

# DORKBOT: HUNTING ZOMBIES IN LATIN AMERICA

*Pablo Ramos*

ESET Latin America, Argentina

Email [pablo.ramos@eset.com](mailto:pablo.ramos@eset.com)

## ABSTRACT

Win32/Dorkbot appeared at the beginning of 2011, and in just a couple of months the volume of Dorkbot detections increased until it became the malware with the most impact in Latin America over the whole year. This threat uses removable media and social networks as its means of spreading and achieved the highest position in threat ranking statistics in only three months. Ngrbot (as its author prefers to call it) or Win32/Dorkbot (as the AV industry prefers) stands out as the favourite crimepack for Latin America's cybercriminals and it is widely disseminated through a wide variety of media and vectors.

Lots of small botnets have been detected and are being used for theft of information such as personal data and home banking credentials from compromised computers. Spreading through LNK files via removable media, customized messages through social networks like *Facebook*, and using local news or compromised web pages, systems are being converted into bots controlled through the IRC protocol.

In this paper the main capabilities and features of Win32/Dorkbot are introduced, and we show its evolution into different versions, starting with AUTORUN spreading, and moving on to the use of LNK files and information-stealing techniques. Win32/Dorkbot.B is the most widely spread variant of this worm, its constructor having been leaked and made available on the web. We tracked down one of the active botnets in the region and reviewed the main activities performed by the cybercriminals.

The investigation came up with thousands of bot computers reporting to the botmaster, who used several servers and vulnerable web pages for the implementation of phishing attacks and propagation of threats.

Social media messages have been used to spread copies of this malware through *Facebook* and *Windows Live Messenger*. Some of the topics used for spreading have included presidents, celebrities and accidents all over the continent and the rest of the world. Also, email accounts are being stolen/hijacked by this malware.

We also comment on why and in what ways Win32/Dorkbot's activity in Latin America differs from the rest of the world, including trends that involve Internet usage, social media and user education. These combinations are a direct cause of the massive infection rates detected in the region. The main features,

including botnet control, bot commands and protocols are described in this paper.

## INTRODUCTION

As part of one of *ESET's* research teams operating out of a laboratory in Latin America, we are particularly focused on trends and threats used by cybercriminals over that region. With this in mind, we track all the actions and new attacks that might differ from those seen in other parts of the world. Based on regional statistics and detection rates we have been working on the analysis of Win32/Dorkbot, a malware family that uses both known and novel infection techniques with the goal of infecting unprotected systems and turning them into bots.

This malware became the most detected threat for Latin America in 2011, and yet during the first months of 2012 it still continued to feature in the top 10 most detected threats for all the countries in the region. As we have seen on other occasions, threats can target a certain country, region or language as a main objective. In this particular case Dorkbot became one of the favourite crimepacks for cybercriminals in Latin America and its particular characteristics are the cause of its being so widespread.

In this paper, we consider the differences that caused this worm to become the most detected threat. We will analyse and review the techniques used for system infection, spreading and social engineering. Dorkbot is technically innovative even though it uses known attack vectors such as the hooking techniques used by Zeus and SpyEye in order to steal user information, and maintain a huge number of bots by means of the IRC protocol.

The research will also include the analysis of an active botnet that has been stealing users' information using fake email campaigns and social engineering techniques for spreading through social networks. With more than 80,000 affected users in one single botnet, Win32/Dorkbot stands out as the most important threat to Latin American users.



Figure 1: Win32/Dorkbot detection rates.

## REGIONALIZATION

One of the most remarkable parts of this investigation is to differentiate between the use of Dorkbot in different regions around the world. Tracking Dorkbot detection rates based on our *ESET Live Grid* system allows us to clarify the differences between countries and continents. Such a clear display of the detection rates is useful to have when a particular group of people is specifically targeted. As the months went by after its initial appearance, the detection rates for Win32/Dorkbot showed some significant changes. As can be seen in Figure 1, the number of detections for this threat reached its highest peak in October 2011.

Nevertheless, the number of detections we saw during 2011 indicates that there may be millions of users affected by this threat who are not even aware that they are at risk, since once a computer is infected with this malware all connections to anti-virus domains are blocked. Statistics and infection rates show that different variants of Win32/Dorkbot have been affecting users across the world, stealing their private and confidential information.

When this information was quantified and the origin of the detections tracked down, it was very easy to conclude that the Latin American region was the most affected. In Figure 2 it is possible to see how Dorkbot detections are mostly concentrated in Latin America.

One of the main reasons for the concentration of infections in Latin America is the lack of education in security topics and the widespread lack of recognition that threats can use social networks for spreading.

Dorkbot can be found on one out of every ten computers in Latin America. Such a detection rate could only mean that millions of computers are still infected and working under the radar. Once a system has been compromised, Dorkbot blocks all the connections to AV companies' servers and OS updates, so it

is likely that all the infected computers where the user's AV vendor does not detect the variant will no longer receive any kind of update.

