаки и превантивни мерки и за всеки казус включва следното:

- Въвеждане на специфични практики за сигурност, които имат доказан ефект при реални кибератаки;
- Погрешни схващания по отношение на киберсигурността: практики, които всяка компания е прилагала и са имали нулево или дори отрицателно въздействие при действителни инциденти.

ИДЕНТИФИКАЦИЯ

Основната цел на този раздел е да помогне на МСП да разграничат различните видове кибер атаки, категоризирани с помощта на модела STRIDE и рамките на MITER ATT&CK. Моделът STRIDE представлява ориентиран към системата модел на заплаха от високо ниво, фокусиран върху идентифицирането на цялостни категории атаки. Има следните 6 категории:

+Подмяна

+Подправяне

+Отхвърляне

+Разкриване на информация

+Отказ от услуги

+Ескалиране на привилегии

За целите на казусите на ENCRYPT 4.0, моделът STRIDE беше използван за идентифициране на заплахите на по-високо ниво, докато рамката MITER ATT&CK беше приложена за по-подробно уточняване на атаките. Рамката ATT&CK умишлено приема гледната точка на атакуващия, за да помогне на организациите да разберат как противниците подхождат, как се подготвят и успешно изпълняват атаките.

РЕАКЦИЯ

Този раздел описва ситуациите, в които заплахата вече е налице, като предоставя анализ на реални кибератаки и съвети как да реагирате в подобни случаи след идентифицирането им.

Кибератаките в казусите са описани в следния формат:

- КОЙ: атакуващия
- КОГО: целевата организация
- ЗАЩО: мотивите зад атаката (била ли е случайна или целенасочена)
- КАКВО: целевият имот
- КАК: описание на атаката и какви са били използваните техники.
- СТРАТЕГИЯ: как е преодоляна заплахата и мерките, които са имали нулев или отрицателен ефект.

ВЪЗСТАНОВЯВАНЕ

Разделът предоставя информация относно последствията от атаката, както и анализ начините за възстановяване на системата, след като някои процеси са били повредени и възстановяване на достъпа до изгубените данни, въз основа на реални случаи на атака, описани в раздел РЕАКЦИЯ. Разделът следва моделите на STRIDE & MITER ATT&CK, очертаващи практики за възстановяване въз основа на всяка определена група киберзаплахи, представени в раздела ИДЕНТИФИКАЦИЯ.

КАЗУСИ

КАЗУС 1: ОБРАТНАТА ОБВИВКА

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Асоциацията Innovalia е частен и независим технологичен център, създаден от Innovalia Груп, за да свърже критична маса, способна успешно да постигне своите дългосрочни изследователски амбиции и стратегически цели. Innovalia е съюз за МСП основани на технология със седалище в Испания. Има международно присъствие с офиси в Баска автономна област, Мадрид, Каталуния, Канарските острови, Европа, Азия, Близкия изток и Централна и Южна Америка. От основаването си Асоциацията Innovalia развива специална чувствителност и осъзнаване на специфичните характеристики на МСП основани на технология. Днес тя се превърна в лидер в областта на научноизследователската и развойна дейност от и за МСП в Испания. Той също така предлага решения за улесняване на международни иновационни процеси, насочени към МСП. Като технологичен агент на Технологичната мрежа на Баската автономна област (Innobasque), Innovalia обединява уменията, лабораториите и ресурсите на дружествата, основали асоциацията.

КАК Е БИЛА ПРИДОБИТА ИНФОРМАЦИЯТА?

Информацията за този казус е събрана чрез задълбочено интервю с ИТ техник на предприятието. По време на взаимодействието интервюиращият задава първоначалните въпроси, така че респондентът да бъде насърчен да отговори. Липсващата информация е допълнена *a posteriori* с данните, предоставени от интервюираното лице.

ПРЕВЕНЦИЯ

Практиката, която Innovalia прилага преди инцидента, е инсталирането на **софтуер за защитна стена**.

Специфични практики за сигурност:

- ☑ **осведоменост на служителите за ненадеждни имейли.** В този случай хакер изпраща привидно легитимен имейл с молба към нашите служители да кликнат върху връзка в имейла, за да нулират паролата за достъп, под предлог, че са регистрирани няколко неуспешни опита за влизане.
- ☑ **инсталиране на вътрешни защитни стени** за укрепване на тяхната стандартна външна защитна стена. По време на пандемията от COVID-19, когато служителите трябваше да

„Инжектирането на команда е кибератака, при която нападателят поема контрола над операционната система на хоста чрез инжектиране на код в уязвимо приложение чрез команда. Този код се изпълнява независимо от какъвто и да е механизъм за сигурност и може да се използва за кражба на данни, срив на системи, повреда на бази данни и дори инсталиране на зловреден софтуер, който може да се използва по-късно“. (StackHawn, 2022 г.).

работят от вкъщи, от тях се изискваше да инсталират защитна стена в домашната си мрежа.

ИДЕНТИФИЦИРАНЕ

Типът и естеството на кибератаката е: **Инжектиране на код (вмъкване на нежелан код) в уязвимостта на уеб сървъра Apache на компанията чрез дистанционно изпълнение на команда**. Този тип атака може да бъде описан подробно в съответствие с рамката на MITER ATT&CK, както е показано по-долу.

- ☑ Разузнаване: Активно сканиране: Сканиране на IP блокове и сканиране за уязвимости
- ☑ Първоначален достъп: Външни услуги с отдалечен достъп
- ☑ Изпълнение : Интерпретатор на команди и скриптове: PowerShell
- ☑ Ескалиране на привилегии:
  - Инжектиране на злонамерен код в процеси: Инжектиране на библиотека за динамично свързване; Инжектиране на преносим изпълним файл; Превземане на комуникационни (имейл) потоци *(Thread Hijacking)*; извикване на асинхронна процедура; Локално съхранение на нишки *(Thread Local Storage)*; Ptrace системни повиквания; Proc памет; Инжектиране на злонамерен код чрез процеса допълнителна памет за прозорец *(Extra Window Memory)*;
  - Изпълнение предизвикано от събитие: Модифициране на конфигурацията на Unix Shell;
- ☑ Заобикаляне на защитата: Инжектиране на процес и шаблон
- ☑ Ексфилтрация: Прехвърляне на данни към акаунт в облак.
- ☑ Въздействие:
  - Манипулиране на данни: Манипулиране на съхранени, предадени данни и данни по време на изпълнение
  - Спиране на услуги
  - Изключване/Рестартиране на системата

РЕАКЦИЯ

- ☑ **КОЙ:** Нападателят не може да бъде идентифициран точно. Известно е само мястото на произход, Китай.
- ☑ **КОГО:** Асоциация Innovalia
- ☑ **ЗАЩО:** Случайно
- ☑ **КАКВО:** Системата на организацията Innovalia
- ☑ **КАК:** Инжектиране на процеси, чрез дистанционно изпълнение команда.

☑ **СТРАТЕГИЯ:** Заплахата е преодоляна със защитната стена на сървъра в този момент. Следвайте стъпките, описани в следващия раздел, за това как да блокирате IP адреси.

ВЪЗСТАНОВЯВАНЕ

Основните последствия от атаката бяха:

☑ Компрометиране на системата
☑ Изследване и анализ
☑ Актуализиране на версията на сървъра
☑ Промяна на данните за идентификация

Стратегията за възстановяване се фокусира върху блокиране на IP през защитната стена:

Първо, влезте в сървъра, на който трябва да блокирате IP адреса. След това щракнете върху *(Старт)*, въведете Защитна стена на Windows с разширена защита и натиснете „Enter“. В левия панел щракнете върху „Входящи правила“, за да покажете текущо конфигурираните правила в средния панел.

В десния панел щракнете върху „Actions >New Rule“ *(Действия > Ново правило)*: За Тип на правило изберете „Custom“ (*По-избор)* и щракнете върху „Next“ *(Напред)*; за Програма изберете „All programs“ *(Всички програми)* и щракнете върху „Next“ *(Напред)*; за Протокол и портове изберете от падащото меню Тип протокол „Any“ *(Всеки)* и щракнете върху „Next“ *(Напред)*; и за „Scope” *(Обхват)*: под Кои отдалечени IP адреси се прилага това правило? изберете радиалната опция: Тези IP адреси: Щракнете върху „Add“ *(Добави)*.

След това въведете IP адреса, който искате да блокирате от сървъра, и щракнете върху OK. Можете също така да изберете да блокирате диапазон от IP адреси, като изберете опцията Този диапазон от IP адреси: радиален. След като приключите с добавянето на IP адресите, щракнете върху „Next“ *(Напред)*. За действие изберете „Block the connection“ *(Блокиране на връзката)* и щракнете върху „Next“ *(Напред)*. За профил оставете всички опции отметнати и щракнете върху „Next“ *(Напред)*. За „Name“ *(Име)* дайте на правилото описателно име, като „Blacklisted Ips“ *(IP адреси в черния списък)*. Също така, можете да въведете незадължително описание на правилото. Щракнете върху „Finish“ *(Готово)*. Новосъздаденото правило с даденото име вече се показва в средния панел с входящи правила. За да подредите правилата по азбучен ред по име, можете да щракнете върху заглавието на колоната „Name“ *(Наименование)*. Ако трябва да деактивирате правилото, щракнете с десния бутон върху правилото в списъка и щракнете върху „Disable Rule“ *(Деактивиране на правилото)*. Ако трябва да промените обхвата на IP адресите за правилото, щракнете с десния бутон върху правилото в списъка и щракнете върху Properties *(Свойства)*. След това щракнете върху раздела Scope tab (*Обхват)*, направете необходимите промени и щракнете върху „Apply“ *(Приложи*).

ИЗВЛЕЧЕНИ ПОУКИ

Научихме, че е по-добре да имаме определени превантивни и защитни мерки, които са полезни при този тип атаки, например като:

☑ Поддържане на сървъра актуализиран
☑ Да се добави мониторинг на машината на сървъра

☑ Сегментиране на мрежата в VLANS, и
☑ Изолиране на машини, които са изложени на открито.

КАЗУС 2: БЕЗРАЗСЪДСТВОТО НА СЛУЖИТЕЛ
(КИБЕР АТАКА 2 НА АСОЦИАЦИЯ „INNOVALIA“)

„През 2021 г. 83% от организациите съобщават, че са претърпели фишинг атаки. През 2022 г. се очаква да се случат допълнителни шест милиарда атаки“. (CyberTalk, 2022 г.).

ПРЕВЕНЦИЯ

Организацията прилага система за откриване на проникване (IDS), която следи мрежата на CARSA за злонамерена дейност или нарушения на правилата. CARSA прилага софтуер за защитна стена, за да защити своята мрежа и система от неоторизиран достъп.

Въведени са специфични практики за сигурност, които имат доказан ефект при други кибер атаки:

Валидиране и дезинфекциране на въведените данни: Сканирайте за екраниращи знаци и други специални символи за езика на приложението и операционната система, като маркировки за коментари, знаци за завършване на ред и разделители на команди. Ако приложението очаква само ограничен набор от стойности, приемете само тези стойности, например като ги включите в белия списък или условно превключете към тях.

Избягване на уязвими конструкции за оценка: ние избягваме използването на функцията „eval()“, както и еквивалентни функции при набор от потребителски входни данни. CARSA използва специални функции, специфични за езика, за безопасно обработване на аргументи, предоставени от потребителя.

Заключване на интерпретатора: Ако имате контрол над конфигурацията на сървъра, по-добре е да ограничите функционалността на интерпретатора до минимума, необходим за приложението, за да предотвратите ескалиране до инжектиране на системна команда. Например, ако вашето PHP приложение не използва функцията system(), можете да деактивирате тази функция във вашия файл php.ini, като я посочите в указанието „disable_functions“ *(деактивирани на функции)*. Често деактивираните функции за PHP включват: exec(), passthru(), shell_exec(), system(), proc_open(), popen(), curl_exec(), curl_multi_exec(), parse_ini_file(), and show_source().

Проверка на нашия код: CARSA използва инструменти за проверка със статичен код, за да сканира за уязвимости, свързани с валидиране на въвеждане и опасна оценка.

Сканиране на приложенията: дружеството използва скенер, за да гарантира, че приложенията са защитени от различни видове атаки. Например, CARSA има система за откриване на проникване.

ИДЕНТИФИЦИРАНЕ

Кибер атаката е извършена в рамките на CARSA и типът на кибер атаката е **„фишинг атака“.** Фишинг атаката е вид атака чрез социално инженерство, често използвана за кражба на потребителски данни, включително идентификационни данни за вход.

Съгласно моделът STRIDE този тип атака има като „Заплаха“ повишаването на привилегията, тъй като нарушеното свойство е „упълномощаването“. При този тип кибер атака потребителят позволява на някого да направи нещо, за което не е упълномощен.

Съгласно рамката MITRE ATT&CK, тази атака е:

☑ Разузнаване: Фишинг атака за информация: услуга спиър фишинг (фалшиви електронни писма), прикачен файл за спиър фишинг и връзка за спиър фишинг.

☑ Първоначален достъп: Фишинг: прикачени фалшиви електронни писма (спиър фишинг), чрез линк или услуга.

☑ Изпълнение: Противниците могат да изпращат фишинг съобщения, за да получат достъп до системата на жертвите. Всички форми на фишинг се осъществяват по електронен път чрез социално инженерство. Фишингът може да бъде насочен, известен като спиър фишинг. При спиър фишинга целта на противника е конкретно лице, компания или индустрия. По-общо, противниците могат да извършват нецелеви фишинг, като например в масови спам кампании за зловреден софтуер.

☑ Разкриване: откриването може да бъде извършено чрез: Регистърът на приложението (съдържание), файлът (създаване на файл) или мрежовия трафик (съдържание или поток).

☑ Странично движение: Вътрешен спиър фишинг .

☑ Ексфилтрация: Социално инженерство и фишинг атаки; изходяща поща, изтегляния към незащитени устройства, качвания към външни услуги и несигурно поведение в облака.

Въздействие: загуба на чувствителни данни, увреждане на репутацията, оттегляне или отлив на клиенти, разходи за престой и др.

РЕАКЦИЯ

КОЙ: Нападателят е неизвестно външно лице/организация, чрез служител на CARSA.

КОГО: Идентификационните данни за достъп до софтуер за плащане (без публичен или отворен код).

ЗАЩО: Кражба на идентификационни данни, както и на чувствителна информация.

КАК: Служител е инсталирал софтуер, който не е разрешен от компанията, както е определено в политиката на компанията. Този тип софтуер не е разрешен поради съмнителна надеждност и сигурност. (По принцип целият софтуер, който е инсталиран на компютрите на служителите, трябва да се контролира от компютърния технически персонал на предприятието.) Този софтуер е имал мрежов „троянски кон“. Съществуват няколко начина, по които „Троянски кон“ атакува дадена система, в този конкретен случай това е бил „infostealer trojan“ *(троянски кон използван за кражба на информация)*, както звучи, този троянски кон търси данни на вашия заразен компютър.

СТРАТЕГИЯ: Следваната стратегия беше да се проследи mac адресът, за да се идентифицират заразената машина и отговорният служител. По-късно зловреднният софтуер беше премахнат, както и вирусът.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: кражба на потребителски идентификационни данни на местно ниво

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ:

☑ Чрез MAC адреса се разкри кой служител е атакуван, без той дори да го осъзнава.

☑ софтуерът, който не е трябвало да бъде инсталиран е деинсталиран.

☑ на конкретната машина са стартирани антивирусни програми, както и програми срещу зловреден софтуер.

☑ Променени са идентификационните данни на компрометираният потребител.

ПО-ДОБРА СТРАТЕГИЯ: целият компютър би трябвало да бъде форматиран, защото никога не можете да сте сигурни в пълното премахване на зловредния софтуер.

ИЗВЛЕЧЕНИ ПОУКИ

Да се повиши отговорността на служителите, чрез :

- ☑ обучение с кратки лекции за важността да не се инсталира необявен софтуер и потвърждение за сигурност от екипа за техническа поддръжка и,
- ☑ запомняне на политиките за сигурност на компанията и общите правила за безопасност в киберсигурността.
- ☑ Да актуализира софтуера на машините на фирмата (софтуер: windows и антивирусни програми). Да напомня на служителите да стартират антивирусното сканиране няколко пъти.

КАЗУС 3: Кредитната карта в МСП чрез WIFI мрежа

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Bodegas Monje се намира в изключителен анклав на остров Тенерифе, на място, известно като „La Hollera“ в община El Sauzal с изглед към Teide. Традиция на дългогодишни винопроизводители съпровожда семейството Monje от 1750 г. Дъбови бъчви и модерни системи за накисване съществуват съвместно, за да придадат на червените, белите и розовите вина специален характер и вкусове, които са идеално адаптирани към най-добрата гастрономия на Канарските острови. Тази винарна също така е домакин на културни, гастрономически и развлекателни инициативи, които разширяват границите на виното и го връщат в социалната среда, от която исторически идва, истински ангажимент към винения туризъм: Wine&Tours.

КАК Е БИЛА ПРИДОБИТА ИНФОРМАЦИЯТА?

Методът, който беше приложен за събиране на информацията по този казус е задълбочено интервю.

