



McAfee Threat-Report: Drittes Quartal 2011

McAfee® Labs™

Im wissenschaftlich-technischen Bereich gibt es die Messgröße namens Signal-Rausch-Abstand. Weniger technisch ausgedrückt, werden damit die Stärke des gewünschten Signals und des Hintergrundrauschens miteinander verglichen. Umgangssprachlich ist häufig das Verhältnis von relevanten zu falschen, nutzlosen oder irrelevanten Informationen gemeint. Irrelevante und häufig nutzlose Informationen? Willkommen in der Welt der Informationssicherheit. Hier haben wir es mit Unmengen an Geräuschen zu tun, die das gewünschte Signal überlagern.

Das dritte Quartal 2011 bot genügend Beispiele für Geräusche und Signale: Malware wird täglich in großem Umfang produziert. Dabei werden jedoch häufig Weiterentwicklungen übersehen, die von der schier Masse überdeckt werden. McAfee Labs beobachtete in diesem Quartal erhebliche Zunahmen bei Stealth-Malware (häufig als Rootkits bezeichnet), wobei die TDSS-Familie eine besonders unrühmliche Rolle spielt. Ebenso stieg die Anzahl der Mobilgeräte-Malware-Varianten unvermindert an. Hier liegt der Fokus vor allem auf dem Android-Betriebssystem. Genau genommen konzentrierten sich die Mobilgeräte-Malware-Autoren sogar ausschließlich auf Android-Geräte – eine Besorgnis erregende Entwicklung!

Spam und E-Mail-Bedrohungen entwickeln sich weiter. Das Gesamtaufkommen ist immer noch auf einem historisch niedrigen Stand. Davon darf man sich aber nicht täuschen lassen. Während die Anzahl der Spam-Nachrichten weltweit gesehen gering ist, wurden gezielte Spam-Angriffe (auch Spearphishing genannt) erheblich weiterentwickelt. Wenn in den Nachrichten wieder einmal von einem großen Angriff die Rede ist, erweisen sich fast immer Spearphishing-E-Mails als ursächliche Methode für die Kompromittierung. Spearphishing hat vieles mit Stealth-Malware oder Rootkits gemeinsam: Es ist dafür ausgelegt, unsere geistige Firewall mithilfe von Täuschungsmanövern oder raffiniert ausgelegten Fallen zu umgehen.

Andere interessante Veränderungen in diesem Quartal betreffen gefälschte Virenschutzprogramme, während Autostart-Malware und Kennwortdiebstahl-Trojaner auf konstantem Niveau blieben. Botnets machten weltweit gesehen große Fortschritte und sind wie bisher in den verschiedenen Regionen und Ländern unterschiedlich verbreitet. Auch die von McAfee Labs beobachteten Spam-Themen sind sehr länderspezifisch. Auch die von McAfee Labs beobachteten Spam-Themen sind sehr länderspezifisch, d. h. Angreifer sind sehr flexibel und passen ihre Themen und Malware-Varianten an die jeweiligen Regionen und Sprachen an.

Die Übersicht der häufigsten Bedrohungen spiegelt diese Vielfalt wider: Die Bedrohungen in Nordamerika haben nur wenig mit denen in Asien, Australien und dem Rest der Welt gemein. Dabei nahm die Vielfalt im Vergleich zum vergangenen Quartal zu.

Zusätzlich stellten wir erneut maßgebliche Aktivitäten in den Bereichen Internetkriminalität, Internetkriegsführung und Hacktivismus in einer Übersicht zusammen. Die Strafverfolger konnten dank zahlreicher Verhaftungen erhebliche Fortschritte machen. Die Preise im internetkriminellen Untergrund zeigen weiterhin starke Bewegungen. Mehrere groß angelegte Angriffe sowie neue Taktiken von Hacktivistengruppen wie Anonymous sorgten für ein spannendes drittes Quartal.

Eines ist gewiss: Das Jahr 2011 bleibt auch weiterhin von Veränderungen, Herausforderungen und Chaos in der Informationssicherheit geprägt.

Inhaltsverzeichnis

Bedrohungen für Mobilgeräte	4
Malware-Bedrohungen	6
Computerinfektionen im weltweiten Vergleich	10
Gefährliche Nachrichten	11
Internet-Bedrohungen	16
Internetkriminalität	20
Hacktivismus	22

Bedrohungen für Mobilgeräte

Im vergangenen Quartal wurde das Mobilgeräte-Betriebssystem Android zur „beliebtesten“ Plattform für neue Malware. In diesem Quartal war Android jedoch die *einzig*e Plattform, die von neuen Mobilgeräte-Malware-Varianten angegriffen wurde. Symbian OS (für Nokia-Geräte) hält zwar den Rekord für die größte Gesamtanzahl von Malware-Varianten, doch derzeit ist Android eindeutig das Ziel Nummer 1.

Trojaner, die Premium-SMS-Nachrichten versenden, sind für Malware-Autoren weiterhin attraktiv. Die Familien Android/Wapaxy, Android/LoveTrp und Android/HippoSMS sind neue Versionen von Trojanern, die ihre Opfer bei SMS-Abonnement-Premiumdiensten anmelden. Die Malware löscht heimlich alle eingehenden Abonnement-Bestätigungen, sodass die Opfer nichts von den böswilligen Aktivitäten merken und die Angreifer noch mehr Geld verdienen können.

Ein großer Anteil der Mobilgeräte-Malware-Varianten dieses Quartals bestand aus Anwendungen, die auf böswillige Weise modifiziert wurden. So versendet die Familie Android/PJApp durchaus SMS-Nachrichten. Die Hauptaufgabe besteht jedoch darin, sensible Telefon-Daten wie die IMEI- und IMSI-Nummer sowie die SIM-Daten zu erfassen. Diese Form des Diebstahls folgt der bekannten Vorgehensweise von Malware für jede Plattform: Zuerst wird das Gerät kompromittiert, um anschließend so viele Daten wie möglich zu stehlen.

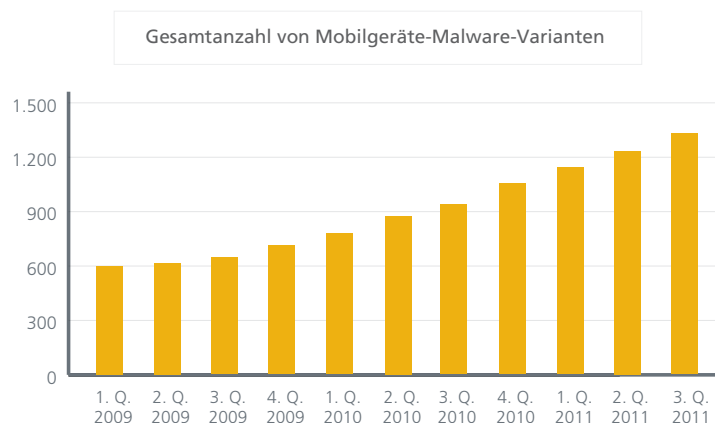
Interessanterweise nutzt Android-Malware immer häufiger eine neue Methode für den Datendiebstahl: Sie zeichnet die Telefongespräche auf und leitet diese an den Angreifer weiter. Beispiele hierfür sind Android/NickiSpy.A und Android/GoldenEagle.A. Da die Angreifer nicht wissen können, ob gleich die ersten Gespräche die gewünschten Informationen liefern, bleibt diese Malware über größere Zeiträume unerkannt auf dem Gerät. Diese Bedrohung ist wahrlich hartnäckig!

Eine andere Form des Informationsdiebstahls erfolgt mithilfe von Root-Exploits, die den Zugriff auf Systemdatenbanken ermöglichen. Dadurch können sich die Angreifer aus der Anwendungs-Sandbox befreien, in die sie bei Android-Geräten normalerweise eingeschlossen sind. Die Folge: Angreifer können auf alle Daten und Prozesse des Geräts zugreifen. Die Familien Android/DroidDeluxe und Android.ApkMon versuchen mithilfe verschiedener Exploits, Root-Zugriff zum Auslesen der Systemdateien (einschließlich der SMS-Datenbank, E-Mails und Kontakte) zu erlangen. Da sich diese Methode auf anderen Plattformen bereits seit Jahren bewährt, wird sich dieser Trend sehr wahrscheinlich fortsetzen.

