Microsoft Security Intelligence Report

Ausgabe 12

JULI–DEZEMBER 2011

ZUSAMMENFASSUNG DER WICHTIGSTEN ERGEBNISSE

www.microsoft.com/sir

Microsoft Security Intelligence Report

Microsoft Security Intelligence Report, Ausgabe 12

Volume 12 des *Microsoft® Security Intelligence Report* (*SIRv12*) bietet eine differenzierte Sichtweise auf Softwareschwachstellen, auf die Ausnutzung solcher Schwachstellen, auf die Bedrohung durch bösartigen Code sowie auf potenziell unerwünschte Software in der Software von Microsoft und Drittanbietern. Microsoft hat diese Perspektiven im Laufe der letzten Jahre basierend auf Trendanalysen entwickelt, wobei das Hauptaugenmerk auf der zweiten Hälfte des Jahres 2011 liegt.

In diesem Dokument werden die wichtigsten Erkenntnisse dieses Berichts zusammengefasst. Der vollständige Bericht enthält außerdem eine umfassende Analyse von Trends in über 100 Ländern/Regionen rund um den Globus und unterbreitet Vorschläge zur Verwaltung der Risiken bezüglich Ihres Unternehmens, Ihrer Software und Mitarbeiter.

SIRv12 enthält die beiden folgenden Schwerpunktartikel, die einen Einblick in die Malware Conficker bzw. in Advanced Persistent Threats (APTs) geben.

Warum sich Conficker weiterhin verbreitet

Dieser Artikel enthält Informationen über eine von Microsoft durchgeführte Analyse, um besser zu verstehen, warum Conficker weiterhin eine ernste Bedrohung bleibt, insbesondere für Unternehmen. Diese Analyse verwendet Informationen, die seit der Erörterung von Conficker in *SIRv7* gesammelt wurden.

Der Artikel legt dar, warum Conficker weiterhin eine ernste Bedrohung bleibt, bietet Hintergrundinformationen zu den Gründen und erläutert, was Unternehmen tun können, um sich zu schützen. Sie können die vollständige Analyse unter www.microsoft.com/sir herunterladen.

Bekannte Gegner und zielgerichtete Angriffe

Seit einigen Jahren schon häufen sich immer mehr Berichte über zielgerichtete Angriffe auf Unternehmen, Regierungen und Einzelpersonen. Dieser Artikel bietet einen Einblick in solche Bedrohungen, die auch als Advanced Persistent Threats (APTs) bezeichnet werden.

Dieser Artikel erörtert die Bedrohungen durch zielgerichtete Angriffe, die von bekannten Gegnern durchgeführt werden, und stellt eine defensive Strategie der Vorbeugung, Erkennung, Eindämmung und Wiederherstellung vor. Sie können die vollständige Analyse unter www.microsoft.com/sir herunterladen.

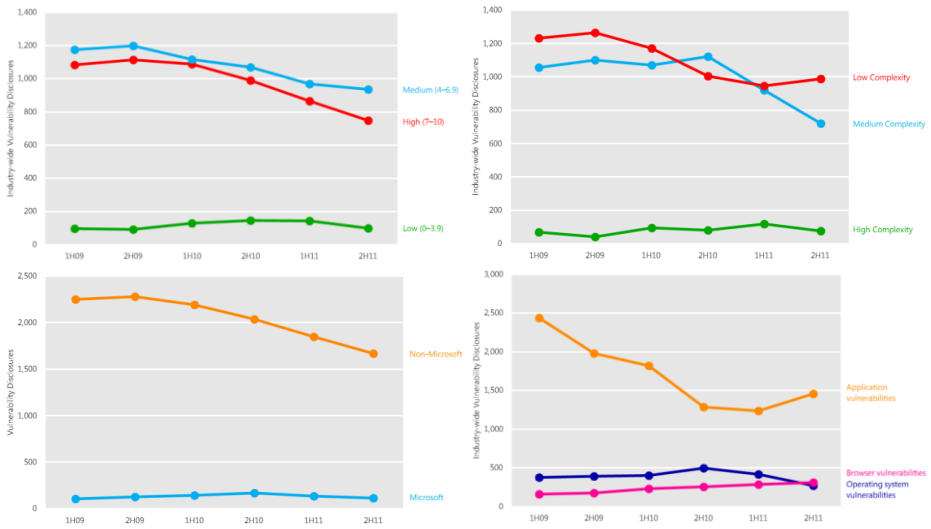
Sie können den vollständigen Bericht sowie frühere Versionen und verwandte Videos unter
www.microsoft.com/sir herunterladen.

