Bericht

McAfee Threat-Report: Zweites Quartal 2010

McAfee® Labs™

Es ist immer wieder interessant, Veränderungen bei Computerbedrohungen über einen längeren Zeitraum zu beobachten. Diese Ausgabe des *McAfee Threat-Report* befasst sich mit dem zweiten Quartal 2010 und kommt im Vergleich zu vorherigen Quartalen zu einigen sehr abweichenden Ergebnissen. Im vergangenen Quartal beobachteten wir eine Stagnation bei einigen Bedrohungsformen und zugleich das Aufkommen neuer Entwicklungen. In diesem Quartal setzten sich das ungebremst starke Wachstum bei Malware und ein etwas geringeres Wachstum bei Spam fort. In unserem Bericht zeigen wir einige sehr interessante und für uns völlig neue Zahlen zu regionalen Unterschieden bei Spam und Botnets. Immer mehr Bedrohungen passen sich an die besonderen Situationen ihrer Opfer – Unternehmen ebenso wie Privatanwendern – in den verschiedenen Teilen der Welt an.

In diesem Quartal unterschieden sich die weltweiten Malware-Zahlen erheblich von denen früherer Quartale. Von Januar bis März waren weltweit die gleichen Malware-Varianten vorherrschend. Dieses Phänomen war völlig neu. In diesem Quartal sind jedoch in den jeweiligen Regionen unterschiedliche Bedrohungen aktiv. In diesem Bericht untersuchen wir die Zunahme bei gefälschter Antiviren-Software, Kennwort stehlenden Trojanern, Social-Networking-Malware wie Koobface sowie bei Malware, die USB- und andere Wechselmedien missbraucht.

Wir beschreiben die Ausnutzung von Ereignissen und Schlüsselwörtern in Suchmaschinen sowie die Schwachstellen, die in diesem Quartal am häufigsten ausgenutzt wurden. Es ist wenig überraschend, dass Ereignisse wie die FIFA-Weltmeisterschaft in Südafrika und Ereignisse im Nahen Osten von Internetkriminellen und politischen Hacktivisten nach Kräften missbraucht wurden. Denken Sie immer daran: Die Gegenseite liest die gleichen Nachrichten wie wir. Wir berichten über Internet- und Netzwerkbedrohungen wie Phishing und das Wachstum bei böswilligen Webseiten und zeigen, welche Regionen der Welt am stärksten von SQL-Injektionsangriffen betroffen sind.

Der Bericht endet mit einer Quartalsübersicht der interessantesten Ereignisse bei Internetkriminalität und Hacktivismus. Wir hoffen, dass Sie diese Ausgabe des *McAfee Threat-Report* erhellend finden.

Inhaltsverzeichnis

Spam wie eh und je 4
Weltmeisterschafts-Fieber führt zu Infektionen 4
Haben Sie diesen Laptop gekauft? 5

Weltweite Spam-Trends 6

Keine Überraschungen: Malware zeigt stetiges Wachstum 9
Neue Zeiten für Mac-Benutzer? 11

Globale und regionale Entdeckungen 11
Autostart weiterhin auf Platz 1 11
Regionale Unterschiede bei Malware 11
Botnets erleben Comeback 13

Kontrolle der Suchmaschinen 13

Anzahl an Malware-Webseiten nimmt dramatisch zu 14

Viele Patches 16
SQL-Injektionsangriffe 17

Internetkriminalität 17
CallService geschlossen 17
Bandenkrieg 18

Hacktivismus 19

Informationen zu den Autoren 20

Über McAfee Labs™ 20

Informationen zu McAfee, Inc. 20

Spam wie eh und je

Das tägliche Spam-Volumen nahm in diesem Quartal im Vergleich zum ersten um lediglich 2,5 Prozent bzw. im Vergleich zum vierten Quartal 2009 um 7 Prozent zu. In diesem Zeitraum lag der Spam-Anteil am gesamten E-Mail-Verkehr im Internet bei 88 Prozent und damit nur leicht unter dem vorherigen Quartal (siehe Abbildung 1).

