September 2016
Feature Article: Botnets

ENJOY SAFER TECHNOLOGY™

Table of Contents

Botnets

David Harley, ESET Senior Research Fellow

I was recently asked by a cyber security research student some questions about botnets. From a technical point of view, I'm probably not the best person to ask about this. It's a long time since I was directly involved with botnet research, though I was one of the authors of a Syngress book on the topic. That said, my participation was fairly peripheral.

Of course, if someone wanted a more historical view, I'd be reasonably well placed: I'm old enough to have seen a lot of history in my time. ☺

Here are the responses (lightly edited).

1. **How should we as an industry be moving to prevent and disable botnets?**

Cooperation is key when it comes to disabling a botnet, though I've seen lots of stories where state agencies tend to take the lion's share of credit for a takedown with a passing reference to companies and researchers who contributed to the operation. (Though it's not unknown for a single security company to give the impression that it was the prime mover in a highly cooperative effort, either.)

In general, security companies tend to provide the bulk of the analysis, and often cooperate across corporate borders. But it's not all about 'find a bot, analyse a bot, detect a bot'. Successful takedowns sometimes start with monitoring forums where malware is sold or rented, of course, so sometimes detection starts even before massive distribution campaigns get underway. But what I'm also thinking about is that security companies don't generally have all the legal capabilities often involved in sinkholing or a takedown, so working with state agencies helps to fill that gap.

Nonetheless, it's not only 'pure' security companies that need to be involved. Consider, for instance how Apple actually hampered one company's efforts by asking for the closure of a domain the AV company was using as part of its Flashback sinkholing operation. While Microsoft, despite having a very good record when it comes to cooperating with external security researchers as well as pursuing its own very significant research, has been known to seize control of machines already controlled by security researchers and used for sinkholing.

2. **How effective current defense measures are against botnets?**

Moderately. You aren't going to get 100% detection of botnet-related malware from anti-virus software, but then people – let alone companies – shouldn't be relying on AV alone, even commercial (for-fee) AV, let alone the free stuff, which tends to lack some

functionality and any direct support. The point of modern security suites on the desktop is that they offer multi-layered security. That doesn't offer perfect protection, but it isn't restricted to direct detection of malicious or suspicious software. Obviously, sensors on the network and on servers offer even more layers of protection than may be present in a security suite: traffic analysis and intrusion protection, for instance.

3. **What impact do you think will IoT devices have on botnets?**

In general, IoT devices don't have the wide-ranging capabilities that a full-strength personal computer or even a modern mobile device has, so they tend not to have the same potential functionality. But that's not to say that they can't ever be used to amplify certain botnet activities. Right now I'm concerned about the possibilities of IoT as a target for ransomware, but I can also see some potential there as a delivery medium for the related (and growing) problem of DDoS.

4. **What is your approach when it comes to fighting botnets?**

Not really my field. I am, as Gilbert O'Sullivan once said, a writer not a fighter. ☺ Or, if you prefer, an educationalist. As a consultant, my main role is in mediating between the techies and analysts of the AV industry and the public at large, in the hope of helping people to understand better the threats that my colleagues at ESET and in the industry at large really *are* fighting in a more direct sense.

Robocalls: Automating Nuisance Calls

David Harley, ESET Senior Research Fellow
This article originally appeared on the ITSecurity UK web site.

Recently I received an email from Nikki Courtney of Radio KTRH, in Houston, requesting a radio interview on robocalls. Why me, I'm not sure, unless it was because of an article I wrote earlier this year for ESET. It's academic really, as I live in entirely the wrong time zone, and was in any case out of office and out of reach of email at the time. As a result, her deadline was long past by the time I saw the email. I did forward some notes in case they were of use to her, but as she apparently didn't use them and I didn't hear back from her, I guess they weren't… The article includes some responses from Maureen Mahoney of the Consumer's Union that might be of interest.

Here are Nikki Courtney's questions and my (edited) responses, in case you might find them useful.