ПРЕВЕНЦИЯ

Организацията не е прилагала никакви практики за киберсигурност преди това събитие. Те имат защитна стена само в интернет доставчика (рутер Movistar).

Специфичните практики за сигурност, въведени в Bodegas Monje, които имат доказан ефект при предотвратяването на този вид събитие, бяха планирани след събитието. По-специално, предприетите действия бяха успешни за предотвратяване на следващи атаки от подобен характер.

ИДЕНТИФИЦИРАНЕ

Клиент на заведението е влязъл във фирмата, за да консумира произведените продукти, и се е свързал с интернет чрез WIFI мрежата. Кибератаката е идентифицирана от самия засегнат клиент. Този човек е открил движения в банковите си сметки с онлайн плащания, направени с кредитната му карта, но не и от него. Всички тези транзакции са били извършени точно след неговото посещение в компанията „Bodegas Monje“.
Клиентът предупреждава банката, за да се опита да анулира тези плащания и да блокира картата, за да попречи на киберпрестъпника да продължи да я използва.
След това той уведомява компанията „Bodegas Monje“, тъй като това е последното място, където всъщност е използвал кредитната си карта.

РЕАКЦИЯ

КОЙ: собствен клиент на компанията, който е влязъл в локалната мрежа за незаконни цели.
КОГО: на друг клиент, чрез компанията**.**
ЗАЩО: за кражба на пари.
КАКВО: присвояване банкови данни и извършване на разходи, облагодетелствайки се от парите на някой друг.
КАК: проникване през Wifi мрежата на клиента.
СТРАТЕГИЯ: Препроектиране на мрежата, за да се отдели връзката на клиентите, посещаващи дружеството, от платежната система и вътрешната мрежа на компанията.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ:

- ☑ Кредитната карта на клиент на дружеството е компрометирана;
- ☑ Доверието на клиентите в сигурността на компанията може да бъде компрометирано и те няма да могат да разчитат на извършването на плащания по този метод толкова лесно;
- ☑ Ако повече клиенти бъдат засегнати от тази кибератака, това ще се отрази директно върху репутацията на дружеството.

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ:

Стратегията, прилагана от собственика на компанията, от момента, в който научава за инцидента, е да изключи wifi и/или да изключи мрежата за гости. След това той се свързва с компания за киберсигурност, за да разреши проблема.

Новата стратегия за възстановяване, изготвена от екипа по киберсигурност, е да се препроектира мрежата, за да се отдели

клиентската мрежа от вътрешната мрежа на дружеството, където се съхраняват най-чувствителните данни (собствените данни на служителите и клиентите, като данни на платежната система).

След препроектирането на мрежата не могат да бъдат възстановени никакви откраднати пари. Клиентът трябва да смени „откраднатата“ стара кредитна карта с нова. Лицето, извършило кибератаката, не може да бъде идентифицирано. Не е възможно да бъдат предприети правни действия.

В тази ситуация трябва да бъде предприета по-добра стратегия. Вместо да се изключва wifi мрежата на дружеството, би могло допълнително да се предприемат следните действия:

- ☑ Да се направи списък на цялата компрометирана информация, с всички данни за контакт на възможните клиенти, които биха могли да бъдат засегнати (по времева линия – на това кои са били в предприятието по същото време, по което е бил и засегнатият клиент).
- ☑ Да се информират другите клиенти, за да бъдат наясно с всякакви странни движения по техните банкови сметки, извършени с онлайн плащания, извършени с тяхната кредитна карта.
- ☑ Да се събере възможно най-много информация, за да може не само да бъде идентифициран виновникът за кибератаката, но и за да се предупредят по-добре клиентите, които също биха могли да бъдат засегнати.

Незабавно да се сменят паролите, за да се избегне внезапно спиране на дружеството, тъй като в този момент мрежата не е била разделена, и е работела едновременно, както за клиенти така за служители.

ИЗВЛЕЧЕНИ ПОУКИ

Сред извлечените поуки, се открояват следните:

- ☑ по-добре е мрежата да бъде сегментирана
- ☑ трябва да се прилагат политики на нулево доверие
- ☑ не е нужно да сте голяма компания, за да претърпите кибератака
- ☑ необходимо е да разполагате с модерно оборудване и активни системи за киберсигурност (с професионална защитна стена, IPS, антивирусна програма и др.).

КАЗУС 4: РАЗКРИВАНЕ НА ИНФОРМАЦИЯ ЗА HANESBRANDS INC.

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Hanesbrands Inc. (HBI) е мултинационална компания за облекло, основана през 1901 г. и базирана в Winston-Salem, САЩ. Те имат над 250 търговски обекта в 47 страни. Сред най-известните марки на компанията са Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold, Celebrity, Maidenform, Zorba, и др. Едно от конкурентните предимства на Hanesbrands е, че 70% от облеклото, което продават, се произвежда в собствените им помещения, както и в тези на изпълнители от партньорски организации. По този начин компанията успява да контролира по-голямата част от веригата за доставки, което

също позволява установяването на силни практики за устойчивост и допринася за нейния световен успех. През 2021 г. HBI беше обявена за една от най-етичните компании в света от Ethisphere и стана част от 100-те най-устойчиви компании на Barron три поредни години. За да гарантира, че компанията следва дългосрочна политика за устойчивост, дружеството е поставило глобални цели за устойчивост за 2030 г. (в съответствие с целите за устойчиво развитие на ООН в три стълба: хора, планета и продукт) и стартира уебсайт за устойчивост.

През 2019 г. компанията има приходи от $7,0 милиарда и около 61 000 служители. Съобщава се, че HBI харчи над $100 000 за киберсигурност, използвайки главно продукти на Akamai като облачни услуги.

КАК Е БИЛА ПРИДОБИТА ИНФОРМАЦИЯТА?

Методът, приложен за събиране на информацията за този казус е проучване по документи, като конкретните източници на информация могат да бъдат намерени в раздела за препратки на настоящия документ.

„Според нов доклад на Blumira и IBM средният жизнен цикъл на пробив отнема 287 дни, като на организациите са необходими 212 дни, за да открият първоначалният пробив и 75 дни, за да го овладеят“. (VentureBeat, 2022 г.)

ПРЕВЕНЦИЯ

☑ **Практики, които нямат ефект:** Удостоверяване на уебсайта - За да проследи своята поръчка на дрехи, потребителят получава връзка за влизане като гост в уебсайта. Гостът - потребител е имал големи права да получава информация за поръчките, направени от всички останали потребители, само чрез промяна на URL адреса на госта. Следователно базата данни е била компрометирана чрез уебсайта, тъй като не е поискала удостоверяване и е считала гостът-потребител за валиден потребител. Данните, видими за други клиенти, се състоят от имена, последните цифри на техните кредитни карти, адрес, телефонен номер и др.

☑ **Практики с доказан ефект при реални кибератаки от този тип:**

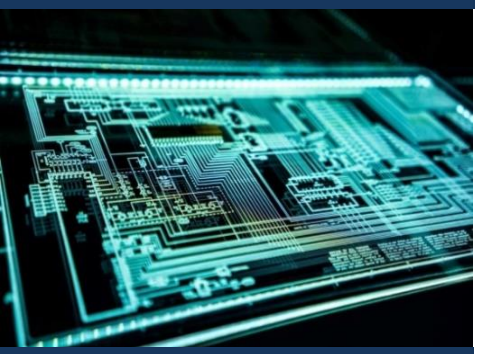
1. Откриване на излагане на данни (с помощта на външни системи за сканиране).
2. Силно удостоверяване (еднократно влизане, позволяващо на потребителя да влезе в няколко различни системи или различни потребителски имена/пароли за всяка система).
3. Приоритизиране на достъпа до данни (например, отделът по „Човешки ресурси“ може да се нуждае само от достъп до информация за служителите, а счетоводният отдел може да има нужда само от достъп до бюджетни и данъчни данни. Потребителите като гости трябва да имат минимален достъп до данни по принцип).

4. Внедряване на инфраструктури за наблюдение и автоматизирани решения, които могат бързо да идентифицират потенциални проблеми, преди да станат спешни, да изолират заразените бази данни и да сигнализират на екипите по поддръжка и ИТ за последващи действия.

ИДЕНТИФИКАЦИЯ

Атаката срещу Hanesbrands Inc. е от **типа разкриване на информация**.

През последната седмица на юни и първи юли 2015 г. Hanesbrands Inc. става жертва на кибератака. След откраднването на данните, компанията е информирана от противниците за пробива, без да посочат мотив за действията си. Много е вероятно уязвимостта на компанията да е открита чрез сканиране [1].



Нападателите създават нареждане за връзка за плащане на „гост-потребител“ на уебсайта на Hanesbrands [2] (без дори да се регистрират на уебсайта). С получената връзка за плащане, хакерите успяват да източат базата данни на компанията, която отговаря за съхраняването на данни за всички поръчки на клиенти (поръчки, направени на техния уебсайт или по телефона) – както се оказа, връзката за плащане на „гост“ има достъп до всяка друга поръчка без удостоверяване. За седмица нападателите успяват да получат информация за над 900 000 клиенти. За да не бъдат разкрити, хакерите най-вероятно са използвали Port Knocking *(Почукване на портове)* [3], за да скрият дейността си. Според Hanesbrands, хакерите са използвали снимка на екрана [4] за извличане на данните, но е много вероятно те да са използвали по-автоматизиран начин – като например скрипт, който ще анализира данните директно [5].

Атаката, описана от рамката MITRE ATT&CK:
[1] Активно сканиране: Сканиране на уязвимостта (T1592.002).
[2] Първоначален достъп: Използване на публично приложение (T1190).
[3] Постоянство: Сигнализация на трафика: Почукване на портове (T1205.001).
[4] Заснемане на екрана (T1113).
[5] Автоматизирано събиране (T1119).

Атаката е идентифицирана от компанията, след като е уведомена от нападателите. Hanesbrands не са знаели, че това се случва, докато хакерите не са ги уведомили.

РЕАКЦИЯ

През юни 2015 г. компанията Hanesbrands Inc. е информирана от нападателите за пробива. Чрез акаунт за плащане като „гост“ на нейния уебсайт, нападателите успяват да извлекат обща потребителска информация за 900 000 клиенти. След като са уведомени за изтичането на информация, Hanesbrands са добавили удостоверяване към своята база данни „поръчки на клиенти“ и опцията „плащане като гост“ е премахната (въпреки, че е коригирана).

КОЙ: Неизвестен извършител.

КОГО: Hanesbrands Inc.

ЗАЩО: Това беше целенасочена атака за получаване на информация за клиентска база данни и списъци с клиенти, но в крайна сметка не беше поискан откуп от противниците. Те току-що бяха информирали Hanesbrands, че са получили данните.

КАКВО: Обща клиентска информация за 900 000 клиенти – имена, адреси, информация за състоянието на поръчката на клиента, телефонни номера и последните 4 цифри от кредитната му карта. Но потребителските имена или паролите на клиентите не са били разкрити. Хакерите не са компрометирали корпоративните системи на Hanesbrands.

КАК: Нападателите са създават нареждане за плащане на акаунт като гост на уебсайта на Hanesbrands. Представяйки се за „гост“, който проверява поръчка (нападателите не са били регистрирани на уебсайта), те успяват да намерят пробив в базата данни на Hanesbrands, използвайки връзката на нареждането. Хакерите успяват да получат достъп до детайлите и статуса на поръчките на клиентите и да извлекат данните за около седмица, използвайки опцията „използване с плащане“ на уебсайта.

СТРАТЕГИЯ: След като са уведомени за пробива от противниците, Hanesbrands добавят удостоверяване към своята база данни, за да спрат изтичането на информация. В допълнение, те са поправили функцията плащане като „гост потребител“, чрез която изтичането е било управлявано. От Hanesbrands са уведомили клиентите си за нарушението чрез електронна поща и писма. След този инцидент, всяка година Hanesbrands инвестира все повече и повече в киберсигурността.

ВЪЗСТАНОВЯВАНЕ

- ☑ **ВЪЗДЕЙСТВИЕ:** Последствията са изтичане на обща информация за клиентите. Не се разкриват съдебни дела или други преки щети.
- ☑ **СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ:** Hanesbrands са информирали своите клиенти за пробива. Поправена е връзката „гост потребител“ [1], за да няма директен достъп до базата данни и като цяло е деактивирана като опция [2]. Предлага се обслужване на клиенти, за да се предоставят отговори, в случай че потребителите имат притеснения. Освен това е извършен на сигурността[3] и сканиране за уязвимости[4] на техните съществуващи системи и се инвестира в обучения по киберсигурност[5].

Описаните от рамката MITRE ATT&CK смекчаващи мерки:

[1] Конфигурация на софтуера (M1054).
[2] Деактивиране или премахване на функция или програма (M1042).
[3] Одит (M1047).
[4] Сканиране на уязвимостта (M1016).
[5] Ръководство за разработчици на приложения (M1013).

☑ **ПО-ДОБРА СТРАТЕГИЯ:** След поправка на връзката „гост потребител“, чрез която клиент може да прегледа покупката си, тази функция беше деактивирана от Hanesbrands като опция. Вместо това, можеше да се добави мониторинг за подозрителна дейност и/или политики за преглед само на определено количество покупки.

ИЗВЛЕЧЕНИ ПОУКИ

Атаките за разкриване на информация стават много редки, тъй като има много съвременни инструменти, които осигуряват автоматична киберсигурност и съветват компаниите какво може да е потенциално изтичане. Атаката срещу Hanesbrands показва, че слабата одитна следа на базата данни и липсата на опит в сигурността могат да бъдат използвани доста лесно. В много случаи базите данни се нарушават поради недостатъчно ниво на експертиза в киберсигурността и липса на подходящо обучение/образование на нетехнически служители, които в резултат на това могат да нарушат основните правила за сигурност на базата данни. ИТ персоналът също може да няма необходимата експертиза за прилагане на политики за сигурност, провеждане на адекватни процеси и действия за докладване на инциденти.

Друг момент е, че базата данни в Hanesbrand е била уязвима поради неправилна конфигурация – базите данни обикновено стават напълно незащитени поради това. Често се забравя, че обикновено хакерите са ИТ специалисти с висок професионализъм, които със сигурност знаят как да се възползват от подобни уязвимости. На това може да се противодейства чрез деактивиране на акаунтите на базата данни по подразбиране в комбинация с обучен и опитен ИТ персонал.

Hanesbrands са имали късмет, че е изтекла само обща информация, както и че нападателите са информирали компанията, след като са извлекли всички данни, които са могли. В допълнение към това, дружеството незабавно е информирало своите клиенти за нарушението, което показва, че компанията иска да бъде откровена с клиентите си и проблемът се приема сериозно.

КАЗУС 5: СПУФИНГ (АТАКА С ПОДМЯНА) НА HUMANA

ЦЕЛЕВАТА ОРГАНИЗАЦИЯ

Humana е здравноосигурителна компания със седалище в Луисвил, Кентъки. Първоначално основана през 1961 г. като оператор на старчески дом, основната дейност на компанията се преобразува в притежаване и управление на болници, след това през 80-те години, към планове за здравно осигуряване. Към май 2015 г. Forbes оценява компанията на 26,7 милиарда долара. През 2020 г. Humana е имала приходи от 77 155 милиарда щ.д и около 48 000 служители. Месечно Humana има разходи на стойност над 100 000 щ.д. за киберсигурност. Humana използва продукти за киберсигурност като „Akamai“ (платформа за доставка в облак) и „Prolexic (решения за сигурност за защита на уеб сайтове, центрове за данни и корпоративни IP приложения от разпределени атаки за отказ на услуга (DDoS)), „Proofpoint“ (решение за защита на хората ви и критични данни от усъвършенствани имейл заплахи), програми „Alert Logic“ (откриване и реакция, управлявани с бели ръкавици) и други.

КАК Е БИЛА ПРИДОБИТА ИНФОРМАЦИЯТА?

Приложеният метод за събиране на информацията по този казус, беше документално проучване, конкретните източници на информация могат да бъдат намерени в раздела за препратки на настоящия документ.

ПРЕВЕНЦИЯ

☑ **Практики, които са с нулев ефект:** Сигнали за неуспешни опити за влизане – Humana прилага тази практика преди инцидента. Не е била ефективна, тъй като на организацията е отнело приблизително един ден, за да предприеме мерки в отговор на получените многобройни неуспешни опити за влизане.

☑ **Практики с доказан ефект при реални кибератаки:**

1. Блокиране на акаунт след неуспешен опит за влизане.
2. Блокиране на интернет трафик от чужди държави, с които организацията не работи.
3. Принудително нулиране на парола.

„Спуфингът е техника за атака, която разчита на фалшифициране на данни в мрежа по начин, който позволява на злонамерен сайт или комуникация да се маскира като надежден“. (Терминологичен речник на Cyberwire, n.d.)

