AVIRA
Mehr als Sicherheit

IT-Sicherheit im täglichen Kampf gegen das Cybercrime - unsere neuesten Waffen und ihre Wirkungen

Michael Witt, Territory Manager

Jens Freitag, Business Line Manager Corporate Products

Köln, 03. Februar 2010

AVIRA
Mehr als Sicherheit

WEB 2.0

Blogs

File-Sharing-Programme

Feed Reader

Office online

WEB 2.0

Social Software Dienste

VoiP

AJAX-Anwendungen

Twittern

Wikis

Online-Datenbanken

Instant Messaging

Personal Webspace

AVIRA
Mehr als Sicherheit

Neue Bedrohungen erfordern neue Lösungen

- Angriffe auf Unternehmen und User werden zielgerichteter
- Motivation hinter den Angriffen ist Geld
- Kombinationen von unterschiedlichen Bedrohungen
- Neben Attacken via E-Mail neue Wege, an Daten von Unternehmen und Usern zu gelangen

AVIRA
Mehr als Sicherheit

Welche Möglichkeiten bietet Web 2.0 für potenzielle Angreifer

- Cross Site Scripting
- Übernahme von Webservern durch SQL Injection
- Umleiten von Inhalten durch manipulierte iFrames
- Ausnutzen von Fehlern in eingebetteten Applikationen

AVIRA
Mehr als Sicherheit

Ausnutzen von Fehlern in eingebetteten Applikationen

- Verteilung des Storm Worm über YouTube
- Javascript Würmer in Orkut, Facebook und anderen Social Network Portalen
- Ausnutzung von Sicherheitslücken in Adobe Flash und PDF
- Ausnutzung von Sicherheitslücken in Browsern und Add-Ons, z.B. Java Script (Heap Spraying)

AVIRA
Mehr als Sicherheit

Heap Spraying

- Die Ausnutzung von Pufferüberläufen
- Dabei gelingt es einem Angreifer, einer Applikation eigenen Maschinencode unterzujubeln und ihn mit deren Rechten zur Ausführung zu bringen.

- Definition (http://en.wikipedia.org/wiki/Heap_spraying):
  - **In computer security, heap spraying is a technique used in exploits to facilitate arbitrary code execution. The term is also used to describe the part of the source code of an exploit that implements this technique. In general, code that *sprays the heap* attempts to put a certain sequence of bytes at a predetermined location in the memory of a target process by having it allocate (large) blocks on the process' heap and fill the bytes in these blocks with the right values. They commonly take advantage from the fact that these heap blocks will roughly be in the same location every time the heap spray is run.**

AVIRA
Mehr als Sicherheit

Malware trends 2009

AVIRA
Mehr als Sicherheit

Malware Bedrohungen 2009

- verstärkter Angiff mit **Drive-by-Downloads**
- neben Web auch internetfähige Handys und Online-Dienste, spezialisiert auf die zentrale Datenhaltung
- weniger ausnutzbare Schwachstellen in gängiger Software, aber intensivere, schnellere Ausnutzung von Sicherheitslücken, um Schadcodes zu installieren.

- Hacker: statt unpersönliche Spam-Mails zunehmend sehr individuell gestaltete Nachrichten

- Schädlinge sind oftmals mit Rootkits versehen, um Malware zu verstecken, derartige Schadcodes kommen häufiger vor als sog. polymorphe Datei-Infektoren und bringen Spionagefunktionen zum Ausspähen von z.B. Bankdaten mit.