1. Are robocalls on the increase and why?

Robocalls are certainly very common. In July 2015 Aaron Foss's estimate was that 35% of all phone calls are automated. Consumer

Reports told us in 2015 that 'Every month more than 150,000 consumers complain to the Federal Trade Commission and Federal Communications Commission.' Youmail's Robocall index posts a monthly estimate of the number of robocalls placed for that month, among other data. Its estimate for July 2016 is 2.4 billion robocalls in that month alone. Which is apparently actually *down* by 6% from June.

2. Who is calling?

Not all automated calls are technically scams, but many of them certainly come from scammers. The Consumer's Union states that an estimated $350m a year is lost to phone scammers. (It's not clear how many of those scammers are using robocalls, though.) Last year, the FTC shut down one offender in the US.

Robocalling is commonly associated with IRS scams, home improvement scams, and home security scams, but just about any phone scam *could* be delivered through automated calls.

Among scams delivered by robocalling in the UK are scams relating to mis-sold PPI (Payment Protection Insurance), mis-sold pensions, and debt management. The UK's Information Commissioner's Office recently fined the now defunct lead generation company Prodial Ltd £350,000 (the largest fine it has imposed to date) for making more than 46 million automated nuisance calls relating to PPI.

3. How do they get our numbers?

They don't necessarily need to get your number. In most cases that I'm aware of, robocalls aren't targeted, so using autodialing software to try every number in a given numeric range isn't difficult. And it can be done cheaply or for free using Voice over IP, so it doesn't matter much to the caller if many of the calls don't reach a likely sales prospect/mark.

4. How can someone stop robocalls?

Sometimes a phone company can block calls from known 'bad' numbers. However, the service is usually limited in the number of callers it blocks, and the service is normally for-fee. The Consumer's Union is, however, promoting a campaign to persuade service providers to block robocalls more effectively. Some models of telephone can include blocking functionality, according to organizations such as Which and Consumer Reports, but in general, only a few numbers can be blocked. Not only is there a huge number of numbers associated with sales, spam and scam calls, but it's also easy to change or spoof a caller ID. Once the scamming community has your phone number, you may receive calls from many *more* numbers. It is sometimes possible to block calls from withheld or international numbers, but that might mean losing legitimate calls as well as spam/scam calls.

There is also a wide range of call-blocking apps available for smartphones. I haven't tried any out, and can't make recommendations

as regards specific software or hardware.

Aaron Foss and Serdar Danis were each awarded $25,000 in 2013 by the FTC for 'intercepting and filtering out illegal prerecorded calls using technology to "blacklist" robocaller phone numbers and "whitelist" numbers associated with acceptable incoming calls.' Foss's Nomorobo service is claimed to be successful for people using VoIP carriers that support Simultaneous Ringing.

5. Is there a do not call list?

Indeed there is. Many countries provide such a service, and the European Union's Data Privacy Directive 2002/58/EC *requires* members states to enact legislation to control cold-calling.

- UK Telephone Preference Service
- Republic of Ireland National Directory Database
- The US National Do Not Call Registry
- An equivalent site for Australians

Some countries refer to such services as a Robinson List

Subscribing to such a service reduces the risk of nuisance calls from *legitimate* organizations, but not (usually) from callers whose intentions are not legitimate, and who are hiding their identity. In general, they simply don't care about such lists. The UK's Telephone Preference Service doesn't actually apply to automated calls. That said, if you're in a country governed by EC legislation you shouldn't receive such calls unless you've already given permission. But it would be naïve to expect problems like these to be solved by legislation alone.

The FTC suggests, quite rightly, that just the fact that you've received a call despite being registered increases the likelihood that it's a scam call. However, some types of unsolicited call are normally permitted. The US service makes such exceptions for political calls, charitable calls, debt collection calls, informational calls, and telephone survey calls. The UK's service also excepts surveys, which is why sales calls often start off trying to sound as much as possible like a survey). Other exceptions to the 'no call' rule may vary from country to country.

David "Don't call me, maybe" Harley (Apologies to Carly Rae Jepsen)

ESET Corporate News

New ESET Secure Authentication Adds Easy Single Touch Push Authentication

ESET announced the service release of 2-factor (2-FA) authentication for businesses: **ESET Secure Authentication**. The new version comes with multiple improvements mainly focused on the enhancement of the end user's experience.

