



A dozen demons profiting at your (in)convenience

By George Moore and Anthony Arrott

Organized web threat families pollute your PC for profit.

Just as personal computers and the Internet have become a regular part of our daily lives, so to have parasitic and malicious software. As the world has become more networked, vandal computer viruses of the early days have evolved into today's larcenous web threats.

Simply put, web threats are malicious software programs such as spyware, adware, trojan horse programs, bots, viruses, worms, etc. that are installed on a PC without the knowledge or permission of the owner. These programs utilize the internet to spread, hide, update themselves, and send stolen data back to perpetrators. They can be combined – for example, a trojan downloads spyware or a worm that is used to infect a PC with a bot.

Another way to consider web threats is as the software of individual malware and adware enterprises. At one end of a spectrum these enterprises are fully-incorporated publicly-disclosed corporations. These include enterprises such as Integrated Search Technologies and Zango.

The darker end of the spectrum gets much more complex. The economy in the darker end of the internet has multiple profitable layers. Resellers of sensitive data, the latest vulnerabilities and authors of toolkits are common new ways of making a buck in the digital black-market.

Until recently, malware variants generally have been treated as separate individual threats. This comes from the legacy of self-propagating viruses and worms where a single variant can spread its vandalism worldwide within hours.

In contrast, the economically-motivated web threats of today use different software as piece-parts of a singular web threat business model. This has led anti-malware threat researchers to group together individual web threats that serve the same malware enterprise – regardless of differences in technical characteristics – see the table on the following page.

How does it get there?	What does it do?	How does it do it?	How does it protect itself?
installed by:	money from:	operates by:	protected by:
<ul style="list-style-type: none"> • exploit • unknowing consent • lack full disclosure • freeloader • trojan • worm 	<ul style="list-style-type: none"> • adware • trackware • keylogger • browser hijacker • fraudulent changes • fraudulent royalty 	<ul style="list-style-type: none"> • browser helper object (BHO) • browser toolbar • layered service provider (LSP) • application • cookie • dialer 	<ul style="list-style-type: none"> • rootkit • watchdog program • mimicry • polymorphic variation

Non-virus web threats on client PCs typically have four components that together characterize the web threat business model.

What emerges from these analyses is a much clearer view of the web threat economy. Web threat families are groupings of individual web threats and variants that serve the same malware enterprises. Web threat families can consist of multiple pieces of software on individual PCs – each piece serving the malware business model in its own specialized way.

Rather than counting up all the software pieces as individual infections or variants, it is more relevant just to consider whether a PC is infected by a web threat family or not. And unlike viruses, where the rate at which an outbreak spreads is so important, web threats are best measured by what fraction of PCs are infected and how long they stay there earning money for their malware enterprise. As a result, the relevant index of web threat families is the average proportion of PCs infected. For example, the Zango web threat family led all

others, infecting on average 9.7% of all PCs throughout 2007.

There is one small consolation in all this for defending PCs from the rising tide of economically-motivated web threats. While malware writers have almost infinite technical variations available to disguise and protect new malware, the web threat business model is far more constrained. Web threat behaviors associated with monetary gain are typically harder to disguise than the underlying technologies for implementing them.

This has helped threat researchers at Trend Micro identify the top perpetrators of web threat families that profit at the inconvenience and expense of PC owners and users. Trend Micro has designated the top twelve of these web threat families the “Dozen Demons”. Here they are:

- | | |
|----------------------|------|
| 1. Zango | 9.7% |
| 2. Hotbar | 7.0% |
| 3. Drivercleaner | 6.7% |
| 4. Winfixer | 6.1% |
| 5. Virtumundo | 6.0% |
| 6. WhenU | 5.7% |
| 7. IBIS | 4.9% |
| 8. Purity Scan | 4.6% |
| 9. Zlob | 4.5% |
| 10. New.net | 4.1% |
| 11. Softomate | 3.4% |
| 12. Starware / Comet | 3.1% |

The proportion of PCs infected with a web threat family is based on weekly averages from HouseCall scans of 2.4 million PCs worldwide measured throughout 2007. Infections from identified web threat families accounted for 67% of all infections.