Insgesamt scheint sich Spam wieder in einem leichten Aufwärtstrend zu befinden, nachdem zwischen dem dritten und vierten Quartal 2009 ein Einbruch von 20 Prozent zu verzeichnen war. Im dritten Quartal 2009 wurde mit 175 Milliarden Spam-Nachrichten pro Tag das bislang höchste Spam-Aufkommen erfasst. Das aktuelle Aufkommen entspricht eher dem von Mitte 2008, kurz bevor der große Spam-Versender McColo im November 2008 vom Netz genommen wurde.

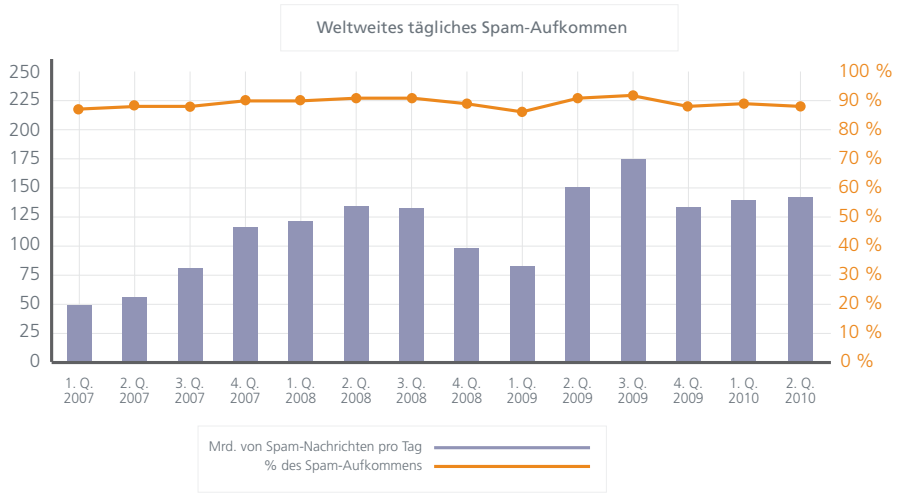


Abbildung 1: Globales Spam-Aufkommen (blaue Balken) und Spam als Anteil am gesamten E-Mail-Aufkommen (orange Linie). In diesem Quartal registrierte McAfee Labs durchschnittlich 142 Milliarden Spam-Nachrichten pro Tag.

Wie bisher auch stellen medikamenten- und gesundheitsorientierte Nachrichten mit Links zu Webseiten für „Kanadische Arzneimittel" auch weiterhin den größten Anteil der Spam-Nachrichten dar, die von infizierten Computern versendet werden. In diesem Quartal stellten gesundheitsbezogene Spam-E-Mails 63 Prozent aller Spam-Nachrichten dar und steigerten ihren Anteil damit sprunghaft, sodass sie nun vor Nachrichten mit generischen Angeboten liegen, die gerade einmal 10 Prozent aller Spam-Nachrichten ausmachten. Phishing-E-Mails, in diesem Quartal der dritthäufigste Spam-Typ, stellte nur 2 Prozent. Ihr Anteil am gesamten Spam-Aufkommen stieg jedoch im letzten Jahr um 81 Prozent.

Weltmeisterschafts-Fieber führt zu Infektionen

Während die Fußballweltmeisterschaft in Südafrika unter den Fußballfans für Erwartung und Anspannung sorgte, freuten sich Internetkriminelle auf ihre eigene Feier, die so gar nichts mit Begeisterung für Fußball zu tun hatte. Stattdessen suchten sie nach Möglichkeiten, das beliebteste Sportereignis der Welt für ihre Zwecke einzusetzen und PCs mithilfe von schädlichem Code zu übernehmen. Jedes große Ereignis – seien es Tragödien, Produktneuerscheinungen, Sport- oder andere beliebte Ereignisse – ziehen eine Vielzahl von Betrügereien und Suchmaschinenmanipulationen nach sich. Dennoch schien die weltweite Popularität dieser Weltmeisterschaft stärker als bisher Kriminelle anzuziehen.

Brasilianische Fußballfans – zu denen beinahe alle Einwohner Brasiliens zählen – erlebten einen Angriff, der den (mittlerweile zurückgetretenen) Trainer der Nationalmannschaft Dunga als Lockvogel ausnutzte. Die Benutzer wurden aufgefordert, für Fotos eines Streits zwischen Dunga und zwei wütenden Fans eine Schaltfläche anzuklicken. Bei dem Download handelte es sich um einen Kennwort stehlenden Trojaner mit dem Namen PWS-Banker.dldr, der weitere Malware nachlädt.

