



Brandeis University
The Rabb School of Continuing Studies
Division of Graduate Professional Studies



Master of Science in Information Assurance

- Part-time degree programs
- Available online
- No GRE or GMAT requirements

Home > News > Fake P2P media files lead to adware attack

Fake P2P media files lead to adware attack

Dan Kaplan

May 07, 2008

RELATED ARTICLES

- [ABN Amro suffers p2p data breach](#)
- [FTC official: peer-to-peer software poses risks](#)
- [KaZaa users warned of p2p worm](#)
- [P2P attacks multiplying](#)

RELATED LINKS

- [McAfee Avert Labs](#)

Researchers at McAfee said they have detected the largest outbreak of malware in three years, an infection impacting hundreds of thousands of users whose machines contain poisoned media files.

The team at McAfee Avert Labs located the malicious files, mostly MP3 or AVI in format, on popular [peer-to-peer](#) (P2P) websites, such as LimeWire, Craig Schmugar, a threat researcher, told SCMagazineUS.com on Wednesday.

The bogus files appear when users employ certain terms when searching for music and video, he said. Once the files are downloaded, users are directed to a website and alerted that they need to install an additional program, or codec, to play them.

That is where the malicious software kicks in. Installing the software and agreeing to the terms and conditions result in adware being placed on the victim's machine, Schmugar said.

Nearly a half-million home-users of McAfee VirusScan Online have the poisoned media files on their computers – the largest single outbreak of a single threat in three years, he said. Most victims have become infected in the past two days.

The criminals behind the scam have socially engineered the files so they appear like the real thing, Schmugar said. To that end, they use terms such as "theme godfather.mp3" to describe the contents and pad the files with null characters to make the sizes appear legitimate.

"These are media format files and people tend to trust them," he said. "These file types are more trusted than typical vectors [to spread code]."

While potentially millions of users' machines worldwide contain the corrupted files, only a fraction of those individuals have actually installed the trojan by agreeing to download the fake media player, Schmugar said.

The attack could have been more destructive had the trojan forced its victims' machines to become part of a bot or sought identity theft through tactics such as password stealing, he added.

Minaxi Gupta, assistant professor of computer science at the Indiana University in Bloomington, who led a 2006 [study](#) on malware in P2P networks, said she and her team located 95 different types of malware, including downloaders, keyloggers and worms, in one-and-a-half months of research.

The problem gets so large because many P2P users unknowingly share rogue files with other users.

"Let's say I download something from a peer-to-peer network and maybe I don't execute it, and I put

FONT SIZE: A | A | A



Most Popular

- It's heere: Windows XP Service Pack 3 released
- IM malware attacks increase, report
- Report: small merchants biggest threat to credit card fraud
- A reason not to celebrate: Spam turns 30
- Massive hacker server discovered
- "Byzantine" botnet uses military, education servers for spam
- Changes to XP SP3, Vista SP1 corrupt data in Microsoft's RMS
- Forensic exam concludes no breach happened at university
- Social networking site for hackers is unveiled
- Military contractor pleads guilty to ID theft

Most Emailed

- IRS phishing scam targets stimulus payments
- The legal implications of the PCI data security standard
- It's heere: Windows XP Service Pack 3 released
- New spam wave uses naked video claim
- CEOs targeted by subpoena spam
- Massive hacker server discovered
- Major botnet infiltrated
- Massive hacker attack continues
- PCI council clarifies impending application rule
- Oracle closes 41 vulnerabilities, 17 in its database

Most Recent

- Secrets stolen? No, just the intellectual property
- Website attacks continue
- FTC halts spammer hawking adult sites
- Fake P2P media files lead to adware attack
- It's heere: Windows XP Service Pack 3 released
- Tech coalition asks judge to toss out Zango appeal
- Yahoo and McAfee team to secure search results

this data inside my shared network," she said. "It does nothing on my system, but it's in my shared directory.

"I think most malware that we see out there is not out of ill intent," Gupta added. "People get it and they spread it."

She told SCMagazineUS.com on Wednesday that file-sharing networks, such as LimeWire, perform limited checks to filter out malware. She and a group of graduate students are currently conducting additional research that will recommend, among other things, that P2P networks should add heuristics to detect malicious files.

"The only thing you can do [to protect yourself] is not join a P2P network and not download anything, or you can scan it to anti-virus when you get something," she said. "Most people don't do that."

In the case of the McAfee discovery, the files do not actually contain malware, so they would not be flagged during an anti-virus scan, Gupta said. However, the trojan would be discovered if the resulting codec -- supposedly required to play the file -- were run against a security check.

While mostly home users are affected by the attack, businesses should stay focused to the risks of file-sharing networks, Schmugar said.