This version of ESET Secure Authentication, now available only for Android devices, comes with easy, single-touch push authentication with smart-watch support and many other enhancements including updated setup and installer, improved security and performance tweaks.

For more information, please visit https://www.eset.com/int/business/endpoint-security/two-factor-authentication.

ESET Achieved the Best Score in VBSpam and Won the Trust of Computer Bild Readers

ESET Mail Security for Microsoft Exchange Server won the latest spam filtering test by leading security testing authority, Virus Bulletin, having achieved a 99.999% spam capture rate with no false positives. As a result, ESET received the VBSpam+ certification, its fifth in a row, confirming its position as market leader in spam protection.

Furthermore, ESET has achieved another big win in Germany and this time both readers and users had their say. ESET Smart Security 9 received the "*Golden Computer*" award for the best product in the category: security for home users, being voted the top choice by readers of Europe's largest consumer IT magazine, Germany's Computer Bild.

The Top Ten Threats

1. JS/Danger.ScriptAttachment

Previous Ranking: 1
Percentage Detected: 15.62%

JS/Danger.ScriptAttachment is a generic detection of suspicious e-mail attachments.

2. Win32/TrojanDrownloader.Agent.CQH

Previous Ranking: N/A
Percentage Detected: 5.63%

Win32/TrojanDrownloader.Agent.CQH is a trojan that tries to download other malware from the Internet, which usually contains one or more URLs, from where it attempts to download several files and execute them directly.

3. JS/TrojanDownloader.Nemucod

Previous Ranking: N/A
Percentage Detected: 5.34%

JS/TrojanDownloader.Nemucod is a trojan that uses HTTP to try to download other malware. It contains a list of URLs and tries to download several files from those addresses. The files are then executed. This Trojan is now associated with ransomware.

4. LNK/Agent.DA

Previous Ranking: 2
Percentage Detected: 3.52%

LNK/Agent.DA is detection name for *.lnk file, which executes trojan Win32/Bundpil.DF. The LNK file is part of a Bundpil infection and is created with the special name "%drive_name% (%drive_size%GB).lnk" on removable drives, convincing users that it's a link to drive content. It actually points to %system32%\rundll32.exe with a Bundpil DLL component as a parameter.

5. Win32/Bundpil

Previous Ranking: 3
Percentage Detected: 3.08%

Win32/Bundpil is a worm that spreads via removable media. The worm contains an URL from which it tries to download several files. The files are then executed and HTTP is used for communication with the command and control server (C&C) to receive new commands. The worm may delete files with the following file extensions:

*.exe

*.vbs

*.pif

*.cmd

*Backup

6. Win64/TrojanDownloader.Agent.W

Previous Ranking: N/A
Percentage Detected: 2.44%

Win64/TrojanDownloader.Agent.W is a trojan that tries to download other malware from the Internet, which usually contains one or more URLs, from where it attempts to download several files and execute them directly.

7. JS/ProxyChanger

Previous Ranking: N/A
Percentage Detected: 2.02%

JS/ProxyChanger is a trojan that prevents access to certain web sites and reroutes traffic to certain IP addresses.

8. Win32/Agent.XWT

Previous Ranking: 5
Percentage Detected: 1.54%

Win32/Agent.XWT is a trojan that serves as a backdoor. It can be remotely controlled and is usually a part of other malware. It collects the operating system version and language settings, then attemps to send the gathered data to a remote machine using HTTP.

9. HTML/Refresh

Previous Ranking: 4
Percentage Detected: 1.53%

HTML/Refresh is a trojan that redirects the browser to a specific URL serving malicious software. The malicious program code is usually embedded in HTML pages.

