Using Honeyclients to Detect New Attacks

Kathy Wang
Syn Ack Labs
knwang@synacklabs.net

Overview

- What’s a honeyclient?
- Why honeyclients?
- How can honeyclients help?
- Design decisions
- Introducing world’s first open-sourced honeyclient
- Honeyclient architecture
- Deployment plans
- Arms race situations
- Legal liabilities
- Related projects
- How can you contribute?
- Acknowlegements

The one rule

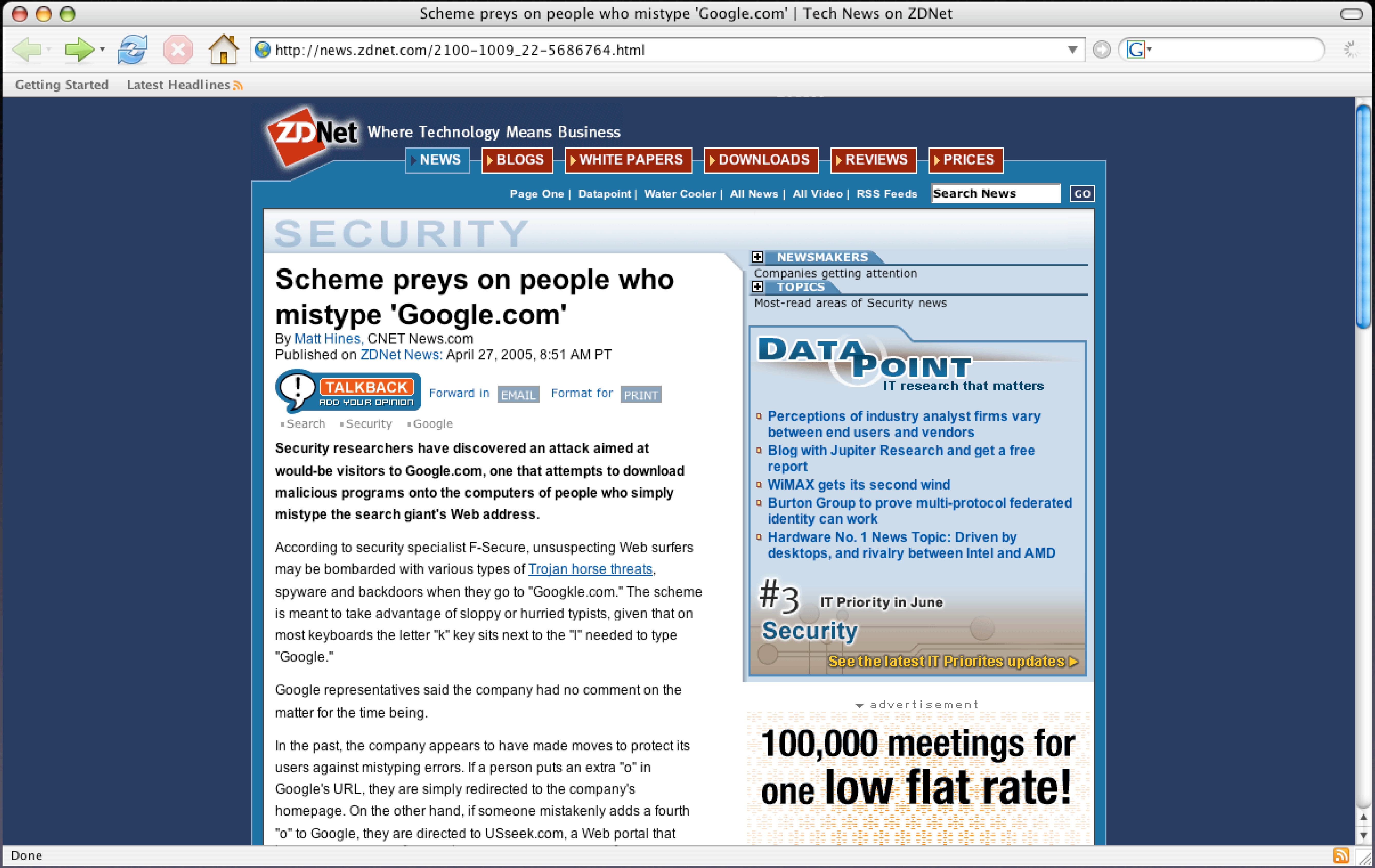
- Questions at end of talk, please

So, what’s a honeyclient?

