

## Microsoft-Analyse zur IT-Sicherheit – Ausgabe 6 (Juli bis Dezember 2008)

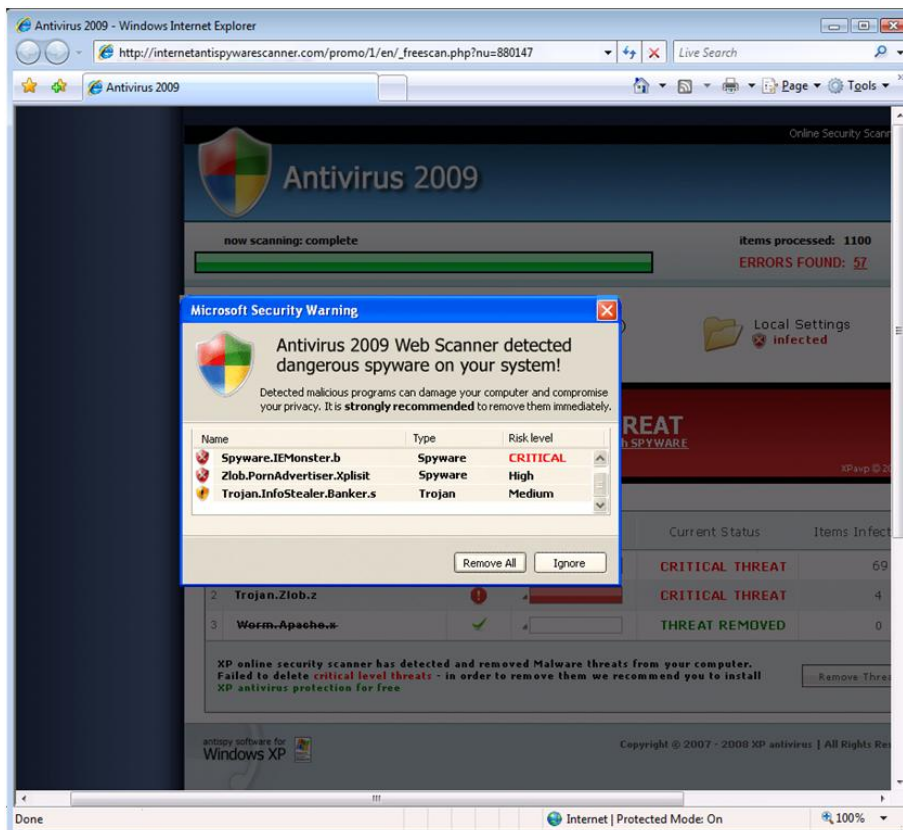
### Zusammenfassung der wichtigsten Ergebnisse

Die 6. Ausgabe der Microsoft®-Analyse zur IT-Sicherheit bietet einen umfassenden Überblick über die von Microsoft in den letzten Jahren beobachteten Software-Sicherheitschwachstellen (sowohl bei Microsoft-Software als auch bei Software von Drittanbietern) und Software-Exploits sowie über Trends bezüglich schädlicher oder potenziell unerwünschter Software. Die Analyse konzentriert sich auf die zweite Hälfte des Jahres 2008 (2H08)<sup>1</sup>. Sie enthält neue Informationen zu Pseudo-Sicherheitssoftware, browserbasierten Exploits und Exploits auf Basis beliebiger Dokumentformate sowie aktualisierte Informationen zu Sicherheits- und Datenschutzverletzungen.

In diesem Dokument sind die wichtigsten Ergebnisse der Analyse zusammengefasst. Die vollständige Analyse zur IT-Sicherheit stellt darüber hinaus Strategien sowie Risikominderungs- und Gegenmaßnahmen vor. Sie kann unter der folgenden Adresse heruntergeladen werden: <http://www.microsoft.com/sir>.

### Rogue Security Software (Pseudo-Sicherheitssoftware, Scareware)

Die Verbreitung von Pseudo-Sicherheitssoftware ist in den letzten drei Halbjahren deutlich angestiegen (siehe Kategorie „Versch. Trojaner“ in Abbildung 16 unten). Pseudo-Sicherheitssoftware setzt Angst- und Belästigungstaktiken ein, um Betroffene davon zu überzeugen, für „Vollversionen“ der Software zu zahlen, um damit Malware zu entfernen und sich vor dieser zu schützen und/oder um die fortwährenden Mitteilungen und Warnungen zu beenden. Beispiele für Social Engineering-Techniken von Pseudo-Sicherheitssoftware, einschließlich Screenshots, sind in der vollständigen Microsoft-Analyse zur IT-Sicherheit zu finden. Die Analyse beinhaltet auch einen Schwerpunktbereich zu rechtlichen Schritten gegen Verteiler von Pseudo-Sicherheitssoftware.



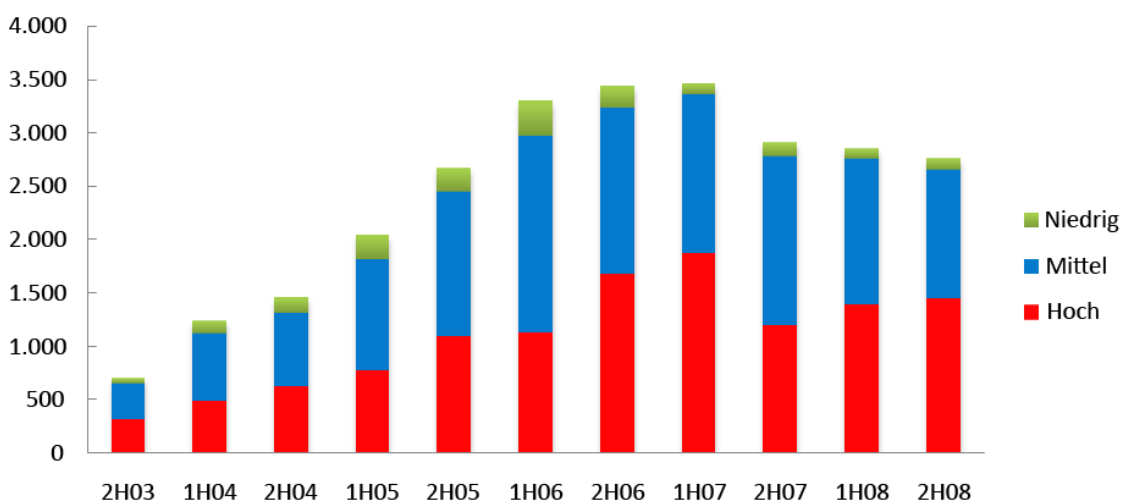
<sup>1</sup> Die in diesem Bericht verwendete Nomenklatur für verschiedene Analysezeiträume ist „nHJJ“, wobei sich „nH“ auf die erste (1) oder zweite (2) Jahreshälfte bezieht und „JJ“ das Jahr angibt. Beispielsweise steht „2H08“ für die zweite Hälfte (1. Juli bis 31. Dezember) des Jahres 2008 und „1H08“ für die erste Hälfte (1. Januar bis 30. Juni) des Jahres 2008.

## Veröffentlichung von Sicherheitsschwachstellen

Sicherheitsschwachstellen sind Lücken in Softwareprogrammen, über die ein Angreifer die Integrität, Verfügbarkeit oder Vertraulichkeit dieser Software gefährden kann. Im schlimmsten Fall erhält ein Angreifer aufgrund einer Sicherheitsschwachstelle die Möglichkeit, schädlichen Code auf gefährdeten Systemen auszuführen. Die Daten zu Sicherheitsschwachstellen in diesem Abschnitt stammen von Drittanbietern sowie aus veröffentlichten Berichten und eigenen Daten von Microsoft.

- In der gesamten Branche wurden im 2H08 insgesamt weniger Sicherheitsschwachstellen gemeldet, wobei die Verringerung bei 3 Prozent gegenüber dem 1H08 lag. Für das gesamte Jahr 2008 wurden insgesamt 12 Prozent weniger Sicherheitsschwachstellen gemeldet als im Jahr 2007.
- Im Gegensatz dazu stieg die Anzahl der Sicherheitsschwachstellen, die nach dem Common Vulnerability Scoring System (CVSS)<sup>2</sup> mit dem Schweregrad „Hoch“ eingestuft werden, gegenüber dem 1H08 um 4 Prozent. Insgesamt wurden rund 52 Prozent aller Sicherheitsschwachstellen mit dem Schweregrad „Hoch“ eingestuft. Für das gesamte Jahr 2008 wurden insgesamt 16 Prozent weniger Sicherheitsschwachstellen mit dem Schweregrad „Hoch“ gemeldet als im Jahr 2007.

