НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

## МАГИСТЪРСКИ ФАКУЛТЕТ

# ДЕПАРТАМЕНТ "ИНФОРМАТИКА"

**ПРОГРАМА „Софтуерни технологии в Интернет”**



### ЗАДАЧА ЗА ТЕКУЩА ОЦЕНКА

**КУРС: INFM102 Компютърна сигурност в Интернет**

**ТЕМА: Въпроси по задача 4**

**НА СТУДЕНТА** : Георги Иванов Георгиев

**Фак. №:** f88683

**Дата:** 14/01/2018 г.

**Преподавател:**

/ доц. В.Къдрев / …………………

София

**Материал 1**

**Как да защитите своите устройства от атаките Meltdown и Spectre**

**Линк:** [**https://thehackernews.com/2018/01/meltdown-spectre-patches.html**](https://thehackernews.com/2018/01/meltdown-spectre-patches.html)

**Резюме:**

На кратко Meltdown и Spectre атаките таргетират пробив в сигурността на много процесори с марката Intel, ARM и AMD, като ако бъдат изпълнени коректно потенциално позволяват на атакуващите да откраднат пароли, криптиращи ключове и всякакъв вид частна (поверителна) информация. И двата вида атаки се възползват от оптимизиращата техника наречена „спекулативно изпълнение“ с цел да придобият достъп до привилигирована памет (памет не принадлежаща на дадено приложение изпълнявано на конкретна машина), дори тази заделена от кернела.

Според някои единствената предпазна мярка е тези чипове да се подменят. Но това е непрактично решение за голяма част от потребителите и компаниите разчитащи на тези чипове. Към момента съществуват следните пачове замаскиращи проблема:

1. ([KB4056892](https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056892))  - секюрити пач на Майкрософт. Не планиран. Пачът ще излезе за Windows 7,8 и 10. Пачът може да не бъде инсталиран на вашата машина в случай на наличието на антивирусна програма, която се опитва неоторизирано да достъпи паметта на кернела.
2. Миграции в iOS 11.2, macOS 10.13.2 и tvOS 11.2 – Епъл съобщиха, че проблемът засяга техните устройства, но до момента няма сигнали за засегнати потребители. Въпреки това от компанията ще предоставят защитни миграции в Сафари с цел да предпазят клиентите си.
3. Android OS – Google съобщи, че потребителите използващи операционната система с последния Януарски секюрити пач са напълно защитени. Това обаче се отнася за всички потребители на техни телефони. Всички останали следва да изчакат за системни обновления.
4. Firefox Web Browser – Защитената версия е 57.0.4 съобщиха от Мозила.
5. Google Chrome Web Browser – на 23 Януари ще бъде пуснат секюрити пач за браузъра на Гугъл. Към момента потребителите могат да позволят експерименталната опция „Изолация на сайт“, която предоставя някаква защита от уеб базирани експлоатации на проблема.
6. Linux дистрибуции – Линукс пуснаха пач версии, които защитават от проблема - 4.14.11, 4.9.74, 4.4.109, 3.16.52, 3.18.91, 3.2.97. Те могат да бъдат свалени от kernel.org
7. VMWare и Citrix – виртуализиращ софтуер – предоставен е лист с продукти на компаниите, който ще бъде защитен чрез защитни обновления.

**Материал 2**

**Новият закон за кибер сигурността в Китай**

**Линк** [**https://www.economist.com/news/business/21722873-its-rules-are-broad-ambiguous-and-bothersome-international-firms-chinas-new-cyber-security**](https://www.economist.com/news/business/21722873-its-rules-are-broad-ambiguous-and-bothersome-international-firms-chinas-new-cyber-security)

**Резюме:**

Новият закон за кибер сигурността в Китай е широкообхватен и разводнен, смятат специалисти. Много от международните компании са объркани и притеснени от него. Законът таргетира две главни цели за китайското правителство, които имат нужда от реформа. Първата е кибер сигурността. Компаниите и индустриите, които са критични за страната, трябва да бъдат сигурни в техните продукти и да предоставят гаранции за техните системи – очакванията са те да бъдат сигурни и контролирани. Изисква се също така те да оперират с информация локално, като я пазят на територията на страната с цел тя да може да бъде одитирана периодично.