SIR – weltweite Einschätzung der Bedrohung

Schwachstellen

Über *Schwachstellen* in Software können Angreifer die Integrität, Verfügbarkeit oder Vertraulichkeit der betreffenden Software oder der von dieser verarbeiteten Daten verletzen. Besonders ausgeprägte Schwachstellen ermöglichen es Angreifern, ein manipuliertes System für eigene Zwecke zu verwenden, indem sie es schädlichen Code ohne Wissen des Benutzers ausführen lassen.

Abbildung 1. Trends beim Schweregrad von Schwachstellen (CVE), Komplexität von Schwachstellen, Offenlegungen nach Vendor und nach Typ über die gesamte Softwarebranche hinweg, 1H09–2H11[1]



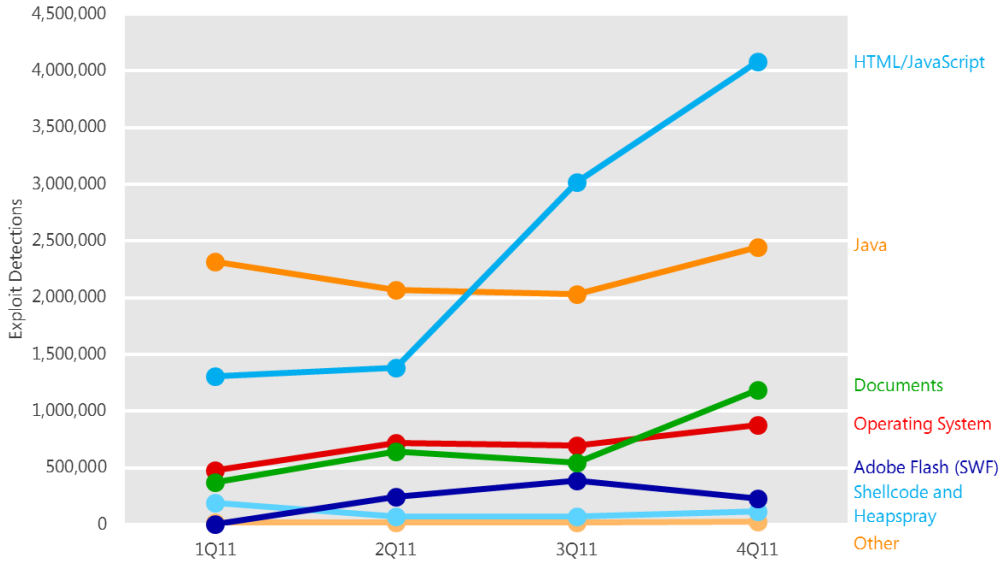
[1] Die im Bericht für die verschiedenen Berichtszeiträume verwendete Nomenklatur lautet „nHjj“, wobei „jj“ das Kalenderjahr und „n“ die erste (1) oder zweite (2) Hälfte des Jahres bezeichnet. Beispielsweise bezeichnet „1H09“ den Zeitraum, der die erste Hälfte des Jahres 2009 (1. Januar bis 30. Juni) abdeckt, und „2H11“ den Zeitraum, der die zweite Hälfte des Jahres 2011 (1. Juli bis 31. Dezember) abdeckt.

- Der Gesamttrend beim Schweregrad von Schwachstellen ist positiv. Alle drei CVSS-Einstufungen der Schweregrade nahmen zwischen 1H11 und 2H11 ab, wobei die Schwachstellen mit mittlerem und hohem Schweregrad in allen Zeiträumen seit 2H09 kontinuierlich abgenommen haben.