  - polymorphen Schädlinge: *Webserver verändert sie schon bei Auslieferung bzw. Download ein wenig. Dadurch nicht erkennbar für Virenscanner, die Dateien nur auf einfache Erkennungsmerkmale hin untersuchen.*

(Vgl.: http://www.avira.de/en/company_news/malware_trends_for_2009.html)

CALL FOR ENTRIES

CIO100

23RD ANNUAL AWARDS COMPETITION

Deadline: Feb. 5, 2010

CIO

White Papers | Webcasts | Solution Centers | Podcasts | IT Jobs | Council | Events | Magazine | Newsletters | RSS

NEWS | ANALYSIS | BLOGS | SLIDESHOWS | VIDEOS | HOW TO

DRILLDOWNS: Applications | Careers | Cloud Computing | Data Center | Mobile | Operating Systems | Security | Virtualization | Web 2.0 | More

Drilldown | Security | News

Phishing Scam Targets Users of Adobe PDF Reader

A new phishing scam is trying to fool people into thinking it comes from Adobe, announcing a new version of PDF Reader/Writer.

By Ellen Messmer — Leave a comment

THU, JANUARY 28, 2010 — Network World — A new phishing scam is trying to fool people into thinking it comes from Adobe, announcing a new version of PDF Reader/Writer. The message is making its way into e-mail boxes today, and the real Adobe urged any recipients to simply delete it.

11 security companies to watch

The phishing scam has a subject line "download and upgrade Adobe PDF Reader – Writer for Windows," includes a fake version of Adobe's logo and provides links that would lead to malicious code or other trouble if a victim clicked on them. The e-mail appears to come from Adobe newsletter@pdf-adobe.org, which is part of the scam.

"It has come to Adobe's attention that e-mail messages purporting to offer a download of the Adobe Reader have been sent by entities claiming to be Adobe," the company said in a statement warning about it. "Many of these e-mails are signed as 'Adobe PDF' (or similar), and in some instances require recipients to register and/or provide personal information. Please be aware that these e-mails are phishing scams and have not been sent by Adobe or on Adobe's behalf."

The real Adobe Reader download page is on the Adobe Web site at http://get.adobe.com/reader/.

COMMENTS | Print | LinkedIn

Originally published on www.networkworld.com. Click here to read the original story.

Security

More from IT Drilldown — « Back to Security

Articles

- FBI Arrests Alleged Cable Modem Hacker
- Chrome Apes IE8, Adds Clickjacking, XSS Defenses
- Phishing Scam Targets Users of Adobe PDF Reader
- US House Leaders Ask for Investigation Into Hackings
- When Standards Bodies Are the Cyber Threat
- Advance-Fee Fraud Scams Rise Dramatically in 2009
- DDoS Attacks, Network Hacks Rampant in Oil and Gas Industry, Other Infrastructure Sectors
- Malware Aims to Evade Windows 7 Safeguards

More Articles »

Mobile Security ABCs

Get up to speed on mobile security. Learn More »

Security Newsletter

Receive the latest security news as it breaks.

SIGN UP »

COMPUTERWORLD OSBC

March 17-18, 2010
Open Source Business Conference

Leveraging Open Source through the Enterprise and Beyond the Firewall

Register Today!

Security MarketSpace

Insight from an Auditor: Ensuring a Successful PCI Audit

Assess Your Data Loss Exposure

IBM ISS X-Force Threat and Risk Report
Read this Trend and Risk report from IBM® ISS X-Force® to learn statistical information about all aspects of threats that affect Internet security, including software vulnerabilities and public exploitation, malware, spam, phishing, web-based threats, and general cyber criminal activity. Learn more »

The Tangled Web: Silent Threats & Invisible Enemies
Learn how a hosted web security and content filtering service intercepts all types of web-borne attacks. Learn more »

Death to PST Files
Learn how a hosted archiving solution enables an enterprise to manage the huge volume of messages, guard against data loss and comply with document-retention regulations. Learn more »

The IT Manager's Guide to Compliance
Learn how to navigate eDiscovery challenges imposed by North American courts and regulations in this MessageLabs white paper. Learn more »

Enforce Your Email and Web Acceptable Usage Policies
Download this guide and learn how to deploy

