Microsoft-Analyse zur IT-Sicherheit

Ausgabe 11

Ein umfassender Einblick in Software-Sicherheitslücken und Exploits, in Bedrohungen durch Schadsoftware sowie in möglicherweise unerwünschte Software in der ersten Jahreshälfte von 2011.

ZUSAMMENFASSUNG DER WICHTIGSTEN ERGEBNISSE

Microsoft

Microsoft-Analyse zur IT-Sicherheit

Dieses Dokument dient lediglich zu Informationszwecken. MICROSOFT ÜBERNIMMT FÜR DIE INFORMATIONEN IN DIESEM DOKUMENT KEINE GARANTIEN – WEDER AUSDRÜCKLICH NOCH KONKLUDENT ODER GESETZLICH.

Dieses Dokument wird ohne Gewähr bereitgestellt. Die darin enthaltenen Informationen und Angaben, einschließlich Internetadressen und anderen Website-Verweisen, können sich ohne vorherige Ankündigung ändern. Microsoft übernimmt keine Haftung für Folgen aus der Nutzung des Dokuments.

Copyright © 2011 Microsoft Corporation. Alle Rechte vorbehalten.

Hier aufgeführte Firmen- und Produktnamen können geschützte Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

Microsoft-Analyse zur IT-Sicherheit, Ausgabe 11 3
Schwerpunkt: Verbreitungsmethoden von Schadsoftware 4
Daten zur weltweiten Bedrohungslage 8
Informationen zu Sicherheitslücken 8
Exploits 9
Dokument-Exploits 11
Schadsoftware und möglicherweise unerwünschte Software 12
Infektionsraten für Betriebssysteme 12
Bedrohungsfamilien und Kategorien 13
Bedrohungen für Unternehmen 14
E-Mail-Bedrohungen 14
Schädliche Websites 15

Microsoft-Analyse zur IT-Sicherheit, Ausgabe 11

Die elfte Ausgabe der *Microsoft®-Analyse zur IT-Sicherheit* (*SIRv11*) bietet umfassende Einblicke in Software-Sicherheitslücken und Exploits, in Bedrohungen durch Schadsoftware sowie in möglicherweise unerwünschte Software in Microsoft- und Drittanbietersoftware. Diese Einblicke wurden von Microsoft auf der Grundlage ausführlicher Trendanalysen im Laufe der letzten Jahre entwickelt. Der Schwerpunkt lag auf dem ersten Halbjahr 2011.

In diesem Dokument werden die wichtigsten Ergebnisse des Berichts zusammengefasst. Der vollständige Bericht enthält zudem umfassende Trendanalysen aus über 100 Ländern/Regionen auf der ganzen Welt sowie Möglichkeiten zum Risikomanagement für Organisationen, Software und Personen.

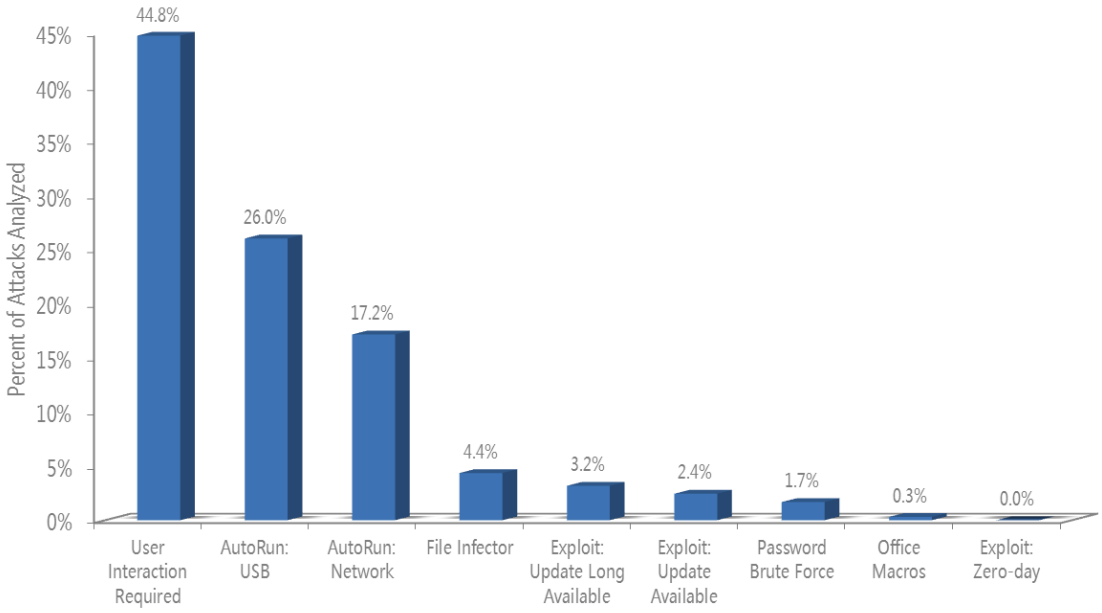
Der vollständige Bericht sowie ältere Ausgaben und entsprechende Videos können unter www.microsoft.com/sir heruntergeladen werden.

