

Quest® STRATEGIC ADVISOR

www.questsys.com

Quest | SECURITY ALERT

Stealth Malware Dangers Loom in 2011 for Every Business

About a year ago, a routine enterprise security analysis turned up 75 gigabytes of stolen data. Thus began the discovery of the 'Kneber botnet', which had hijacked 74,000 computers at more than 2,500 organizations around the world.

Operating undetected for a year, the Kneber botnet's 74,000 'zombies' managed to steal some 68,000 corporate logins to e-mail accounts, online banking accounts, and a variety of public email and social networking sites.

It also grabbed nearly 2,000 SSL certificate files used to secure the likes of online banking transactions.

Sight unseen

Why was this botnet able to steal so much for so long? Because less than 10% of antivirus software could recognize the sophisticated Kneber malware. Nor was it spotted by existing intrusion detection systems.

"That's the whole idea of stealth malware," says Tim Burke, President and CEO of Quest. "Cybercriminals don't want people to know what's being done to them. Our own

experience shows that as many as fifty to sixty percent of the organizations infected like this don't even understand it's happening."

property – and then sell it all to the highest bidder.

"The bad guys are looking at IP addresses," explains Tim. "They don't care about the size or nature of your business. They scan all the time with automated bots, and if they find a vulnerability, the bot breaks in and deposits its malware, which seeks out the types of information it's been designed to grab – social security numbers, credit card numbers, competitive data, customer lists, and so on."

There are some five million spam-sending botnets now. They control 50 million to 100 million PCs worldwide, say analysts, and accounted for more than three-quarters of all

MALWARE DANGERS 2011 (Cont. on p.2)



THE BOTTOM LINE

The odds are greater than ever that your business will suffer a malware attack in 2011 – and without the right protection, you probably won't know until it costs you plenty.

A malware pandemic that's getting worse

Malware has become pandemic and no one is immune from infection. Today malware feeds a multi-billion dollar industry that uses systematic, coordinated campaigns to steal computing resources, identities, and intellectual

IN THIS ISSUE

Why 2011 may become the year of stealth malware

2 From Tim Burke: Beware: We're All Targets

3 Profile: Quest's New Malware Protection System

3 Did You Know? Glimpsing the Dark Side of Creativity

4 What's New... Malware in 2011

MALWARE DANGERS 2011 (Cont. from p. 1)

spam in 2010. Besides launching distributed denial-of-service (DDOS) attacks, they're increasingly used to exploit all manner of yet-to-be-recognized zero-day vulnerabilities in popular applications as well as mobile devices and even programmable logic controllers.

Malware solutions that work

"I have no doubt we'll see more complex botnet attacks in 2011," says Mike Dillon, Quest's Chief Technology Officer. "As businesses migrate to Software-as-a-Service, they'll have to open up more to the Internet. And that will significantly increase the chances of their systems being compromised."

Mike estimates that the number of infected sites is growing by 20% to 25% a year. "If your company is shifting more toward cloud services and hasn't addressed security, you *will* be attacked," he predicts.

Sadly, the traditional protections businesses have implemented in the past — OS patch management, good firewall practices, intrusion detection/prevention, and antivirus updates — are no longer sufficient to stave off today's and tomorrow's malware.

That's why Quest now offers its Malware Protection System in partnership with malware protection provider FireEye, whose multi-stage inspection solution combines heuristic analysis and deep packet inspection within instrumented virtual machines.

Next-generation threat prevention

"There has to be a coordinated solution that offers the ability to detect zero-hour malware, stop known attacks, and block the outbound callbacks of previous infections," notes Jeff Williams, Vice President of Sales & Business Development at FireEye. "Integrating inbound and outbound blocking protects against data exfiltration and the

FROM TIM BURKE...

Beware: We're All Targets

A hospital administrator told me recently that he'd been informed by his IT team not to put in too many security defenses because this would attract hackers.

Rationale: The more you give hackers something to crack, the more they'll want to have a go at you.

Unfortunately, hackers looking for a challenge are no longer the real threat. Cybercrime is a mega business worth billions. These folks aren't doing it for bragging rights. They want data they can sell, like social security numbers, customer databases, company credit cards, the health records of employees — information every business has on hand.