According to *ESET Live Grid* information, 60% of the reports are from Latin America, where the detections are three times greater than in Europe. In other words, the propagation of this bot has been clearly focused in this region:

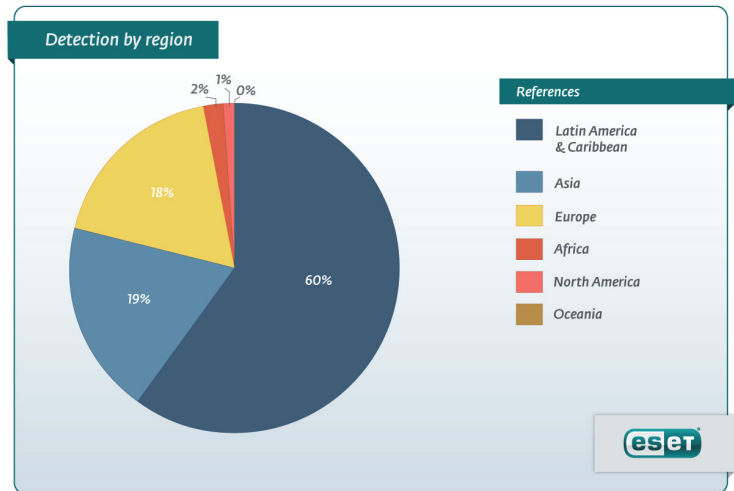


Figure 3: Win32/Dorkbot detections by region.

A deeper look into the statistics for each country shows that Mexico is the most affected country, with more detections even than bigger countries such as Russia or China. The total number of detections in Mexico alone is greater than positions two and three combined (Peru and Russia: see Figure 4). Furthermore, among the 25 countries most affected by Dorkbot we can find 13 countries from Latin America.

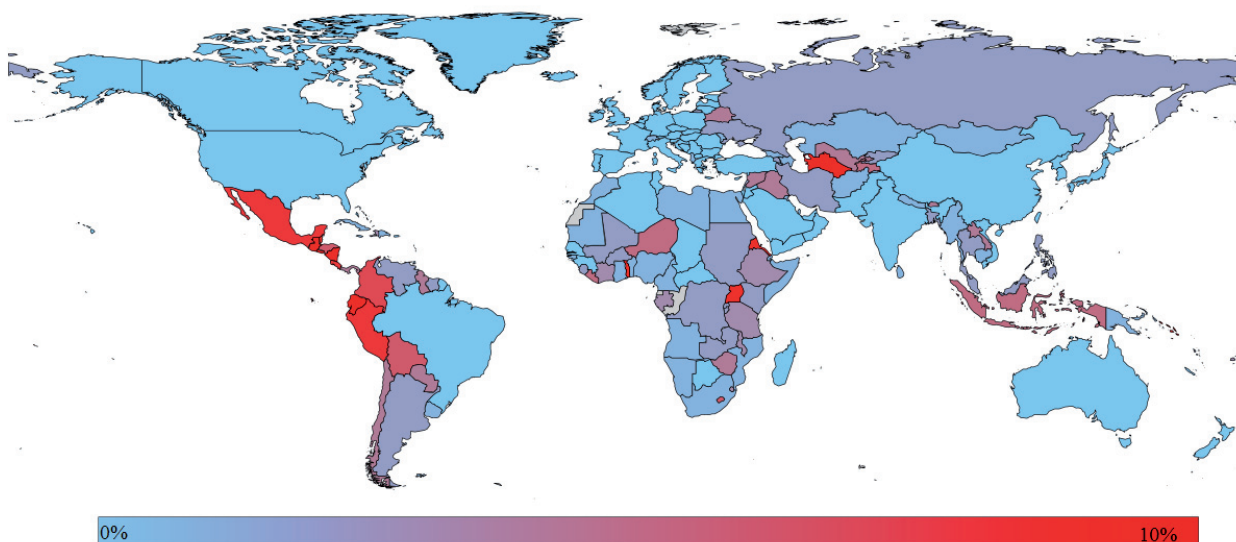


Figure 2: Dorkbot detections for 2011.

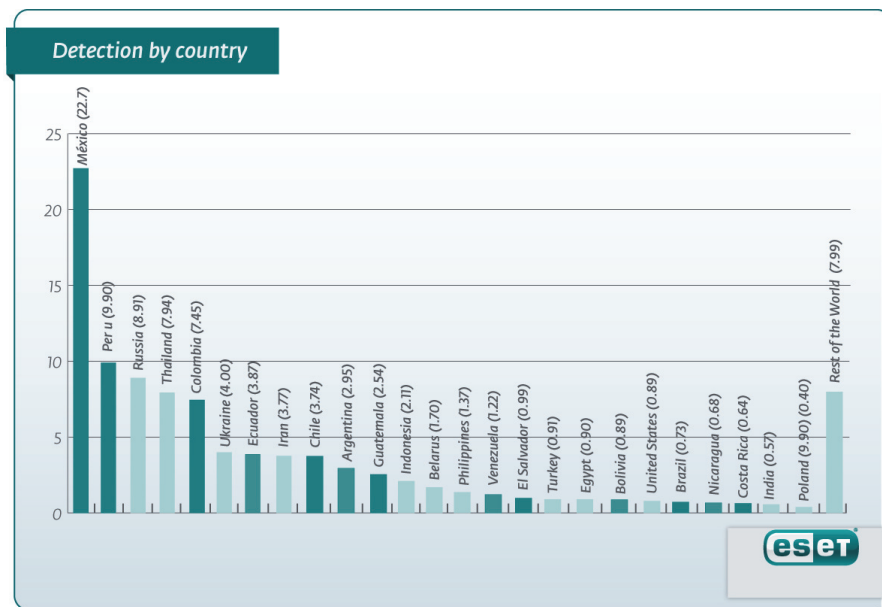


Figure 4: Top 25 countries affected by Dorkbot.