- Opposite of a honeypot
- Drives client application to connect to servers
- Will gather data from malicious servers
- Started working on honeyclient last November
- World’s first open-sourced honeyclient released today

Client-side attacks are on the increase

April 2005


Scheme preys on people who mistype 'Google.com' | Tech News on ZDNet
http://news.zdnet.com/2100-1009_22-5686764.html
Getting Started
Latest Headlines
Done

ZDNet Where Technology Means Business

NEWS | BLOGS | WHITE PAPERS | DOWNLOADS | REVIEWS | PRICES

Page One | Datapoint | Water Cooler | All News | All Video | RSS Feeds | Search News | GO

SECURITY

Scheme preys on people who mistype 'Google.com'

By Matt Hines, CNET News.com
Published on ZDNet News: April 27, 2005, 8:51 AM PT

TALKBACK ADD YOUR OPINION Forward in EMAIL Format for PRINT

▪Search ▪Security ▪Google

Security researchers have discovered an attack aimed at would-be visitors to Google.com, one that attempts to download malicious programs onto the computers of people who simply mistype the search giant's Web address.

According to security specialist F-Secure, unsuspecting Web surfers may be bombarded with various types of Trojan horse threats, spyware and backdoors when they go to "Googkle.com." The scheme is meant to take advantage of sloppy or hurried typists, given that on most keyboards the letter "k" key sits next to the "l" needed to type "Google."

Google representatives said the company had no comment on the matter for the time being.

In the past, the company appears to have made moves to protect its users against mistyping errors. If a person puts an extra "o" in Google's URL, they are simply redirected to the company's homepage. On the other hand, if someone mistakenly adds a fourth "o" to Google, they are directed to USseek.com, a Web portal that

