CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Екип за реагиране при инциденти в компютърната сигурност

Мониторинг на актуалните киберновини – към 09.04.2020 г.

Съдържание

Слабост в PowerPoint създава възможности за Mouse-over злонамерена атака

8 април 2020

Нов хак позволява на нападател да създаде Mouse-over във файл на PowerPoint, който задейства инсталирането на зловреден софтуер.

Това е нов тип векторна атака, която позволява на хакери да манипулират файл на PowerPoint, за да се изтегли и да започне инсталирането на зловреден софтуер, просто докато задържате курсора на мишката си върху хипертекстова връзка.

Техниката изисква жертвата да приеме един изскачащ диалогов прозорец, за да се стартира или инсталира програмата. Поради тези причини, Microsoft не счита това за уязвимост. Но изследователите на са съгласни.

Атаката е в състояние да заобиколи ограничението на PowerPoint да не може да се добави отдалечен файл към HyperLink, който при опит да се добави чрез GUI, е невъзможно. А текстът на диалоговия прозорец, съдържащ името на файла, може да бъде манипулиран, за да изписва каквото и да е, включително „Windows Update.bat“ или „Зареждане .. Моля, изчакайте.exe.“ Слабостта е в отворените XML слайдшоу

файлове на PowerPoint, наречени PPSX. Този тип PowerPoint файлове са предназначени само за възпроизвеждане на презентации и не могат да бъдат редактирани.

В PowerPoint е възможно да настроите действие при преминаване на мишката. В своята PoC атака, наречена „Hover with Power“, изследовател по сигурността заобикаля предишните ограничения на PowerPoint, въведени от Microsoft през 2017 г., за да пропусне злонамерени връзки в PowerPoint да инсталират локални изпълними програми, докато задържате курсора върху хипертекстова връзка.

Тъй като атаката Hover with Power задейства само един изскачащ диалогов прозорец - който може да бъде манипулиран от нападателя - изследователят разглежда това като уязвимост. Когато обаче се свързва с Центъра за реакция на сигурността на Microsoft (MSRC), на 2 април му е отговорено, че разследването му ще бъде „затворено“, тъй като атаката изисква елемент на социално инженерство.

Запитване на Threatpost към Microsoft потвърди същото. „За да бъде успешна тази социално-инженерна техника, потребителят трябва първо да предприеме действия, за да отхвърли предупреждението за сигурност. Ние насърчаваме нашите клиенти да практикуват добри компютърни навици, включително да проявяват предпазливост при кликване върху връзки към уеб страници, отваряне на неизвестни файлове или приемане на прехвърляне на файлове “, пише в съобщение служител на Microsoft.

За повече информация:

https://threatpost.com/powerpoint-weakness-mouse-over-attack/154589/

Множество приложения, подобни на Skype, крият злонамерен софтуер

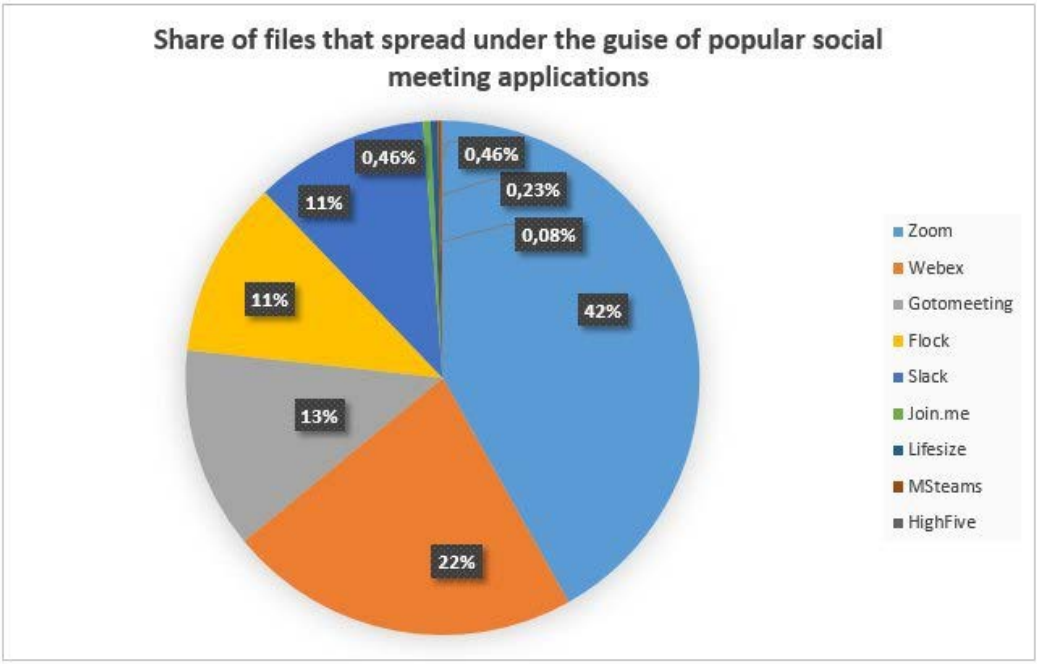
8 април 2020

Стотици хиляди файлове за злонамерен софтуер са прикрити като добре познати приложения за социални конференции и сътрудничество.