ИДЕНТИФИКАЦИЯ

Атаката срещу Humana е от типа **Спуфинг (Атака с подмяна).**

На 3 юни 2018 г. Humana беше обект на сложна кибернетична атака, извършена на Humana.com. В същия ден Humana разбра за значително увеличение на опитите за грешка при влизане от IP адреси на чужди държави[1]. За да не разкрият истинското си местоположение, нападателите използват Multi-Hop Proxies [2]. Обемът на опитите за влизане в Humana.com предполага, че е стартирана голяма и широкообхватна атака. Естеството на атаката и наблюдаваните поведения показваха, че атакуващият разполага с голяма база данни с потребителски самоличности и съответните пароли, които са били въведени с намерението да идентифицират кои може да са валидни за Humana.com чрез „атака с груба сила“[3]. Прекомерният брой грешки при влизане предполагаше, че информацията за идентификационни данни не произхожда от Humana [4] (и най-вероятно е закупена от „тъмната” мрежа). На 4 юни Humana блокира IP адресите. Въз основа на тези факти, това може да бъде описано като атака с подправяне на самоличност. Противниците са събрали данни [5] за около 65 000 потребители, които включват:

- ☑ Медицински, зъболекарски и зрителни искове, включително извършени услуги, име на доставчика, дати на обслужване, такси и платени суми и т.н.
- ☑ Информация за разходна сметка, като например разходи за здравна спестовна сметка и информация за салдо.

След инцидента Humana предприема допълнителни мерки като блокиране на акаунт след неуспешен опит за влизане, блокиране на интернет трафик от чужди държави, с които организацията не работи, и принудително повторно задаване на парола.

Атаката описана от рамката MITRE ATT&CK:
[1] Интерпретатор на команди и скриптове: Мрежово устройство CLI (T1059.008).
[2] Прокси: Multi-hop Proxy (T1090.003).
[3] Атака с „груба сила“: Пълнене на идентификационни данни (T1110.004).
[4] Събиране на информация за самоличността на жертвата: Идентификационни данни (T1589.001).
[5] Автоматизирано събиране на данни (T1119).
Атаката е идентифицирана чрез предупреждения за грешки при множество опити за влизане.

РЕАКЦИЯ

- ☑ **КОЙ:** Неизвестен извършител

- ☑ **КОГО:** Humana
- ☑ **ЗАЩО:** Кражба на самоличност (вероятно за да бъде продадена на трети страни)
- ☑ **КАКВО:** Чувствителна информация за потребителите (медицински, зъболекарски и зрителни претенции, включително извършени услуги, име на доставчици, дати на обслужване, такси и платени суми и т.н.; информация за разходната сметка, като например разходи за здравна спестовна сметка и информация за салдото).
- ☑ **КАК:** Хакерите събират големи количества акаунти и идентификационни данни. След това с помощта на проксита с множество станции за атака с груба сила за влизане с акаунтите, които имат. След успешно влизане атакуващите събират потребителски данни чрез прехвърляне на данни с малък размер.
- ☑ **СТРАТЕГИЯ:** След като Humana забелязва значителното увеличение на броя на грешките при опитите за влизане, операторите за киберсигурност на дружеството са блокирали чуждестранните IP адреси, от които са направени множеството опити за влизане. След това Humana налага принудително нулиране на паролите на всички акаунти, за които е известно, че са били пробити, както и дружеството пуска продукт – предложение на членовете защита от кражба на самоличност за една година.

ВЪЗСТАНОВЯВАНЕ

- ☑ **ВЪЗДЕЙСТВИЕ:** Последствията се състоят в изтичането на поверителна информация за потребителите (медицински, зъболекарски и зрителни претенции, включително извършени услуги, име на доставчици, дати на обслужване, такси и платени суми и т.н.; информация за разходната сметка, като разходи за здравна спестовна сметка и информация за салдото). След това срещу Humana бяха заведени много дела за проявена небрежност. Няма информация дали съдебните дела са били спечелени от компанията, което предполага, че резултатите вероятно са били отрицателни.
- ☑ **СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ:** Humana е уведомила редица членове, за да ги информира за нарушението на данните, след изтичането на един месец. Също така са предприети редица стъпки за повишаване на киберсигурността на компанията, включително: 1) принудително повторно задаване на парола [1]; 2) внедряване на нови сигнали за успешни и неуспешни влизания[2] и 3) блокирани акаунти, които са били свързани с подозрителна дейност[3]. В допълнение, компанията внедри серия от технически контроли за подобряване на сигурността на уеб портала (блокиране на атаки с груба сила, защита от SQL инжектиране [4], инсталиране на SSL сертификат за сигурност [5] и т.н.). Компанията също така блокира всички чуждестранни IP адреси, които не са свързани с нейните операции[6].

  Предприети мерки от Humana за смекчаване, описани от рамката MITRE ATT&CK:

  [1] Политики за пароли (M1027).
  [2] Предотвратяване на проникване в мрежата (M1031).
  [3] Политики за използване на акаунта (M1036).
  [4] Конфигурация на софтуер (M1054).
  [5] Инспектиране на SSL/TLS (M1020).
  [6] Филтриране на мрежовия трафик (M1037).

☑ **ПО-ДОБРА СТРАТЕГИЯ:**

Humana би могла да уведоми потребителите по-рано. Също така, биха могли да добавят допълнителни мерки за сигурност като:

- Използване на автентификация, базирана на обмен на ключове между машините в мрежата на организацията или многофакторна автентификация за отдалечен достъп;
- Използване на списък за контрол на достъпа за отказ на частни IP адреси на интерфейси надолу по веригата;
- Реализиране на филтриране на входящ и изходящ трафик;
- Конфигуриране на рутери и комутатори – ако е възможно – за отхвърляне на пакети, произхождащи извън локалната мрежа на организацията, която твърди, че произхожда от нея;
- Активиране на сесии за криптиране на рутера на организация, така че доверените хостове извън нейната мрежа да могат сигурно да комуникират с нейните локални хостове.

ИЗВЛЕЧЕНИ ПОУКИ

Извлечените поуки могат да бъдат идентифицирани като необходимостта да се постави по-голям акцент върху защитата на личните данни на потребителите, организиране на обучения на персонала с цел повишаване на осведомеността за кибер заплахите, уведомяване на потребителите за изтичане на данни поради многобройните съдебни дела за небрежност срещу Humana след инцидента (Humana не разкрива информация, че е имало подобна атака до месец по-късно).

Ефектите от атаката са свързани не само с разходи за справяне с атаката и съдебните дела, но и с големи щети върху репутацията на Humana и надеждността на компанията. Тъй като фирмата е в сферата на здравното осигуряване, за нея е изключително важно да има най-високи мерки за сигурност и доверие на своите клиенти, тъй като данните, съхранявани в нейните системи, са много чувствителни и поверителни. Ето защо Humana беше и си остава върхова цел за кибератаки много преди посочената в този случай, а и след това. Като се има предвид това, грешката в преценката на тежестта на тази атака може да се счита за изненадваща.

КАЗУС 6: ОТКАЗ НА УСЛУГА ОТ WILLIAM HILL

ЦЕЛЕВА ОРГАНИЗАЦИЯ

William Hill е компания за онлайн хазарт със седалище в Лондон, Англия - първоначално основана през 1934 г. от William Hill. Компанията сменя собствениците си много пъти – за първи път е закупена през 1971 г. от Sears Holdings. След като беше продаден многократно през април 2021 г., той беше придобит от Ceasars Entertainment. През 2020 г. компанията имаше приходи от 1324,3 милиона британски лири и 12 000 служители (8000 в Обединеното кралство) през

2021 г. Компанията имаше повече от 1400 пункта за залагания, но през 2019 г. започна да затваря повече от 800 магазина поради ниски печалби, но твърдейки, че ще запази своите персоналът непокътнат.

William Hill is an online gambling company with headquarters in London, England - originally founded in 1934 by William Hill. The company changed hands many times – it was bought for a first time in 1971 by Sears Holdings. After being sold numerous times in April 2021 it was acquired by Ceasars Entertainment. In 2020 company had revenue of £1,324.3 million and 12000 employees (8000 in UK) in 2021.The company used to have more than 1400 betting shops but in 2019 it started closing more than 800 shops due to low profits but claiming they will keep its personnel intact.

Monthly, William Hill are spending over $100,000 for cyber security. The firm is using cyber security products like “Prolexic“ (security solutions for protecting web sites, data centers, and enterprise IP applications from Distributed Denial of Service (DDoS) attacks)”, “Proofpoint” (solution to protect your people and critical data from advanced email threats), “F5 BIG-IP Application Security Manager” (flexible web application firewall that secures web applications in traditional, virtual, and private cloud environments) , “Check Point” (protects its customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and advanced targeted threats), etc.

КАК Е БИЛА ПРИДОБИТА ИНФОРМАЦИЯТА?

Методът, приложен за събиране на информацията за този казус е документално проучване, конкретните източници на информация могат да бъдат намерени в раздела за препратки на настоящия документ.

ПРЕВЕНЦИЯ

☑ **Практики, който нямат ефект:**

1. Мрежово разпространение на Anycast – William Hill има такъв тип защита – която е полезна за задържане на огромни количества клиенти, посещаващи уебсайта на компанията, или може да претопи огромни количества нежелан мрежов трафик (като DDoS атака). Тази стратегия обикновено работи в повечето случаи на DDoS атаки.
2. Простото увеличаване на честотната лента на мрежата (колко трафик може да побере) не се оказва ефективно при тази атака.

☑ **Практики с доказан ефект при реални кибератаки от този тип:**

1. Внедряване на DDoS защита на ниво сървър – допълнителни правила, които помагат за идентифициране и блокиране на злонамерен мрежов трафик.
2. Добавяне на мрежово разпространение на Anycast на трета страна – това може да помогне на компаниите да увеличат значително способността си да поемат много повече мрежов трафик или да се справят с DDoS атаки.

ИДЕНТИФИЦИРАНЕ

Атаката срещу William Hill е била от **типа „Отказ на услуга”.**

На 1 ноември 2016 г. Компанията William Hill е била обект на високопроизводителна дистрибутирана атака от типа „отказ на услуга“[1]. Преди атаката, нападателите са събрали информация относно подробностите за мрежата на уебсайта на William Hill[2]. След това хакерите заливат уебсайта на William Hill със заявки за трафик, така че той не може да функционира правилно. Атаката отказва клиентите да правят залози за мачовете от Шампионската лига на УЕФА във вторник вечерта. Атаката срещу William Hill е била извършена с помощта на зловреден софтуер, наречен „Mirai”[4], който създава мрежа от множество компютърни системи, известна като „botnet”[3], за да започне чрез тях атака за отказ от услуга (DDoS).

„Според Cloudflare през четвъртото тримесечие на 2021 г. производствената индустрия е получила най-много DDoS атаки на ниво приложение, записвайки 641% увеличение спрямо тримесечието на броя на атаките“. (Cook, 2022)

Атаката описана от рамката MITRE ATT&CK:

[1] Мрежов отказ от услуга: Директно наводняване на мрежата (T1498.001).
[2] Събиране на информация за мрежата на жертвата: IP Адреси (T1590.005).
[3] Придобиване на архитектура: Botnet *(Ботнет)* (T1583.005).
[4] Саморазпространяващ се вирус червей, който използва база данни с идентификационни данни по подразбиране. С тези идентификационни данни IoT устройства (интелигентни устройства като фитнес тракери, гласови асистенти, аксесоари за интелигентен дом и др.) се сканират и заразяват.
Атаката е била идентифицирана веднага след като уебсайтът на William Hill престава да реагира и да бъде достъпен.

РЕАКЦИЯ

КОЙ: неизвестен извършител.
КОГО: William Hill.
ЗАЩО: Бизнес вражди – много е вероятно съперникът на компанията да предприеме подобни действия, особено по време на популярни спортни събития като Шампионска лига на УЕФА / Изнудване – ако William Hill не успее да се справи със ситуацията, вероятно ще бъде поискан откуп
КАКВО: Уебсайтът на William Hill спря да работи за 24 часа, което причини загуби за £4,4 милиона. Отне дни на William Hill да възстанови напълно своите системи и уебсайт.
КАК: На уебсайта на William Hill беше извършена високоефективна насочена атака за отказ на услуга с „ботнет“ мрежа (множество компютри, които бяха заразени със зловреден софтуерен вирус и

използвани за извършване на такава атака без тяхно знание или съгласие), създадена от зловреден софтуер, наречен „Mirai“.

СТРАТЕГИЯ: След като беше забелязано, че уебсайтът не работи, ИТ специалистите на William Hill започнаха да филтрират входящия трафик. William Hill използва мрежова дифузия на Anycast - изпращане на мрежов трафик, разпръсквайки го в мрежа от сървъри на компанията. Това смекчаване разпредели мрежовия трафик до точката, където трафикът се поема от мрежата на компанията. Полезността на тази стратегия зависи от това колко голяма е мрежата на компанията и колко голяма е атаката за отказ на услуга (DDoS). В случая с William Hill – дори с неговата първокласна инфраструктура и сигурност не беше достатъчно, за да се справят с подобна атака.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: DDoS атаката срещу William Hill накара сайта му да остане недостъпен за повече от 24 часа, през които клиентите не са могли да залагат на мачовете от Шампионската лига на УЕФА. Това е довело до загуби за над £4,4 милиона за един ден. За щастие на William Hill само уебсайтът му беше набелязан, което запази чувствителните данни на потребителите непокътнати (което е улика, че хакерите са искали да откажат на потребителите да посещават уебсайта, а не да откраднат данни). Отне над 4 дни денонощна работа на ИТ специалистите на William Hill, за да възстановят своя уебсайт и засегнатите системи.

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ: За да се справи с атаката, William Hill филтрира входящия мрежов трафик[1]. Филтриране на мрежовия трафик – блокиране на трафика за атака и разрешаване само на легитимен такъв. Също така, компанията започна да използва доставчици на мрежова дифузия Anycast на трети страни (компании, които предлагат такъв тип услуга – която размива DDoS атаката, когато разпръсква целия входящ трафик през мрежата си).

ПО-ДОБРА СТРАТЕГИЯ:

☑ Проверка на изправността на хоста, която ще предупреди ИТ специалистите на компанията, когато се открие ненормално използване на мрежата [2]. Ако бъдат открити навреме, могат да се предприемат действия, за да се поддържа услугата на уебсайта достъпна.

☑ Може да се използва „маршрутизиране на черни дупки“. Това е техника, която насочва както законния, така и злонамерения трафик към нулев маршрут и отпада от мрежата. Това не е идеалното решение, тъй като прави уебсайта недостъпен.

☑ Ограничаване на скоростта. Това ограничава броя на заявките, които сървърът може да получи – сам по себе си не може да спре DDoS атаката, но е полезен инструмент в цялостната стратегия за защита.

Стратегията за възстановяване описана в рамките на MITRE ATT&CK:

а) [1] Филтриране на мрежовия трафик (M1037).
б) [2] изправност на сензорите: Статус на хоста (DS0013).

ИЗВЛЕЧЕНИ ПОУКИ

Атаката срещу William Hill може да ни покаже, че дори компания с изключителна киберсигурност и такава, която е готова да се справи с подобни атаки, може да пострада от тях.

Въпреки че нейният уебсайт беше свален от DDoS атака (обикновено подобни атаки са само димна завеса за действителната атака), сигурността на компанията от най-високо ниво е непокътната и функционираща, като поддържа чувствителната информация на клиента защитена. Това показа на клиентите на дружеството, че са в безопасност и запази доверието в компанията. Като се има предвид, че хакерите не са се опитали допълнително да използват уязвимостта на William Hill, най-вероятно атаката е била извършена поради бизнес съперничество (конкурентна компания, която иска да се възползва от пазара на залагания) или опит за изнудване (компанията разчита на своите уебсайт и задържането му от противници генерира загуби).

С навлизането в ерата на интелигентните устройства (IoT), когато всичко може да се управлява дистанционно (интелигентни домашни лампи, прахосмукачки, хладилници, смарт часовници и др.), трябва да помислим и за сигурността, която трябва да се прилага. Всички тези смарт устройства имат IP адрес и могат да бъдат хакнати през мрежата – за получаване на информация или „зомбирани“ (устройството ви се контролира без да знаете и започва да работи по странен начин) и използвани в DDoS атаки за наводняване на уебсайт.

КАЗУС 7: COBALT STRIKE: ИЗПОЛЗВАНЕ НА ЧЕРВЕНИ ЕКИПНИ ИНСТРУМЕНТИ ОТ КИБЕР ПРЕСТЪПНИЦИ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Cobalt Strike е инструмент за обединяване на червени екипи, разработен още през 2012 г. Основната му цел е да помогне на червените екипи да тестват и симулират кибератаки. Тъй като

инструментът има добри възможности за заобикаляне на границите на сигурността чрез укриване, нападателите са отвлекли някои негови версии, за да го злоупотребяват като инструмент за доставка на злонамерени полезни товари, като рансъмуер. Този казус не се фокусира върху една организация, тъй като Cobalt Strike се използва в природата за извършване на масови атаки, насочени към различни типове организации като фабрики, финансови институции, телекомуникационни компании и др.

КАК Е БИЛА ПРИДОБИТА ИНФОРМАЦИЯТА ?

Методът, приложен за събиране на информацията за този казус е проучване по документи, като конкретните източници на информация могат да бъдат намерени в раздела за препратки към настоящия документ.