**Abbildung 1: Industrieweit gemeldete Veröffentlichungen von Sicherheitsschwachstellen nach CVSSv2-Schweregrad pro Halbjahr, 2H03 bis 2H08**

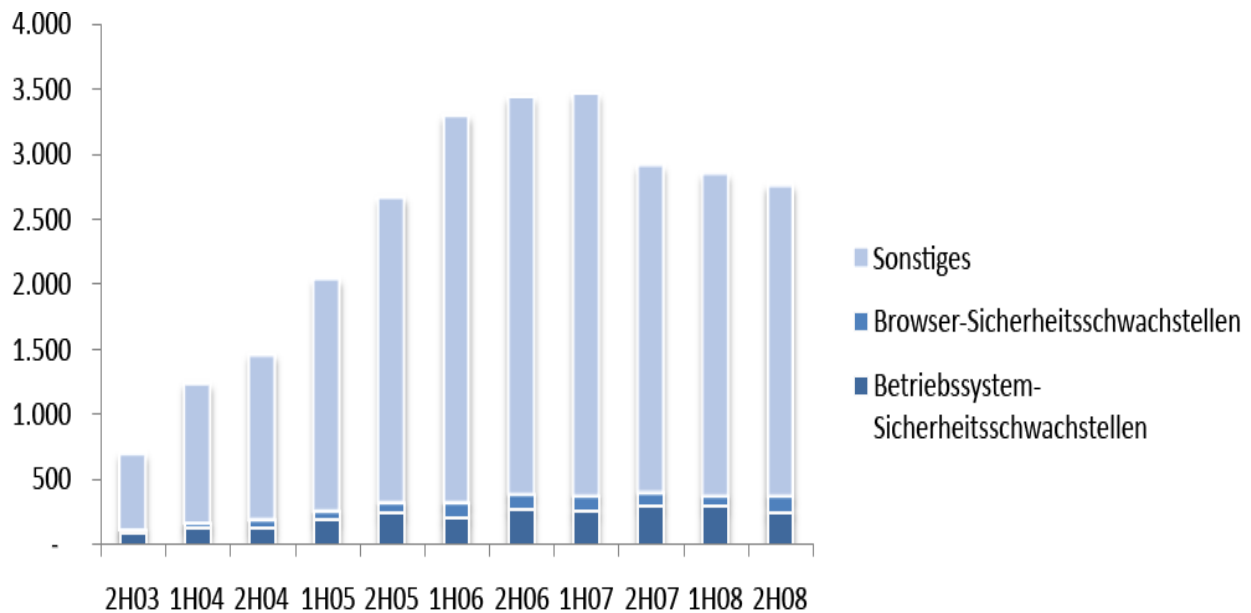


- Zusätzlich zum Anstieg der Sicherheitsschwachstellen mit dem Schweregrad „Hoch“ ist festzustellen, dass sich der Anteil der veröffentlichten leicht auszunutzenden Sicherheitsschwachstellen ebenfalls erhöht hat: Für die Ausnutzung von 56 Prozent der Sicherheitsschwachstellen war nur ein geringes Maß an Komplexität erforderlich.<sup>3</sup>
- Der Anteil veröffentlichter Sicherheitsschwachstellen in Betriebssystemen ist in der gesamten Branche weiterhin gesunken. Über 90 Prozent der veröffentlichten Sicherheitsschwachstellen betrafen Anwendungen oder Browser.

<sup>2</sup> CVSS ist ein Industriestandard zum Bewerten des Schweregrads von Softwaresicherheitsschwachstellen. Weitere Informationen finden Sie unter <http://www.first.org/cvss/>.

<sup>3</sup> Definition: Mell, Peter, Karen Scarfone und Sasha Romanosky: „A Complete Guide to the Common Vulnerability Scoring System Version 2.0“ (<http://www.first.org/cvss/cvss-guide.html>) Abschnitt 2.1.2.

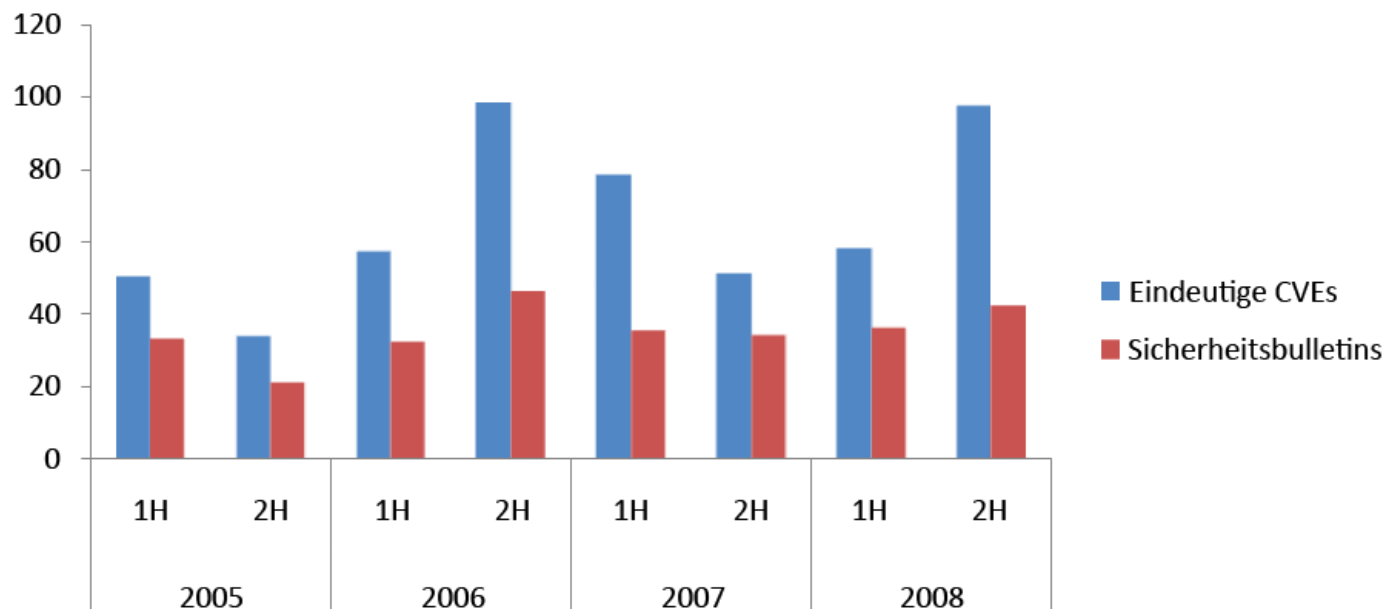
**Abbildung 2: Industrieweit gemeldete System-, Browser- und sonstige Sicherheitsschwachstellen, 2H03 bis 2H08**



### Einzelheiten zu Microsoft-Sicherheitsschwachstellen im 2H08

Im 2H08 wurden von Microsoft 42 Sicherheitsbulletins veröffentlicht, die 97 verschiedene CVE-identifizierte Sicherheitsschwachstellen betrafen. Dies war eine Steigerung von 67,2 Prozent verglichen mit der Anzahl der im 1H08 veröffentlichten Sicherheitsschwachstellen. Im gesamten Jahr 2008 wurden von Microsoft 78 Sicherheitsbulletins veröffentlicht, die 155 Sicherheitsschwachstellen betrafen – eine Steigerung von 16,8 Prozent gegenüber dem Jahr 2007.

**Abbildung 3: Veröffentlichte Sicherheitsbulletins und betroffene CVEs pro Halbjahr, 1H05 bis 2H08**

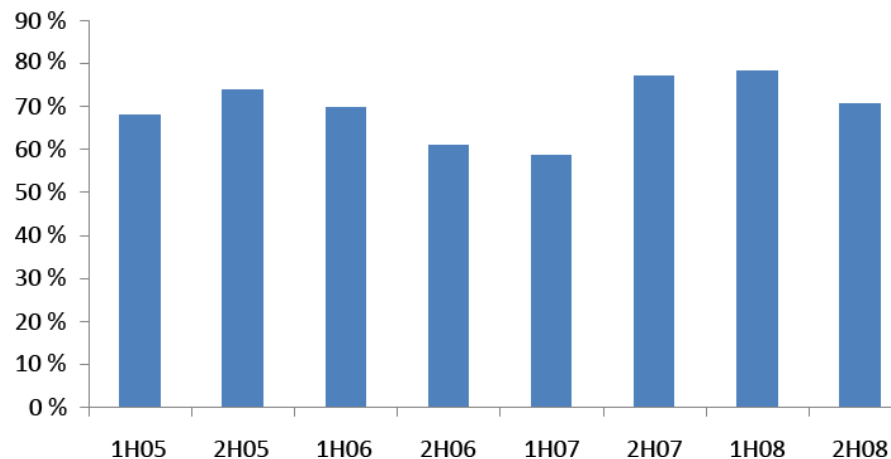


## Verantwortungsvolle Veröffentlichung

*Responsible Disclosure* („Verantwortungsvolle Veröffentlichung“) bedeutet, dass Sicherheitsschwachstellen auf vertrauliche Weise dem betroffenen Hersteller mitgeteilt werden, damit dieser ein umfassendes Sicherheitsupdate für die Sicherheitsschwachstelle entwickeln kann, bevor die Einzelheiten zu der Sicherheitsschwachstelle veröffentlicht werden. Diese Vorgehensweise erhöht die Sicherheit für Benutzer, da sie verhindert, dass potenzielle Angreifer von neu entdeckten Sicherheitsschwachstellen erfahren, bevor Sicherheitsupdates zur Verfügung stehen.

