

# McAfee Threat-Report: Viertes Quartal 2010

McAfee® Labs™

Für die Internetsicherheit bedeutete das vergangene Jahr Transformation und Evolution. Das gesamte Jahr hindurch nahmen gezielte Angriffe und die Qualität der Angriffe zu. Außerdem beobachteten wir eine Zunahme bei Angriffen, die sich auf neue Geräteklassen konzentrieren und immer wieder auftreten. Es ist nicht einfach, alle potenziellen Gerätenutzer über diese Bedrohungen zu informieren, ohne sie dabei unnötig zu beunruhigen. Das Ziel von McAfee Labs besteht darin, die Nutzung einer Technologie bei maximaler Sicherheit zu ermöglichen. Dazu müssen wir die Folgen unserer Beobachtungen offen analysieren und erläutern.

In diesem Quartal fanden einige der interessantesten Veränderungen dieses Jahres statt. Das Spam-Aufkommen lag in den vergangenen drei Monaten auf dem niedrigsten Niveau seit 2007. Gleichzeitig gab es Angriffe auf neue Geräte wie Smartphones mit dem Betriebssystem Android. Malware und Bedrohungen für Mobilgeräte sind seit Jahren im Umlauf. Mittlerweile sind sie jedoch zu einer festen Größe herangewachsen, mit der Mobilnutzer ständig rechnen müssen. In diesem Quartal gab es zudem drastische Veränderungen bei der Vielfalt weltweit verbreiteter Malware-Varianten, d. h. je nach Land sehen sich Benutzer sehr verschiedenen Bedrohungen gegenüber. Seit dem vergangenen Quartal änderte sich zudem die weltweite Vielfalt bei Botnets – dadurch ist Cutwail nicht mehr weltweit führend. Die Formen der digitalen Bedrohungen für Benutzer hängen davon ab, wo sie sich befinden und welche Geräte sie nutzen.

Es ist unmöglich, über dieses Quartal zu berichten, ohne Hacktivismus, WikiLeaks und die Hacktivistengruppe Anonymous zu erwähnen. Möglicherweise definieren solche politischen Aktionen – die Kompromittierung von Daten und Aktionen von Vertretern gegensätzlicher Interessensgruppen – die Ereignisse des Jahres 2010. Unabhängig von der Einstellung eines Benutzers oder Unternehmens werden Hacktivismus und die WikiLeaks-Aktivitäten zukünftig Einfluss auf Probleme wie Datenverlust, Datenkompromittierung und politischen Aktivismus haben. Neben dem Rummel um WikiLeaks gab es in diesem Quartal weltweit zahlreiche andere Hacktivismus-Aktionen. Gleichzeitig machten die Strafverfolgungsbehörden in den osteuropäischen Ländern einige erhebliche Fortschritte.

Ende 2010 erreichte das Malware-Wachstum einen neuen Höchstwert – wobei die Vielfalt bei den Malware-Klassen weiterhin sehr groß war. In diesem Bericht werden die neuesten Aktivitäten einiger „alter Bekannter“ wie Koobface, gefälschte Virenschutz-Software, Kennwort stehlende Trojaner und Autostart-Malware beleuchtet.

McAfee Labs sagte Ende 2009 voraus, dass sich Internetkriminelle im Jahr 2010 sehr auf Adobe-Produkte konzentrieren werden. Dies hat sich eindeutig als wahr erwiesen. Adobe-Software ist bei Exploit-Autoren bei weitem beliebter als Microsoft-Produkte. Die Angriffe zielen häufig auf Adobe Reader sowie seine webbasierten Plug-Ins ab. Bei Schwachstellenaktivitäten und SQL-Injektionsangriffen gab es in diesem Quartal einige Überraschungen. McAfee Labs beobachtete einige Veränderungen beim Missbrauch von Suchmaschinen und -begriffen sowie dabei, wohin diese böswilligen Links tatsächlich führen.

In dem Maße, in dem Unternehmen und Verbraucher neue Technologien übernehmen und immer intensiver online tätig sind, erschließen sich für Internetbedrohungen und Internetkriminalität neue Tätigkeitsfelder. Kriminelle folgen immer dem Geld und den Daten. Daher wäre es unrealistisch – und gefährlich – zu vermuten, dass sich das jetzt ändert.

## Inhaltsverzeichnis

Mobile Bedrohungen nehmen stark zu	4
Führung bei Botnets wechselt	6
Malware erreicht Rekordzahlen	7
Vergeht Kriminellen die Lust am Spam?	10
Internet-Bedrohungen	12
Suchmaschinen, Suchbegriffe und neue nicht autorisierte Anwendungen	14
Schwachstellen und Netzwerkangriffe	15
Angriffe mit SQL-Skripteinschleusung	16
Internetkriminalität	17
Hacktivismus	18
Aktionen gegen Internetkriminelle	19
Informationen zu den Autoren	20
Über McAfee Labs™	20
Informationen zu McAfee	20

### Mobile Bedrohungen nehmen stark zu

Bedrohungen für Mobilgeräteplattformen (vor allem Smartphones) sind nicht neu. Scheinbar konzentrieren sich Internetkriminelle aus verschiedenen Gründen von neuem auf Mobilgeräte. Bei den meisten kriminellen Handlungen handelt es sich um Gelegenheitstaten, und Internetkriminelle sehen derzeit eine gute Gelegenheit zur Ausnutzung einer Vielzahl von Mobilgeräteplattformen. Immer mehr Verbraucher verwenden Mobilgeräte und Tablet-Computer im privaten wie im geschäftlichen Alltag. Unternehmen müssen immer mehr Geräte unterstützen und in diesem Rahmen ihre Unternehmensfirewall und -dienste in Bereiche erweitern, auf die sie möglicherweise nicht vorbereitet sind.

Während der vergangenen Jahre beobachtete McAfee Labs ein stetes Wachstum bei der Anzahl der Bedrohungen für Mobilgeräte. Die Anzahl kann zwar nicht mit dem Gesamtaufkommen bei PC-basierter Malware mithalten, das beständige Wachstum ist dennoch bemerkenswert.

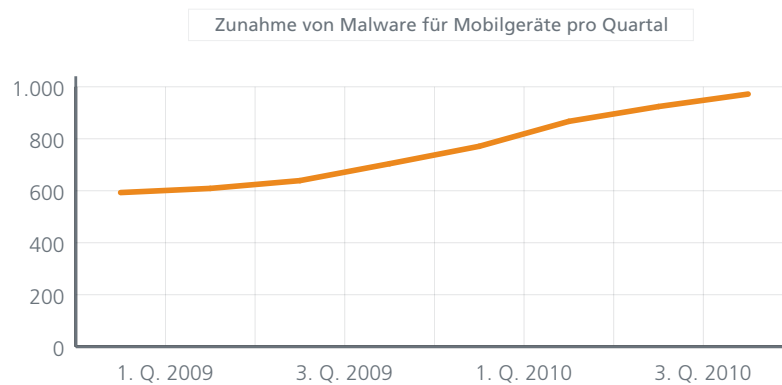


Abbildung 1: Die Anzahl neuer Malware-Versionen für Mobilgeräte stieg 2010 im Vergleich zu 2009 kontinuierlich um 46 Prozent.

Das Forschungs- und Analyseteam von McAfee Labs stellte fest, dass sich die meisten Bedrohungen zwar auf bestimmte Plattformen konzentrieren, Internetkriminelle jedoch jede gewünschte Mobilgeräteplattform angreifen können.

Bedrohungen für Mobilgeräte nach Plattform, 2009–2010

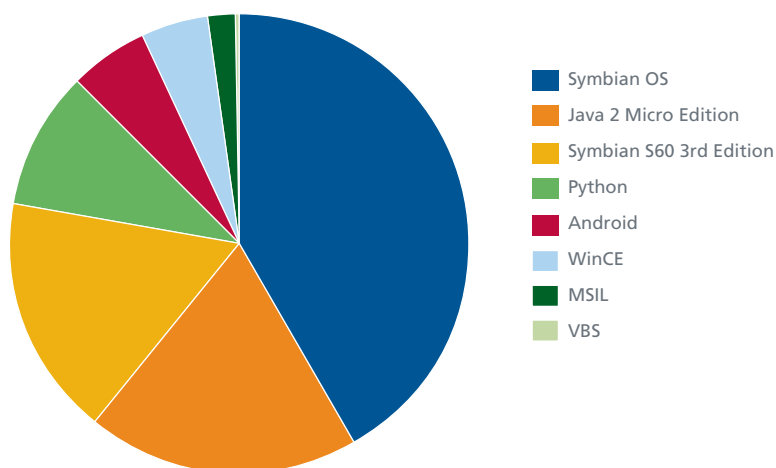


Abbildung 2: Das Betriebssystem Symbian OS (das auf Nokia-Smartphones verwendet wird) ist bei Entwicklern für Mobilgeräte-Malware die beliebteste Plattform. McAfee Labs identifizierte in den vergangenen zwei Jahren 188 neue Bedrohungen, seit 2004 insgesamt 668.