Seit die SpyEye-Crimeware-Familie langsam Zeus überholt, haben die SpyEye-Autoren offensichtlich das Bedürfnis, eigene Funktionen zur SMS-Weiterleitung zu entwickeln. Da diese Funktion ausschließlich zur erfolgreichen Abwicklung betrügerischer Online-Banking-Transaktionen benötigt wird, sind diese Trojaner sehr einfach strukturiert. Android/Spitmo.A ist ein Trojaner mit SMS-Weiterleitung, der in dieser Hinsicht sehr der Zitmo-Familie ähnelt. Wozu eine komplexe Routine schreiben, wenn es auch ganz einfach geht?

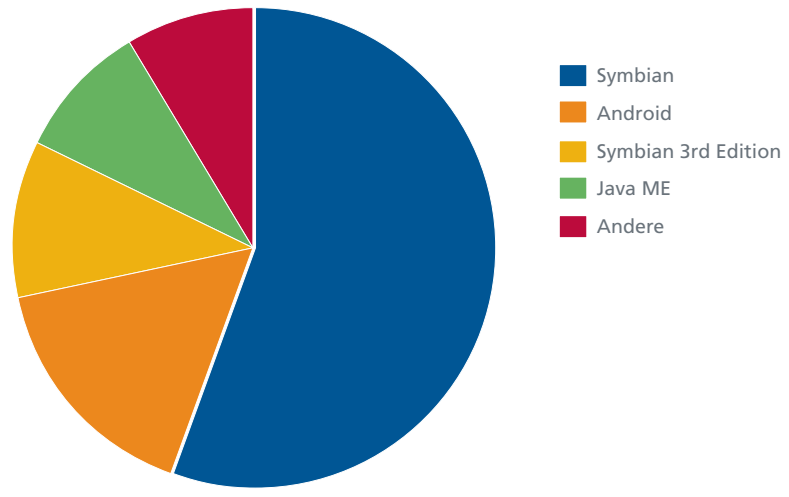
Statistische Daten zu Mobilgeräte-Malware

Das Diagramm unten verdeutlicht, dass das Aufkommen von Mobilgeräte-Malware im Jahr 2011 eindeutig die Zahlen des vergangenen Jahres übersteigt. Damit ist es das bisher aktivste Jahr in der kurzen, aber interessanten Geschichte der Mobilgeräte-Malware.

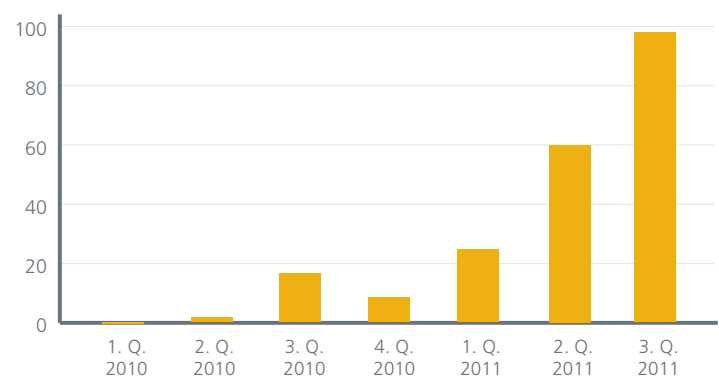


Dabei ist Android das Hauptziel von Autoren aktueller Mobilgeräte-Malware.

Gesamtanzahl von Mobilgeräte-Malware-Varianten, nach Plattform

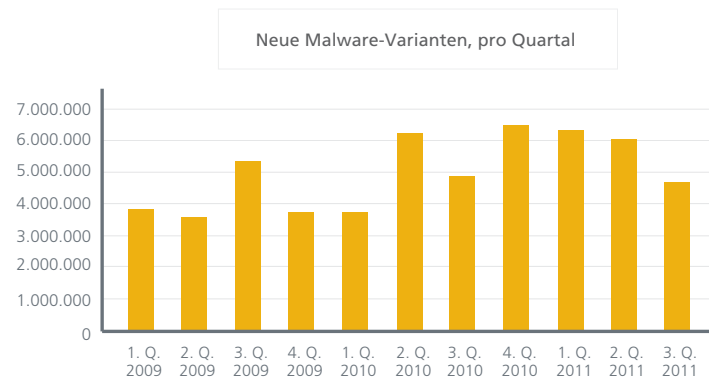
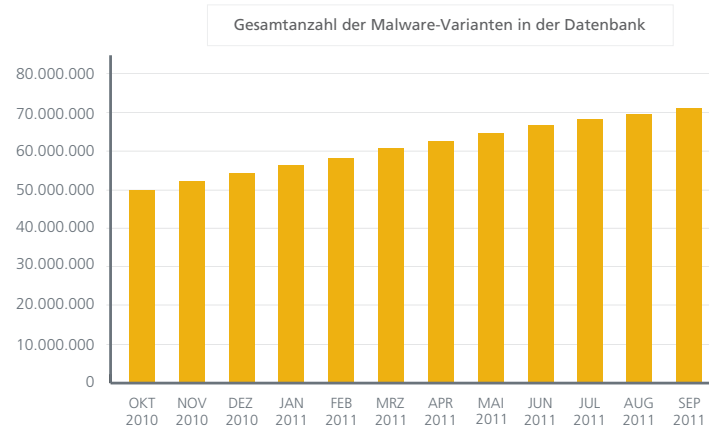


Anzahl von Android-Malware-Varianten, pro Quartal

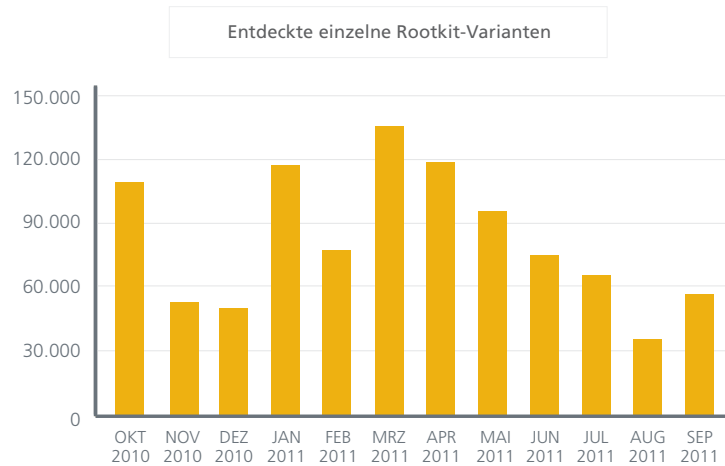


Malware-Bedrohungen

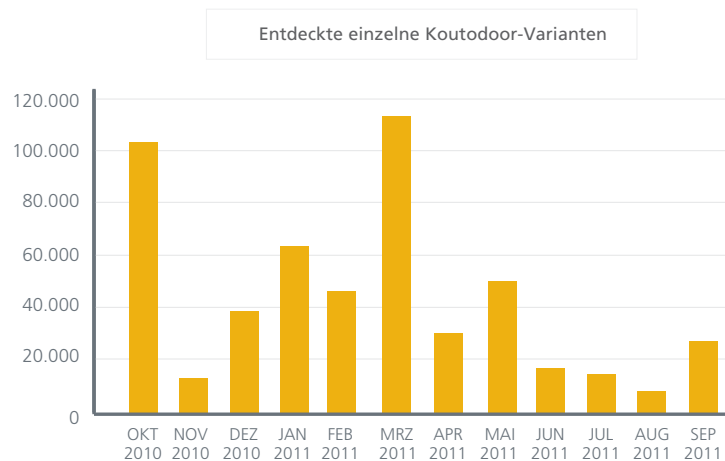
Die Gesamtzunahme bei Malware ging in diesem im Vergleich zum letzten Quartal leicht zurück, folgt jedoch in etwa dem Trend des gleichen Zeitraums im vergangenen Jahr. Das Wachstum im dritten Quartal fiel geringer aus als in den zweiten Quartalen der vergangenen zwei Jahre – vielleicht genießen die Malware-Autoren genau wie wir ihre Ferien. Das ist jedoch kein Grund, sich entspannt zurückzulehnen: Die Gesamtzahl der Malware-Varianten hat die 70-Millionen-Marke überschritten. Diese Zahl hatten wir im vergangenen Jahr vorausgesagt. Bis Jahresende erwarten wir etwa 75 Millionen eindeutige Malware-Varianten.