- Im 2H08 wurden bei 70,6 Prozent der veröffentlichten Microsoft-Sicherheitsschwachstellen die Methoden der verantwortungsvollen Veröffentlichung befolgt. Dieser Anteil fiel im Vergleich zu den 78,2 Prozent aus dem 1H08 geringer aus. Im gesamten Jahr 2008 war der Anteil der verantwortungsvollen Veröffentlichungen deutlich größer als im Vorjahr.
- Die direkte Kommunikation mit der Sicherheits-Community und die proaktive Vorgehensweise bei Sicherheitsproblemen tragen dazu bei, dass die Mehrheit der Probleme verantwortungsvoll gemeldet wird.

**Abbildung 4: Anteil der verantwortungsvollen Veröffentlichungen von Sicherheitsschwachstellen an allen Veröffentlichungen, 1H05 bis 2H08**



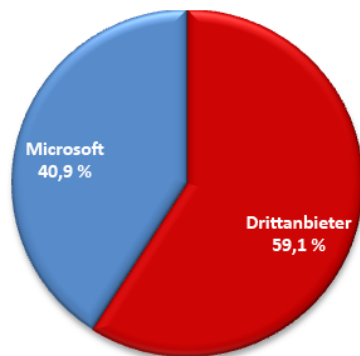
## Browserbasierte Exploits

Um die relative Verbreitung browserbasierter Exploits im 2H08 zu bewerten, analysierte Microsoft Datensample von Vorfällen bei Kunden, eingereichten Schadcode und Microsoft Windows®-Fehlerberichte. Die Daten beziehen sich auf mehrere Betriebssysteme und Browserversionen, von Windows XP bis hin zu Windows Vista®. Weiterhin sind Daten von Browsern von Drittanbietern enthalten, die das Internet Explorer-Renderingmodul „Trident“ hosten.<sup>4</sup>

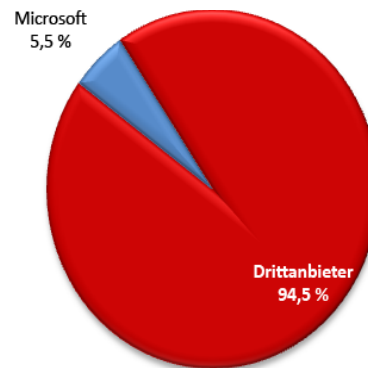
- Browserbasierte Exploits waren mit 32,4 Prozent aller Vorfälle am häufigsten in der Systemsprache Englisch (USA) zu finden, gefolgt von Chinesisch (vereinfacht) mit 25,6 Prozent aller Vorfälle.
- Browserbasierte Angriffe auf Windows XP-basierte Computer machten 40,9 Prozent aller Microsoft-Sicherheitsschwachstellen aus – eine leichte Verringerung verglichen mit 42 Prozent im 1H08. Für Windows Vista-basierte Computer war der Microsoft-Anteil mit nur 5,5 Prozent der Gesamtanzahl wesentlich geringer; im 1H08 waren noch 6 Prozent zu verzeichnen gewesen.

<sup>4</sup> Weitere Informationen zu Trident finden Sie unter [http://msdn.microsoft.com/de-de/library/aa939274\(en-us\).aspx](http://msdn.microsoft.com/de-de/library/aa939274(en-us).aspx).

**Abbildung 5: Browserbasierte Exploits für Microsoft- und Drittanbieter-Software auf Computern mit Windows XP im 2H08**

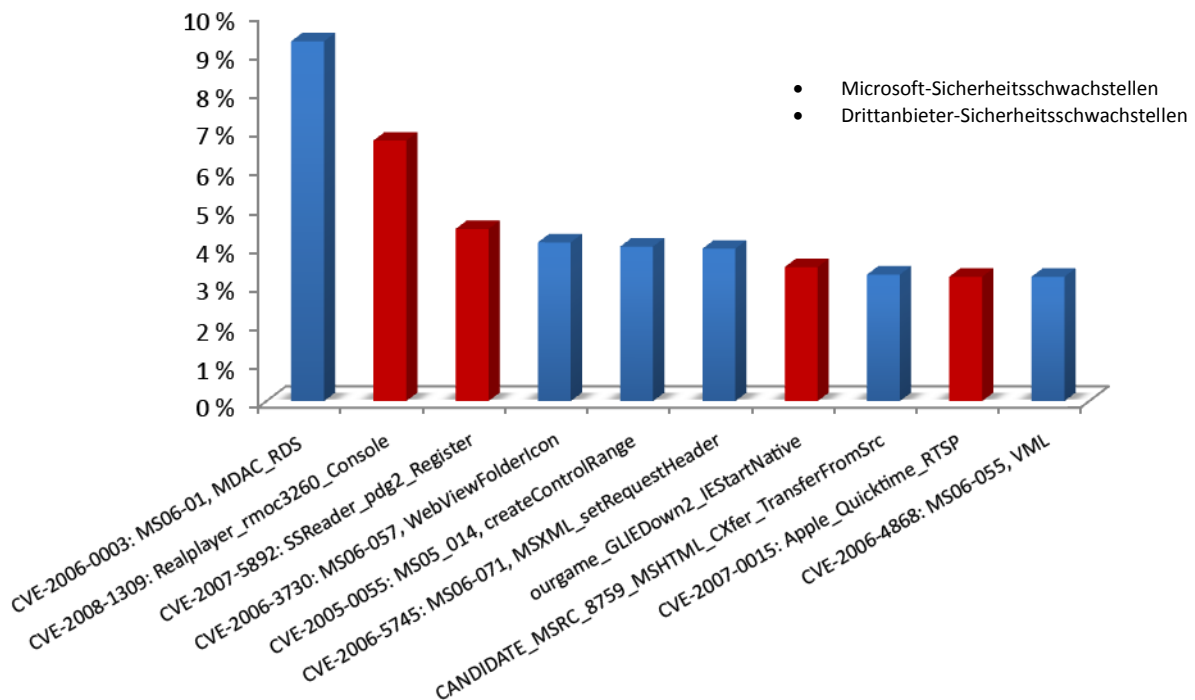


**Abbildung 6: Browserbasierte Exploits für Microsoft- und Drittanbieter-Software auf Computern mit Windows Vista im 2H08**

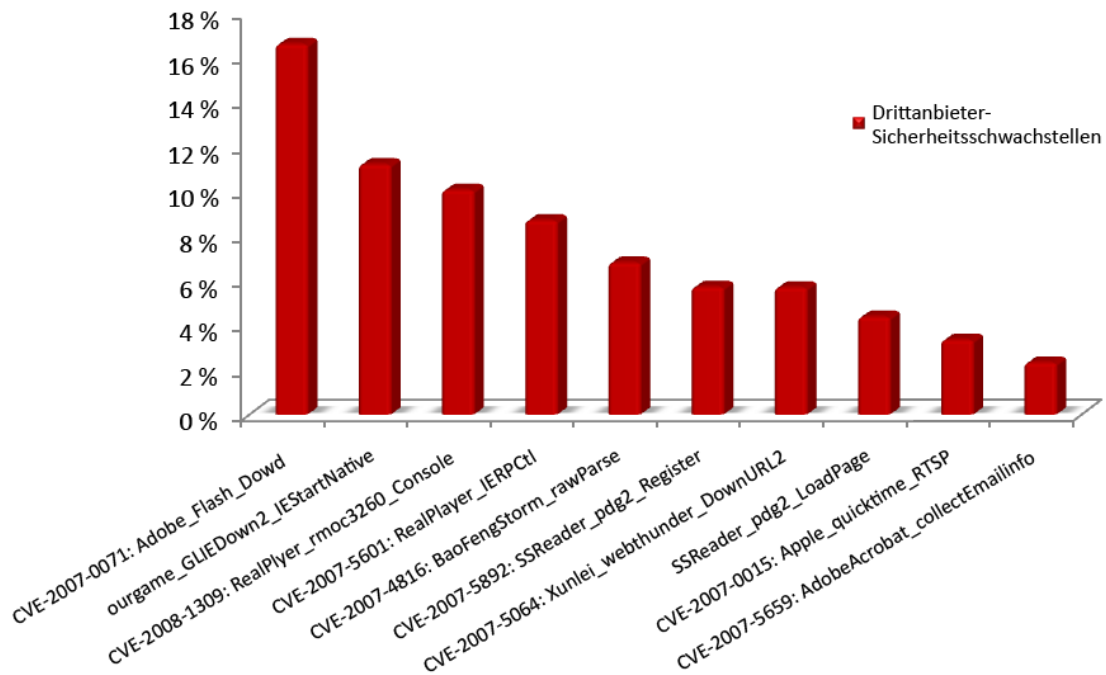


- Der Anteil von Microsoft-Software lag bei 6 der 10 browserbasierten Sicherheitsschwachstellen, die im 2H08 Angriffe auf Computer mit Windows XP ermöglichten, wobei sich der Anteil bei Windows Vista-Computern auf Null belief – ähnlich dem im 1H08 beobachteten Muster. In den folgenden Abbildungen werden die 10 browserbasierten Hauptsicherheitsschwachstellen verdeutlicht, die Angriffe auf Windows XP-basierte und Windows Vista-basierte Computer ermöglichten. Für jede Sicherheitsschwachstelle ist die relevante Nummer des CVSS-Bulletins bzw. des Microsoft-Sicherheitsbulletins aufgeführt.