Zu den interessantesten Bedrohungen für Mobilgeräte gehörten in diesem Quartal „SymbOS/Zitmo.A“ und „Android/Geinimi“. Die erstere verbreitete Bedrohung schlug Anfang des Quartals zu. Es schien, dass die Kriminellen hinter dem Zeus-Botnet eine eigene Spyware erstellten, um ebenso wie bei TANs (Transaction Authentication Numbers) von PCs nun auch von Mobilgeräten mTANs (mobile TANs) abfangen zu können. Es stellte jedoch heraus, dass einfach eine alte Version eines kommerziellen Spyware-Pakets umfunktioniert wurde. Dieses Szenario sagten wird bereits im Jahr 2007 voraus.

Android/Geinimi ist wahrscheinlich eine der wichtigsten Bedrohungen des Quartals. Dabei handelt es sich um einen Trojaner, der in legitime Mobilanwendungen und -spiele (z. B. MonkeyJump2 und Hardcore Dirt Bike) für die Android-Plattform eingefügt wird. Er wurde in China gefunden und ähnelt anderer Mobilgeräte-Malware und anderen Mobilgeräte-Botnets aus dieser Region (z. B. SymbOS/XMJTC, Yxe.A und „sexy“ worm). Der Unterschied besteht jedoch darin, dass der Benutzer ihn auf dem Gerät installieren muss.

Dieser Trojaner verwendet einen Signaturschlüssel für die Anwendung und versucht auf diese Weise, den Anschein einer legitimen Anwendung aufrecht zu erhalten. Für die Signatur wird jedoch ein Debugbuild-Standardtestzertifikat des Standard-Android-SDK eingesetzt, was zeigt, dass der Malware-Autor nicht viel Aufwand betrieben hat. Im Gegensatz dazu registrierten die Autoren der Wurmfamilie „SymbOS/XMJTC“ und seiner nahen Verwandten Entwicklerzertifikate, um ihre Malware zu signieren. Diese Zertifikate können (zur Identitätsfälschung) nachverfolgt und (zum Schutz nicht infizierter Benutzer) zurückgezogen werden.

Der Aufwand weist darauf hin, dass es sich bei Geinimi eher um einen ersten Versuch auf einer neuen Plattform als um eine fertige Malware von einem Android-Entwickler handelt.

Android/Geinimi enthält einen Satz festcodierter URLs, die in sich verschlüsselt sind und für die Verbindung zu den Botnet-Befehlsservern verwendet werden. Die Malware enthält zudem Code, der zum Senden von Daten des Mobiltelefons, des Mobilfunkanbieter und des Benutzers an Kontrollserver verwendet wird, sowie Code zur Aktualisierung der Serverliste und des Verschlüsselungsschlüssels. Die Malware kann außerdem Software von den Servern des Angreifers herunterladen. Derzeit sind jedoch alle Server inaktiv. Es ist unwahrscheinlich, dass die Malware ein aktives Botnet umfasst – zumindest bisher.

McAfee Labs erwartet im Jahr 2011 weitere Entwicklungen bei Bedrohungen dieser Klasse.

**Führung bei Botnets wechselt**

Im letzten Quartal war Cutwail eindeutig der weltweite Führer bei Botnet-Aktivitäten. In diesem Quartal war Rustock in vielen Teilen der Welt am weitesten verbreitet, Cutwail und Bobax zeigten sich jedoch weiterhin sehr aktiv.

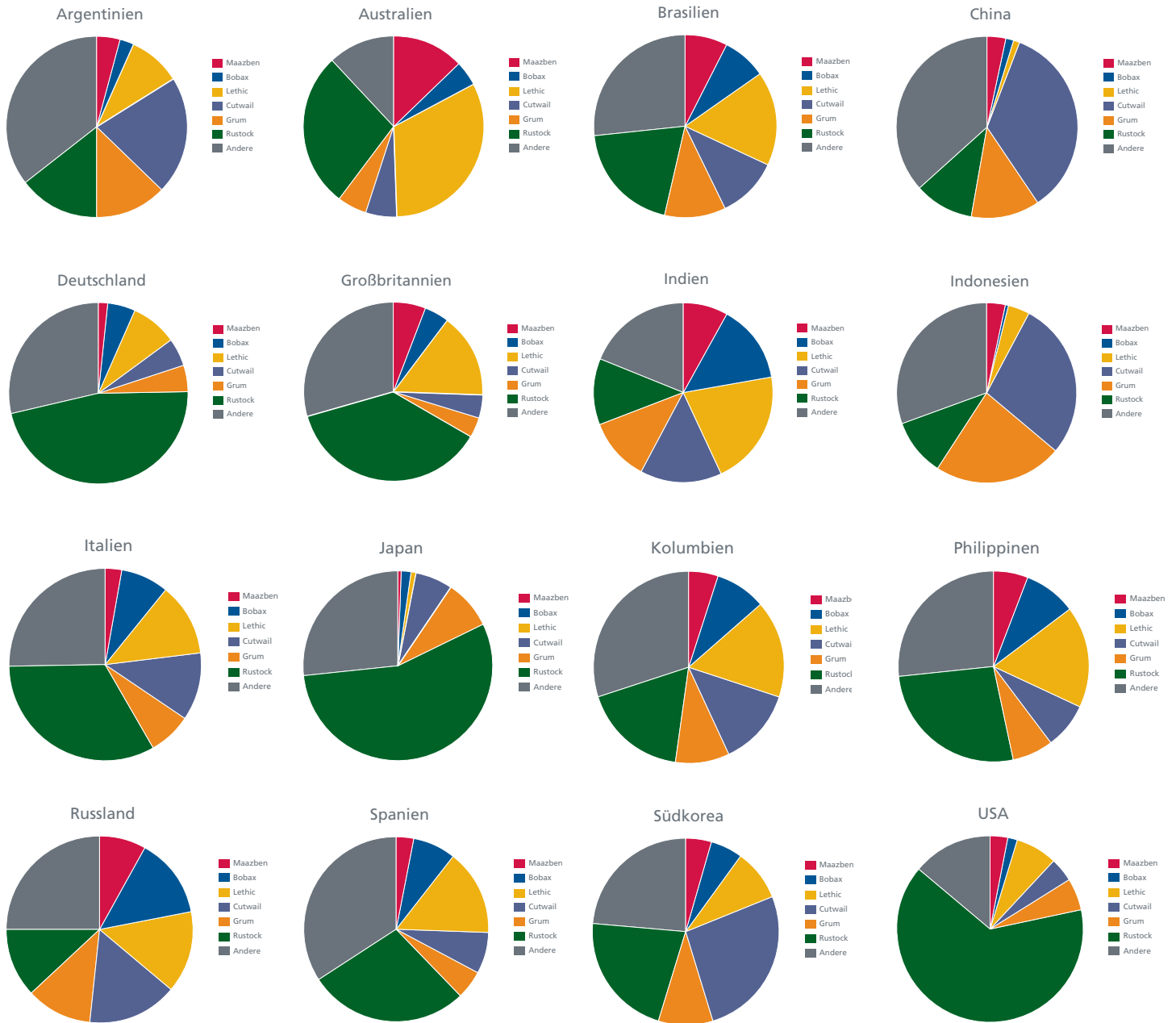


Abbildung 3: Botnets variieren in ihren Auswirkungen nach Ländern. Weltweit betrachtet war Rustock in diesem Quartal am weitesten verbreitet.

Aufgrund der Verbreitung so vieler neuer Plattformen erwartet McAfee Labs, dass Botnets zukünftig auch diese Geräte infizieren und sich darauf verbreiten werden. Das mangelhafte Sicherheitsbewusstsein unter Mobilgerätenutzern und die eher unzureichenden Sicherheitsmaßnahmen bieten Internetkriminellen eine hervorragende Möglichkeit, Schaden anzurichten.