Schwerpunkt: Verbreitungsmethoden von Schadsoftware

Zur besseren Nachvollziehbarkeit der Häufigkeit von Zero-Day-Exploits und der sich daraus ergebenden Risiken für Kunden wurde von Microsoft eine entsprechende Analyse erstellt. Die Informationen aus dieser Analyse ermöglichen Sicherheitsexperten eine bessere Priorisierung von Risiken sowie ein effektiveres Risikomanagement. Auch für IT-Abteilungen gilt: Zeit, Budget, Personal und Ressourcen für die Planung und Ausführung der anfallenden Aufgaben sind begrenzt. Daher ist es für Sicherheitsexperten hilfreich, über exakte und aktuelle Informationen zur Bedrohungssituation zu verfügen, um eine effektive Priorisierung von Gegenmaßnahmen sowie den Schutz von Netzwerken, Software und Mitarbeitern zu ermöglichen.

Im Rahmen der Analyse wurden Bedrohungen, die während des ersten Halbjahres 2011 (1H11) vom Tool zum Entfernen bösartiger Software (Malicious Software Removal Tool, MSRT) erkannt wurden, anhand der Verbreitungsart klassifiziert, die für die jeweilige Bedrohungsfamilie als Infektionsmethode dokumentiert ist. Bei Bedrohungen, für die mehrere Infizierungsmethoden bekannt sind, wurde die Anzahl der vom MSRT gemeldeten Infektionen für diese Familie entsprechend dividiert und gleichmäßig auf die einzelnen Methoden aufgeteilt. Das Ergebnis der Analyse finden Sie in Abbildung .

Abbildung . Im ersten Halbjahr 2011 vom MSRT erkannte Schadsoftware, sortiert nach dokumentierter Verbreitungsmethode



- Im Anschluss werden die in Abbildung angegebenen Verbreitungsmethoden für Schadsoftware beschrieben:
  - **User Interaction Required** (Benutzerinteraktion erforderlich). Zur Gefährdung des Computers muss vom Benutzer eine Aktion ausgeführt werden. In diesem Zusammenhang ist mit „Aktion“ eine bewusste Aktion gemeint, die sich von der normalen Verwendung des Computers unterscheidet.
  - **AutoRun: USB** (AutoAusführen: USB). Von der Bedrohung werden über das AutoAusführen-Feature von Windows USB-Speichergeräte und andere Wechselmedien infiziert.
  - **AutoRun: Network** (AutoAusführen: Netzwerk). Von der Bedrohung werden über das AutoAusführen-Feature von Windows Netzwerkvolumes mit zugeordnetem Laufwerkbuchstaben infiziert.
  - **File Infector** (Dateiinfektion). Die Bedrohung wird durch Verändern von Dateien (häufig EXE- oder SCR-Dateien) verbreitet. Hierbei werden einige Codesegmente über- oder umgeschrieben.

- **Exploit: Update Long Available** (Exploit: Update lange verfügbar). Vom Anbieter wurde mindestens ein Jahr vor dem Angriff ein Sicherheitsupdate zur Beseitigung der Sicherheitslücke veröffentlicht.
- **Exploit: Update Available** (Exploit: Update verfügbar). Vom Anbieter wurde weniger als ein Jahr vor dem Angriff ein Sicherheitsupdate zur Beseitigung der Sicherheitslücke veröffentlicht.
- **Exploit: Zero-day** (Exploit: Zero-Day). Vom Anbieter wurde bis zu dem Angriff noch kein Sicherheitsupdate zur Beseitigung der Sicherheitslücke veröffentlicht.
- **Password Brute Force** (Brute-Force-Kennwortangriff). Die Bedrohung verbreitet sich durch Brute-Force-Kennwortangriffe auf verfügbare Volumes, beispielsweise mithilfe des Befehls `net use`.
- **Office Macros** (Office-Makros). Die Bedrohung verbreitet sich per Infizierung von Microsoft Office-Dokumenten mit schädlichen VBA-Makros (Visual Basic® for Applications).
- **Exploit Zero-day** (Zero-Day-Exploit). Vom Anbieter wurde bis zu dem Angriff noch kein Sicherheitsupdate zur Beseitigung der Sicherheitslücke veröffentlicht.