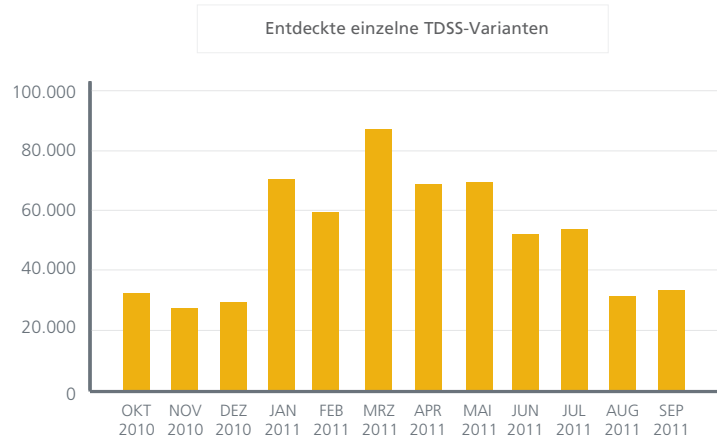


Auch wenn wir einen leichten Rückgang bei Rootkit-Varianten beobachten konnten, gibt es hier eine interessante Entwicklung. Rootkits (oder Stealth-Malware) gehören derzeit zu den unangenehmsten Bedrohungen. Sie sind darauf ausgelegt, nicht entdeckt zu werden und sich dadurch für längere Zeiträume in Systemen „einzunisten“. Im folgenden Diagramm wird deutlich, dass ihre Gesamtanzahl wieder zunimmt.

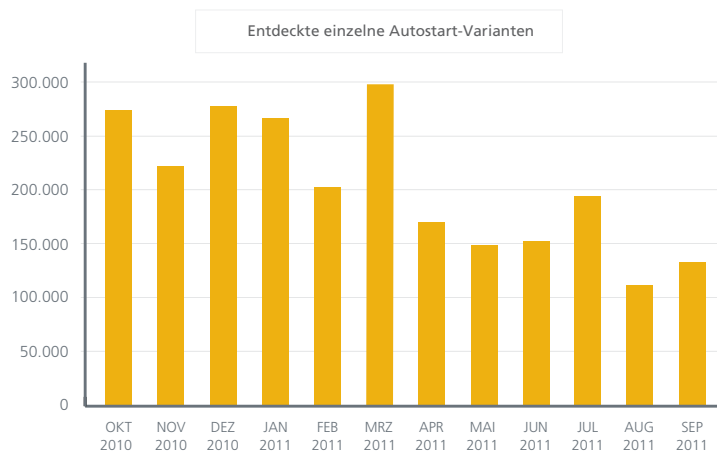
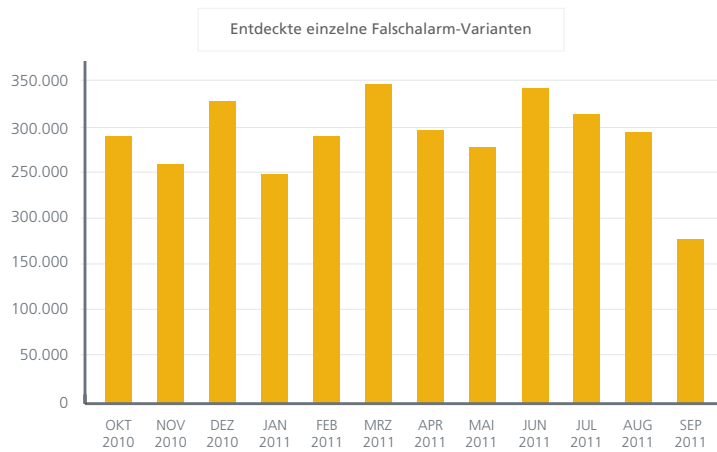


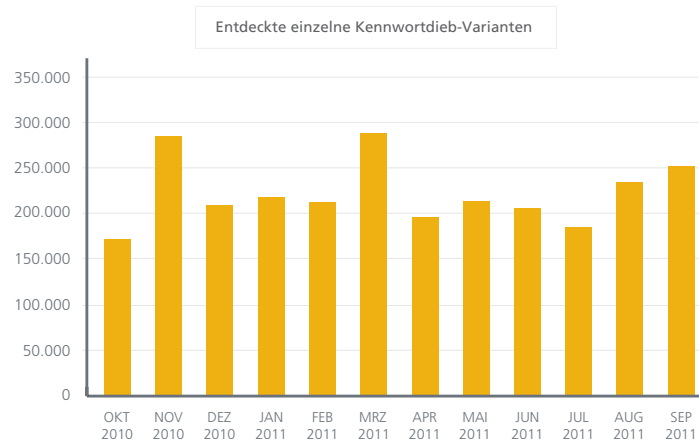
Die Sache wird noch interessanter, wenn wir die am weitesten entwickelten und verbreiteten Rootkits – Koutodoor und TDSS – betrachten. Beide Familien sind sehr beliebt, wobei TDSS etwas intensiver weiterentwickelt wird. Dies wird in den beiden nachfolgenden Diagrammen deutlich.



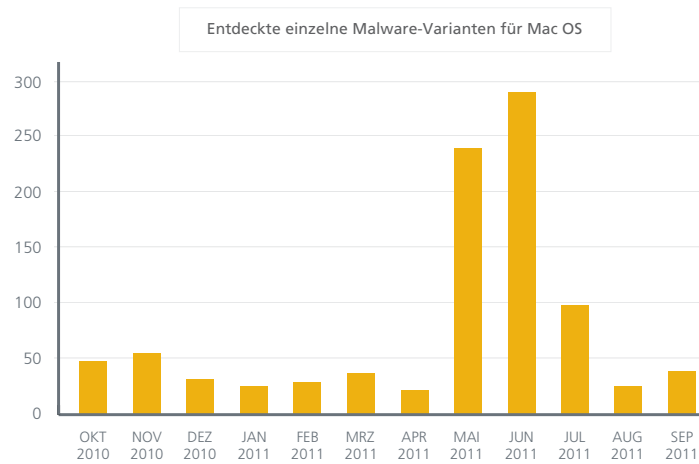


Betrachten wir einige altbekannte Malware-Formen: gefälschte Virenschutz-Software, Autostart-Malware und Kennwortdiebstahl-Trojaner. Das Aufkommen von gefälschter Virenschutz-Software, die auch als Falschalarm- oder nicht autorisierte Software bezeichnet wird, ging im Vergleich zu vergangenen Quartalen stark zurück. Autostart-Malware und Kennwortdiebstahl-Trojaner blieben hingegen auf etwa gleichem Niveau.

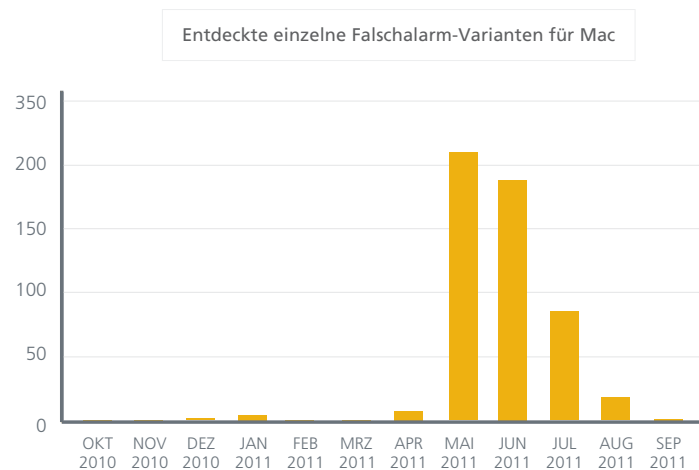




Mac-Malware, die zuvor häufig nicht richtig ernst genommen wurde, nimmt weiterhin leicht zu. Lassen Sie sich jedoch nicht täuschen. Bei Betrachtung der Gesamtzunahme von Mac-Malware scheint die Entwicklung unauffällig.



Die Situation stellt sich jedoch anders dar, wenn wir gefälschte Virenschutz-Software für Mac-Computer betrachten.



Dabei wird deutlich, dass gefälschte Virenschutz-Software für Mac im zweiten Quartal dieses Jahres stark zunahm. Auch wenn dieses Quartal weniger Aktivitäten aufwies: Jedes Betriebssystem kommt als Ziel in Betracht. Bleiben Sie wachsam.

Computerinfektionen im weltweiten Vergleich

Die häufigsten Bedrohungen ändern sich weiterhin weltweit von Quartal zu Quartal. Während im vergangenen Quartal Downloader und einige potenziell unerwünschte Programme eine große Rolle spielten, waren in diesem Quartal parasitäre Malware und Exploits beliebter, wobei wir letztere weltweit häufiger entdeckten. Diese Daten spiegeln tatsächliche Erkennungen von weltweiten Erkennungstechnologien wider. Daher wird Malware zusammen mit potenziell unerwünschten Programmen und anderen Bedrohungen aufgeführt. Die Aufstellung nach Land zeigt, dass in einigen Regionen Varianten eines Themas dominieren, während es andere Regionen mit völlig unterschiedlichen Bedrohungen zu tun haben. Webbasierte Ausnutzungen, die zu Infektionen mit parasitärer Malware führen, sind überall verbreitet. Und auch Kennwortdiebstahl-Trojaner spielen weiterhin eine wichtige Rolle.