M

erheit

09/en/

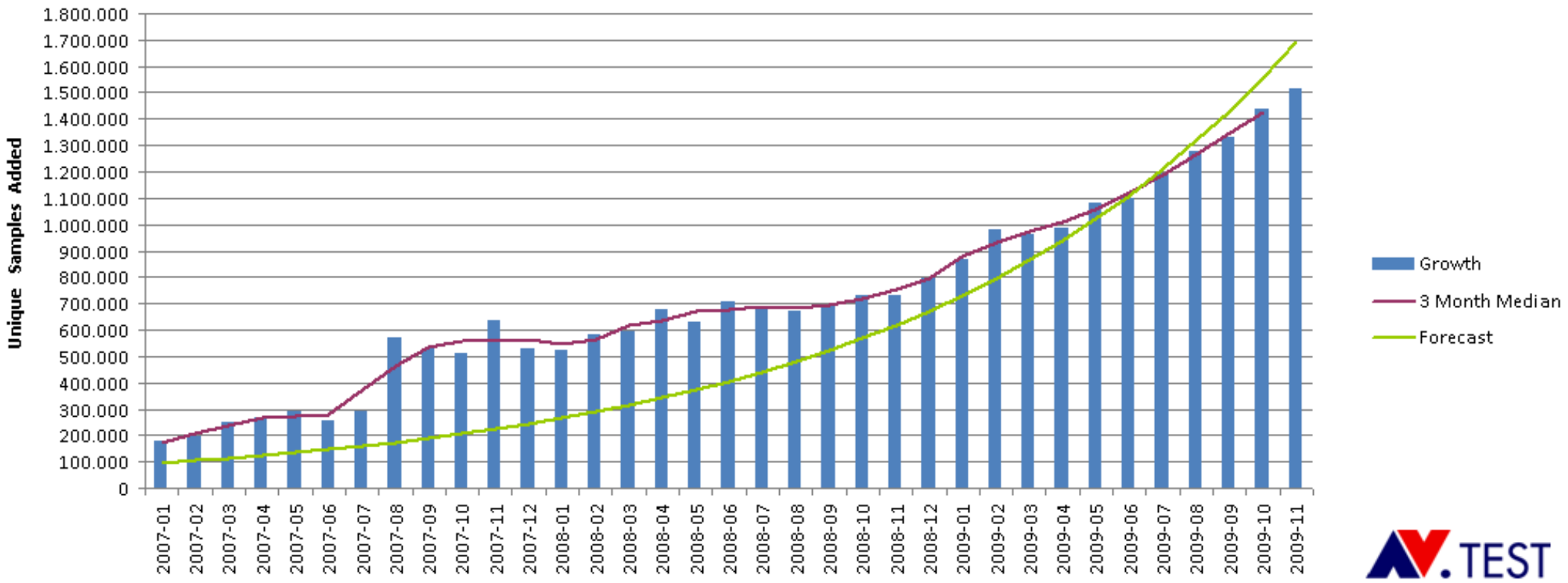
AVIRA
Mehr als Sicherheit

Malwareschutz : Wichtiger denn je!