ПРЕВЕНЦИЯ

Откриването и предотвратяването на атака, която използва инструментите на червения екип Cobalt Strike, включва верига за сигурност в цялата инфраструктура. Това започва още със софтуера за защита и наблюдение на клиента на крайната точка и стига до нивото на мрежата. Освен това активното разузнаване на заплахи също е необходимо, за да се поддържат актуални базираните на сигнатури инструменти за откриване.

Това основно включва:

- ☑ Сигурност на крайната точка (като антивирусна програма, хост-базиран мониторинг)
- ☑ Мрежова сигурност (като защитна стена, прокси, откриване на подпис/модел в трафика)
- ☑ Сигурност на електронната поща
- ☑ Правилно конфигурирани правила за хост/сигурност

ИДЕНТИФИЦИРАНЕ

Cobalt Strike е многофункционален търговски инструмент, който изпълнява различни техники за атаки. Като се има предвид самият инструмент и неговите възможности, той може да бъде категоризиран като Разкриване на информация и Повишаване на привилегия. Въпреки това, тъй като може да се използва и за допълнително премахване на злонамерени полезни товари, особено след като бяха наблюдавани атаки на ransomware в комбинация с Cobalt Strike, списъкът може да бъде разширен с подправяне и отказ на услуга.
Като се имат предвид всички характеристики на инструмента, той е инструмент за отдалечен достъп с възможности за странично движение. Това води до огромен списък от техники за атаки,

използвани от Cobalt Strike, и затова тук ще разгледаме само някои от тях.

- ☑ Механизъм за контрол на повишаване на злоупотребата (T1548) След като Cobalt Strike бъде изпълнен на система, тя има възможностите да изпълнява различни техники, използвани за получаване на по-високи разрешения.
- ☑ BITS Jobs (T1197) BITS е инструмент за Windows, който може да се използва от Cobalt Strike за изтегляне на полезни товари.
- ☑ Интерпретатор на команди и скриптове (T1059) Cobalt Strike може да използва различни инструменти за изпълнение на команди, кодове и скриптове. Това включва PowerShell, Windows Command Shell, Visual Basic, Python и JavaScript.
- ☑ Експлоатация за ескалация на привилегии (T1068) За да получи по-високи привилегии, Cobalt Strike може да използва уязвимости в операционната система.

Заснемане на вход (T1056)/Заснемане на екран (T1113) Cobalt Strike може също да действа като кийлогър (keylogger) и да събира екранни снимки от заразената система.

РЕАКЦИЯ

- ☑ **КОЙ:** Неизвестен извършител
- ☑ **КОГО:** Множество организации по целия свят
- ☑ **ЗАЩО:** Cobalt Strike се използва в множество кампании, фокусирани върху различни цели. Причината за атаката е да се получи достъп до вътрешната организационна мрежа за странично движение. Друга причина може да бъде нанасяне на щети на компании чрез атака на компрометираната мрежа с например с рансъмуер.
- ☑ **КАКВО:** Основно за отдалечен достъп, компрометиране на мрежата и странично движение..
- ☑ **КАК:** Cobalt Strike е търговски инструмент на червения екип, който се използва за симулиране на кибератаки, които са били откраднати. Инструментът се използва за получаване на първоначален достъп до фирмена мрежа, както и за по-нататъшни действия с компрометираната мрежа.
- ☑ **СТРАТЕГИЯ:** В зависимост от атакуваната компания, информацията за това как са идентифицирали и реагирали на атаката не е известна.

ВЪЗСТАНОВЯВАНЕ

- ☑ **ВЪЗДЕЙСТВИЕ:** Нападателят може да получи пълен мрежов достъп в рамките на компанията. Това може да доведе до разкриване на информация, както и до допълнителни атаки, които се извършват в зависимост от оператора на атаката.
- ☑ **СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ:** В зависимост от атакуваната компания, информацията как е изглеждала стратегията им за възстановяване е неизвестна.
- ☑ **ПО-ДОБРА СТРАТЕГИЯ:**
  - Поддържайте антивирусните системи актуални
  - Използвайте системи за откриване и предотвратяване на проникване
  - Наблюдавайте правилно системите за подозрителни дейности
  - Правилно конфигурирайте системите и деактивирайте ненужните услуги
  - Обучете информираността на служителите

– Използвайте сегментиране на ниво мрежа и ограничете разрешената комуникация до необходимия минимум.

ИЗВЛЕЧЕНИ ПОУКИ

Въпреки че е необходимо да се изградят червени инструменти за екипиране, които могат да се използват за симулация на атака в мрежа, за да се намерят възможни уязвими точки, все пак трябва да се има предвид, че такъв инструмент също може да бъде компрометиран и използван от нападател.

КАЗУС 8: АТАКА ОТ НУЛЕВ ДЕН - ХАКЕРСКА ГРУПА HAFNIUM, НАСОЧЕНА КЪМ ОБМЕННИ СЪРВЪРИ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

В началото на 2021 г. изследователите откриха множество критични уязвимости в Microsoft Exchange Server, които доведоха до масова експлоатация по целия свят. Уязвимостите бяха използвани в публичното пространство от множество престъпни организации, най-вече от групата HAFNIUM, преди да бъдат предоставени корекции от Microsoft. Това направи атаките особено трудни за реагиране и възстановяване от тях.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Приложеният метод за събиране на информацията по този казус е документално проучване, като конкретните източници на информация могат да бъдат намерени в раздела за препратки към настоящият документ.

ПРЕВЕНЦИЯ

Десетки хиляди компании бяха засегнати от тази атака. Поради общото излагане на сървърите на Microsoft Exchange на интернет и потенциала за заобикаляне на удостоверяването на атаката, на първо място беше много трудно атаката да бъде предотвратена. Това допълнително води до предположението, че различните практики за сигурност, които се прилагат за тези компании, са били с нулево въздействие.

ИДЕНТИФИЦИРАНЕ

Има четири различни уязвимости, довели до описаните атаки. Уязвимостите са **CVE-2021-26855, познато като ”ProxyLogon”, CVE-2021-27065, CVE-2021-26857, и CVE-2021-26858**. Техниката за използване на тези уязвимости е описана като **„Експлоатация за клиентско изпълнение“ (T1203)** в рамките на MITER ATT&CK.

CVE-2021-26855 е байпас за удостоверяване, използващ вътрешния прокси сървър от Exchange Server. С това нападателят може да получи привилегирован достъп до самия сървър. Комбинирането му с друга уязвимост като CVE-2021-27065, която позволява запис на произволни файлове в системата, или CVE-2021-26857, за получаване на достъп до СИСТЕМАТА (T1078) чрез несигурна десериализация, създава верига за експлоатация без ограничения.

Атаките са извършени в средата, преди Microsoft да успее да пусне корекция за уязвимостите. Според множество източници този период от време е бил около 58 дни експлоатация от нулевия ден. Първата група, която е свързана с тези уязвимости, е HAFNIUM. По-късно множество други групи започнаха да злоупотребяват с тези уязвимости. Възможностите на атаката позволиха множество сценарии, вариращи от кражба на данни (T1567) до внедряване на ransomware (T1486).

Следва списък на действията, предприети от групата HAFNIUM, използвайки този вектор на атака:

☑ T1589 – Събиране на имейл адреси за потребители, към които са възнамерявали да се насочат

☑ T1071 – C2 рамка с отворен код (напр. спогодба)

☑ T1560 – 7-Zip, WinRAR за компресиране на откраднати файлове за извличане

☑ T1059 – Експортиране на данни от пощенска кутия чрез PowerShell

☑ T1567 – Ексфилтриране на данни чрез сайтове за споделяне, включително MEGA

☑ T1105 – Изтегляне на зловреден софтуер и инструменти на компрометирани хостове (напр. Nishang, PowerCat)

☑ T1003 – Изхвърляне на идентификационни данни на LSASS и бази данни на Active Directory (NTDS.DIT)

☑ T1505 – Разполагане на WebShells на компрометирани хостове (SIMPLESEESHARP, SPORTSBALL, и др.)

Идентифицирането на атаките може да бъде осъществено чрез проверка на регистрационни файлове на възможни компрометирани машини. Microsoft пусна насоки за откриване на всяка уязвимост според техния индикатор за компрометиране .

РЕАКЦИЯ

КОЙ: HAFNIUM (вероятно спонсорирана от държавата група с връзки с Китай).

КОГО: различни компании по целия свят, предимно американската индустрия.

ЗАЩО: Ексфилтриране на данни и вероятно печелене на пари чрез рансъмуер

КАКВО: Фирмена информация, като данни, имейл адреси, пощенски кутии

КАК: Използване на множество уязвимости в Microsoft Exchange Server, за да се позволи не-автентифицирано дистанционно изпълнение на код

СТРАТЕГИЯ: Сканиране на IP обхвата на интернет за събиране на IP списъци на Microsoft Exchange сървъри. Използване на споменатите уязвимости за внедряване на уеб черупки или C2 маяци. Използването на този достъп позволява компресиране и ексфилтриране на данни чрез уебсайтове за онлайн споделяне като MEGA. От време на време внедряване на рансъмуер „DearCry“. Това е възможно поради късен ъпдейт и лошото управление на ъпдейта от компаниите.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Последствията от настоящата атака могат да се считат за загуба на информация, тъй като ексфилтрацията и рансъмуерът попадат в тази категория. Освен това, ако организациите са се опитали да платят откупа, за да си върнат данните, те също така са претърпели и финансови щети.

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ: В зависимост от конкретната атака възстановяването може да се различава. Процесът на възстановяване от рансъмуер може да отнеме много време. Всички заразени системи трябва или да бъдат преинсталирани, или трябва архивираното копие да бъде върнато. Ако архивите са били съхранени в заразена система, те очевидно не могат да бъдат използвани в процеса на възстановяване. Възстановяването от кражба на данни е различно. Първоначално трябва да се приложат налични ъпдейти и да се отстранят следи от уеб черупки или C2 маяци. Важно е да се оцени кои и колко данни са откраднати, за да може да се измери въздействието.

ПО-ДОБРА СТРАТЕГИЯ

- ☑ Поддържайте антивирусните системи актуални
- ☑ Използвайте системи за откриване и предотвратяване на проникване
- ☑ Наблюдавайте правилно системите за подозрителни дейности
- ☑ Правилно конфигурирайте системите и деактивирайте ненужните услуги
- ☑ Бързо управление на корекции за отстраняване на уязвимости възможно най-скоро
- ☑ Използвайте сегментиране на ниво мрежа и ограничете разрешената комуникация до необходимия минимум

ИЗВЛЕЧЕНИ ПОУКИ

Експлоатацията от нулев ден с вериги за атаки изглежда много смущаваща. Ключът към справянето с тези предизвикателства е правилното сегментиране на мрежата и мониторинг на системата за своевременно идентифициране на възможни атаки. Системите за мрежово проникване и предотвратяване също могат да помогнат за откриването на такива атаки. Това, което също е важно е, че ъпдейтите за критични уязвимости трябва да бъдат приложени възможно най-скоро, за да се коригират допълнително векторите на атака.
Като друга извлечена поука искам да спомена изследователите по сигурността от DevCore, които първи откриха уязвимостите и помогнаха на Microsoft в процеса на корекция. Това засилва значението на независимото изследване на сигурността в името на добрата кауза.

КАЗУС 9: WannaCry: КОГАТО СОФТУЕР ЗА ОТКУП ПАРАЛИЗИРА ЗДРАВНАТА СИСТЕМА

ЦЕЛЕВА ОРГАНИЗАЦИЯ

През 2017 г. нов софтуер за откуп (рансъмуер), наречен WannaCry (WannaCrypt), който е насочен към операционната система на Windows, зарази хиляди и хиляди клиенти по целия свят. Вместо да е насочена към конкретна организация, атаката беше широко разпространена и засегна много компании в различни области.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Приложеният за събиране на информация метод по този казус е документално проучване, като конкретните източници на информация могат да бъдат намерени в раздела за препратки на настоящия документ.

ПРЕВЕНЦИЯ

Множество компании са засегнати от тази атака, което води до предположението, че различните практики за сигурност, които се прилагат за тези компании, са имали нулево въздействие.

ИДЕНТИФИКАЦИЯ

WannaCry е злонамерено приложение, което се класифицира като **рансъмуер**, тъй като криптира специфични за потребителя файлове в целева система. Това води до подправяне на данните и тяхното унищожаване, тъй като собственикът на заразената система не може да дешифрира файловете. Това впоследствие завършва с атака за отказ на услуга поради липсващите файлове и данни.

Една от основните характеристики на WannaCry е неговата техника, използвана за автоматично търсене на потенциални целеви системи, които впоследствие рансъмуерът също се опитва да зарази. Тъй като този зловреден софтуер може да зарази други системи от вече заразена такава, той също се нарича червей. За постигането на тази цел се използва експлойт за софтуерна уязвимост в SMB протокола на Microsoft Windows, наречен Eternal Blue, който се свързва с MITER ATT&CK ID T1210.

Преди злонамереният софтуер да може да се разпространи и зарази други системи, той първо трябва да ги търси и намери. Това се осъществява чрез различни техники като сканиране за отдалечени системи (T1018), изброяване на активна сесия на отдалечен работен плот (T1563), сканиране за нови прикачени устройства на заразената система (T1120). След като бъде

намерено потенциално отдалечено устройство или диск, WannaCry се опитва да се копира в целевата система и изпълнява злонамереното си поведение.

Преди рансъмуерът да стартира своето криптиране, той извършва промени в заразената система, за да деактивира опциите за възстановяване, което се посочва от T1490. След това търси специфични за потребителя файлове в различни директории (T1083) и започва да криптира всеки намерен файл (T1486). За комуникация на команден и контролен сървър се използва мрежата Tor (T1573/T1090).

За идентифициране на тази атака въз основа на поведението могат да се използват следните техники на MITRE ATT&CK:

- ☑ T1210: Използване на отдалечени услуги
- ☑ T1018: Откриване на отдалечена система
- ☑ T1563: Отвличане на сесия на отдалечена услуга (отвличане на .002 RDP)
- ☑ T1120: Откриване на периферно устройство
- ☑ T1490: Инхибиране на възстановяването на системата
- ☑ T1083: Откриване на файлове и директории
- ☑ T1486: Шифровани данни за въздействие
- ☑ T1573: Криптиран канал (.002 асиметрична криптография)
- ☑ T1090: Прокси (.003 Multi-hop Proxy)

„Разпространението на WannaCry засяга над 200 000 компютъра в над 150 държави. Това коства на Обединеното кралство 92 милиона £ и глобални разходи, които възлизат до колосалните 6 милиарда £“. (Acronis, 2020 г.)

РЕАКЦИЯ

През 2017 г. нов рансъмуер, наречен WannaCry (WannaCrypt), който е насочен към операционната система Windows, заразява хиляди и хиляди клиенти по целия свят. Вместо да е насочена към конкретна организация, атаката е широко разпространена. Големи компании, като някои от тях управляват бизнеса си в световен мащаб, като производителя на автомобили са засегнати от рансъмуера. Засегнати обаче бяха и други организационни групи като обществен транспорт, здравни услуги или телекомуникационни услуги.

- ☑ **КОЙ:** Неизвестен извършител
- ☑ **КОГО:** Различни компании по целия свят
- ☑ **ЗАЩО:** Постигане на големи щети поради загуба на данни и вероятно за печалба на пари
- ☑ **КАКВО:** Фирмена информация, като данни
- ☑ **КАК:** Заразяване с рансъмуер, който е разпространен чрез открита уязвимост в Microsoft Windows
- ☑ **СТРАТЕГИЯ:** Бележката за откуп, използвана от WannaCry, се появява на екрана на системите, които са заразени. Антивирусните системи и защитните стени забелязват заразата и разпространението

на рансъмуера и следователно не възпират по-нататъшното заразяване на системите и щетите.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Последствията от тази атака могат да се считат за загуба на инфо рмация, тъй като всички файлове, които са били криптирани от рансъмуера, вече не могат да се четат. Освен това, ако организациите са се опитали да платят откупа, за да си върнат данните, те също са претърпели и финансови щети.

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ: Процесът на възстановяване от рансъмуер може да отнеме много време. Всички заразени системи трябва или да бъдат преинсталирани, или трябва да бъде върнато резервното копие. Ако архивите са били съхранени в заразена система, очевидно те не могат да бъдат използвани в процеса на възстановяване.

ПО-ДОБРА СТРАТЕГИЯ

- ☑ Keep antivirus systems up to date
- ☑ Use Intrusion Detection and Intrusion Prevention Systems
- ☑ Properly monitor systems for suspicious activities
- ☑ Properly configure systems and disable not required services
- ☑ Fast patch management to fix vulnerabilities as soon as possible
- ☑ Train awareness of employees
- ☑ Use segmentation on a network level and limit the allowed communication to a required minimum

ИЗВЛЕЧЕНИ ПОУКИ

В днешно време, атаките със софтуер за откуп са често срещани и могат да засегнат всички компании. Силно препоръчително е да се следват познатите практики за сигурност, за да може ИТ инфраструктурата да бъде възможно най-сигурна, с оглед ограничаване до минимум на щетите от атаката.