### Malware erreicht Rekordzahlen

Böswilliger Code ist – aufgrund der scheinbaren Vielfalt und der sich ständig ändernden Ziele – die größte Bedrohung, die McAfee Labs täglich bekämpft. Der Funktionsumfang und die Effizienz von Schadcode nehmen von Jahr zu Jahr weiter zu. Seit Jahren beobachten wir, dass sich die angegriffenen Plattformen beständig verändern – und die Methoden für den Datendiebstahl werden immer raffinierter. Im Jahr 2010 identifizierte McAfee Labs mehr als 20 Millionen Malware-Exemplare.

Moment, noch einmal:

Mehr als 20 Millionen neue Malware-Varianten wurden im vergangenen Jahr erfasst. Das entspricht fast 55.000 Malware-Bedrohungen pro Tag. Das sind mehr Bedrohungen als 2009, mehr als 2008 und erheblich mehr als 2007. Von den fast 55 Millionen Malware-Varianten, die McAfee Labs identifizierte und vor denen es Schutz bot, wurden 36 Prozent im Jahr 2010 geschrieben!

Im Folgenden zeigen wir Ihnen einige Zahlen und verbreitete Malware-Klassen.

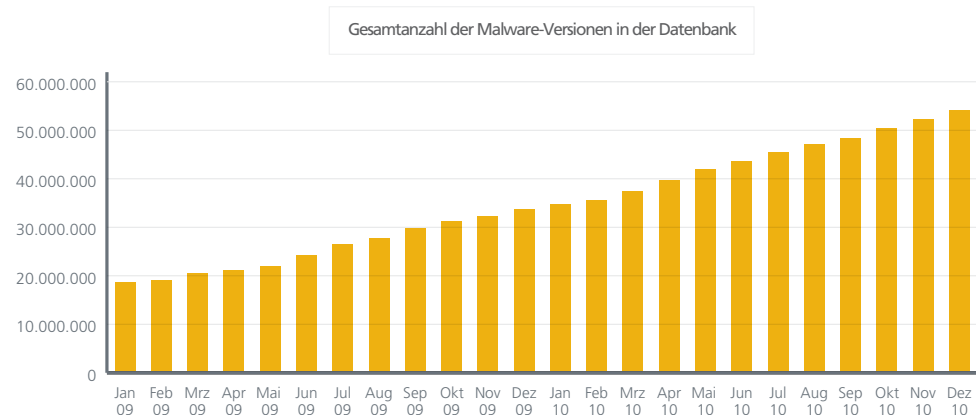


Abbildung 4: Die Gesamtzahl eindeutiger Malware-Exemplare (einschließlich Varianten) in der McAfee Labs-Datenbank.

Im vorhergehenden Diagramm ist – v. a. bei Betrachtung der Daten zu den letzten drei Jahren – deutlich zu erkennen, dass der Malware-Ansturm niemals zu enden scheint. Es bleibt abzuwarten, wie sich die Verbreitung von Handheld- und IP-fähigen Geräten auf das Wachstum auswirken wird. Ein Rückgang der Zahlen ist jedoch unwahrscheinlich.

Was ist mit den Malware-Stapeln? In den folgenden Diagrammen sehen Sie, dass Autostart-Malware seit kurzem zunimmt, während das Aufkommen bei gefälschter Sicherheits-Software stabil bleibt und bei Kennwort stehlenden Trojanern seit einem Jahreshöchstwert im Mai sogar zurückging. Koobface war Ende dieses Quartals am aktivsten, wobei die Zahlen niedriger liegen als in der ersten Hälfte dieses Jahres. (Weitere Details zu gefälschter Sicherheits-Software können Sie im vor kurzem veröffentlichten Bericht von François Paget, einem hochrangigen Forscher bei McAfee Avert Labs, nachlesen.<sup>1)</sup>)

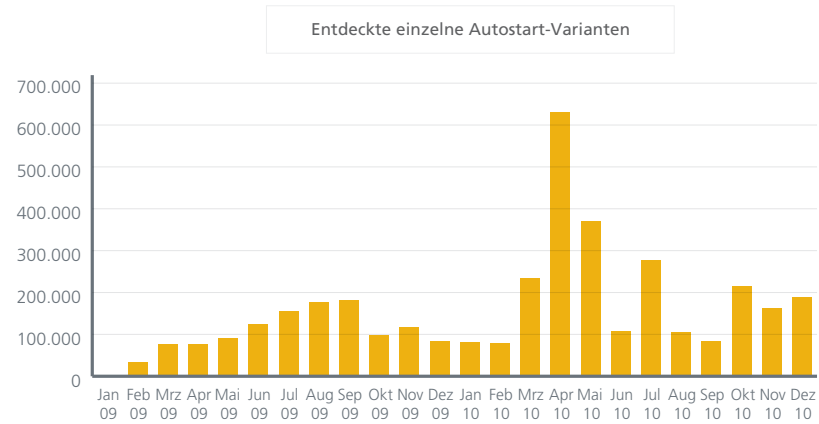


Abbildung 5: Die Anzahl der Autostart-Würmer steigt im Vergleich mit dem vorherigen Quartal wieder leicht.

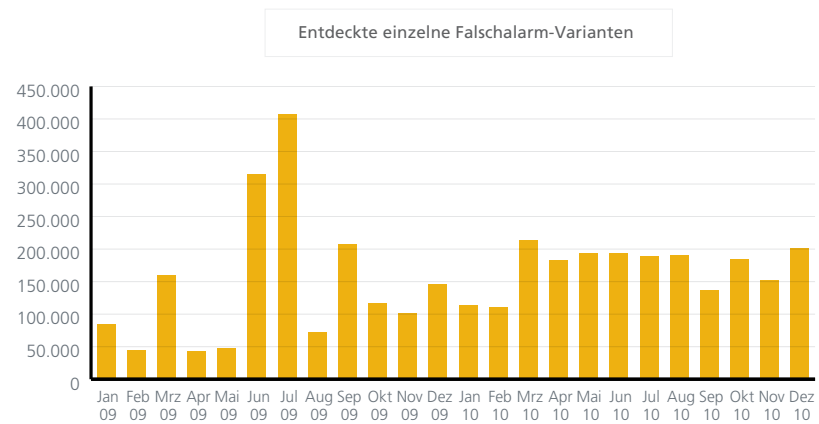


Abbildung 6: Die Anzahl der Varianten gefälschter Sicherheits-Software blieb den größten Teil des Jahres über konstant.

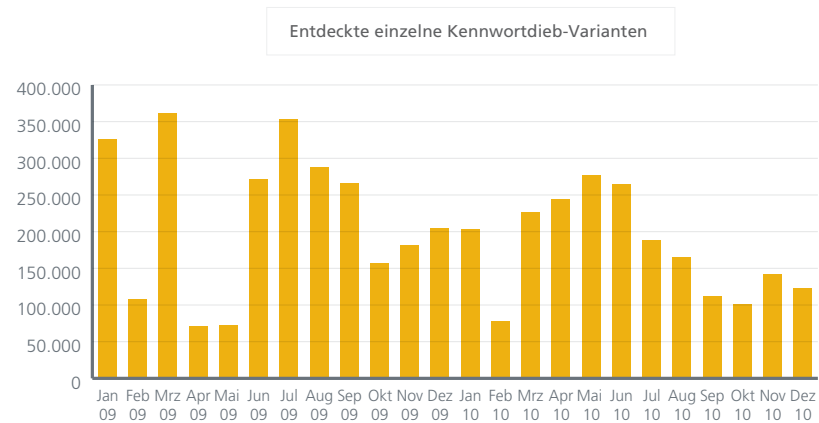


Abbildung 7: Kennwort stehlende Trojaner haben es hauptsächlich auf die Bankkontodaten der Opfer abgesehen.