Neueste Waffen und ihre Wirkung

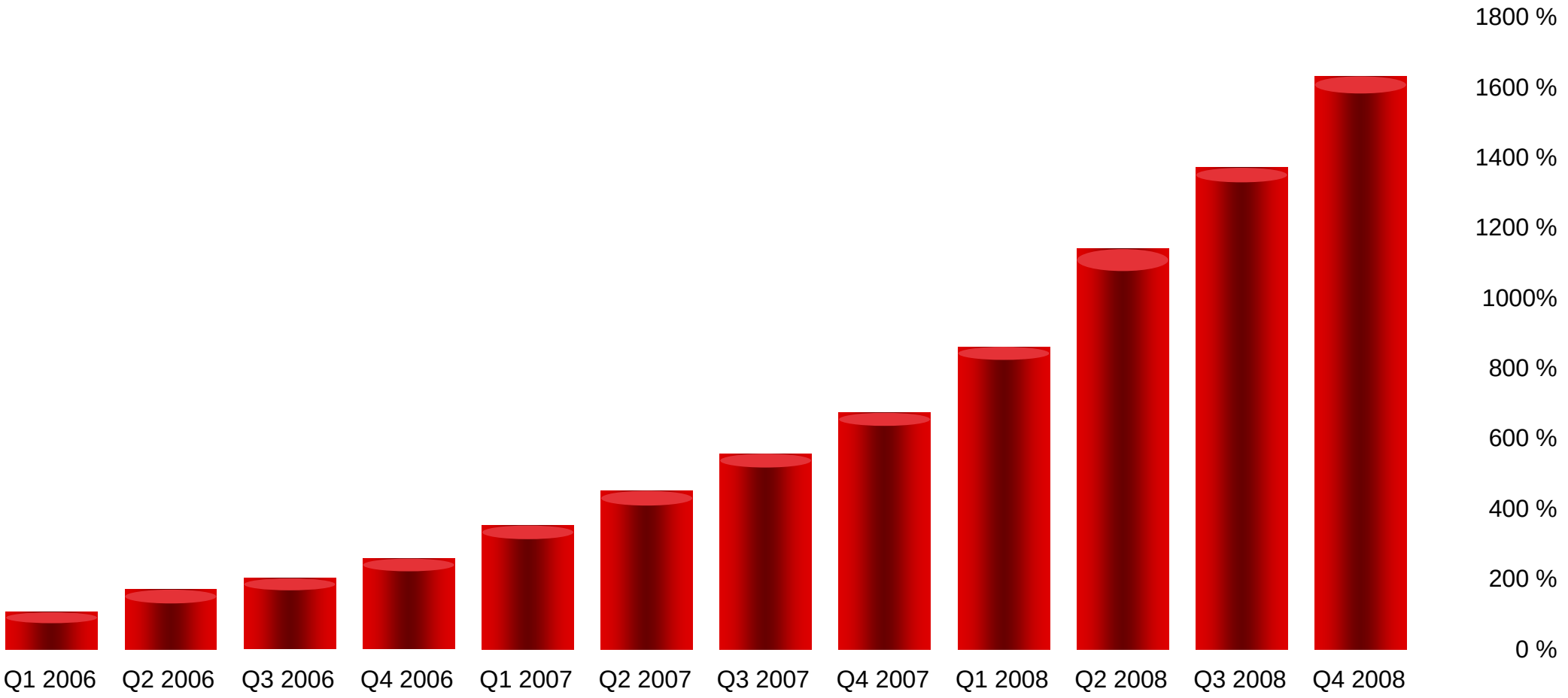
AVIRA
Mehr als Sicherheit

New Unique Samples Added to AV-Test.org's Malware Collection



AV-TEST

Anstieg web-basierter Angriffe



AVIRA
Mehr als Sicherheit

Anstieg web-basierter Angriffe

- Ca. alle 14 Sekunden eine neue infizierte Webseite
- Monatlich ca. 6000 neue infizierte Webseiten
- Ca. 83 % davon sind „legale“ Seiten, die gehackt oder kompromittiert wurden
- Juni 2007: MAL/IFrame infiziert mehr als 10.000 italienische Webseiten, darunter Webseiten von Städten, Touristeninformationen etc.
- Dezember 2007: JS/Adred-A Wurm auf brasilianischer Interaktions- und Kommunikationsseite Orkut. 670.000 Anwender infiziert.

Ham vs Spam

Internet-Sicherheitsbedrohungen im Juli 2009: Steigende Spam-Rate in Deutschland
Quelle: MessageLabs

AVIRA
Mehr als Sicherheit

Ham vs Spam

- Spam-Emails
  - Ca. **80 %** aller SPAM Emails enthalten Links zu potentiell gefährlichen Webseiten oder zu Malware
  - Trend: den Empfänger in betrügerischer Absicht auf Webseiten leiten (**Phishing**), zu gefährlichen Downloads zu verleiten oder nur durch das Besuchen der Webseite den Rechner des Empfängers zu infizieren (Drive-By Downloads)