**Abbildung 7: Die Top 10 der browserbasierten Sicherheitsschwachstellen, die im 2H08 auf Computern mit Windows XP ausgenutzt wurden**



**Abbildung 8: Die Top 10 der browserbasierten Sicherheitsschwachstellen, die im 2H08 auf Computern mit Windows Vista ausgenutzt wurden**



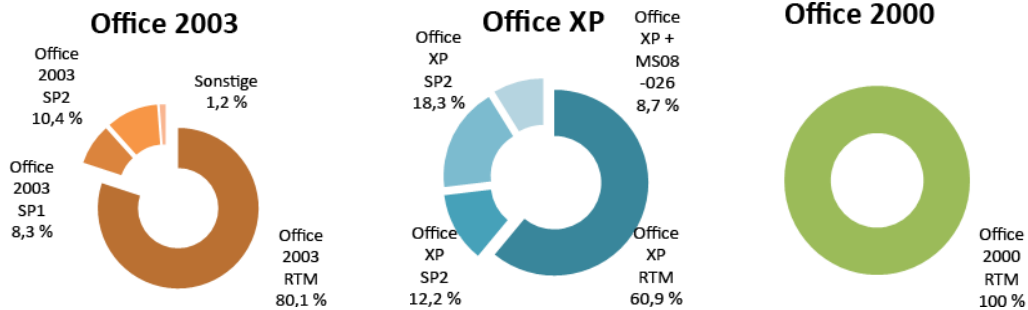
### Exploits auf der Basis von Dokumentdateiformaten

Angrifer verwenden verstärkt gängige Dateiformate als Übertragungsvektoren für Exploits. Die meisten modernen E-Mail- und Instant Messaging-Programme sind so konfiguriert, dass sie die Übertragung von potenziell gefährlichen Dateien anhand der Dateierweiterung blockieren. Diese Programme lassen in der Regel jedoch die Übertragung von verbreiteten Dateiformaten wie Microsoft Office und Adobe Portable Document Format (PDF) zu. Diese Formate werden täglich von vielen Benutzern auf vollkommen legitime Weise verwendet, deshalb schien ein Blockieren bisher nicht nötig. Dies hat die Formate zu einem attraktiven Ziel für die Entwickler von Exploits gemacht.

#### Dateien im Microsoft Office-Format

- Die am häufigsten ausgenutzten Sicherheitsschwachstellen in Microsoft Office-Software gehörten auch zu den ältesten. 91,3 Prozent der untersuchten Angriffe nutzten eine einzige Schwachstelle aus, für die seit mehr als zwei Jahren ein Sicherheitsupdate zur Verfügung steht (CVE-2006-2492).
- Dateiformatbasierte Exploits waren mit 32,5 Prozent aller Vorfälle am häufigsten in der Systemsprache Englisch (USA) zu finden, gefolgt von Chinesisch (traditionell) mit 15,7 Prozent aller Vorfälle.
- In den meisten Fällen waren für die angegriffenen Anwendungsversionen keine aktuellen Service Packs installiert worden. Bei jeder Version betraf die klare Mehrheit der Angriffe die RTM-Version (Release to Manufacturing) der Anwendung, für die keine Service Packs installiert worden waren. Im Fall von Office 2000 betrafen beispielsweise 100 Prozent der Angriffe die RTM-Version der Anwendungssuite, die 1999 veröffentlicht wurde, obwohl seit dem Jahr 2000 zahlreiche Service Packs und andere Sicherheitsupdates veröffentlicht wurden.

**Abbildung 9: Angriffe nach Updateversion für Office 2003, Office XP und Office 2000 im Datensample infizierter Computer im 2H08**

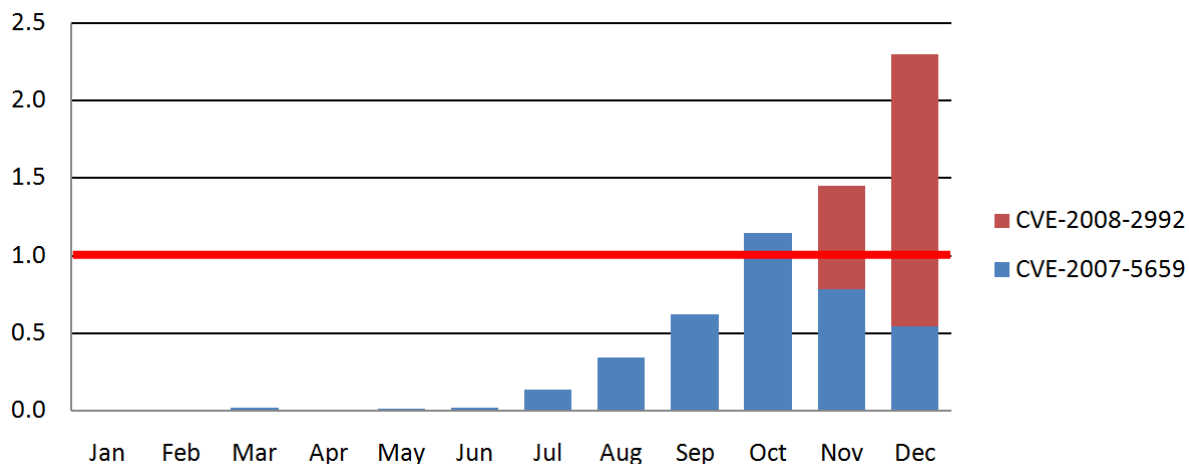


### Dateien im Adobe PDF-Format

Die Verwendung des PDF-Formats als Angriffsvektor ist im 2H08 stark angestiegen, wobei im Juli mehr als doppelt so viele Angriffe zu verzeichnen waren als im gesamten 1H08. In den verbleibenden Monaten des Jahres wurde die Zahl weiterhin jeweils verdoppelt bzw. beinahe verdoppelt.

- In den untersuchten Datensample waren zwei Sicherheitsschwachstellen für alle Angriffe verantwortlich (CVE-2008-2992 und CVE-2007-5659). Für beide Sicherheitsschwachstellen sind Sicherheitsupdates von Adobe verfügbar. In aktuellen Versionen der betroffenen Adobe-Produkte sind die Sicherheitsschwachstellen nicht vorhanden.

**Abbildung 10: Adobe Reader-Exploits nach Monaten im Jahr 2008, gemessen am 2H08-Durchschnitt**



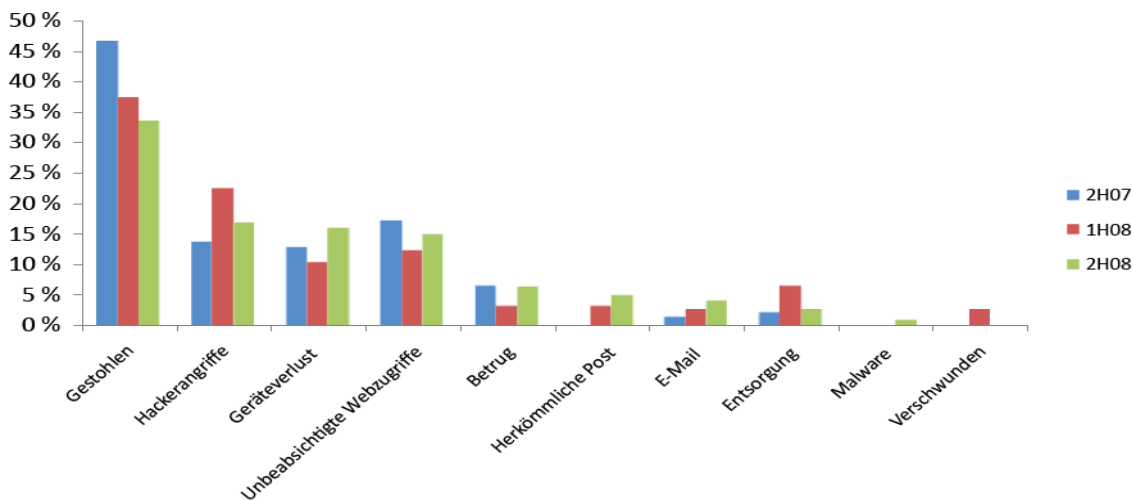
### Trends bei Sicherheitsverletzungen

In diesem Abschnitt der Analyse werden die weltweit gemeldeten Sicherheitsverletzungen eingehender untersucht. Dies erfolgt anhand von Daten aus der OSF Data Loss Database der Open Security Foundation, zu finden unter <http://datalossdb.org>.