- Über ein Drittel der analysierten Schadsoftwareerkennungen ist auf einen Missbrauch des AutoAusführen-Features in Windows® zurückzuführen.
  - Die Bedrohungen, bei denen ein Missbrauch der automatischen Ausführung vorlag, wurden in Bedrohungen, die sich über Wechselmedien verbreiten (26 Prozent), und Bedrohungen, die sich über Netzwerkvolumes verbreiten (17 Prozent), unterteilt.
  - Zum Schutz der Kunden wurden von Microsoft mehrere Schritte gegen diese Bedrohungen unternommen. Hierzu zählt auch die Veröffentlichung eines automatischen Updates für Windows XP- und Windows Vista®-Plattformen im Februar 2011, mit dem für das AutoAusführen-Feature der gleiche hohe Sicherheitsstandard erreicht wird wie in Windows 7.
- Etwa sechs Prozent der analysierten, vom MSRT erkannten Bedrohungen sind auf *Exploits* zurückzuführen – also auf Schadsoftware, mit der versucht

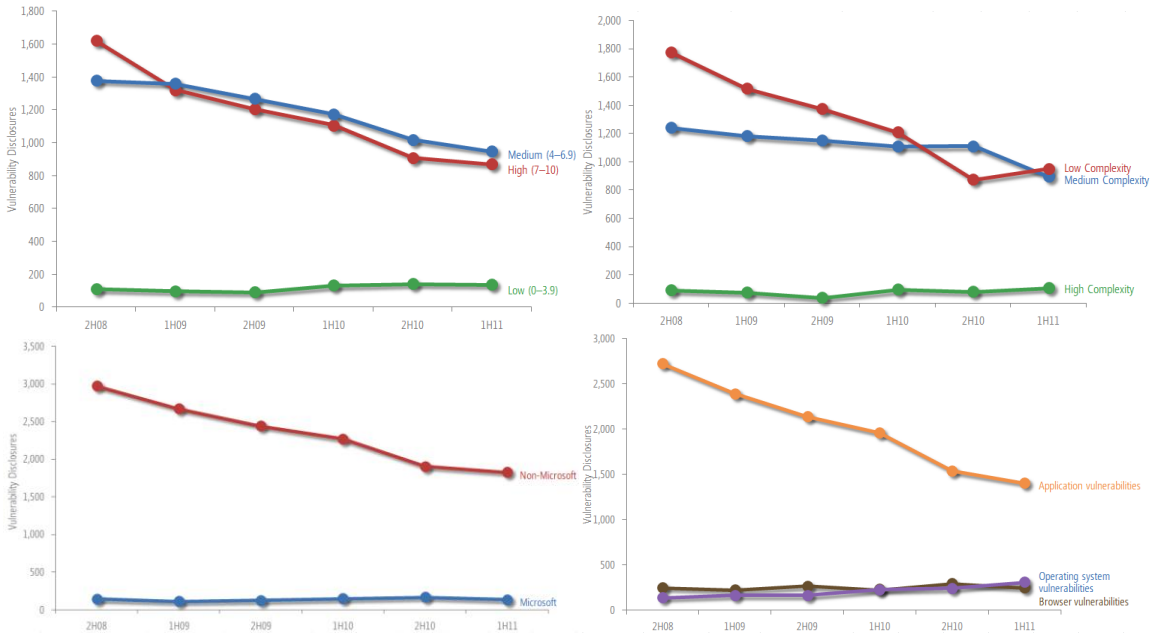
wird, Sicherheitslücken in Anwendungen und Betriebssystemen auszunutzen.

- Für keine der Top-Familien im MSRT liegen Berichte über die Nutzung von Zero-Day-Exploits innerhalb des ersten Halbjahrs 2011 vor.
- Auf Zero-Day-Exploits entfällt weniger als ein Prozent aller vom MMPC ermittelten Exploits.

Daten zur weltweiten Bedrohungslage

Informationen zu Sicherheitslücken

Abbildung . Trends für den Schweregrad von Sicherheitslücken (CVE), die Komplexität von Sicherheitslücken, Offenlegungen durch den Anbieter und Offenlegungen nach Typ



- Der allgemeine Trend hinsichtlich des Schweregrads von Sicherheitslücken (gemäß CVE-Nummer [Common Vulnerabilities and Exposures]) kann als positiv bezeichnet werden. Im ersten Halbjahr 2011 offengelegte Sicherheitslücken mit mittlerem und hohem Schweregrad sind im Vergleich zum zweiten Halbjahr 2010 um 6,8 Prozent bzw. um 4,4 Prozent zurückgegangen.

- Die besonders einfach auszunutzenden Sicherheitslücken mit geringem Schweregrad sind innerhalb der letzten 12 Monate um 41,2 Prozent zurückgegangen.

