Consequences of Botnets Spreading to Mobile Devices

Anne Ruste Flø\textsuperscript{1} and Audun Jøsang\textsuperscript{2}

\textsuperscript{1} Department of Informatics, University of Oslo, Norway,
\textsuperscript{2} UNIK, University of Oslo, Norway

Abstract. Botnets represent a serious security threat on the Internet. Current security mechanisms are typically inadequate for protecting against the latest breed of botnets, as botherders constantly develop new techniques and methods to frustrate investigators. Until recently, mobile networks have been relatively isolated from the Internet, so there has been little need for protecting against botnets. However, this situation is rapidly changing. Mobile networks are now well integrated with the Internet, so that threats on the Internet most likely will migrate over to the mobile networks and vice versa. Botnets of malware injected into mobile devices will probably appear very soon, and there are already signs of this happening. This paper analyses the potential threat of botnets based on mobile networks.

Key words: Botnet, Security, Threat, Malware, Mobile device, Mobile network

1 Botnet on the Internet

A botnet [14] is a set of computers that are infected by a specific bot virus which gives an attacker (aka. Botherder) the ability to remotely control those computers.

Most botnets are developed for organized crime where doing targeted attacks to gain money. Example of attacks are sending spam [13], denial of service attack (DOS) or collecting and sale of information that can be exploited for illegal purposes.

Researchers who fight against botnets are in general one step behind the attackers. Once they have found a solution to discover and take down a botnet the botherders change their botnet to fight back.

Botnet starts their lifecycle [13] when a vulnerability in an operating system or software are exploited or users have been fooled to run unwanted software on their computer. Malware is often distributed as spam within a malicious attachment, spam linked to infected websites, open file shares, through instant messaging (IM) or by scanning after vulnerabilities. Compared to older malware they spread much faster on the Internet than through floppy disk or Bluetooth. After exploiting the desktop computer a secondary infection that installs and updates the botclient appears.
Evolution of botnets has made them more difficult to discover [5] and take down because they hide their communication between the legitimate traffic on the Internet by using TCP port 80 [3] and they use peer to peer (P2P) technology that make them more resilient.

Web based C&C [4] uses pull rather than push technology. Web servers can passively wait for the botclients to make contact. This lowers the network traffic between the botclients and the servers making it harder to spot the botnet on the network. To evade shutdown efforts the C&C needs to be constantly moving by using techniques like multihoming, fast flux and distributed C&C (Superbotnet).

Waledac is a botnet on the Internet that is web based and communicates using XML messages as payload. MMS messages have a body field [9] where the XML message from Waledac can be hidden. Can Waledac infect mobile devices and use MMS and SMS to communicate with its C&C?

2 Threat of Botnets Spreading to Mobile Networks

Mobile devices are nowadays capable of using Internet connection [7], [11] through High-Speed Downlink Packet Access (HSDPA), Evolution-Data Optimized (EVDO), Universal Mobile Telecommunication System (UMTS), Enhanced Data Rates for GSM Evolution (EDGE) and General Packet Radio Service (GPRS) which are different IP based technologies evolved within the mobile network and wireless network (WLAN).

The next generation of network technology will be mobile broadband where the mobile device will stay online and connected to the Internet all the time. Mobile terminals become more and more like desktop computers. Several studies on botnets and mobile devices predict communicating on the Internet. This paper will study botnet communicating on the mobile network.

The connection between the traditional Internet and the mobile network may act as a gateway for malware to move freely between these networks. Infection vectors used to spread Internet malware [15] are extended using MMS, SMS, Bluetooth and synchronizing between the computer and the mobile device. Malware on mobile devices can move using infections vectors on the Internet as email, web pages and social engineering.

What benefits can be gained using mobile device as a botclient? Are there any economic gains, is there any malicious action to do through the mobile network? Can mobile botnet become as difficult to track and close down as botnets on the Internet?

By having a botclients on mobile devices a botherder will be able to exploit services in the mobile network. By their nature mobile devices will not be available on the Internet all the time. They switch between available communications channels on the Internet or on the mobile network.