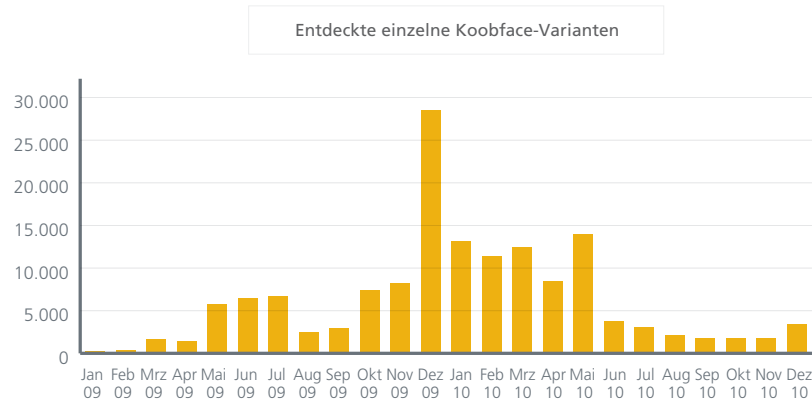


Abbildung 8: Die Anzahl neuer Koobface-Varianten, mit denen Facebook-Nutzer angegriffen wurden, stieg nach einem relativ stabilen zweiten Halbjahr im Dezember leicht an.

Seit mehreren Quartalen waren die häufigsten Malware-Bedrohungen weltweit in etwa gleich, d. h. in Nordamerika führten meist die gleichen Bedrohungen die Ranglisten an wie in Südamerika und Asien. In diesem Quartal gab es zwischen den verschiedenen Ländern erhebliche Unterschiede. Diese Unterschiede spiegeln den allgemeinen Trend wider, dass Bedrohungen sich immer mehr an Nutzer, Gewohnheiten und Ereignisse in einem bestimmten Gebiet anpassen. Wenn wir die Hintergründe bedenken, ergibt dieser Trend Sinn: Nutzer haben Vorlieben und Abneigungen, die mit ihrer Kultur und ihrem Land zusammenhängen. Internetkriminelle sind sich dieser Tatsache bewusst und greifen Nutzer daher in verschiedenen Ländern mit unterschiedlichen Methoden an.

Insgesamt waren traditionelle Viren in diesem Quartal sehr präsent. Ramnit rangierte mit einigen wenigen Varianten an der Spitze. Zu den verbreiteten Bedrohungen gehörten die Autostart-Malware „Favorites“ generic!atr, Bank-Trojaner und Downloader (manchmal als PWS oder generic.dx bezeichnet) sowie webbasierte Exploits wie StartPage und exploit-MS04-028. Zudem zeigten Adware und verschiedene Bedrohungen, die sich auf Messenger konzentrierten, ebenfalls gefährliche Aktivitäten.

Rang	Top 5 der weltweiten Malware
1	W32/Ramnit.a
2	Generic!atr
3	W32/Ramnit.a!htm
4	Exploit-MS04-028
5	Generic StartPage

Rang	Nordamerika
1	W32/Ramnit.a
2	Exploit-MS04-028
3	Generic!atr
4	W32/Ramnit.a!htm
5	Adware-OneStep.n

Rang	Europa
1	W32/Ramnit!htm
2	Generic!atr
3	W32/Ramnit.a
4	Adware-OneStep.n
5	Generic PWS.o

Rang	Südamerika
1	PWS-Banker!goj
2	Generic!atr
3	Downloader-CEW
4	W32/Jahlover.worm.gen
5	MessengerPlus

Rang	Afrika
1	Generic!atr
2	W32/Rontokbro.b@MM
3	Generic PWS.y!bfi
4	Generic.dx!cyf
5	W32/Rontokbro.gen@MM

Rang	Asien
1	Generic StartPage
2	Generic!atr
3	Generic.dx
4	W32/Rontokbro.gen@MM
5	W32/HLLP.Philis.remnants

Rang	Australien
1	Uploader-R
2	Generic.dx!vhp
3	VBS/FWBypass
4	Generic.dx
5	Generic VB.c

### Vergeht Kriminellen die Lust am Spam?

In diesem Quartal erreichte das Spam-Aufkommen den geringsten Wert seit dem ersten Quartal 2007, also seit fast vier Jahren. Außerdem machten Spam-Nachrichten in diesem Zeitraum lediglich 80 Prozent des gesamten E-Mail-Aufkommens aus – der niedrigste Anteil seit dem dritten Quartal 2006, als das Gesamt-Spam-Aufkommen sein kometenhaftes Wachstum begann, das drei Jahre später seinen Höhepunkt erreichte. Seit diesem Spitzenwert sank die Anzahl von Spam-Nachrichten um 70 Prozent. Das entspricht sogar noch weniger Spam als nach der Stilllegung von McColo, einem der größten Spam-Hostanbieter, im November 2008.

Das Aufkommen fiel in diesem Quartal im Vergleich zum vergangenen Quartal um 47 Prozent und seit Anfang 2010 um mehr als 62 Prozent. Der größte Rückgang erfolgte dabei in den letzten sechs Wochen des Jahres.

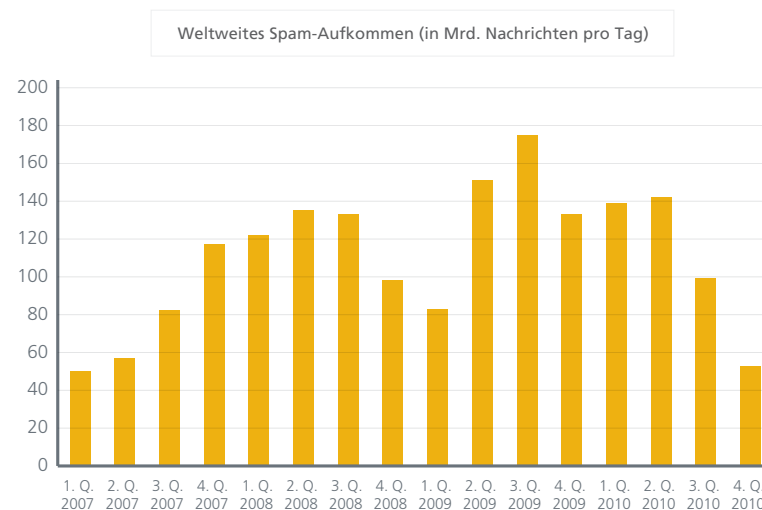


Abbildung 9: Das Spam-Aufkommen, gemessen an der durchschnittlichen Anzahl von Nachrichten pro Tag, fiel in den vergangenen zwei Quartalen schlagartig und erreichte ein so geringes Niveau wie seit 2007 nicht mehr.

Im Verlauf des Jahres schlossen einige wichtige Spam-Verbreiter ihre Tore. So stellte Spमित, ein notorischer Spammer, der für viele „Medikamenten“-E-Mails verantwortlich war, im September seinen Betrieb ein. Im Oktober erfuhren wir, dass das Bredolab-Botnet zusammen mit Teilen des Zeus-Botnets geschlossen wurde (das Zeus-Netzwerk ist jedoch weiterhin sehr aktiv). Im März wurde zudem das Mariposa-Botnet zerschlagen.

In der Weihnachtszeit erhielten Benutzer in diesem Jahr ein weiteres Geschenk, da Spam aus den Rustock-, Lethic- und Xarvester-Botnets fast vollständig ausblieb. Wir stellten um Silvester ein Wieder-aufleben des Waledac-Botnets fest. Es war Teil einer eCard-Spam-Kampagne, die zeitweise für eine von 1.000 Spam-Nachrichten verantwortlich war. Unabhängig davon führen derzeit die Bobax- und Grum-Botnets Liste der wichtigsten Spam-Verbreiter an.

Ist dies der von Bill Gates seit langem vorhergesagte Niedergang? Wohl kaum. Vielmehr scheinen wir uns in einer Übergangsphase zu befinden, in der mehrere große Botnets zu einer Zeit mit typischerweise zunehmendem Spam-Aufkommen eine Pause einlegen. Die Anzahl der Spam-Nachrichten geht im ersten Quartal meist zurück. In Anbetracht des derzeit relativ geringen Ausgangspunktes ist es eher unwahrscheinlich, dass die Zahlen viel weiter zurückgehen werden. Wir vermuten, dass die Botnet-Betreiber in den kommenden Monaten Veränderungen am Code ihrer Botnets vornehmen und sich die Machtverhältnisse zwischen den Botnets neu einpegeln werden, was wahrscheinlich zu einer erneuten Zunahme von Spam-Nachrichten führen wird.



