CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 31.03.2020 г.

Съдържание

Незащитен доставчик на облачно хранилище разкрива клиентски данни

30 март 2020

„Защитен“ доставчик на облачно хранилище в крайна сметка се оказа не толкова „сигурен“ за клиентите си. Пореден ден, поредно нарушение на данните - този път изследователите идентифицираха масивна група от данни, изложени на незащитена Amazon S3 bucket.Най-лошото е, че всеки, който има интернет връзка, може да получи достъп до данните, тъй като няма никаква автентификация на сигурността.

Според изследователския екип на vpnMentor, базата данни е собственост на Data Deposit Box., канадски доставчик на сигурно облачно съхранение. Задълбочен анализ показва, че неправилно конфигурираната S3 bucket съдържа около 270 000 лични файла, качени от клиентите на компанията, използвайки нейната сигурна услуга за съхранение в облак.

Тревожната част е, че сред други чувствителни данни като потребителски имена, пароли, IP адреси, имейл адреси и глобално уникални идентификатори за ресурси (GUID), базата данни съдържа и лична информация на клиенти - всички в обикновен текстов формат.

Въпреки че не е ясно дали базата данни е била достъпна от трета страна със злонамерено намерение, ако е била, тя излага клиентите на измами и кражби на идентичност в реалния живот. Нападателят може да използва и открити идентификационни данни за вход, за да хакне акаунти на жертви на други уебсайтове, в случай че използва същата парола.

Независимо от това, на риск са изложени не само акаунти в социални медии и лични имейл акаунти, но и се създава възможност мошеници да разпространяват зловреден софтуер между контактите на засегнатите потребители.

Ако имате акаунт в базата данни, е време да промените паролата си заедно с имейл адреса си. Препоръчва се също така потребителите да разчитат на фалшив имейл адрес, направен единствено за споделяне на файлове и други услуги, които не изискват личната им информация за регистрация.

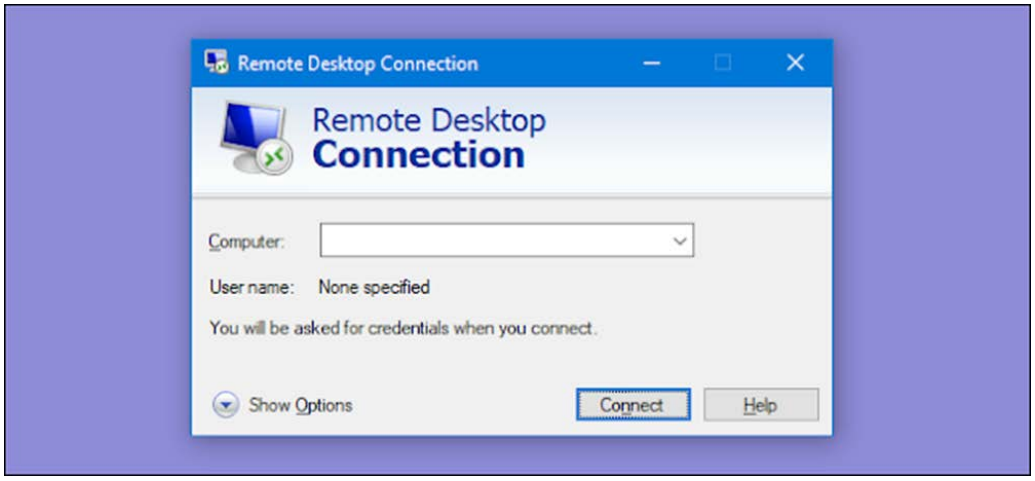
Както може би вече знаете, това не е първият път, когато Amazon S3 bucket е изложила такива лични данни на нищо неподозиращи потребители.

За повече информация:

https://www.hackread.com/secure-cloud-storage-provider-plain-text-data/

Експерти по сигурността твърдят, че голям брой мрежи в Руската федерация са достъпни чрез RDP

31 март 2020



Хакерите може да се опитат да получат достъп до компютри, работещи под Windows 7, Windows Server 2008 или Windows Server 2008 R2

Експерти заявиха, че броят на мрежите в Руската федерация, достъпни чрез протокола за отдалечен десктоп (RDP) за три седмици (от края на февруари 2020 г.)е нарастнал с 9% и достига над 112 000.

Достатъчно е хакерите да изпратят специална RDP заявка на уязвими услуги за отдалечен десктоп (RDS) за атака. Не се изисква удостоверяване. Ако успее, нападателят може да инсталира и изтрива програми на компрометирана система, да създава акаунти с най-високо ниво на достъп и да чете и редактира поверителна информация. Уязвимостите засягат операционните системи Windows 7, Windows Server 2008 и Windows Server 2008 R2.

Хакерите се опитват да получат достъп през сървъри и да влязат в локалната мрежа. Този бум е причинен от прехвърлянето на служителите на работа от разстояние.

За сигурна отдалечена връзка служителите трябва да използват специален gateway. За RDP връзки се изисква RDG, за VPN се изисква VPN gateway. Експертите не препоръчват да се свързвате директно с работното място. Те предупреждават, че отварянето на достъп до отделни подмрежи за всички потребители на VPN наведнъж значително намалява сигурността на организацията и не само дава широки възможности на външен нападател, но и увеличава риска от вътрешна атака.