КАЗУС 10: ШПИОНИРАНЕ НА ЧУВСТВИТЕЛНИ ЛИЧНИ ДАННИ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

През есента на 2020 г. на национално ниво беше обявен нов сигнал за тревога по отношение на киберсигурността. По-точно, много публични и частни субекти са били сериозно засегнати, подобно на други предишни последователни вълни, от **злонамерени атаки от типа EMOTET**, което води до множество проблеми. EMOTET е **злонамерен софтуер**, който заразява компютри, работещи с операционната система Microsoft Windows чрез заразени злонамерени връзки или прикачени файлове (напр. PDF, DOC, ZIP, и др.).

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Необходимата информация за описание на тази кибератака беше събрана чрез интервю с ИТ техник на компанията. Взаимодействието беше осъществено при условие за анонимно запазване на чувствителната информация. Дори и интервюираният да желаеше да опише инцидента, част от информацията не можеше да бъде получена, тъй като проблемът е бил делегиран на специализирана компания и трябваше да бъде разследван отделно.

ПРЕВЕНЦИЯ

Въпреки че са проведени кампании от специализирани субекти и организации за повишаване на осведомеността относно мерките, които трябва да бъдат предприети, според съществуващите доклади са били засегнати много публични и частни организации.

В случая на анализираната компания, от гледна точка на киберсигурността, действаха специфични процедури и механизми, но те не са били достатъчни поради ниския опит в областта на дигиталната област на някои служители.

ИДЕНТИФИКАЦИЯ

Emotet е троянски кон, първоначално свързан с банкови измами, който от 2017 г. е ограничен до спам и вторично разпространение на полезни данни. В момента могат да бъдат идентифицирани множество варианти на Emotet и за съжаление този зловреден софтуер продължава да се развива в нови варианти с по-сложни възможности и техники за избягване.

Въз основа на предоставените описания и допълнителни съобщения от медиите, следните подробности са включени в инцидента:

- ☑ Получен е фишинг имейл, проектиран чрез социално инженерство, с прикачен компресиран архив и парола, включена в съобщението.
- ☑ Зловредният софтуер е шифрован и защитен с парола в архивиран файл
- ☑ Избягване на решенията за защита от злонамерен софтуер чрез използване на защитени с парола архиви като прикачени файлове
- ☑ Програмата за зареждане на троянски кон съдържа доброкачествен код от Microsoft DLL за избягване на антивирусни решения
- ☑ Отвличане на нишки за разпространение на зловреден код, използвайки защитени с парола архиви като прикачени файлове
- ☑ Компрометираните системи са използвани за изпращане на злонамерени имейли до други контакти
- ☑ Системите за електронна поща се изключват временно, за да спрат по-нататъшното разпространение на троянския кон
- ☑ Засегнати вътрешни мрежи

Съгласно рамката на MITER ATT&CK тази честота може да бъде описана по следния начин:

1. T1566.001 – Прикачен файл за спиър фишинг
2. T1204.002 – Потребителско изпълнение: Злонамерен файл
3. T1027 – Скрити файлове или информация
4. T1036 – Маскиране
5. T1586.002 – Компрометирани акаунти: имейл акаунти
6. T1586.002 – Компрометирани акаунти: имейл акаунти
7. T1499 – Крайна точка на отказ на услуга
8. T1498 – Мрежов отказ на услуга

“ЕМОТЕТ е много повече от просто зловреден софтуер. Това, което прави ЕМОТЕТ толкова опасен, е, че злонамереният софтуер е предложен за наемане на други киберпрестъпници, за да инсталират други видове зловреден софтуер, като банкови троянски коне или рансъмуери, на компютъра на жертвата. (ЕВРОПОЛ, 2022 г.).”

РЕАКЦИЯ

КОЙ: Нападателят не може да бъде идентифициран точно. Единствено е известно мястото на произход, Виетнам.
КОГО: не е конкретно насочена атака
ЗАЩО: Събиране на чувствителни данни и изплащания за откуп
КАКВО: Фирмени/ потребителски данни
КАК: Прикачен файл за спиър фишинг, изпълнение на скрипт, инжектиране на процес.
СТРАТЕГИЯ: Заплахата е започнала от компютър без антивирусна програма и се е разпространила странично. Извършено е почистване от специализирана в IT&C фирма.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Основните последици от атаката са следните:

- ☑ Загуба на данни
- ☑ Нарушаване на редовната активност
- ☑ Компрометиране на системата
- ☑ Финансови разходи

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ: Стратегията за възстановяване е насочена към почистване и преинсталиране на компрометираните компютри, почистване и/или повторно активиране на компрометираните имейл кутии.

ПО-ДОБРА СТРАТЕГИЯ

- ☑ Инсталиране и поддръжка на актуализиран антивирусен/антизлонамерен софтуер
- ☑ Прилагане на защита срещу проникване в мрежата

- ☑ Ограничаване на уеб базираното съдържание
- ☑ Осигуряване на информираност на потребителя
- ☑ По-добри политики за пароли
- ☑ Привилегировано управление на акаунти
- ☑ Деактивиране или премахване на функция или програма
- ☑ Предотвратяване на изпълнението
- ☑ Одит
- ☑ Управление на потребителските акаунти
- ☑ Превенция на поведението в крайна точка
- ☑ Политики за използване на акаунта.

Фишингът означава общ термин за атаки от типа на социалното инженерство, които се извършват в момента чрез имейли или приложения за социални мрежи.

ИЗВЛЕЧЕНИ ПОУКИ

Дори Emotet да бъде свален чрез международна съгласувана дейност, остава да се види дали това ще има въздействие в дългосрочен план.

Трябва да се отбележи, че злонамерените програми използват почти същите техники за проникване и разпространение в средата, така че е задължително да сте наясно и да бъдете внимателни, тъй като кибератаките ще продължат да съществуват и в бъдеще. Мерки като обмисляне на комуникация със света с помощта на компютър, изолиран от мрежата, който хоства критична инфраструктура, използване на жизнеспособни и актуализирани решения за сигурност, обмисляне наличието на най-нови актуализации са някои мерки, които трябва да бъдат предвидени.

КАЗУС 11: ПОЛУЧАВАНЕ НА НЕЗАКОНЕН ДОСТЪП ДО ИДЕНТИФИКАЦИОННИ ДАННИ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Както във всяка съвременна компания и в този казус най-предпочитаният начин за комуникация с клиентите и доставчиците на компанията са електронните комуникации през Интернет. В рамките на този вид комуникация, една от най-използваните е електронната поща. Позволява асинхронно поддържане на контакт със заинтересованите страни, управлявани по ефективен начин от повече от един човек. Компанията, установена повече от половин век на пазара, е силно развита в дигитализацията във всеки отдел, като в този контекст е включен и отделът за връзка с клиенти. За свързани служители е създадена група за електронна поща за управление на онлайн заявки от специализирани компютри, защитени с антивирусна функция и функция за филтриране на спам на имейл сървъра.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Необходимата информация за описание на тази кибератака е събрана чрез интервю с ИТ техник на компанията. Взаимодействието е осъществено при условие за анонимно запазване на чувствителната информация. Дори и интервюираният да желае да опише инцидента, част от информацията не може да бъде получена, тъй като проблемът е управляван от друг екип.

ПРЕВЕНЦИЯ

Въпреки че Националната дирекция за киберсигурност е провела кампании за повишаване на осведомеността относно мерките, които трябва да бъдат предприети, според съществуващите доклади са били засегнати много обществени, частни организации и лица.

Компанията е наложила използването на инструменти за сигурност и персонализирани правила за онлайн работа, но те не са били достатъчни поради малкия опит в областта на цифровизацията на някои служители.

ИДЕНТИФИКАЦИЯ

Фишингът обозначава общ термин за **атаки от типа на социалното инженерство**, които се извършват в момента чрез имейли или приложения за социални мрежи. Обикновено киберпрестъпниците изпращат групови непоискани съобщения. Те искат да се насочат към възможно най-много хора, за да хванат някои от тях с трика си.

Киберпрестъпниците се опитват да използват тенденцията на някакви „страхотни оферти“ или с някои административни инструкции. Много от тези видове съобщения изглеждат легитимни, тъй като използват същата визуална идентичност като на добре известни компании, онлайн услуги или приложения. Някои примери включват компании като Google, Amazon, Microsoft, Yahoo, LinkedIn и т.н. или популярни банкови услуги и приложения като това за управление на уеб базиран имейл.

Целта е достоверността да бъде постигната чрез копиране на цветовата схема, стила, логото и девизите на копираната идентичност. Използват се типични атрактивни теми.

Въз основа на предоставеното описание и допълнителни медийни доклади, следните подробности са включени в инцидента:

- ☑ Получен е социално проектиран фишинг имейл, който твърди, че е необходимо спешно да се промени паролата за достъп, за да се избегне краят на услугата;
- ☑ Предоставянето на идентификационни данни на нелегитимния субект е довело до достъп до имейл акаунта и прекратяване на легитимния достъп чрез промяна на паролата;
- ☑ Компрометираният акаунт е използван за непоискани фишинг съобщения, изпратени до съществуващите контакти и други адреси, притежавани от нападателя;

- ☑ Поради масивни спам съобщения, изпратени по интернет, имейл услугата е включена в черния списък, така че се нарушава нормалната работа;
- ☑ Системата за електронна поща е спряна временно, за да спре по-нататъшното разпращане на спам;
- ☑ Засегнати са онлайн операциите.

Съгласно рамката на MITER ATT&CK тази честота може да бъде описана по следния начин:

1. T1598.001 - Спиър фишинг услуга
2. T1598.002 - Прикачен файл за спиър фишинг
3. T1598.003 - Връзка за спиър фишинг

РЕАКЦИЯ

- ☑ **КОЙ:** Нападателят не може да бъде точно идентифициран, тъй като са регистрирани източници от няколко държави. Включено е възможно използване на VPN.
- ☑ **КОГО:** не конкретно насочена атака
- ☑ **ЗАЩО:** Събиране на чувствителни данни и изнудване за пари
- ☑ **КАКВО:** Фирмени/потребителски данни
- ☑ **КАК:** Фишинг, кражба на идентификационни данни.
- ☑ **СТРАТЕГИЯ:** Заплахата е започнала с отварянето на имитиран имейл, достъп до фалшиви връзки и изпращане на чувствителни данни. Нулирането на идентификационните данни и премахването от услугите за черни списъци бяха извършени от ИТ екипа.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Основните последствия от атаката са както следва:

- ☑ Загуба на идентификационни данни
- ☑ Нарушаване на регулярната активност
- ☑ Компрометиране на системата.

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ: Стратегията за възстановяване беше фокусирана върху нулиране на идентификационните данни и почистване на компрометираните имейли на клиенти.

ПО-ДОБРА СТРАТЕГИЯ

- ☑ Инсталиране и поддръжка на актуализиран антивирусен/антизлонамерен софтуер/ Система за филтриране на имейли
- ☑ Прилагане на защита срещу проникване в мрежата
- ☑ Ограничаване на уеб базираното съдържание
- ☑ Осигуряване на информираност на потребителя
- ☑ По-добри политики за пароли
- ☑ Привилегировано управление на акаунти
- ☑ Деактивиране или премахване на функция или програма
- ☑ Предотвратяване на изпълнението
- ☑ Одит
- ☑ Управление на потребителските акаунти
- ☑ Превенция на поведението в крайна точка
- ☑ Политики за използване на акаунта

ИЗВЛЕЧЕНИ ПОУКИ

Дори ако фишингът не е нова техника, той остава един от основните начини при много атаки срещу киберсигурността.

Трябва да се отбележи, че злонамерените програми в повечето случаи използват тази техника за проникване и разпространение в средата, така че е задължително да сте наясно и да внимавате, тъй като кибератаките по този начин ще продължат да съществуват. Следва да бъдат предприети мерки като обмисляне на използването на по-добре актуализирани защитени имейл услуги, повече осведоменост относно достъпа до имейли и правилно анализиране на легитимността на подателя,.

КАЗУС 12: ОСТАРЕЛИ ИЗЛОЖЕНИ ОНЛАЙН ПРИЛОЖЕНИЯ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

В днешно време много фирми промениха начина на предоставяне на своите услуги, като се преместиха онлайн. Такъв е случаят с неизползвания пример, където предоставяните на бюрото услуги от финансов тип, стартирани през 1998 г., са мигрирани онлайн за повече от десетилетие. Новият подход подобри цялостната дейност на компанията и удовлетвореността на клиентите. Въпреки това, тези постижения бяха възможни само след важни усилия за разработване на необходимия персонализиран собствено разработен софтуер.

Това онлайн приложение позволи на клиентите и служителите да извършват необходимите операции. Предоставената платформа, разработена в популярната по онова време рамка, се поддържаше, докато поддръжката беше налична преди пускането на новата основна надстройка. С течение на времето броят на служителите беше намален поради автоматизацията на съществуващите процеси и промените на пазара. Надграждането до новата дистрибуция беше отложено, тъй като бяха необходими основен хардуер и софтуер.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Необходимата информация за описание на тази кибератака е събрана чрез интервю с изпълнителния директор на компанията.

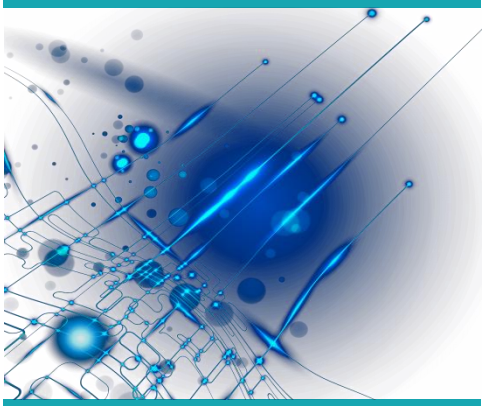
Взаимодействието беше осъществено при условие за запазване на анонимността на чувствителната информация.

ПРЕВЕНЦИЯ

Въпреки че Националната дирекция по киберсигурност провежда кампании за повишаване на осведомеността относно мерките, които трябва да бъдат предприети, много публични или частни организации пренебрегват или забавят решението и действията, необходими за актуализиране на техните информационни системи.

Компанията е наложила използването на известни решения за сигурност, защитни стени, сегментиране на мрежата и т.н., но това не е било достатъчно, тъй като остана изложена уязвимост в един от управляваните софтуерни модули.

ИДЕНТИФИКАЦИЯ



Атаките с инжектиране на поток злоупотребяват със способността на онлайн уеб приложение да приема качено съдържание, като различен тип документи или файлове с изображения. Използвайки подхода за отдалечено включване на файлове, нападателят може да използва уязвимостта в кода от страна на сървъра, за да приеме URL на друг сайт като валиден вход. Впоследствие това действие се използва за изпълнение на кода на злонамерен нападател. Освен това включването на локален файл може да се използва, за да получите уеб приложение, което да върне желаното съдържание от локалната файлова система

Популярен пример се среща в случай на PHP рамка, използвана от WordPress, позволяваща на хакера да получи достъп до нейният конфигурационен файл. Тази атака също може да позволи достъп за изтегляне на всички файлове с изходен код на PHP, работещи на уебсайта, предлагайки нови възможности за други уязвимости в сигурността. Последните версии на PHP са защитени от включване на отдалечен файл по подразбиране, но ако по погрешка включване на локален файл е изложено, този тип атака все още е възможна.

Въз основа на предоставеното описание, допълнителни технически доклади, бюлетини за сигурност и уязвимости, следните подробности са включени в инцидента:

- ☑ Чрез атака от тип груба сила се осъществява нелегитимен достъп до акаунт, защитен със слаба парола;
- ☑ Разкритите идентификационни данни позволяват да се променят данните, свързани с акаунта;
- ☑ Компрометираният акаунт позволи да бъде разкрита уязвимостта на инжектиране на поток и нежелано изпълнение на код на сървъра беше използвано за премахване на регистрационните файлове на хронологията на достъпа;

- ☑ Поради неконтролирано изпълнение на код от страна на сървъра, някои модули на приложението стават неизползваеми и водят до спиране на услугата, така че нормалната работа е нарушена;
- ☑ Системата беше временно прекъсната от интернет за по-нататъшно разследване, свързано с неизправността на уеб приложението;
- ☑ Онлайн операциите бяха засегнати.

Този инцидент може да бъде описан по следния начин съгласно рамката MITRE ATT&CK:

1. T1110.001 – Отгатване на парола
2. T1078 - Валиден достъп до акаунти
3. T1518 - Откриване на софтуер
4. T1082 - Откриване на системна информация
5. T1007 - Откриване на системна услуга
6. T0826 - Загуба на наличност

РЕАКЦИЯ

- ☑ **КОЙ:** Нападателят не може да бъде идентифициран точно.
- ☑ **КОГО:** не конкретно насочена атака
- ☑ **ЗАЩО:** Събиране на чувствителни данни и отказ на услуга
- ☑ **КАКВО:** Фирмени/потребителски данни
- ☑ **КАК:** Атака с груба сила, кражба на идентификационни данни и изпълнение на код чрез инжектиране на поток.
- ☑ **СТРАТЕГИЯ:** Заплахата е започнала от атака с груба сила, която е довела до откриване на слаби идентификационни данни, използване на уязвимост в софтуерен модул, който не е публично достъпен и след това неоторизирано изпълнение на код. Слаба стратегия за защита на онлайн достъпа, остарял софтуерен модул и неподдържан код са основната причина за инцидента.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Основните последици от нападението са следните:

- ☑ Загуба на идентификационни данни
- ☑ Компрометиране на системата
- ☑ Нарушаване на регулярната активност.

