CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 28.05.2020 г.

Съдържание

Групата за кибершпионаж Turla използва интерфейса на Gmail за командване и контрол

27 май 2020

Изследователите на ESET разкриха нова версия на един от най-старите злонамерени софтуери – задната вратичка ComRat - управляван от групата Turla. Turla е скандална група за кибершпионаж, която е активна повече от десет години. Най-интересната характеристика на актуализираната задна вратичка е използването на уеб интерфейса на Gmail за изпълнение на команди и извличане на данни.

Групата краде чувствителни документи и от 2017 г. е атакувала поне три правителствени институции.

Основната употреба на ComRAT е кражба на поверителни документи. Операторите му дори са въвели .NET изпълним файл, за да взаимодействат с централната база данни на MS SQL Server на жертвата, съдържаща документите на организацията. Операторите на зловредния софтуер използват обществени облачни услуги като OneDrive и 4shared за извличане на данни.

Фактът, че нападателите се опитват да избегнат софтуера за сигурност, е обезпокоителен. Това показва нивото на усъвършенстване на тази група и намерението й да се задържи на едни и същи машини за дълго време. Освен това най-новата версия на зловредния софтуер ComRAT, благодарение на използването на уеб интерфейса на Gmail, е в състояние да заобиколи някои контроли за сигурност, тъй като не разчита на злонамерен домейн.

Ъпгрейдът на задната вратичка бе открит за първи път от ESET през 2017 г. Тя използва изцяло нова база от кодове и е много по-сложна от своите предшественици.

ComRAT, известен също като Agent.BTZ, е злонамерена задна вратичка, която стана известна след използването й през 2008 г. Първата версия на този зловреден софтуер, вероятно издадена през 2007 г., показа възможности за разпространение на червеи чрез подвижни устройства.

Как да се предпазите?

- Поради сложността на работа на зловредния код и мерките за избягване на механизмите за защита, ако не използвате публични облачни услуги (напр.

OneDrive и 4shared) и е възможно, забранете качването (upload) на данни към тях.

- Ако не използвате GMail може да забраните достъпа до GMail или да следите за зачестен трафик към GMail или за наличие на такъв в необичайни часове.
- Понеже зловреденият код се разпространява чрез PowerShell dropper, е препоръчително да забраните PowerShell на машините, на които не се използва.
- IOCs: https://github.com/eset/malware-ioc/tree/master/turla#turla-comrat-v4-indicators-of-compromise
- Детайлен технически анализ на компонентите на ComRAT е достъпен на следния линк:

https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

За повече информация:

https://www.informationsecuritybuzz.com/news/cyber-espionage-group-turla-a-k-a-snake-now-uses-gmail-web-interface-for-command-and-control-eset-discovers/

Apple публикува 11 сигнала за сигурност – инсталирайте корекциите сега

27 май 2020 г.

Apple представи най-новия си набор от актуализации.

За пълнота актуализациите са номерирани APPLE-SA-2020-05-25-1 до APPLE-SA-2020-05-25-11 и обхващат:

iOS 13.5 и iPadOS 13.5

iOS 12.4.7

macOS Catalina 10.15.5

Актуализация на сигурността 2020-003 за Mojave и High Sierra

tvOS 13.4.5

watchOS 6.2.5

watchOS 5.3.7

Safari 13.1.1 (тази актуализация е вградена в поправката на Catalina)

iTunes 12.10.7 за Windows

iCloud за Windows 11.2

icloud за Windows 7.19

Windows Migration Assistant 2.2.0.0

11 от тези уязвимости засягат софтуера в мобилните Apple продукти, Mac и Windows продуктите.

Какво да направите?

Дори и да сте настроили вашия Mac или iDevice да се актуализират автоматично, редовно проверявайте дали наистина са актуални:

- За Mac, отидете на System Preferences > Software Update.
- За iPhone or iPad, отидете на System > General > Software Update.

За повече информация:

https://nakedsecurity.sophos.com/2020/05/27/apple-sends-out-11-security-alerts-get-your-fixes-now/

Злонамереният софтуер Valak атакува сървърите на Microsoft Exchange за кражба на корпоративни пароли

28 май 2020 г.

Злонамереният софтуер Valak за първи път е наблюдаван през 2019 г.

Изследователите наблюдават нова кампания на зловредния софтуер, която е насочена по-специално към САЩ и Германия. В новата кампания той е разработен като сложен, многоетапен модулен зловреден софтуер.

В новата кампания общият вектор на заразата са документите на Microsoft Word, в които е вграден злонамерен макро код.

Установено е, че документът е създаден на английски и немски език и се разпространява в зависимост от геолокацията на целта. Във фазата на разузнаване той събира следните данни от заразените хостове като: информация за потребители, машина и мрежа от заразени хостове, също така проверява за геолокация на машината на жертвата.