Популярните приложения за конферентна връзка се превърнаха в основна примамка за киберпрестъпления по време на ерата COVID-19 за работа от дома - и Skype е безспорният лидер, когато става въпрос за изтегляния на злонамерени файлове.

Анализ от април на Касперски разкри общо 120 000 подозрителни пакета зловреден и рекламен софтуер, маскиран като версии на приложението за видеообаждане.

Трябва да се отбележи, че Skype не е единствен: Изследването установи, че сред общо 1300 подозрителни файла, които не използват името на Skype, 42 процента са били прикрити като Zoom, следвани от WebEx (22 процента), GoToMeeting (13 процента)), Flock (11 процента) и Slack (11 процента).



С нарастването на физическото дистанциране, експерти от Касперски изследват пейзажа на заплахите за приложенията за социални срещи, за да се уверят, че потребителите са в безопасност. Приложенията за социални срещи в момента предоставят лесни начини за свързване на хората чрез видео, аудио или текст, когато няма други средства за комуникация. Въпреки това киберизмамниците не се колебаят да използват този факт и се опитват да разпространяват различни киберпрестъпления под прикритието на популярни приложения.

Злонамерени скайп приложения за социални срещи

Някои от злонамерените файлове се оказват просто версии на вече съществуващи такива, но сред откритите действителни заплахи, на преден план излизат няколко зловредни файлове и типове файлове, включително две семейства на рекламен софтуер: DealPly и DownloadSponsor.

И двете семейства са инсталатори, които показват реклами или изтеглят рекламни модули. Такъв софтуер обикновено се появява на устройствата на потребителите, след като бъдат изтеглени от неофициални пазари.

Има и някои заплахи за злонамерен софтуер, прикрити като .LNK файлове - преки пътища към приложения - които Kaspersky откри като Exploit.Win32.CVE-2010-2568. Това е стар, но все още широко разпространен злонамерен код, който позволява на нападателите да заразят целта със зловреден софтуер. Старата, закърпена уязвимост, която се използва, е Windows Shell, която не се обработва правилно по време на показване на икони в Windows Explorer, което позволява произволно изпълнение на код чрез специално създадени .LNK или .PIF файлове за бърз достъп. Засяга най-вече Windows XP, Vista и Windows 7.

Троянците също са популярен тип злонамерен софтуер, откриван във фалшивите приложения, особено в Skype.

В сегашното положение, когато повечето от нас работят от вкъщи, е изключително важно да се уверим, че това, което използваме като инструмент за онлайн социална среща, е изтеглено от легитимен източник, настроено е правилно и няма сериозни незакърпени уязвимости.

За повече информация:

https://threatpost.com/skype-apps-hide-malware/154566/

Нова версия на операционната система Tails 4.5 беше издадена с поправки на проблеми в сигурността

9 април 2020

Tails s е ориентирана към сигурността операционна система, базирана на Debian, която не изисква инсталация. Можете да използвате операционната система на всеки компютър от USB флашка или DVD.

Операционната система има за цел да осигури поверителност и анонимност, всички нейни комуникации се осъществяват чрез мрежата TOR.

Тя не оставя следи на компютъра и използва най-съвременни криптографски инструменти за криптиране на вашите файлове, имейли и незабавни съобщения.

Новата версия 4.5

Tails 4.5 беше пуснат с функция за защита Secure Boot, която е предназначена да защитава системата от изпълнение на злонамерен код в процеса на зареждане.

Докато системата зарежда, всеки път, когато фърмуерът на UEFI проверява двоичния файл за валиден подпис, ако се зарежда невалиден двоичен файл, докато защитното зареждане е активирано, потребителят се известява и системата ще откаже да се стартира.

Новата версия на Tails включва и поправка на няколко грешки в защитата, тя също така включва коригиране на няколко уязвимости на Firefox.

Talis се предлага и с актуализираната версия на Tor Browser 9.0.9, можете също да изтеглите браузъра Tor от страницата за изтегляне.

Как да актуализирате?

За да актуализирате с най-новата версия, просто свържете Tails 4.2 или по-нова версия към интернет и преминете към процеса на автоматично ъпдейтване, ако по някаква причина актуализацията се провали или използва стара версия, опитайте ръчния процес.

Тук ще намерите стъпките за изпълнение на новата инсталация с Windows, macOS & Linux. Също така имайте предвид, че всички данни на USB флашка ще бъдат загубени.

Можете да изтеглите Tails 4.5 директно от тук за USB стикове и за DVD и виртуални машини.

Версия Tails 4.6 е планирано да бъде пусната на 5 май.

За повече информация:

https://gbhackers.com/new-version-tails-4-5/