Mobile devices using the Internet may stay behind a firewall and normally they get dynamic private IP addresses that are not available on the Internet. The botherder will thus not be able to contact and send commands to the botclient directly through Internet connection. This challenge has already been solved.
Consequences of Botnets Spreading to Mobile Devices

with web based botnets where the botclients connect to web servers and poll updates.

Waledac is a web based botnet [3] on the Internet, very similar to Storm known as the biggest mass emailing botnet on the Internet. Waledac seems to be an updated version of Storm and is based on a three-tiered architecture existing of C&C, proxy servers and botclients. Botclients that respond to HTTP requests act as proxies to the backend C&C servers. None of the botclients communicate directly with the backend C&C.

The payload of HTTP requests falls in two parts. The first part of the payload contains the XML elements. The second part of the payload contains IP addresses if the sender is a proxy and AAAAAA (36 0-bits that are Base 64 encoded) if the sender is a botclient. All requests and responses have a payload forming at least <lm> XML element in plaintext. Sub XML elements differ depending on the type of message that is being send within the botnet.

Mobile devices mostly communicate on the mobile network and thus are unavailable on the Internet. Sending SMS and MMS messages containing payload like, XML elements those used in Waledac, will give the botclient on the mobile device the opportunity to maintain connection to its C&C through the proxy servers. The proxy server may be a device that understand and read the SMS and MMS message and have access to the Internet. By monitoring incoming messages the botclient can delete the message before it is added to the inbox to hide its existence.

Waledac uses P2P technology, meaning that infected mobile devices would have to communicate with each other to exchange list of active proxy servers. This can be done through MMS messages communicated between the infected devices on the mobile network.

Waledac on the Internet update their list with IP-addresses. Mobile devices do not use IP-addresses when sending SMS or MMS. Every device on the mobile network has a International Mobile Subscriber Identity (IMSI) and MSISDN. IMSI [10] can be used to identify, authenticate and register the device on the mobile network. MSISDN [9] is the number you use when calling another mobile device or sending a message. Then the list of proxy servers must contain MSISDN numbers together with IP-addresses in case the botclients would connect to the Internet thus communicate directly with the proxy servers on the Internet. Domain name does not exist on the mobile network. This makes it impossible to use techniques like fast flux and multihoming on devices in the mobile network. The consequence is that mobile devices cannot act as proxy servers as they very soon will be detected.

Symantec reported [2] on 13 July 2009 that the first botclient on Symbian OS may have been developed. SymbOS.Exy.C, (aka Sexy Space) is a worm similar to other worms made for Symbian OS but the difference is the client that tries to contact a malicious server reporting the mobile device's phone type, International Mobile Equipment Identity (IMEI) and IMSI. Symantec mentions that this may be the first occurrence of a true botnet client on a mobile device.
Waledac has not been ported to an operating system for mobile devices and therefore does not pose a threat yet, but this may only be a matter of time.

2.1 Possible attacks on mobile devices

Waledac is known for sending email. A infected mobile device can send MMS or SMS to other mobile devices or to service numbers. Victims can be chosen by the botherder or they can randomly be chosen from the address book or contact list on the infected mobile device.

In Norway there are some contests where you can vote for your favorite song, person, TV program and so on. A botnet consist of many infected computers and the voting system will not be able to detect if a botherder uses his botnet to send a short message to the voting service. But will anyone pay a botherder to vote up his or her favorite song or person? Maybe someone would in context of political elections.

Instead of using the voting application, a DDOS attack [5] against core of the mobile network can be done to stop people voting by making the voting system unavailable during the voting period.

There exist service phones where you can give money to charity. If you call a specific service number the mobile device subscriber pays a preset amount. Example are *Nationalforeningen for Folkehelse* or *Kirkens Nødhjelp* in Norway where you can call their respective service numbers to donate NOK 100, or other service numbers where you would donate twice as much. What if a botherder creates his own service number and programs all his botclients to call that number. The price should be low so the subscribers would not notice and be suspicious about the extra charges.

Mobile devices are being more common to our daily life. They are small and you can carry them everywhere you go and you will probably lose some of them too. Mobile devices can be used to communicate between people both through voice and messaging. [8], play games alone or with others on the Internet, make payments, check the status on your bank accounts, store private information [6] like contact information (name, phone number, email addresses), personal information (social security number, PIN codes, account numbers, private pictures or business related data) and other informations that criminals can exploit and misuse for financial gain.