NEWSMAKERS
Companies getting attention

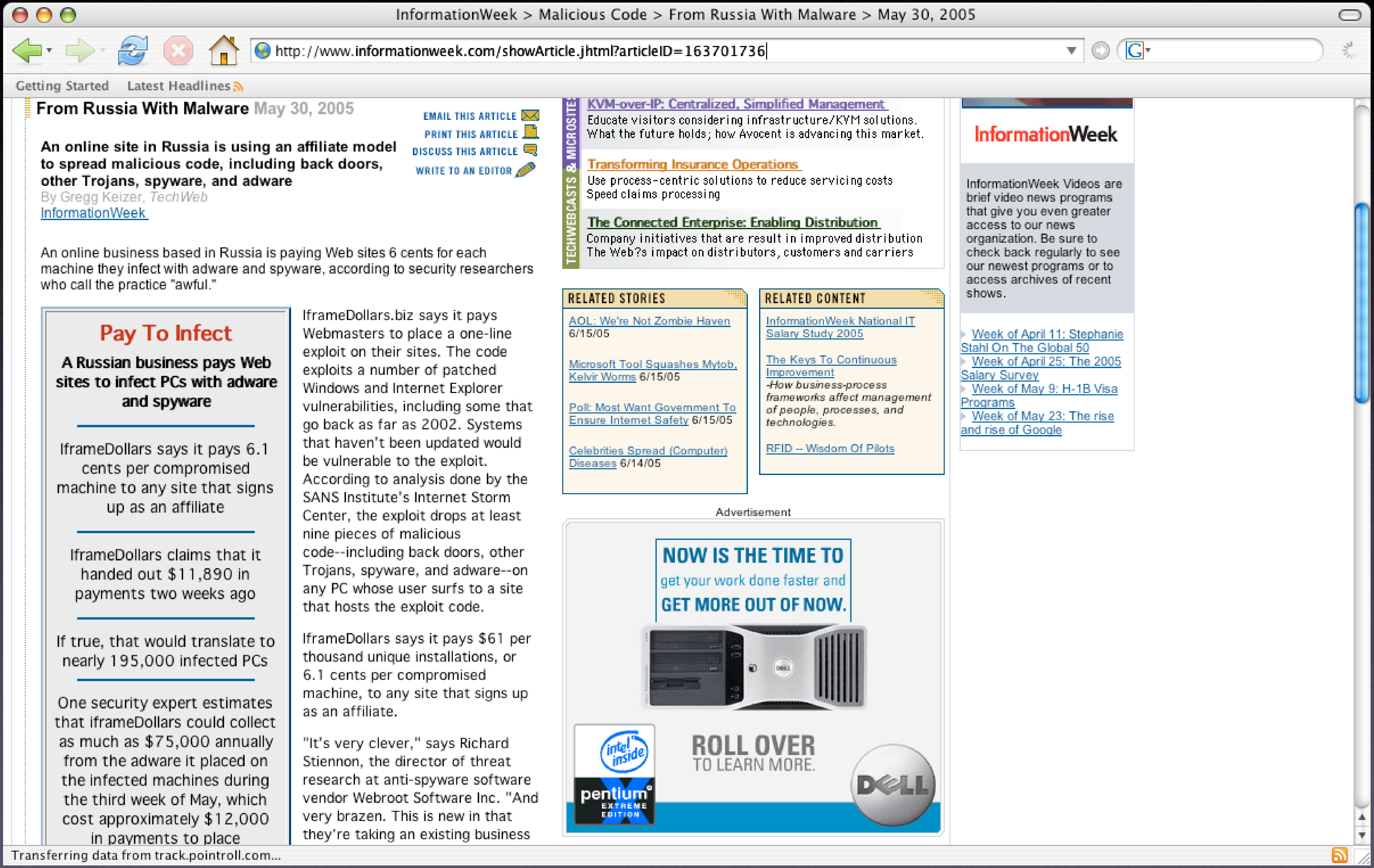
TOPICS
Most-read areas of Security news

DATA POINT IT research that matters

- Perceptions of industry analyst firms vary between end users and vendors
- Blog with Jupiter Research and get a free report
- WiMAX gets its second wind
- Burton Group to prove multi-protocol federated identity can work
- Hardware No. 1 News Topic: Driven by desktops, and rivalry between Intel and AMD

#3 IT Priority in June
Security
See the latest IT Priorites updates ▸

May 2005



InformationWeek > Malicious Code > From Russia With Malware > May 30, 2005

http://www.informationweek.com/showArticle.jhtml?articleID=163701736

From Russia With Malware May 30, 2005

An online site in Russia is using an affiliate model to spread malicious code, including back doors, other Trojans, spyware, and adware

By Gregg Keizer, *TechWeb*
InformationWeek

An online business based in Russia is paying Web sites 6 cents for each machine they infect with adware and spyware, according to security researchers who call the practice "awful."

Pay To Infect

A Russian business pays Web sites to infect PCs with adware and spyware

IframeDollars says it pays 6.1 cents per compromised machine to any site that signs up as an affiliate

IframeDollars claims that it handed out $11,890 in payments two weeks ago

If true, that would translate to nearly 195,000 infected PCs

One security expert estimates that iframeDollars could collect as much as $75,000 annually from the adware it placed on the infected machines during the third week of May, which cost approximately $12,000 in payments to place

IframeDollars.biz says it pays Webmasters to place a one-line exploit on their sites. The code exploits a number of patched Windows and Internet Explorer vulnerabilities, including some that go back as far as 2002. Systems that haven't been updated would be vulnerable to the exploit. According to analysis done by the SANS Institute's Internet Storm Center, the exploit drops at least nine pieces of malicious code--including back doors, other Trojans, spyware, and adware--on any PC whose user surfs to a site that hosts the exploit code.

IframeDollars says it pays $61 per thousand unique installations, or 6.1 cents per compromised machine, to any site that signs up as an affiliate.

"It's very clever," says Richard Stiennon, the director of threat research at anti-spyware software vendor Webroot Software Inc. "And very brazen. This is new in that they're taking an existing business

TECHWEBCASTS & MICROSITE

KVM-over-IP: Centralized, Simplified Management
Educate visitors considering infrastructure/KVM solutions.
What the future holds; how Avocent is advancing this market.

Transforming Insurance Operations
Use process-centric solutions to reduce servicing costs
Speed claims processing

The Connected Enterprise: Enabling Distribution
Company initiatives that are result in improved distribution
The Web?s impact on distributors, customers and carriers

RELATED STORIES

AOL: We're Not Zombie Haven 6/15/05

Microsoft Tool Squashes Mytob, Kelvir Worms 6/15/05

Poll: Most Want Government To Ensure Internet Safety 6/15/05

Celebrities Spread (Computer) Diseases 6/14/05

RELATED CONTENT

InformationWeek National IT Salary Study 2005

The Keys To Continuous Improvement
-How business-process frameworks affect management of people, processes, and technologies.