Exploits

Ein *Exploit* ist schädlicher Code, der Softwareschwachstellen ausnutzt, um einen Computer ohne Zustimmung und normalerweise auch ohne Wissen des Benutzers zu infizieren, zu stören oder zu kontrollieren. Exploits zielen auf Schwachstellen in Betriebssystemen, Webbrowsern, Anwendungen oder Softwarekomponenten ab, die auf dem Computer installiert sind. Um weitere Informationen zu erhalten, laden Sie das vollständige Dokument *SIRv12* unter www.microsoft.com/sir herunter.

Abbildung 2. In den vier Quartalen des Jahres 2011 durch Microsoft Anti-Malware-Produkte entdeckte und blockierte Exploits, nach anvisierter Plattform oder Technologie



- Die Menge der aufgedeckten, über HTML oder JavaScript eingeschleusten Exploits nahm in der zweiten Hälfte des Jahres 2011 stark zu, vor allem durch das Auftauchen von JS/Blacole. Hierbei handelt es sich um eine Familie von

Exploits, die vom so genannten Exploit-Kit „Blackhole“ eingesetzt werden, um schädliche Software über infizierte Webseiten einzuschleusen.

- Im Zeitraum 4Q11 stieg die Menge der erfassten Exploits an, die Schwachstellen in Dokumentenlesern und Editoren nutzen, was sie zum dritthäufigsten Exploit in diesem Quartal machte. Dies war vor allem auf einen Anstieg an Exploits mit Adobe Reader als Ziel zurückzuführen.

Trends bei Malware und potenziell unerwünschter Software

Sofern nicht anders angegeben, wurden die Informationen in diesem Abschnitt aus Telemetriedaten kompiliert, die weltweit von mehr als 600 Millionen Computern und einigen der am stärksten ausgelasteten Onlinedienste generiert wurden. Die Infektionsraten werden mithilfe des Messwerts „Computers cleaned per thousand“ (CCM) dargestellt, was die Anzahl gemeldeter Computer darstellt, die jeweils pro 1.000 Überprüfungen mit dem Windows® Malicious Software Removal Tool bereinigt wurden (das M in „CCM“ steht für das lateinische Wort für Eintausend, „Mille“). Dieses Tool wird über Microsoft Update und die Website Microsoft Safety & Security Center zur Verfügung gestellt.

Für einen Überblick über die Infektionsmuster weltweit zeigt Abbildung 3 die Infektionsraten nach Standorten rund um den Globus in CCM. Bei der Erkennung und Bereinigung kann es in einzelnen Ländern/Regionen je nach Quartal starke Abweichungen geben.