Rang	Top 5 der weltweiten Bedrohungen
1	Böswillige Iframes
2	Böswillige Windows-Verknüpfungsdateien
3	Parasitäre Dateinfektoren
4	USB-basierte parasitäre Autostart-Malware
5	Webbasierte Dateinfektoren

Rang	Nordamerika
1	Böswillige Iframes
2	Böswillige Windows-Verknüpfungsdateien
3	Parasitäre Dateinfektoren
4	Webbasierte Dateinfektoren
5	USB-basierte parasitäre Autostart-Malware

Rang	Südamerika
1	Banking-Trojaner-Varianten
2	Varianten von Kennwortdiebstahl-Trojanern
3	Varianten von Kennwortdiebstahl-Trojanern
4	Varianten von Kennwortdiebstahl-Trojanern
5	USB-basierte parasitäre Autostart-Malware

Rang	Europa
1	Webbasierte Dateinfektoren
2	Parasitäre Dateinfektoren
3	USB-basierte parasitäre Autostart-Malware
4	Generische Downloader-Trojaner
5	Adware.HotBar

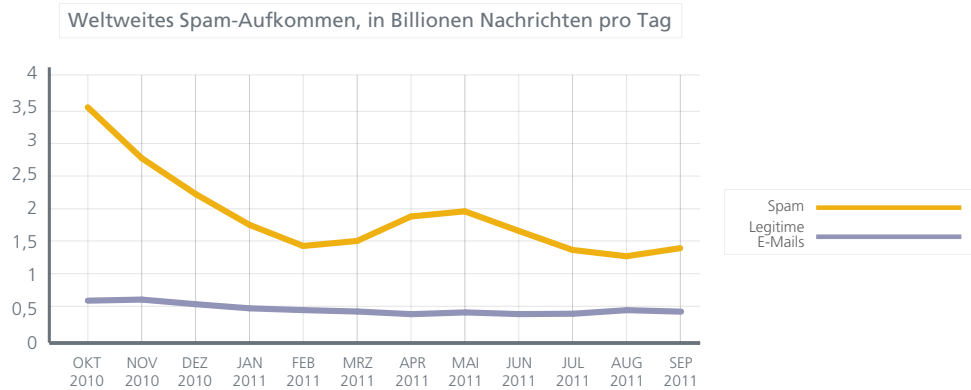
Rang	Asien
1	Parasitäre Dateinfektoren
2	Varianten von Kennwortdiebstahl-Trojanern
3	USB-basierte parasitäre Autostart-Malware
4	Generische Downloader-Trojaner
5	Varianten von Kennwortdiebstahl-Trojanern

Rang	Afrika
1	Varianten von Kennwortdiebstahl-Trojanern
2	USB-basierte parasitäre Autostart-Malware
3	Adware.HotBar
4	Böswillige Windows-Verknüpfungsdateien
5	Varianten des Mabezat-Wurms

Rang	Australien
1	Varianten von Kennwortdiebstahl-Trojanern
2	Böswillige Windows-Verknüpfungsdateien
3	Varianten böswilliger Windows-Verknüpfungsdateien
4	Parasitäre Dateinfektoren
5	Varianten von Zeus/SpyEye-Trojanern

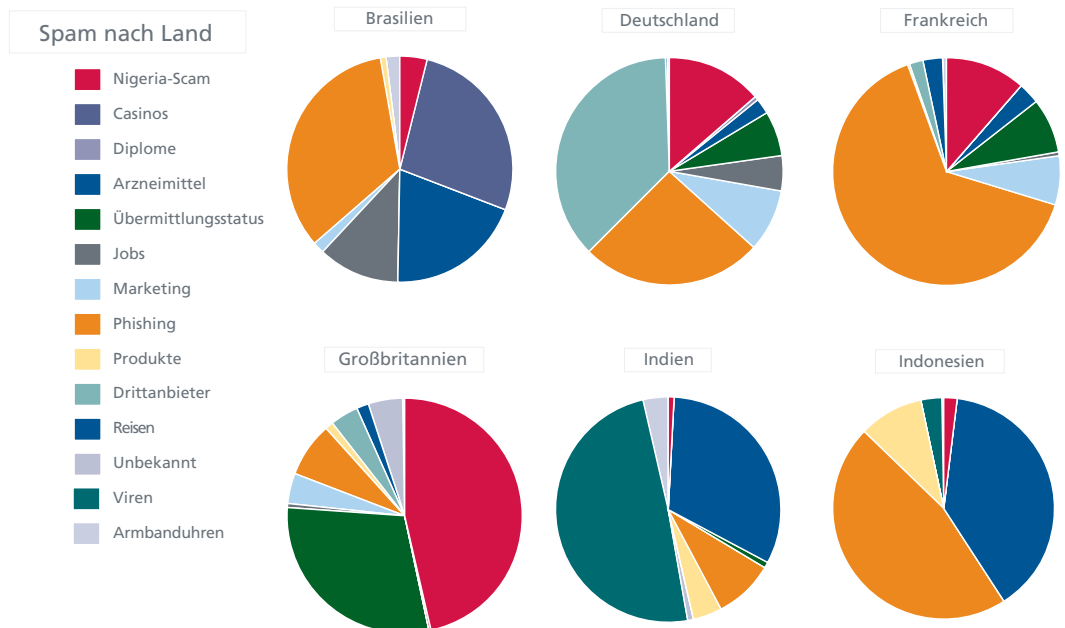
Gefährliche Nachrichten

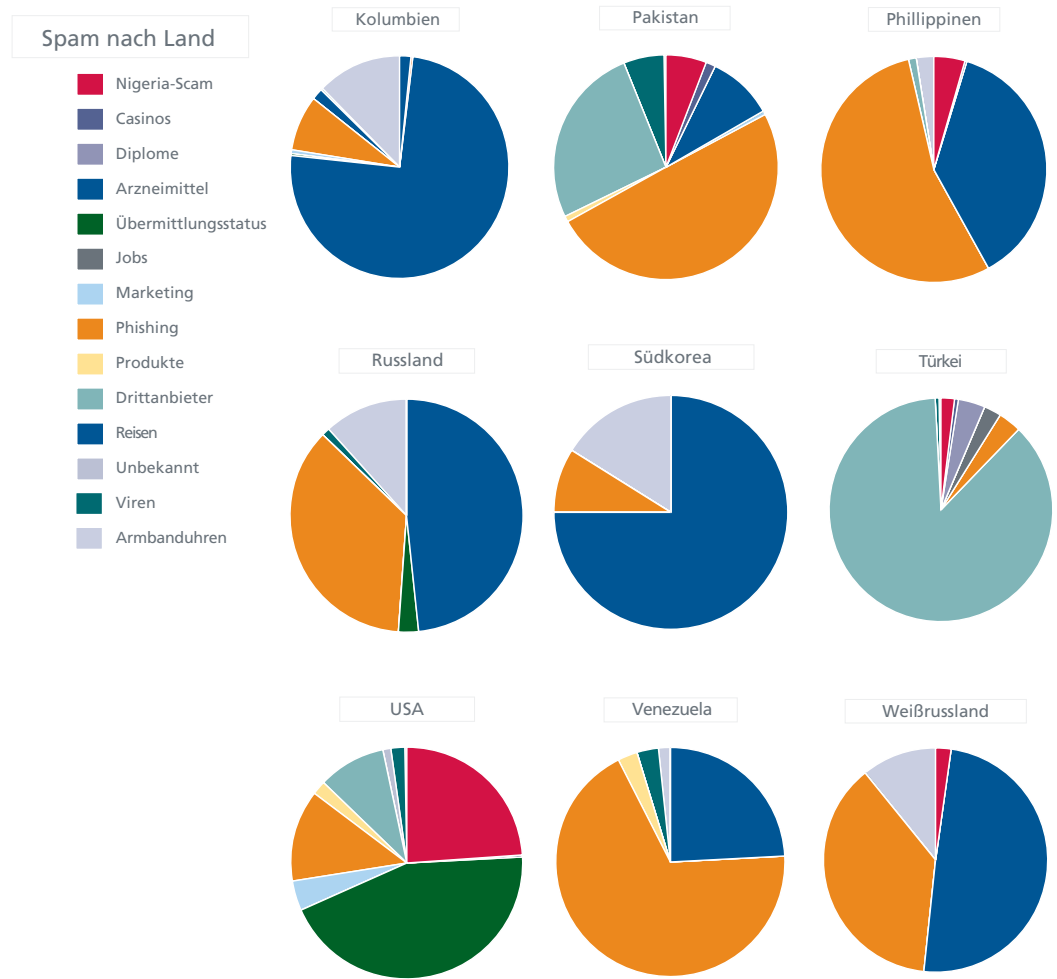
Auf der ganzen Welt zeigt Spam einen rückläufigen Trend und kommt den Werten des Jahres 2007 nahe. Obwohl das Spam-Aufkommen erheblich gesunken ist, sind gezielte Spam-Angriffe (das so genannte Spearphishing) nach Beobachtungen von McAfee Labs im Vergleich zu den letzten Jahren auf einem Höchststand. Ebenso wie bei Malware lässt uns das Rauschen also glauben, dass das Spam-Niveau zurückgegangen ist, während uns das Signal verrät, dass die Kriminellen ihre Taktik geändert haben. Sie schützen ihr Geschäftsmodell und legen dabei eine Raffinesse an den Tag, die die Angriffe noch gefährlicher macht.