RFID -- Wisdom Of Pilots

Advertisement

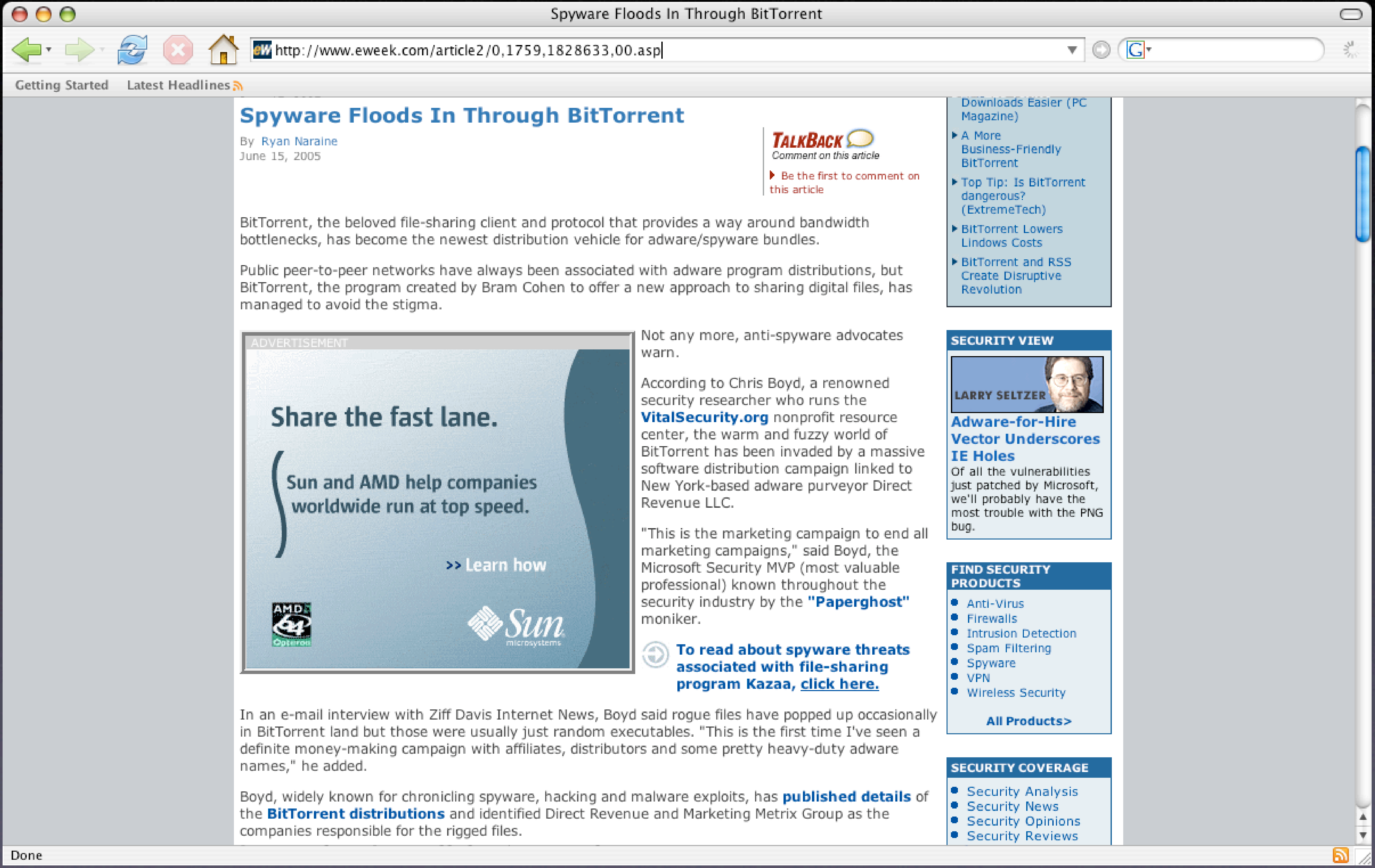
InformationWeek

InformationWeek Videos are brief video news programs that give you even greater access to our news organization. Be sure to check back regularly to see our newest programs or to access archives of recent shows.

- Week of April 11: Stephanie Stahl On The Global 50
- Week of April 25: The 2005 Salary Survey
- Week of May 9: H-1B Visa Programs
- Week of May 23: The rise and rise of Google

Transferring data from track.pointroll.com...

June 2005



Spyware Floods In Through BitTorrent
http://www.eweek.com/article2/0,1759,1828633,00.asp
Getting Started
Latest Headlines

Spyware Floods In Through BitTorrent

By Ryan Naraine
June 15, 2005

TALKBACK
Comment on this article
Be the first to comment on this article

BitTorrent, the beloved file-sharing client and protocol that provides a way around bandwidth bottlenecks, has become the newest distribution vehicle for adware/spyware bundles.

Public peer-to-peer networks have always been associated with adware program distributions, but BitTorrent, the program created by Bram Cohen to offer a new approach to sharing digital files, has managed to avoid the stigma.

Not any more, anti-spyware advocates warn.

According to Chris Boyd, a renowned security researcher who runs the **VitalSecurity.org** nonprofit resource center, the warm and fuzzy world of BitTorrent has been invaded by a massive software distribution campaign linked to New York-based adware purveyor Direct Revenue LLC.

"This is the marketing campaign to end all marketing campaigns," said Boyd, the Microsoft Security MVP (most valuable professional) known throughout the security industry by the **"Paperghost"** moniker.

To read about spyware threats associated with file-sharing program Kazaa, click here.

In an e-mail interview with Ziff Davis Internet News, Boyd said rogue files have popped up occasionally in BitTorrent land but those were usually just random executables. "This is the first time I've seen a definite money-making campaign with affiliates, distributors and some pretty heavy-duty adware names," he added.

Boyd, widely known for chronicling spyware, hacking and malware exploits, has **published details** of the **BitTorrent distributions** and identified Direct Revenue and Marketing Metrix Group as the companies responsible for the rigged files.