Abbildung 10: In den einzelnen Ländern werden bei Spam höchst unterschiedliche Themen angesprochen. In diesen Diagrammen wird die relative Häufigkeit der häufigsten Themenbereiche in den jeweiligen Ländern gezeigt. Dabei erstreckt sich die Aufstellung jedoch nicht auf das gesamte Spam-Aufkommen, sondern nur auf die ersten Plätze. DSN (Delivery Status Notification) bezeichnet gefälschte Benachrichtigungen über den Zustellstatus, die behaupten, dass Ihre E-Mail das Ziel nicht erreicht hat.

**Internet-Bedrohungen**

In diesem Quartal beobachteten wir einige neue Exploits. Malware folgt weiterhin häufig der Vorgehensweise des Conficker-Wurms: Sie greift auf zahlreiche zufällig ausgewählte Domänen zu, die angepingt werden. Die böswilligen unter diesen Domänen warten darauf, dass die Malware „nach Hause telefoniert“. Die meisten dieser Domänen existieren jedoch überhaupt nicht. Die Taktik der Malware: Sie versteckt die wirklich böswilligen Domänen wie eine Nadel im Heuhaufen. Die Anzahl potenziell böswilliger Domänen und URLs stieg in diesem Quartal rasant. Die Domänen enthielten verschiedene gefährliche Aktivitäten wie Download- und Datendiebstahl-Tools (die „nach Hause telefonieren“), Beacons, Anonymisierer (die für böswillige Zwecke verwendet werden) oder Umleitungs-URLs (die Opfer zu böswilligen Downloads weiterleiten sollen). Im Gegensatz dazu beobachtete McAfee Labs, dass die monatliche Gesamtzahl aktiver URLs (die z. B. für Browser-Exploits oder zum Hosten von böswilligen Downloads verwendet werden) moderater zunahm. Einige der aktivsten Bedrohungen des letzten Jahres – darunter Zeus-Murofet, Conficker und Koobface – tauchten zusammen mit zahlreichen Drive-by-Exploit-Webseiten wieder auf.

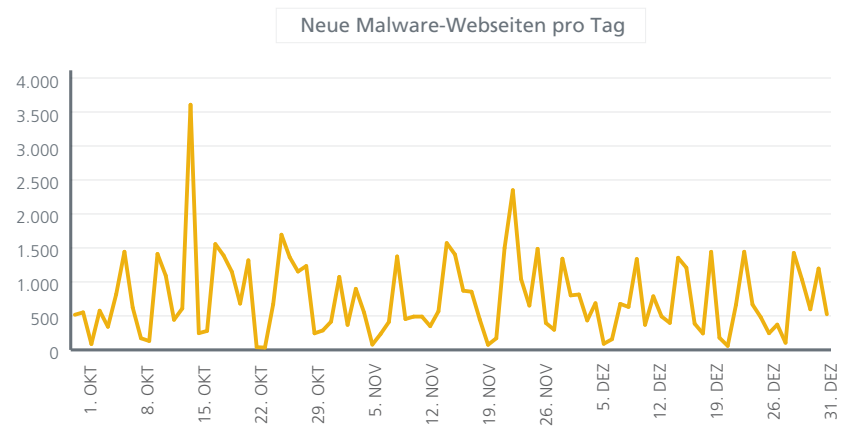


Abbildung 11: Hilfe! Conficker, Koobface und Zeus! Die Überwachung der Entwicklung verschiedener Malware-Familien und das Reverse Engineering möglicher „Heimatstandorte“ brachten einige neue böswillige URLs hervor.

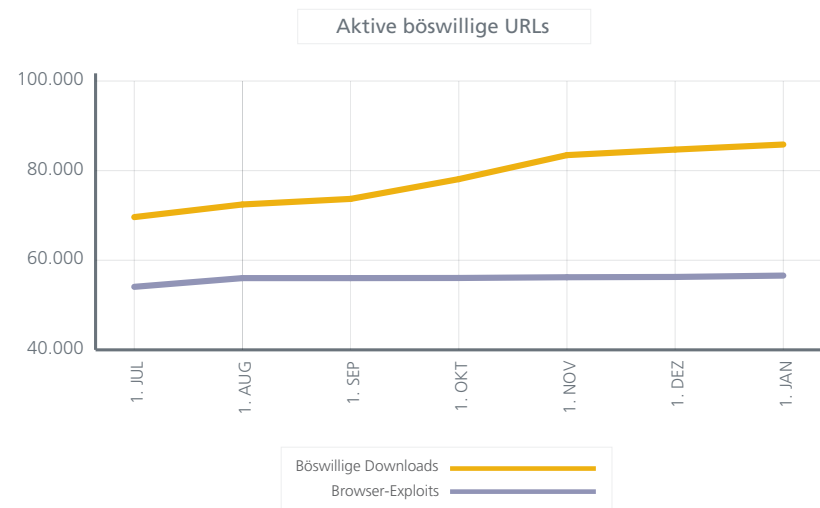


Abbildung 12: Bei den aktiven URLs stellten wir einen deutlichen Anstieg bei Webseiten fest, die böswillige Daten hosten, während die Anzahl der Browser-Exploit-Hoster in etwa gleich blieb.

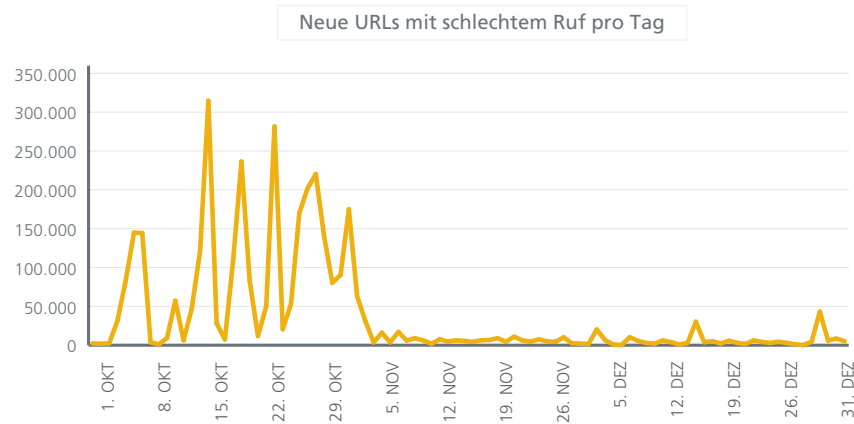


Abbildung 13: Im Oktober beobachteten wir eine große Anzahl von Domänen, IP-Adressen und URLs, die für potenziell böswillige Kommunikation reserviert waren. Der kleine Anstieg Ende Dezember wurde durch Fast-Flux und andere Crawling-Technologien verursacht.

Obwohl Phishing-URLs in diesem Quartal im Vergleich zu den vorherigen drei Monaten zurückgingen, blieb das Niveau im Vergleich zum Vorjahr sehr hoch. Wir sahen den Anfang verschiedener Angriffe, die sich auf die US-Steuerbehörde bezogen, sowie die konstante Ausbreitung in verschiedene profitable Bereiche wie Geschenkgutscheine, Gutschriftenkonten und Social-Networking-Konten.

