CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 21.05.2020 г.

Съдържание

Нова DNS уязвимост позволява на атакуващи да стартират мащабни DDoS атаки 2

Най-добрите начини за откриване и справяне със съмнителни прикачени файлове 4

[Ръководство] Намиране на най-добрата алтернатива за аутсорсинг на сигурност за вашата организация 8

Нова DNS уязвимост позволява на атакуващи да стартират мащабни DDoS атаки

20 май 2020 г.

Израелските изследователи по киберсигурност разкриха подробности за нов недостатък, влияещ на DNS протокол, който може да се използва за стартиране на широкомащабни разпределени атаки за отказ от услуги (DDoS), насочени към сваляне на уебсайтове.

Недостатъкът, наречен NXNSAttack, зависи от механизма на делегиране на DNS, принуждавайки DNS-разрешителите да генерират повече DNS заявки към сървъри по избор на нападателя, което потенциално причинява мащабно ботнет прекъсване на онлайн услугите.

След отговорно разкриване на NXNSAttack, няколко от компаниите, отговарящи за интернет инфраструктурата, включително PowerDNS (CVE-2020-10995), CZ.NIC (CVE-2020-12667), Cloudflare, Google, Amazon, Microsoft, притежаваният от Oracle Dyn, Verisign и IBM Quad9, пачнаха софтуера си с цел справяне с проблема.

Инфраструктурата на DNS преди това беше атакувана от DDoS атаки чрез скандалния ботнет Mirai, включително тези срещу Dyn DNS услугата през 2016 г., засягайки някои от най-големите сайтове в света, включително Twitter, Netflix, Amazon и Spotify.

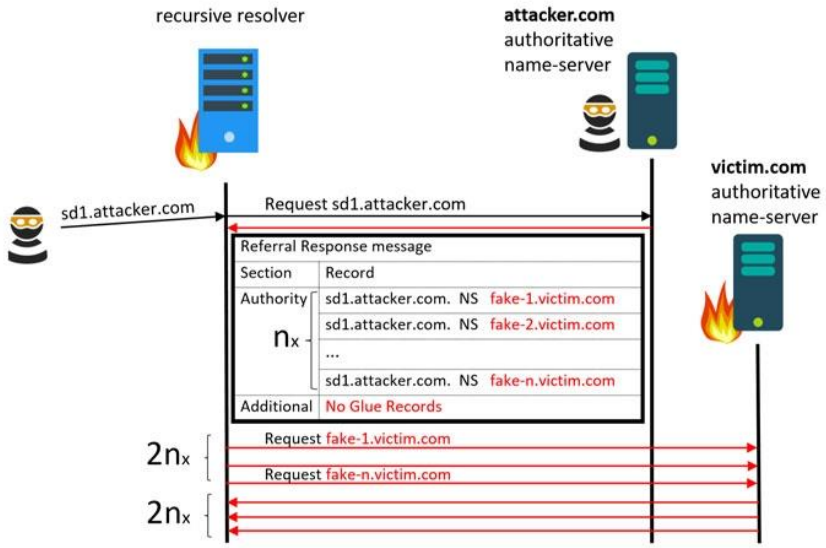
Методът на NXNSAttack

Рекурсивно търсене на DNS се случва, когато DNS сървър комуникира с множество авторитетни DNS сървъри в йерархична последователност, за да намери IP адрес, свързан с домейн (например www.google.com) и да го върне на клиента.

Разрешаването обикновено започва с DNS резолютор, контролиран от вашите интернет доставчици или обществени DNS сървъри като Cloudflare (1.1.1.1) или Google (8.8.8.8), и е конфигурирано според вашата система.

Разрешителят предава заявката на авторитетен сървър за DNS имена, ако не е в състояние да намери IP адреса за дадено име на домейн.

Но ако първият авторитетен сървър за DNS имена не съдържа желаните записи, той връща съобщението за търсене на адреси на следващите авторитетни сървъри, към които DNS резолюторът отправя запитване.



Този йерархичен процес продължава, докато DNS исканото разрешение не достигне правилния авторитетен сървър, който предоставя IP адреса на домейна, позволяващ на потребителя достъп до желания уебсайт.