Downloads Easier (PC Magazine)
- A More Business-Friendly BitTorrent
- Top Tip: Is BitTorrent dangerous? (ExtremeTech)
- BitTorrent Lowers Lindows Costs
- BitTorrent and RSS Create Disruptive Revolution

SECURITY VIEW

LARRY SELTZER

Adware-for-Hire Vector Underscores IE Holes

Of all the vulnerabilities just patched by Microsoft, we'll probably have the most trouble with the PNG bug.

FIND SECURITY PRODUCTS

- Anti-Virus
- Firewalls
- Intrusion Detection
- Spam Filtering
- Spyware
- VPN
- Wireless Security

All Products>

SECURITY COVERAGE

- Security Analysis
- Security News
- Security Opinions
- Security Reviews

Done

July 2005 and beyond

What’s next???

How will honeyclients help?

- Allows proactive monitoring of malicious servers
- This can be extended beyond just HTTP clients
    - Any other client-server based protocol will work

Design decisions

- Low interaction vs high interaction honeyclient
  - Low interaction -> WGET
  - High interaction -> Actually drive client
- How often to do integrity checks
- How to pull info from clients
  - For IE, could not get URLs out of cache file (binary file)
  - So, proxy implementation was used

World’s first open-sourced honeyclient

- BSD-licensed
- Runs on Windows 2K/XP
- Drives Internet Explorer
- Two Perl scripts
  - driver.pl
  - proxy.pl

Integrity checks

- Baselining of host files and registries
- Files are MD5 hashed
- Check files and registries after each URL is completely accessed
- Would like to check memory as well
  - Future feature (idea thanks to Thorsten Holz)

Testing 1, 2, 3

- Tried to get one-line exploit code from Russian site
- Which sites are malicious?
  - Surprisingly, not the pr0n sites
  - Also, not the drug sites
- We know very little about malicious sites
  - So, where are they?
  - What exactly do they do?

Honeyclient deployment plan

- The more people use honeyclients, the better
  - More unique data points to analyze
  - Perhaps implements a SETI@home like distributed info gathering architecture?
- Share findings with security community
- Have honeyclients deployed in different locations
  - Prevent malicious servers from blocking one address

ToDo

- Integrity check for memory space
- Have honeyclient send logs to Linux host
  - Protect against file deletion when honeyclient virtual host infected
- Signatures database
- Distributed data sharing a la SETI@home
- More protocol support
  - FTP, DNS, P2P, etc

Possible arms races

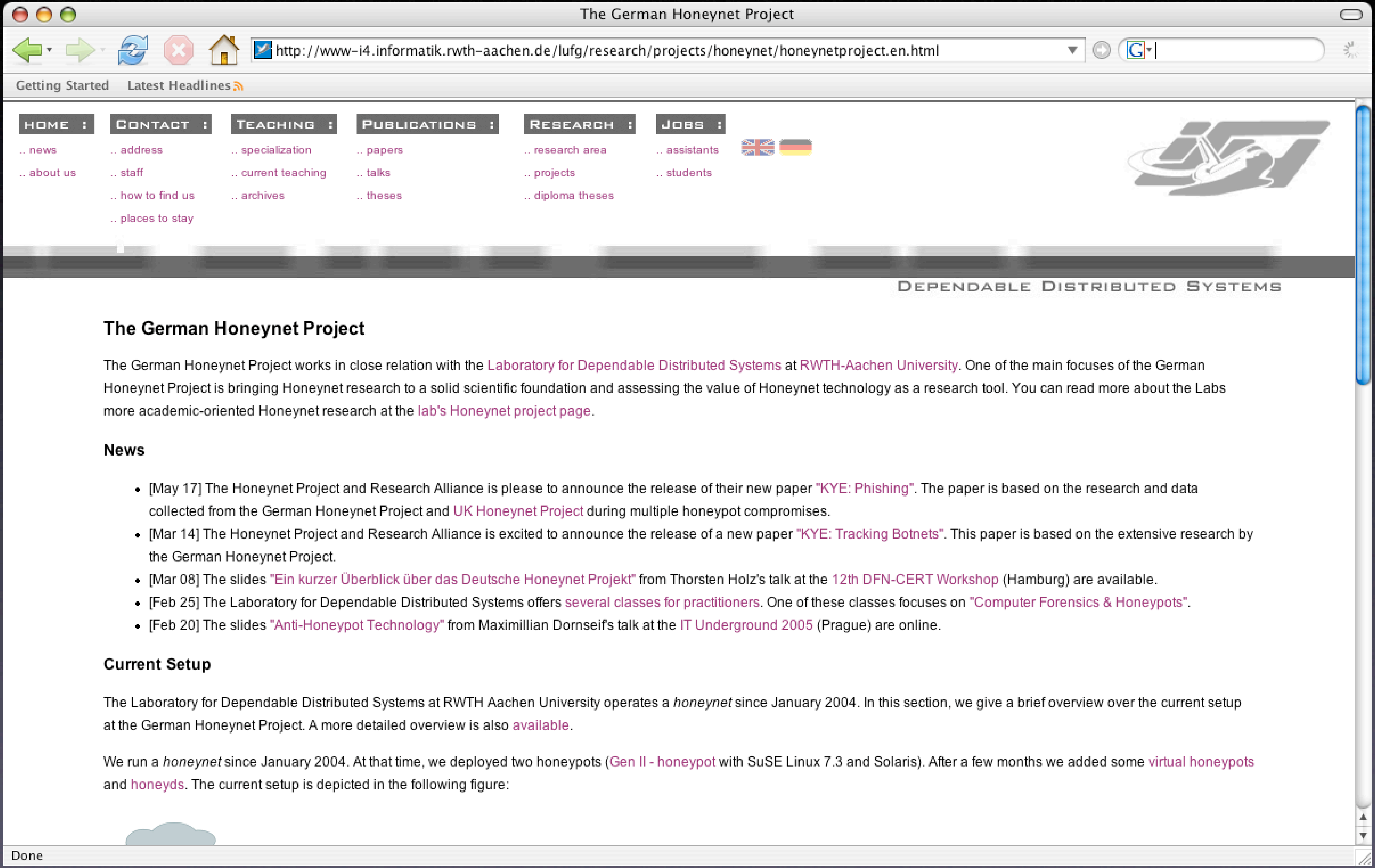
- Web bugs
- Color-on-color URLs
- Robots.txt files
- Order URLs are accessed
- Timing of URL access
- Flash sites