Infected mobile device will be able to act as spyware in the same way as botclient on desktop computers collecting personal information and send it to the attacker. Waledac is a plug-in based botnet and it is easy [3] to add plug-ins to extend functionality. There will be a possibility to create a plugin that scans the mobile device. The result can be reported back to the C&C in an XML document formed as an MMS.

Most people [12] are trained to enter private data like social security number and credit card number on the mobile device using the mobile network. Is this safe anymore as the traffic in UMTS and newer technologies are routed within the IP-network?
3 Mitigation Strategies against Mobile Botnets

Techniques [15] as antivirus scanning, intrusion detection system (IDS) and packet filtering may be used together to stop malware spreading. Like Waledac hiding its traffic through legitimated web traffic, Waledac on mobile devices can hide its traffic through legitimate MMS and SMS traffic making it harder for the researchers to spot botnets on the mobile network. Botclients communicate with each other and would adopt the same resilient behavior as botnets on the Internet.

Waledac has a predefined structure on the messages. If you know what to look for there is possible to search and analyze the network traffic after specific signatures that Waledac or other known botnet creates.

In front of email systems there may be an antivirus scanner that scans every incoming and outgoing email for malware. This requires extra resources, but may be necessary to protect end users against attack. MMS work in similar way as the email system where MMS messages is send from an MMS client to an MMS proxy server where it is converted to standard Internet MIME format to permit various media components to be carried over the Internet environment. The receiving MMS proxy server will convert it back to MMS format before delivering the message to the MMS server which stores MMS message. To protect users from spam and malware attack the mobile network operator should use an antivirus scanner in front of their MMS server scanning incoming and outgoing messages to stop malicious messages to be delivered to the end users.

Security on mobile devices are not safeguarded [6] in the same way as it is on desktop computers making the mobile devices easier to exploit. Compromised items inside a corporate network will constitute a threat since many security systems on the network can easily be bypassed. Mobile devices are often ignored. Jansen and Scarfone write in their article [6] that most corporate networks do not have centrally managed system to take care of the security policy and security update on mobile devices. It may also be difficult to update the mobile device due to lack of knowledge about how to do it. Many mobile device applications do not have update managers like applications on desktop computers do. A system is only as secure as its least secure component and mobile devices often fall into this category.

To overcome this problem Janson and Scarfone [6] suggest several techniques. By using PIN codes the access to the SIM card is protected. Additional memory cards will not have the same protection since they can be taken out and put into other devices. By turning off interfaces like Bluetooth, Infrared (IR), WLAN and other wireless access protocols until they are needed, the attack surface on the mobile device can be reduced. Install antivirus software can provide protection against incoming malware, but the application will drain battery power very fast. Use certificate based solutions to sign applications even if the newest worm Sexy Space [2] shows that this too is exploitable.

Compared to malware and botnet evolution on the Internet, mobile platform are 7-8 year [1] behind. Experience from malware on the Internet can be transferred to malware on mobile device. Norman [1] predicts that malware on mobile
device will evolve faster since techniques are already explored. Security mechanism on mobile devices there for have to follow the same evolution as those on desktop computers. Windows Update for Windows Mobile 6 exists already. Adobe Updater, Java Update Manager exists for desktop applications so why not implement these on mobile devices too?

4 Conclusion

Mobile devices are becoming more and more similar to desktop computers although their computational and storage capacities remain smaller. Mobile devices normally stay connected online all the time because of their default characteristics and user behavior. As a consequence of the integration of mobile networks into the Internet, security treats on one network will affect the other network. This opens the potential for botnets spreading to mobile networks. In the past the security of mobile networks has been relatively well controlled by the networks operators. By turning mobile devices into general purpose computation and communication platforms, new security vulnerabilities will emerge. The possibility of downloading Internet application to mobile devices also brings the risk of malware infection. People need to become aware that mobile devices are vulnerable to being infected by malware, and thereby can be turned into a botclient as part of a botnet. In this paper we have shown that there are potential profitable business models for exploiting mobile botnets. It is therefore necessary to start thinking about methods for reducing the threat of botnets on mobile networks.

References

Consequences of Botnets Spreading to Mobile Devices


