

T.I.S.P. Community Meeting 2010

Köln, 03./04.11.2010

Stephan Sachweh
Pallas GmbH

URL-Filter und Websicherheit

Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information(at)pallas.de
<http://www.pallas.de>





- **Giftige Webserver**: die neue Hauptbedrohung
- Was man zum **Schutz** machen kann
- Was einen guten **URL-Filter** auszeichnet



- 82 % halten **Bedrohung** für wachsend oder stark wachsend
- Nur 3 % rechnen mit sinkenden **Sicherheitsausgaben** in 2010

eco Umfrage Internetsicherheit 2011 läuft noch bis 15.11.2010 <http://www.eco-umfrage.de/internetsicherheit>

Wichtigste technische Themen



Ein Webangriff ... Start auf der Terrasse



Suche nach Terrakotta-Hersteller



Google

Pallas RealTime Web Security - Mozilla Firefox

Web

Tipp: Such

TREQUA
Attualmen
e figli (19
www.cera

III. CONT
21 ott 200
Figli, 1971
archivio.m

pottery b
benocci c
our leader

FEHLER

Der angeforderte URL konnte nicht geladen werden

Während des Versuches, den URL <http://www3.goforscan51p.xorg.pl/?p=p52dcWp/eFqtqKRxb2qVYZadYmGRZWle16HDpKXZaonV> zu laden, trat der folgende Fehler auf:

- Zugriff verweigert auf Basis der Pallas
- Anfragende IP: 192.168.1.100
- Benutzername: Administrator
- Kategorien der URL:
 - 42 Malware
 - 10 Compromised

pottery barn hostess gifts pottery - Mozilla Firefox

http://www.benocci.nl/

pottery barn hostess gifts pottery

- 868 pennsylvania bujno pottery
- 869 t p co pottery
- 870 bennington pottery maple syrup pitcher
- 871 19th century virginia pottery
- 872 pottery signed a mccawley
- 873 pottery barn stuffed bear
- 874 mary dye pottery
- 875 pottery barn fake flowers
- 876 fulper art pottery
- 877 mexican clay pottery urns
- 878 making pottery on a wheel
- 879 old time pottery louisville
- 880 a potter's function in pottery
- 881 pottery barn kids in pittsburgh
- 882 developed a type of unglazed pottery
- 883 attaching handle to cup pottery
- 884 kl germany pottery
- 885 old time pottery barn destin
- 886 haegler pottery macomb il
- 887 evelia sanchez pottery mukilteo
- 888 mccarty pottery in marigold ms
- 889 jacobson pottery hawaii
- 890 sales stats for pottery barn
- 891 phil rogers pottery
- 892 pottery barn kids rose bedding
- 893 west troy pottery
- 894 pottery barn warehouse long island
- 895 craigslist pottery barn leather sectional
- 896 pottery classes near martinsville indiana
- 897 wholesale mexico pottery
- 898 art pottery eureaka springs
- 899 buchan pottery thistle soup jug
- 900 state college pottery
- 901

Google-Link nach Holland löst polnischen Angriff aus



Security Threat Analysis

System folders

- Shared Documents: 9 Viruses found
- My Documents: 3 Viruses found
- Hard drive (C:): 12 Viruses found

Security

Windows Security
Security is affected by virus

100%
Checking: C:\...\Local Settings\Temporary Internet Files\Content.IE5\SET4.tmp

Your Computer is infected

Name	Type
Packed.Generic.287	Virus
Trojan.Vundo!gen5	Virus
AdvWare.Hotbar	Virus
W32.Downadup	Virus
W32.Fujacks.CE!inf	Virus

Recommend: Click "Start Protection" button to erase all threats

Start Protection

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:
Packed.Generic.287	vmmreg32.dll
Trojan.Vundo!gen5	perfc019.dat
AdvWare.Hotbar	cidaemon.exe
W32.Downadup	secupd.dat
W32.Fujacks.CE!inf	ds16gt.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.

Die Seite mit der Adresse <http://www3.saveus36.xorg.pl> meldet:

Your system has been damaged due to recent virus attack. Press 'OK' to fix it.

OK Abbrechen

Öffnen von packupdate_build7_289.exe

Sie möchten folgende Datei herunterladen:

- packupdate_build7_289.exe

Vom Typ: Binary File
Von: <http://www3.defenderofpc24pd.xorg.pl>

Möchten Sie diese Datei auf einem Datenträger speichern?

Datei speichern Abbrechen

Will Datei mit Scareware unterschieben



VirusTotal analysiert verdächtige **Dateien und erleichtert die schnelle Erkennung** von Viren, Würmern, Trojanern und jeglicher Art von Malware, welche von den Antivirus-Engines festgestellt werden. [Weitere Informationen...](#)

Datei **packupdate_build7_258.exe** empfangen **2010.04.12 07:16:16 (UTC)**
Status: **Beendet**
Ergebnis: **7/39 (17.95%)**