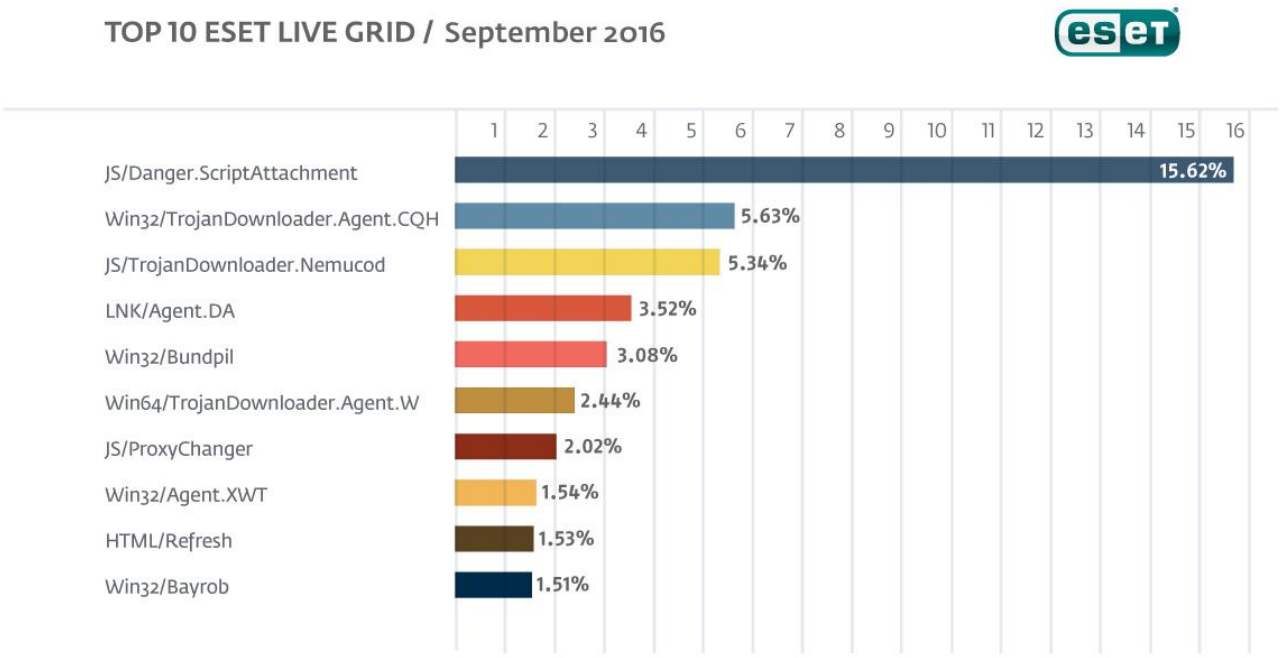
10. Win32/Bayrob

Previous Ranking: N/A
Percentage Detected: 1.51%

Win32/Bayrob is a trojan that serves as a backdoor and can be controlled remotely. When executed, the trojan registers itself as a system service, in order to be executed at every system start. It collects the following information: operating system version, computer name and IP address, information about the operating system and system settings, MAC address, and a list of running services. The trojan can then send the information to a remote machine using HTTP.

Top Ten Threats at a Glance (graph)

Analysis of ESET LiveGrid®, a sophisticated malware reporting and tracking system, shows that the highest number of detections this month, with 15.62% of the total, was scored by JS/Danger.ScriptAttachment.



About ESET

ESET®, the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company has continued to lead the industry in proactive threat detection. By obtaining the 97th award in July 2016, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organizations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.

The Company has global headquarters in Bratislava (Slovakia), with regional distribution centers in San Diego (U.S.), Buenos Aires (Argentina), and Singapore; with offices in the United Kingdom, Jena (Germany), Prague (Czech Republic) and Sao Paulo (Brazil). ESET has malware research centers in Bratislava, San Diego, Buenos Aires, Singapore, Prague, Košice (Slovakia), Krakow (Poland), Montreal (Canada), Moscow (Russia) and an extensive partner network for more than 180 countries.

More information is available via About ESET and Press Center.

Additional Resources

Keeping your knowledge up to date is as important as keeping your AV updated. For these and other suggested resources, please visit:

- VirusRadar
- ESET White Papers
- ESET Conference Papers
- WeLiveSecurity
- ESET Podcasts
- ESET Videos
- Case Studies