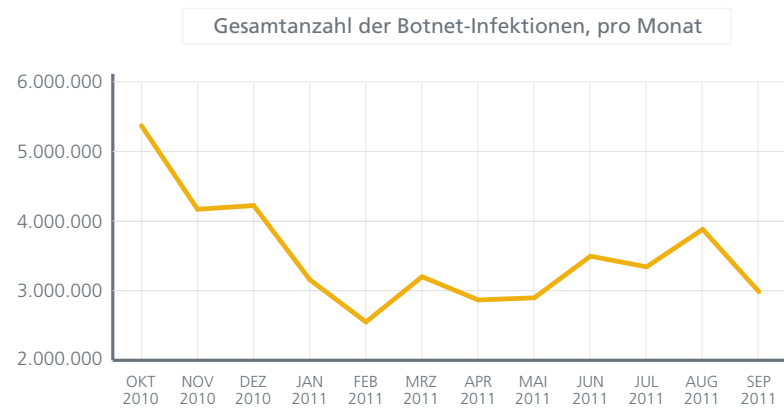
Social Engineering spricht Ihre Sprache

Wie auch bisher unterscheiden sich die Social-Engineering-Köder in den Betreffzeilen von Spam-Nachrichten je nach Region und Sprache erheblich. Diese Köder können sich monatlich oder saisonal bedingt ändern und nutzen oft Ferien oder Sportereignisse als Lockmittel. Die Angreifer zeigen ein bemerkenswertes Wissen darüber, was in der jeweiligen Kultur und Region das größte Interesse weckt. Während in Frankreich Phishing-Betrug erfolgreich ist, dominieren in Großbritannien Nigeria-Scams. In der Zwischenzeit bevölkert Medikamenten-Spam die Posteingänge der Computernutzer in Südkorea und Russland, und in den USA locken Spam-Verteiler häufig mit E-Mail-Sendefehlern. Die Angreifer zeigen viel Fantasie und wissen genau, wie sie ihre Opfer überlisten können.





Das weltweite Botnet-Wachstum zeigte zum Ende des Quartals einen leichten Rückgang. In einigen Regionen nahmen die Aktivitäten jedoch massiv zu.



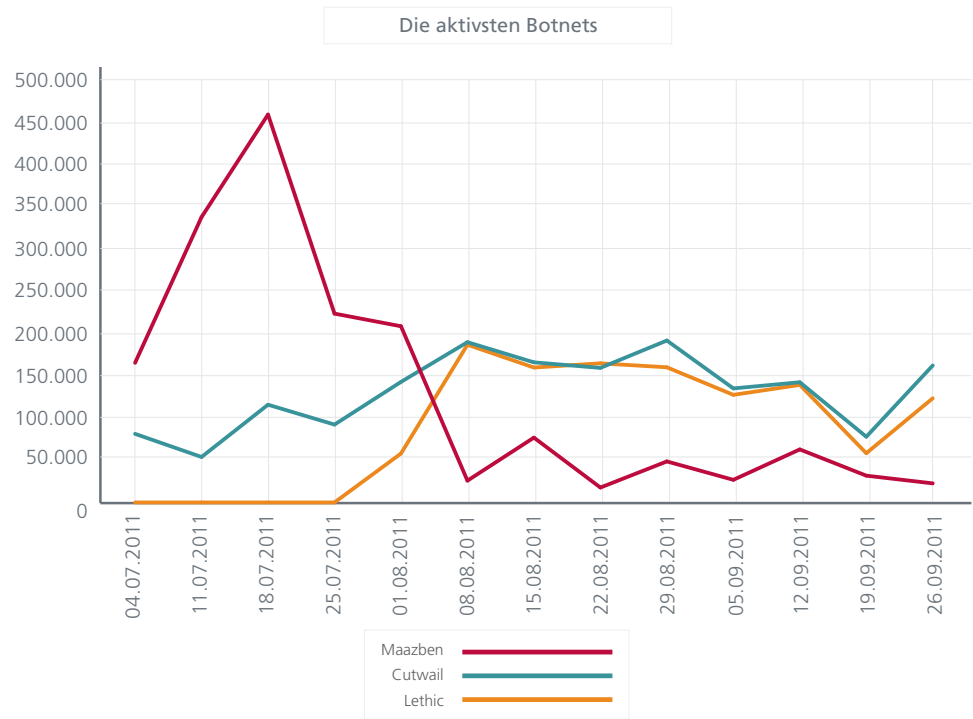
Quellen für neue Botnets, nach Land



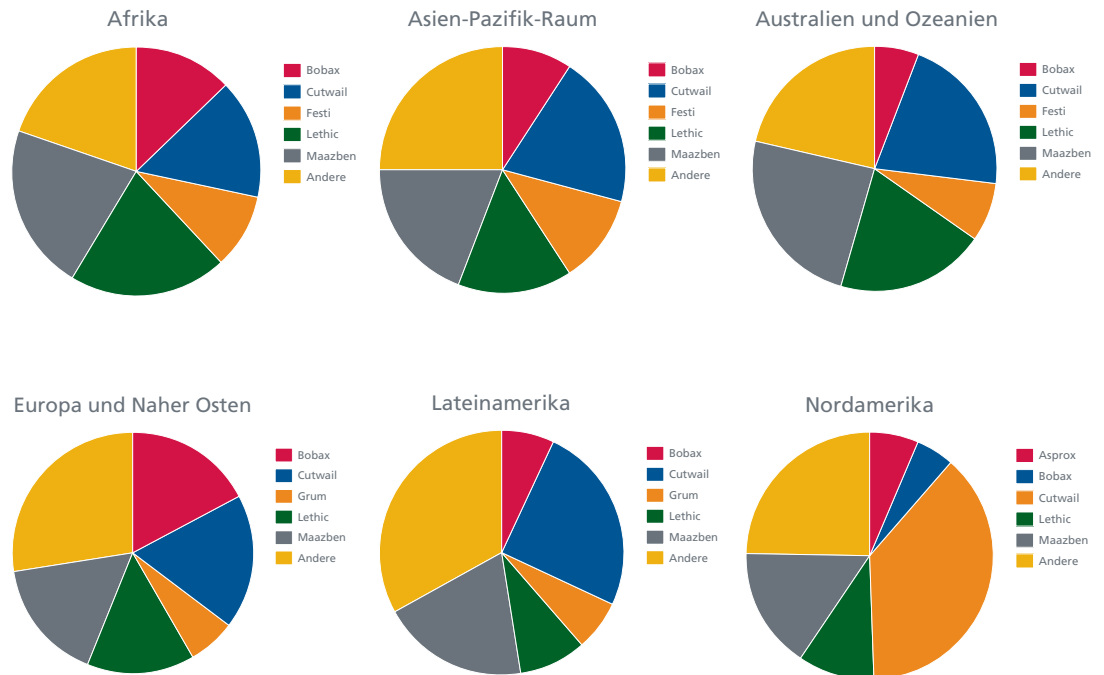
Quellen für neue Botnets, nach Land



In mehreren Ländern stieg die Zahl der Botnet-Infektionen erheblich an. Cutwail, Festi und Lethic führen die Liste der aktivsten Botnets dieses Quartals an, während die Infektionen durch Grum, Bobax und Maazben zurückgingen.