The difference between Latin America and the rest of the world is remarkable. The huge quantity of small botnets that have been detected during the last year points to an outstanding difference between Dorkbot and the common banking trojans.

Local pharming attack techniques are very frequently used by simpler threats like Win32/Qhost or other kinds of botnets such as Volk. Instead of this approach, Dorkbot uses hooks to block certain DNS servers and to redirect the user's web traffic to phishing servers. Users will not notice any strange behaviour in their systems and in the absence of adequate protection systems or security education regarding this kind of threat, they are completely vulnerable. In addition, no user privileges are required where the affected computer runs newer operating systems such as *Windows 7*.

## CONQUERING LATIN AMERICA

Since the very beginning of the investigation, we focused on Dorkbot propagation through the region. We aimed to explain what caused this threat to be so widely distributed and how it became the number one threat in Latin America. During the

research we considered all the possible hypotheses as to what factors took this IRC-controlled bot to the top position in less than three months, and have been very much engaged in actively monitoring its activities in the second part of 2011.

Looking at the different variants we were able to discover that the LNK spread technique was highly effective, and Dorkbot was able to infect millions of removable devices. At the same time it tricked the users into failing to notice that their systems were infected. The two most highly propagated variants are Win32/Dorkbot.B and Win32/Dorkbot.D.

The use of USB devices is very common, especially among students and within companies; these two groups are the most affected by this worm according to our observations so far. Taking into consideration that Win32/Dorkbot.D is the detection

signature for the LNK spread through removable media, this appears to explain its effectiveness compared to the other variants. It also has to be taken into consideration that even other kinds of threat could have tried to duplicate this method as it became highly effective.

In Win32/Dorkbot.A, the spreading method through removable media combined the Autorun.inf file and LNK exploit. Win32/Dorkbot.B stopped using the Autorun.inf method and remained with the LNK spreading technique; it works in *Windows 7*, *Windows Server 2008*, *Windows Vista*, *Windows Server 2003* and *Windows XP* and it's highly effective.

With this volume of attacks, thousands and thousands of different campaigns spread through all the different countries. We have been working to track the cybercriminal techniques and trends used to deceive users and convert their systems into bots.

Campaigns detected in Latin America involve the use of fake emails, social networks and USB devices. The range of topics used as social engineering hooks is as diverse as imagination

Signature	Date	Main functionalities	Description
Win32/Dorkbot.A	4 April 2011	Autorun.inf, LNK spread	First Dorkbot variant, not so widely spread.
Win32/Dorkbot.B	16 May 2011	Includes social network spreading ( <i>Facebook</i> , <i>Twitter</i> , etc.)	Most used malware variant. Includes different versions and capabilities.
Win32/Dorkbot.C	6 June 2011	Implements MS04-011 exploit for spreading	
Win32/Dorkbot.D	18 July 2011	LNK spread	Really effective technique, uses shortcuts to execute the malware deceiving the user.

Table 1: Dorkbot variants.

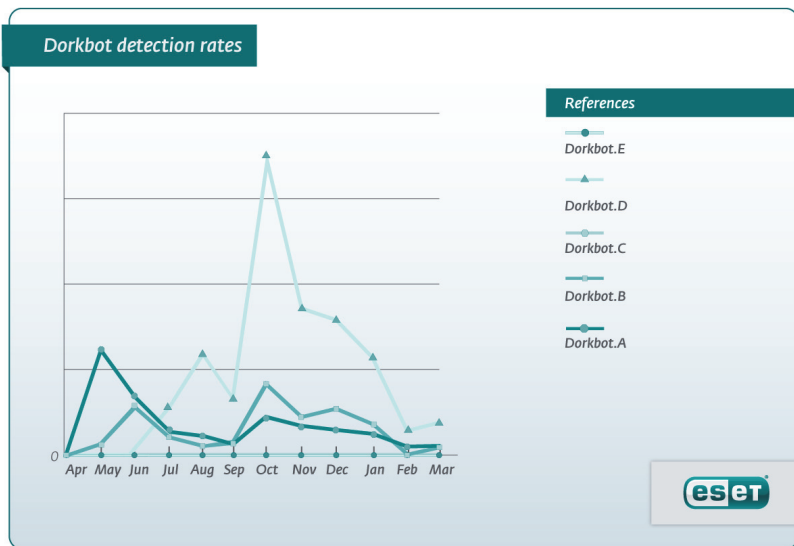


Figure 5: Dorkbot variant detection rates in Latin America.



Figure 6: Fake email campaign spreading Dorkbot.

allows: from love letters to free gifts or simply using fake news about famous people like Jennifer Lopez or Lionel Messi. The image shown in Figure 6 belongs to one of the campaigns detected on Valentine’s Day.