Abbildung 3. Infektionsraten nach Land/Region in 4Q11, in CCM

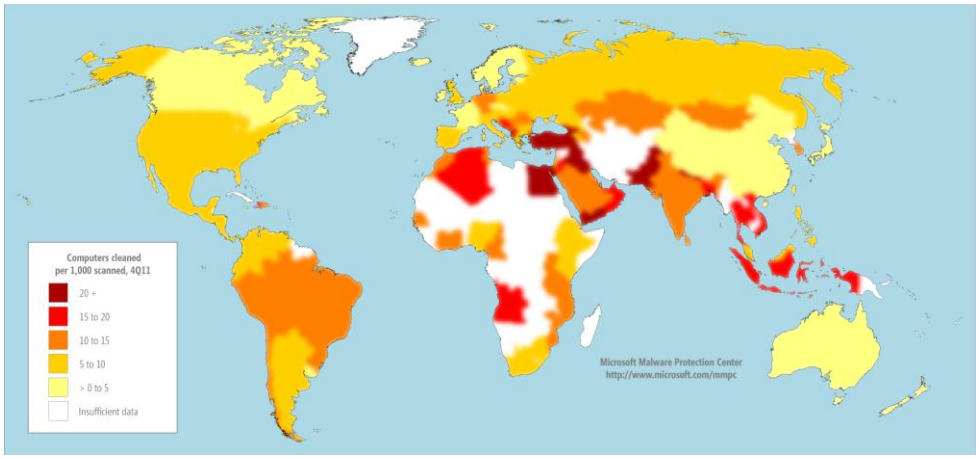


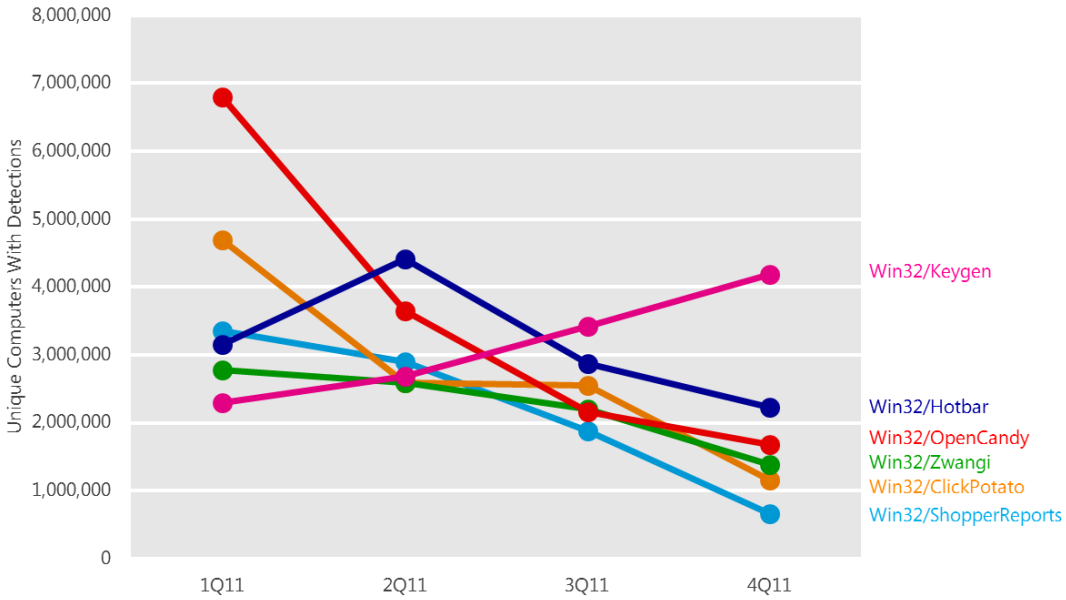
Abbildung 4. Infektionsrate (CCM) nach Betriebssystem und Service Pack im 4Q11

„32" = 32-Bit-Edition. „64" = 64-Bit-Edition. SP = Service Pack. RTM = Zur Produktion freigegeben oder kein Service Pack. Darstellung der unterstützten Betriebssysteme mit insgesamt mindestens 0,1 Prozent an Ausführungen im 4Q11.

- Diese Daten sind normalisiert: Die Infektionsrate für jede Version von Windows wird berechnet, indem eine gleiche Anzahl an Computern pro Version (z. B. 1.000 Computer mit Windows XP SP3 und 1.000 Computer mit Windows 7 RTM) verglichen wird.

Bedrohungsfamilien

Abbildung 5. Erfassungstrends für eine Reihe an wichtigen Familien in 2011



- Win32/Keygen war die am häufigsten erfasste Familie im 4Q11 sowie die einzige unter den Top-Ten-Familien mit mehr Erkennungen im vierten Quartal des Jahres als im ersten. Keygen ist eine generische Erkennung für Tools, die Schlüssel für unrechtmäßig bezogene Versionen verschiedener Softwareprodukte generieren.
- Keygen, Win32/Autorun und Win32/Sality waren die einzigen unter den Top-Ten-Familien mit mehr Erkennungen im 4Q11 als im 3Q11.

Bedrohungen im privaten Bereich und in Unternehmen

Ein Vergleich der Bedrohungen für Domänen- und Nichtdomänencomputer kann Einblick in die verschiedenen Mittel und Wege bieten, die für Angriffe auf Unternehmen und Privatanwender genutzt werden und welche Bedrohungen in jeder Umgebung eher erfolgreich sind.