Als eine Methode zum Entlocken persönlicher Daten setzten Kriminelle auf Phishing-Betrug, der scheinbar mit den Veranstaltern der Weltmeisterschaft in Zusammenhang stand. Die betrügerische E-Mail enthielt ein offiziell aussehendes Logo und mehrere Erwähnungen der FIFA und der Weltmeisterschaft im Text. Dieser spezielle Phishing-Betrug unterschied sich deshalb von den bislang üblichen Vorgehensweisen, weil die Benutzer nicht sofort nach Kreditkartennummern und Prüfnummern sowie PINs gefragt wurden. Stattdessen wurde in der E-Mail nach Wohnort, Firmenname, E-Mail-Adresse und Mobilfunknummer gefragt. Obwohl es sich dabei auf den ersten Blick nicht um sensible Informationen handelt, können diese Daten in den falschen Händen zu Spam, weiteren Betrugsversuchen oder Malware auf mobilen Geräte führen – ganz zu schweigen von gezielten Phishing- oder böswilligen E-Mails in den Postfächern der Opfer.

Außerdem beobachteten wir einen sehr gezielten Angriff im Zusammenhang mit der Weltmeisterschaft, bei der eine PDF-Zero-Day-Schwachstelle ausgenutzt wurde. (Diese Vorgehensweise könnte sich mithilfe der Daten, die von den Opfern des vorherigen Betrugs geliefert wurden, jederzeit wiederholen.) Bei diesem Angriff wurde ein böswilliger Backdoor-Trojaner übertragen, der Computer in Spam- oder Malware sendende Zombies verwandelt. Die Opfer dieses Trojaners hatten meist keine Ahnung von der Kompromittierung, da die Ausnutzung im Hintergrund erfolgte, während die Benutzer Bilder sehr begeisterter Fans anzeigten.

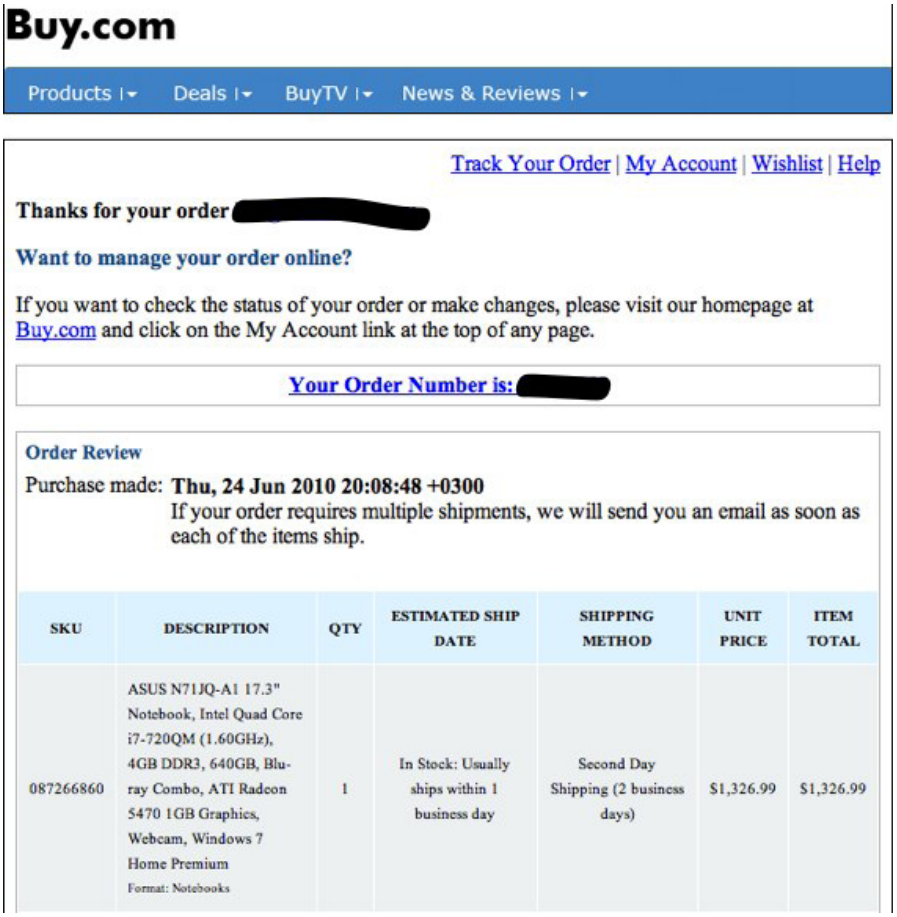
Angreifer können Suchmaschinenergebnisse manipulieren, um den Opfern gefälschte Links zu böswilligen Webseiten anzuzeigen. Angriffe im Zusammenhang mit der Weltmeisterschaft enthielten bekannte Begriffe wie „Bafana Bafana“ (der Spitzname des südafrikanischen Teams) und „best place to listen live World Cup“ (bester Ort zum Genießen der Weltmeisterschaft). Jedes Mal, wenn die Benutzer auf solche Ergebnisse klickten, gelangten sie auf Webseiten mit gefälschter Antiviren-Software.

