

Spyware Up Close:



During the month of March, Trojan Downloader Zlob was the most commonly found Trojan worldwide. This Trojan often silently downloads and installs bogus security programs such as SpywareQuake, SpyFalcon, SpyLocked and WinAntivirusPro, but may install other malware as well. Some variants of Trojan Downloader Zlob have backdoor functionality, giving an attacker the ability to remotely control and use the infected machine for malicious purposes.

Trojan Downloader Matcash is usually disguised as a harmless software program and is generally distributed as an e-mail attachment. Opening the attachment may cause an auto-installation process that loads the Trojan onto your computer without your knowledge or consent. Once installed, Matcash may download and install adware, spyware or other malware from multiple servers or sources on the internet.your web browser.

Adware

Adware is advertising-supported software that displays pop-up advertisements. Adware is often bundled with or embedded within freeware programs like screensavers, file sharing applications, messengers, etc. Although seemingly harmless, some adware programs track your Web surfing habits and deliver that information to a third party.

Worst case scenario: Adware may track a user's online habits and transmit this information to a third party. Additionally, Adware delivers pop-up ads which can cause overall system performance issues and dramatically slow your web browser.

Threat Name	Current Rank	Previous Rank	Threat Level
180search Assistant/Zango	1	1	Low
Hotbar/Zango	2	2	Low
Starware Toolbar	3	4	Very High
VirusBurst FakeAlert	4	6	Critical
Comet Cursor	5	5	Very High
VirusBurst	6	7	Very High
BraveSentry FakeAlert	7	4	Very High
Maxifiles	8	8	Very High
PurityScan	9	9	Critical
Seekmo Search Assistant	10	10	Low

Trojans

A Trojan horse is a program that allows a hacker to make changes to your computer. Typically, a Trojan will install itself on your computer without prior knowledge or consent. Unlike viruses, a Trojan does not replicate itself. A Trojan usually disguises itself as a harmless software program and is acquired by clicking on Internet pop-ups, downloading software, or by opening an e-mail attachment. Once installed on your computer, Trojans have the ability to create, delete, rename, view, or transfer files to and from your computer. Trojans may use a program manager that allows a hacker to install, execute, open, or close software programs. The hacker may have the ability to open and close your CD-ROM drive, gain control of your cursor and keyboard, and even send spam by sending mass e-mails from your infected computer. A Trojan typically runs in the background, hiding its presence.

Worst case scenario: A third party may gain access to your computer and steal your identity or download so much spyware that it renders the computer useless.

Threat Name	Current Rank	Previous Rank	Threat Level
Trojan Downloader-Zlob	1	1	Critical
Trojan Agent Winlogonhook	2	2	Critical
SDBot	3	3	Critical
Trojan Downloader Matcash	4	4	Critical
Trojan Downloader Ruin	5	5	Critical
p2pnetwork	6	7	Very High
Trojan Busky	7	6	Very High
Scumware-remover Trojan	8	8	Very High
Trojan-Backdoor-us15info	9	9	Critical
FastVideoPlayer	10	10	Very High

System Monitors

A System Monitor is tracking software used to monitor computer activity. System Monitors range in capabilities and may monitor some or all of the following:

- Key strokes
- E-Mails
- Chat room conversations
- Instant Messaging
- Websites Visited
- Running Programs
- Time spent on the computer
- Usernames
- Passwords

Information on these activities is gathered via remote access or sent by e-mail to a third party and then stored for future use or sold to another party.

Worst-case scenario: A third party may be able to view your personal conversations and may gain access to private information such as usernames, passwords, credit card numbers, or Social Security Numbers.

Threat Name	Current Rank	Previous Rank	Threat Level
Perfect Keylogger	1	1	Critical
AtomicLog	2	2	Critical
Potentially rootkit-masked files	3	3	Critical
NetNanny Chat Monitor	4	4	Critical
Family Keylogger	5	5	Critical
Golden Eye Cookie	6	6	Critical
007 Spy	7	8	Critical
Ardamax Keylogger	8	9	Critical
Phisher-GoldNow	9	6	Critical
Sc-Keylog	10	10	Critical