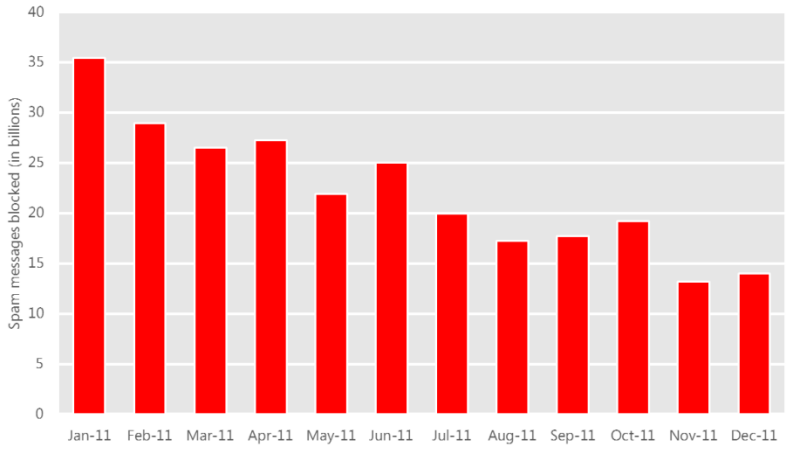
- In beiden Listen sind fünf Familien häufig anzutreffen, vor allem die generischen Familien Win32/Keygen und Win32/Autorun sowie die Exploit-Familie JS/Blacole.
- Zu den vorherrschenden Familien auf Domänencomputern gehören Conficker, die Botnet-Familie Win32/Zbot sowie das potenziell unerwünschte Softwareprogramm Win32/RealVNC.
- Zu den vorherrschenden Familien auf Nichtdomänencomputern gehören die Adware-Familien JS/Pornpop und Win32/Hotbar sowie die generische Erkennung ASX/Wimad. Wimad ist eine Erkennung für schädliche Dateien im Advanced Stream Redirector-Format (ASX), das von Windows Media Player verwendet wird.

E-Mail-Bedrohungen

Blockierte Spamnachrichten

Die Informationen in diesem Abschnitt des *Microsoft Security Intelligence Report* wurden aus Telemetriedaten mithilfe von Microsoft Forefront® Online Protection for Exchange (FOPE) kompiliert. Dieses Programm bietet Filterdienste für Spam, Phishing und Malware für Tausende von Microsoft-Unternehmenskunden, die Monat für Monat zig Milliarden Nachrichten verarbeiten.

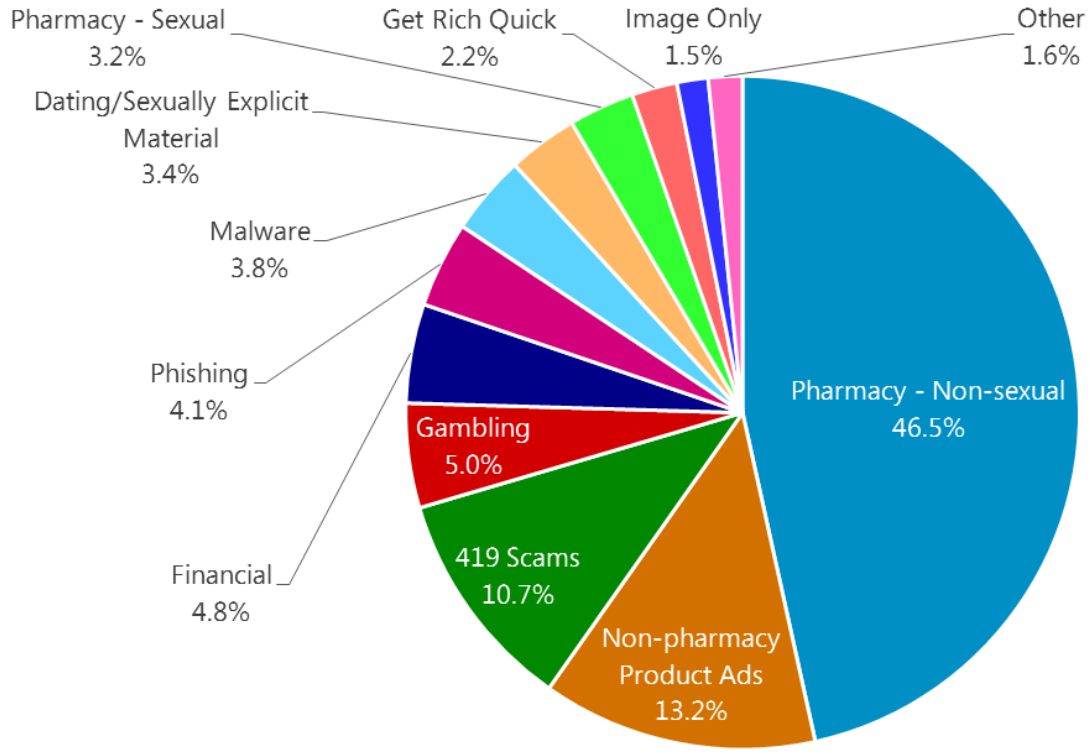
Abbildung 6. Durch FOPE monatlich blockierte Nachrichten im Jahre 2011