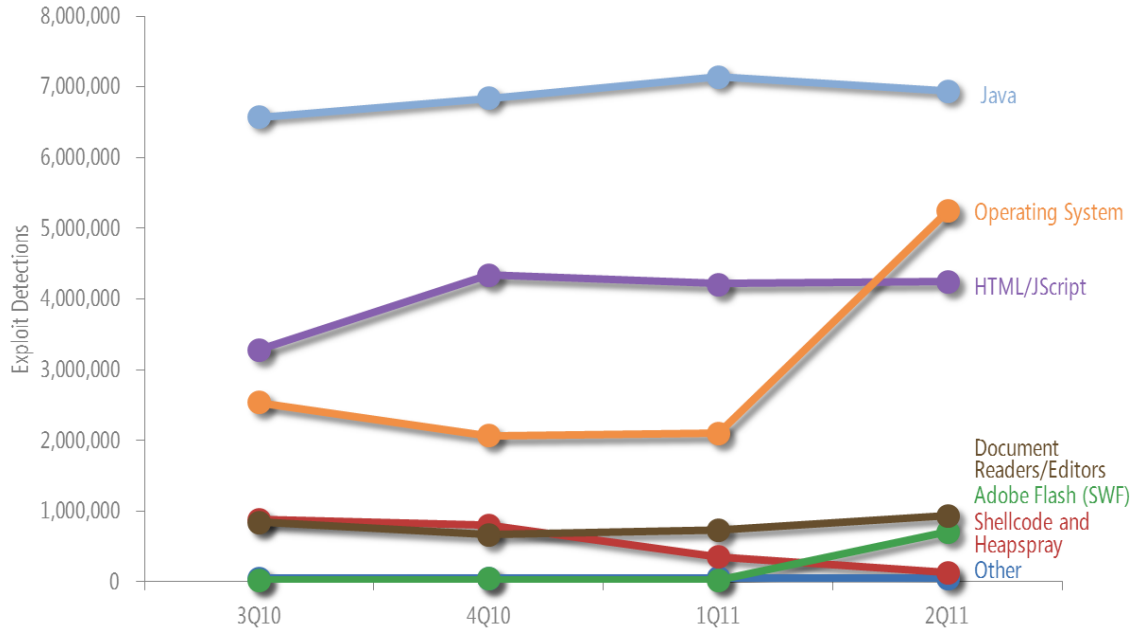
- Der Anteil offengelegter Sicherheitslücken in Betriebssystemen und Browsern bleibt seit einigen Jahren nahezu unverändert und beläuft sich auf 12,7 Prozent bzw. 15,7 Prozent aller im ersten Halbjahr 2011 offengelegten Sicherheitslücken.

- Sicherheitslücken in Produkten von Microsoft machen 6,9 Prozent aller im ersten Halbjahr 2011 offengelegten Sicherheitslücken aus. Im zweiten Halbjahr 2010 lag dieser Wert noch bei 8,2 Prozent.

Exploits

Abbildung gibt Aufschluss über die Verbreitung unterschiedlicher Arten von Exploits im Zeitraum zwischen dem 3. Quartal 2010 (3Q10) und dem 2. Quartal 2011 (2Q11).

Abbildung . Von Microsoft-Antischadsoftware erkannte und blockierte Exploits im Zeitraum 3Q10 - 2Q11, sortiert nach betroffener Plattform oder Technologie



- Der im 1. Halbjahr 2011 am häufigsten beobachtete Exploit-Typ war die Ausnutzung von Sicherheitslücken in der Java-Laufzeitumgebung (Java

Runtime Environment, JRE), in Java Virtual Machine (JVM) und in Java SE im Java Development Kit (JDK) von Oracle (ehemals Sun). Java-Exploits machten in den vier zurückliegenden Quartalen jeweils zwischen 33 und 50 Prozent aller Exploits aus.

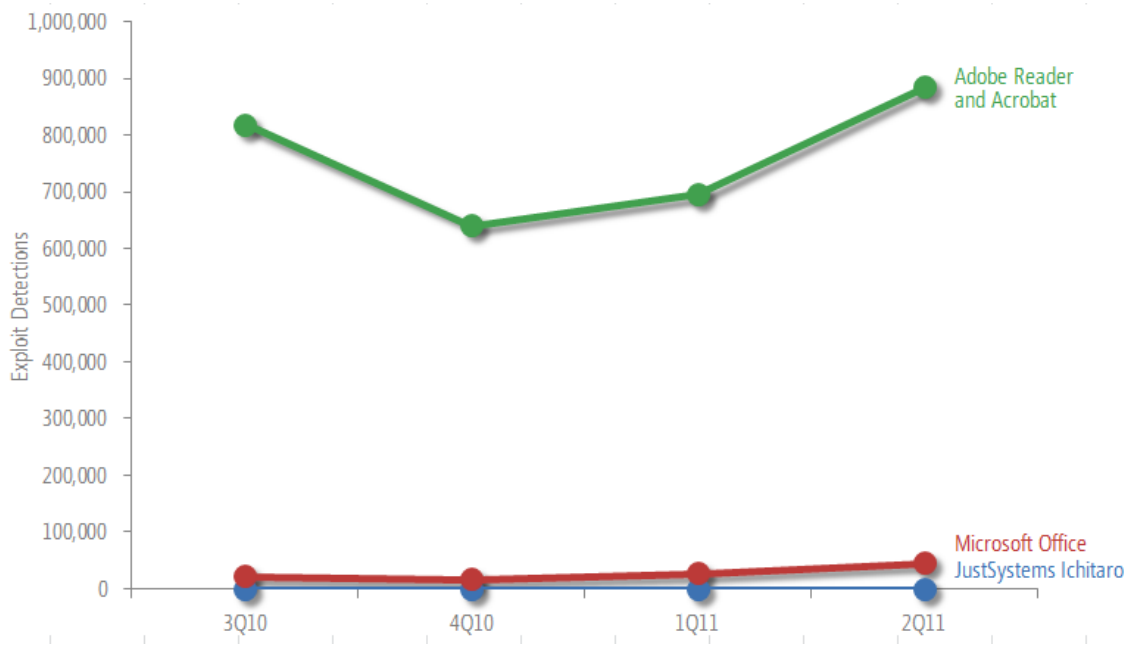
- Bei der Anzahl der erkannten Betriebssystem-Exploits ist im 2. Quartal 2011 ein sprunghafter Anstieg zu verzeichnen. Dieser ist auf die vermehrte Ausnutzung der Sicherheitslücke CVE-2010-2568 zurückzuführen.