Зловредният софтуер прави и скрийншоти на заразената машина и изтегля плъгини и друг зловреден софтуер като Ursnif или IcedID за извършване на други операции.

Новата версия на злонамерения зловреден софтуер го разширява с няколко компонента на плъгини за разузнаване и кражба на информация.

Valak е категоризиран като най-скрития злонамерен софтуер, който използва модерни техники като ADS и скриване на компоненти в системния регистър.

Зловредният софтуер е насочен главно към администраторите и мрежата на предприятията, той събира и краде чувствителна информация от пощенската система на Microsoft Exchange, включително идентификационни данни и сертификат за домейн.

Изследователите забелязват, че зловредният софтуер използва споделена инфраструктура в почти всичките му различни версии.

Зловредният софтуер Valak с разширените му възможности предполага, че той може да се използва със или без да се обединява с друг зловреден софтуер.

Как да избегнете инсталирането на зловреден софтуер?

Препоръчва се да не изтегляте, да не инсталирате какъвто и да е софтуер чрез изтеглящи устройства от трети страни, инсталатори, от неофициални уебсайтове, Peer-to-Peer мрежи (например торент клиенти, eMule), безплатни хостинги на файлове и други подобни канали. Обичайно е такива канали да се използват като инструменти за разпространение на зловреден софтуер. Софтуер трябва да се изтегля само от

официални уебсайтове и чрез директни връзки за изтегляне. Освен това инсталираният софтуер трябва да се актуализира чрез внедрени функции и / или инструменти, които са проектирани от официални разработчици. Приложенията (или уеб връзките) в неподходящи имейли, които са получени от неизвестни, подозрителни адреси, никога не трябва да бъдат отваряни, без първо да ги анализирате. Софтуерът никога не трябва да се активира чрез неофициални инструменти за активиране („cracking“). Не е законно и често причинява инсталиране на високорисков зловреден софтуер. Още едно важно нещо е редовно да сканирате компютъра за заплахи с реномиран антишпионски или антивирусен софтуер и винаги да го актуализирате.

Какво да предприемете, ако вече сте заразени?

Ако смятате, че компютърът ви вече е заразен, препоръчваме да стартирате сканиране с Malwarebytes за Windows, за да елиминирате автоматично инфилтрирания зловреден софтуер. Можете да видите как да премахнете зловредния софтуер и ръчно.

Ако сте проверили списъка с програми, работещи на вашия компютър, например, използвайки мениджъра на задачи и сте идентифицирали програма, която изглежда подозрителна, трябва да продължите с тези стъпки:

Стъпка 1: Изтеглете програмата, наречена Autoruns. Тази програма показва приложения за автоматично стартиране, местоположения в системния регистър и файловата система:

Стъпка 2: Рестартирайте компютъра си в Safe mode

Стъпка 3: Разархивирайте изтегления архив и стартирайте файла Autoruns.exe

Стъпка 4: В приложението Autoruns щракнете върху „Опции“ в горната част и премахнете отметката на "Hide Empty Locations" и "Hide Windows Entries". След тази процедура щракнете върху иконата "Refresh".

Стъпка 5: Проверете списъка, предоставен от приложението Autoruns и намерете файла със злонамерен софтуер, който искате да премахнете. Трябва да напишете пълния му път и име. Обърнете внимание, че някои злонамерени софтуери крият имена на процеси под законни имена на Windows. На този етап е много важно да се избягва премахването на системни файлове. След като намерите подозрителната програма, която искате да премахнете, щракнете с десния бутон на мишката върху нейното име и изберете "Delete".

След като премахнете злонамерения софтуер чрез приложението Autoruns (това гарантира, че зловредният софтуер няма да се стартира автоматично при следващото стартиране на системата), трябва да потърсите името на зловредния софтуер на вашия компютър. Не забравяйте да активирате скрити файлове и папки, преди да продължите. Ако намерите името на файла на злонамерения софтуер, не забравяйте да го премахнете.

Рестартирайте компютъра си в нормален режим. Следвайки тези стъпки, трябва да премахнете всеки зловреден софтуер от вашия компютър. Обърнете внимание, че ръчното отстраняване на заплаха изисква усъвършенствани компютърни умения. Ако нямате тези умения, оставете премахването на злонамерен софтуер на антивирусни и анти-зловредни програми. Тези стъпки може да не работят при напреднали злонамерени програми. Най-добре е да се предотврати заразяване, отколкото да се опитате да премахнете злонамерен софтуер. За да защитите компютъра си, инсталирайте най-новите актуализации на операционната система и използвайте антивирусен софтуер.

За да сте сигурни, че компютърът ви няма злонамерени програми, препоръчваме да го сканирате с Malwarebytes за Windows.

За повече информация:

https://gbhackers.com/valak-malware/