In Figure 6 we can see an email from an airline company pretending to offer potential victims free trips to Punta Cana.

All those people who were fooled by this email and tried to claim their prize were infected by Dorkbot.

Using social engineering techniques and stolen email accounts, this kind of campaign can infect thousands of users. But the idea of this paper is not to present how social engineering might help cybercriminals to propagate a new Dorkbot bot. We will now explain how a botnet can grow, based on a real case that has been spreading all over the region, using all the details we have been able to collect in the course of detecting and tracking the spread of the malware.

### HUNTING ZOMBIES IN LATIN AMERICA

As Dorkbot detection has spread throughout all the countries in the region, we have been monitoring huge numbers of small botnets (and a few that are not so small). Every one of these campaigns has been customized to fit the targeted country. The following analysis deals with an active botnet in Peru that has been targeting users in order to obtain their banking credentials and private information (email addresses and social network account data).

Our Dorkbot analysis made it possible for us to capture the basic information from the samples received in the laboratory. With this handy information, every Dorkbot sample we received could be automatically analysed in order to retrieve the C&C and phishing sites’ IP addresses. Despite all Dorkbot’s capabilities it is mainly used for phishing attacks and stealing credentials, so most of the affected users are unlikely to realize that their computers are infected.

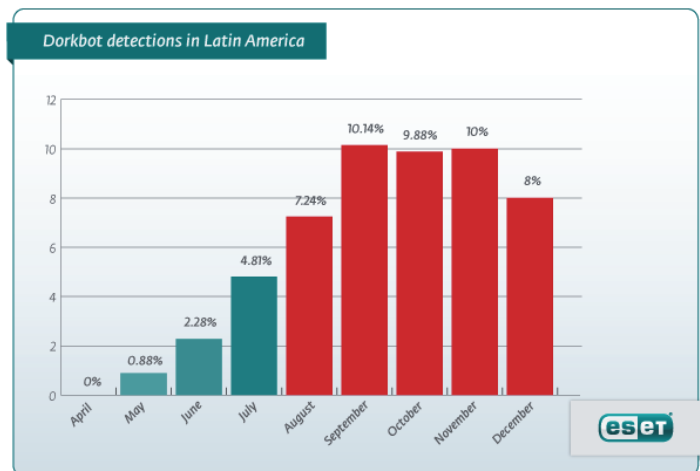


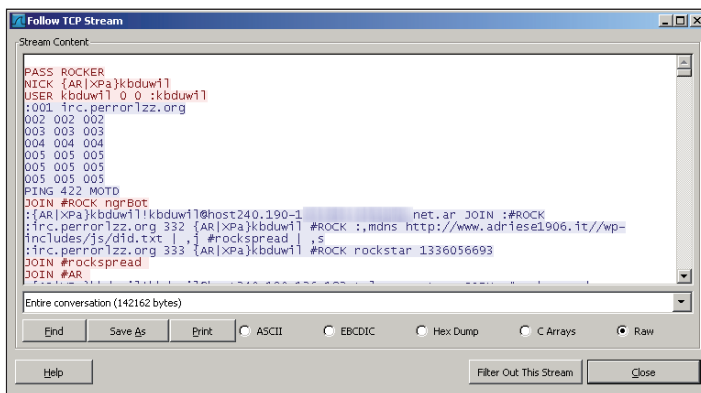
Figure 7: Dorkbot detection rates in Latin America.

As we have been talking about Dorkbot spreading in Latin America, we will now focus on botnet tracking and how this might impact on user privacy and data leakage. In the following section we will try to explain how one Dorkbot botnet can

deploy more than 80 different bots in less than six months and how the cybercriminal tried to stay under the radar, countering the blocking of his phishing campaigns as the servers where the fake bank web pages hosted were blocked or shutdown every time they were discovered. Compromised websites were used by the attacker to store new malware updates and the list of blocking sites where the phishing sites were hosted. Having all the botnet administration data kept in different locations made it harder to track it down and close the malicious websites.

### Botnet tracking

The tracking of this particular case began by publicizing a fake offer of a free mobile phone, ostensibly from a communications company well known in Peru and Chile. All the deceived users who were fooled by the promise of receiving a brand new phone and whose systems were not adequately protected became part of the botnet controlled by the cybercriminal.



```

Stream Content
PASS ROCKER
NICK {AR|XPa|kbbduw1}
USER kbbduw1 0 0 :kbbduw1
:001 irc.pernor1zz.org
002 002 002
003 003 003
004 004 004
005 005 005
005 005 005
005 005 005
PING 422 MOTD
JOIN #ROCK ngrBOT
: {AR|XPa|kbbduw1|kbbduw1}@host240.190-1 net.ar JOIN :#ROCK
:irc.pernor1zz.org 332 {AR|XPa|kbbduw1} #ROCK :.mdns http://www.adriese1906.it/wp-
includes/js/did.txt | #rockspread | ,s
:irc.pernor1zz.org 333 {AR|XPa|kbbduw1} #ROCK rockstar 1336056693
JOIN #rockspread
JOIN #AR
  
```

Figure 8: Bot connection information.

