CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 07.04.2020 г.

Съдържание

Zoombombing: какво е това и как можете да го предотвратите при вашите конферентни разговори

05 април 2020 г.

На фона на блокадата покрай Covid-19, използването на софтуер за видеоконферентна връзка се наблюдава често, било то свързано с работа, с преподаване или просто за социализиране. Използването на видео чатове се увеличи и с него тревогите по отношение на сигурността нараснаха.

Един такъв софтуер - „Zoom“, който е доста популярен за видеоконференции, привлича вниманието на изследователите и журналистите по сигурността върху проблемите с поверителността и сигурността. Дори разследващата агенция на Съединените щати ФБР издаде предупреждение на гражданите да бъдат предпазливи, докато използват приложението, като цитират за увеличаване на случаите, когато обажданията са прекъснати от „порнографски и / или непристойни изображения и заплашителен език“, а агенцията също така поиска софтуерните компании да практикуват "надлежно старание и предпазливост" в мерките си за сигурност.

Zoombombing е инцидент, когато обажданията ви за видеоконферентна връзка се прекъсват от нежелан / неканен участник и нарушават срещата.

Мерки от Zoom за предотвратяване на Zoombombing

Изпълнителният директор на Zoom Ерик Юан публикува публикация в блога, насочена към тези проблеми. Той спомена, че Zoom ще замрази актуализациите на функциите на приложението и ще се съсредоточи върху разработването на решения за сигурност през следващите 90 дни. Той съобщава, че тези деветдесет дни ще бъдат посветени на „ресурсите, необходими за по-добра идентификация, адресиране и коригиране на проблемите“. Той написа, че тези инициативи ще се съсредоточат върху провеждане на цялостен преглед с експерти и представителни потребители, за да се разбере и гарантира сигурността на всички случаи на използване на приложението.

Стъпки, които можете да предприемете, за да предотвратите "Zoombombing"

Има няколко прости настройки, които можете да промените в приложението си Zoom, за да не се прекъсват обажданията ви от нежелани лица.

- Не използвайте личния си идентификационен номер за срещата, вместо това използвайте предишен идентификационен номер, включително за настояща среща. Има уроци на Zoom, които ще ви помогнат да разберете как да генерирате случаен идентификационен номер за среща.

- Активирайте функцията "чакалня" в управлението на акаунта. Това ще ви позволи да видите кой се опитва да се присъедини към срещата и да му предоставите достъп.
- След като срещата започне и всички са в нея, заключете срещата за външни лица.
- Уверете се, че не публикувате идентификационния номер на срещата в обществени платформи.
- Ако някой външен човек влезе, можете да го заключите, като отидете в списъка с участници в страничната лента за навигация, превъртите до „още“ и щракнете върху „заключване на срещата“. Можете също да ги премахнете, като щракнете върху „Mute all” в списъка с участници.

За повече информация:

https://www.ehackingnews.com/2020/04/zoombombing-what-is-it-and-how-you-can.html

TLS 1.3: Бавното възприемане на по-силно уеб криптиране дава възможности на лошите

06 април 2020

В продължение на дванадесет години стандартното криптиране в Интернет е Transport layer Security(TLS) 1.2.Първата версия на Secure Socket Layer (SSL), е разработена през 1995 г. от Netscape, но никога не е пусната, поради факта, че е пълна с уязвимости в сигурността. Следват SSL 2.0 и 3.0, но те също имат своите проблеми.

TLS 1.3

Първата итерация на TLS - 1.0 - се базира на SSL 3.0 и е публикувана през 1999 г. от Internet Engineering Task Force (IETF). Въпреки че има разлики, двата протокола споделят достатъчно сходства, така че SSL и TLS често се използват взаимозаменяемо.