- FOPE blockierte im Dezember 2011 14,0 Milliarden Nachrichten, weniger als die Hälfte der im Januar blockierten Nachrichten. Der signifikante Rückgang an blockierten Nachrichten im Laufe des Jahres 2011 ist wahrscheinlich auf Eindämmungsaktionen zurückzuführen, die gegen eine Reihe großer Botnets durchgeführt wurden, darunter das Rustock-Botnet im März und das Kelihos-Botnet im September. Diese Aktionen, die von Microsoft in Zusammenarbeit mit anderen Mitgliedern der Softwareindustrie und Strafverfolgungsbehörden durchgeführt wurden, hatten scheinbar erhebliche Auswirkungen auf die Fähigkeit von Spammern, ihre Nachrichten an ein breites Publikum zu senden.

- Die FOPE-Inhaltsfilter erkennen eine Reihe an bekannten Spamnachrichtentypen. Die folgende Abbildung zeigt die relative Verbreitung dieser Spamtypen im Jahre 2011.

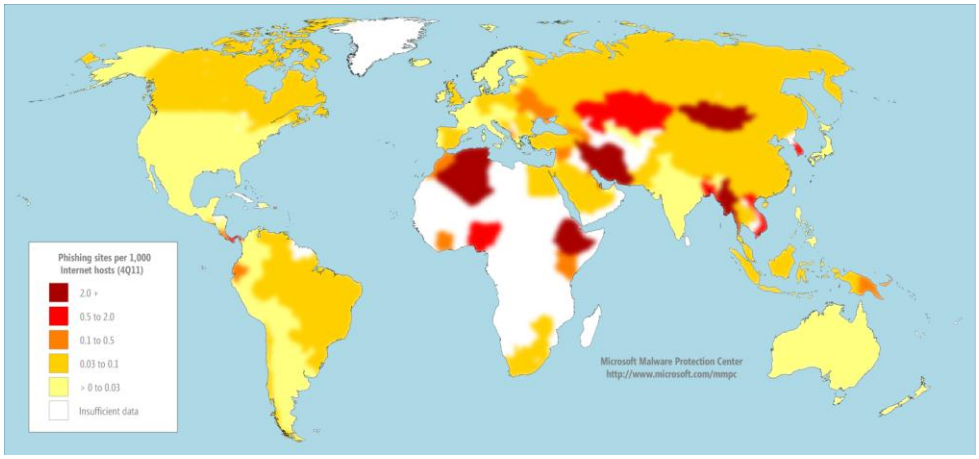
Abbildung 7. Durch FOPE-Filter blockierte eingehende Nachrichten im 2H11, nach Kategorie



