CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

*Екип за реагиране при инциденти в компютърната сигурност*

# Мониторинг на актуалните киберновини – към 11.05.2020 г.


## Съдържание

## Microsoft Edge активира нова функция за намаляване на уеб спама

09 май 2020 г.

Microsoft Edge вече дава на потребителите възможност да скрият онези досадни диалогови прозорци за уведомяване на браузъра, които обикновено се използват от уебсайтовете, за да показват съдържанието си или дори спам пред посетителите.

За тези, които не са запознати с термина „известия в браузъра“, те са функция, която позволява на уебсайтовете да питат посетителите дали биха искали да се регистрират, за да получават известия за ново съдържание. След това уебсайтовете могат да изпращат съдържание към абонатите чрез браузъра, дори когато посетителят не е на уебсайта или когато браузърът не се използва.

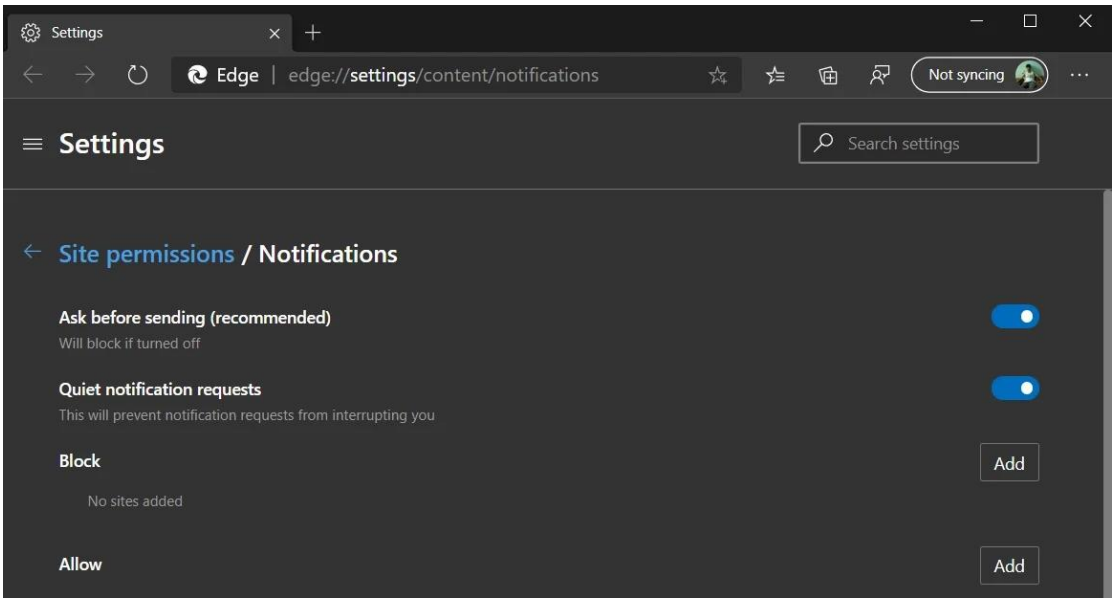
Напоследък често срещана тактика на сайтовете за измами е да се показват диалогови прозорци за известия на браузъра и да се посочи, че трябва да „разрешите“ известията, преди да можете да възпроизвеждате видео, да изтеглите файл или да посетите сайта.

След като приемете абонамента, тези сайтове за измами ще започнат да изпращат постоянен поток от нежелани реклами, свързани със сайтове за онлайн запознанства, нежелани разширения на браузъри, сайтове за възрастни, уеб игри и дори злонамерен софтуер.

Microsoft предлага нова функция, наречена "Quiet notification requests" в браузъра Edge, която ще блокира показването на всички диалогови прозореци на браузъра.

Тази функция вече е налична в Microsoft Edge Beta 83 и можете да я изпробвате сега, като изпълните следните стъпки:

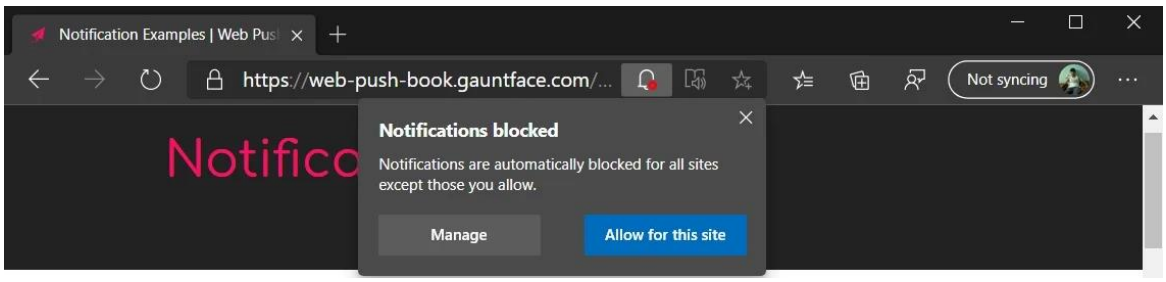
- Отворете настройките на Edge.
- Отворете Site permissions > Notifications




- Активирайте “Quiet notification requests”

След като тази функция е активирана, когато посещавате сайт, който обикновено показва диалогов прозорец за абонамент за браузър, браузърът ще скрие поканата и ще покаже малка икона на звънец в адресната лента.

Ако потребителят иска да види известието, той може да кликне върху звънеца и ще се отвори диалогов прозорец, който му позволява да реши дали иска да разреши известията или не.




Тази функция е много полезна, тъй като хората обикновено получават реклами чрез известия от уебсайтове и нямат представа как ги получават.

Чрез заглушаване на постоянния поток от диалогови прозорци за известяване, значително ще намалее количеството уеб спам, който потребителите получават.

**За повече информация:**

**https://www.bleepingcomputer.com/news/microsoft/microsoft-edge-is-getting-a-new-feature-to-reduce-web-spam/**

## Хакери заразяват автентично 2FA приложение, за да заразят Mac устройства със зловреден софтуер

10 май 2020

Смята се, че скандалната група Lazarus стои зад този зловреден софтуер.

Много киберпрестъпни групи през годините са си създали име благодарение на последователността и решителността си в провеждането на атаки. Една такава група е Lazarus, за която се смята, че е от Северна Корея и действа от 2009 г.

Изследователи от Malwarebytes Labs се натъкват на още една атака на скандалната група, при която злонамерен софтуер е вмъкнат в базирано на macOS 2FA приложение, наречено MinaOTP.

Целта на злонамерения софтуер е да разпространи троянец с име Dacls, който може да бъде използван от нападателите за получаване на отдалечен достъп. Функциите, които може да изпълнява, включват изпълнение на команди, управление на файловете на системата, управление на процесите в системата, проследяване на трафика и сканиране за червеи.

След като събере данните, злонамереният софтуер се свързва към своя C2 сървър чрез TLS връзка, „извършва маяк“, криптира данните и след това я прехвърля на SSL, „използвайки алгоритъма RC4“.

Коментирайки как работи, изследователите заявяват в своя блог пост, че този RAT се запазва чрез LaunchDaemons или LaunchAgents, които вземат файл със списък на свойствата (plist), който определя приложението, което трябва да бъде изпълнено след рестартиране. Разликата между LaunchAgents и LaunchDaemons е, че LaunchAgents изпълняват код от името на влезлия в профила си потребител, докато LaunchDaemon изпълнява код като root потребител.

Тези, които следят света на киберсигурността отблизо, знаят, че троянец със същото име съществува за Windows и Linux, като тази нова версия е техен вариант. Това стана ясно от анализа, извършен от изследователи, който разкри, че имената на следните 2 файла са еднакви в троянския файл за всички 3 операционни системи:

c_2910.cls – the certificate file

k_3872.Cls – the private file.

Освен това, плъгините се съдържат във всички версии за иницииране на различни процеси. Преглед на macOS варианта разкри, че шест от 7 приставки са същите като тази на Linux.

Новото е плъгинът SOCKS, който се използва за свързване към самия малуер и C2 сървъра чрез прокси.

В заключение, това не е първият път, когато тази група атакува macOS. Следователно ние като потребители можем да предприемем прости предпазни мерки като инсталиране на реномирана антивирусна програма, изтегляне на файлове заедно със сканиране за всеки злонамерен софтуер с надежден антивирусен софтуер и проверка на хешовете им, за да проверим оригиналността им.

Можете също да следвате тези 11 лесни съвета, за да защитите вашия Mac от хакери:

1. **Създайте стандартен потребителски акаунт**

Стандартният потребителски акаунт е неадминистраторски акаунт на Mac. Препоръчва се използването на стандартен потребителски акаунт за ежедневни дейности и администраторски потребителски акаунти за конфигуриране на системата. Ползата от това е, че всеки път, когато неоторизирано приложение се опита да се инсталира във вашата система, то ще поиска администраторски привилегии и можете да определите дали приложението е ненадеждно.