СТРАТЕГИЯ ЗА ВЪЗСТАНОВЯВАНЕ: Стратегията за възстановяване беше фокусирана върху основната надстройка на платформата, пренаписвайки важна част от кода.

ПО-ДОБРА СТРАТЕГИЯ

- ☑ Инсталиране и поддръжка на актуализиран софтуер
- ☑ Прилагане на политика за силни пароли
- ☑ Политика за използване на акаунта
- ☑ Прилагане на двустепенен механизъм за удостоверяване
- ☑ Прилагане на защита срещу на проникване в мрежата

- ☑ Ограничаване на отдалечения достъп
- ☑ Осигуряване на информираност на потребителя
- ☑ Провеждане на периодичен одит на сигурността
- ☑ Управление на потребителските акаунти
- ☑ Превенция на поведението в крайна точка

ИЗВЛЕЧЕНИ ПОУКИ

Дори ако е известно, че остарелият работещ софтуер е склонен към уязвимости в сигурността, той остава един от основните начини за много атаки за киберсигурност.

Тъй като уеб приложенията са достъпни по целия свят, те са изложени на много уязвимости и като следствие изискват специално внимание от много гледни точки.

Мерки като обмисляне на постоянно актуализиране на софтуера, подобрения и приемане на нови техники и решения за механизми за удостоверяване, приемане на процес на редовен одит са някои от общите мерки, които могат да бъдат разгледани.

КАЗУС 13: РИСКОВЕТЕ ОТ АТАКА, ИЗВЪРШЕНА ОТ БИВШ СЛУЖИТЕЛ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Организацията, срещу която е извършена кибератаката, развива дейност в областта на търговско проследяване в автомобилен клон с приблизително 2000 служители. Намира се в щата Парана и Санта Катарина в Бразилия.

Кибератаката е била насочена към областта на информационните технологии, поради познанията, които хакерът е имал поради факта, че е бивш служител на организацията, което от своя страна му дава предимството да убеди системата.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Информацията в този казус се основава на казус за рисковете от кибератака, проведена от бивш служител. Казусът е изготвен от гледна точка на организацията, претърпяла кибератаката.

Общата цел по този казус е да демонстрира значението, което компаниите трябва да обърнат във връзка със социалното инженерство в техните среди, за да избегнат нахлувания и/или измами, причинени от безразсъдството или неволното съдействие на от страна на служителите към нарушенията на хакера.

ПРЕВЕНЦИЯ

С цел предотвратяването на евентуални щети, компанията вече разполага с ИТ отдел, който управлява защитни стени, инструменти за изтичане на информация и криптиране на данни.

ИДЕНТИФИКАЦИЯ

В този казус, дигиталната следа започва с различни посещения на уеб страницата на асоциацията, с намерението да се разбере тяхната динамика, техния бизнес и особено техните

марки (като се има предвид, че нападателят е насочил търсенето на данни, които хакерът все още не е знаел). В началото на атаката и когато вътрешната и специфична информация е на страната на нападателя, той се насочва към създаването на връзки към един от магазините във веригата, за разкриване имената на мениджърите и хората, които имат привилегирован достъп в рамките на организацията. За да постигне това, нападателят се представя по телефона за клиент, който има правни проблеми с компанията. За да разреши този проблем, компанията би се обадила на клиента и би го помолила да говори с управителя на въпросния магазин, като се има предвид, че той/тя би бил човекът с най-голяма автономност, който отговаря за такава ситуация. Благодарение на това взаимодействие, името на мениджъра, мястото, където той/тя работи и телефонния номер беше лесно постижимо.

След това обаждане е направен опит за връзка с управителя по информираните канали за проверка на събраната информация. Повторното задаване на парола е извършено при контакт с отдела за информационните технологии, представяйки се за самия служител, за да накара този отдел да го информира за данните за достъп на потребителя.

Използвайки малко убеждаване и аргумента, че данните за борда зависят от този достъп, накрая техникът нулира паролата и съобщава новата парола по телефона. Нещо повече, беше възможно да бъде убеден да създаде VPN достъп (технология за отдалечен достъп до средата на компанията), така че хипотетичният потребител да може да работи извън офиса.

РЕАКЦИЯ

КОЙ: Нападателят е бивш служител;
КОГО: Организация, която работи върху търговското проследяване в автомобилния бранш;
ЗАЩО: Атаката е насочена към организацията с неизвестни мотиви;

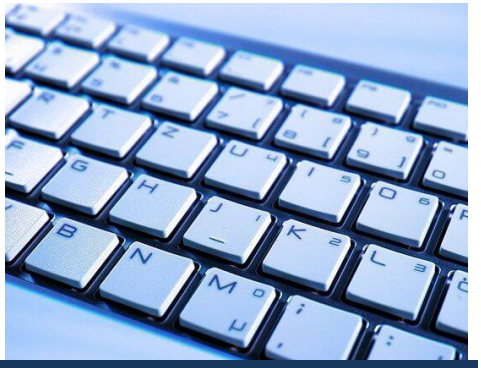
КАКВО: Набелязаният актив е отделът по информационни технологии с цел събиране на вътрешна информация за организацията и лични данни на настоящите служители;
КАК: Атаката започва с получаване на името на управителя на един магазин, продължава със свързване с отдела по информационни технологии на компанията, убеждавайки ги да нулират паролата. По този начин бившият служител се представя за управител и има достъп до всичко свързано с вътрешната информация, лични данни на служители и клиенти и каквото хакерът иска.

ВЪЗСТАНОВЯВАНЕ

Компанията е започнала да обучава сътрудниците си да обръщат внимание на видовете информация, която обикновено предават на трети страни, особено ако това е критична информация. Никога, при никакви обстоятелства, служител не трябва да предава критична информация, като например пароли, по телефона. Те трябва да бъдат предоставени на заинтересованите страни чрез безопасни методи, като препоръчани писма или чрез отговорния мениджър.

Също така, трябва да се предостави и обучение, за да се накарат служителите да бъдат внимателни с информацията, която споделят в интернет. Обучение, фокусирано върху рисковете, които споделената информация може да донесе за тяхната професия, но също и за личния живот, като отвличания, подробности от живота и лична сигурност.

Тази компания е наясно, че трябва да осигури технически и физически условия за прилагане на добри практики за сигурност, но преди всичко да цени и насърчава приемането на най-добри практики и по-строги протоколи за сигурност от своите служители, независимо дали в корпоративна или лична среда в за да се контролира по възможно най-добрия начин най-слабият фактор на информационната сигурност: човешкият фактор.



ИЗВЛЕЧЕНИ ПОУКИ

Организацията трябва да установи информацията в проста процедура, която може да разочарова хакера. Тази процедура има 3 етапа:

☑ **Публична:** Информация, която може да бъде предоставена на всеки, например на търговски контакти и конкретни корпорации, информация между клиенти и икономическата дейност на корпорацията;

☑ **Частна:** Информация, която не може да бъде предоставена на никое лице и която се отнася само до корпоративната среда. В тази категория са обхванати информация, отнасяща се до вътрешни процедури, корпоративни данни, административни и стратегически аспекти на компанията;

☑ **Конфиденциална:** Информация и данни, които не трябва да се споделят вътре и извън компанията, като данни за регистрация на служители, компенсации, резултати от сектори и стратегически действия, които се отнасят само до ръководството или председателството.

Освен това организациите трябва да имат вътрешни процедури за защита от атаки на социалното инженерство. Операторите трябва да са добре обучени за процесите, които трябва да следват, и действията, които трябва да предприемат в ситуации, в които компанията се чувства атакувана, като например прехвърляне на повикването към лице, обучено да се справя с този вид ситуации. Простите действия могат да доведат до неуспех на атаката. Веднага може да се каже, че първоначален контролен списък за потвърждаване на данните на кандидата вече би затруднил достъпа на хакера. Като се има предвид, че личните данни не са нещо много трудно за получаване, техниците биха могли да възприемат процес на връщане на контакта към регистрирания телефонен номер на служителя, за да потвърдят, че това всъщност е въпросният служител.

КАЗУС 14: КИБЕРАТАКИТЕ КАТО НОВО ПРЕДИЗВИКАТЕЛСТВО ЗА ВЪТРЕШНАТА СИГУРНОСТ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Португалските държавни органи (особено Министерството на вътрешната администрация), силите за сигурност и големи компании.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Информацията по този казус е събрана чрез документално проучване, отнасящо се до магистърска теза, където авторът прилага изследване и няколко проучвателни интервюта със специалисти и хора, отговорни за националните сили за сигурност, за да заключи дали феноменът на хактивизма представлява заплаха за португалските сили за сигурност

ПРЕВЕНЦИЯ

За да се предотвратят атаки, една от стъпките, които ИТ екипът, отговорен за киберсигурността в тези организации, предприема, е да наблюдава социалните канали, например: IRC *(общуване в интернет в реално време)*, всички видове чатове, Facebook, всичко, от което е възможно да

бъде получена информация в интернет, също така, те осъществяват проследяване и се опитват да видят дали има подозрителни действия.

Според „modus operandi“, определен от условията на групата Anonymous (Португалия), те първоначално рекламират в социалните мрежи (IRC и Facebook), действията, които ще предприемат и тогава започват да общуват помежду си. След това използват частни чат канали, за да комуникират помежду си, което доведе до внедряването на SOC (Център за операции по сигурността) към Министерство на вътрешната администрация, за да се подготвят за този тип атаки.

ИДЕНТИФИЦИРАНЕ

Последствията от тези атаки варират в зависимост от вида на атаката. Много се занимаваха с атака за отказ на услуга (DOS, DDOS), която причинява изчерпване на ресурси по отношение на системи или комуникации. Освен това те се занимават с някои типове опити за проникване, като SQL инжектиране и изтривания. Фишингът по имейл също е една от най-честите атаки, водеща понякога до достъп до лична информация.

През ноември 2011 г. беше извършена атака срещу уебсайта на Националния съюз за кариерно развитие на началниците на PSP с разкриване на лични и поверителни данни (патенти, телефонни номера и имейл адреси) на 107 служители на PSP.

„Честотата на атаките за отказ на услуга (DDoS), непрекъснато нараства през последните няколко години. Според доклад на Cloudflare DDoS атаките за откуп са се увеличили с почти една трета между 2020 г. и 2021 г. и са скочили със 75% през Q4 на 2021 г. в сравнение с предходните три месеца“. (Кук, 2022 г.).

РЕАКЦИЯ

Атаката срещу полицията за обществена сигурност беше поета от групата LulzSec Португалия. Португалската анонимна група пое отговорност за няколко атаки срещу правителствени уебсайтове и съответните институции. Обикновено профилът на хакера е на някой млад, в училищна възраст, в средно ниво (10-ти до 12-ти клас). Може да има една или друга ситуация, в която те вече са по-възрастни хора, може би с по-малко познания в технологичната област, но недоволни от обществото.

Този тип атака е достъпна за всеки гражданин. Просто човекът търси в интернет инструменти, методи и групи и започва да участва. Тези групи от анонимни хора по време на атаките провеждаха семинари за това как да се направи атака, курсове „abc“ за това как да разберем атаката. Те предоставят вече разработени инструменти и че всеки може да получи достъп до сайта, необходимо е само да вмъкнете адреса на местоназначението и приложението развива атаката

Повечето от нападателите, тоест младите хора, които все още учат, използват инструменти, които се използват от много специалисти, тези специалисти са хора с по-напреднала академична степен и по-възрастни, които използват вече разработени инструменти за целите на кибератаките. Тоест, в интернет е възможно да се търси и получава информация за извършване на атаката, как да се направи това и какви инструменти се използват, за да се помогне за осъществяването на атаката.

Атаката, извършена от LulzSec Португалия, беше оправдана в Twitter, твърдейки, че в отговор на действието на агенти провокатори са проникнали в организирана от тях демонстрация.

Но през повечето време тези атаки се случват, защото тези хора търсят видимост или искат да застрашат организациите, тъй като това често е свързано с недоволството на хората по отношение на текущия контекст, в

който живеят португалските граждани, и хората често демонстрират своето недоволство по този начин. Друг път това е просто шега за нападателите, които са на възраст между 16 или 17 години, които нямат много социални притеснения, често защото го правят приятели и за да се популяризират в групата на приятелите си, друг път това е заради преживяването, защото е ерата на експериментирането на нови неща. През повечето време те не осъзнават въздействието, което биха могли да имат тези атаки.

Всичко започва с група хакери, които имат техническите познания и разработват инструменти, които да могат да бъдат използвани от групи хора, които нямат същите познания, което прави процеса на хакване лесен за всеки.

Характеристика на португалските групи е да атакуват незащитени уебсайтове и да използват уязвимости. Те планират атаки срещу IRC *(Общуване през Интернет в реално време)* и чат стаи, не приемат вашата самоличност и не използват псевдоними. Португалските хактивисти използват наличните онлайн инструменти за извършване на атаките, т.е. „те не произвеждат персонализирани програми, а използват тези, които са налични в мрежата“.

Що се отнася до хората, които поемат организацията и ръководството на този тип инициативи, те често са хора с малък технически опит, посвещаващи се на правенето на съобщения и разпространението на действията, които трябва да бъдат разработени, и често „тези, които дори имат много специализирани технически умения , те нямат представа, че са най-компетентните и специализирани в групата, те си мислят, че са хора, които знаят малко и че просто помагат на други, които знаят повече”.

Групата Анонимните използва конвенционални хакерски методи като Havij114 и Инжектиране SQL, като основната й иновация е създаването на уебсайтове, които извършват DoS атаки (атака за отказ на услуга).

ВЪЗСТАНОВЯВАНЕ

Възможните последици са кражба на информация, недостъпност на услугите и повреди на сайта, където се правят промени в информацията, тъй като хакерите понякога премахват информация, те могат също да я добавят.

Тези атаки могат да застрашат доверието на гражданите в институциите, които са жертви на тези групи, но също така идентифицирането на уязвимости и влиянието на други хора с определени идеали са ситуации, които могат да се случат.

Тези видове атаки се развиват и техниките се подобряват с течение на времето и организациите трябва да се адаптират и да се развиват за защита на своята мрежа. Те се принуждават да спрат достъпа до мрежата, докато не бъдат изпълнени условията, за да се гарантира, че сигурността на вътрешната информация се поддържа. И те вече го правят, най-много час. Също така, в някои случаи някои услуги са недостъпни през нощта.

Разработва се Национален център по киберсигурност (CNCseg), който ще се занимава повече с въпросите за националната отбрана, отколкото Центърът по киберзащита, който е в компетенциите на Министерството на националната отбрана, чиято основна дейност е атаката срещу хакери, които може да разработват атаки , извършвайки откриването и контраатаката на тези елементи

MIA ще участва, поне в CNCseg, те работят заедно с GNS, което е субектът, който има тази компетентност и ще бъде един от информационните входове за този тип киберсигурност, идеята е този център да има информация по отношение на какво се случва на национално ниво, целта е да бъде събрана информация както от технологичните центрове на публичната администрация, банките, промишлеността, различните области на португалското общество и с това да има представа за въздействието и обхвата, които определен тип атака би могла да има.

ИЗВЛЕЧЕНИ ПОУКИ

Хактивизмът се разглежда като ново предизвикателство за институциите и, особено в случая на силите за сигурност, хактивистката атака може да причини вредни последици, които дори могат да повлияят на изпълнението на техните мисии, като следователно се считат за реална заплаха, в смисъл, че това се характеризира с противоречие на целите на организацията, причинявайки, като правило, материални и/или морални щети.

Способността на хактивистките групи да извършат атака обикновено е ниска, тъй като те използват инструменти, налични в мрежата, и не са много иновативни по отношение на хакването, като се възползват от използването на съществуващи уязвимости. Що се отнася до възможността, всеки от компютър с достъп до мрежата и с известно знание или желание да се учи от информацията, налична в мрежата, е способен да развие кибератака и този факт става тревожен за силите за сигурност.

По отношение на компютърната сигурност често се казва, че няма пълна безопасност и няма 100% сигурни системи, така че правителството и Португалия не са изключение. Това, на което сме свидетели, е създаването на набор от инфраструктури, които позволяват структура за сигурност, която може да съответства и да отговори на този тип явление: наскоро създадения CNCseg, създаден от PJ за борба с киберпрестъпността. Образовайки хората със сигурност е

нещо, което ще накара всички да осъзнаят, че ние също използваме нови технологии, интернет платформи и други мрежи, които имат силата да променят безопасността на своите граждани.

Последици от хактивистка атака срещу националните сили за сигурност:

- ☑ Преки: икономически, социални, политически и последици за сигурността.
- ☑ Косвени: чувството за сигурност, социална дерегулация и в крайна сметка суверенитета на страната, институциите и семействата.