Since the very beginning of the research we performed passive monitoring in order to analyse the social engineering techniques used and to try to quantify the size of the botnet. At the very beginning there were more than 2,800 active bots used to steal information such as OS version, user privileges, email accounts, social network information and banking credentials.

As time went by the size increased to 6,000 bots and then the volume of infected computers eventually increased to more than 80,000 unique remote connections into the IRC channel. With such a huge number of affected systems the likelihood that the cybercriminal will obtain valid banking credentials is much higher.

Nevertheless, not all the affected users were from Chile or Peru. Connections from more than 50 different countries were tracked, from which we can conclude that the scope of this Latin American botnet has widened to infect computers in all the remaining continents. There are many explanations for this, but the most important detail is that 44% of the connections came from Chile. This is quite important if we take into consideration the fact that almost all the targeted banks were from that country. Four out of every ten users that were victims of this attack were also from Chile. The other countries most affected were Peru and Argentina, with 15% and 11% of the bots respectively.

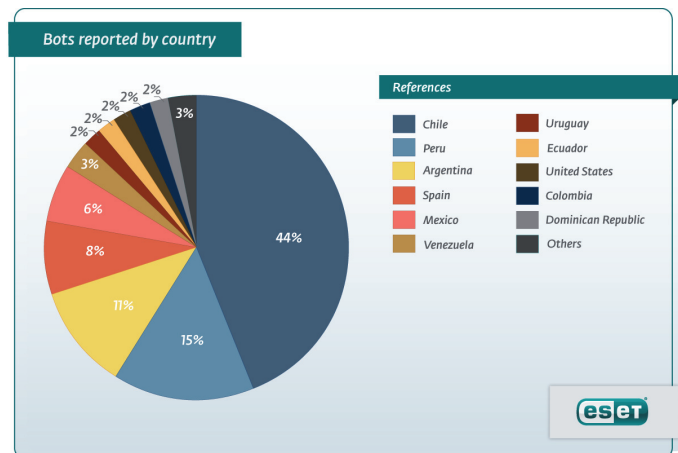


Figure 9: Bots per country.

In five months the information we collected revealed very useful details about how the botmaster interacts with infected systems. This is very important because when we talk about security we have to take into consideration all the possible vectors that cybercriminals can use to deceive the users or infect their systems.

We can conclude that it is really important for us to continue working on providing better security education as well as developing new and improved technologies. If we based our study and product development on what customers are using and how they are behaving we would understand them better and then be able to give them what they need to be safe. The problem with this is that if we do not work on providing security education, they will never know how to protect themselves.

### Affected systems and user privileges

From that total of more than 80,000 connections we have been able to identify which operating systems the victim used and the privilege level of the users infected. This information is provided by default as part of the bot payload. As we will describe later in this paper, every time a machine joins the network it provides the attacker with information about the country, OS, user privileges and IP address.

Before the bot joins the IRC channel it will request geolocation information from *WIPmania* (<http://www.wipmania.com>).

Analysing the information gives a very clear indication of the state of the affected system. As we expected, *Windows XP* was the OS most affected, with *Windows 7* in second place. We also got reports of *Windows Server 2003* (169 bot reports) and *Windows Server 2008* (94 bot reports) compromises: this suggests that many corporations might have their infrastructure compromised by this threat.

User privilege levels in older operating systems like *Windows XP* or *Windows Server 2003* differ from those in more recent *Windows* versions. In Table 2 user privilege level is shown: 55% of the victims had administrator accounts on the infected

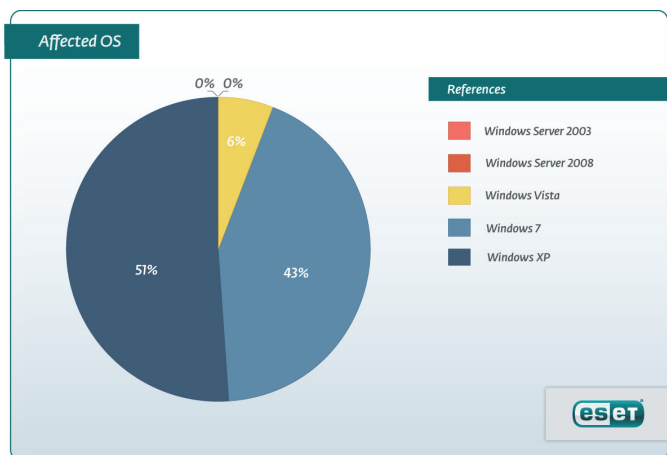


Figure 10: Reported bots per OS.

Operating System	Admin users	Non-admin users	Total
Windows Server 2003	147 (86%)	22 (%14%)	169
Windows Server 2008	27 (28%)	67 (%72)	94
Windows Vista	869 (17,6%)	4051 (82,4%)	4920
Windows 7	6335 (18,1%)	28673 (81,9%)	35008
Windows XP	37509 (90,6%)	3863 (9,4%)	41372
<b>Total</b>	<b>44887 (55,03%)</b>	<b>36676 (44,97%)</b>	<b>81563</b>

Table 2: User privilege levels and OS version.

computers. This decreases when *Windows 7*, *Windows Vista* or even *Windows Server 2008* are analysed.