Filter

Drucken der Ergebnisse

Antivirus	Version	letzte aktualisierung	Ergebnis
a-squared	4.5.0.50	2010.04.12	-
AhnLab-V3	5.0.0.2	2010.04.10	-
AntiVir	7.10.6.56	2010.04.12	-
Antiy-AVL	2.0.3.7	2010.04.09	-
Authentium	5.2.0.5	2010.04.12	W32/FraudLoad.C!Generic
Avast	4.8.1351.0	2010.04.11	-
Avast5	5.0.332.0	2010.04.11	-
AVG	9.0.0.787	2010.04.11	-
BitDefender	7.2	2010.04.12	-
CAT-QuickHeal	10.00	2010.04.12	-
ClamAV	0.96.0.3-git	2010.04.12	-
Comodo	4574	2010.04.12	Heur.Suspicious
DrWeb	5.0.2.03300	2010.04.12	Trojan.Fakealert.7869
eSafe	7.0.17.0	2010.04.11	-
eTrust-Vet	35.2.7418	2010.04.09	-
F-Prot	4.5.1.85	2010.04.12	W32/FraudLoad.C!Generic
F-Secure	9.0.15370.0	2010.04.12	-
Fortinet	4.0.14.0	2010.04.10	-
GData	19	2010.04.12	-
Ikarus	13.1.1.80.0	2010.04.12	-
Jiangmin	13.0.900	2010.04.12	-
Kaspersky	7.0.0.125	2010.04.12	-
McAfee-GW-Edition	6.8.5	2010.04.12	-
Microsoft	1.5605	2010.04.12	-

Die allermeisten AV-Scanner erkennen den Angriff nicht! (32/39)

Pallas RealTime Web Security - Mozilla Firefox

FEHLER

Der angeforderte URL konnte nicht geholt werden

Während des Versuches, den URL <http://www3.goforscan51p.xorg.pl/?p=p52dcWpscV/Cj8bYbnOCdVik12qZVp/ZatramleZm5qiw8J/eFqtqKRxb2qVYZadYmGRZWle16HDpKXZaonVoFerm6rRxqBfmJ2ImXVarqLGPkGMMqBqZWtskmGXXmOZW5eK1Zadb57Z1> zu laden, trat der folgende Fehler auf:

- Zugriff verweigert auf Basis der Pallas RealTime URL Filter Datenbank powered by Commtouch
- Anfragende IP: 192.168.1.123
- Benutzername: admin
- Kategorien der URL:
 - 42 Malware
 - 10 Compromised

Aber der Pallas-URL-Filter

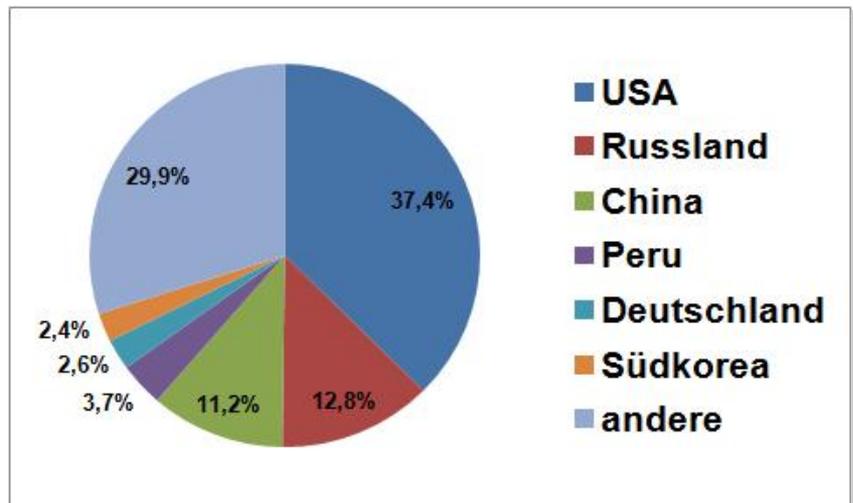
Wichtigstes technisches Thema 2010: Schadsoftware im Web



- Malware wird zu 2/3 übers **Web** verbreitet, nur 1/3 per Email, durch Ansurfen (= **Drive-by-Downloads**) sofort übertragen
 - 2 Mio Behörden-Botnet übers Web infiziert (Spiegel Online 04/09)
- Per Suchergebnis/Email-Link wird angelockt (**Blended Threat**)
 - 90 % des Spam enthält Links (Symantec 01/09)
 - 3/4 der Links verweisen auf Mal/Spam-Sites (Websense 06/08)
 - 3/4 der Malpages auf seriösen Servern (Websense 01/09)

- 50.000 neu infizierte Webseiten täglich in 2009
(Sophos, searchsecurity 02/10)

Anteil infizierter Webseiten 2009
(Sophos, searchsecurity 02/10)





Web-Kategorien, die am wahrscheinlichsten verseucht sind

Commtouch, Q4/2009

Top 10 Web Categories Infected with Malware	
Rank	Category
1	Business
2	Computers & Technology
3	Pornography/Sexually Explicit
4	Search Engines and Portals
5	Health & Medicine
6	Education
7	Shopping
8	Personal Sites
9	Real Estate
10	Travel

Source: Commtouch Labs

Top 10 Web Categories Manipulated by Phishing	
Rank	Category
1	Computers & Technology
2	Search Engines & Portals
3	Business
4	Personal Sites
5	Shopping
6	Finance
7	Education
8	Health & Medicine
9	Real Estate
10	Streaming Media & Downloads

Source: Commtouch Labs



Für Webinfektion bei einem Spontanbesuch greift die **Deliktische Haftung** (ohne Vertragsverhältnis). Voraussetzung:

- 1) **Rechtsverletzung** liegt vor
(z.B. Datenveränderung, Computersabotage, § 303a/b StGB)
- 2) Ein **Schaden** ist eingetreten
(z.B. Kosten der Entgiftung;
Kausalzusammenhang zu 1) ist nachzuweisen)
- 3) **Verschulden** des Site-Betreibers liegt vor
(z.B. Fahrlässigkeit; dies wird bei Vorliegen von 1) und 2) o.w.
vermutet, der Betreiber muss darlegen, dass er die verkehrsübliche
Sorgfaltspflicht beachtet hat)

Auch deshalb: **Vorsorgliche Sicherheitsmaßnahmen!**



Der eco Arbeitskreis Sicherheit (Leitung Dr. Brand, Pallas) empfiehlt:

Serverbetreiber	Websitebetreiber	Nutzer
Server härten	Sichere Softwarearchitektur und sichere Programmierung	Virenschutz frisch halten
Firewall vorschalten	Fremdprogramme aktuell halten	Browser und wichtige Programme aktuell halten
Auf Schadsoftware prüfen	Web Application Firewall vorschalten	URL-Filter zwischenschalten

Kopf einschalten und Experten fragen!