"P2P has additional repercussions in corporate environments, most notably data leakage," he said. "I think that people close to that issue are fully aware of the risks. It boils down to acceptable-use policies and whether or not companies want their employees downloading media files."

Gartner Vice President and Senior Fellow John Pescatore told SCMagazineUS.com on Wednesday that businesses should, at least, run executables against known viruses.

"We basically tell businesses that there is no such thing as a business-quality peer-to-peer file-sharing type thing, he said. "There's vast quantities of corrupted things on there."

A LimeWire representative could not be reached for comment.

Tags: [Emerging Threats](#) [Trojans](#) [Consumer Threats](#)

Comments

 Login  Follow this discussion 

There are no comments posted yet. [Be the first one!](#)

Post a new comment

Enter text right here!

Name *

Email (track replies)

Blog URL

Claim my comments! [Why?](#) | [Login](#)

Or post using [OpenID](#)

SUBMIT COMMENT



[Get better comments for your blog](#)

- [Social networking site for hackers is unveiled](#)
- [Massive hacker server discovered](#)
- [Mozilla Messaging fixes five bugs in Thunderbird email client](#)

Featured White Papers

[Unauthorized Applications - Taking Back Control](#)

Employees installing and using unauthorized applications like Instant Messaging, VoIP, games and peer-to-peer...

[View Now](#)

[Facilitating PCI DSS Compliance](#)

The Payment Card Industry Data Security Standard is a detailed series of 130+ requirements that anyone who stores or...

[View Now](#)

[The Impact of the New FRCP Rules on Your Business](#)

Have you adjusted your data retention policies and electronic discovery procedures to comply with the new Federal Rules...

[View Now](#)

[Delivering Availability to the Adaptive Enterprise: Measuring the ROI of Mission Critical Services](#)

This paper discusses availability services as an enabler of change and IT operational efficiency. It explores...

[View Now](#)

[GoToMeeting Security White Paper](#)

This document provides a technical description of the security features built into GoToMeeting. It has been written for...

[View Now](#)

[View More Research](#)

Popular Tags

[Analyst Reports & Industry Surveys Breaches & Exposures Browser Flaws Compliance](#)
[Consumer Threats Education Email](#)

Security Emerging Threats
Finance Government Healthcare
High Tech IT Security
Training Lawbreakers & Cybercrime Legal &
Professional Services Manufacturing Microsoft
Mobile Endpoint Security Non-
Microsoft Patches Non-Profits Patch
Management Phishing Spam Techniques
Trojans Vulnerabilities & Flaws

westcoast labs



Click here to
find out more
information

Sponsored Links

Increase confidence on your site and see more conversions with help from the latest in SSL for your site - Extended Validation (EV) SSL. Read the free white paper to learn more.

The Power of Electronic Evidence

Setec Investigations combines today's most advanced computer forensics and litigation support expertise with a business- and legal-friendly approach. Expertise includes Computer Forensics, Electronic Discovery, Litigation Support, and Expert Witness Testimony.
www.setecinvestigations.com

Identity GRC Survival Kit

Security breaches, failed audits, fraud. Access and identity control exposures are treacherous. The Identity GRC Survival Kit offers tools and advice for managing risk associated with user access. Download now .

Master's Degree in Information Assurance

Brandeis University now offers a Master of Science in Information Assurance. Gain the technology and management expertise to develop, manage, and support enterprise-wide security objectives. A part-time program, available online. www.brandeis.edu/rabbgrad

Worry-Free Security in Just a Few Seconds

With the only integrated behavioral-based protection.
Zero-Minute. Zero-Touch. Zero-False Positive.
Smart Network. Smart Business.
From Radware.

The CSO Check-Up: 5 Pragmatic Tips for Maintaining Security without Losing Your Sanity

Date/Time: Available on demand

Click to register for FREE

During this entertaining and informative webcast, Mike Rothman, president and principal analyst, Security Incite, will present his straightforward, pragmatic approach to successfully managing your information security program and securing your data - without losing your sanity. [Sponsored by Core Security Technologies.](#)

60 online experts offer advice.

AOTA '08 Summit

Future of Online Trust

June 4-5, 2008 - Seattle

Gain insight from 60 experts, including Craig Newmark /Craig's List, Hemanshu Nigam /Chief Security Officer, Fox Interactive Media / MySpace.

[Home](#) | [News](#) | [Newsletters](#) | [Products](#) | [Blogs](#) | [Buyers Guide](#) | [Jobs](#) | [Events](#) | [Subscribe](#) | [Contact Us](#) | [About Us](#) | [Advertising](#) | [Editorial](#) |



RSS

This material may not be published, broadcast, rewritten or redistributed in any form without prior authorization.

Your use of this website constitutes acceptance of Haymarket Media's [Privacy Policy](#) and [Terms & Conditions](#)