- Datenverluste aufgrund von Sicherheitsverletzungen ergaben sich im 2H08 nach wie vor in erster Linie aus dem Diebstahl von Geräten wie Laptops (33,5 Prozent aller veröffentlichten Datenverluste). Zusammen mit verlorenen Geräten machte dies 50 Prozent aller veröffentlichten Vorfälle aus.
- Sicherheitsverletzungen durch Hackerangriffe oder Malware machen weiterhin weniger als 20 Prozent aller Vorfälle aus.
- Diese Ergebnisse unterstreichen die Notwendigkeit passender Datenverwaltungsrichtlinien und -methoden.<sup>5</sup>

<sup>5</sup> Microsoft bietet Ressourcen und Anleitungen für die Datenverwaltung unter <http://www.microsoft.com/mscorp/twc/privacy/datagovernance/default.aspx>

**Abbildung 11: Anteil der Sicherheitsverletzungen nach Typ, 2H07 bis 2H08**

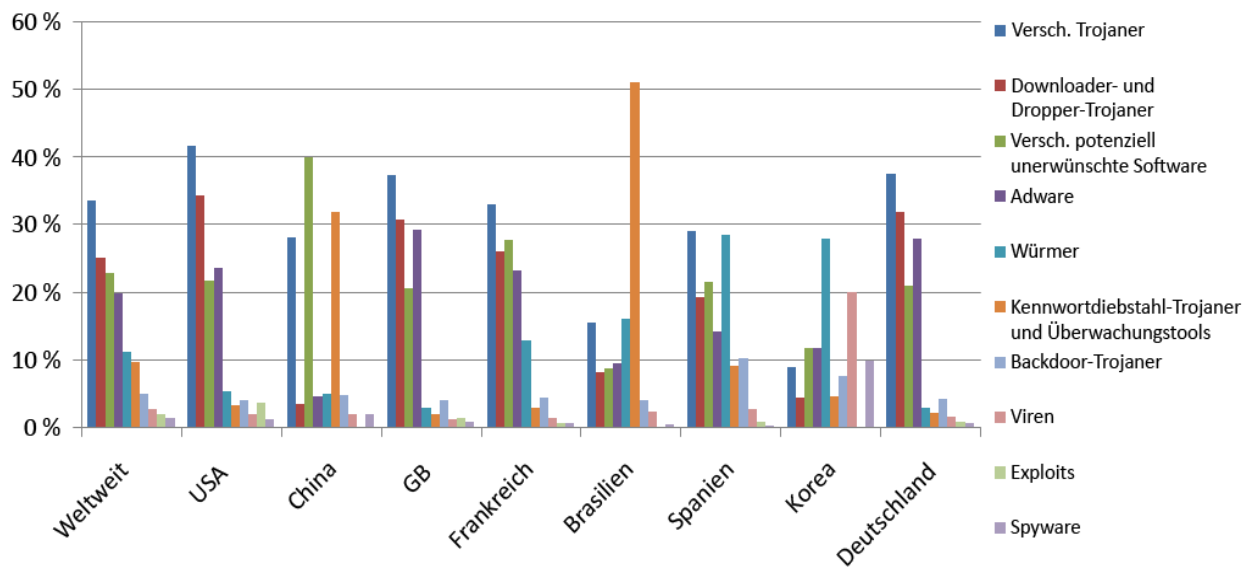


## Schädliche und potenziell unerwünschte Software Weltweite Trends

Mit expliziter Zustimmung der Benutzer werden durch Microsoft-Sicherheitsprodukte Daten bezüglich schädlicher und potenziell unerwünschter Software von vielen Millionen Computersystemen weltweit und aus den am intensivsten genutzten Internet-Onlinediensten gesammelt. Durch Analyse dieser Daten ergibt sich eine einzigartige, umfassende Übersicht über die weltweiten Aktivitäten in den Bereichen Malware und potenziell unerwünschte Software.

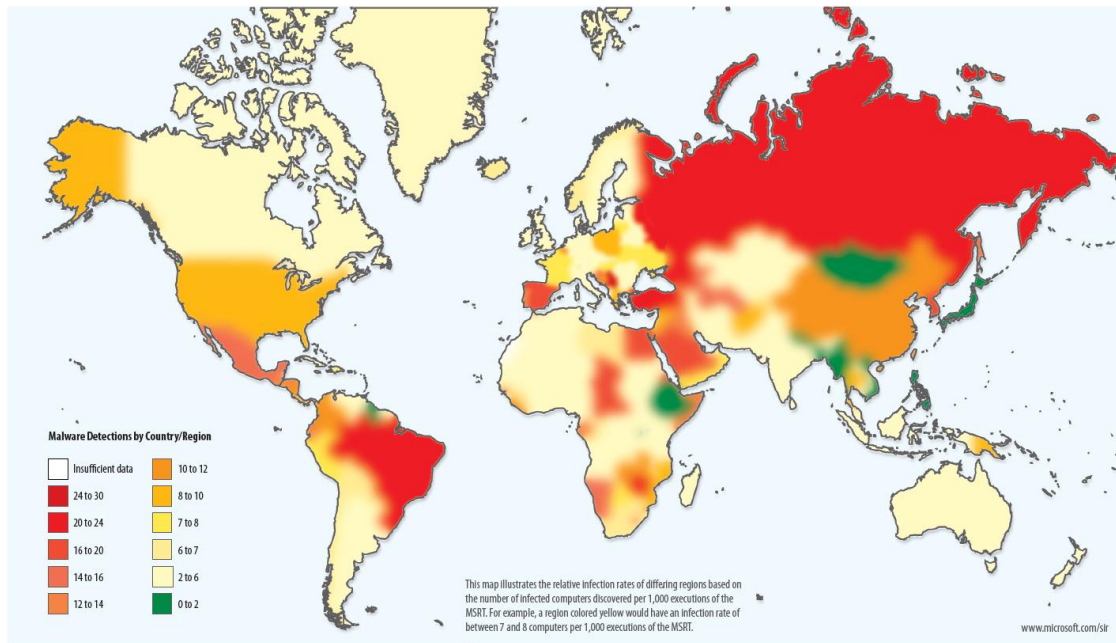
- Trotz der globalen Ausrichtung des Internets sind die Arten der Bedrohungen, die Benutzer in den verschiedenen Teilen der Welt betreffen, sehr unterschiedlich. Je mehr sich das Malwareumfeld auf Social Engineering verlässt, umso mehr hängen Bedrohungen weltweit von sprachlichen und kulturellen Faktoren ab: So sind in China mehrere schädliche Browser Modifier im Umlauf, in Brasilien ist vor allem Malware verbreitet, die Benutzer von Onlinebanken angreift, und in Korea sind Viren wie Win32/Virut und Win32/Parite üblich.

**Abbildung 12: Bedrohungskategorien weltweit und an den acht Standorten mit den meisten bereinigten Computern im 2H08, Verteilung nach Vorfall**



- Auf der folgenden Karte sind die Infektionsraten in verschiedenen Ländern/Regionen in CCM dargestellt<sup>6</sup>.

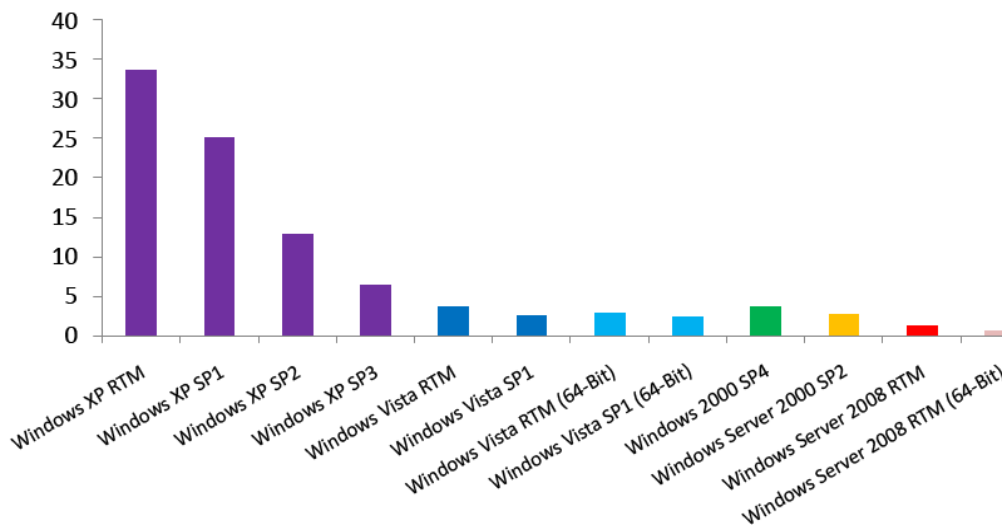
**Abbildung 13: Infektionsraten nach Land/Region im 2H08**



### Betriebssystem-Trends

- Die verschiedenen Microsoft Windows-Betriebssystemversionen zeigen aufgrund der unterschiedlichen Verwendung der einzelnen Versionen durch Benutzer und Unternehmen sowie aufgrund der verschiedenen Funktionen und verfügbaren Service Packs unterschiedliche Infektionsraten.