AVIRA
Mehr als Sicherheit

Beispiel: Phishing

Bank of America Alert!: Account locked.. - Nachricht (HTML)

Nachricht

Antworten | Allen antworten | Weiterleiten | Löschen | In Ordner verschieben | Regel erstellen | Andere Aktionen | Absender sperren | Listen sicherer Adressen | Keine Junk-E-Mail | Kategorisieren | Nachverfolgung | Als ungelesen markieren | Suchen | Verwandt | Markieren

Von: Bank of America [bankofamerica@replies.em.bankofamerica.com]
Gesendet: Fr 29.01.2010 18:14
Betreff: Bank of America Alert!: Account locked..

Bank of America

Online Banking Alert

Sign In

http://bank0famerica-com.z2.newmail.ru/secure_membin_BankOfAmeri_caemail_id43432gjg98987ihgwq72k9878e.htm?securelogin=yes?ssl_encryptlink=yes&source=bankofamericaEMAILdefaultaspx?refererident=341348B3767313d1683678CADD124HJ8S748FGHHJC1AjkCB&cookieid=43562714&nocachelocal

signing in.

Click here to Securely Sign in and update your account

Thank you for banking with Bank of America, the industry leader in safe and secure online banking and we apologise for any inconvinience this may have caused you.
Sincerely,
Bank of America Customer Service

This alert is sent automatically. If you would like to make any changes to your Online Banking Alerts service, please sign in to Online Banking and click on the Customer Service Tab. The security and confidentiality of your personal information is important to us. **This E-Mail Box Is Not Equipped To Handle Replies. Mails sent here will not be processed**
We respect your privacy, and you can be rest assured that we protect your information, including your email address, and will never sell or share it with marketers outside Bank of America.
To find out more, please read our Privacy Policy. Bank of America E-mail, 6th Floor, 101 North Tryon Street, Charlotte, NC 28255-0001 XVF

Bank of America Higher Standards

Online Banking

Sign In

Enter Online ID:

(5 - 25 numbers and/or letters)

Save this online ID (How does this work?)

Enter Passcode:

(4 - 12 numbers and/or letters)

Account in:

Sign In

Not yet enrolled for online banking? You are required to sign up

Reset passcode

Forgot or need help with your ID?

Not using Online Banking?
Enroll now
for Online Banking »

Learn more
about Online Banking »

Service Agreement »

Pay By Phone user's guide »

Stop writing checks
and you could save $53
Learn more »

Secure Area

Home • Locations • Contact Us • Help • Sign in • Site Map
Personal Finance • Small Business • Corporate & Institutional
About the Bank • In the Community • Finance Tools & Planning • Privacy & Security

Official Sponsor 2000-2004 U.S. Olympic Teams

USA

AVIRA
Mehr als Sicherheit

TR/Spy.Banker (bzw. TR/Banker)

- Zeigen Fake Login Screens
- Zusätzlich können sie die Windows Hostfiles verändern um Onlinebanking Webseiten auf Phishing Webseiten umzuleiten
- Die User Eingaben aus den Login Screens werden dann, wenn Informationen gesammelt wurden, per Email an den Autor verschickt
- Weitere Malware Techniken werden von Bankern mit Fake Login Screens nicht benutzt, diese sind recht einfach, zumeist mit Borland Delphi programmiert
- Varianten aus den Banker Familien kommen mit deutlich aufwändigeren Malware Techniken daher, diese beinhalten dann z.B.:

  Rootkits oder Keylogger (die bei Besuch einer Banking Webseite) aktiviert werden.