Better than nothing

To his credit, the hospital administrator actually had a security policy: Don't do too much in the way of security.

Foolhardy, yes — but at least he'd thought about what his security policy should include. Which is more than can be said for too many CEOs and CFOs, especially at small/medium-sized companies.

I think the single most preventable misstep CEOs and CFOs make regarding security is not talking about what they want to protect.

I'm not referring to a conversation about how to protect the data — that's for technical folks. I mean a higher-level conversation about what should be protected, who should have access.

If you're not comfortable starting a security policy conversation, get help from a trusted partner. Do it now. In this new world of stealth malware, every company is a target.



long-term compromise of critical customer systems."

That's not all. "Businesses need to couple threat prevention technologies with easy-to-use policy management tools," Jeff believes. "Next-generation threat prevention systems like FireEye's need to be complemented by security information management software and next-generation gateways that manage Web application and firewall access rules as well as URL policies."

And, most importantly, behind all these tools is the security policy itself.

"Security isn't just a technical issue," says Tim. "C-level people must be the ones who decide what's valuable to the organization and how that value should be protected. Once those decisions are made, an organization can rely on a trusted Managed Services partner to devise the ongoing protections needed to do business without being victimized by cybercriminals."

Quest's Malware Protection System:

Managed Real-time Malware Protection You Can Afford

Never before has malware posed such an extreme threat to even mid-sized and small organizations.

Fortunately, Quest knows how to plug the gap in conventional network security exposed by recent zero-day malware exploits that use stealth tactics — such as embedding attacks in PDF documents, placing malicious code on web pages, or playing on undiscovered application and operating system vulnerabilities.

Real-time protection from zero-day attacks

Quest's Malware Protection System (MPS) appliance from FireEye provides a whole new level of security that prevents theft of information and resources.

Using an advanced multi-phase analysis engine, MPS dynamically learns new *unknown* vulnerabilities, exploits, and techniques *in real time* so it can accurately block malware without the hassles of tuning to quell false positives.

Low-cost enterprise-class protection

MPS serves as an enterprise-class security gateway that's deployed at an organization's Internet egress point to capture suspicious traffic, analyze it with advanced heuristics, confirm it using virtual-machine replay, block it, terminate any malicious outbound communications, and then track those outbound communications to their criminal source.

Intelligence gathered from FireEye appliances is shared globally so appliances can stay updated about the latest bots, trojans, and advanced, persistent threats.

Quest Managed Security Services: Always Tailored to Your Needs

Quest offers a comprehensive portfolio of Managed Security Services that are designed to be tailored to each client's specific needs.

- Security Posture Assessment and Client VPN Design services help you shape and maintain the security you need.
- Site-to-Site VPN, Intrusion Detection, Wireless Intrusion Prevention, Firewall, Patch Management, Vulnerability Scanning, Email and OS Antivirus, SPAM Filtering, Web Filtering, and HTTP Malicious Code Filtering services keep your organization and its data protected 24/7.
- Enterprise Reporting and Event Correlation services ensure you get the feedback you need.
- Response Team services enable you to quickly recover from any breaches.

Quest can install and manage the Malware Protection System for as little as \$795 per month. And, of course, Quest always makes sure its MPS plays well with its other Managed Security Service offerings.

DID-YOU-KNOW?

Glimpsing the Dark Side of Creativity

Every quarter, Cisco issues a *Global Threat Report* describing its encounters with security threats. The most recent report, 3Q10*, should raise the eyebrows of anyone who thinks bad things happen only to other people (or companies). Here's why:

- Roughly 10% of all third-quarter web malware was encountered through search engine traffic.
- Enterprise users experienced an average of 133 web malware encounters per month in the third quarter of 2010.
- Less than two-thirds of web-based malware encounters were blocked prior to exploit code; the three most common exploits targeted Adobe Reader/Acrobat, Sun Java, and Adobe Flash.

- Third-quarter email spam ruses included links disguised as a PDF that actually pointed to a copy of a worm, a spoofed LinkedIn email, and the 'Here You Have' email, which garnered 79% of its clicks in its first three hours.
- The Stuxnet botnet, which exploits a vulnerability in Windows' print spooler, accounted for more than 5% of third-quarter events handled by Cisco's Remote Operations Service; this pales beside the Rustock botnet, which was responsible for 21% of third-quarter events.
- Four types of SQL injection attacks — which use malformed SQL statements to control SQL servers, alter database contents, extract SQL data, etc. — kept Cisco busy in the third quarter.