- Die Anzahl erkannter Exploits für Adobe Flash hat im 2. Quartal 2011 gegenüber dem 1. Quartal 2011 um mehr als das 40-Fache zugenommen, was im Vergleich zu einigen anderen Exploit-Typen durchaus ungewöhnlich ist. Grund hierfür ist die Ausnutzung einiger neu entdeckter Sicherheitslücken.

- Die Anzahl von Exploits, die die Sicherheitslücke CVE-2010-2568 in Windows Shell zum Ziel hatten, nahm im 2. Quartal 2011 deutlich zu und ist die Ursache für den allgemeinen Anstieg der Anzahl von Betriebssystem-Exploits im 2. Quartal 2011. Die Sicherheitslücke wurde erstmalig Mitte 2010 entdeckt, als sie mithilfe der Familie Win32/Stuxnet ausgenutzt wurde.

Dokument-Exploits

Abbildung . Von Microsoft-Antischadsoftware erkannte und blockierte Dokumentparser-Exploits im Zeitraum 3Q10 - 2Q11



- Exploits für Adobe Acrobat und Adobe Reader machten den Großteil der im ersten Halbjahr 2011 erkannten Dokumentformat-Exploits aus. Nahezu alle diese Exploits gehörten der allgemeinen Exploit-Familie Win32/Pdfjsc an.

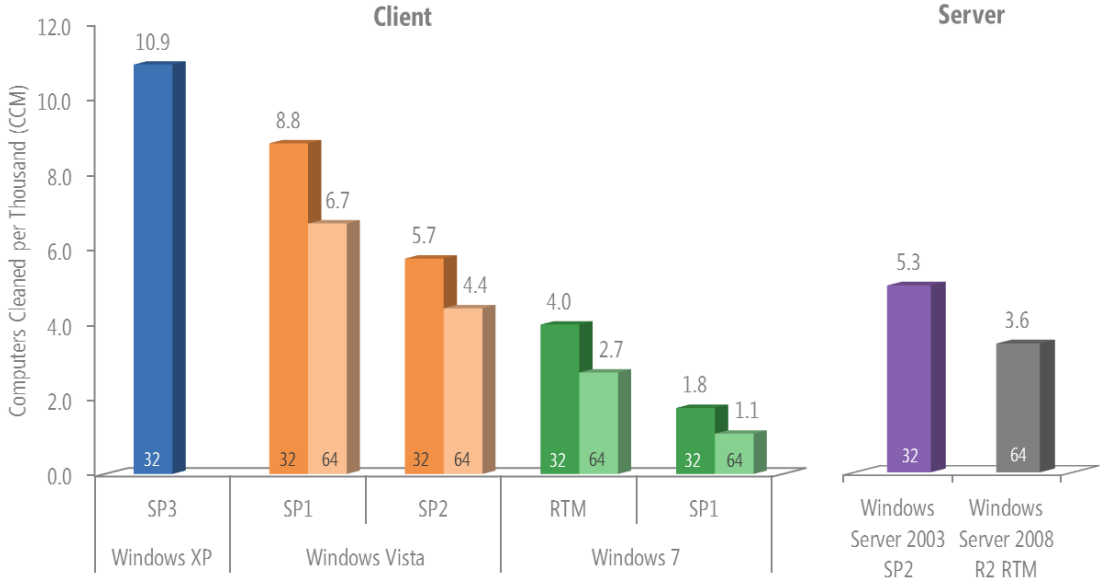
- Über die Hälfte der Microsoft Office-Exploits war auf CVE-2010-3333 zurückzuführen – eine Sicherheitslücke im RTF-Parser (Rich Text Format) von Microsoft Word-Versionen.

Schadsoftware und möglicherweise unerwünschte Software

Sofern nicht anders angegeben, stammen die Informationen in diesem Abschnitt aus Telemetriedaten, die auf der Grundlage von über 600 Millionen Computern weltweit sowie einiger der gefragtesten Onlinedienste im Internet generiert wurden. Die Infektionsraten werden in *CCM* (Computers Cleaned per Mille) angegeben. Hierbei handelt es sich um die Anzahl von gemeldeten Computern innerhalb eines Quartals, die pro 1000 Anwendungen des Tools zum Entfernen von bösartiger Software bereinigt wurden. Weitere Informationen zum CCM-Messwert finden Sie in der *Microsoft-Analyse zur IT-Sicherheit* im Abschnitt zu Schadsoftware (Malware; möglicherweise in englischer Sprache).

