



The Threat posed by Greynets

A Voco White Paper

This document is the copyright of Voco Limited

September 2009

The Threat Posed by Greynets

Executive summary

Recent improvements in network monitoring capabilities have allowed organizations to identify an increase in so called greynet activity on company networks. This activity consists in the main of peer to peer (P2P) file sharing, instant messaging (IM) and adware, spyware or malware.

This activity should concern CEOs/CIOs because:

- It consumes bandwidth. This is an additional cost and greynets can reduce the availability of resources.
- It results in systems working slowly or becoming unusable. The cost of rebuilding systems is high.
- Any questionable activity is directly attributable to the company thereby affecting its reputation.
- Systems are being compromised and may be part of a botnet.
- This activity is providing an attack vector directly into the heart of company networks potentially leading to the loss of important data.

This activity can be greatly reduced by:

- Developing a greynet policy and having users adopt it.
- Removing administrative rights from users.
- Configuring firewalls, Internet proxies and web filters to only allow Internet browsing.
- Deploying a networking monitoring capability to detect and prevent breaches of policy.

*Systems are being
compromised and may be
part of a botnet*

The measures suggested here will help:

- Manage the use of legitimate applications.
- Block the use of P2P networks that could breach company security policy.
- Prevent malware from being accidentally or intentionally downloaded by users.
- Compliance with data privacy and information security legislation.

It may be easier than you think.

Greynets

Wikipedia describes a greynet as:

'An elusive networked computer application that is downloaded and installed on end user systems without express permission from network administrators and often without awareness or cognition that it is deeply embedded in the organization's network fabric. These applications may be of some marginal use to the user, but inevitably consume system and network resources. In addition, greynet applications often open the door for systems to become compromised by additional applications, security risks and malware.'

Typically greynets manifest themselves as P2P file sharing, spyware, adware and instant messaging:

P2P File Sharing

Whilst not all file-sharing activity is illegal this software is often used to distribute music and movie files. Some file-sharing software comes bundled with malware such as spyware, viruses, adware, or otherwise privacy-invasive software. Additionally, malware is often integrated into media and application files that users share. In many cases such malware can interfere with the correct operation of web browsers, anti-virus software, anti-spyware and software firewalls; can cause degraded performance on affected systems; and in some cases may secretly compromise a user's privacy or security.

Systems Spyware can even change computer settings

Examples frequently encountered on networks in New Zealand include:

E Donkey
Limewire
Gnutella
MegaUpload

Spyware/Adware

While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information such as Internet surfing habits and sites that have been visited. Spyware can also interfere with a user's control of the computer in other ways, such as installing additional software, redirecting web browsers, and accessing websites that will cause more harmful viruses. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs.

Adware or advertising-supported software is any software package that automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. Some types of adware are also spyware and can be classified as privacy-invasive software.

Examples frequently encountered on networks in New Zealand include:

- Fun Web products
- Context Plus
- My Websearch Toolbar
- Asksearch Toolbar
- Alexa Search Toolbar
- VPP Technologies
- Hotbar
- Coolwebsearch

Instant Messaging

Instant messaging (IM) and chat are technologies that create the possibility of real-time text-based communication between two or more participants over the Internet or some form of internal network/ intranet. IM channels are increasingly being exploited as a means to spread malware.

Examples frequently encountered on networks in New Zealand include:

- MSN Messenger
- Google Chat
- ICQ
- Yahoo Messenger
- Skype
- AOL IM

Network Monitoring

It is one thing to know that these greynets are now infiltrating company networks; it is another to detect them. Thankfully recent improvements in network monitoring solutions enable security staff to have an improved view of network activity. Intrusion detection technologies, application-aware firewalls, web filtering solutions and anti-virus/anti-malware solutions can all help detect greynet activity. There are even some solutions now that are specifically designed to identify and secure greynet activity. This would be particularly useful for an organization, such as a trading house, that relies on IM for real time communications but wants to limit IM activity to one approved solution, record all conversations, and prevent any other greynet applications from being used.

