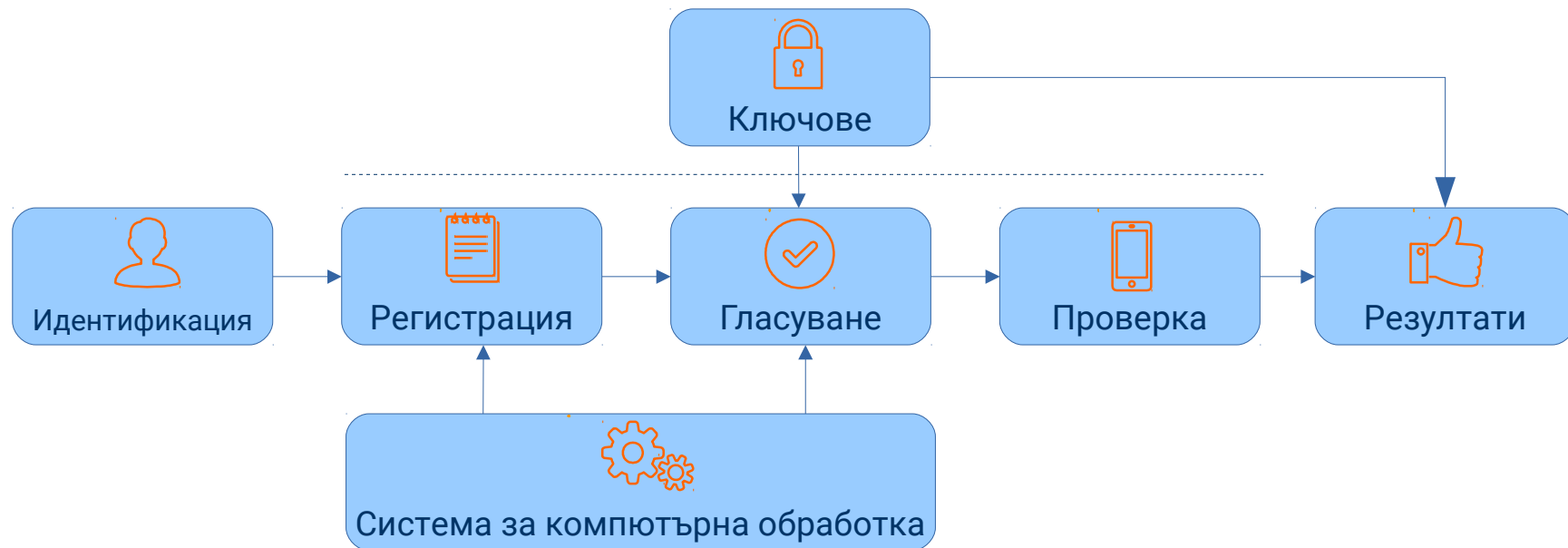


B.A.E.S

Технологични аспекти на дистанционното електронно гласуване. Анализ на рисковете и заплахите.

Александър Станев, alex@stanev.org
Илия Горанов, ilia.goranov@gmail.com

VI НКИС, 4-5 декември, София



B.A.E.S

Фази на ДЕГ

подготовка

гласуване

обработка

результати

- Регистри на партии/коалиции от партии (ЦИК/РИК/ОИК)
- Регистри на кандидати (ЦИК/РИК/ОИК)
- Гласоподаватели по секции и провеждани избори (ГРАО)
- Данните трябва да се зареждат от системата за компютърна обработка и респективните регистри
- Защита на личните данни и спазване на изискванията на GDPR

- Регистрацията трябва да става след надеждна идентификация в съответствие с ЕС Регламент ЕС 910/2014
- Възможността за регистрация трябва да бъде обвързана с критериите за допустимост до съответния вид избор
- Към момента разполагаме с електронен подпис и наличните в него идентификационни данни за гражданина
- Проблеми с идентификационни данни от доставчици на квалифицирани удостоверителни услуги извън България

- Идентификация → Вид избор → Електронна бюлетина
- Криптиране на електронната бюлетина
- Подписване с електронен подпис на криптираната електронна бюлетина
- Как може да получим недействителни гласове при ДЕГ?

- Отчетен ли е правилно гласът?
- Дали устройството, през което сме гласували не е компрометирано?
- Проверката трябва да става по алтернативен канал
- Какво прави гласоподавателят, ако проверката е негативна?