Infektionsraten für Betriebssysteme

Abbildung . Infektionsrate (CCM) nach Betriebssystem und Service Pack im 2. Quartal 2011



„32“ = 32-Bit-Edition; „64“ = 64-Bit-Edition. SP = Service Pack. Gezeigt werden unterstützte Betriebssysteme mit einem Ausführungsanteil von mind. 0,1 Prozent im 2. Quartal 2011...

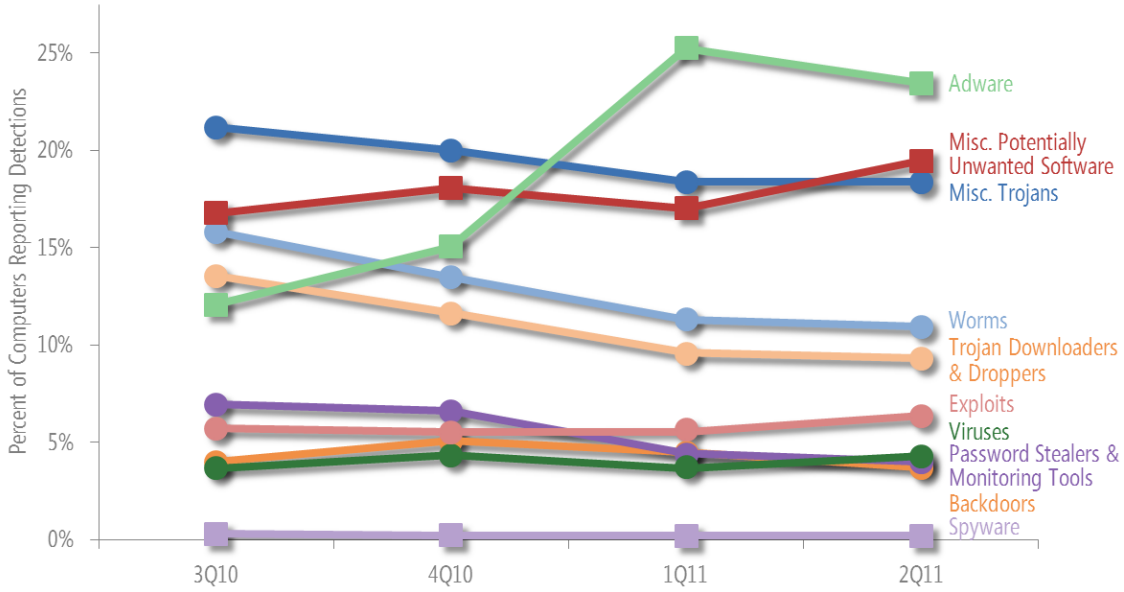
- Auch diesmal waren die Infektionsraten bei neueren Betriebssystemen und Service Packs wieder durchgehend niedriger als bei älteren Versionen. Dies gilt sowohl für Client- als auch für Serverplattformen. Windows 7 und Windows Server® 2008 R2 – die neueste Windows-Client- bzw. -

Serverversion – zeichnen sich durch eine besonders niedrige Infektionsrate aus (siehe Abbildung).

- Die Infektionsraten für Windows XP SP3 und Windows Vista sind seit der Veröffentlichung eines automatischen Updates im Februar 2011, mit dem die Funktionsweise des AutoAusführen-Features an die Funktionsweise in Windows 7 angepasst wurde, zurückgegangen. Die Auswirkungen dieser Änderung werden in der Infektionsstatistik für „Win32/Rimecud“ deutlich. Bei „Win32/Rimecud“ handelt es sich um die im 1. Halbjahr 2011 weltweit am neunthäufigsten erkannte Bedrohungsfamilie sowie um eine der Hauptmissbrauchsquellen für das AutoAusführen-Feature.

Bedrohungsfamilien und Kategorien

Abbildung . Erkennungen nach Bedrohungskategorie im Zeitraum 3Q10 - 2Q11, sortiert nach prozentualem Anteil aller Computer, von denen Erkennungen gemeldet werden



Kreise stehen für Schadsoftwarekategorien, Quadrate für Kategorien möglicherweise unerwünschter Software.

- Die Bedrohungsfamilie Win32/OpenCandy wurde im 1. Halbjahr 2011 insgesamt am häufigsten erkannt. Bei OpenCandy handelt es sich um ein Adware-Programm, das unter Umständen mit Installationsprogrammen bestimmter Drittanbietersoftware gebündelt wird.