Schädliche Websites

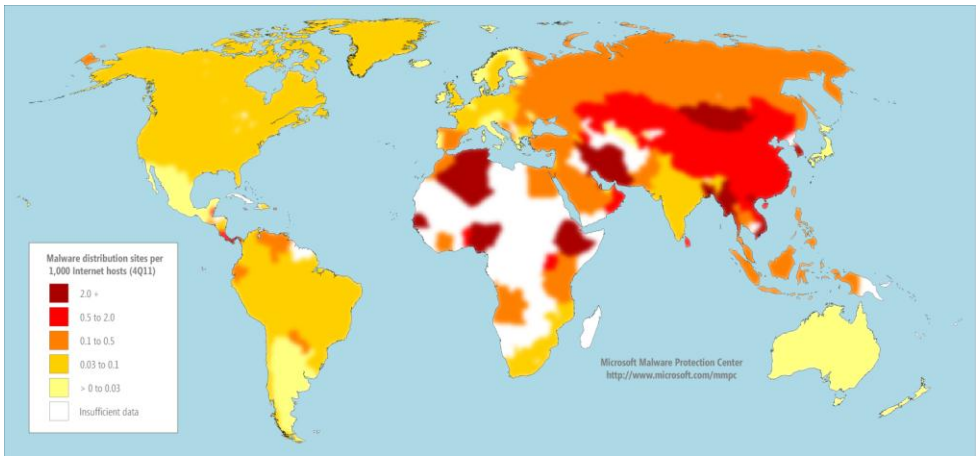
Phishingsites werden auf der ganzen Welt verteilt auf kostenfreien Hostingsites gehostet, auf infizierten Webservern und in vielen anderen Kontexten.

Abbildung 8. Phishingsites pro 1.000 Internethosts für Standorte weltweit im 2H11



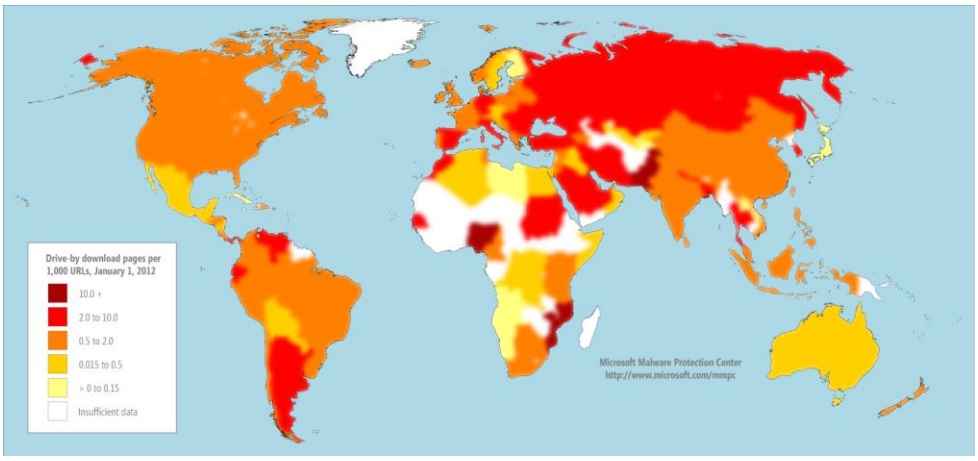
Signifikante Standorte mit ungewöhnlich hohen Konzentrationen an Malware hostenden Websites umfassen Iran mit 16,8 pro 1.000 Hosts und Korea mit 5,52.

Abbildung 9. Malware verbreitende Sites pro 1.000 Internethosts für Standorte weltweit im 2H11



Eine *Drive-by-Download*-Site ist eine Website, die eine oder mehrere Exploits hostet, die auf Schwachstellen in Webbrowsern und deren Add-ons abzielt. Benutzer mit Computern, die Schwachstellen aufweisen, können mit Malware infiziert werden, indem sie einfach eine solche Website besuchen, selbst wenn sie keinen Download starten.

Abbildung 10. Von Bing indizierte Drive-by-Download-Seiten gegen Ende des 4Q11, pro 1.000 URLs in allen Ländern/Regionen



Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security