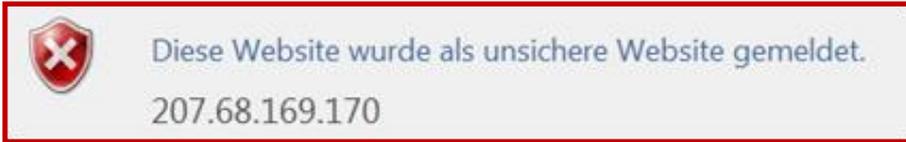


- **Sicherheit**
Schutz vor Malware im Web
- **Produktivität**
Nur Zugriff auf Job-relevante Webseiten
- **Compliance mit Gesetzen und Richtlinien**
Waffen, Gewalt, Extremismus,... / Jugendschutz
- Früher stand **Jugendschutz** im Vordergrund
- Heute Fokus Richtung **Echtzeit-Schutz vor Gefährdungen**



Internet Explorer SmartScreen-Filter (unter "Extras")

- Eingeführt im IE 8 (in Erweiterung des Phishingfilters im IE 7)
- URLs gesendet an SmartScreen Webservice von Microsoft



Firefox SafeBrowsing (unter "Extras\Einstellungen\Sicherheit")

- Eingeführt im Firefox 3
- Basiert auf der Google SafeBrowsing Datenbank, lokal gehalten

Grenzen: Keine Lösung für einen Unternehmensstandard

- Einsatz hängt vom User ab
- Malware versteckt sich vor Suchmaschinen

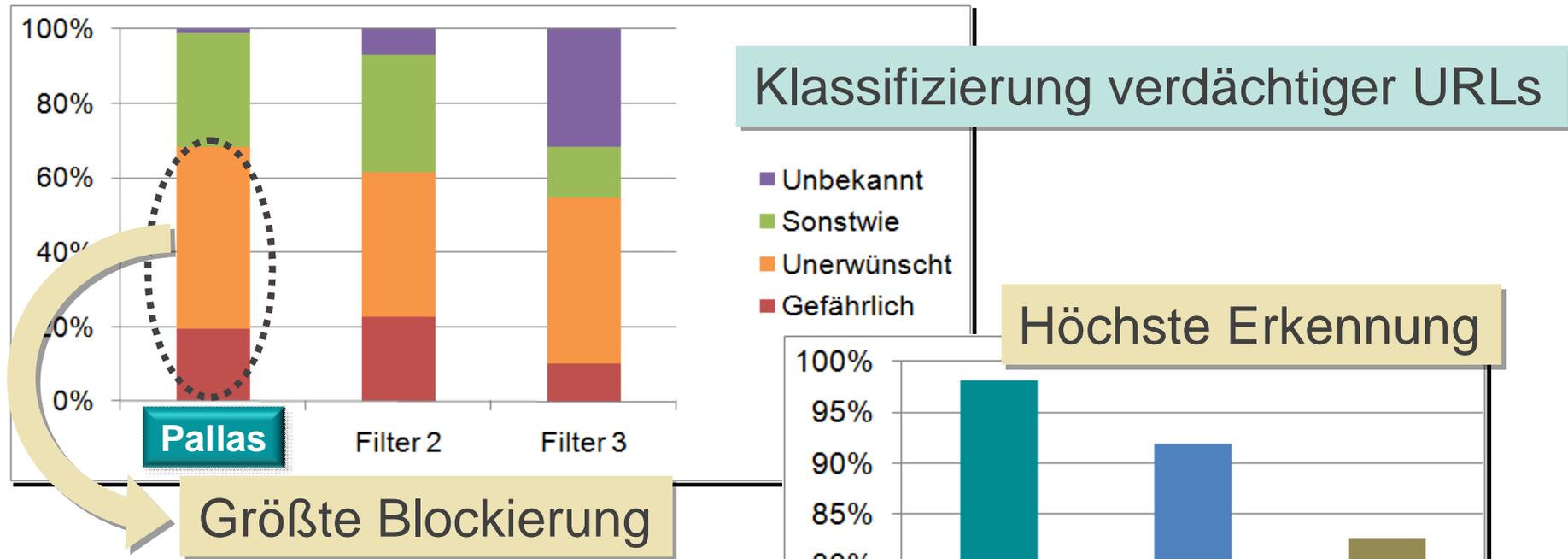
3 Business-URL-Filter im Test bei Pallas



