

haymarket

[Subscribe](#) [Contact Us](#) [About Us](#) [Advertising](#) [Editorial](#) [SC UK](#) [SC Asia](#) [SC Aus/NZ](#)



▶ [Get the eBook: The Definitive Guide to Security Management](#)



Search

- [Home](#)
- [News](#)
 - [Features](#)
 - [Opinions](#)
 - [Newsletters](#)
- [Products](#)
 - [First Looks](#)
 - [Reviews](#)
 - [Group Tests](#)
 - [Best of 2007](#)
 - [Industry Innovators 2007](#)
- [Blogs](#)
 - [The News Team Blog](#)
 - [The Data Breach Blog](#)
 - [The IT Security Roundup](#)
- [Buyers Guide](#)
- [Whitepapers](#)
- [Jobs](#)
- [Events](#)
 - [SC World Congress](#)
 - [Awards](#)
 - [Forum](#)
 - [Podcasts](#)
 - [Digital Download](#)
 - [Editorial Webcasts](#)
 - [Vendor Webcasts](#)
 - [eConference](#)
- [Subscribe](#)
 - [Newsletters](#)
 - [Subscribe To SC](#)
- [Issue Archive](#)

- **Topic Center:**
- [Email Security](#)
- [Compliance](#)
- [Patch Management](#)
- [Financial Services](#)
- [Healthcare](#)
- [RSA 2008](#)

[RSS](#) | [Login](#) | [Register](#)

[Home](#) > [News](#) > [Finjan: Chinese cybercrime networks fill void left by Russian Business Network](#)

Finjan: Chinese cybercrime networks fill void left by Russian Business Network

[Jim Carr](#)

December 18, 2007

- Font Size: [A](#) | [A](#) | [A](#)
- [Print](#)
- [Email](#)

- [Order Reprint](#)
- [BOOKMARK](#)

Related Articles

- [Finjan: Developed countries host the most malware](#)
- [Finjan: Complex-code attacks to spike this year](#)
- [People on the move: Appointment at Finjan](#)
- [Trojan 2.0 era about to begin: Finjan](#)

Related Links

- [Finjan](#)

Related Reviews

- [Finjan Vital Security NG-6100](#)
- [Finjan Vital Security Web Appliance NG-5100](#)
- [VSA NG-5000](#)
- [Finjan Vital Security Appliance NG 1100](#)
- [Vital Security Appliance NG-5100](#)

Updated Tuesday, Dec. 18 at 2:53 p.m. EST.

An intricate network of servers operated by Chinese criminals has moved into the void created when the notorious [Russian Business Network](#) (RBN) shut down, according to a report from anti-crimeware vendor [Finjan](#).

December's "Malicious Page of the Month" report from Finjan's Malicious Code Research Center (MCRC) notes that the RBN "has suddenly picked up from its St. Petersburg digs and diversified...spreading its activity to new chunks of IP addresses, with RBN-like activity almost immediately appearing on newly registered blocks of Chinese and Taiwanese IP addresses."

Ifach Amit, director of security for the MCRC, told SCMagazineUS.com that the Chinese group's activity is "an evolution of the Russian Business Network."

"All of the criminal activity over the internet has financial gain behind it, and if you shut down one part of the system, it's bound to bounce back because of market forces," he said.

The report also noted that MI5, the United Kingdom's counter-intelligence agency, warned 300 U.K. chief executives and security experts of an increased risk from Chinese hackers following an attack on government servers.

Amit said Chinese cybercriminals scan the internet searching for vulnerable U.S. and European hosts at universities and government offices. The hackers then take advantage of misconfigured or unpatched systems, infecting them with [IFRAME](#) or [JavaScript](#) code, Amit said. The victim is then redirected to a series of sites containing IFRAMES, including those belonging to the Chinese network.

Other trojans are then downloaded to the victim's compromised PC and another IFRAME sends personal data, such as banking authentication credentials, to the network of Chinese servers. That information is used for tracking and statistics, as well as online transactions, without user knowledge, said Amit.

"It's very sophisticated," he said. "They are able to circumvent many of the security measures the banks have taken."

- Tags:
 - [Email Security](#)
 - [Mobile Endpoint Security](#)
 - [Government](#)
 - [Education](#)
 - [Finance](#)
 - [Analyst Reports & Industry Surveys](#)
 - [Emerging Threats](#)
 - [Lawbreakers & Cybercrime](#)
 - [Trojans](#)
 - [Phishing](#)
- Company:
 - [Finjan](#)

Ads by Google

כנס הפיסגה של ההיי-טק
כנס גרטנר השנתי. כל המגמות החדשות 22 מומחים, 37 הרצאות. לחץ להרשמה

www.gartner.co.il
Web Attacks: The Anatomy
SQL Injection: Knowledge is power Free white paper. No Commitment
www.breach.com
Trojan Computer Virus
Download Free Trojan & Spyware Scan Recommended & Used By The Experts
www.PCTools.com

- [This blog post](#)
- [All blog posts](#)

Subscribe to this blog post's comments through...