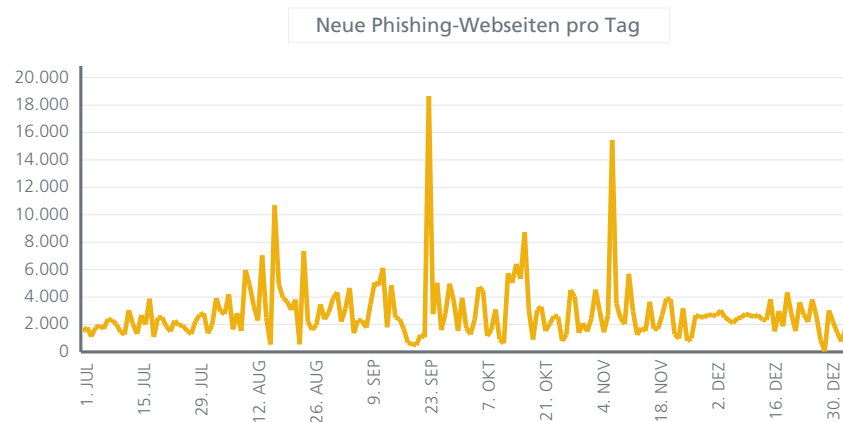
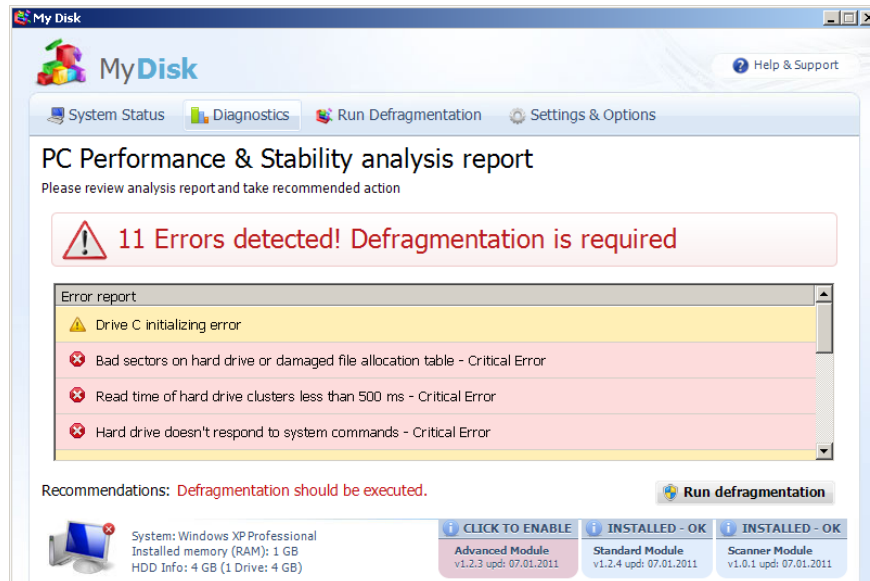
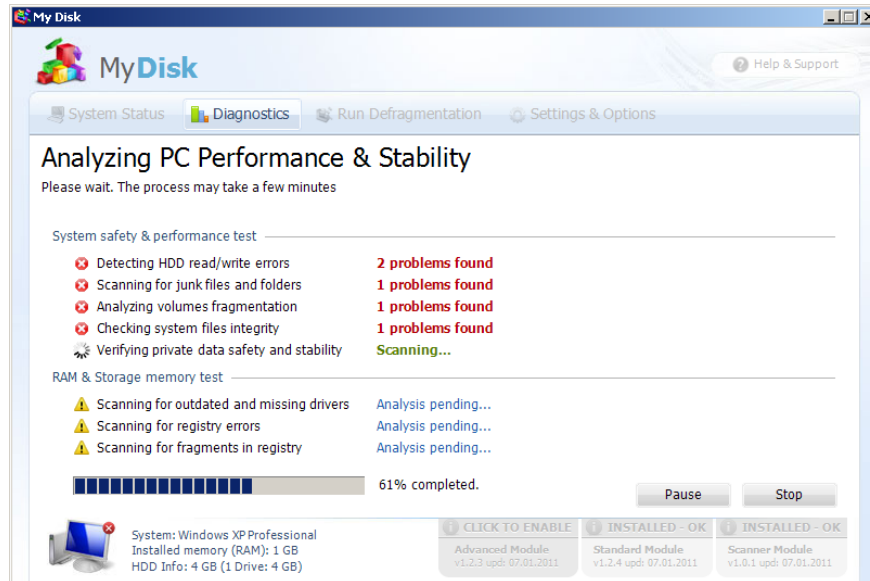


Abbildung 14: Im Jahr 2010 tauchten erheblich mehr neue Phishing-URLs auf. Im letzten Quartal nahm die Anzahl im Vergleich zum vorherigen Quartal leicht ab.

Da immer mehr Nutzer mit immer mehr Geräten auf das Internet zugreifen, werden diese Arten webbasierter Bedrohungen an Umfang und Raffinesse zunehmen. Unabhängig davon, mit welcher Hardware Nutzer ins Internet gehen – ob Computer, Tablet-PC, Smartphone oder Internet-TV-Gerät – das Internet ist immer das gleiche.





Es bleibt abzuwarten, ob gefälschte System- und Datenträgerprogramme gefälschte Virenschutz-Software als Haupteinnahmequelle für Internetkriminelle ersetzen werden. McAfee Labs wird auf jeden Fall alles daran setzen, gegen diese neue Entwicklung vorzugehen.

### Schwachstellen und Netzwerkangriffe

Für 2009 hatte McAfee Labs vorausgesagt, dass sich Malware-Autoren und Internetkriminelle zur Malware-Verbreitung und Kompromittierung von Systemen und Netzwerken definitiv auf Schwachstellen in Adobe-Produkten konzentrieren würden. Diese Voraussage ist eingetroffen. Das ganze Jahr 2010 hindurch nutzten Malware-Entwickler Schwachstellen in Flash- und vor allem in PDF-Technologien intensiv aus. Eine Analyse unserer Malware-Datenbank zeigt, dass die meisten eindeutigen Malware-Varianten in Adobe-PDF-Dateien gefunden wurden. Damit waren sie die beliebtesten Ziele bei der Clientausnutzung.

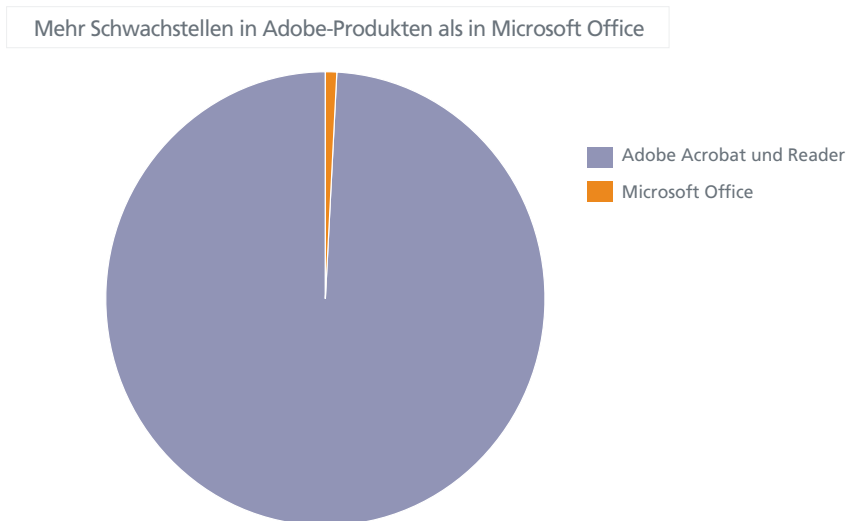


Abbildung 15: Im Jahr 2010 zählte McAfee Labs 214.992 Malware-Varianten, die die Schwachstellen in Adobe Acrobat und Reader ausnutzten. Im Gegensatz dazu nutzten lediglich 2.227 Malware-Varianten Schwachstellen in Microsoft Office-Produkten aus.

McAfee Labs ist sich sicher, dass sich diese Konzentration auf Adobe-Produkte in diesem Jahr fortsetzen wird, weil viele Mobilgeräte und Nicht-Microsoft-Betriebssysteme Adobe-Technologien unterstützen.

Hier finden Sie eine kurze Liste nennenswerter Schwachstellen dieses Quartals:

- CVE-2010-3962. Uninitialized Memory Corruption Vulnerability (Sicherheitsanfälligkeit bezüglich Speicherbeschädigung aufgrund von Nichtinitialisierung): Diese Zero-Day-Schwachstelle wurde aktiv von Malware ausgenutzt. Sie betrifft die Internet Explorer-Versionen 6, 7 und 8 und kann zuverlässig ausgenutzt werden. Die Ausnutzung lässt sich durch Aktivierung von Speicherschutzmechanismen wie die Datenausführungsverhinderung verhindern.
- CVE-2010-3971. Microsoft Internet Explorer CSS Parsing Remote Code Execution Vulnerability (Remotecodeausführungs-Schwachstelle bei der CSS-Verarbeitung in Microsoft Internet Explorer): Diese Schwachstelle wurde auf einer Schwachstellendiskussionsplattform in China veröffentlicht. Sie galt anfangs als Denial-of-Service-Schwachstelle. Später zeigte sich jedoch, dass sie mithilfe öffentlich verfügbarer Informationen ausgenutzt werden kann. Seither beobachtete McAfee Labs einige aktive Ausnutzungen. Für diese Schwachstelle stand bis zum Verfassen dieses Berichts noch kein Patch zur Verfügung. Es werden immer wieder Angriffe gestartet, die auf diese Schwachstelle abzielen. Daher raten wir allen Nutzern dringend, die Sicherheits-Software auf dem aktuellen Stand zu halten, um die Ausnutzung dieser Schwachstelle blockieren zu können.
- CVE-2010-3654. Adobe Acrobat, Reader and Flash Player Remote code execution vulnerability (Remotecodeausführungs-Schwachstelle in Adobe Acrobat, Reader und Flash Player): Hierbei handelt es sich um eine weitere Zero-Day-Schwachstelle, die aktiv ausgenutzt wird. In diesem Fall sind mehrere Adobe-Produkte auf Windows-, Mac OS X-, Solaris-, Android- und Linux-Plattformen anfällig.<sup>2</sup> McAfee Labs rät allen betroffenen Nutzern dringend, die entsprechenden Patches sofort zu installieren.