Viele Angriffe werden mehrstufig ausgeführt. Beispielsweise kann eine E-Mail mit einem Link zu einer Phishing-Webseite die Opfer zuerst zu einer URL weiterleiten, die eine ungepatchte Schwachstelle auf ihrem Computer ausnutzt. Auf diese Weise wird der Computer des Opfers infiziert, noch bevor der eigentliche Betrug stattgefunden hat.

Haben Sie diesen Laptop gekauft?

Bei einem weiteren Betrugsversuch könnten in diesem Quartal einige IT- und Einkaufsmanager hinters Licht geführt worden sein. Ihre E-Mails enthielten scheinbare Kaufbestätigungen großer Versandwebseiten wie Amazon, eBay oder Buy.com. Während dieser Kampagne wurden zahlreiche Händler auf diese Weise missbraucht.

Dieser Betrug wurde besonders sorgfältig ausgeführt und wirkt auf den ersten Blick sehr echt – sofern das potenzielle Opfer nicht genau hinsieht. Die Links in den E-Mails führten entweder zu kompromittierten legalen Webseiten, die unwissentlich böswillige ausführbare Dateien hosteten, oder direkt zu böswilligen Webseiten.



Buy.com

Products | Deals | BuyTV | News & Reviews

Track Your Order | My Account | Wishlist | Help

Thanks for your order [redacted]

Want to manage your order online?

If you want to check the status of your order or make changes, please visit our homepage at Buy.com and click on the My Account link at the top of any page.

Your Order Number is: [redacted]

Order Review

Purchase made: **Thu, 24 Jun 2010 20:08:48 +0300**
If your order requires multiple shipments, we will send you an email as soon as each of the items ship.

SKU	DESCRIPTION	QTY	ESTIMATED SHIP DATE	SHIPPING METHOD	UNIT PRICE	ITEM TOTAL
087266860	ASUS N71JQ-A1 17.3" Notebook, Intel Quad Core i7-720QM (1.60GHz), 4GB DDR3, 640GB, Blu-ray Combo, ATI Radeon 5470 1GB Graphics, Webcam, Windows 7 Home Premium Format: Notebooks	1	In Stock: Usually ships within 1 business day	Second Day Shipping (2 business days)	$1,326.99	$1,326.99

Abbildung 2: Echt wirkende Kaufbestätigung, die Käufer zum Klicken auf böswillige Links bringen soll.

Weltweite Spam-Trends

McAfee besitzt zahlreiche Knoten auf der ganzen Welt, die Daten zum E-Mail-Verkehr sammeln, mit denen Spam-Trends untersucht werden. Durch die genaue Analyse dieser Daten werden die Ursprungsländer für bestimmte Spam-Typen ermittelt. Es ist zwar schwierig, diese Rohdaten aus unterschiedlichen Regionen der Welt genau zu vergleichen. Sie bieten jedoch eine gute Übersicht über die Arten von Spam-E-Mails, die häufig aus einem bestimmten Land versendet werden. Der Betreff von Spam bezieht sich häufig auf Themen, die für Menschen in diesen Ländern interessant sind.

In diesem Abschnitt finden Sie einige Kreisdiagramme, die die häufigsten Spam-Typen aus 34 Ländern zeigen. Die in den Diagrammen genannten Spam-Typen werden in Kategorien gegliedert und weiter erläutert. Diese Aufstellung ist nicht vollständig, sondern zeigt nur die häufigsten Spam-Typen auf.

