CERT BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

*Екип за реагиране при инциденти в компютърната сигурност*

# Мониторинг на актуалните киберновини – към 30.03.2020 г.


## Съдържание

# TrickBot Mobile App заобикаля двуфакторното удостоверяване за банкови услуги, осъществявани по интернет

25 март, 2020


Авторите на зловреден софтуер, създали TrickBot banking Trojan, са разработили ново приложение за Android, което може да прихваща еднократни кодове за разрешение, изпратени до клиенти на интернет банкиране чрез SMS или сравнително по-сигурни push известия, и да извърши измамни транзакции.

Името TrickMo е директна препратка към подобен вид Android зловреден софтуер, наречен ZitMo, който е разработен от бандата за киберпрестъпления Zeus през 2011 г., за да победи двуфакторната автентификация, базирана на SMS.

Веднъж инсталиран, TrickMo стартира себе си, след като устройството стане интерактивно или след получаване на ново SMS съобщение. В допълнение, той разполага със сложен механизъм за настройки, който позволява на отдалечен атакуващ да издава команди за включване / изключване на специфични функции (напр. разрешения за достъп, състояние на запис, статус на SMS приложение) чрез сървъра за командване и управление (C2) или чрез SMS съобщение.

Когато бъде стартиран злонамереният софтуер, той дава достъп до широк спектър от информация, включително:

- Лична информация за устройството;
- SMS съобщения;
- Записване на насочени приложения за еднократна парола (TAN);

- Снимки.

Но за да избегне подозрение при кражба на TAN кодовете, TrickMo активира заключен екран, като по този начин предотвратява достъпа на потребителите до своите устройства. По-конкретно, той използва фалшив екран за актуализиране на Android, за да маскира своите OTP кражби.

И на последно място, той предлага функции за самоунищожение и премахване, което позволява на бандата за киберпрестъпления зад TrickMo да премахне всички следи от присъствието на зловреден софтуер от устройство след успешна операция.

Превключвателят за премахване на зловредния софтуер може да се активира и чрез SMS, но изследователите на IBM откриха, че е възможно да се декриптират шифрованите SMS команди с помощта на твърдо кодиран RSA частен ключ, вграден в изходния код, като по този начин е възможно да се генерира публичния ключ и да се изработи SMS съобщение, което може да включва функцията за самоунищожение.

**За повече информация:**

https://thehackernews.com/2020/03/trickbot-two-factor-mobile-malware.html

## Хакерите използват 0-day бъгове в Draytek устройства, за да се насочват към корпоративни мрежи

27 март, 2020

Най-малко две отделни групи хакери са експлоатирали две критични уязвимости, позволяващи дистанционно инжектиране на команди (CVE-2020-8515), засягащи DrayTek Vigor суичове, load-balancers, рутери и VPN gateway устройства, за да подслушват мрежовия трафик и да инсталират backdoor .

0-day атаките започнаха някъде в края на миналия ноември или в началото на декември и потенциално продължават срещу хиляди публично изложени суичове DrayTek, Vigor 2960, 3900, 300B устройства, които все още не са пачнати с най-новите фърмуер актуализации, пуснати миналия месец.

Списъкът на засегнатите версии на фърмуера е следният:

Vigor2960 < v1.5.1

Vigor300B < v1.5.1

Vigor3900 < v1.5.1

VigorSwitch20P2121 <= v2.3.2

VigorSwitch20G1280 <= v2.3.2

VigorSwitch20P1280 <= v2.3.2

VigorSwitch20G2280 <= v2.3.2

VigorSwitch20P2280 <= v2.3.2

**За повече информация:**

https://thehackernews.com/2020/03/draytek-network-hacking.html

## Как да предпазите вашия рутер и Wi-Fi от хакери

27 март, 2020

Вашият рутер помага за разпространението на интернет в цялата ви мрежа, но също така крие известни рискове. Хакерите са станали достатъчно интелигентни, за да

разпространяват зловреден софтуер, ransomware и други заплахи за киберсигурност, за да изложат цялата ви мрежа на опасност.

Хакерите използват уязвими рутери, за да пренасочват потребителите към злонамерено приложение, свързано с COVID-19, насочено към вашите лични данни. Въпросът е как човек може да защити своите рутери от подобни заплахи? Въпреки че това може да изглежда като непреодолима задача, има неща, които можете да направите, за да запазите рутера и Wi-Fi в безопасност от хакери.