От 25 години насам виждаме как протоколите се подобряват, но това върви невероятно бавно. Това е така, защото и TLS, и SSL преди него се формират чрез отворени стандарти и за да могат ефективно да се развиват, те трябва да бъдат приети масово. Производителите на устройства, доставчиците на уеб браузъри, приложенията (Facebook и неговите сървъри например), всички трябва да го приемат, за да се гарантира, че няма пропуски –но това включва милиони единици.

Ето защо, въпреки че TLS 1.3 съществува от 2018 г. и предлага по-голяма сигурност от TLS 1.2, последният фактически е стандартът. Има голям тласък от американските организации за широкото приемане на TLS 1.3, но то ще отнеме време.

Други стандартни протоколи, които продължават да се използват, са системата за имена на домейни (DNS) и протокола за прехвърляне на хипертекст (HTTP). Първият често е наричан „телефонен указател на интернет“ и представлява фактически огромна база данни, пълна с IP адреси. Последният се използва за изпращане на данни през връзката. И двата използват ясен текст, което означава, че всяка атака "man-in-the-middle" (MITM) може много лесно да идентифицира до кои сайтове се опитва да получи достъп потребителят.

Защо TLS 1.3?

TLS осигурява сигурна комуникация между уеб браузъри, приложения и сървъри, насочени към крайния потребител, чрез криптиране на предаваната информация, предотвратяване на подслушване или подправяне на атаки. Пълният процес разчита на два типа криптиране: асиметрично, което изисква публичен и частен ключ, и симетрично, което използва споделен ключ.

Асиметричното криптиране се използва по време на „ръкостискане“, което се извършва преди изпращането на всякакви данни. „Ръкостискането“ определя кой шифров пакет да се използва за сесията - с други думи, типа на симетричното криптиране - така че браузърът и сървърът да са съгласни. Протоколът TLS 1.2 отнема многобройни конекции между клиент и сървър, докато TLS 1.3 е много по-плавен процес, който изисква само една конекция. Това спестява милисекунди от всяка връзка.

Друга характеристика на TLS 1.3 е, че той може да работи заедно с DNS през HTTPS (DoH). Този протокол вижда заявката за URL / IP, изпратена през криптирана връзка с протокол за защита на хипертекстовия пренос (HTTPS) и я скрива в рамките на редовен трафик, което означава, че снупърите не могат да идентифицират заявките. Следователно те не знаят в кои сайтове се опитва да влезе човек и не могат да подправят връзката.

Когато бъде напълно приет, TLS 1.3 ще направи интернет по-безопасно място, но докато това не се случи, се дава възможност на лошите.

Една атака, която продължава, е „Bleichenbacher“. Кръстен на швейцарски криптограф, вариантът за атака има множество версии, насочени към алгоритъма за декриптиране на RSA. Докато авторите на TLS се опитват да затруднят разкриването на ключа за декриптиране на RSA, всеки нов вариант на Bleichenbacher успява да го направи. Като такова, всяко устройство, което използва функции, базирани на TLS, е уязвимо. TLS 1.3 се опитва да ограничи използването на RSA, но приемането ad-hoc

означава понижаване до TLS 1.2, което често се случва и атаките са широко разпространени.

Има и много хора, които твърдят, че DoH всъщност отслабва усилията за киберсигурност, като все повече и повече родни мрежи използват способността си за криптиране, за да заобиколят традиционните DNS мерки и други наследени технологии. Шифрованите заявки означават, че те попадат под радара на типичните мерки и не позволяват корпоративните инструменти за киберсигурност, които разчитат на локални DNS сървъри и DNS мониторинг, да блокират определени заявки за достъп. Това потенциално би могло да доведе до пренасочване на служители към сайтове, заразени със злонамерен софтуер.

Какво трябва да направят компаниите, за да се защитят?

Фирмите трябва да предприемат стъпки, за да гарантират, че всичките им устройства, сървъри и всичко под техния контрол поддържа TLS 1.3. Въпреки това, вероятното понижаване до 1.2 при работа с външни точки означава, че уязвимостите на по-стария протокол все още трябва да бъдат управлявани. За щастие, 1.3 има вградена функция, която блокира, когато се извърши тази реверсия, така че компаниите да могат да се справят със ситуацията.