Test 1: verdächtige URLs, insbesondere

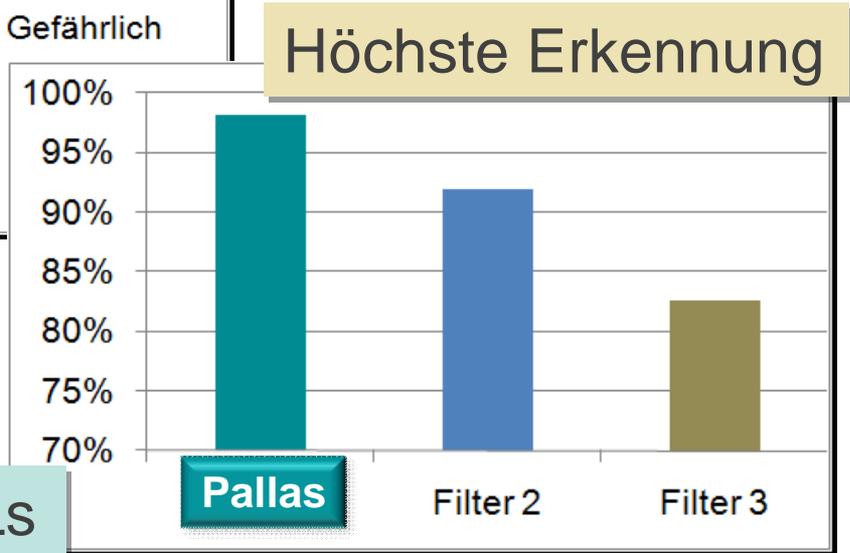
Gefährliche: criminal, illegal, compromised, malicious...

Unerwünschte: gambling, porno, dating...

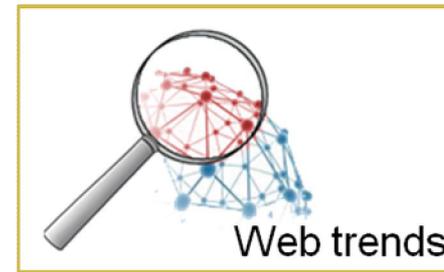


Test 2:

Erkennungsrate bei 25.000 URLs



Datenquellen für den Pallas URL-Filter



© Commtouch



Besonders guter Schutz

- **Hunderte Millionen Websites** klassifiziert in 64 Kategorien (davon 8 Sicherheits-Kategorien)
- Kategorisierung von **Deep Links** schützt vor Malware im Web 2.0 und auf infizierten, regulären Seiten
- Erkennung und Abfrage **Realtime in the Cloud** (Web-Traffic-Analyse entdeckt Malware-Ausbrüche in Zero-Hour Zeit); zus. lokaler Cache
- **Multiple Kategorisierung** eingebetteter URLs (Suchergebnisse: Werbung/Übersetzung)

Beispiellose Genauigkeit

Intelligente Automatismen, ob und wie tief eine Site gescannt wird:

- **Trigger**: aufgerufene URLs werden untersucht
- **Analyse**: Dynamik der Site (Content unabhängig) → Scan-Granularität
- **Tracking**: Exakte Klassifizierung jeder URL zu jeder Zeit