- Верификация на електронните подписи върху криптираните бюлетини
- Идентифициране на последните подадени от всеки гласоподавател електронни криптирани бюлетини
- Отстраняване на гласувалите в СИК на хартия или машинно*
- Електронно подписан експорт само на криптираните бюлетини

- Верификация и зареждане на криптираните бюлетини
- Логически проверки върху декриптираните данни
- Сумиране по видове избори и по секции
- Връщане на информацията към системата за компютърна обработка за сумиране и окончателен резултат

§ 145. (1) При произвеждане на избори след 1 януари 2018 г. се създава възможност за експериментално дистанционно електронно гласуване. Експериментално дистанционно електронно гласуване се провежда на три последователно произведени избори, **включително частични избори.**

- Кмет на кметство Звиница, община Кърджали, област Кърджали
498 избиратели, гласували 340
- Кмет на кметство Средище, община Кайнарджа, област Силистра
1117 избиратели, гласували 674
- Кмет на кметство Брест, община Гулянци, област Плевен
1912 избиратели, гласували 1152
- Кмет на кметство Кочово, община Велики Преслав, област Шумен
571 избиратели, гласували 333
- Кмет на кметство Енчец, община Кърджали, област Кърджали
311 избиратели, гласували 189

* Предложения на ЦИК до Президента за насрочване на частични избори.
Данните за избирателите и гласувалите са от тур I, МИ2015

§ 145. (8) Всеки избирател, гласувал **експериментално** дистанционно, може да гласува на същите избори с хартиена бюлетина или машинно.

- След експеримента, веднъж регистрирани за ДЕГ, само по ДЕГ
- Гласуване в контролирана среда срещу неконтролирана
- 48 часа за компютърна обработка:

Конвенционално + Машинно + ДЕГ = Мисията невъзможна!

§ 145. (14) ... Системата трябва да:

- 9. позволява използване от избирателя на всички операционни системи
- 12. бъде сертифицирана по най-висок ISO стандарт за качество и устойчивост на използвания софтуер и хардуер
- 26. предоставя възможност на избирателя да сигнализира по неявен начин за посегателство срещу избирателните му права и за неотчитане на гласа му в тези случаи

§ 145. (24) Гласуването чрез приложението по ал. 20 включва следните етапи:

- 5. избирателят може трикратно да промени избора си преди потвърждаването му

Total Bandwidth

Last Week

2 TB

Cached Bandwidth

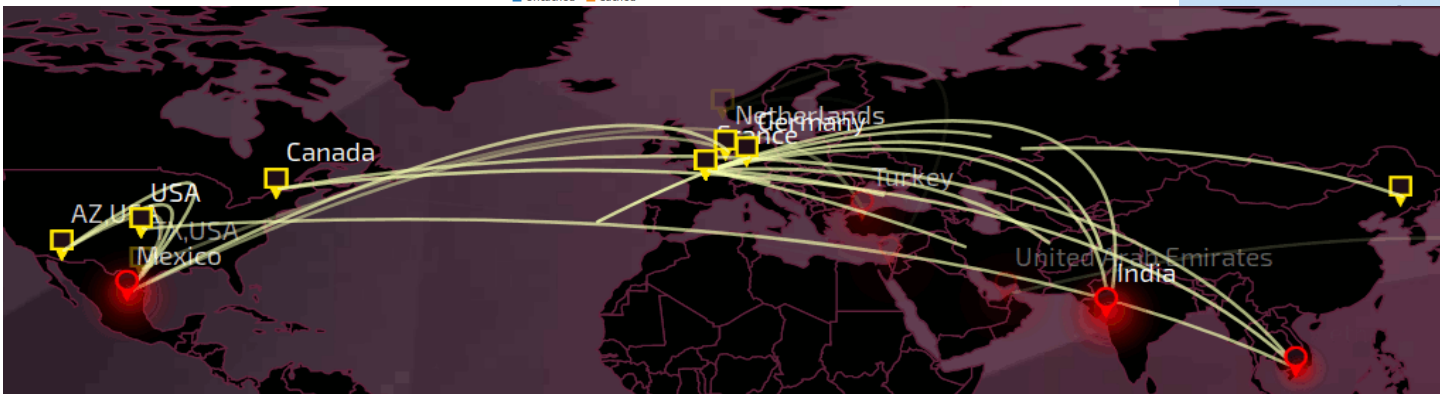
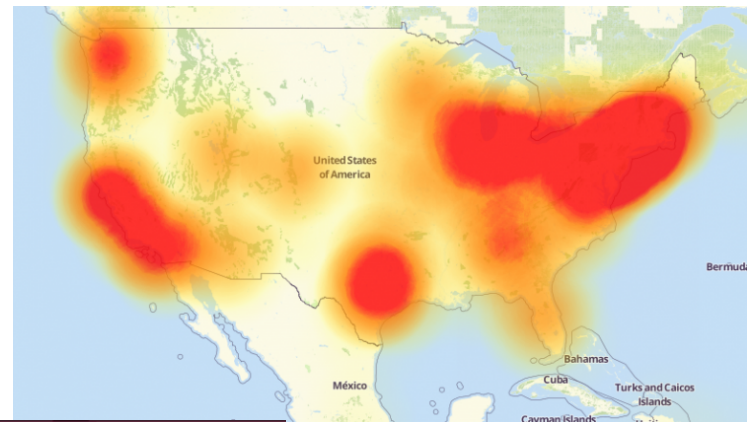
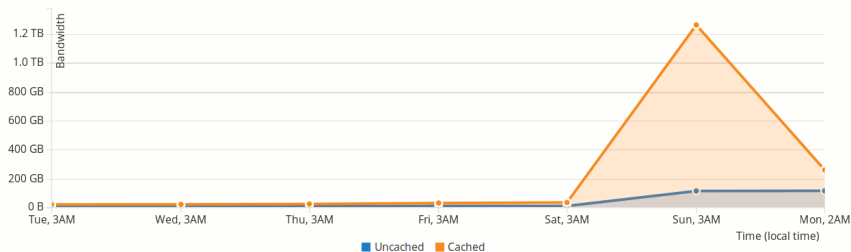
Last Week