КАЗУС 15: „ЗЛАТНАТА ЕРА“ НА „РАНСЪМУЕРА “. КАК ДА ПРЕДОТВРАТИТЕ И ДА СЕ СПРАВИТЕ С ОТВЛИЧАНЕ НА ДАННИ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Повечето португалски компании са от „поколение 3“ по отношение на киберсигурността, а атаките са от „поколение 6“. В този казус научаваме как да процедираме, за да предотвратим все по-честите атаки на рансъмуер като тази, с която се сблъсква групата IMPRESA.

IMPRESA е най-голямата медийна група в Португалия, опериращa в три икономически области — печат, цифрови технологии и телевизия.

„Рансъмуерът ще струва на жертвите над 265 милиарда долара годишно до 2031 г. (сп.“ Cybersecurity Ventures“).

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Информацията за този казус е получена чрез новинарска статия за предотвратяването на атаки със злонамерен софтуер за откуп (рансъмуер), която включва интервюто на Руи Дуро, експерт по киберсигурност.

ПРЕВЕНЦИЯ

Времената на пандемията улесниха разрастването на този тип рансъмуер атаки. От една страна, работата от вкъщи, което води до разпиляване на системите и увеличава риска. От друга страна, все повече приложения мигрират системи към „облак“.

„Това крие няколко свързани риска“, казва Руи Дуро. Системите вече са „в друг доставчик на услуги“ и е необходимо „да се закупи технология и за облака, защото тя сама по себе си не е сигурна“. За специалиста „тази еволюция към „облака“ често беше по-бърза от еволюцията на знанията на служителите в информационните технологии“.

От друга страна, много компании бяха изпреварени от сложността на атаките. „Ние (групата IMPRESA) сме в поколение 6 на защита срещу атаки и повечето от компаниите все още са в поколение 3, в много ранен етап

на защита предвид еволюцията на атаките. Манталитетът трябва да се промени, трябва да има бюджет и ресурси за адаптиране към тази нова реалност”, обяснява Руи Дуро.

ИДЕНТИФИЦИРАНЕ

На страниците на уебсайтовете на групата се появява съобщение, подобно на полученото от SIC (португалски телевизионен канал): „Вътрешните данни на системите бяха копирани и изтрити. 50 TB данни са в наши ръце. Свържете се с нас, ако искате данните обратно”.

Руи Дуро обяснява, че „обикновено рансъмуерът се появява в компаниите чрез това, което наричаме поставяне на първоначален „полезен товар“ в компанията“.

Това се случва по различни начини, като например чрез фишинг атака срещу елемент от компанията. Друг път някой от компанията по невнимание „изтегля“ зловредния софтуер. Все още има трети начин, когато участниците имат за цел да атакуват конкретна компания и търсят уязвимости - това е „целева атака“.

След като първоначалният зловреден софтуер е вътре в компанията, той изтегля втори зловреден софтуер, който изпълнява рансъмуера. След това започва да прави „сканиране“, търсейки сървъри и други системи. Целта е да се направи възможно най-голяма печалба - според експерта за престъпниците „няма смисъл да криптират един или два компютъра, идеята е да криптират колкото се може повече компютри и за предпочитане жизненоважните“.

След това хакерите инсталират зловреден софтуер на възможно най-много системи, но той не криптира данните веднага. Обикновено „се оставя за няколко седмици, понякога и повече“.

Тези, които атакуват, знаят, че един от начините за възстановяване на компаниите е чрез архивиране - така че очакват да има резервно копие и щом се възстанови, пак има инфекция.

Когато се извърши криптиране, нападателите оказват натиск върху компаниите, обикновено за да поискат паричен откуп – обикновено в криптовалути.

РЕАКЦИЯ

Два дни след като хакерската група „Lapsus$ Group“ атакува сайтовете на Impresa group, те все още са недостъпни.

Португалската съдебна полиция потвърди, че разследва случая заедно с Националния център за киберсигурност (CNCS), тъй като медийната група вече е напреднала.

Това забавяне при нулиране на системите е често срещано при атаки като тази. Според Руи Дуро, отговорен за „Check Point Software“ в Португалия, „времето, необходимо за справяне с тези атаки, варира значително. Зависи много от размера на компанията, атаката, капацитета на компанията по отношение на информационните технологии (ИТ) и колко е била подготвена компанията да подмени системите. В една малка компания понякога отнема ден или два, ако е голяма компания, може да отнеме дори няколко седмици, а понякога може да включва преработване на цяла инфраструктура“.

Атаката с рансъмуер вече се е превърнала в реална и непосредствена заплаха за компании по целия свят - и Португалия не прави изключение. За Европейската агенция за киберсигурност (ENISA) пандемията донесе със себе си „златен век“ за киберпрестъпниците.

Според агенцията между април 2020 г. и юли 2021 г. е имало 150% увеличение на регистрираните атаки.

В Португалия все още няма официални данни за последната година, но в годишния доклад за вътрешната сигурност за 2020 г., рансъмуерът вече е идентифициран като „най-често срещаната форма на компютърен саботаж, като поддържа високи нива на случаи и особено засяга институциите на правителството и малките и средни предприятия“.

Според този доклад кибератаките в Португалия са се удвоили от 2019 г. (754 инцидента) до 2020 г. (1418 инцидента). В областта на информационната сигурност, където преобладават атаките с рансъмуер, през 2020 г. е имало около 10 пъти повече инциденти, отколкото през 2019 г. Руи Дуро, ръководител на „Check Point Software“ в Португалия, обяснява, че „90 до 95% от случаите не се докладват или не са известни. Компаниите в крайна сметка се възстановяват чрез резервни копия и не докладват за атаки“.

Според данни от проучване, публикувано от ръководената от него компания, която създава технологични решения за сигурност за най-големите компании в света, португалските организации страдат средно от 947 атаки на зловреден софтуер на седмица, брой по-висок от глобалната средна стойност от 870 атаки. Около 90% от злонамерените файлове пристигат по имейл.

Данните от „Check Point Software“ показват също, че през декември 2021 г. атаките с рансъмуер са достигнали повече от 2,5% от португалските компании.

ВЪЗСТАНОВЯВАНЕ

Рансъмуерът е форма на злонамерен софтуер (комбинация от английските думи „злонамерен“ и „софтуер“), предназначен да криптира сървъри и компютърни зони за съхранение.

Обикновено „хакерите“ зад атаката показват съобщения, изискващи плащане на сума за дешифриране на системата и връщането ѝ на собственика. Според експерта по киберсигурност атаките с рансъмуер стават все по-сложни и пиратите все по-често се опитват да „удвоят или утроят изнудването“.

При двойно изнудване, „по време на периода, когато зловредният софтуер чака резервно копие, хакерите копират значителни данни от бази данни, имейл сървъри, финансови сървъри, опитват се да търсят чувствителни данни и експортират огромни количества данни. И казват, че не си струва да се опитвате да възстановите услугата с резервни копия, защото те имат данните като заложници“.

В случай на тройно изнудване, с чувствителните данни, които притежават, пиратите заплашват да се насочат към клиентите и доставчиците на компанията, ако компанията не плати откупа.

ИЗВЛЕЧЕНИ ПОУКИ

За да предотвратите атака, е необходимо да промените начина си на мислене и да приемете, че тя ще се случи. За експерта по киберсигурност това е най-важното. „Имам над 30 години на пазара, работейки в тази област, започнах, когато атаките бяха шега, в сравнение с това, което са днес, но дори днес виждам хората, вземащи решения, да си мислят, че това все още не е нещо тревожно, не е от значение и смятат, че няма да им се случи. Първата стъпка е да

променим този манталитет. Може да се случи на всеки, преди малко се случи с EDP. Когато се случи, трябва да бъдем подготвени за това“.
Погледнете сериозно на трите стълба на киберсигурността: хора, процеси и технологии:

а) Хора

„Често дори компаниите, които имат сериозно отношение към киберсигурността, се фокусират твърде много върху технологиите като начин да се защитят и забравят, че е необходимо хората да се обучават, за да имат безопасно поведение“, казва експертът.

б) Процеси

„Важно е да има процес за възстановяване от бедствието, да управляваме и квалифицираме информацията, да имаме ефективен процес на архивиране, да имаме информационни хранилища. Много компании не са подготвени и първите часове са пълен хаос, защото не са били внимателни, за да подготвим процеса за възстановяване“, разкрива той.

в) Технология

„Използване на технология, подходяща за реалността, която имаме днес. Много компании купуват технология и това е, което аз наричам купуване на „фалшиво чувство за сигурност“ – те купуват технология, но тя вече не е адекватна за реалността, която имаме днес. Традиционната защитна стена, вместо да се купува усъвършенствана крайна точка, която избягва системно криптиране, се използва проста крайна точка, която открива някакъв зловреден софтуер, но не предотвратява тези криптирания“.

Специалистите припомнят, че в тези случаи „паниката изобщо не помага“. В тези ситуации е необходимо да информирате властите и никога да не плащате откупа, тъй като това е същото като увековечаване на престъплението, казвайки на престъпниците, че си струва. Специалистите считат, че един от процесите, които компаниите трябва да имат предварително, е как компанията да бъде възстановена от такава атака, за да бъде спокойна и всеки да знае своята роля в този процес

КАЗУС 16: ЗЛОВРЕДЕН СОФТУЕР/KEYLOGGER

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Малка семейна производствена компания използва широко онлайн банкирането. Служител от Счетоводния отдел влиза в системата за онлайн банкиране с фирма и потребителско име и парола. Трябва да отговори на два предизвикателни въпроса за транзакции над 1 000 евро.

Собственикът е уведомен, че е иницииран платежен превод от 5000 евро от неизвестен източник. След свързване с банката се установява, че само за една седмица киберпрестъпниците са направили десет превода от банковите сметки на компанията на обща стойност 10 000 евро. Как? Един от техните служители е отворил имейл от някой, който смятаха за

доставчик на материали, но вместо това, се оказва че това е злонамерен имейл, примесен със зловреден софтуер от акаунт на измамник.

Нападателите са успели да инсталират злонамерен софтуер в компютрите на компанията, използвайки кийлогър за прихващане на банковите идентификационни данни. Кийлогърът е софтуер, който безшумно следи натисканията на клавишите на клавиатурата и изпраща информацията на киберпрестъпниците. След това те могат да имат достъп до банкови и други финансови услуги онлайн, като използват валидни номера на сметки и пароли.

Кийлогърът е софтуер, който безшумно следи натисканията на клавишите на кавиатурата и изпраща информацията на киберпрестъпник.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Информацията за тази кибератака е събрана чрез две интервюта, едно със собственика на компанията и едно с техник от поддържащата ИТ компания. И двамата бяха готови да опишат и дадат подробности за инцидента, но поискаха и двете компании да запазят анонимност, тъй като информацията е твърде чувствителна за тях.

ПРЕВЕНЦИЯ

В анализираната компания процедурите и механизмите за киберсигурност бяха определени като незадоволителни. Въпреки че компютрите на компанията имат инсталиран антивирусен софтуер, той не беше актуализиран. Освен това не са провеждани кампании за повишаване на осведомеността и някои служители изглежда имат ограничено разбиране относно киберрисковете.

ИДЕНТИФИКАЦИЯ

Въз основа на предоставената информация, за инцидента са събрани следните данни:

☑ Получен е социално проектиран фишинг имейл с архивиран компресиран файл, прикачен като потвърждение към поръчка на доставчик.

☑ Отваряйки файла, зловреден софтуер е инсталиран на компютъра

☑ Инсталиран е софтуер за кийлогър, който безшумно следи натисканията на клавишите на компютъра и изпраща информацията на киберпрестъпника.

☑ След това киберпрестъпникът използва уловените идентификационни данни за достъп до банковата сметка и извършва превода, използвайки валидни номера на сметки и пароли.

☑ Инцидентът е идентифициран едва когато киберпрестъпникът се направил опит да направи превод над 1 000 евро.

РЕАКЦИЯ

Тъй като компанията е нямала въведен план за киберсигурност, отговорът на компанията на атаката се е забави.

КОЙ: Нападателят не може да бъде идентифициран точно. Беше известен само имейл адрес и възможният произход.

КОГО: не конкретно насочена атака

ЗАЩО: Събиране на чувствителни данни и използване на такива за кражба на пари

КАКВО: Идентификационни данни за банкова сметка на фирмата

КАК: Кийлогър, който следи безшумно натисканията на клавишите на клавиатурата на компютъра

СТРАТЕГИЯ: Заплахата стартира от компютър без антивирусна програма. Процесът на почистване беше извършен от ИКТ експерт на компанията. Банковата сметка е затворена и идентификационните данни са променени. ИКТ компанията спомогна да извършат пълен преглед на киберсигурността на своите системи и да идентифицират източника на инцидента. Те също така препоръчват надстройки на софтуера за сигурност на компанията.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Компанията закрива банковата си сметка и предприема съдебни действия за възстановяване на загубите си. Фирмата успява да възстанови малка част от загубите. Не са възстановени загубите за време и разходите за адвокатски такси.

ВЪЗСТАНОВЯВАНЕ: Стратегията за възстановяване е фокусирана върху затварянето на банковата сметка, за да се избегнат повече загуби. Други предприети действия са почистване на компрометирания компютър и компрометираната електронна пощенска кутия. Извършена бе проверка на всички компютри на компанията за други атаки.

СТРАТЕГИЯ: Компанията трябва да предприеме различни действия за предотвратяване на подобни инциденти. Стратегията ѝ трябва да бъде съсредоточена върху следните действия/стъпки:

- ☑ Прилагане на политики за сигурност, като например политика за промяна на паролата и политика за управление на потребители на акаунти.
- ☑ Инсталиране и поддържане на актуализиран антивирусен/антизлонамерен софтуер.
- ☑ Изпълнение на програми за обучение за осигуряване информираността на служителите.
- ☑ Ограничаване на уеб базираното съдържание.
- ☑ Извършване на редовни проверки и одити.
- ☑ Изпълнение на превенция и прилагане на система за управление на риска.

ИЗВЛЕЧЕНИ ПОУКИ

- ☑ Известия – настройване на сигнали за транзакции за всички кредитни, дебитни карти и банкови сметки.
- ☑ Контрол на достъпа. Ограничаване на достъпа до чувствителни акаунти само до тези служители, които имат нужда от достъп; честа промяна на паролите.
- ☑ Компанията трябва да оцени своя риск и да оцени възможностите за застраховане на кибер отговорност.

- ☑ Избиране на банки, които предлагат множество нива на удостоверяване за достъп до сметки и транзакции.
- ☑ Създаване, поддържане и изпълнение на план за реагиране при кибер инциденти, който е бързо приложим.
- ☑ Киберпрестъпниците доставят и инсталират зловреден софтуер по имейл. Обучение на служителите относно сигурността на електронната поща.

КАЗУС 17: ОТКРАДНАТ КОМПЮТЪР ПРИЧИНЯВА СЕРИОЗНО НАРУШЕНИЕ НА СИГУРНОСТТА НА ДАННИТЕ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Консултантска компания от 10 души изпраща малък екип в Унгария, за да завърши клиентски проект. По време на техния престой старши консултантът оставя своя служебен лаптоп, който има достъп до чувствителна клиентска информация и банкови данни на компанията, в заключена кола, докато изпълнява работата. Колата е разбита, а лаптопът е откраднат. За съжаление, данните на компютъра не са били криптирани, тъй като служителят не е приложил политиката на компанията за криптиране на всички чувствителни данни на своя компютър. Сега компанията се страхува от кибератака срещу нейните системи, банкови сметки и изтичане на клиентски данни.

Тип на атаката: Физическа кражба на некриптиран компютър. Шифроването е процес на кодиране на четим текст, така че да може да бъде прочетен само от лицето, което има ключа за декриптиране. Това създава допълнителен слой на сигурност за чувствителната информация.

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Необходимата за описание на инцидента информация е събрана чрез интервю със старши консултант на компанията и ИТ техник на ИКТ компания, която поддържа консултантската фирма. Взаимодействието беше извършено с условието за запазване на чувствителната информация анонимно. Дори и интервюираният да желаеше да опише инцидента, част от информацията за криптиране не можеше да бъде получена и това е причината, която поради която поддържащата ИКТ компания беше помолена да разясни случая.

ПРЕВЕНЦИЯ

Въпреки че инцидентът не е ясна кибератака, това е един сериозен и много често срещан инцидент, който причинява поредица от значителни кибератаки.

В случая на анализираната компания, от гледна точка на киберсигурността, имаше въведени специфични политики и механизми, но те не бяха приложени от някои служители поради слабият им опит в областта на информацията и рисковете за киберсигурността.

ИДЕНТИФИЦИРАНЕ

Служителят веднага е подал сигнал в полицията и фирмата си за кражбата. Банката също е била информирана да следи транзакциите по сметката. Компанията съответно информира фирмата за поддръжка на ИКТ да деактивира отдалечения достъп на лаптопа и да започне да наблюдава дейността. Лаптопът е бил оборудван с инструменти за сигурност и защита с парола. Данните, съхранявани на твърдия диск, не са били криптирани – това включва чувствителни данни на клиенти и банкови данни на компанията.