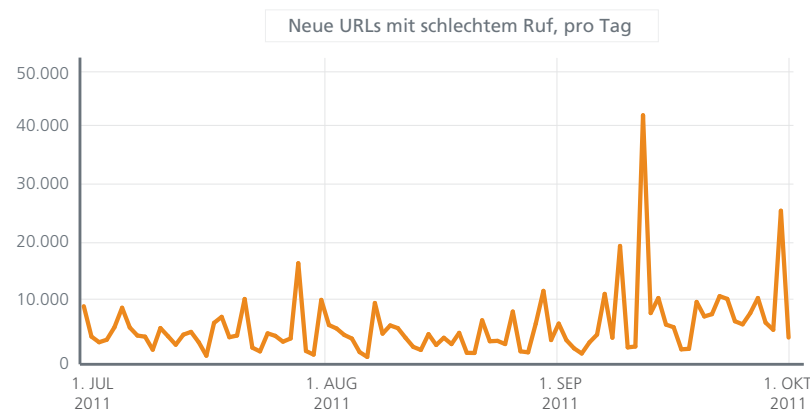
Bedenken Sie jedoch, dass rückläufige Infektionsraten nicht automatisch verringerte Botnet-Aktivitäten bedeuten. Bei der Analyse der Botnets nach Region stellen wir fest, dass einige noch immer sehr aktiv sind, selbst wenn die Zahl der Neuinfektionen vorübergehend stagniert.



Internet-Bedrohungen

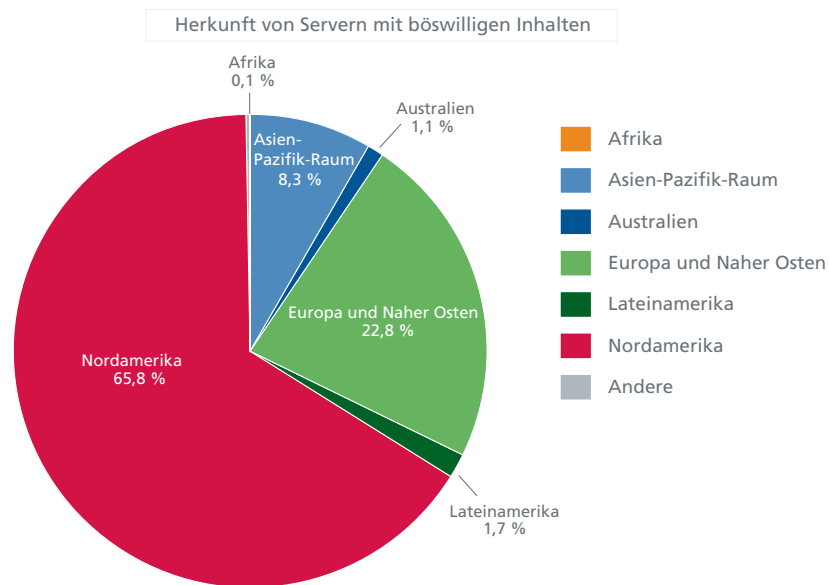
Webseiten werden aus verschiedenen Gründen als gefährlich eingestuft. Ihre Reputation kann auf der Gesamtdomäne und beliebigen Unterdomänen sowie auf einer bestimmten IP-Adresse oder URL basieren. Die Einstufung als böswillige Webseite kann sich durch das Hosten von Malware, potenziell unerwünschten Programmen oder das Fungieren als Phishing-Webseite ergeben. Häufig beobachten wir Kombinationen aus fragwürdigem Code und ebensolchen Funktionen. Bei der Bewertung der Webseiten-Reputation werden viele Faktoren berücksichtigt.

Im ersten Quartal erfasste McAfee Labs pro Tag durchschnittlich 7.300 neue gefährliche Webseiten. Dieser Wert sank im zweiten Quartal geringfügig auf 6.500 Neuentdeckungen, also etwa die gleiche Anzahl wie im gleichen Quartal des vergangenen Jahres. Im August wurden im Durchschnitt mehr als 3,5 Webseiten pro Minute als gefährlich eingestuft.

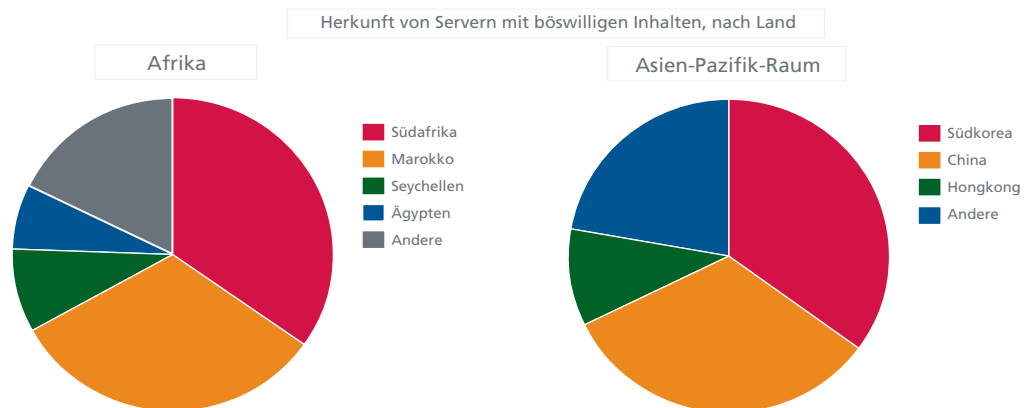


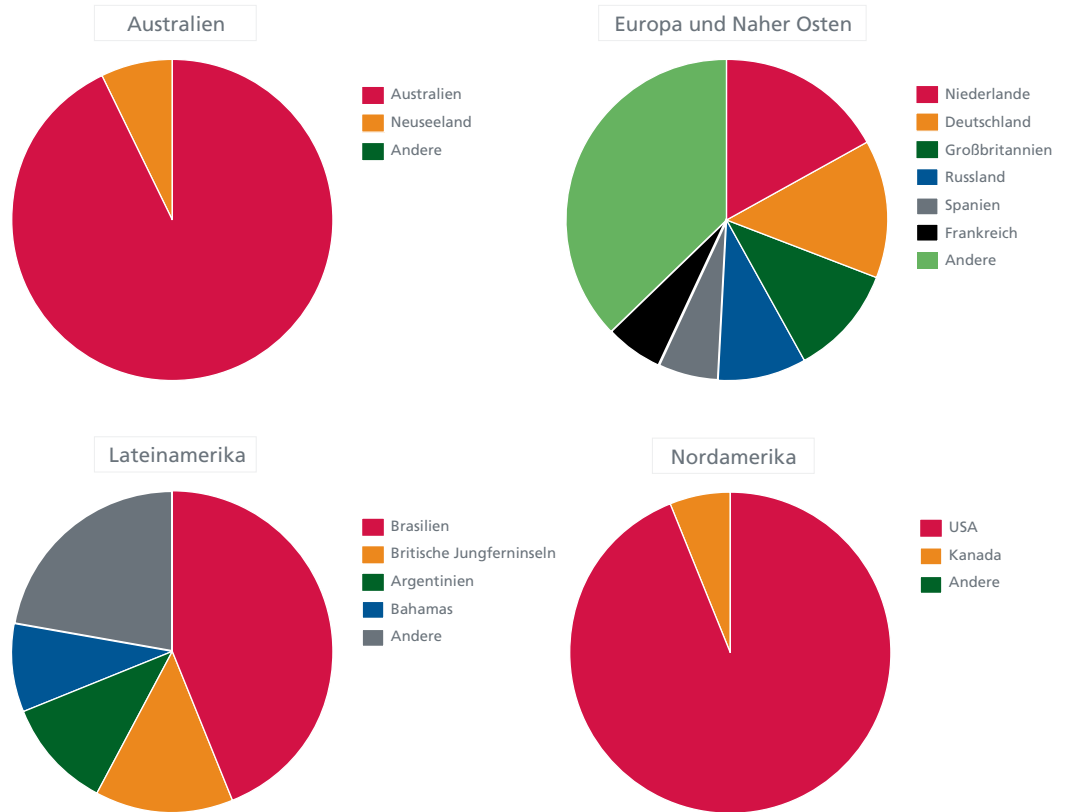
Wir beobachteten in diesem Quartal vier starke Spitzen bei Webseiten mit böswilligen Inhalten, die nicht mit bestimmten Angriffen zusammenhängen. Stattdessen wurden interne oder externe Sensoren aktualisiert, die regelmäßig Daten an unsere Internet-Bedrohungsdatenbank senden. Im Folgenden gehen wir genauer darauf ein.