2 TB

Uncached Bandwidth

Last Week

276 GB



1.8 million Chicago voter records exposed online

by [Selena Larson](#) @selenalarson

🕒 August 17, 2017: 8:36 PM ET



Data on 198M voters exposed by GOP contractor

BY JOE UCHILL - 06/19/17 09:00 AM EDT

12,472 SHARES



SHARE



TWEET



PLUS ONE



Republic of the Philippines

COMMISSION ON ELECTIONS

...protecting the sanctity of the ballot since 1940

Voter Registration

Cybersecurity

Elections ▾

Overseas Voting ▾

[Home](#) > [Cybersecurity](#)

What Happened

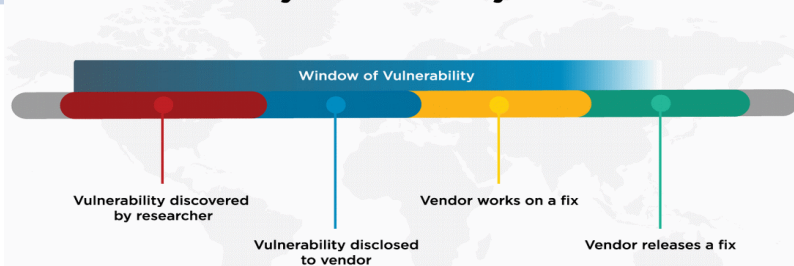
Posted: 21 June 2016

On 27 March 2016, the Commission on Elections became aware of a cybersecurity incident that resulted in the defacement of the COMELEC Public Information website, and the theft of what is being claimed to be the entire COMELEC database. The COMELEC also learned that the data claimed to have been stolen was subsequently uploaded to the internet.

The RNC Files:
Inside the Largest
US Voter Data Leak

Updated on November 28, 2017 by Dan O'Sullivan
Filed under: [Data Breaches](#)

Zero Day Vulnerability Timeline



ars TECHNICA



BIZ & IT

TECH

SCIENCE

POLICY

CARS

GAMING & CULTURE

FORUMS

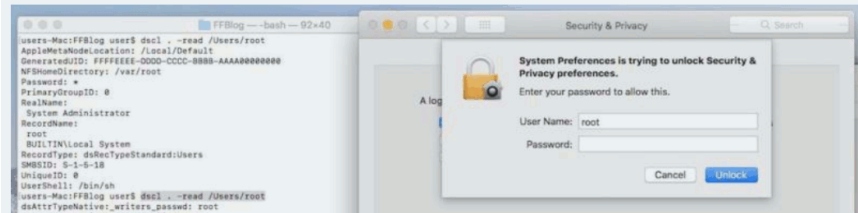


MOTHER OF ALL BUGS —

macOS bug lets you log in as admin with no password required

Here's how to protect yourself until Apple patches bafflingly bad bug.