Aktuelles Beispiel:

Phishing Mobile: Kreditkartenklau per Kurznachricht

AVIRA
Mehr als Sicherheit

Phishing mobile

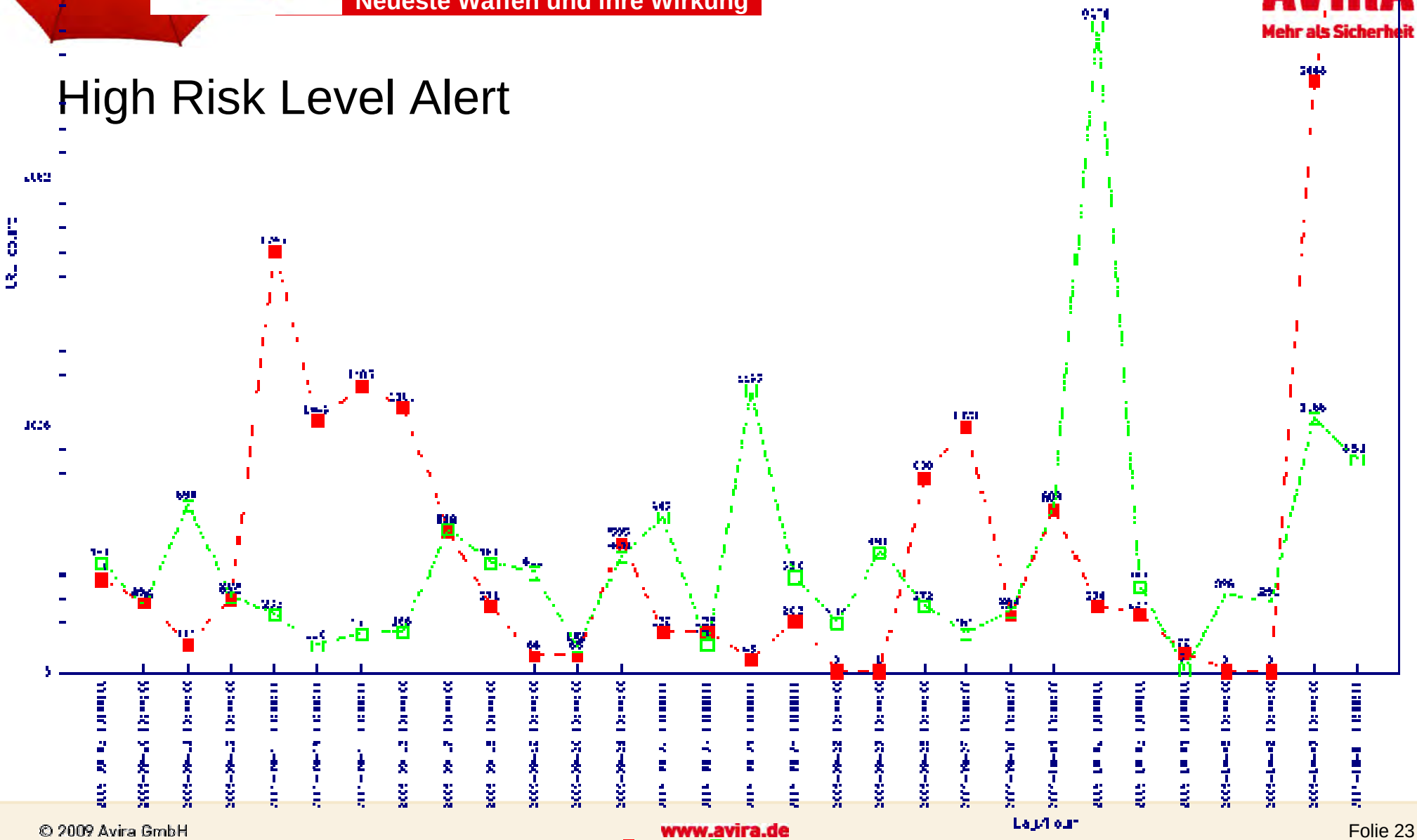
- Das **Internet Storm Center (ISC)** berichtete von einem Phishing-Versuch über Mobiltelefonnetze in den USA.
- Die Opfer bekommen per SMS eine Nachricht auf ihr Handy, die besagt, es gebe Probleme mit dem Account.
- Zur Lösung des Problems sollen die Nutzer eine kostenlose Nummer anrufen
- Ansageroboter verlangt dort nach einer
  - Kreditkartennummer,
  - dem Ablaufdatum
  - und einer PIN,

  um das Problem zu beheben.