1. Zango - 2007 average proportion of PCs infected: **9.7%**

Zango software includes known adware and spyware typically required to access partner's games, DRM-protected videos and software. Zango's consumer website asserts that the company is "committed to creating a content economy built on a foundation of safe and ethical practices by protecting consumer privacy while offering a fulfilling and high-value content experience." Zango content includes sports, comedy, dance, erotic videos, online games, and screensavers. Warner Bros. and others have been known to provide content, although Warner Bros. has terminated its business relationship with Zango after an on-line outcry.

Zango Easy Messenger

Undesirable behaviors associated with Zango Easy Messenger include:

- automatically runs on startup
- displays pop-up advertisements
- installs adware.

Zango Cash Toolbar

• A number of user pages on the MySpace domain which have videos that look like they are from YouTube. The videos have an installer embedded within them for the Zango Cash Toolbar. When users click on the video, they are directed to a copy of the video, which is hosted on a site called Yootube.info.

Third parties are paid by Zango to install Zango software without the required user consent. Zango's past features a remarkable series of bad-actor distributors, from exploit-based installers to botnets to faked consent. Even today, some distributors continue to install Zango without providing the required notifications and consents.

Seekmo

Seekmo is an adware program by Zango that claims to be a free tool to provide content such as mp3 files, screen savers and videos. Seekmo can pop-up advertisements even if you have a pop-up blocker on your computer, and will monitor your computer usage to gen-

erate ads that you are more likely to respond to.

2. Hotbar - 2007 average proportion of PCs infected: **7.0%**

Hotbar (also known as HbTools) is a plugin for Internet Explorer, Microsoft Office Outlook, and Outlook Express. Hotbar adds a toolbar and the option of extra skins to these programs. It also allows the user to add emoticons to emails created in Outlook or Outlook Express or check the weather report. Its major revenue comes from the excessive use of pop-ups which are displayed according to a user's behavior and current URL. The application can show over 15 pop-ups a day, depending on how much Internet browsing has occurred.

Undesirable behaviors associated with Hotbar include:

- bombards users with ads in pop-ups, web browser toolbars, Windows Explorer toolbars, auto-opening sidebars, and even desktop icons
- failing to affirmatively show a license agreement.

Originally independent, Hotbar has since been acquired by Zango.

3. Drivecleaner - 2007 average proportion of PCs infected: **6.1%**

DriverCleaner is a program that is silently installed by using an exploit or social engineering. The program falsely claims the PC is infected and will not clean until you purchase the software. This threat is often installed along side the Vundo Trojan that holds position 5 on the dozen demons list.

4. Winfixer - 2007 average proportion of PCs infected: **6.1%**

Winfixer is a program that is silently installed by using an exploit or social engineering. The program falsely claims the PC is infected and will not clean until you purchase the software. This threat is often installed along side the Vundo Trojan that holds position 5 on the dozen demons list.

5. **Virtumundo** - 2007 average proportion of PCs infected: **6.0%**

Virtumundo is a trojan that typically uses social engineering tricks and silent install websites to get installed. Many have been observed to install fraudulent security software such as Winfixer or DriverCleaner.

Also known as VirtualMundo and VirtuMonde, Virtumundo facilitates the spread of adware and spyware that results in large amounts of unsolicited pop-up advertisements. The threat regularly contacts predetermined web sites to receive ads and additional instructions. Virtumundo is also bundled with spyware and advertising-supported applications that automatically run on every Windows startup.

6. **WhenU** - 2007 average proportion of PCs infected: **5.7%**

WhenU, a popular adware company make an array of products such as Save Now and WhenU search. These products are installed by themselves as well as bundled with 3rd party applications such as screen savers and shareware.

WhenU offers contextual advertising through their software. The software selects which advertisements and offers to show you based on several factors, including which web pages you visit, search terms you use while searching online, the content of the web pages you view, and your local zip code (if you have supplied it.)

WhenUSearch

WhenUSearch is an adware application that creates a special desktop toolbar, monitors user Internet activity, collects details of performed web searches and serves marketing and advertising content. WhenUSearch can update itself via the Internet. The adware is bundled with ad-supported WhenU.com software. It can also be manually installed. WhenUSearch runs on every Windows startup.

SaveNow

SaveNow is adware that delivers relevant offers, coupons, and advertisements to you based on your web browsing habits. SaveNow

may track which web pages you visit, the search terms you use while searching online, the content of the web pages you view, and your local zip code. This information may be used to base which advertisements and offers to show you.