If we want to minimize this kind of attack we do have to take into consideration the importance of awareness about risk and threats for end-users. As mentioned earlier, the most frequently detected variant is Win32/Dorkbot.D. One of the most effective methods by which Dorkbot spreads is via removable media. This technique is highly effective and works on all the *Microsoft* operating systems.

### Bot and phishing updates

When the bot connects to its IRC channel it will download new malware updates and lists of phishing sites. This action is quite interesting as it lets us know that every time a phishing site was reported and taken down, the attacker updated the phishing information in order to prevent users from noticing that their system was infected.

This botnet mainly connects to the following URLs:

- rlz1jmv.info
- jmlrz01.info
- rlz8jmv.info

The IP addresses changed as time went by and many different servers have been used to host the IRC server used for botnet control. Over the period of the investigation we detected 10 different IP addresses where the bots were communicating.

During five months of activity (from 1 January to 1 June) the botmaster sent 88 updates for this malware. Figure 11 shows how these files are stored under %appdata% and renamed after every update. This method is being retained in order to keep track of the latest bot and avoid losing track of any infected computer.

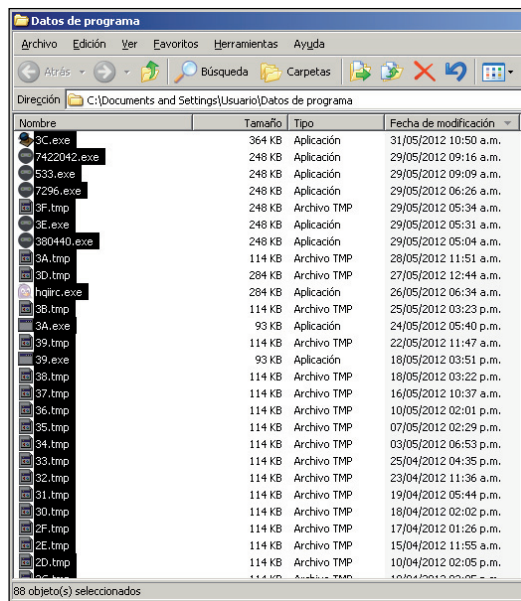


Figure 11: Bot updates on an infected machine.

The same behaviour was observed in relation to the phishing site information as the botnet size increased; 24 different URLs were being redirected to nine fake servers in order to steal banking credentials from Peruvian and Chilean users. In this way all the URLs were updated periodically and the attacker needed to exploit vulnerable websites in order to spread the updates. For this reason five vulnerable websites were used as locations from which bots were able to download the newest versions of the redirect lists and new variants of the malware.

### Data stealing

Dorkbot does not use local pharming attacks, unlike most banking trojans in Latin America. Instead, this threat uses hooks in order to block connections to servers used by most AV companies, to capture login credentials, or to redirect users to the phishing servers. This is one of the reasons it has been so widely adopted by cybercriminals in the region. It can also be used to steal email accounts for POP3 connections. During the botnet analysis we were able to catch the botmaster at the moment he executed the command to recover all the stolen credentials.

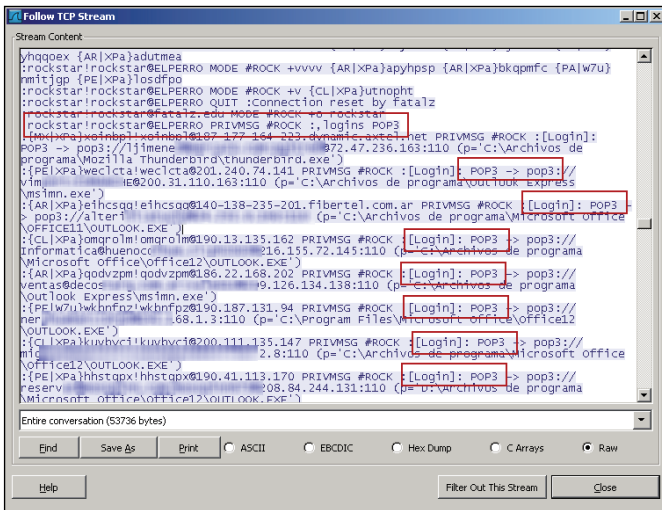


Figure 12: POP3 stolen information.

More than 2,100 sets of email credentials were sent to the attacker just after he sent the command to retrieve this information. Out of all the stolen credentials 1,164 belong to users from Chile, 299 to users from Argentina and 246 were credentials from users in Peru. This information has been used to spread fake emails with a better chance of infecting users by localizing the attack more accurately. Stolen information is sent in the following format:

```
:{<Country>|<OS><user type>}>nickname!<nickname><ip> PRIVMSG # <IRC Channel>: [Login]:POP3 ->pop3://<email>:<password><ip>:<port> (<program>)
```

### Social engineering and Dorkbot spread

One of the latest campaigns we have detected for this botnet is directly targeting users from Chile by offering the prize of an iPhone 4 (Figure 13). When users try to download a form in order to claim their brand new phone a new variant for this malware is downloaded under the name 'Formulario-IPHONE4'.

Social engineering has always been used by attackers to deceive users and trick them into infecting their system. Dorkbot includes modules for spreading through social networks such as Facebook and Twitter and also uses Windows Live Messenger – and the botmaster has made ‘good’ use of them.