genauer
frischer
umfangreicher

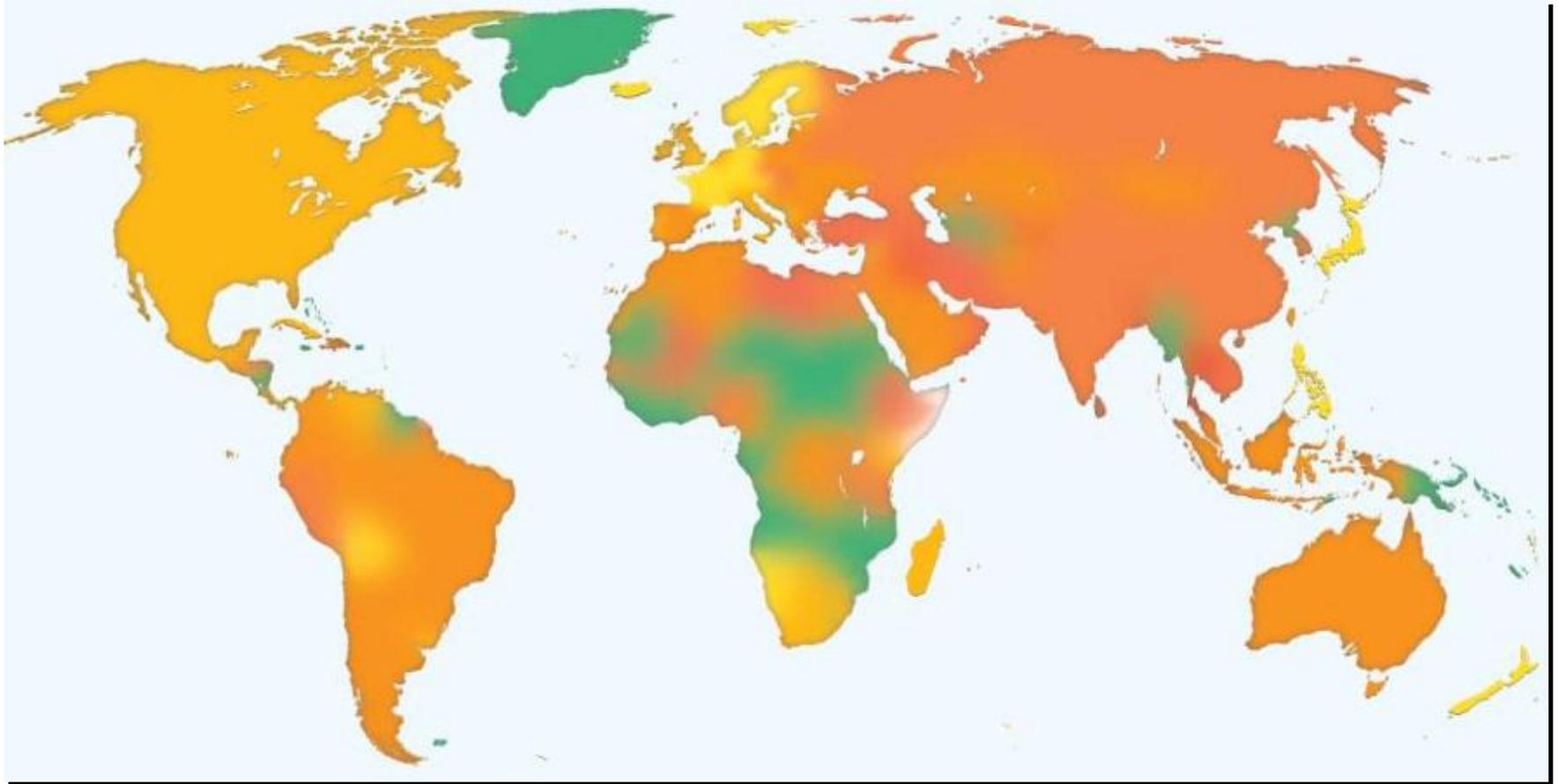
Gerne beantworte
ich Ihre Fragen



Stephan Sachweh
Pallas GmbH
Hermülheimer Straße 10
50321 Brühl

information (at) pallas.de
<http://www.pallas.de>

Giftige Webserver – Verseuchung weltweit



Grün ist gut (0 % vergiftet), **Rot** ist schlecht (5 %),
in **Deutschland** sind es 0,1%, in der **Türkei** 1,3 %

Aus: Microsoft-Analyse zur IT-Sicherheit, Ausgabe 8, 2.HJ 2009



- Eingeführt in Internet Explorer 8
- Ergänzt den bereits in IE7 enthaltenen Phishingfilter
- Funktionsweise
 - URL Daten werden per https an den SmartScreen Webservice von Microsoft zur Evaluation geschickt
 - Bei entsprechender Antwort generiert der IE Fehlerseiten
 - Microsoft sichert zu, die gelieferten Daten nicht zur Identifikationsfeststellung oder Werbung zu verwenden



■ Beispiel: Unsichere Web-Seite

This screenshot shows a warning dialog box with a red border. On the left is a red shield icon with a white 'X'. The text reads: 'Diese Website wurde als unsichere Website gemeldet. 207.68.169.170'. Below this, it says 'Es wird empfohlen, dass Sie nicht zu dieser Website wechseln.' A green checkmark icon is followed by the link 'Stattdessen zu meiner Startseite wechseln'. Further down, it states 'Diese Website wurde Microsoft als unsichere Website gemeldet, die möglicherweise persönliche oder Finanzinformationen offenlegt.' At the bottom, there is a blue link 'Weitere Informationen' with a small downward arrow icon.

■ Beispiel: Unsicherer Download

This screenshot shows a dialog box titled 'Unsicherer Download - Sicherheitswarnung'. It features a red header bar with a red shield icon containing a white 'X' and the text 'Dieser Download wurde als unsicher gemeldet.' The main body of the dialog contains the following text: 'Die Datei, die Sie heruntergeladen, wurde als unsicher gemeldet. Die Download-Website enthält Links zu Viren oder anderer Software, die den Computer beschädigen oder persönliche Informationen offenlegen können. Aus Sicherheitsgründen wird empfohlen, den Download für diese Datei abzubrechen.' Below this, there are two blue links: 'Ignorieren und Download der unsicheren Datei fortsetzen (nicht empfohlen)' and 'Melden, dass dieser Download sicher ist'. A blue button labeled 'Abbrechen' is located in the bottom right corner.



- Aktivierung bzw. Administration
 - Als Benutzer
 - Sicherheit -> SmartScreen-Filter
 - Als Administrator
 - Mittels Group Policy
 - *Verwalten von Phishingfilter deaktivieren*
 - *Verwalten von SmartScreen Filter deaktivieren*
 - *Umgehung der SmartScreen-Filterwarnungen verhindern*

- + Zentral Verwaltbar in AD-Umgebungen
- - **Eine Umgehung des SmartScreen-Filter ist für jeden User mit lokalen Admin-Rechten möglich!**



- Eingeführt in Firefox 3
- Basiert auf der Google SafeBrowsing Datenbank

- Funktionsweise
 - Periodische Updates der lokalen SafeBrowsing DB
 - Die DB enthält nur gehashte URLs
 - Vor Abfrage einer URL
 - Prüfung des Hashes der URL gegen die DB
 - Bei möglicher Gefahr Validierung über Google Webservice
 - Warnung an den Benutzer über Fehlerseite

 - Google loggt die abfragende IP, ggf. Cookie und den Hash für „einige“ Wochen. Es gilt die Google Privacy Policy



■ Beispiel einer Fehlerseite



Als Betrugsversuch gemeldete Webseite!

Die Webseite auf www.yewknee.com wurde als Betrugsversuch gemeldet und gemäß Ihrer Sicherheitseinstellungen blockiert

Mit Betrugsseiten versuchen Kriminelle Sie dazu zu bringen, persönliche oder finanzielle Daten preiszugeben. Dabei ahmen sie in betrügerischer Absicht Webseiten oder E-Mails nach, denen Sie eventuell vertrauen.

Falls Sie hier persönliche Daten eingeben, müssen Sie mit Identitätsdiebstahl oder sonstigem Betrug rechnen.

[Diese Seite verlassen](#) [Warum wurde diese Seite blockiert?](#)

[Diese Warnung ignorieren](#)

■ Test und Diagnose Seite von Google SafeBrowsing



Safe Browsing

Diagnoseseite für promoddl.com

Ratgeber - bereitgestellt von 

Wie ist die gegenwärtige Einstufung von promoddl.com?