Другата страна на закона засяга частната собственост. Много фирми в страната са манипулирали данни за и на своите потребители и това е всеизвестно. От компаниите опериращи в страната се изисква да пазят данните за местни граждани локално и да изискват разрешение преди изпращането им извън страната.

Колкото и разбираеми да изглеждат тези проблеми и техните решения законът е стряскащ и прекалено задължаващ. Много от компаниите се страхуват от него, като смятат, че той представлява Троянски кон целящ да засили политиката на Китай по крадене на ноу хау и чуждестранни иновации.

**Материал 3**

**Malware сервира порно реклами в приложения за деца**

**Линк:** <https://www.infosecurity-magazine.com/news/malware-serves-up-porn-ads-in-kids/> **Резюме:**

Зловреден софтуер направен с цел да атакува мобилни приложения, включително игри за деца, бе открит в GOOGLE Play. Той е бил разпространен и свален между 3 и 7 милиона пъти.

Софтуерът има за цел да промотира порнографско съдържание. Това обаче не е всичко. Той също така се опитва да заблуди потребителите да инсталират несъществуващи или зловредни защитни програми с цел да се регистрират и да заплащат такси. Това става чрез визуализирането на реклами целящи да объркат потребителя като му внушат, че устройството му е заразено с вируси. След това потребителят е пренасочван към страница на измислено приложение лъжливо целящо да защитава потребителското устройство. Потребителите са подмамени да плащат за премиум услуги като програмата ги лъже, че вземат участие в томбола за Iphone.

**Материал 4**

**МaMi malware отвлича DNS настройки**

**Линк:** <http://www.securityweek.com/mami-mac-malware-hijacks-dns-settings>

**Резюме:**

Изследователя Патрик Уардъл описва нов малуер целящ да отвлича DNS настройки на устройства работещи на macOS. Към момента този зловреден код може да бъде открит само на устройства на фирмата Ikarus.

Отвлечените устройства сменят автоматично своя DNS на 82.163.143.135 и 82.163.143.137. Все още не е ясно как този зловреден код се разпространява. Предположенията са, че е бил доставен чрез комуникация по имейл, фалшиви поп-ъп реклами на уебсайтове или атаки от тип социално инженерство. За сега софтуерът не изпълнява никакви други функции, но от ESET предполагат, че пълното му разгръщане изисква някакъв тип външно потребителско действие. От компанията обаче споделят, че макар за сега софтуерът на практика да е безвреден, той би могъл да се използва за атаки от тип man-in-the-middle’ing. Софтуерът не е разработен да заразява Windows устройства.

**Материал 5**

**Проблем в Мак позволява на потребителите да се автентикират в AppStore настройки с всякаква парола**

**Линк:** [**https://www.cnet.com/news/apple-mac-high-sierra-app-store-preferences-login-password-flaw-bug/**](https://www.cnet.com/news/apple-mac-high-sierra-app-store-preferences-login-password-flaw-bug/)

**Резюме:**

Проблемът не е считан за огромен риск за сигурността, но въпреки това е вторият такъв проблем намерен в операционната система за последната година. През ноември 2017 потребители откриха, че всеки може да се автентикира в устройството използвайки потребителско име root и без никаква парола. Епъл не отвърна веднага на молбата за коментар по отношение на проблема. Въпреки това устройствата със сигурност не остават защитени, защото освен факта, че можете да се автентикирате по този начин вие получавате администраторски права.

Колкото до новооткрития проблем – за да бъде експлоатиран той следва потребителя да бъде логнат с администраторски права. Само тогава той би могъл да променя настройките на машината без парола – дори тези които принадлежат на конкретен потребител. Проблемът засяга последната версия на операционната система 10.13.2.

Проблемът не е изключително опасен за потребителите поради факта, че за да се възползва от него атакуващия следва да изчака неподозиращ Мак потребител да остави машината си без надзор и автентикирана. След това той трябва да отвори приложението App Stora и менюто настройки и да въведе каквато и да е клавишна комбинация за да поеме контрол над менюто. Накрая атакуващият може да направи нещо неприятно като например да деактивира автоматичните обновления на машината на потребителя.