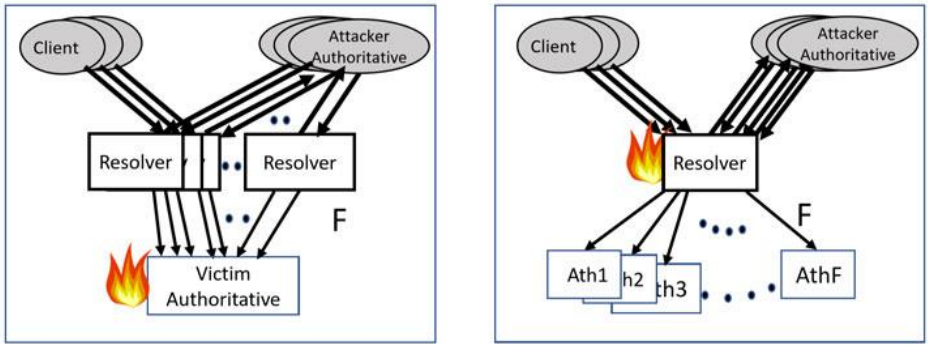
По този начин непрекъснато могат да бъдат изпращани голям брой пакети към целевия домейн, вместо към законни авторитетни сървъри.

За да стартира атаката, нападателят трябва да притежава авторитетен сървър. Това може да бъде лесно постигнато чрез закупуване на име на домейн.

NXNSAttack работи, като изпраща заявка от атакуващ домейн (напр. "Attacker.com") към уязвим сървър за разрешаване на DNS, който ще препрати DNS заявката на контролиран от атакуващия авторитетен сървър.

Вместо да връща адреси към реалните авторитетни сървъри, контролираният от атакуващия авторитетен сървър отговаря на DNS заявката със списък фалшиви имена на сървъри или поддомейни, контролирани от участника на заплахата. DNS сървърът след това препраща заявката към всички несъществуващи поддомейни, създавайки масивен трафик към сайта на жертвата.

Според изследователите атаката може да увеличи броя на разменяните пакети с коефициент над 1620, като по този начин затрупа не само DNS-разрешителите с повече заявки, с колкото те могат да се справят, а и да „наводни“ целевия домейн с излишни заявки и да го свали.



(a) (b)

NXNSAttack targeting the authoritative server (a) and the recursive resolver (b)

Нещо повече, използването на ботнет като Mirai може допълнително да увеличи мащаба на атаката. А контролът и придобиването на огромен брой клиенти и голям брой авторитетни сървъри от нападател е лесно и евтино.

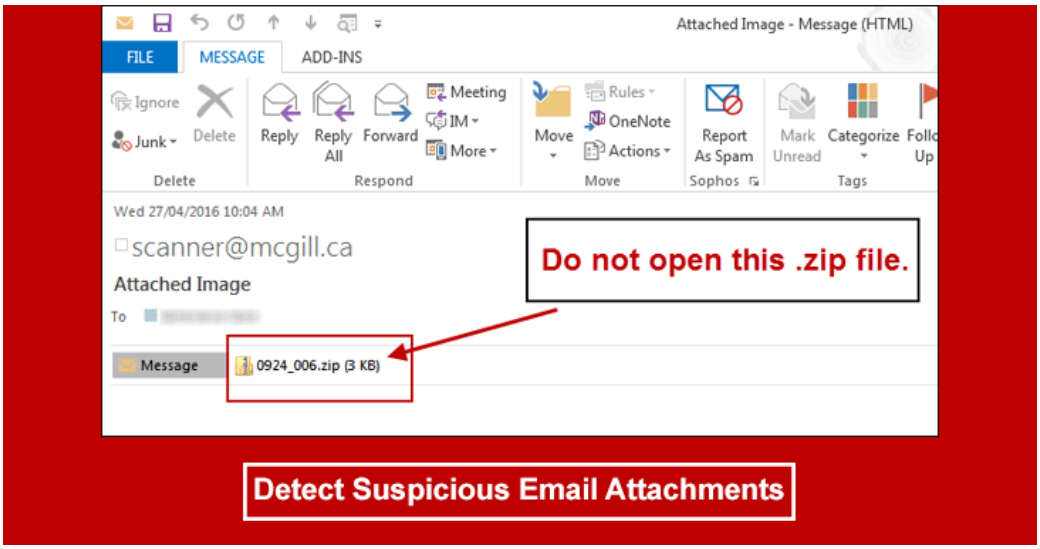
Силно препоръчително е мрежовите администратори, които управляват свои собствени DNS сървъри, да актуализират своя DNS resolution софтуер до най-новата версия.