Diese Website ist gegenwärtig nicht als verdächtig eingestuft.

Welche Befunde hat Google beim Besuch dieser Website festgestellt?

Bei 2 Seite(n) von insgesamt 114 Seiten dieser Website, die wir in den letzten 90 Tagen getestet haben, wurde festgestellt, dass Malware (Schadsoftware) ohne Einwilligung des Nutzers heruntergeladen und installiert wurde. Der letzte Besuch von Google auf dieser Website war am 2010-02-13 und verdächtiger Content wurde auf dieser Website zuletzt am 2010-01-21 gefunden.

Die Malware wird in 2 Domain(s) gehostet, darunter warez-box.net/, ddl-city.com/.

Bei der Verteilung von Malware an Besucher dieser Website fungieren anscheinend 2 Domain(s) als Überträger, darunter moscowteiment.mybb.ru/, spamfreeforums.net/.

This site was hosted on 1 network(s) including [AS43350 \(NFORCE\)](http://AS43350).

Hat diese Website als Überträger zur Weiterverteilung von Malware fungiert?

In den letzten 90 Tagen hat promoddl.com anscheinend nicht als Überträger für die Infektion von Websites fungiert.

Hat diese Website Malware gehostet?

Nein, diese Website hat in den letzten 90 Tagen keine Malware gehostet.

Nächste Schritte:

- [Zur vorherigen Seite zurückkehren](#).
- Falls Sie Eigner dieser Website sind, können Sie eine Überprüfung Ihrer Website mit den Google [Webmaster-Tools](#) anfordern. Weitere Informationen über den Prüfprozess erhalten Sie in der [Hilfe für Webmaster](#).

Updated 6 hours ago



- Aktivierung bzw. Administration
 - Als Benutzer
 - Extras -> Sicherheit
 - Webseite blockieren, wenn sie als attackierend gemeldet wurde
 - Webseite blockieren, wenn sie als Betrugsversuch gemeldet wurde
 - Als Administrator
 - Verteilung von prefs.js
 - FirefoxADM / ADMXPI
 - GPO for Firefox

=> keine wirklich empfehlenswerte zentrale Administration

- - **Eine Umgehung des SafeBrowsing ist für jeden User mit lokalen Admin-Rechten möglich!**



- Browser Plugin, verfügbar für Firefox und IE
 - Chrome in der Entwicklung
- Funktionsweise
 - Community erstellt Bewertung für die Kategorien
 - Vertrauenswürdigkeit
 - Händlerzuverlässigkeit
 - Datenschutz
 - Jugendschutz
 - Einstellbare Reaktion auf Kategorien
 - Warnen ab einem einstellbaren Level
 - Blockieren ab einem einstellbaren Level
 - Jugendschutz aktivierbar
 - Jeder Web-Request wird vom Plugin per http-get auf ihre Bewertungen geprüft



WOT-Warnung: Diese Seite hat einen schlechten Ruf. [Bewertungsdetails](#)

PLAYBOY
ENTERTAINMENT GAMES MAGAZINE ADVICE NIGHTLIFE PLAYBOY U

Warnung!

Diese Seite hat einen schlechten Ruf.
playboy.com

[i](#) [Bewertungsdetails und Kommentare anzeigen](#)

	Vertrauenswürdigkeit	Ausgezeichnet
	Händlerzuverlässigkeit	Ausgezeichnet
	Datenschutz	Ausgezeichnet
	Jugendschutz	Sehr schlecht

[! Site ist sicher. Ich möchte sie bewerten](#) [Warnung ignorieren und Website aufrufen](#) [➔](#)

ENTERTAINMENT ENTERTAINMENT ENTERTAINMENT

<http://www.playboy.com/>

WOT [Ausgezeichnet](#) [Einstellungen](#) | [Leitfaden](#)

playboy.com

WOT-Bewertung Meine Bewertung

Vertrauenswürdigkeit:
 Ausgezeichnet

Händlerzuverlässigkeit:
 Ausgezeichnet

Datenschutz:
 Ausgezeichnet

Jugendschutz:
 Sehr schlecht

[i](#) [Detailanzeige auf der Bewertungsliste.](#)
[Eigenen Kommentar hinzufügen.](#)

Meine Aktivitätspunkte Meine Seite anzeigen
 0

Bewerten Sie für Aktivitätspunkte neue Websites.

Are you a Facebook user? Press the Like button and show your friends that you like WOT for safe surfing, shopping and searching. [Click here to like WOT on Facebook.](#)



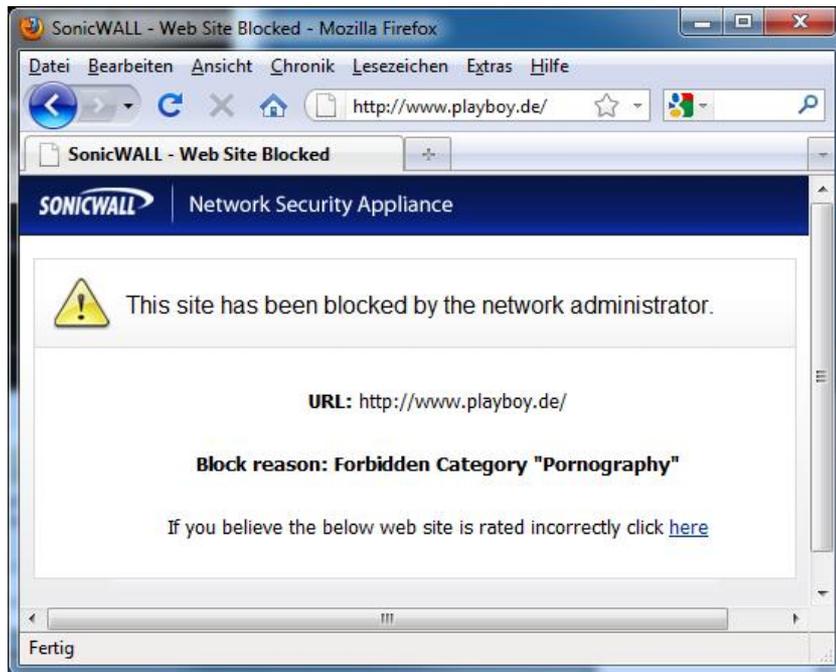
- Aktivierung bzw. Administration
 - Als Benutzer durch Plugin
 - *Keine zentrale Administration*
- Eingeschränkt RealTime
 - Technologisch RealTime
 - Community muss schnell genug sein
- Umgehung durch den Benutzer ist immer möglich
- Sicherheitsverbesserung aber keine Lösung für Unternehmensstandard