- ➔ Transaktion werden danach nahezu in Echtzeit vorgenommen!

High Risk Level Alert

High Risk Level Alert



AVIRA
Mehr als Sicherheit

High Risk Level Alert

- Hohe Anzahl von neuen URLs, die auf Malware Dateien und Phishing Seiten verweisen
- Gründe sind sehr wahrscheinlich das Yahoo, Google, Hotmail und AOL Accounts „abgephisht“ wurden
- Anzahl Spam ebenfalls gestiegen:
  - Erste 8 Tage Oktober 2009 → 36% vom gesamten September
  - 44% Zuwachs zu September

- **Ändern Sie Ihr Kennwort!!!**

AVIRA
Mehr als Sicherheit

Gegenmaßnahmen!

AVIRA
Mehr als Sicherheit

Welche organisatorischen und technischen Maßnahmen sind für eine sichere Nutzung notwendig?

- (H)IPS – (Host) Intrusion Prevention System
- Webseiten blockieren
- HTML MIME Typen blockieren
- Sicherheitsrichtlinien erstellen
- Nutzerrechte einschränken
- Sicherheitsbelehrungen
- Mehrstufiges Firewall Konzept

AVIRA
Mehr als Sicherheit

Wie kann die Web 2.0 Nutzung in ein gesamtheitliches Sicherheitskonzept integriert werden?

- Es muss ein Firmenweites Sicherheitskonzept bestehen
- Nutzer müssen entsprechend dem Sicherheitskonzept geschult werden
- Generelle Sensibilisierung für Sicherheitsprobleme im Web 2.0
- Regelmäßige Überprüfung der Sicherheitskonzepte
- Externes Auditing von zertifizierten Firmen

AVIRA
Mehr als Sicherheit

Gegenmaßnahmen

Heute und Morgen

AVIRA
Mehr als Sicherheit

Signatur-basiertes Scanning

- Update des Virenscanners bringt Erkennung der Schädlinge
- Häufiges Update ist Pflicht
- Ohne Signaturen - keine Erkennung!
- **Aktuelle Virendefinitionen - unerlässlich für den Schutz Ihres Systems**

- Signaturen enthalten oft Desinfektionsroutine

AVIRA
Mehr als Sicherheit

AntiViren-Heuristik

- Code-Muster kann analysiert werden und mit bekanntem Schadcode verglichen werden
  - Generische Erkennung

- Die Heuristik kann anhand der Beschaffenheit einer Datei, der Abfolge signifikanter Code-Sequenzen oder bestimmter Verhaltensmuster mit sehr hoher Wahrscheinlichkeit feststellen, ob es sich um eine schädliche oder virulente Datei handelt. Ist erst einmal Alarm geschlagen, bietet die Virenschutzsoftware die Wahl, die potenziell virenverseuchte Datei in Quarantäne zu nehmen oder vom Rechner zu löschen.

*Die AntiVir-Heuristik **AHeAD** ist zudem in der Lage, manipulierte HTML-Dateien proaktiv auf Gateways zu überprüfen. Auf diese Weise wird wirksam verhindert, dass Hacker eventuelle Exploits in Browsern ausnutzen können.*

HIPS

- **Re-aktiver Schutz**
  - Signatur-basierte Erkennung→ bekannte Malware
  - Generische Erkennung → bekannte Malware
- **Pro-aktiver Schutz**
  - Heuristik-basierte Erkennung → neue Malware
  - HIPS = verhaltens-basierte oder proaktive Erkennung → neue Malware