2. **Деактивирайте автоматичното влизане на потребители**

По подразбиране Mac е настроен автоматично да влиза в потребителския ви акаунт. Това е потенциален проблем, когато сте свързани с обществена Wi-Fi мрежа или пътувате. Можете да промените това във вашата OS X, като направите това:

- Кликнете върху бутона „Apple“
- Кликнете върху “System Preferences”
- Изберете раздела “User & Groups”
- Щракнете върху бутона Lock по-долу, въведете вашата администраторска парола.
- Кликнете върху раздела “Login Options”
- Изберете “Off” от изскачащия прозорец, след като щракнете върху “Automatic Login”
- Изберете “Name and Password” от изскачащия прозорец, след като щракнете върху “Display login window as.”

### 3. Изключете Java и автоматичното изтегляне в браузъра Safari

Препоръчва се да премахнете Java, но ако ви е необходимо, изключете го, ако не го използвате. За да деактивирате автоматичното изтегляне в браузъра Safari:

- Отидете в настройките на браузъра си сафари
- Премахнете отметката от “Open safe files after downloading” в раздела General.

### 4. Премахнете самостоятелния Flash Player

Ако не се нуждаете от самостоятелно приложение за флаш плейър, премахнете го от системата на Mac. За да премахнете ръчно Flash Player, следвайте това официално ръководство на Adobe.

### 5. Деактивирайте отдалеченото влизане

Apple има възможност да разреши на други устройства отдалечен достъп до вашия Mac. Това е добър вариант, ако пътувате и бихте искали да получите достъп до устройството си. Но това е и заден прозорец за хакерите да имат достъп до устройството си от разстояние. За да деактивирате тази опция:

- Кликнете върху бутона „Apple“.
- Изберете “System Preferences” за достъп до опцията.
- Изберете опцията „Sharing“.
- Премахнете отметката от “Remote Login.”

**6. Задайте на GateKeeper да предотвратява изпълнението на цифрово неподписани приложения**

GateKeeper е приложение за проверка на злонамерен софтуер, което защитава вашия Mac от злонамерен софтуер и недобросъвестни приложения, изтеглени от интернет. Настройте вашия GateKeeper да ви предупреждава, когато изтеглите всяко цифрово неподписано приложение или ако файлът не е от магазина на Apple.

**7. Инсталирайте антивирусен софтуер на Mac**

Изтеглете антивирус, те засега са предимно безплатни, който постоянно да проверява системата ви .

**8. Актуализирайте редовно своя Mac OS X**

Apple непрекъснато актуализира софтуера си OS X. Препоръчва се незабавно да актуализирате своя Mac, тъй като той получава актуализация от Apple:

- Кликнете върху бутона „Apple“.
- Изберете “System Preferences” за достъп до опцията.
- Изберете опцията “Software Update”
- Изберете опцията “Check for update”
- Изберете честота „дневна“ (или задайте ръчна честота).

**9. Инсталирайте приложението Tracker**

Инсталирайте някакво приложение за проследяване като застрахователна мярка на вашия Mac и смартфон, за да защитите вашите данни. В случай че вашият Mac или смартфон бъде откраднат, можете да изтриете личните си данни дистанционно от всяко от устройствата.

**10. Използвайте VPN софтуер**

За да осигурите вашата мрежова сигурност и онлайн поверителност, използвайте някои най-добри за Mac VPN системи, за да осигурите шифроване на Mac, онлайн сигурност и достъп до блокирано съдържание.

**11. Използвайте две вградени защитни стени**

Mac има две силни вградени защитни стени в системата си. Това са IPFW Packet-Filtering Firewall and Application Firewall.

Защитната стена на приложението предотвратява задаването на ограничение за входяща програма от други компютърни мрежи. Настройте защитна стена на приложението, ползвайки ръководството на Apple.

IPFW Packet-Filtering е защитна стена от високо ниво, която изисква редактиране в хост файла, което е трудно за следване от следващите потребители. Можете да го запазите до настройките по подразбиране или да следвате ръководството на Университета в Северна Каролина.

**За повече информация:**

**https://www.hackread.com/hackers-infect-2fa-app-infect-mac-with-malware/**