DAN GOODIN - 11/29/2017, 1:05 AM



ars TECHNICA



BIZ & IT

TECH

SCIENCE

POLICY

CARS

GAMING & CULTURE

FORUMS



BIZ & IT —

0-days hitting Fedora and Ubuntu open desktops to a world of hurt

If your desktop runs a mainstream release of Linux, chances are you're vulnerable.

DAN GOODIN - 12/15/2016, 11:36 PM

The Hacker News
Security in a serious way

Immediately Patch Windows 0-Day Flaw That's Being Used to Spread Spyware

Wednesday, September 13, 2017 Mohit Kumar



Tweet



Share



Share

51



Share

1.72k

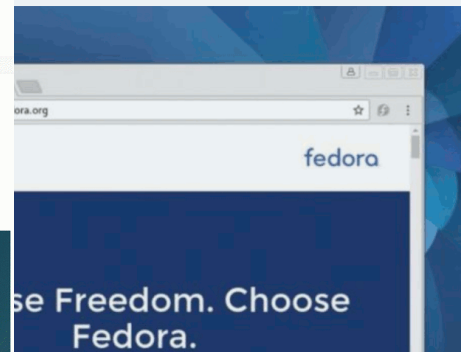
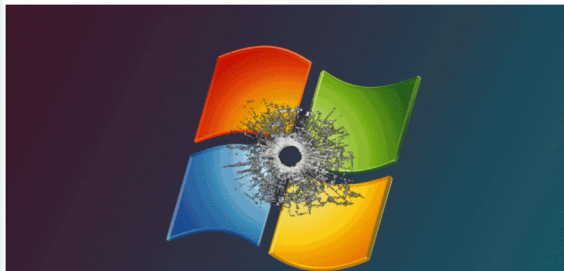


Share

3.71k



Share



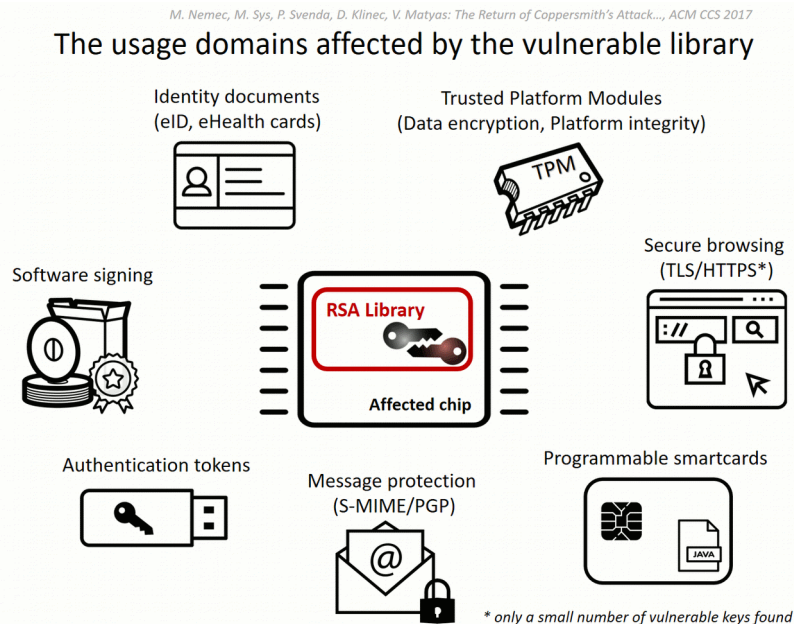
В.А.Е.С Заплахи – „сигурни“ компоненти - ROCA

- Уязвимост срещу криптографска библиотека
- Възстановяване на частния ключ от публичния – ресурси
- Смарткарти, TPM ...

Резултати

- Естония – 760 000 eID спрени*
- Словакия – 300 000 eID спрени
- Испания – всички издадени след април 2015, 59M+

* Проведени местни избори на 15 октомври 2017



- Наличие на устройства за сигурна идентификация и електронно подписване при гласоподавателите
- Включване на трайно живеещи извън страната граждани
- Контролиран вот – платен, корпоративен, семеен...
- Доверие в процеса
- Организация на процесите и обединение на информацията от трите начина на гласуване

B.A.E.S

Благодаря за вниманието!

**Технологични аспекти на
дистанционното електронно
гласуване
Анализ на рисковете и заплахите**

Александър Станев, alex@stanev.org
Илия Горанов, ilia.goranov@gmail.com