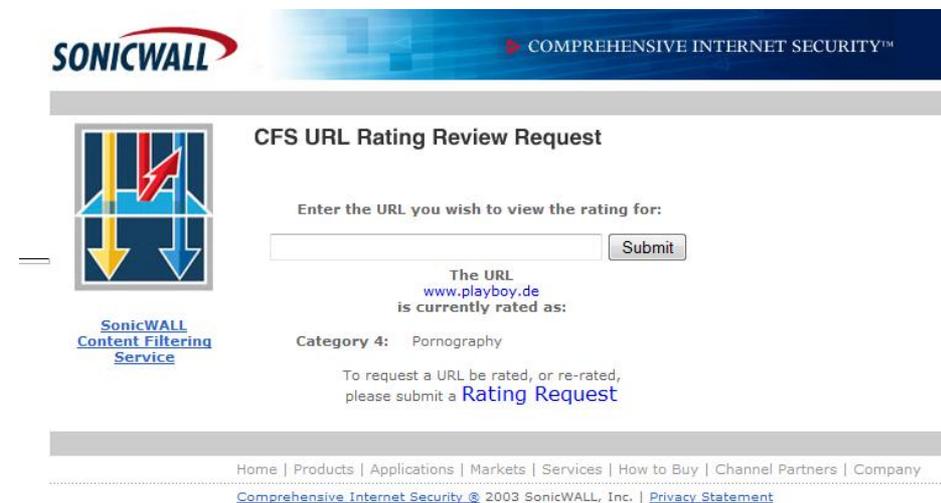
- Hersteller von UTM Security Appliances
- **Content Filtering Service** als integrierter Service in der Appliance
- 64 Kategorien, davon 1 Security relevant
 - 28. Hacking/Proxy Avoidance System
- Manuelles White- und Blacklisting möglich
- Bindung der Security Policy an IP-Bereiche
- Als Security Gateway **verpflichtende** Kontrolle für die Benutzer
- **Blockade Seite** frei gestaltbar
- **https** Sites nur auf IP-Basis prüfbar
- Kategoriebewertungen über <http://cfssupport.sonicwall.com> einsehbar



- Exemplarische Blockade-Seite



- Anzeige der Kategorie einer Web-Site





- **Zentrale Administration** durch Security Gateway möglich
- Umgehung durch den Benutzer **unmöglich**
- Recht kleiner URL-Cache => **Online Verbindung benötigt**
- **Wenig** Security relevante Kategorien
- Nutzbar mit **jedem** Browser
- **Kein Realtime!**

- Für kleine Installationen und geringere Anforderungen brauchbar
- Für große Installationen ungeeignet



- Als Software und als Appliance nutzbar
- URL-Filter Teil der Lösung, weitere Teile
 - SSL-Scanner
 - Malware-Scanner
 - Content-Scanner
- Sehr **flexible Aktionen** (Allow, Block, Authorized Override, Coaching, Delay, Quotas, Timeframes)
- Bindung der Policy an IP-Adressen, Namen
- Lokale Datenbank mit inkrementellen Updates
 - Alle 3 Stunden wird geprüft
 - Ca. 1-2 mal am Tag Änderungen der Datenbank

=> **nicht Realtime**



- 98 Kategorien, davon 10 Security Relevant
 - Criminal Activities
 - Malicious Sites
 - Hacking/Computer Crime
 - Spyware/Adware
 - Phishing
 - Spam URLs
 - Illegal Software
 - Anonymizers
 - Anonymizing Utilities
 - Residential IP Addresses
- Block gemäß Web-Reputation möglich
- Einsicht in Kategorien und Bewertungen unter
 - <http://www.trustedsource.com/>



■ Exemplarische Fehlermeldung

Webwasher - Notification - Mozilla Firefox

http://www.playboy.de/

Fehlermeldung

Anforderung von URL-Filter-Datenbank geblockt

Ihre Anforderung der URL <http://www.playboy.de/> wurde durch die URL-Filter-Datenbank von Webwasher geblockt.

Die URL wurde in die Kategorie(n) Pornography eingestuft und der Reputationsstufe "Neutral" zugeordnet. Der Zugriff darauf ist aufgrund der Einstellungen, die Ihr Administrator vorgenommen hat, nicht erlaubt.

Seriennummer der URL-Filter-Datenbank: 21792

Meldung erstellt am 22/Feb/2010:16:04:56 +0100

Fertig

■ TrustedSource Bewertung

Information for 'www.playboy.de'

This page shows general information on the domain playboy.de, its message volume and the number of unique IPs sending email during the last 30 days, and IP addresses in this domain sending substantial amounts of email.