За повече информация:

https://thehackernews.com/2020/05/dns-server-ddos-attack.html

Най-добрите начини за откриване и справяне със съмнителни прикачени файлове

20 май 2020



Хакерите използват прикачените файлове за електронна поща, за да се насочат към нищо неподозиращия потребител. Прикачените файлове могат да съдържат троянци и вируси, могат да се използват и за хакване на мобилния ви телефон. Те непрекъснато намират начини да подмамят автоматичната електронна защита и филтри, за да влязат във входящите пощенски кутии. Ако го направят в пощенската кутия, отварянето на опасен прикачен файл може да доведе до огромни проблеми.

Ако получите имейл от неизвестен източник, никога не отваряйте прикачения файл. Въпреки че можете да четете имейла без притеснение, при условие че вашият компютър е актуализиран, трябва да избягвате да отваряте прикачени файлове. Доставчиците на имейл услуги обикновено сканират и премахват опасните прикачени файлове, но някои от тях успяват да се промъкнат.

Дори имейли от предполагаеми надеждни източници могат да бъдат фишинг имейли, прикрити с цел да компрометират мобилния ви телефон или компютър с помощта на прикачени файлове.

Когато разглеждате прикачен файл в имейл, първо трябва да обърнете внимание на неговото разширение. Разширението може да ви помогне да се ориентирате за типа на прикачения файл. Например, ако файлът ви завършва с .jpg, това е изображение. Ако е .avi, това е видео.

Едно разширение, което обикновено трябва да избягвате, е .exe, което ще изпълни инсталация и изпълняваната програма може да бъде злонамерена. Докато

повечето доставчици на имейл услуги блокират тези файлове, те понякога могат да се промъкнат. Няколко други разширения, които трябва да избягвате, включват .jar, .cpl, .com, .bat, .msi, .js, .wsf и много други. Ако разширението изглежда странно, трябва да сте подозрителни.

Тези прикачени файлови формати може да са злонамерени

Ами ако това е просто Office файл? Трябва да е наред, но трябва да вземете някои предпазни мерки. Може да съдържа макроси, които са поредица от инструкции, които ще изпълнят задача. Ако вашият Office файл завършва с m, той съдържа макроси. Те включват .docm. pptm и .xlsm. Някои безопасни файлове също използват макроси, но трябва да ги избягвате, освен ако не можете да проверите, че са от надежден източник.

Правилото е да отваряте само разширения, на които можете да се доверите. Файловете с изображения, Office файловете и PDF файловете обикновено са безопасни, при условие че сте извършили всички актуализации.

Това криптиран архив ли е?

Архивните файлове са полезни по много причини. Те позволяват на хората да компресират няколко файла в един пакет, което улеснява изпращането. Те обаче могат да се използват и от хакери. Ако получите имейл и той има разширение за архив, като .7z, .rar или .zip, и изисква да въведете парола, файлът може да е съмнителен.

Защо хакерите защитават файла с парола? Те криптират архива, така че вирусен скенер да не може да го забележи. Могат да направят това, за да скрият злонамерен софтуер. Разбира се, може да има парола, защото съдържа чувствителна информация. Още веднъж се уверете, че архивът идва от надежден източник, преди да го отворите.

Кой е Подателят?

Както знаем, обикновено можете да се доверите на някой, който ви изпраща прикачен файл, ако го познавате. Ако не познавате човека, той може да ви изпраща зловреден софтуер. Въпреки това, някой, когото познавате, може сам да се зарази и злонамереният софтуер ще ви изпрати файл от името на човека, за да изгради доверие, така че внимавайте. Ако някой, когото познавате, ви изпраща макро файл в Office, без да ви е съобщил за това, проявете повишено внимание. Трябва да се свържете с човека, за да проверите дали той е изпратил подозрителния прикачен файл. Ако го е направил, можете да го отворите, но ако не е така, изтрийте имейла си и сигнализирайте на подателя, че е бил хакнат.

Какво е съдържанието на имейла?

Преди да отворите прикачен файл, прочетете имейла. Ако изглежда, че е от надежден източник, но съдържанието изглежда съмнително, това може да е знак, че е зловреден софтуер. Обикновено хакерите извършват фишинг измами, като се маскират като банка или сайт, който съдържа ваша платежна информация, като ви приканват да въведете информацията си поради компрометиране на акаунта.

Тези имейли може да съдържат правописни грешки. Ако получите имейл от Amazon, приканващ ви да изтеглите нещо и след това да го стартирате, това може да е знак за измама. Повечето фирми не биха ви накарали да правите това.