Der überwiegende Teil der neuen böswilligen Webseiten befindet sich in den USA, gefolgt von den Niederlanden, Kanada, Deutschland, Südkorea, China und Großbritannien. Im letzten Quartal führten die gleichen Länder die Liste an, jedoch in einer anderen Reihenfolge. In unserer Übersicht werden die häufigsten Hosts für böswillige Inhalte nach Region aufgeschlüsselt.

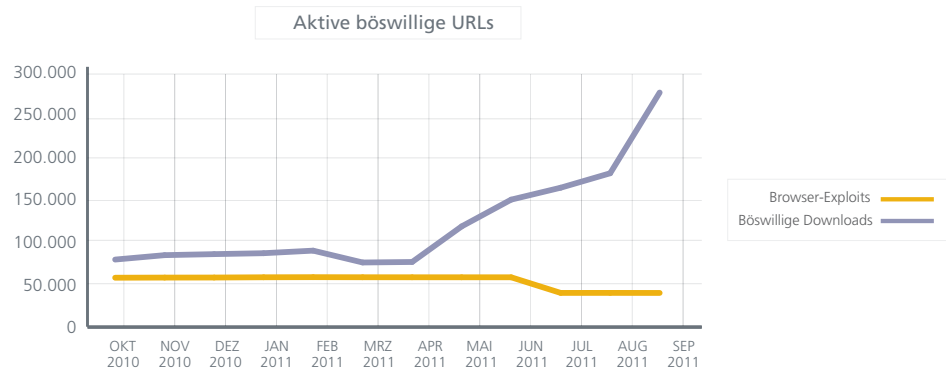


Nordamerika führt mit großem Abstand (mit 68 Prozent im ersten, 60 Prozent im zweiten und 66 Prozent im dritten Quartal dieses Jahres), gefolgt von Europa und dem Nahen Osten (18 Prozent, 25 Prozent und 23 Prozent in diesem Quartal). Sehen wir uns die einzelnen Region einmal genauer an.

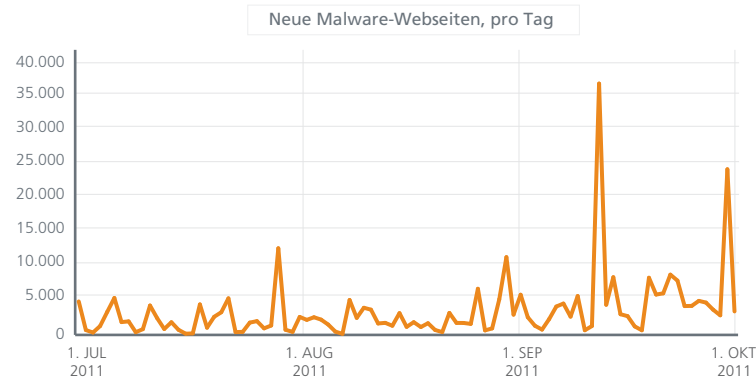




Während die Anzahl von Webseiten, die böswillige Downloads hosten, in diesem Quartal erneut stieg, ging die Anzahl von Browser-Exploit-Hostern leicht zurück.



Im folgenden Diagramm wird die Anzahl der von McAfee Labs in diesem Quartal entdeckten Webseiten dargestellt, die Malware und potenziell unerwünschte Programme hosten.

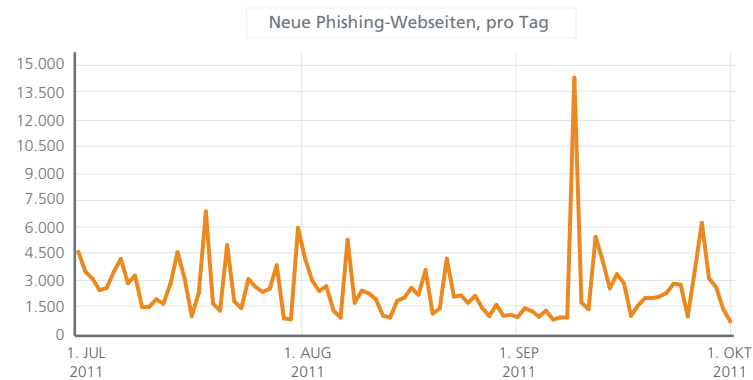


Wir beobachteten in diesem Quartal mit etwa 3.500 neuen Webseiten pro Tag einen Anstieg gegenüber den täglich 3.000 Webseiten des vergangenen Quartals.

Die beiden großen Spitzen am 12. und 30. September wurden durch umfangreiche Aktualisierungen unserer Sensoren verursacht, die URLs mit Malware erfassen.

In diesem Quartal registrierten wir täglich etwa 2.700 Phishing-URLs. Dies entspricht in etwa den Zahlen des letzten Quartals. Im gleichen Zeitraum des vergangenen Jahres kamen wir auf 2.900 URLs pro Tag.

Am 9. September kam es zu einer Spitze mit mehr als 14.000 neu erkannten böswilligen Webseiten, die durch eine Aktualisierung unserer Phishing-Sensoren erstmals erfasst werden konnten. An diesem Tag fanden wir besonders viele URLs bei Taobao (einem chinesischen Online-Händler), Citibank, Numericable (französischer Internetanbieter), Bank of America, PayPal sowie Wells Fargo.



Internetkriminalität

In diesem Quartal bieten wir erneut einen Überblick über die Preise des Untergrundmarktes.

Im September analysierte der Sicherheitsexperte Brian Krebs einige Aktivitäten, die mit dem TDSS-Botnet und ganz besonders awmproxy.net zusammenhingen. Dieser Dienst, der dank Ausnutzung gekidnappter Computer anonymen Internetzugang anbietet, wurde als „der schnellste anonyme Proxy“ für den Internetzugang angepriesen.¹ Innerhalb kurzer Zeit öffnete der AWM-Proxy mit neuer URL auf einer neuen Webseite. Internetkriminelle lassen sich meist nicht lange von ihren Aktivitäten abhalten und erlangen im Allgemeinen wieder die Kontrolle über ihr Geschäft.

Exklusive und individuelle Proxies

Diese Proxies werden für die anonyme Nutzung des Internets, von ICQ und FTP sowie für Online-Spiele wie Kasino, Poker und Roulette verwendet. Nach Aussagen der Verkäufer sind die Proxies für jeden Kunden einmalig.

Produktname		Exclusive-100	Exclusive-200	Exclusive-500
Anzahl der Proxies		100	200	500
Anzahl der Veränderungen in der Liste pro Tag		50	100	200
Automatischer Austausch „toter“ Proxies durch Wahl eines Landes mit hoher Priorität		Alle Russland USA oder Kanada		
Preise	1 Woche	90 USD	160 USD	300 USD
	2 Wochen	160 USD	290 USD	550 USD
	30 Tage	290 USD	550 USD	1.000 USD

Produktname		Individual-5	Individual-15	Individual-30
Anzahl der Proxies		100	200	500
Anzahl der Veränderungen in der Liste pro Tag		50	100	200
Preise	2 Wochen	40 USD	60 USD	100 USD
	30 Tage	60 USD	100 USD	160 USD

Persönliche Proxies

Mit Browser-Proxies ist der anonyme Zugriff auf Pornografie-Seiten, Unterhaltungsangebote für Online-Kasinos, Bezahlssysteme sowie andere Webseiten möglich, die den Zugriff aus bestimmten Ländern blockieren.

Zeitraum	1 Tag	2 Wochen	1 Monat
Preise (für unbegrenzten Datenverkehr)	3 USD	15 USD	25 USD
Anzahl der zugreifbaren IP-Adressen	1	3	3
Dauer (in Tagen)	1	14	30

Private HTTP-Proxies

Diese privaten HTTP-Proxies bieten Käufern die Vorteile statischer IP-Adressen in einem bestimmten Land oder die Verbesserung der Leistung für E-Mail-Kampagnen.

	Elementary	Advanced	Professional	Unlimited	Unlimited-90
Preise	35 USD	50 USD	60 USD	95 USD	240 USD
Zeitraum	1 Monat			90 Tage	
Anzahl der zugreifbaren IP-Adressen	1	2	3	3	3
Anzahl der Threads pro Konto	100	200	400	Unbegrenzt	Unbegrenzt

HTTP/SOCKS-Proxies

Dazu gehören HTTP, HTTPS, SOCKS4 und SOCKS.