*http://www.cisco.com/en/US/prod/collateral/vpndevc/3q10_cisco_threat.pdf

IN THE MEDIA ROOM

Visit <http://www.questsys.com/media.aspx> for:

VIDEOS

NEW VIDEO! Service Delivery Centers: Find out about Quest's several Service Delivery Centers – and watch as we focus in particular on Quest's Business Resumption Center, strategically located at one of California's most seismically stable and secure locations. We'll show you why you can count on Quest when you're looking for the ultimate in disaster preparedness.

Who We Are: Colleagues describe achieving business systems success with Quest's help.

Data Security Video: Hear direct from the FBI, security experts, and your peers about in-depth security issues and how Quest can help protect your company.

Business Continuity Planning/Disaster Recovery: More than 25% of businesses damaged by natural and/or man-made disasters never recover. Ensure your future.

Video overview of our Infrastructure Services: Wireless, Broadband, Fiber-optics, Fiber Splicing, Infrastructure Cabling, and more.

PODCASTS

QUEST ON THE RADIO: Download the podcast on Quest's Threat Review Process.

PCI Compliance podcast: Join (Co-Hosts) Scott Draughon (My Technology Lawyer) and Oliver Rist (InfoWorld) as they interview Mike Dillon (Quest CTO) and Jon Bolden (Quest Director of Professional Services) about PCI (Payment Card Industry) compliance.

NEWSLETTERS:

Get current and back issues of our popular newsletter.

Manage your Newsletter subscription.

Let us know how you want your newsletter sent at

<http://www.questsys.com/SANpreference.aspx>

Choose hard copy via USPS or the electronic version through your email.

FROM THE QuestCatalog.com

Discover where the HOT DEALS are and which PRODUCTS are TOP SELLERS.

Check it out at www.Questcatalog.com

Coming in the next issue of *Quest Strategic Advisor*:
The Virtues of Virtualization

What's New...

A from-the-helicopter look at emerging malware trends comes from the Symantec MessageLabs Intelligence 2010 Annual Security Report*:

- The proportion of spam sent from botnets accounted for more than 77% of all spam in 2010. In 2011, botnets will employ steganography techniques – so their commands will be hidden in images, music files, social networking sites, etc., thus eliminating the need for a host botnet ISP.
- Each of the world's five million botnets sent 77 spam emails per minute in 2010 (that means malware in about one in 284 emails), and more than 339,000 malware strains have been identified in blocked emails. In 2011, targeted attacks will become more diverse, and efforts to profile specific job titles will become more sophisticated and effective.
- The average number of websites blocked each day as malicious rose to 3,188 in 2010 (29% higher than 2009); almost 90% of them were compromised legitimate domains. In 2011, more malware will identify and compromise legitimate websites that will see higher than usual traffic due to current events, like the World Cup. Also, expect cybercriminals to exploit router vulnerabilities in order to re-route traffic for malicious intent before sending it on to legitimate sites.

*http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf

Quest STRATEGIC ADVISOR

Publisher: Tim Burke
Editor: Barbara Klide

Contact the editor at
barbara_klide@questsys.com

All contents copyright © 2011 by Quest Media & Supplies, Inc, unless otherwise noted. *Quest Strategic Advisor* is published bimonthly by Quest Media & Supplies, Inc. Information contained in this newsletter is believed to be reliable but cannot be guaranteed to be complete or correct. Quest Media & Supplies, Inc. assumes no liability for any use of this newsletter and/or the information or opinions it contains. *Quest Strategic Advisor* and questsys.com are trademarks of Quest Media & Supplies, Inc. Other product, service, and company names mentioned herein may be servicemarks, trademarks, or registered trademarks of their respective holders. To the best of Quest's knowledge, cited data and research findings belong to the organizations to which they are attributed and Quest Media & Supplies, Inc. asserts no claim to them. Quest® is a Registered Trademark of Quest Media & Supplies, Inc.



Dilbert.com DilbertCartoonist@gmail.com



10-14-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.



DILBERT: © Scott Adams/Dist. by United Feature Syndicate, Inc.