The most effective vector is now no longer Windows Live Messenger, but Facebook. Nevertheless, both methods were actively used by Dorkbot for social engineering topics that involved presidents, actors and famous soccer players like Lionel Messi. To update the messages being distributed, Dorkbot includes the command HTTP.set for social networks and MSN.set for Windows Live Messenger (Figure 14).

All the information presented demonstrates the importance and adaptability that Dorkbot offers an attacker. In order to infect a system and remain undetected this malware not only includes effective spreading techniques, but will prevent the infected system from communicating with security websites, inject malicious code into every process running in the system, remove other threats in order to keep running itself, and track



Figure 13: Fake email spreading Win32/Dorkbot.

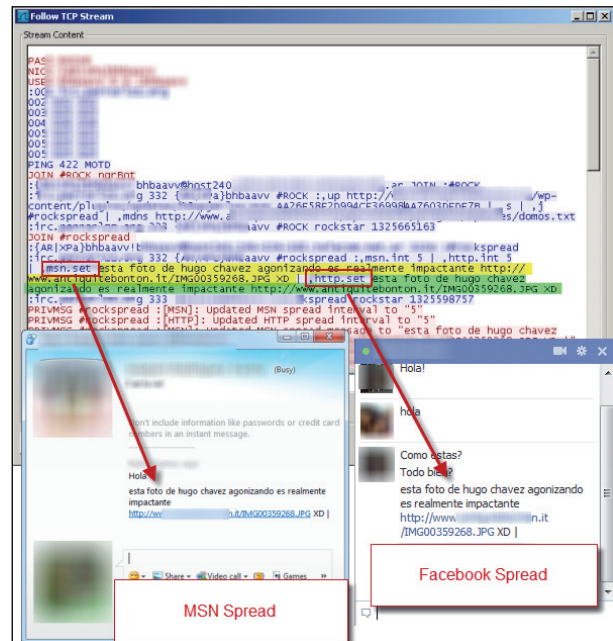


Figure 14: Dorkbot spreading through social networks.

the user’s activities. For this reason Dorkbot became the favourite malware for cybercriminals in Latin America, and was widely used in 2011.

## WIN32/DORKBOT CAPABILITIES

### Installation

The first time the malware executes, it creates a hidden file in the %appdata% directory and also creates a Windows registry key in order to start at system boot in 'HKEY\_CURRENT\_USER\Software\Microsoft\CurrentVersion\Run\filen\_ame.exe'. Both files are hidden so they cannot be found by the user.

Besides this, Dorkbot will inject itself into every running process in the system and create remote threads. For communication it creates a PIPE in order to receive commands and send the captured information.

The named PIPE looks like '\\.\pipe\pipe\_name', where pipe\_name is the very same name used for copies stored in the USB devices that are connected to the infected computer. This value is actually the RC4 key used for data encryption in the malware strings.

## API hooking

Dorkbot hooks to an API in the operating system in order to protect itself from removal, to steal user information, or for spreading through social media and USB devices. Each one of the hooks is intended to perform a specific function. This kind of behaviour has been seen in many other malicious files, and a few of these methods are quite similar to those we see used by Zeus or SpyEye.

The hook may change according to the variant. For example, in Win32/Dorkbot.A a hook exists to DeleteFileW and DeleteFileA in the kernel23.dll, but in Win32/Dorkbot.B this hook is no longer present. We will detail the most important hooks and their main role in the process of sniffing user information.

Hooks are written every time a new process is launched; the process is performed by the main thread concealed in explorer.exe. It uses WriteProcessMemory in order to hook the previous functions and to capture the information needed in order to steal user information, block access to websites or even redirect web traffic to fake servers.

## Commands and capabilities

Dorkbot includes a set of commands to enable it to perform very diverse activities; it will connect to the C&C using the IRC protocol. Every time it connects to the C&C it will send information such as:

- Country (ISO 2 characters)
- OS (XP, W7, VIS, 2K3, 2K8)
- UserType (a for admins, u for users)
- IRC nickname
- IP

A connection string example looks like this:

```
:{AR|W7a}deltmts!deltmts@xxx.xxx.xxx.xxx
```

In order to retrieve information about the country and IP address it will contact <http://api.wipimania.com> and parse the response in order to use that information. The data for the current OS is retrieved by executing the GetVersionExA function in kernel32.dll.

```
BOOL WINAPI GetVersionEx(
    __inout LPOSVERSIONINFO lpVersionInfo
)
```

The command list that Dorkbot can execute is very diverse and can be modified if the attacker owns one of multiple builders. The Ngrbot crimepack has been leaked, and this caused a direct increase in the use of this bot.

## LNK exploit

The most effective spreading technique for Dorkbot is detected as Win32/Dorkbot.D. When a USB device is connected to an infected computer all the existing files will be hidden and shortcuts are created in order to deceive users.