	Biweekly	Monthly/ Limited	Monthly/ Unlimited	Unlimited-90
Preise (E-Mail-Versand nicht zulässig)	65 USD	95 USD	195 USD	500 USD
Preise (E-Mail-Versand zulässig)	–	350 USD	550 USD	1.400 USD
Anzahl der zugreifbaren IP-Adressen	Jeder Kunde erhält Zugriff auf alle angebotenen Proxies (daher werden in den Blacklists so viele Proxies aufgeführt).			
Anzahl an Threads	350	350	Unbegrenzt	Unbegrenzt

Crimeware-Tools

Das bemerkenswerteste neue Produkt der vergangenen Monate ist ein Linux-Exploit-Paket, das über russische Untergrundkreise verfügbar ist und von getozz entwickelt wurde.

Name des Tools	Preise	Funktionen
LinuQ (im Juli erschienen)	200 USD (öffentliche Version) 1.500 USD (mit privatem Exploit)	Dieses Paket ist halb Bot, halb Exploit-Paket und wurde zur Kompromittierung von Linux-Servern entwickelt. In der öffentlichen Version werden vier PMA-Schwachstellen ausgenutzt: CVE-2009-1148 (unbestätigt) CVE-2009-1149 (unbestätigt) CVE-2009-1150 (unbestätigt) CVE-2009-1151 (bestätigt)
BlackHole Exploit Kit Version 1.2.0 (September)	Jahreslizenz: 1.500 USD Halbes Jahr: 1.000 USD 3 Monate: 700 USD	Die neue Version enthält die gleichen neun Exploits, wobei sechs aus dem Jahr 2010 stammen.
Bleeding Life Version 3 (August)	Neukunden: 1.000 USD Preisnachlass für Bestandskunden: 250 USD	Im Bericht für das erste Quartal führten wir Version 2 auf. Jetzt ist die teurere Version auf dem Markt, die zehn Exploits enthält.

Aktionen gegen Internetkriminelle

Ort	Beschreibung
Hongkong (August)	Die Polizei von Hongkong verhaftete einen 29-Jährigen, der für einen Internetangriff auf die Börsenwebseite der Stadt verantwortlich gemacht wird. Durch den Angriff am 10. August wurde der Handel mit Aktien von sieben Unternehmen unterbrochen, darunter das große Bankunternehmen HSBC. ²
Ukraine (August)	Der Sicherheitsdienst SBU der Ukraine verhaftete vier Personen, die der Erstellung gefälschter Zahlungskarten mithilfe gestohlener Informationen beschuldigt werden. Durch die Aktivitäten der Beklagten entstand Schaden in Höhe von 20 Millionen US-Dollar. ³

Hacktivismus

In diesem Quartal startete die Gruppe Anonymous viele Angriffe⁴, die ebenso zahlreich wie verwirrend waren, da die eigentlichen Ziele vielfach unklar blieben. So riefen einige zu verstärkten Protesten gegen PayPal auf, während andere im gleichen IRC-Kanal vorschlugen, PayPal-Konten zu eröffnen, um auf diese Weise Spenden erhalten zu können. Ebenso forderten einige den Angriff auf Facebook, während andere dort Seiten erstellten, um ihre Meinung und Aktivitäten bekannt zu geben. Höhepunkte dieses Quartals:

- 1. Juli: Arizona Fraternal Order of Police (Berufsverband der Polizisten von Arizona)
- 3. Juli: Demokratische Partei von Orange County (Kalifornien)
- 11. Juli: Booz Allen Hamilton (Unternehmensberatung)
- 12. Juli: Monsanto (Gentechnik-Unternehmen)
- 29. Juli: ManTech (IT-Unternehmen)
- 14. August: Bay Area Rapid Transit (Nahverkehrsbetreiber in Kalifornien)
- 19. August: Vanguard Defense Industries (Militärausrüster)
- 2. September: Texas Police Chiefs Association (Polizeiverband in Texas)
- 26. September: Österreichische Polizei
- 27. September: Goldman Sachs (Finanzunternehmen)

Wichtige Ereignisse

Am 28. Juli gaben südkoreanische Behörden bekannt, dass es chinesischen Hackern möglicherweise gelungen ist, die persönlichen Daten von 35 Millionen Nutzern des Portals Nate sowie der Blogging-Webseite Cyworld zu stehlen. Beide werden von SK Communications betrieben.

Die Nationale Polizeibehörde von Südkorea bezeichnete diesen Angriff als den schwerwiegendsten Hacker-Vorfall in der Geschichte des Landes und nannte eine chinesische IP-Adresse als Quelle des Angriffs.⁵ Es gelang den Hackern, die Namen, Personenkenn-Nummern, Geburtsdaten, das Geschlecht, E-Mail-Adressen, Telefonnummern, Wohnanschriften sowie Benutzernamen der 35 Millionen Kontoinhaber auszuspähen.

Nach dem am 15. März bekannt gewordenen Comodo-Zwischenfall und dem am 17. März gemeldeten RSA-Angriff hat der iranische Hacker, der sich zu diesen Angriffen bekannt hatte, seine Angriffe offensichtlich wieder aufgenommen. In diesem Quartal übernahm er die Verantwortung für den Einbruch bei der niederländischen Zertifizierungsstelle DigiNotar, der am 19. Juli entdeckt wurde.⁶ An diesem Tag hatte DigiNotar einen Einbruch in seine CA-Infrastruktur entdeckt, der zur missbräuchlichen Ausgabe von Public-Key-Zertifikatsanforderungen für zahlreiche Domänen wie Google.com, Yahoo!, Mozilla-Add-Ons sowie verschiedene Geheimdienste geführt hatte. Kurze Zeit später stellte das Unternehmen seinen Betrieb ein. (Die Übernahme einer Zertifizierungsstelle (oder auch nur die Nutzung gefälschter Zertifikate) erhöht die Erfolgswahrscheinlichkeit von Angriffen enorm. Stuxnet und Duqu nutzten diese Tatsache aus.)

Ein Hauch von Internetkrieg

Ort	Beschreibung
Ost-Turkistan (Juli)	Kurz vor dem zweiten Jahrestag der ethnischen Unruhen in Ost-Turkistan wurde die Webseite des Weltkongresses der Uiguren (World Uyghur Congress, WUC) erneut zum Ziel von Internetangriffen. Die Webmaster gaben an, dass die Angriffe ihren Ursprung wahrscheinlich in China haben. ⁷
Großbritannien (September)	Die russische Botschaft in London gab am 11. September bekannt, dass ihre Webseite nach einem mutmaßlichen Hacker-Angriff ausfiel. Dieser Zwischenfall ereignete sich kurz vor dem Besuch des britischen Premierministers David Cameron in Moskau. Dabei handelt es sich um den ersten Besuch eines britischen Staatsoberhauptes seit dem Mord an Alexander Litvinenko im Jahr 2006. Der Kreml-Kritiker und ehemalige russische Agent starb an einer Vergiftung mit radioaktivem Polonium-210. ⁸
Japan (September)	Mitsubishi Heavy Industries, ein großer japanischer Militärausrüster, stellte fest, dass Internetangreifer im August in seine Computernetzwerke eingedrungen waren. ⁹

Informationen zu den Autoren

Dieser Bericht wurde von Toralv Dirro, Paula Greve, David Marcus, François Paget, Craig Schmuagar, Jimmy Shah und Adam Wosotowsky von McAfee Labs vorbereitet und geschrieben.

Über McAfee Labs

McAfee 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 ist ein hundertprozentiges Tochterunternehmen der Intel Corporation (NASDAQ: INTC) und der weltweit größte auf IT-Sicherheit spezialisierte Anbieter. 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 ist stets auf der Suche nach neuen Möglichkeiten, seine Kunden zu schützen.

www.mcafee.com/de

1. <http://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/>
2. <http://www.physorg.com/news/2011-08-hong-kong-stock-exchange-hacking.html>
3. http://www.pcworld.com/businesscenter/article/238579/ukraine_arrests_four_in_carding_scam.html
4. Weitere Informationen zu diesem schwer fassbaren Phänomen finden Sie hier:
<https://blogs.mcafee.com/mcafee-labs/the-rise-and-fall-of-anonymous>
5. <http://www.reuters.com/article/2011/07/28/us-hackers-attack-idUSTRE76R19M20110728>
6. http://www.vasco.com/company/press_room/news_archive/2011/news_diginotar_reports_security_incident.aspx
7. <http://www.unpo.org/article/12841>
8. <http://uk.reuters.com/article/2011/09/11/uk-russia-britain-website-idUKTRE78A1IX20110911>
9. <http://www.pcadvisor.co.uk/news/security/3304711/cyberattackers-hit-japanese-defense-giant-with-trojan/>