Is this your domain? Request more in depth information with our [Domain Health Check](#) !

Web Reputation

Reputation: 2010-02-22

Minimal Risk Unverified Medium Risk High Risk

SmartFilter Category: Pornography

[Make Category Suggestions](#)

IP: [193.201.12.60](#)

Nameservers: [ns1-chi.playboy.com](#)
[ns15.customer.level3.net](#)
[ns2-chi.playboy.com](#)
[ns21.customer.level3.net](#)
[ns29.customer.level3.net](#)



- **Zentrale Administration** durch Proxy Security Gateway
- Umgehung durch den Benutzer **unmöglich** sofern Proxy Zwang konfiguriert
- Enterprise Lösung
- Lokale Datenbank
- **Umfangreiche Kategorien**
- Nutzbar mit **jedem** Browser
- **Kein Realtime!**

- Für große Installationen mit feingranularen Einstellmöglichkeiten geeignet
- **Sehr flexible Lösung**



- SDK für Integration in OEM Lösung
- Teil der Gesamtlösung von Commtouch für Realtime Dienste
- Commtouch liefert für einen Deep Link bis zu 5 Kategorien
- Aktionen werden durch OEM realisiert
 - Allow
 - Block
- Bindung der Policy wird durch OEM realisiert
 - IP-Adressen
 - Namen möglich
- Lokaler Cache
 - Realtime Abfrage
 - Caching liegt überlicherweise bei >99 %



- 64 Kategorien, davon 8 Security relevant
 - Anonymizers
 - Compromised
 - Criminal Activity
 - Phishing & Fraud
 - Spam Sites
 - Malware
 - Botnets
 - Hacking
 - Illegal Software

- Einsicht in Kategorien und Bewertungen unter
 - Pallas Kundenportal für Pallas Kunden
 - <http://www.commtouch.com/url-miscat>



■ Exemplarische Fehlermeldung

FEHLER

Der angeforderte URL konnte nicht geholt werden

Während des Versuches, den URL **http://www.playboy.de/** zu laden, trat der folgende Fehler auf:

- Zugriff verweigert auf Basis der Pallas RealTime URL Filter Datenbank powered by Commtouch

- Anfragende IP: 10.234.1.222
- Benutzername: ssachweh
- Kategorien der URL:

33 Pornography/Sexually Explicit

Aufgrund von Zugriffsbeschränkungen ist Ihre Anfrage zur Zeit nicht erlaubt.
Bitte kontaktieren Sie Ihren Service Provider, wenn Sie der Meinung sind, daß dies nicht korrekt ist.

- Rot markiert Daten des aufrufenden Benutzers

■ Commtouch Kategorie(n)

 pallas Pallas Kundenportal

Commtouch Realtime Web Security

Web-Adresse (URL):

URL	CatID	KategorieName
www.playboy.de	33	Pornography/Sexually Explicit

Kommentar für diese Meldung (optional)



- Kategorisierung von **Deep Links** schützt vor Malware
 - auf **Community Sites** wie z.B. Facebook, Xing, Linked-In, Blogspot
 - auf infizierten, **regulären Seiten**
- Realtime durch
 - **in the Cloud** Echtzeitabfrage beschleunigt durch Cache
 - Integration mit Real-Time Anti-Spam und Zero-Hour Mail-Security
 - **URLs in Malware/Spam Mails** werden in Echtzeit kategorisiert
 - Häufung von Kategorie „Unbekannt“ führt zur Kategorisierung, **User Feedback Schleife**



- **Zentrale Administration** durch Proxy Security Gateway
- Umgehung durch den Benutzer **unmöglich** sofern Proxy Zwang konfiguriert
- Enterprise Lösung
- Lokaler Cache (> 99% Cache Hit Rate)
- **Umfangreiche Kategorien**
- Nutzbar mit **jedem** Browser
- **Realtime!**
- **Deep Links werden bewertet!**

- Technologisch High End
- Für große und mittlere Installationen geeignet, „kleine“ Installationen über Pallas Mietmodell

Ein Bewertungsbeispiel



"Anwalt" <anwalteq@gmx.de> - Montag 21.09.2009 10:37

Rechnung
Anwalt an: Administrator
Bitte antworten an "Anwalt" <anwalteq@gmx.de>

Sehr geehrte Damen und Herren,

vielen Dank für ihre Anmeldung bei unserem Online Casino.
Bitte holen Sie ihr Geld Gewinn über 136,52 Euro ab.

Hier sind ihre Zugangsdaten:

Ihr User Name: cyberstar-881753
Ihr Passwort: Rtw

Ihre IP Adresse wurde bei der Anmeldung gespeichert.

Ihre IP: 217.136.112.153
Uhrzeit: 21:47 Uhr

Auf ihren Spielerkonto sind aktuell:

Betrag: 136,52 Euro

Letzte Kontobewegung: Gestern um 21:47 Uhr.

Sie können ihr Geld einfach und direkt auszahlend
Downloaden. Starten Sie einfach kostenlos
dann können Sie sofort über ihr Geld verfüge

<http://luckygames365.net>

Unser Online Casino hat ein Gütesiegel vom Computer Bild und ist Testsieger von 2009.

comintouch
Real Security. In Real Time.

URL:
Malware

[View Current URL Classification](#)

McAfee | TrustedSource™

McAfee Web Gateway (Webwasher) versions >= 6.5

[Check URL](#)

URL	Status	Categorization	Reputation
http://luckygames365.net	Categorized URL	- Games	Unverified