**1: Коригирайте настройките на вашия рутер**

Първата стъпка, която трябва да направите, е да проверите настройките за сигурност на вашия рутер. Много потребители ще оставят настройките по подразбиране, без да осъзнават, че те могат да бъдат коригирани. Тяхното ниво на регулиране зависи от самия рутер, но всички рутери имат известна защита.

Влезте в настройките на вашия рутер. Информацията за вход трябва да се предоставя с рутера, който обикновено включва IP адрес и парола. Там трябва да промените данните за вход, за да направите паролата уникална и трудна за гадаене, така че хакерите да не могат лесно да влязат във вашата мрежа.

**2: Промяна на името на Wi-Fi**

Следващото нещо, което трябва да направите, е да промените името на вашия Wi-Fi. Идентификаторът на набор от услуги (SSID) е името по подразбиране на вашата мрежа. Оставяйки го такъв, какъвто е, ще улесни външни хора просто да сканират името на вашата мрежа, за да го намерят. Ако промените името, няма да е толкова лесно да намерят мрежата ви.

**3: Деактивирайте излъчването на име на мрежата**

Това трябва да е в настройките на вашия рутер. Това е функция, която се използва от мрежи, които споделят Wi-Fi, като кафенета, библиотеки или хотели. Това не е необходимо за вашата частна домашна мрежа. Изключването му ще премахне вашата мрежа от отворения списък от мрежи.

**4: Включете мрежовото си криптиране**

Много рутери се предлагат с вградена настройка за криптиране, която обикновено се изключва. Вижте дали можете да го включите, когато първоначално сте настроили своя рутер. Наличното криптиране трябва да бъде WPA2.

**5: Вижте дали вашият рутер има създадена мрежа за гости**

Не искаме да внушаваме, че приятелите може да не са в безопасност с вашата парола, но ако можете да им дадете достъп до гост мрежа чрез вашия рутер, а не до действителната ви мрежа, ще увеличите общата сигурност на вашата мрежа.

Наистина не бива да предоставяте свободно мрежовата си парола, така че ако имате възможност да разрешите на посетителите да се възползват от вашия интернет, като същевременно поддържате безопасността на мрежата, това е пътят.

**6: Проверете защитната стена на вашия рутер**

Всички три-лентови или дву-лентови рутери се предлагат с някакъв тип защитна стена, която вече е вградена. Това обаче не означава, че защитната стена се включва автоматично. Софтуерна защитна стена е налице, за да защити вашата мрежа от нахлувания. Ако вашият рутер няма защитна стена, трябва или да помислите за нов рутер, или за закупуване на отделно устройство за защитна стена, за да поддържате мрежата си възможно най-безопасна.

**7: Използвайте VPN**

VPN или виртуалната частна мрежа е начин за криптиране на комуникацията ви, идваща от вашата мрежа. Те работят, като смесват комуникациите, влизащи и излизащи от вашата мрежа, така че никой да не може да вижда смислена комуникация. След като информацията пристигне на вашия компютър, вашата VPN ще я дешифрира.

**8: Поддържайте софтуера и фърмуера актуални**

Производителите актуализират софтуера и фърмуера за своите устройства от време на време, актуализирайки всяка информация за нов зловреден софтуер или вируси. Когато има налични актуализации за сигурност, никога не отлагайте изтеглянето им.

Ако сте интелигентни с поверителността на мрежата си и поддържате всичко актуално, ще можете да запазите рутера си в безопасност.

**За повече информация:**

https://www.hackread.com/how-to-keep-your-router-and-wifi-safe-from-hackers/

## Домашни рутери се използват за за кражба на информация чрез злонамерения софтуер „Oski“

29 март, 2020

Разпространението на злонамерен софтуер чрез приложения, които се изтеглят от потребителите в името на „най-новата информация и инструкции за COVID-19“ е сред една от най-разпространените заплахи, наблюдавани след избухването на новия коронавирус. В резултат на това потребителите са принудени да изтеглят приложения като COVID19Tracker или Covid Lock, като приложението заключва смартфони и иска откуп от 100 долара в Bitcoin за освобождаване на техните данни.