- Bei JS/Pornpop, der am zweithäufigsten erkannten Bedrohungsfamilie des 1. Halbjahrs 2011, handelt es sich um die Erkennung speziell erstellter,

JavaScript-fähiger Objekte, durch die im Webbrowser des Benutzers Pop-Under-Anzeigen angezeigt werden.

- Die Bedrohungsfamilie Win32/Hotbar wurde im 2. Quartal 2011 am häufigsten und im 1. Halbjahr am dritthäufigsten erkannt. Bei dieser Bedrohungsfamilie handelt es sich um Adware, durch die eine Browsersymbolleiste für die Anzeige speziell ausgerichteter Werbe-Pop-Ups angezeigt wird, die auf der Überwachung der Browseraktivitäten basieren.

- Die Anzahl der Erkennungen von Win32/FakeRean nahm im 2. Quartal 2011 gegenüber dem 1. Quartal 2011 um 300 Prozent zu und ist somit die am häufigsten erkannte Rogue Security Software-Familie des zweiten Quartals.

Bedrohungen für Unternehmen

- Bei den drei Schadsoftwarefamilien, die am häufigsten auf Computern erkannt wurden, die einer Domäne angehören, handelte es sich um Würmer. Domänencomputer sind hauptsächlich in Unternehmensumgebungen zu finden.

- Zu den Schadsoftwarefamilien, die besonders auf Domänencomputern verbreitet sind, gehören Win32/Conficker und die möglicherweise unerwünschte Software Win32/RealVNC. Bei „RealVNC“ handelt es sich um ein Programm, dass die Remotesteuerung eines Computers ermöglicht (ähnlich den Remotedesktopdiensten). Das Programm kann zwar durchaus hilfreich sein, es wurde aber auch schon von Angreifern dazu genutzt, die Steuerung von Benutzercomputern zu übernehmen, um Schaden anzurichten.

- Die Virusfamilie „Win32/Sality“ belegt im 1. Halbjahr 2011 den zehnten Platz, war im Jahr 2010 aber nicht unter den Top-10-Familien, die auf Domänencomputern gefunden wurden.

E-Mail-Bedrohungen

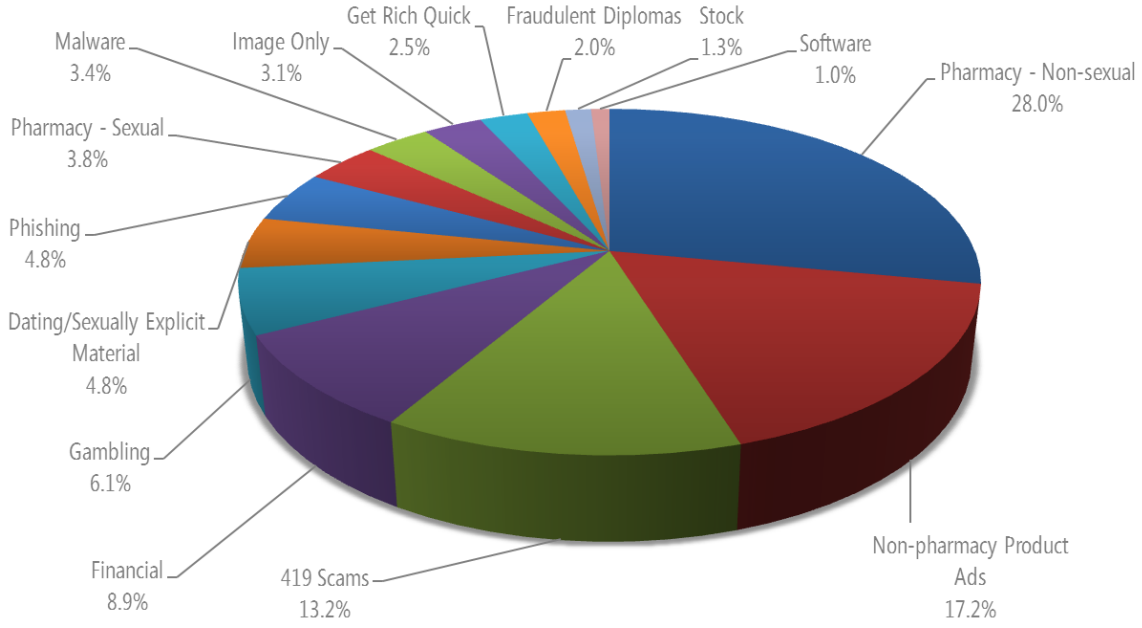
- Die Menge an Spam, die durch Microsoft Forefront® Online Protection for Exchange (FOPE) blockiert wurde, hat in den letzten 12 Monaten drastisch abgenommen – von 89,2 Milliarden Nachrichten im Juli 2010 auf 25,0 Milliarden Nachrichten im Juni 2011. Hauptursache hierfür ist die Zerschlagung zweier großer Botnets: Cutwail, das im August 2010

zerschlagen wurde, und Rustock, das im März 2011 nach einer im Januar beginnenden Ruhephase zerschlagen wurde. [1]

- Auch in diesem Zeitraum setzt sich der Trend aus früheren Zeiträumen fort: Werbung für Arzneimittel ohne sexuelle Wirkung (28,0 Prozent des Gesamtaufkommens) sowie Werbung für arzneimittelfremde Produkte (17,2 Prozent) machte den Hauptteil der Spamnachrichten aus, die im 1. Halbjahr 2011 von den FOPE-Inhaltsfiltern blockiert wurden.