### Angriffe mit SQL-Skripteinschleusung

China und die USA sind weiterhin die Hauptquellen für Angriffe mit SQL-Skripteinschleusung. In diesem Quartal übernimmt China erneut die Führung, gefolgt von den USA und dem Iran (nach einer Zunahme der Angriffe um das zehnfache) auf dem dritten Platz. Diese Angriffe dienen in erster Linie dem Zugriff auf verschiedene Datenbankentypen und werden meist sehr professionell umgesetzt. Bei den Tätern handelt es sich im Allgemeinen um sehr entschlossene Angreifer.

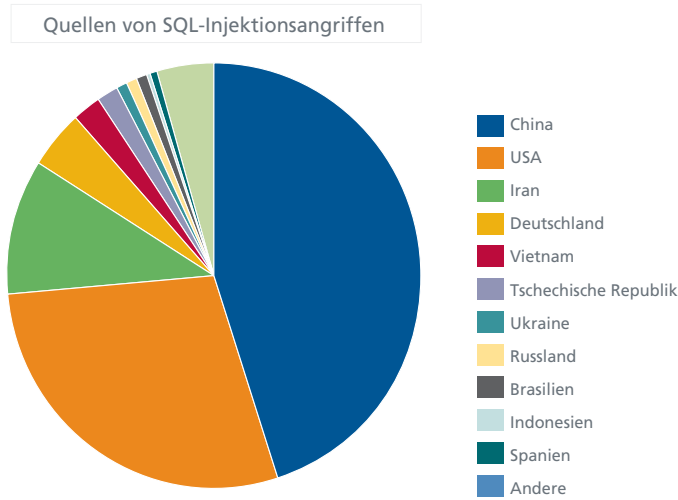


Abbildung 16: China und die USA, die Anführer der Top 10, werden in diesem Quartal überraschend vom Iran gefolgt, der seit dem letzten Quartal mehrere „Konkurrenten“ überholte.

**Internetkriminalität**

Die Ausnutzung sozialer Netzwerke kann sehr verschiedene Formen annehmen. In Anbetracht hunderter Millionen Nutzer sind sie das logische Ziel für internetkriminelle Aktivitäten. Die Konten in sozialen Netzwerken können auf verschiedenste Weise missbraucht werden. So könnten eigens erstellte Konten in Foren für Sponsoring oder Spam-Kampagnen verwendet werden. Dabei werden sie zum Versenden von Spam, Phishing-Links, Links zu gefälschten Produkten, Diensten oder böswilligen Downloads eingesetzt. Die Kosten für die Bereitstellung solcher manipulierter Konten hängen von der Kontoqualität ab. Die teuersten Konten sind dabei meist geprüfte Konten, für die eine Bestätigung per Telefonansage oder SMS erforderlich ist.

**Angebote für Konten Anzahl von Konten mit Preisen in US-Dollar**

Plattform	Kontotyp	Anzahl / Preis (USD)
Facebook	Einfaches Konto:	100/15 USD
		250/35 USD
	Konto mit mehreren Bildern:	100/22 USD
		250/55 USD
Geprüft:	50/100 USD	
	100/200 USD	
YouTube	Einfaches Konto:	100/12 USD
		250/30 USD
		500/60 USD
		1.000/120 USD
Geprüft:	100/45 USD	
	250/100 USD	
Yahoo	Einfaches Konto:	100/3 USD
		500/8 USD
		1.000/15 USD
		5.000/50 USD
Geprüft:	10.000/100 USD	
	10.000/150 USD	
Google Mail	Einfaches Konto:	100/20 USD
		250/40 USD
		500/65 USD
		1.000/120 USD
Geprüft:	100/30 USD	
	250/75 USD	
Hotmail	Einfaches Konto:	500/10 USD
		1.000/15 USD
		5.000/65 USD
		10.000/120 USD
Geprüft:	500/15 USD	
	1.000/20 USD	
Twitter	Einfaches Konto:	100/15 USD
		500/65 USD
MySpace	Einfaches Konto:	250/35 USD
		1.000/100 USD
Hushmail	Einfaches Konto:	500/10 USD
		5.000/90 USD
AOL	Einfaches Konto:	1.000/20 USD
		10.000/160 USD

Es werden auch Dienste für den Fall angeboten, dass Benutzer die Größe ihres Fan-Clubs oder ihrer Freundesliste vergrößern wollen:

Angebote	Preise
Facebook-Freunde/Fans für eine Fan-Seite	1.000 Fans weltweit: 50 USD
YouTube-Abonnenten und -Bewertungen	100 Abonnenten und Bewertungen: 7 USD 200 Abonnenten und Bewertungen: 16 USD 300 Abonnenten und Bewertungen: 32 USD 500 Abonnenten und Bewertungen: 38 USD

In diesem Quartal kamen drei Exploit-Bausätze (die auch als Crimeware bezeichnet werden) in die Schlagzeilen. Damit können Botnet-Netzwerke mithilfe vorkompilierter Exploit-Sets erstellt werden, die Software-Schwachstellen ausnutzen.

Crimeware-Name	Preise	Beschreibung
<b>Blackhole v1.0.0 beta</b>	<b>Lizenz</b> Ganzes Jahr: 1.500 USD Halbes Jahr: 1.000 USD 3 Monate: 700 USD	Neues Exploit-Kit aus Russland mit integriertem Datenverkehr-umleitungssystem, Selbstschutzmodul und erweiterten Statistikfunktionen.
<b>Phoenix v2.4</b>		Das Phoenix-Exploit-Kit erschien erstmals im Jahr 2007 und wurde regelmäßig aktualisiert. Unter den 16 Exploits sind acht, die aus dem Jahr 2010 stammen: <ul style="list-style-type: none"> <li>• LibTiff-Bibliothek von Adobe Reader: CVE-2010-0188</li> <li>• IE-Komponente iepeers: CVE-2010-0806</li> <li>• getValue-Methode von Java: CVE-2010-0840</li> <li>• Java SMB/JDT: CVE-2010-0886</li> <li>• SWF-Inhalt von Adobe PDF: CVE-2010-1297</li> <li>• QuickTime: CVE-2010-1818</li> <li>• Windows-Hilfecenter: CVE-2010-1885</li> <li>• PDF-Schriften: CVE-2010-2883</li> </ul>
<b>Eleonore v1.6 und v1.6.2</b>	2.000 USD (mit Option auf Preisnachlass zum Jahreswechsel)	Für 2010 wurde eine neue Version angekündigt. Sechs der zehn Exploits stammen aus dem Jahr 2010: <ul style="list-style-type: none"> <li>• IE-Komponente iepeers: CVE-2010-0806</li> <li>• getValue-Methode von Java: CVE-2010-0840</li> <li>• Java SMB/JDT: CVE-2010-0886</li> <li>• JDT: CVE-2010-1423</li> <li>• Windows-Hilfecenter: CVE-2010-1885</li> <li>• PDF-Schriften: CVE-2010-2883</li> </ul>

### Hacktivismus

Der politische Hauptakteur war in diesem Quartal die Aktivistengruppe Anonymous, deren Mitglieder Anfang des Quartals an verschiedenen Internetdemonstrationen gegen Urheberrechtsschutzgruppen sowie später im Quartal gegen WikiLeaks-Zensoren und -Kritiker tätig waren. In diesem Zeitraum gab es viele weitere beachtenswerte Ereignisse. In einigen Fällen vermuten wir eine gewisse Unterstützung durch Länder, von denen aus die Hacktivismus-Aktionen gestartet wurden. Die Grenzen zwischen Hacktivismus und Internetkrieg verschwimmen immer weiter.