Друг пример е откриването на нов тип атака, която е насочена към домашните рутери. Той пренасочва жертвите към заразен уебсайт след промяна на настройките на DNS и след това сваля файл за шифроване на злонамерен софтуер „Oski“, който криптира важните файлове в системата на жертвата. Той използва сложен алгоритъм за криптиране на файловете и добавяне на разширение .Osk към всеки файл. След като успешно извърши процеса на шифроване, злонамереният софтуер оставя бележка за откуп във всички папки, съдържащи криптирани данние „КАК ДА ВЪЗСТАНОВИТЕ КРИПТИРАНИ ФАЙЛОВЕ.TXT.“

„За да изглежда файлът легитимен (сякаш името на файла е признак за легитимност), атакуващите го кръщават„ runset.EXE “„ covid19informer.exe “или„ setup_who.exe “.

**За повече информация:**

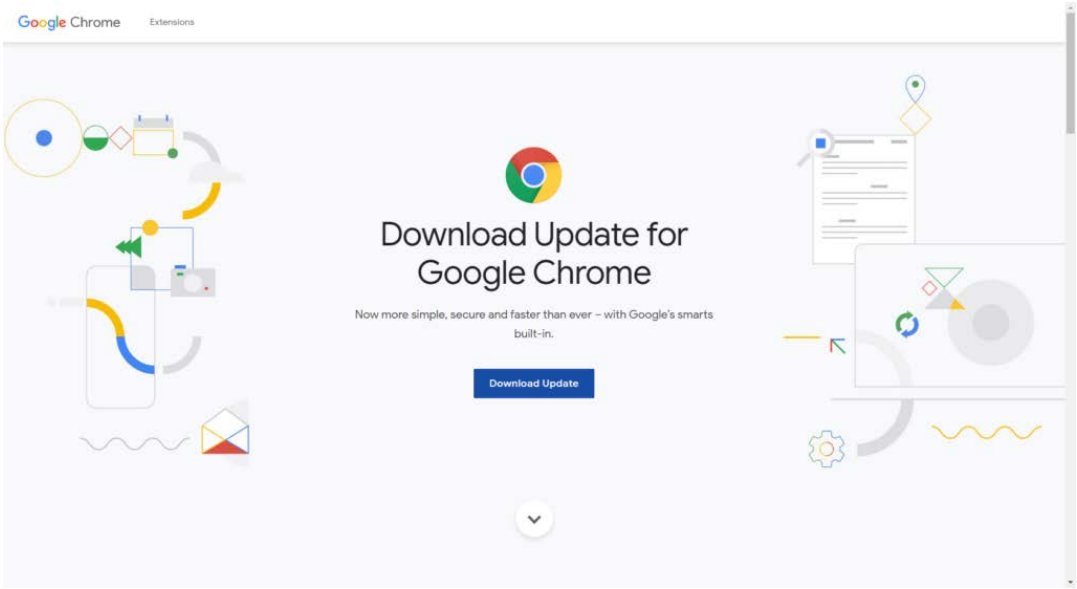
https://www.ehackingnews.com/2020/03/home-routers-hijacked-to-deliver-info.html

## Много потребители хакнати чрез фалшива актуализация на Google Chrome от компрометирани уебсайтове на WordPress

30 март, 2020

Фалшива актуализация на Chrome разпространява backdoor от компрометирани уебсайтове на WordPress. Тази актуализация улеснява последващите атаки на хакерите със злонамерен софтуер. Хакерите успяват да получат администраторски достъп до целевите уебсайтове и да вградят злонамерен JavaScript код на компрометираните

страници. Когато посетител достигне заразените страници, той бива пренасочван към фишинг уебсайт. Този сайт приканва посетителя да изтегли фалшива актуализация на браузъра Chrome.




Тъй като фишинг страницата изглежда легална, потребителите могат да кликнат върху бутона за изтегляне и несъзнателно изтеглят backdoor. По отношение на механизма на заразяване, накратко изпълнението на инсталатора създава папка в директорията „userappdata“, съдържаща файлове за приложението TeamViewer. След това извлича два SFX архива, защитени с парола, единият от които е злонамерена библиотека msi.dll, която улеснява установяването на непозволена връзка с целевото устройство. Вторият архив включва скрипт за заобикаляне на откриването на Microsoft AV. След като присъствието е установено, хакерите могат да използват backdoor, за да доставят payloads като keylogger, infostellers или троянски коне за отдалечена връзка.

**За повече информация:**

https://latesthackingnews.com/2020/03/30/many-users-hacked-via-fake-google-chrome-update-from-compromised-wordpress-websites/