Legal Liabilities?

- Need to limit outbound traffic (cripples malware)
  - Honeypots face same problem
- Accidentally causing damage to innocent sites
  - Same liability as spidering technology
- Need to ensure future distributed deployments do not DoS sites being accessed
- So, honeyclients have combined liabilities of both honeypots and spiders

Related Projects

German Honeynet Project



The German Honeynet Project

The German Honeynet Project works in close relation with the Laboratory for Dependable Distributed Systems at RWTH-Aachen University. One of the main focuses of the German Honeynet Project is bringing Honeynet research to a solid scientific foundation and assessing the value of Honeynet technology as a research tool. You can read more about the Labs more academic-oriented Honeynet research at the lab's Honeynet project page.

News

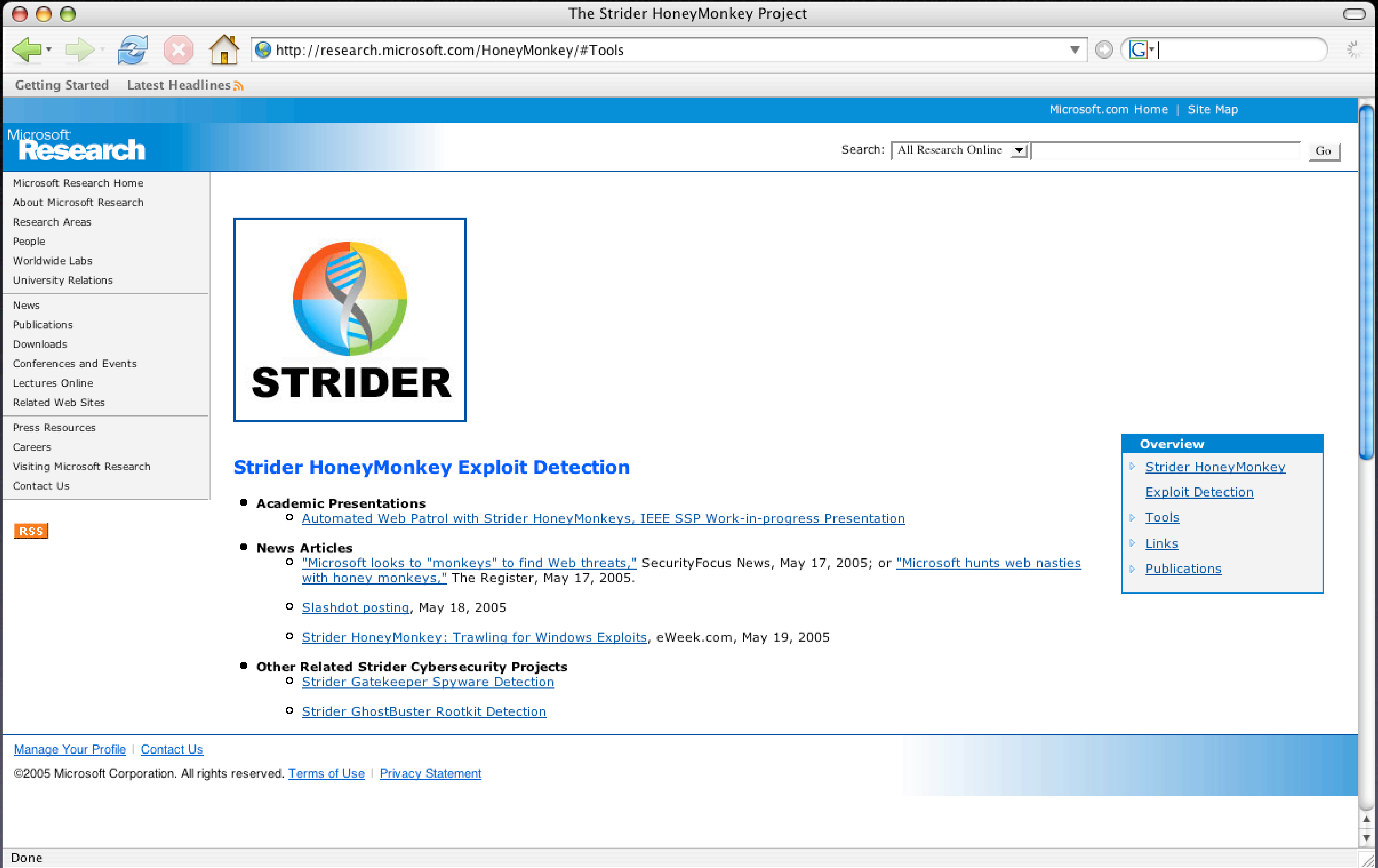
- [May 17] The Honeynet Project and Research Alliance is please to announce the release of their new paper "KYE: Phishing". The paper is based on the research and data collected from the German Honeynet Project and UK Honeynet Project during multiple honeypot compromises.
- [Mar 14] The Honeynet Project and Research Alliance is excited to announce the release of a new paper "KYE: Tracking Botnets". This paper is based on the extensive research by the German Honeynet Project.
- [Mar 08] The slides "Ein kurzer Überblick über das Deutsche Honeynet Projekt" from Thorsten Holz's talk at the 12th DFN-CERT Workshop (Hamburg) are available.
- [Feb 25] The Laboratory for Dependable Distributed Systems offers several classes for practitioners. One of these classes focuses on "Computer Forensics & Honeypots".
- [Feb 20] The slides "Anti-Honeypot Technology" from Maximillian Dornseif's talk at the IT Underground 2005 (Prague) are online.