The LNK files created contain the string that will execute the malware and infect the system. After a USB memory stick is connected to the infected computer the target field in the LNK will contain a string like the following:

```
%windir%\system32\cmd.exe /c "start %cd%RECYCLER\
<nombre_malware>.exe &&%windir%\explorer.exe
%cd%Folder 1
```

Hook	Category	Function
MoveFileA/MoveFileW (kernel32.dll)	Malware protection	Flags that an attempt is being made to remove the malware.
GetAddrInfoW (ws2_32.dll)	Malware protection	Blocks access to AV sites.
PR_WriteFile (nspr4.dll)	Data stealing	Looks for the target site and if it matches it will send the captured information.
HttpSendRequestW/HttpSendRequestA (wininet.dll)	Data stealing	Looks for the target site and if it matches it will send the captured information.
InternetWriteFile (wininet.dll)	Data stealing	Looks for the target site and if it matches it will send the captured information.
DnsQuery_A/Dns_QueryW (dnsapi.dll)	Malware protection	Blocks access to AV sites.
Send (ws2_32.dll)	Data stealing	Used to intercept POP3 and ftp connections.
URLDownloadToFileA/URLDownloadToFileW (urlmon.dll)	File blocking	Checks for file extensions and blocks all attempts to download 'exe', 'com', 'pif' and 'scr'.

Table 3: Dorkbot hooks.



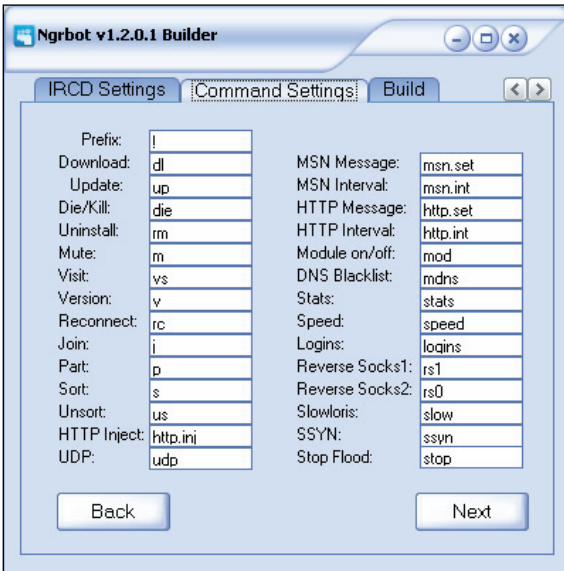


Figure 15: Dorkbot default commands.

When the user double-clicks on the shortcut he will see a new *Explorer* window with the requested folder and will not be aware that the system has been infected.

## CONCLUSION

The analysis presented in this paper shows that even with complex or less complex threats, users are vulnerable to malware: besides the technological attacks they might also be exposed to data theft due to a lack of education in information security.

The analysis and capabilities of Win32/Dorkbot and the reasons why this crimepack has been widely used in Latin America have been demonstrated. Dorkbot provides attackers with a stable and effective platform for spreading itself and for stealing information from users. The use of the malware in Latin America has been so high that the detection rates for older threats like Autorun.inf as an infection technique have decreased considerably (Figure 16).

The relationship between the LNK exploit (Win32/Dorkbot.D) and modern operating systems caused detection rates to increase well above the other most common threats we see in the region. We also have to take into consideration the fact that the Dorkbot (aka Ngrbot) crimepack is available for downloading in quite a few hacking forums so that criminals do not even have to pay for it, making it even more suitable for their purposes.

During 2011, *ESET Latin America's* Awareness Team visited more than 90 universities in 15 different countries (around 12,500 students and teachers) and about half of the students had seen an infected USB device where the folders were hidden and replaced by shortcuts (Win32/Dorkbot.D). Even so, they did not know what that meant: their removable devices were infected with a variant of Win32/Dorkbot. Half of the users in universities have seen bot-compromised computers and used them to access their social networks, email accounts and personal information.

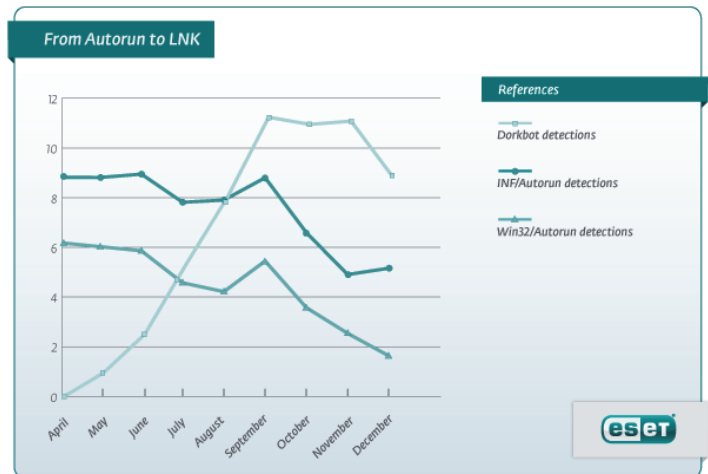


Figure 16: Dorkbot vs. Autorun.inf.

Dorkbot is part of a crimepack specially designed to target users, and the present study shows how it can affect thousands and thousands of them. We must face up to the challenge of explaining how threats can affect user privacy and the importance of awareness when we talk about information security. We need to teach users what we do and why, and how we are protecting them against this kind of threat. In the industry we understand the importance of updates and concern about the content we see from our daily activities, but we need to talk to end-users in their own language.