**Abbildung 14: Anzahl bereinigter Computer pro 1000 Anwendungen des MSRT im 2H08, nach Betriebssystem**



<sup>6</sup> Die Infektionsraten in diesem Bericht wurden anhand einer Metrik namens „Computers Cleaned per Mil“ (CCM) berechnet, der Anzahl von Computern, die pro eintausend Anwendungen des MSRT bereinigt wurden.

- Die Infektionsrate von Windows Vista liegt bei allen Konfigurationen erheblich unter der des Vorgängersystems Windows XP.
  - Beim Vergleich der neuesten Service Packs für die einzelnen Versionen liegt die Infektionsrate von Windows Vista SP1 um 60,6 Prozent niedriger als die von Windows XP SP3.
  - Beim Vergleich der RTM-Versionen dieser Betriebssysteme ist die Infektionsrate der RTM-Version von Windows Vista um 89,1 Prozent niedriger als die der RTM-Version von Windows XP.
- Die Infektionsrate von Windows Server 2008 RTM ist um 52,6 Prozent niedriger als die des Vorgängersystems Windows Server 2003 SP2.
- Je höher die Service Pack-Version, umso niedriger ist die Infektionsrate. Dieser Trend kann bei allen Client- und Serverbetriebssystemen festgestellt werden. Dafür gibt es zwei Gründe:
  - Service Packs beinhalten alle zuvor veröffentlichten Sicherheitsupdates. Sie können außerdem zusätzliche Sicherheitsfunktionen, Risikominderungsmaßnahmen oder Änderungen an den Standardeinstellungen zum Schutz der Benutzer enthalten.
  - Benutzer, die Service Packs installieren, warten ihre Computer in der Regel besser als Benutzer, die keine Service Packs installieren. Erstere sind zudem oft vorsichtiger beim Surfen im Internet, beim Öffnen von Anhängen und bei anderen Aktivitäten, die Computer für Angriffe anfällig machen können.
- Serverversionen von Windows zeigen in der Regel eine niedrigere durchschnittliche Infektionsrate als Clientversionen. Server haben oft eine geringere effektive Angriffsfläche als Computer, auf denen Clientbetriebssysteme ausgeführt werden, da sie eher unter kontrollierten Bedingungen von geschulten Administratoren verwendet und durch mindestens eine Sicherheitsschicht geschützt werden. Insbesondere Windows Server 2003 und die Nachfolgerversionen sind auf verschiedene Weise besser gegen Angriffe geschützt.

### Die Bedrohungslandschaft im privaten Bereich und in Unternehmen

- Computer, auf denen Forefront Client Security ausgeführt wird (normalerweise in Unternehmensumgebungen), waren wesentlich häufiger mit Würmern infiziert als Heimcomputer, auf denen Windows Live OneCare ausgeführt wird. Auf Heimcomputern war dagegen ein deutlich größerer Anteil von Trojanern, Downloader- und Dropper-Trojanern, Adware und Exploits zu finden. Die Anteile von entdeckten Backdoor-Trojanern und Spyware waren bei beiden Produkten ähnlich.

**Abbildung 15: Von Windows Live OneCare und Forefront Client Security im 2H08 entfernte Familienkategorien nach Anteil an der Gesamtanzahl der von jedem Programm bereinigten Computer**

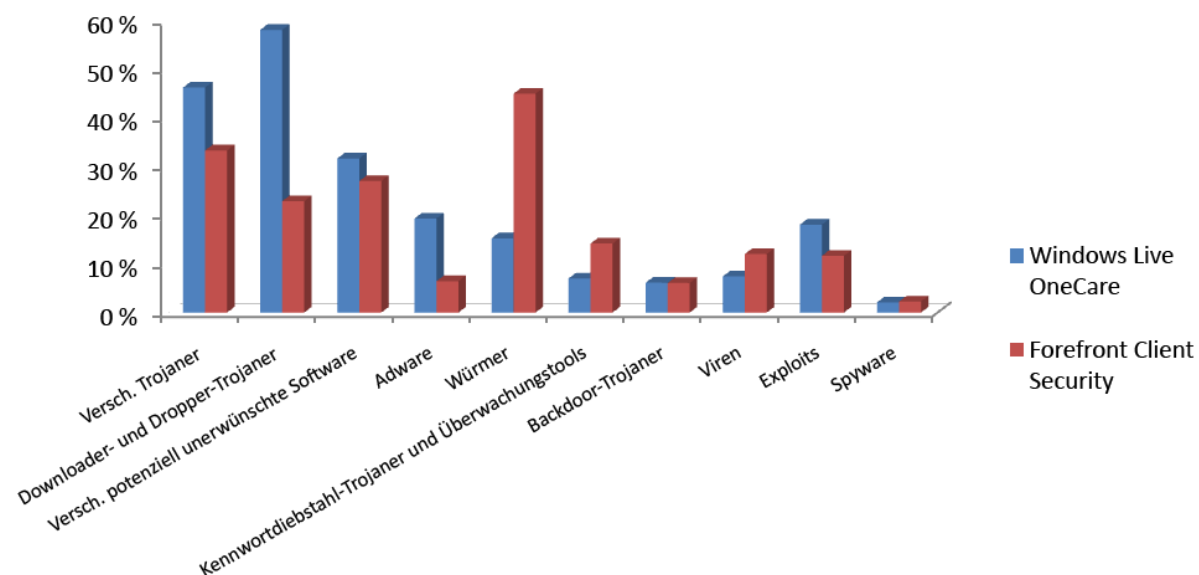
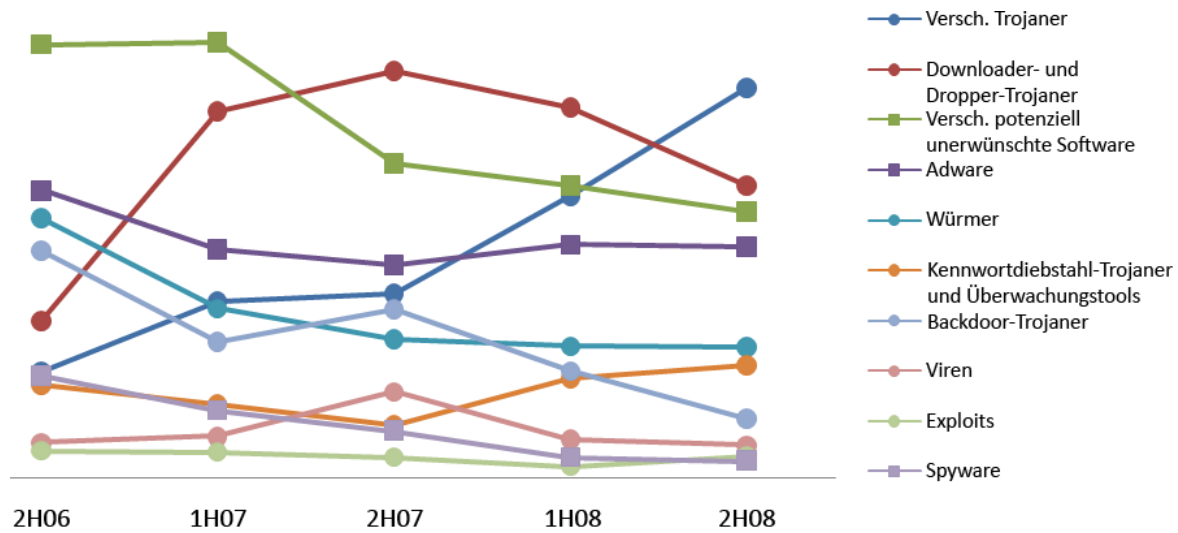


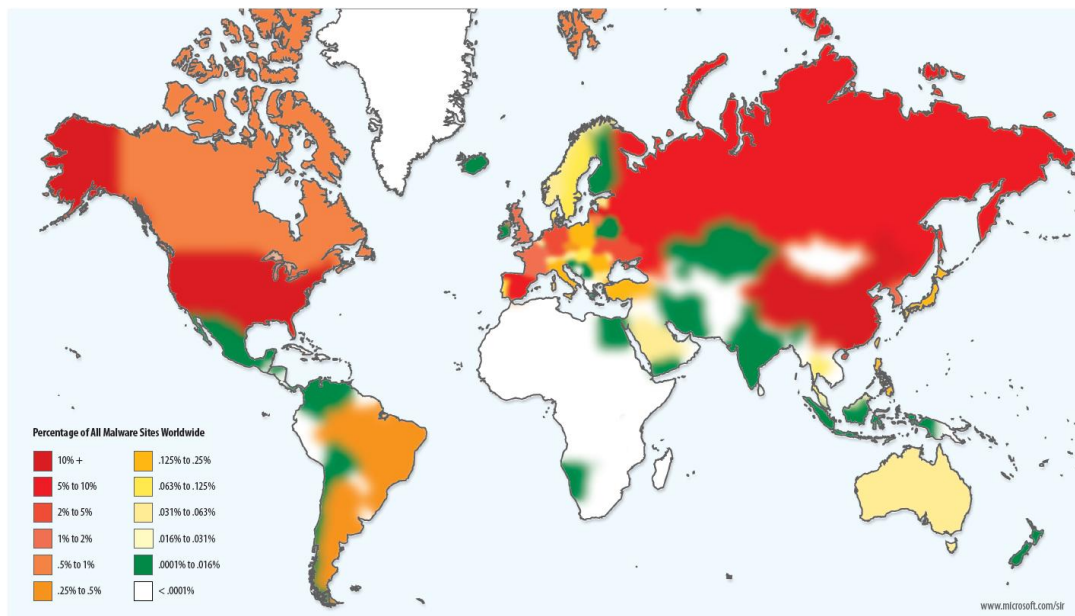
Abbildung 16: Anteil bereinigter Computer nach Bedrohungskategorie in den Halbjahreszeiträumen 2H06 bis 2H08