- Der Anteil von Spamnachrichten, die nur Bilder enthielten, sank von 8,7 Prozent im Jahr 2010 auf 3,1 Prozent des Gesamtaufkommens im 1. Halbjahr 2011.

Abbildung . Eingehende Nachrichten, die im 1. Halbjahr 2011 von den FOPE-Filtern blockiert wurden (sortiert nach Kategorie)



Schädliche Websites

- Zwar waren für Phisher bislang besonders finanzbezogene Websites von Interesse, der größte Anteil an Phishing-Impressionen des 1. Halbjahrs 2011

[1] Weitere Informationen zur Zerschlagung von Cutwail finden Sie in der *Microsoft-Analyse zur IT-Sicherheit – Ausgabe 10 (Juli - Dezember 2010)*. Weitere Informationen zur Zerschlagung von Rustock finden Sie im Microsoft Download Center unter „Der Kampf gegen die Bedrohung durch Rustock“.

entfiel jedoch auf Websites, die auf soziale Netzwerke ausgerichtet waren. Im April wurde bei Impressionen dieser Art ein Höchststand von 83,8 Prozent erreicht. (Bei einer Phishing-Impression handelt es sich um eine einzelne Instanz eines Benutzers, der mit Windows Internet Explorer® versucht, eine bekannte Phishing-Website zu besuchen, und vom SmartScreen®-Filter daran gehindert wird. Weitere Informationen hierzu finden Sie auf der Website der Microsoft-Analyse zur IT-Sicherheit im Abschnitt zu schädlichen Websites (Malicious Websites; möglicherweise in englischer Sprache). Auf soziale Netzwerke abzielende Impressionen machten insgesamt 47,8 Prozent aller Impressionen im 1. Halbjahr 2011 aus. An zweiter Stelle folgen mit 35,0 Prozent auf Finanzinstitute ausgerichtete Impressionen.

- Im Gegensatz dazu ergab sich bei auf Finanzinstitute ausgerichteten Phishing-Websites ein durchschnittlicher Anteil von 78,3 Prozent an aktiven Phishing-Websites, die in den Monaten des 1. Halbjahres 2011 überwacht wurden. Der Anteil für soziale Netzwerke liegt hier lediglich bei 5,4 Prozent. Von den Phishern werden teilweise mehrere hundert Finanzinstitute ins Visier genommen, und für jedes Institut wird ein eigener Phishing-Ansatz benötigt. Die Anzahl der beliebten sozialen Netzwerke ist deutlich geringer, weshalb Phisher, die sich sozialen Netzwerken zuwenden, pro Website eine größere Anzahl von Benutzern angehen können. Die Aussicht auf den direkten unerlaubten Zugang zu den Bankkonten der Opfer sorgt allerdings dafür, dass Finanzinstitute weiterhin das Hauptziel für Phishing-Versuche bleiben, weshalb auf diese Gruppe jeden Monat auch der größte bzw. zweitgrößte Anteil an Impressionen entfällt.
- Dieses Phänomen lässt sich in kleineren Dimensionen auch bei Onlinediensten und Spielewebsites beobachten. Da eine kleine Anzahl von Onlinediensten den Hauptanteil des Datenaufkommens für solche Websites ausmacht, beläuft sich der Anteil der Impressionen für auf Onlinedienste ausgerichtete Phishing-Websites auf 11,0 Prozent, wobei der Anteil der Websites lediglich 3,6 Prozent beträgt. Das Datenaufkommen für Onlinespiele verteilt sich in der Regel auf eine größere Anzahl von Websites, weshalb sich bei den auf Onlinespielewebsites ausgerichteten Phishing-Websites ein Anteil von 8,9 Prozent der aktiven Websites ergab und der Anteil der Impressionen bei lediglich 4,3 Prozent lag.

Auf E-Commerce ausgerichtete Phishing-Websites machen 3,8 Prozent der aktiven Websites und 1,9 Prozent der Impressionen aus. Dies deutet darauf hin, dass E-Commerce-Websites von Phishern nicht als sonderlich lohnenswerte Ziele betrachtet werden.

Informationen zum Schutz Ihrer Organisation, Ihrer Software und Ihrer Mitarbeiter (Protecting Your Organization, Software, and People; möglicherweise in englischer Sprache) finden Sie auf der Website der Microsoft-Analyse zur IT-Sicherheit (*Microsoft Security Intelligence Report* (möglicherweise in englischer Sprache) im Abschnitt zum Risikomanagement.
http://www.microsoft.com/sir

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