➔ **Avira AntiVir ProActiv**

AVIRA
Mehr als Sicherheit

HIPS

- Flags:
  - Installer/SFX
  - Program having probably legal Structures
  - Program having indifferent Structures (neither legal nor suspicious)
  - Program having suspicious Structures
  - Legal/Commercial Runtime-Packer
  - "normal" Runtime-Packer
  - Suspicious Runtime-Packer
  - Program was downloaded from the internet
  - Program is stored in critical directories (%Root%, %System%" etc.)
  - Program is stored inside a NTFS-Stream
- Sensoren:
  - File Sensor
  - Registry Sensor
  - Process Sensor
  - Kernel Mode API Sensor
  - User Mode API Sensor

Kombination von allen

AVIRA
Mehr als Sicherheit

Neue Technologie:
„Generic repair”

AVIRA
Mehr als Sicherheit

Generic repair

- Script-basiertes Reparatursystem:
  - Beseitigt bekannte Malware
  - Braucht Signatur-Datei

- **NEU**: generisches Reparatursystem:
  - Beseitigt Malware, ohne vorhandene Reparaturinformationen
    - Malware integriert sich selbst in das Betriebssystem, mit eindeutig definierten Methoden und an bekannte Orte
    - Überprüft die Registrierung an best. Stellen auf Malware Einträge z.B.: `HKLM\Software\Microsoft\Windows\CurrentVersion`
    - Beseitigt Registrierung-Schlüssel oder ~-Werte, welche von einer Malware hinzugefügt wurden und setzt sie in den Originalzustand zurück

AVIRA
Mehr als Sicherheit

Gründe für Virenschutz gibt es viele. Vor allem für unseren

AVIRA
Mehr als Sicherheit

Avira - Virenschutz aus Deutschland:

- Deutscher Anbieter von systemübergreifenden IT-Security-Lösungen
- Über 350 Mitarbeiter
- Überdurchschnittliches Wachstum
- Unabhängig durch 100% Innenfinanzierung
- Eigene Produktentwicklung
- Zwei eigene Malware Research Center
- Enge Zusammenarbeit mit dem BSI (Ü1 Zertifizierung)
- Über 20 Jahre Erfahrung im Bereich IT-Sicherheit
- Mehr als 3000 Avira Vertriebs- und Consulting-Partner

SecurITy made in Germany

AUERBACH STIFTUNG

Avira – Eine Frage des Vertrauens:

Die freiwillige Selbstverpflichtung: No Backdoors!

- IT Security made in Germany: nur Avira verpflichtet sich als einziger Antivirenexperte den ITSMIG Richtlinien (www.itsmig.de), keine Daten von den IT-Systemen der Kunden auszuschleusen!

AVIRA
Mehr als Sicherheit

Avira - Sicherheit für alle:

- Kleine und mittlere Unternehmen
- Großunternehmen
- Öffentliche Auftraggeber
- Bildungseinrichtungen
- OEM und Technologie-Integratoren
- Privatanwender

Avira Sicherheitslösungen sind in mehr als 30.000 Unternehmen im Einsatz

Mehr als 120 Millionen Menschen weltweit schützen sich mit Avira AntiVir®

AVIRA
Mehr als Sicherheit

Avira – Immer die richtige Wahl:

Der flexible Einsatz.

- Plattformübergreifender Einsatz unter Windows und Unix (Linux, Novell, Solaris)
- Unix-Technologieführer durch On-Access-Scanning (Dazuko-Modul)
- Lösungen für Windows Mobile

Windows Mobile | Microsoft GOLD CERTIFIED Partner | Ready for IBM Systems with Linux | SOFTWARE SAP PARTNER | redhat READY | solaris | PartnerNet TECHNOLOGY PARTNER Novell

AVIRA
Mehr als Sicherheit

AVIRA

Michael Witt
Territory Manager

Jens Freitag
Business Line Manager Corporate Products

Avira GmbH
Lindauer Str. 21
D-88069 Tettnang
http://www.avira.de

Telefon: +49 (0) 7542-500 0
Fax: +49 (0) 7542-500 10
Email: vertrieb@avira.com