За идентифициране на тази атака въз основа на поведението могат да бъдат използвани следните техники на MITRE ATT&CK:

- ☑ T1027 - Скрити файлове или информация
- ☑ T1036 – Маскиране
- ☑ T1586.002 – Компрометирани акаунти: Имейл акаунти

РЕАКЦИЯ

Реакция: Компанията трябва да спазва държавните закони, тъй като те се отнасят до нарушение на сигурността на данните. Държавните закони и разпоредбите на ЕС относно GPDR са много строги и с високи глоби.

- ☑ **КОЙ:** Нападателят не може да бъде идентифициран. Известно е само мястото на инцидента
- ☑ **КОГО:** не конкретно насочена атака
- ☑ **ЗАЩО:** Събиране на чувствителни данни и печалба на пари от продажбата на откраднато оборудване
- ☑ **КАКВО:** Чувствителни данни на клиенти и фирмени банкови данни
- ☑ **КАК:** загуба на оборудване, изтичане на чувствителни данни и атака на банкова сметка
- ☑ **СТРАТЕГИЯ:** Заплахата стартира на компютър без антивирусна програма и се разпространява странично. Извършено е почистване от специализирана IT&C фирма.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: The consulting company spent more than €20,000 on implementation, monitoring, and operational improvements. A data breach does impact a brand negatively and trust has to be rebuilt.

The main consequences of the attack were as follows:

- ☑ Загуба на данни
- ☑ Загуба на компютър
- ☑ Компрометиране на системата
- ☑ Финансови разходи

ВЪЗСТАНОВЯВАНЕ: Стратегията за възстановяване е фокусирана върху понижение на репутацията на марката и мониторинг и контрол на вътрешните системи и банкови сметки на компанията. Превантивно всички идентификационни данни за банкови сметки бяха променени и системните привилегии на служителите бяха спрени и променени.

СТРАТЕГИЯ: Компанията трябва да предприеме различни действия за предотвратяване на подобни инциденти. Стратегията му трябва да се концентрира върху:

- ☑ Изпълнение на програми за обучение, за осигуряване информираността на служителите
- ☑ Извършване на редовни проверки и одити
- ☑ Изпълнение на система за превенция и внедряване на система за управление на риска

ИЗВЛЕЧЕНИ ПОУКИ

- ☑ Компаниите трябва да създадат и обучат служители за сигурно боравене с устройства, издадени от работата.
- ☑ Устройствата трябва да се съхраняват безопасно, когато не са в непосредствено присъствие на служителя.
- ☑ Компаниите трябва да предприемат стъпки за криптиране на данни, където и да се съхраняват или предават.
- ☑ Служителите трябва да имат ясно разбиране за значението на криптирането и как да го използват.
- ☑ Компаниите трябва да разбират и знаят своите отговорности съгласно законите за уведомяване при нарушаване на данните на държавата, в която работят.
- ☑ Редовният преглед на практиките за сигурност на компанията е наложителен в съвременните организации за предотвратяване на инциденти, откриване на уязвимости и намаляване на въздействието на инциденти.

КАЗУС 18: АТАКА ЗА ОТКАЗ НА УСЛУГА (DDOS) СПИРА ВАЖНИ УСЛУГИ

ЦЕЛЕВА ОРГАНИЗАЦИЯ

Целевата организация е била компания за предоставяне на хостинг услуги. Нападателите изравниха масивна дистрибутирана атака за отказ на услуга срещу конкретен уебсайт в средата на декември 2021 г., достигайки честотна лента от 1,5 гигабита в секунда и почти 100 милиона пакета в секунда, най-голямата атака, пред която е изправена хостинг компания.

Компанията смята, че нападателят се е съсредоточил върху уебсайтовете с онлайн казино игри, а хостинг доставчикът не е бил действителната цел. Дистрибутираната атака за отказ на услуга (DDOS) води до прекъсване на достъпността на услугите на клиента за повече от 12 часа.
Дистрибутираната атака за отказ на услуга е злонамерен опит за прекъсване на нормалния трафик на целевия сървър, услуга или мрежа чрез претоварване на целта или заобикалящата я инфраструктура с поток от интернет трафик. DDoS атаките постигат ефективност чрез използване на множество компрометирани компютърни системи като източници на трафик на атака. Експлоатираните машини могат да включват компютри и други мрежови ресурси, като интелигентни устройства.

„През 2019 г. е установено увеличение с 57% на вариантите на ботнет мрежата Mirai. Вариантите на Mirai обикновено се използват за атаки с груба сила на IoT устройства. През 2019 г., тези атаки са се увеличили с 51%, докато увеличението на уеб експлойтите е 87%“. (MCCART, 2022 г.).

КАК Е ПРИДОБИТА ИНФОРМАЦИЯТА?

Необходимата информация за описание на тази кибератака е събрана чрез две интервюта (срещи лице в лице), едно с главния изпълнителен директор на компанията и едно с ИТ инженер на компанията. И двамата бяха готови да опишат и дадат подробности за инцидента, но поискаха да запазят анонимността на двете компании и имената им, тъй като информацията е твърде чувствителна за тях

ПРЕВЕНЦИЯ

Въпреки че хостинг доставчикът има няколко процедури и механизми за киберсигурност, изглежда, че нападателите са намерили уязвима точка, която да изследват.

Техникът на компанията е забелязал, че уебсайтът изведнъж стана бавен, но е предположил, че това е законен скок в трафика поради празничния сезон. Атаката е идентифицирана веднага след като уебсайтът е станал недостъпен и клиентът се е оплакал.

ИДЕНТИФИЦИРАНЕ

Нападателите са използвали трафик от източници по целия свят. Изглежда, че атаката за отказ на услуга е създадена от ботнет на Mirai. И тъй като ботнетът Mirai има способността да изпраща около 600 мегабита в секунда, нападателите използват атака от второ ниво с различен ботнет Mirai.

Mirai е злонамерен софтуер, който заразява интелигентни устройства, работещи с ARC процесори, превръщайки ги в мрежа от дистанционно управлявани ботове или „зомбита“. Тази мрежа от ботове, наречена ботнет, често се използва за стартиране на DDoS атаки.

Хостинг доставчикът използва инструменти за анализ на трафика, за да идентифицира атаката. Основната характеристика на атаката е големият обем, идващ от същата поредица от IP адреси. Инженерите успяха да изолират тези IP адреси и уебсайтът се върна.
След това те се опитват да идентифицират защо инструментът за анализ на трафика не е открил атаката от първите етапи.
Съгласно рамката на MITER ATT&CK този инцидент може да бъде описан по следния начин:

- ☑ T1499 – Отказ на обслужване на крайна точка
- ☑ T1498 - Мрежов отказ на услуга

РЕАКЦИЯ

- ☑ **КОЙ:** Нападателят не може да бъде идентифициран. Атаката идва от цял свят
- ☑ **КОГО:** Целта е конкретен уебсайт, хостващ онлайн казино игри
- ☑ **ЗАЩО:** За да бъде прекъсната работата.
- ☑ **КАКВО:** Уеб сайтът на компанията.
- ☑ **КАК:** DDOS атака използваща ботнет Mirai.
- ☑ **СТРАТЕГИЯ:** Атаката е започнала на сървър на хостинг доставчик, за да прекъсне работата на определен уебсайт. Инструментът за анализ на трафика не е успял да предупреди за възможността от кибератака. Компанията е увеличила чувствителността на алармите в инструмента за анализ на трафика, така че в бъдеще да бъдат избегнати подобни инциденти.

ВЪЗСТАНОВЯВАНЕ

ВЪЗДЕЙСТВИЕ: Хостинг доставчикът претърпява някои допълнителни значителни разходи, за да покрие атаката, а също така има сериозни щети по репутацията. За да възстанови уебсайта и неустойките по SLA споразумението с клиента, доставчикът е понесъл допълнителни разходи за труд,. Общите разходи са оценени на приблизително 40 000 евро.

ВЪЗСТАНОВЯВАНЕ: Стратегията за възстановяване е фокусирана върху изолирането на атакуващите IP адреси, за да бъде спряна атаката и да се възстанови работата на уебсайта. Други действия, които бяха предприети са увеличаване на чувствителността на алармите на

инструмента за анализ на трафика. Проверка на всички хостинг сървъри и услуги за всякакви други атаки или подозрителни дейности.

СТРАТЕГИЯ: Компанията трябва да предприеме различни действия за предотвратяване на подобни инциденти. Стратегията на фирмата трябва да се концентрира върху:

- ☑ Увеличаване на чувствителността на инструмента за анализ на трафика
- ☑ Инсталиране на втори инструмент за допълнителна сигурност
- ☑ Изпълняване на програми за обучение, за да осигурите информираността на служителите
- ☑ Ограничаване на някои IP диапазони
- ☑ Извършване на редовни проверки и одити
- ☑ Изпълнение на система за превенция и внедряване на система за управление на риска
- ☑ Сертифициране на инфраструктурата и услугите на компанията по ISO27001 и ISO22301

ИЗВЛЕЧЕНИ ПОУКИ

- ☑ Прекъсването идва в много форми. Прекъсванията или забавянията могат да се появят под много форми, особено за доставчиците на хостинг услуги. Когато бъде идентифицирана атака, подходящите екипи за реагиране трябва да отделят ресурси за справяне с нея.
- ☑ Много кибератаки са лесно предотвратими. Сложните кибератаки могат да причинят много щети, но много от тях могат лесно да бъдат предотвратени с правилната сигурност. Важно е да се изгради силна и проактивна система за управление на сигурността, за да се спрат атаките. Такава система за управление изисква непрекъсната поддръжка, наблюдение на всички системи и устройства в мрежата, включително актуализиране на технологиите и прилагане на корекции за сигурност за известни експлойти.
- ☑ Дистрибутираните атаки за отказ на услуга трябва да бъдат приемани сериозно. Понастоящем DoS и DDoS атаки са различни, тъй като са по-злонамерени, целенасочени и способни.
- ☑ Няма ограничение във времето. Атаките на мрежовия слой могат да продължат повече от 48 часа, докато атаките на приложния слой могат да продължат с дни. Проникване в системи и мрежи за шпиониране - седмици и месеци.
- ☑ Киберсигурността трябва да бъде приоритет. Киберсигурността трябва да бъде един от най-високите приоритети за всички субекти, работещи в днешния пейзаж. Тези атаки се превърнаха в сложни, целенасочени, способни и нерегулирани. Всички заплахи трябва да се приемат сериозно, включително DDoS атаките, които стават все по-чести.

ЗАКЛЮЧЕНИЕ

Въз основа на диверсифицираното портфолио, което е представено в документалния архив на ENCRYPT 4.0 за кибератаки, могат да бъдат направени следните заключения:

- ☑ С развитието на ИКТ и в контекста на Индустрия 4.0, киберсигурността придобива нарастващо значение и **компаниите без адекватна киберзащита излагат дейността си на сериозен риск.**
- ☑ **Служителите играят ключова роля в киберзащитата**, следователно служителите както в МСП, така и в големите предприятия трябва да получат поне основно обучение за това как да защитават фирмените данни и да работят с чувствителна информация, тъй като по-голямата част от кибератаките се случват поради липса на знания по отношение на тези аспекти, особено в контекста на дистанционната работа по време на пандемията от COVID-19.
- ☑ **МСП, независимо от сектора, в който оперират, се превръщат в основна цел за хакери и организирани киберпрестъпници**, но в същото време само 1/3 от МСП имат план как да овладеят потенциална кибератака, следователно МСП трябва да предвидят киберсигурността като основен приоритет, за да се гарантира тяхната конкурентоспособност в дългосрочен план.

РЕФЕРЕНЦИИ

1. Acronis, 2020 г. Кибер атаката срещу Националното управление по здравеопазване на Великобритания (NHS). [Онлайн] Acronis. Наличен на: https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/

2. Barber, B., 2016 г. William Hill се извинява след атаката на уебсайта. [Онлайн] Racing Post. Налично на: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (Казус 6)

3. Blue goose, n.d. Информационна сигурност в William Hill. [Онлайн] blue goose. Налично на: https://bluegooseis.co.uk/work/william-hill (Казус 6)

4. Braue, D., 2022 г. Предвижда се, че глобалните разходи за щети от рансъмуер ще надхвърлят 265 милиарда долара до 2031 г. [онлайн] 2022 г. списание „Cybersecurity Ventures“. Налично на: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

5. Cook, S., 2022 г. Статистика и факти за 20+ Дистрибутирани атаки за отказа на услуга (DDoS) за 2018-2022 г. [Онлайн]. Comparitech. Наличен на: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

6. Craver, R., 2015 г. Базата данни на Hanesbrands хакна 900K телефона, засегнати онлайн клиенти. [електронен журнал] *Winston-Salem Journal.* Наличен на: https://journalnow.com/business/hanesbrands-database-hacked/article_543b338e-3664-11e5-b77e-c77df1e08b5c.html (Казус 4)

7. Обсерватория за кибер стратъп. Наличен на: https://cyberstartupobservatory.com/ (Казус 4)

8. CyberNews, 2021 г. Медицинските данни на хиляди клиенти на Humana са изтекли онлайн след атака. [Онлайн] 2022 г. Cybernews. Наличен на: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/ (Казус 5)

9. CyberTalks, 2022 г. Топ 15 статистики за фишинг атаки (и те биха могли да ви изплашат) [Онлайн]. CyberTalks. Наличен на: https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

10. Cyware, 2018. Уебсайтове на Humana, засегнати от сложни измамни атаки от „чужди държави“. [Онлайн] Cyware. Наличен на: https://cyware.com/news/humana-websites-hit-by-sophisticated-spoofing-attack-from-foreign-countries-5ac77624 (Казус 5)

11. Dissent, 2018 г. Humana уведомява членовете след атака с кражба на идентификационни данни от Humana.com и Go365.com. [онлайн] 2009 – 2022 г., DataBreaches.net и DataBreaches LLC. Наличен на: https://www.databreaches.net/humana-notifies-members-after-credential-stuffing-attack-on-humana-com-and-go365-com/ (Казус 5)

12. ЕВРОПОЛ, n.d. Най-опасният зловреден софтуер в света EMOTET спрян чрез глобални действия. [Онлайн] EUROPOL 2022 г. Наличен на: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

13. Kolbasuk McGee, M., 2018 г. Humana уведомява жертвите за атака с „фалшифициране на самоличността“. [онлайн] *Data Breach Today*. Наличен на: https://www.databreachtoday.asia/humana-notifying-victims-identity-spoofing-attack-a-11153 (Казус 5)

14. McCart, C., 2022 г. 15+ Шокиращи ботнет статистики. [Онлайн] Comparitech. Наличен на :https://www.comparitech.com/blog/information-security/botnet-statistics/

15. Mimecast, 2022 г. Изправяне срещу НОВАТА ВЪЛНА ОТ КИБЕР АТАКИ: Състоянието на сигурността на електронната поща, Доклад 2022 г. Mimecast. Наличен на: https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-2022.pdf

16. Moore, J., 2022 г. Списък с Топ 10 факти относно киберсигурността за 2022 г. [Онлайн] Elevity. Наличен на: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

17. Morran, Ch., 2015 г. Уебсайтът на Hanes е най-новата, най-странна жертва на нарушаване на данните. Consumerist. Наличен на: https://consumerist.com/2015/07/30/hanes-website-is-the-latest-oddest-victim-of-data-breach/ (Казус 4)

18. StackHawk, 2022 г. Какво е инжектиране на команди? [Онлайн]. StackHawk, наличен на: https://www.stackhawk.com/blog/what-is-command-injection/

19. The Cyber Wire, n.d. Определение за спуфинг. [Онлайн]. The Cyber Wire. Наличен на: https://thecyberwire.com/glossary/spoofing

20. VentureBeat, 2022 г. Доклад: Средното време за откриване и ограничаване на пробив е 287 дни. [Онлайн] VentureBeat. Наличен на: https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/

21. Verizon, 2021 г. DBIR: Доклад за разследване на изтичане на данни за 2021 г. Verizon, 2021. Наличен на: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

22. Wallarm, 2021 г. Най-големите хакерски атаки срещу хазарта. 10. [Онлайн] Wallarm. Наличен на: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (Казус 6)

Съфинансиран от програма
„Еразъм+“
на Европейския съюз

ПАРТНЬОРИ ПО ПРОЕКТА

ENCRYPT 4.0

Съвместна инициатива за развитие на работна сила за подпомагане на европейската индустрия в преодоляването на недостига на професионалисти по киберсигурност

Проектът ENCRYPT4.0 (2020-1-RO01-KA202-079983) има за цел да даде възможност на ръководството на производствените МСП да приеме проактивен подход към киберсигурността, като ги подкрепи в процеса на анализиране, идентифициране и справяне с кибер рисковете и заплахите, приложими за тяхната организация. Насърчаване на интерактивно обучение, базирано на проекти с цел повишаване на уменията и компетенциите за киберсигурност на служителите на МСП и/или специалистите по киберсигурност.

„Джордж Емил Паладе” - Университет по Медицина, Фармация, Наука и Технологии, Търгу Муреш, Румъния

Координатор по проекта

Европейски център за качество ООД , Консултантска фирма - България

Avantalia, МСП, базирано на технологии - Испания

Instituto de Soldadura e Qualidade, Технологична Институция - Португалия

FH Joanneum, Университет по приложни науки- Австрия

PCX Management, Computers & Information Systems Ltd. - Кипър