-  netvibes
-  newsgator
-  MY YAHOO!
-  Rojo
-  feedblitz

-  Pageflakes
-  Google
-  Bloglines
-  Windows Live

 [RSS Feed](#)

[Follow the discussion](#)
[Login](#)

Comments

[Close](#) **Login to an existing account**

Email:
Password:
[Use OpenID!](#)
[Forgot login? Login](#)

[Close](#) **Login with your OpenID**

OpenID URL:

[Back](#)
[Login](#)
[Dashboard](#) | [Edit profile](#) | [Logout](#)

- Logged in as

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

Post a new comment

Name * Email (track replies) Blog URL

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

Your OpenID *

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

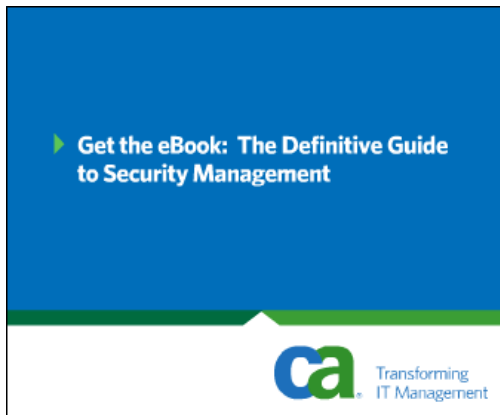
[Submit Comment](#)
[Or post using OpenID](#)
[Get better comments for your blog](#)

[Go to Intense Debate](#)
Related Directory Listings

Finjan

Listed under:

- [Anti-malware](#) > [Multi-Functional/Integrated Appliances](#)
- [Anti-malware](#) > [Network Security](#)
- [Patch management](#) > [Patch Management](#)
- [Anti-malware](#) > [Anti Adware/Spyware](#)
- [Anti-malware](#) > [Anti-Virus](#)



Most Popular

- [Adobe Flash threat widens, but patch is available](#)
- [Latest phishing schemes target Apple](#)
- [Exploits target new Adobe Flash bug](#)
- [Hackers strike Comcast website](#)
- [Streamlining compliance efforts in the health care industry](#)
- [Web TV network blames anti-P2P firm for DoS attack](#)
- [Californian indicted in \\$50,000 scam of E-Trade, Schwab.com](#)
- [Apple releases latest Leopard OS update](#)
- [Harvard professor accuses Zango of more deception](#)
- [DoJ combating health care fraud](#)

Most Emailed

- [Bank of New York Mellon loses data on 4.5 million](#)
- [Proliferating HIPAA complaints and medical record breaches](#)
- [It's heere: Windows XP Service Pack 3 released](#)
- [LendingTree sued over data breach](#)
- [Massive hacker server discovered](#)
- [Adobe Flash threat widens, but patch is available](#)
- [Counterfeit networking gear: A security threat?](#)
- [Major botnet infiltrated](#)
- [Personal info on six million Chileans posted](#)
- [Blame XP SP3 problems on Microsoft, Symantec says](#)

Most Recent

- [Researchers breach Microsoft's CardSpace ID technology](#)
- [Web TV network blames anti-P2P firm for DoS attack](#)
- [Californian indicted in \\$50,000 scam of E-Trade, Schwab.com](#)
- [Hackers strike Comcast website](#)
- [DoJ combating health care fraud](#)
- [Apple releases latest Leopard OS update](#)
- [Harvard professor accuses Zango of more deception](#)
- [Adobe Flash threat widens, but patch is available](#)
- [Latest phishing schemes target Apple](#)
- [Exploits target new Adobe Flash bug](#)



ESET NOD32 Antivirus
Business Edition

A scalable, end-point, security solution that proactively eliminates malware.

[Download a Free Trial >](#)



Featured White Papers

[State of Internet Security Report: Protecting Business Email](#)

Business dependence on email is greater than ever before and the volume of threats has spiked dramatically. For the SOIS...

[View Now](#)

[Extending Network Monitoring Tool Performance](#)

This paper explores how monitoring tools can achieve higher levels of performance without forklift upgrades. It proposes...

[View Now](#)

[Appliance Update Management](#)

Appliances are complex combinations of hardware and software that enterprises put into production environments to meet...

[View Now](#)

[Anti-Malware Battlefield Tools: Customer Perspectives and Reference RFI](#)

In this Methodologies and Best Practices document, Burton Group Research Director Daniel Blum recounts customer...

[View Now](#)

[Exchange 2007 Data Protection and Disaster Recovery](#)

In Quest's new white paper, learn how to implement a solid data protection, recovery, compliance and e-discovery...

[View Now](#)

[View More Research](#)

Popular Tags

[Analyst Reports & Industry Surveys](#) [Apple Threats Breaches & Exposures](#) [Browser Flaws](#) [Compliance](#) [Consumer Threats](#) [Education](#) [Email Security](#) [Emerging Threats](#) [Finance](#) [Government](#) [Healthcare](#) [High Tech](#) [Insider Threats](#) [IT Security](#) [Training](#) [Lawbreakers & Cybercrime](#) [Microsoft](#) [Non-Microsoft Patches](#) [Open Source](#) [Patch Management](#) [Patch Tuesday](#) [Phishing](#) [Privacy](#) [Regulation](#) [Spam](#) [Techniques](#) [Vulnerabilities & Flaws](#)

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.](#)

- [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.](#)

- [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.](#)

- [FTC investigations and penalties](#)

Date/Time: Tuesday, June 17, 2007 at 2:00 p.m. EST/11:00 a.m. PST

[Click to register for FREE](#)

How do you ensure that you don't fall victim to data thieves, which may lead to Federal Trade Commission (FTC) investigations and long-lasting penalties? We talk to experts about protecting critical data and learn more about FTC expectations and rules.

- [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.

- [Finding and Stopping the Invisible Threats](#)

Date/Time: Wednesday, June 25, 2007 at 2:00 p.m. EST/11:00 a.m. PST

[Click to register for FREE](#)

Organized crime rings and malicious insiders are using policy evasion technologies to establish invisible and covert connections to external dynamic DNS ranges or servers. These techniques reroute customers to rogue websites potentially exposing critical artifacts from within the organization. This webcast will review what is critically at stake for your organization and examine how companies found solutions to these tough network security problems by implementing NetWitness' extensible NextGen monitoring infrastructure and highly customizable analytic and alerting applications.

[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](#)