Следователно ИТ специалистите трябва да поддържат сегментиране на мрежата и да разпределят необходимия брой VPN пулове.

Освен това експертите препоръчват да се обърне внимание на критичната уязвимост (CVE-2019-19781) в софтуера Citrix, който се използва в корпоративните мрежи. Уязвимостта в PHP 7 (CVE-2019-11043), която беше включена в списъка на най-опасните до края на 2019 г., трябва да бъде премахната.

За повече информация:

https://www.ehackingnews.com/2020/03/security-experts-say-number-of-network.html

Промишлени контролери все още са уязвими към атаките в стил Stuxnet

31 март 2020

Наскоро изследователите демонстрираха, че хакерите могат да започнат атака в стил Stuxnet срещу програмируеми логически контролери (PLCs) на Schneider Electric, но се смята, че продуктите на други доставчици също могат да бъдат уязвими към същия тип атака.

Прословутият злонамерен софтуер Stuxnet, който Съединените щати и Израел използваха за нанасяне на щети по ядрената програма на Иран, е насочен към SIMATIC S7-300 и S7-400 програмируеми логически контролери (PLCs), произведени от Siemens. Stuxnet внедри злонамерен код в насочени PLC, като злоупотреби със софтуера STEP7 на Siemens, който се предоставя от германския индустриален гигант за контролери за програмиране.

Stuxnet замени библиотека с име s7otbxdx.dll, която STEP7 използва за достъп до PLC, със злонамерена версия, използвайки метод, наречен отразяващо зареждане на DLL, който включва зареждане на DLL от паметта. Това позволява на нападателите да инжектират своя злонамерен код в целевия контролер.

Изследователите от Airbus CyberSecurity са анализирали модула на PLC на Schneider Electric Modicon M340, за да установят дали той е уязвим на подобни атаки. Атаката е насочена към контролера чрез инженерния софтуер на Schneider EcoStruxure Control Expert, известен преди като Unity Pro. Техният анализ води до откриването на

уязвимост, която може да се използва за качване на злонамерен код в PLC Modicon M340 и M580 чрез замяна на един от DLL файловете, свързани с инженерния софтуер.

Подобна атака може да доведе до сериозни последици, включително до прекъсване на производствените процеси или други видове щети. По-интересното е, че от ИТ гледна точка, нападателят може да трансформира PLC в прокси. Това би му позволило да изпраща заявки и да комуникира с мрежата, към която е свързан PLC. Например, той може да получи достъп до вътрешната корпоративна мрежа за кражба на интелектуална собственост или да предприеме атаки срещу други свързани системи.

Експертите посочват също, че нападателят може да поддържа контролирането на компрометираното устройство по интернет и без да има достъп до корпоративната мрежа, след като уязвимостта е била използвана и злонамереният код е зареден.

Легитимният софтуер за автоматизация ще работи, без да показва признаци, че е вградена злонамерена програма. Зловредната част периодично ще изпраща заявки до командния и контролен сървър, контролиран от нападателя през интернет.

Въпреки че подобна атака може да бъде силно вредна или разрушителна - или може да даде предимство на нападателя - използването на уязвимостта не е лесна задача. Най-напред хакерът трябва да получи достъп до периметъра на ICS на целевата организация и да може да комуникира с целевия PLC.

Това вече е много значима операция, която вероятно ще включва привилегирован достъп до редица машини. Ако нападателите са стигнали до този момент, множество защитни мерки за сигурност или не са въведени, или са се провалили.

След това нападателят трябва да изтегли програмата за автоматизация от PLC. Това може да стане от компрометирана инженерна станция или ако PLC е достъпен за всяка машина в мрежата без удостоверяване. След това нападателят трябва да прекомпилира програмата за автоматизация, използвайки техниките, описани от изследователите на Airbus, и да създаде злонамерена програма, която те вграждат в законния софтуер за автоматизация. И накрая, нападателят трябва да качи модифицираната програма в PLC и да я изпълни, но това изисква спиране и стартиране на софтуера за автоматизация и експертите казват, че тази операция може да бъде забелязана.

От друга страна, изследователите предупреждават, че нападателят може да проектира и компилира всяка дадена програма и да я изпрати през C&C сървъра.

Програмата DownloadExec на PLC ще я изтегли и изпълни в движение (няма нужда да преминава през последователност за спиране / стартиране).

Уязвимостта, открита от изследователите на Airbus в продуктите на Schneider Electric, се проследява като CVE-2020-7475 и се класифицира с висока тежест. Компанията е предоставила пач за EcoStruxure Control Expert и актуализации на фърмуера за контролери Modicon M340 и M580. Предоставени са инструкции за справяне с недостатъка.

Schneider посочва, че тези видове уязвимости засягат и продуктите на други доставчици, въпреки че не ги посочва конкретно.

За повече информация:

https://www.securityweek.com/industrial-controllers-still-vulnerable-stuxnet-style-attacks