Land/Ziel	Datum	Beschreibung
Weltweit	Oktober–November	Die Aktivistengruppe Anonymous startete mehrere groß angelegte DDoS-Angriffe (Distributed Denial of Service) gegen Webseiten von Urheberrechtsschutz-Organisationen und Anbieter von Erotikfilmen: <ul style="list-style-type: none"> <li>• SGAE (spanische Verwertungsgesellschaft für Musik-Produkte)<sup>3</sup></li> <li>• Hadopi (französische Behörde, die gegen Urheberrechtsverletzungen im Internet vorgeht)</li> <li>• Hustler (führender Anbieter für Porno-Videos)<sup>4</sup></li> <li>• Recording Industry Association of America (Verband der Musikindustrie in den USA)<sup>5</sup></li> </ul>
Survival International (internationale Organisation, die weltweit indigene Völker unterstützt)	Oktober	Eine Woche, nachdem Survival ein schockierendes Video über indonesische Soldaten zeigte, die Ureinwohner von Papua folterten, und vier Wochen, nachdem Touristen wegen der lang anhaltenden Verfolgung der Kalahari-Buschmänner zum Boykott von Botswana aufgerufen wurden, wurde ein DDoS-Angriff gestartet.
Vietnamesische Dissidenten	Oktober	Bei einer Polizeirazzia in Vietnam wurden regierungskritische Blogger verhaftet, deren Webseiten zuvor von mehr als 15.000 infizierten Computern per DDoS angegriffen wurden. <sup>6</sup>
China/Südkorea	Oktober	Die südkoreanische Geheimdienst South Korean National Intelligence Service gab bekannt, dass chinesische Hacker mithilfe von E-Mails, die angeblich vom Blue House oder von Diplomaten aus dem Ausland stammten, erfolgreich vertrauliche Informationen vom Auswärtigen Dienst und von Sicherheitsbeauftragten gestohlen wurden. <sup>7</sup>
Myanmar (Burma)	November	Kurz vor den ersten richtigen Wahlen seit mehr als 20 Jahren wurden die größten Internetanbieter von Myanmar Opfer massiver DDoS-Angriffe, die den Dienst im gesamten Land störten. <sup>8</sup> Die Motive hinter dem Angriff sind unbekannt. Es wird jedoch vermutet, dass die Regierung von Myanmar das Land kurz vor den Wahlen am 7. November isolieren wollte.
Tibetanische Diaspora	November	Phayul.com, ein führendes Nachrichtenportal der tibetanischen Diaspora, wurde Opfer eines DDoS-Angriffs, der die Webseite stark verlangsamte und zeitweise unzugänglich machte. Hinter dem Angriff steckten möglicherweise chinesische Hacker.
WikiLeaks	November–Dezember	Die Kompromittierung von mehr als 250.000 diplomatischen Depeschen des US-Außenministeriums über WikiLeaks erschütterte viele Menschen. WikiLeaks wurde ebenso wie seine Unterstützer und Gegner Opfer mehrerer DDoS-Angriffe der jeweiligen Gegenseite.

### Aktionen gegen Internetkriminelle

Obwohl osteuropäische Länder häufig für ihre nachlässige Haltung kritisiert werden, entschied sich das russische Innenministerium, gegen verschiedene internetkriminelle Organisationen vorzugehen:

Land	Beschreibung
Russland	<ul style="list-style-type: none"> <li>• Die Polizei zerschlug eine internationale kriminelle Gruppe aus mindestens 50 Verdächtigen (Russen, Ukrainer und Armenier), die für den Diebstahl von mehr als 20 Millionen Rubel von 17 russischen Banken im Zeitraum zwischen Januar und Juni 2010 verantwortlich gemacht werden.</li> <li>• Gegen Igor Gusev, einen der weltweit größten Spammer, wurde ein Strafverfahren eingeleitet. Dem Geschäftsmann wird vorgeworfen, die Glavmed/Spamit-Partnerwebseiten betrieben zu haben, über die bezahlte Spammer online Medikamente und Produkte zur Verbesserung der sexuellen Leistungsfähigkeit bewarben.<sup>9</sup></li> <li>• Verhaftete Mitglieder der kriminellen Gruppen werden für die Infizierung von Bankautomaten mit einem Computervirus verantwortlich gemacht. Der Anführer der Gruppe warb über ein internationales Internetforum einen Hacker an, der die Malware anpasste, was die Gruppe 100.000 Rubel (etwa 2.400 EUR) kostete.<sup>10</sup></li> </ul>
Niederlande, Armenien	Die Abteilung für Hightech-Kriminalität der niederländischen Kriminalpolizei löste das Bredolab-Botnet auf, das weltweit aus mindestens 30 Millionen Computersystemen bestand, die seit Juli 2009 infiziert worden waren. Die armenischen Behörden verhafteten einen 27-jährigen wegen Verdacht auf Betrieb und Anmietung des Botnets.
USA	<ul style="list-style-type: none"> <li>• Operation In Our Sites 2.0: Die US-Behörde zum Schutz von Urheberrechten (National Intellectual Property Rights Coordination Center) beschlagnahmte 82 Domänen, die nachgemachte Waren vertrieben.</li> <li>• Lin Mun Poo, ein Malaysier, wurde nach einem Treffen mit einem verdeckten Ermittler des U.S. Secret Service verhaftet, der ihm 1.000 US-Dollar in bar für 30 aktive Kredit- und Geldkarten angeboten hatte. Zum Zeitpunkt seiner Verhaftung verfügte Poo über Daten zu 400.000 gestohlenen Kredit- und Debitkartennummern.<sup>11</sup></li> <li>• In Las Vegas wurde ein junger Russe verhaftet. Laut einer Erklärung des FBI betrieb er das Mega-D-Botnet, das für Spam-Kampagnen eingesetzt wurde.<sup>12</sup></li> </ul>

3. <http://www.infosecurity-magazine.com/view/13056/anonymous-cyberprotest-group-stages-ddos-attack-on-spains-copyright-society/>

4. <http://www.myce.com/news/anonymous-calls-off-hadopi-attack-targets-hustler-35675/>

5. <http://www.app.com/article/20101102/NEWS06/101102049/Cyber-group-hacks-recording-industry-group-s-site-in-response-to-LimeWire-shutdown>

6. <http://www.vhcc.com/article/stories/51812949.shtml?cat=10077>

7. <http://joongangdaily.joins.com/article/view.asp?aid=2927242>

8. <http://www.mmtimes.com/2010/news/547/news54716.html>

9. <http://www.nytimes.com/2010/10/27/business/27spam.html>

10. <http://news.hostexploit.com/cybercrime-news/4686-russian-gang-used-customized-virus-bought-from-hacker-forum-on-atms.html>

11. <http://garwarner.blogspot.com/2010/11/in-mun-poo-hacker-of-federal-reserve.html>

12. <http://www.v3.co.uk/v3/news/2273647/fbi-botnet-spam-nikolaenko>

### Informationen zu den Autoren

Dieser Bericht wurde von Pedro Bueno, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, Craig Schmugar, Jimmy Shah und Adam Wosotowsky von McAfee Labs vorbereitet und geschrieben.

### Über McAfee Labs™

McAfee Avert Labs ist das weltweit agierende Forschungsteam von McAfee. Es ist die einzige Forschungsorganisation, die alle Bedrohungsvektoren – Malware, Internet, E-Mail, Netzwerk und Schwachstellen – abdeckt. McAfee Labs erfasst Daten von Millionen Sensoren und seinem cloudbasierten Dienst McAfee Global Threat Intelligence. Die 350 multidisziplinären Forscher, die in 30 Ländern für McAfee Labs arbeiten, überwachen permanent das gesamte Bedrohungsspektrum, identifizieren Anwendungsschwachstellen, analysieren und korrelieren Risiken und arbeiten an Fehlerbehebungsmaßnahmen, um Unternehmen und Privatpersonen zu schützen.

### Informationen zu McAfee

McAfee (NYSE: MFE) ist der weltweit größte dedizierte Spezialist für IT-Sicherheit. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer, ITK-Netze und Mobilgeräte auf der ganzen Welt vor Angriffen schützen und es den Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von der einzigartigen Global Threat Intelligence-Technologie entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. McAfee sichert Ihre digitale Welt. [www.mcafee.com/de](http://www.mcafee.com/de)