7. **IBIS** - 2007 average proportion of PCs infected: **4.9%**

IBIS are a company that distributed a toolbar that used several unique methods to make it difficult to be manually removed or cleaned with security software. This toolbar was discontinued by Ibis LLC last year but still remains installed on many users machines.

IBIS Toolbar

IBIS Toolbar is a web browser toolbar that may redirect your search requests and display pop-up advertisements. IBIS Toolbar may monitor your Internet activity, including your search requests, websites you are visiting, products you are buying, and data you enter into forms. IBIS Toolbar may share this information with third party partners. IBIS Toolbar may also download and install adware without your knowledge or permission. IBIS Toolbar may prevent you from visiting various anti-spyware websites. IBIS Toolbar is typically distributed through pop-up advertisements and bundles with other spyware, such as Cydoor.

8. **Purity Scan** - 2007 average proportion of PCs infected: **4.6%**

Purity Scan is a program that is supposed to scan your PC for pornography. This program has been installed with the use of exploits and social engineering tricks. Purity Scan is owned by Clickspring and is also known to go by the alias VirtuScope.

PurityScan is a free tool that checks your computer for objectionable adult content. PurityScan scans your computer files and Internet history for keywords that may hint at pornographic material. When it locates questionable content, it displays the URL, word, or file name in a display table so you may delete it. After installation, when you connect to the Internet PurityScan may also launch advertisements, and automatically update itself.

PurityScan upgrades may include the automatic installation of third party applications.

9. Zlob - 2007 average proportion of PCs infected: **4.5%**

Zlob is commonly assigned to trojans that pose as video codecs on adult websites and have also been noted to spoof popular video services such as YouTube. These trojans have been noted in the wild to install fraudulent security applications as well as DNS hijackers.

Zlob is a backdoor designed to give the attacker remote control over a compromised PC. It changes essential computer settings and modifies certain files. Zlob starts automatically on every Windows startup and hides its activities by injecting code into explorer.exe. It waits for remote connections and allows the attacker to download and install additional software, execute certain commands and manage the entire computer. Zlob can be very dangerous. Use antivirus and malware removal tools in order to get rid of this spyware.

Zlob Trojan installs many popular rogue anti-spyware programs, among them are IEDefender, AntiVirGear, SpyShredder, WinAntiVirus Pro 2007, Ultimate Cleaner and SecurePCCleaner.

10. New.net - 2007 average proportion of PCs infected: **4.1%**

NewDotNet is a layered service provider to the TCP/IP stack that allows other domain suffixes besides .com such as .xxx and .shop. This application is commonly bundled with other software.

NewDotNet is an Internet Explorer plug-in that sends a web browser to sponsored web sites whenever the user enters a non-existent or mistaken site address into the address bar. The threat can track user browsing habits and may show commercial pop-up advertisements. It is able to silently update itself via the Internet. NewDotNet is bundled with a variety of advertising-supported products. It also can be manually installed. The threat runs on every Windows startup.

NDotNet is an adware program that associates non-existent domain names with sponsored content. When a user enters a keyword into a browser address bar or types a mistaken or non-existent URL, the adware redirects the user to a sponsored page.

11. Softomate - 2007 average proportion of PCs infected: **3.4%**

Softomate are a company that provides customizable toolbars. Some of the toolbars created are used in a malicious fashion and others are used for legitimate purposes.

Softomate toolbars may change your browser settings and redirect your search requests through a parent server. Softomate may also monitor your Internet activity and habits and launch pop-up advertisements accordingly.

12. Starware / Comet Systems - 2007 average proportion of PCs infected: **3.1%**

Starware is an Internet Explorer toolbar with specialized search functions and a pop-up blocker. Starware Toolbar may display advertisements and redirect your search requests through their parent server. Bug fixes and new features may be added to Starware Toolbar without your notice.

George Moore is a senior threat researcher at Trend Micro specializing in spyware and adware. He focuses on the methods by which Web threats surreptitiously install and protect themselves on user PCs as well as the organization and economics of malware publishers.

Anthony Arrott is a special assistant to the CTO at Trend Micro. He manages threat analytics operations and threat data sharing agreements with outside organizations.

Together in 2007, the authors led the project team for Trend Micro HijackThis v2.0 - enhancing the popular malware diagnostic tool originally developed by Merijn Bellekom.