Systems IM channels are increasingly being exploited as a means to spread malware

The Threat

This activity is of concern because:

- It consumes bandwidth. This has a financial cost to companies and may result in slower network performance for authorized activity.
- It results in systems working slowly or becoming unusable. This requires a company to spend more on systems administration.
- The sharing of movie and music files is illegal. The IP address that would be detected in an investigation is registered to the company. Any questionable activity is directly attributable to the company and may be the responsibility of the CIO and CEO.
- Systems in New Zealand are being compromised. Compromised systems may be part of a botnet. Botnet is a term used to refer to a collection of compromised computers (called zombie computers) running software, usually installed via worms, trojan horses, or backdoors, under a common command-and-control infrastructure. Botnets are used for sending email spam and for conducting Denial of Service (DoS) attacks. It would be highly embarrassing for a company's PCs to be identified as being the source of a DoS attack or Spam. Botnets are controlled by command and control servers.
- Company systems will communicate with identified command and control servers and Russian Business Network servers. The Russian Business Network (commonly abbreviated as RBN) is a cybercrime organization, specializing in personal identity theft for resale. It is the originator of MPack (software) and the operator of the Storm botnet. The RBN, which is notorious for its hosting of illegal and dubious businesses, originated as an Internet Service Provider for child pornography, phishing, spam, and malware distribution physically based in St. Petersburg Russia.
- This activity provides an attack vector directly into the heart of a company network. This vector often evades existing network security controls.

Systems in New Zealand are being compromised

Security Controls

This activity can be greatly reduced by:

- Developing a greynet policy and having users adopt it. The policy should explain what users are allowed to do and the threat that greynets pose.
- Removing administrative rights from users. The majority of these products require an application or client to be installed on the user's PC. In order to install a piece of software the user requires Administrative rights. If the user cannot install the software there is no greynet issue.

- Configuring the company Internet proxy and firewalls to only allow Internet browsing. Internet browsing should be limited to only allow users access to ports 80, 8080 and 443. Should users require additional access they should submit a request to the company's help desk. All essential administrative functions should be identified separately and configured as exceptions. Examples might include SMTP, FTP and SSH.

The measures suggested here will help:

- Manage the use of legitimate applications.
- Block the use of P2P networks that could breach a company's security policy.
- Prevent malware from being accidentally or intentionally downloaded by users.
- Secure the network against worms, trojans, malware and rootkits.
- Compliance with data privacy and information security legislation.

Acknowledgements

Wikipedia was used as a source for definitions.

About the Author



Paul Hortop contributes over 20 years of experience in all facets of physical, network and data security to Voco's transformational capability. Drawing on his experience as an ethical hacker, computer forensics expert and computer incident response team lead allows him to design and deliver solutions that work in the largest of enterprises.

About Voco

Voco Limited is a New Zealand owned company that provides a local alternative to multinational consultancies in the specialist area of ICT consultancy. Voco was established in early 2001 by Michael Foley and Paul Gordon, who along with Jon Wallace are the company's directors. The company's independent chairman is Marcel van den Assum.

Voco undertakes strategy, architecture, design, sourcing and programme management in the telecommunications, converged ICT and customer interaction areas. The company has successfully undertaken large-scale, often high-profile projects for over 70 private and public sector organisations. It employs over 20 experienced professionals in Wellington and Auckland.

Having no physical premises, Voco operates as a "company without walls", using secure internet-based portals in a virtual office model that enables consultants to maximise their effectiveness and the targeted application of the company's intellectual property for clients wherever they need to be.

Voco can provide consultancy and design services to help your organisation tackle the issues that greynets pose.

Services we offer include:

- Risk snapshots for CIOs and CEOs
- Developing policy
- Designing technical controls to detect and prevent non-compliance
- Audits
- Investigations

Learn more about Voco at <http://www.voco.co.nz>