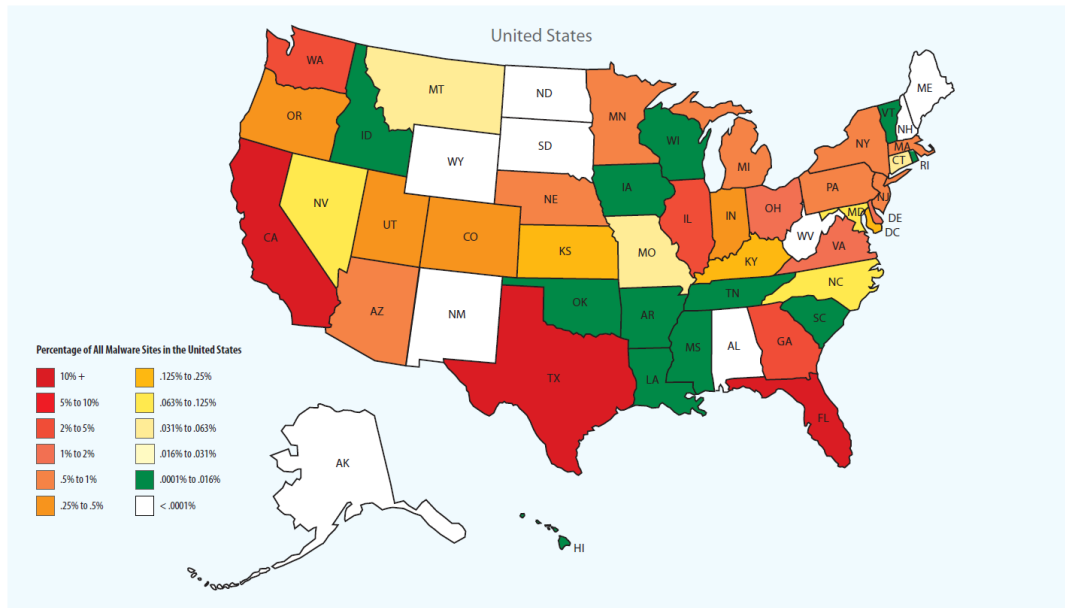
### Geografische Verteilung von Malwarehosting Websites

Malwarehosting zeigt keine großen Zahlenschwankungen und bleibt auch geografisch konstanter als Phishinghosting. Dies ist möglicherweise das Ergebnis der relativ neuen Nutzung von Serverabschaltungen und Informationen zur Seriosität bzw. Vertrauenswürdigkeit von Websites als Maßnahmen im Kampf gegen die Malwareverteilung. Malwareverteiler waren also nicht gezwungen, ihre Hostingmaßnahmen zu verändern. Die Abbildungen 17 und 18 zeigen die geografische Verteilung von Malwarehosting Websites weltweit und innerhalb der USA, die Microsoft im 2H08 gemeldet wurden.

Abbildung 17: Im 2H08 erkannte Malwarehosting Websites nach Land/Region, gemessen am Durchschnitt aller Standorte



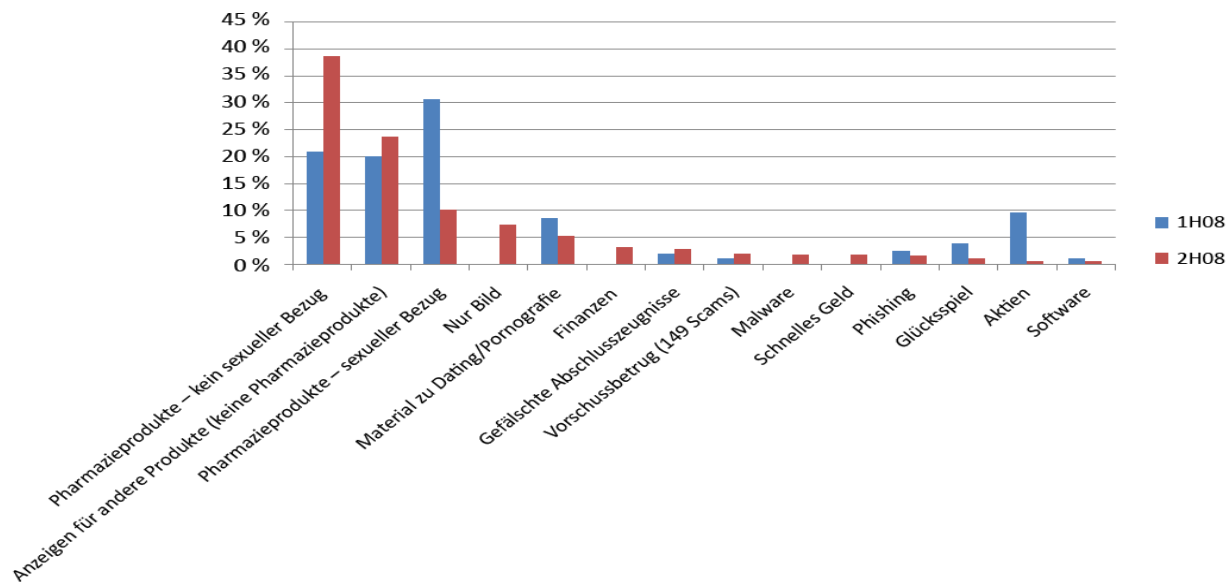
**Abbildung 18: Im 2H08 in den USA erkannte Malwarehosting Websites, gemessen am Durchschnitt aller Standorte**



### E-Mail-Bedrohungen

- Mehr als 97 Prozent der über das Internet versendeten E-Mail-Nachrichten sind unerwünscht. Sie enthalten schädliche Anhänge oder werden als Phishingangriffe oder Spam versendet.
- Wie auch in früheren Zeiträumen war Spam im 2H08 von Produktwerbung dominiert, darunter hauptsächlich Werbung für pharmazeutische Produkte (48,6 Prozent der Gesamtanzahl). Zusammen mit Anzeigen für nicht-pharmazeutische Produkte (23,6 Prozent der Gesamtanzahl) machten Produktanzeigen im 2H08 72,2 Prozent aller Spamnachrichten aus.

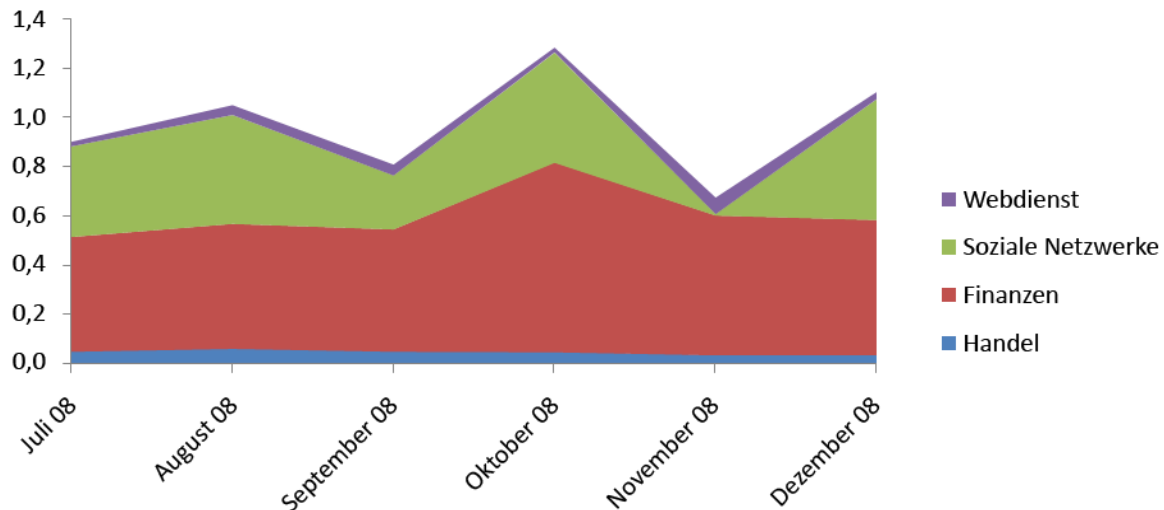
**Abbildung 19: Durch EHS-Inhaltsfilter (Exchange Hosted Services) blockierte eingehende E-Mails nach Kategorie, 1H08 bis 2H08**



## Schädliche/Gefährliche Websites

Die meisten Phishingseiten zielen zwar auf Finanzunternehmen ab, aber gemessen an den Aufrufen (Fälle, in denen Benutzer versuchen, eine gemeldete Phishingseite aufzurufen) sind auch soziale Netzwerke gängige Ziele.