Current Setup

The Laboratory for Dependable Distributed Systems at RWTH Aachen University operates a *honeynet* since January 2004. In this section, we give a brief overview over the current setup at the German Honeynet Project. A more detailed overview is also available.

We run a *honeynet* since January 2004. At that time, we deployed two honeypots (Gen II - honeypot with SuSE Linux 7.3 and Solaris). After a few months we added some virtual honeypots and honeyds. The current setup is depicted in the following figure:

Microsoft HoneyMonkey Project



Strider HoneyMonkey Exploit Detection

- **Academic Presentations**
  - Automated Web Patrol with Strider HoneyMonkeys, IEEE SSP Work-in-progress Presentation
- **News Articles**
  - "Microsoft looks to "monkeys" to find Web threats," SecurityFocus News, May 17, 2005; or "Microsoft hunts web nasties with honey monkeys," The Register, May 17, 2005.
  - Slashdot posting, May 18, 2005
  - Strider HoneyMonkey: Trawling for Windows Exploits, eWeek.com, May 19, 2005
- **Other Related Strider Cybersecurity Projects**
  - Strider Gatekeeper Spyware Detection
  - Strider GhostBuster Rootkit Detection

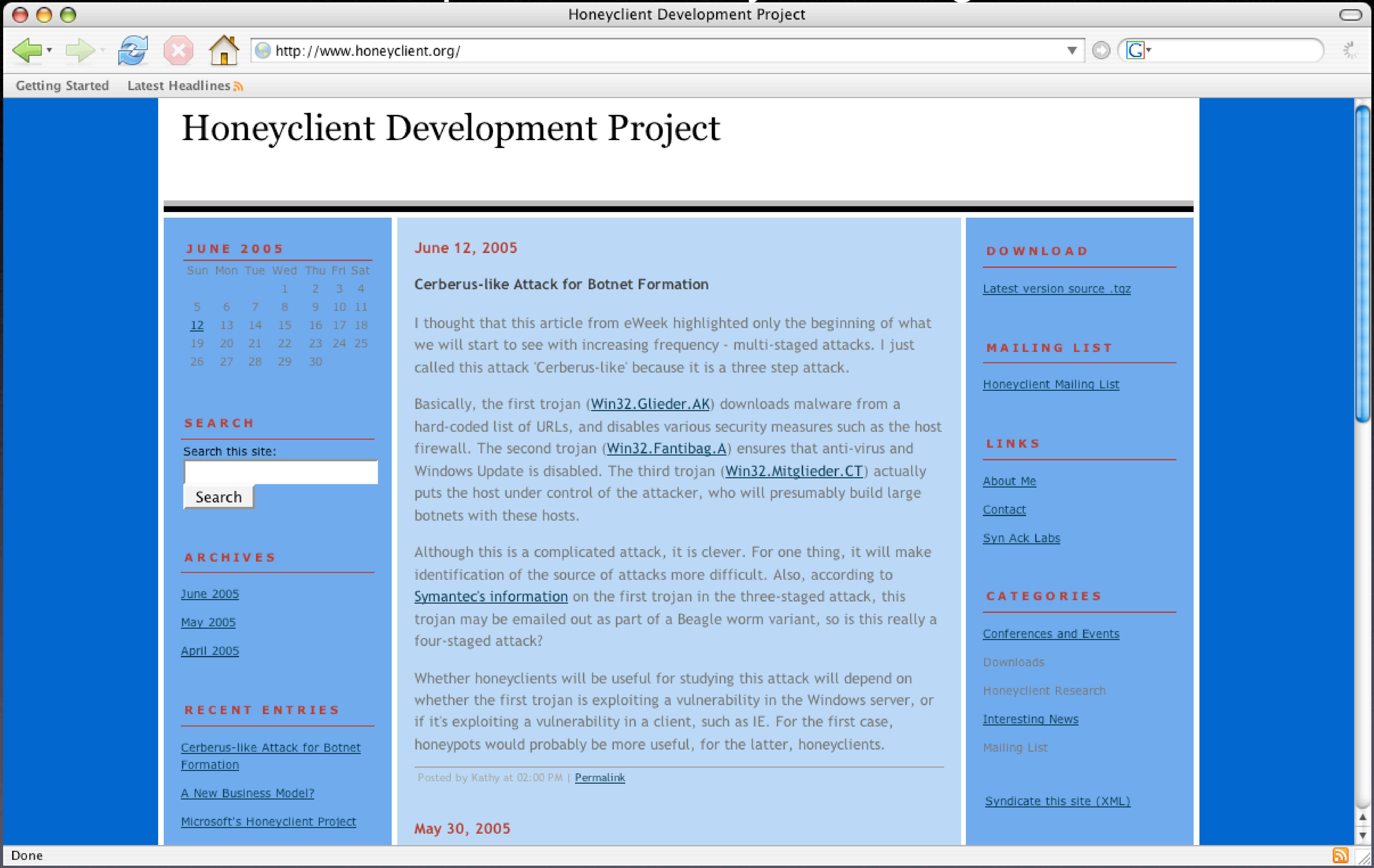
Manage Your Profile | Contact Us

Interesting link...

```
131.107.0.79 - - [03/Jun/2005:16:55:57 -0400] "GET /en/s/kwang.html
HTTP/1.1" 304 0 "http://msrweb/strider/webpatrol/honeymonkey/"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; ESB
{15228BCE-4E47-4A11-82B2-0406FD52D429}; .NET CLR 1.1.4322)"
```

Interested in Contributing?

Honeyclient Development Project Page
http://www.honeyclient.org/



Honeyclient Development Project

JUNE 2005

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

SEARCH

Search this site:

Search

ARCHIVES

June 2005

May 2005

April 2005

RECENT ENTRIES

Cerberus-like Attack for Botnet Formation