Задълбочавайки се, компаниите трябва да осигурят създаването на инструменти за мрежов мониторинг, за да се справят с добавеното криптиране, което TLS 1.3 носи и как то може да бъде използвано от нападателите, за да получат предимство. Обикновено компаниите използват MITM междинна кутия, която анализира заявки, направени в TLS 1.2 и решава дали заявката е истинска или не, преди да бъде издаден съответният сертификат. Но този процес е невъзможен с 1.3, тъй като криптира аспектите, използвани от средната кутия за преценка на исканията. Предприятията трябва да се стремят да засилят сигурността на крайните точки, за да помогнат за смекчаване на първоначалния достъп на натрапници до мрежите, като същевременно гарантират, че екипите за сигурност получават актуално обучение за реагиране и достъп до разузнаването в реално време за идентифициране и анализ на атаките.

Преминаването към TLS 1.3 ще намали закъснението и ще премахне уязвимите места, налични в TLS 1.2. Но бизнесът не може просто да го възприеме, а след това да седне и да се отпусне. С по-старите протоколи, които все още се използват широко и техните уязвимости са експлоатирани, организациите трябва да подобрят мерките за сигурност на крайните точки и експертния опит на своите екипи за сигурност.

За повече информация:

https://www.helpnetsecurity.com/2020/04/06/tls-1-3-adoption/

BGP отвличане на трафик от Google, Amazon и други известни мрежи

Уеб трафикът е бил отвлечен от стотици мрежи, за да бъде пренасочен

07 април 2020 г.

Според доклади, телекомуникационен доставчик, който е собственост на Русия, е пренасочил трафик, предназначен за най-непосредствените мрежи за доставка на съдържание (CDN) и облачни доставчици на хостове в целия свят. Цялото пренасочване продължило около час и засегнало над 8 500 маршрута за движение в интернет. Засегнатите организации са повече от известни.

Според източници, засегнатите са добре познати имена като Cloudflare, Digital Ocean, Linode, Google, Joyent, Facebook, LeaseWeb, Amazon, GoDaddy и Hetzner.

Всички признаци на тази атака сочат, че става въпрос за отвличане на Border Gateway Protocol (BGP). Това е нелегитимно превземане на IP префикси от похитител за пренасочване на трафика.

Тази техника прави похитителите силни, защото те могат по всяко време да „публикуват съобщение“, заявявайки, че сървърите на определена компания са в тяхната мрежа. В резултат на това, целият трафик, напр. трафикът на Amazon, ще бъде пренасочен на сървърите на похитителя.

В миналото, когато протоколът за прехвърляне на хипертекст не беше толкова широко използван за криптиране на трафика, отвличането на BGP беше доходоносен начин за извършване на атаки от типа man-in-the-middle (MitM) и улавяне и промяна в трафика. Но в последно време анализът и декриптирането става по-лесно заради отвличането на BGP, тъй като с времето криптирането отслабва.

Това затруднение не е ново. То тревожи киберсвета от няколко десетилетия, главно защото целта е да се повиши сигурността на BGP. Въпреки работата по няколко проекта, не е постигнат голям напредък в подобряването на протокола.

Мрежата на Google е ставала жертва на отвличане на BGP от нигерийска група и преди. Изследователите споменават, че не е необходимо отвличането на BGP да бъде злонамерено.

Съобщава се, че „заблуждаването на ASN“ (номер на автономна система) е една от другите основни причини за отвличането на BGP, тъй като това е кодът, чрез който се разпознават интернет единици и това може случайно да завърши с пренасочване на трафика.

За изследователите е доста трудна задача да кажат със сигурност дали в случая отвличането на BGP е било умишлено или случайно.

За повече информация:

https://www.ehackingnews.com/2020/04/bgp-hijacking-victimizes-google-amazon.html