**Abbildung 20: Aufrufe für jede Art von Phishingseite pro Monat im 2H08, gemessen an der durchschnittlichen Anzahl monatlicher Aufrufe im Zeitraum.**



- Die Abschaltung von McColo Mitte November hatte eine drastische Auswirkung auf die Phishingaufrufe, die im Vergleich zwischen Oktober und November um 46,2 Prozent fielen. Besuche von Phishingseiten, die auf Kontaktwebsites zielen, fielen von 34,1 Prozent aller Aufrufe im Oktober auf nur 1,1 Prozent im November.
- Die meisten Phishingseiten wurden in den USA gehostet, wobei Texas der Bundesstaat mit der höchsten Anzahl an gehosteten Phishingseiten war.

**Abbildung 21: Weltweite Verteilung von Phishingseiten im 2H08, gemessen am Durchschnitt aller Standorte**

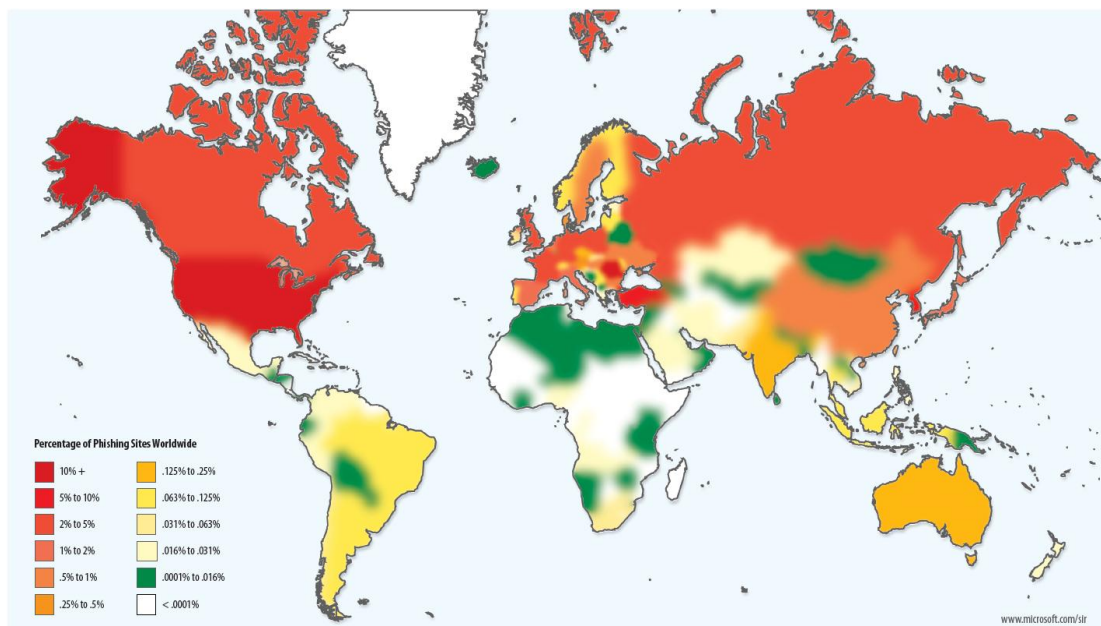
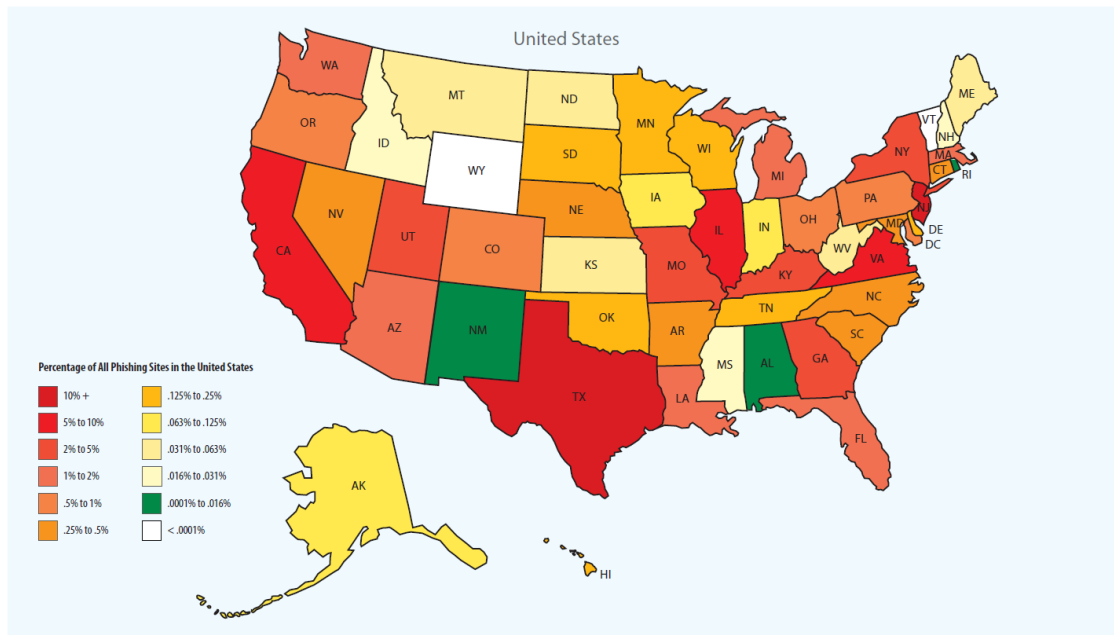


Abbildung 22: Im 2H08 in den USA erkannte Phishingwebsites, gemessen am Durchschnitt aller Standorte



### Drive-by Downloadseiten

- Mehr als eine Million Drive-by Downloadseiten wurden seit Anfang 2H08 monatlich von Live Search erkannt. Dies entspricht 0,07 Prozent aller indizierten Seiten (rund eine von 1.500).
- Die Top Level Domänen (TLD) mit der höchsten Rate von Seiten, auf denen Drive-by-Exploits gehostet wurden, waren „.name“ (0,23 Prozent aller Seiten) „.edu“ (0,19 Prozent) und „.net“ (0,19 Prozent).
- Eine geringe Zahl von Servern stellt hierbei die Exploits bereit, die von der Vielzahl der Drive-by Downloadseiten verwendet werden.

## Helfen Sie Microsoft bei der Verbesserung der Analyse zur IT-Sicherheit

Vielen Dank, dass Sie sich die Zeit genommen haben, die neueste Ausgabe der Microsoft-Analyse zur IT-Sicherheit zu lesen. Unser Anliegen ist es, diese Analyse für unsere Kunden so sinnvoll und relevant wie möglich zu gestalten. Wenn Sie Anmerkungen zu dieser Ausgabe haben oder Vorschläge zur Verbesserung zukünftiger Ausgaben machen möchten, senden Sie bitte eine E-Mail an folgende Adresse: [sirfb@microsoft.com](mailto:sirfb@microsoft.com).

Wir danken Ihnen und verbleiben mit freundlichen Grüßen,

Microsoft Trustworthy Computing

Diese Zusammenfassung dient nur zu Informationszwecken. MICROSOFT SCHLIESST ALLE GARANTIEEN, GLEICH OB AUSDRÜCKLICH, KONKLUDENT ODER RECHTLICH, IN BEZUG AUF DIE IN DIESER ZUSAMMENFASSUNG ENTHALTENEN INFORMATIONEN AUS. Kein Teil dieser Zusammenfassung darf ohne ausdrückliche schriftliche Genehmigung von Microsoft für irgendwelche Zwecke vervielfältigt, auf einem Retrieval-System gespeichert, geladen oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufnehmen oder auf andere Weise) dies geschieht.

Es ist möglich, dass Microsoft Rechte an Patenten bzw. angemeldeten Patenten, an Marken, Urheberrechten oder sonstigem geistigen Eigentum besitzt, die sich auf den Inhalt dieser Zusammenfassung beziehen. Durch die Bereitstellung dieser Zusammenfassung erhalten Sie jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird in einer schriftlichen Lizenzvereinbarung von Microsoft ausdrücklich vereinbart.

Copyright © 2009 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft, das Microsoft-Logo, Windows, Windows XP, Windows Vista und Microsoft Office sind entweder eingetragene Marken oder Marken der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern. In diesem Dokument aufgeführte Namen tatsächlicher Firmen und Produkte sind Marken der jeweiligen Eigentümer.