A New Business Model?

Microsoft's Honeyclient Project

June 12, 2005

Cerberus-like Attack for Botnet Formation

I thought that this article from eWeek highlighted only the beginning of what we will start to see with increasing frequency - multi-staged attacks. I just called this attack 'Cerberus-like' because it is a three step attack.

Basically, the first trojan (Win32.Glieder.AK) downloads malware from a hard-coded list of URLs, and disables various security measures such as the host firewall. The second trojan (Win32.Fantibag.A) ensures that anti-virus and Windows Update is disabled. The third trojan (Win32.Mitglieder.CT) actually puts the host under control of the attacker, who will presumably build large botnets with these hosts.

Although this is a complicated attack, it is clever. For one thing, it will make identification of the source of attacks more difficult. Also, according to Symantec's information on the first trojan in the three-staged attack, this trojan may be emailed out as part of a Beagle worm variant, so is this really a four-staged attack?

Whether honeyclients will be useful for studying this attack will depend on whether the first trojan is exploiting a vulnerability in the Windows server, or if it's exploiting a vulnerability in a client, such as IE. For the first case, honeypots would probably be more useful, for the latter, honeyclients.

Posted by Kathy at 02:00 PM | Permalink

May 30, 2005

DOWNLOAD

Latest version source .tgz

MAILING LIST

Honeyclient Mailing List

LINKS

About Me

Contact

Syn Ack Labs

CATEGORIES

Conferences and Events

Downloads

Honeyclient Research

Interesting News

Mailing List

Syndicate this site (XML)

Honeyclient Mailing List

- honeyclient-subscribe@synacklabs.net

Acknowledgments

- Todd MacDermid
- Thorsten Holz
- JD Durick
- Jack Whitsitt

Questions?