Предупреждения за вируси

Ако вашият имейл е от основен доставчик на услуги, като Yahoo !, Gmail или Hotmail, той ще сканира прикачения файл и ще ви предупреди, ако е потенциално опасен. Разбира се, в имейла може да се твърди, че предупреждението за антивирус се дължи на грешка или нещо подобно, но това очевидно е лъжа.

Ако все пак изтеглите прикачения файл и вашата собствена антивирусна програма ви казва да не го правите, послушайте я. Тя очевидно открива нещо нередно. Въпреки това, понякога вашият антивирусен софтуер може да не засече нищо. Това не означава, че файлът е безопасен, тъй като антивирусните програми понякога грешат.

Бъдете предпазливи и бъдете в безопасност!

Когато видите прикачен файл, трябва да сте скептично настроени към съдържанието му и да приемете, че може да е опасен. Никога не отваряйте прикачен файл, освен ако не знаете със сигурност, че е от надежден източник и сте го очаквали.

Обикновено електронната ви услуга ви позволява да преглеждате прикачени файлове без изтегляне, така че използвайте това в своя полза. Вижте съдържанието му и ако всичко изглежда наред, изтеглете. Въпреки че не трябва да се плашите от всичко, което получавате, трябва да сте нащрек.

За повече информация:

https://gbhackers.com/how-to-detect-suspicious-email-attachments/

[Ръководство] Намиране на най-добрата алтернатива за аутсорсинг на сигурност за вашата организация

20 май 2020 г.

Тъй като кибератаките продължават да се разпространяват по обем и се увеличава усъвършенстването им, много организации признават, че част от ИТ защитата им трябва да бъде възложена на външни изпълнители.

Cynet пусна Ръководството за аутсорсинг на сигурността (изтеглете оттук), като предоставя на ръководителите в сферата на ИТ сигурността ясни и приложими насоки за плюсовете и минусите на всяка алтернатива на аутсорсинг.

Причината за аутсорсинг на сигурността с нарастваща скорост е, че за разлика от традиционните ИТ, кибер заплахите се развиват с много по-бързи темпове.

Докато сравнително не много отдавна антивирусния софтуер и защитната стена покриваха повечето от нуждите на киберсигурността на стандартната организация, днес никоя позиция за сигурност не може да се счита за завършена без определено ниво на способности за реагиране на инциденти, приоритизиране, анализ на първопричините, разследване и специалист по сигурността, който е достатъчно квалифициран в тази област.

Разликата между сигнал, който показва потенциален системен риск, и сигнал, задействан от незначителна неправилна конфигурация, далеч не е тривиална и предизвикателството се засилва, когато припомним, че много малки и средни организации разчитат на своите ИТ служители да опазват тяхната киберсигурност на непълно работно време, без специален екип на място.

Ръководството за аутсорсинг на сигурност превежда своя читател чрез широкия набор от алтернативи за аутсорсинг, както и посочва уникалните характеристики, които биха помогнали на всяка организация по най-добър начин.

Аутсорсингът за сигурност бива разделен на три семейства:

- **IR ориентирано:** това семейство включва възлагане само на дейности, свързани с IR и разполага с широк диапазон - от просто наблюдение и уведомяване чрез отдалечена помощ и насоки до пълна криминалистична

проверка и възстановяване. От гледна точка на бизнес моделите, помощта може да бъде фиксирана или предоставяна при поискване. Типичните доставчици на услуги на тези семейства са MSSP и MDR.

- **Постоянно ориентирано управление:** това семейство се прилага за организации, които биха предпочели дори ежедневното функциониране на техните технологии да бъде наблюдавано с цел предотвратяване и откриване на заплахи. Компаниите, избрали такъв тип аутсорсинг, предпочитат наблюдението да се извършва от по-квалифициран екип и най-вече такива организации се намират сред организациите с малко опит в областта на сигурността и без специален екип за сигурност. Тук също има различни нюанси, които могат да варират от управление само на по-модерните инструменти за откриване и наблюдение до пълно управление на защитата. Типични доставчици на услуги от това семейство са MSSP, MDR и MSP.

- **Ориентиран към дизайна и настройката:** това е най-обширното семейство по отношение на функционалностите, които се възлагат на външен изпълнител и включва аутсорсинг на решението какви продукти да изберете и инсталирате, как да ги интегрирате заедно и кои заплахи трябва да бъдат приоритетни. Типични доставчици на услуги на тези семейства са MSSP, MSP и системните интегратори.

За повече информация:

https://thehackernews.com/2020/05/best-security-outsourcing.html