Gemessen am Gesamtaufkommen machen die aufgeführten E-Mails zwischen 40 und 70 Prozent aller in der jeweiligen Region erfassten Daten aus. Persönliche Nachrichten, allgemeine Kommunikation und geringvolumige Spam-Kampagnen wurden in der Aufstellung nicht berücksichtigt. Die Ergebnisse sind repräsentativ, stellen jedoch keine vollständige Übersicht über die E-Mail-Typen dar, die aus den einzelnen Ländern stammen.

Wir entschieden uns für 20 allgemeine Kategorien zur Klassifizierung dieser Spam-E-Mails. Im Folgenden eine kurze Beschreibung:

Armbanduhren: Diese unverwechselbaren E-Mails sind die häufigste Form von Produkt-Spam.

Arzneimittel: Zu dieser Kategorie gehören Spam-E-Mails zu gefälschten kanadischen Arzneimitteln, die meist ihren Ursprung in China haben, sowie angebliche Mittel für Gewichtsreduzierung, usw.

Benachrichtigung über den Zustellstatus (Delivery Status Notification, DSN): Diese werden auch als NDRs (Non-Delivery Receipts) bzw. Non-Delivery Notifications (NDN) bezeichnet. Zwar können diese E-Mails legitim sein, meist handelt es sich jedoch um Spam, der von einer gefälschten Absenderadresse zurückgesendet wird.

Casinos: Diese E-Mails machen Werbung für Casinos. Sie werden häufig Botnet-Aktivitäten zugeordnet, und ihre Opfer müssen für die Teilnahme an diesen Spielen Software herunterladen und installieren.

Diplome und Abschlüsse: Hier wird auf Webseiten verwiesen, auf denen Kunden gefälschte Dokumente und Diplome kaufen können, die als „Nachweis" für den Abschluss an einer bestimmten Lehreinrichtung dienen sollen.

Drittanbieter: Diese E-Mails liegen zwischen Marketing und Produkt-Spam. Das Unternehmen an einem Ende der Spam-Kette ist legitim, und die Empfänger haben wahrscheinlich unbeabsichtigt zugestimmt, E-Mails von Werbepartnern zu erhalten.

Einsame Frauen: Häufig eine Form von Vertrauensbetrug. Die Kriminellen (wahrscheinlich Männer, die sich als Frauen ausgeben) versuchen, von ihren Opfern Geld für Flugtickets, Visa, Verpflegung, Reise- oder andere Kosten zu erhalten, das diese gern zahlen, um ihre „Angebetete" endlich in den Armen halten zu können.

Horoskope: Bietet Listen Ihrer persönlichen Horoskope an.

Jobs: Bei vielen dieser Scam-E-Mails handelt es sich um Formen von Nigeria- oder Vertrauensbetrug.

Kreditwürdigkeit: Die E-Mails versprechen Geld, Kredite oder versuchen, die Kreditwürdigkeit des Empfängers auszunutzen.

Malware: Hierzu werden alle E-Mails gezählt, die mit einem Virus oder Trojaner als Anlage versendet werden oder Sie zum Besuch einer infizierten Webseite auffordern.

Marketing: Hierzu zählt die Werbung für oder der Verkauf von Produkten an Empfänger, die ihre Zustimmung für den Empfang von E-Mails gegeben haben. Ein Beispiel dafür sind Fluglinien oder Reiseagenturen, die den Empfängern eine Angebotsliste zusenden. Bei diesen E-Mails handelt es sich um Erstanbieter-Werbung, d. h. die Empfänger wissen normalerweise, warum sie die E-Mail erhalten.

Nachrichten: Spam, bei dem echte Nachrichten legaler News-Webseiten missbraucht werden.

Newsletter: Eine Informations-E-Mail, für deren Empfang sich die Empfänger registrieren müssen. Bei Newslettern wird meist nicht direkt versucht, Produkte zu verkaufen. Stattdessen wird jedoch durch geschickte Wortwahl und reißerische Texte die Aufmerksamkeit der Empfänger erregt.

Nigeria-Scam: Dabei handelt es sich um einen Vorschussbetrug, bei dem versucht wird, die Opfer mit einer tragischen Geschichte oder dem Versprechen einer Belohnung zur Zahlung von Geld zu bewegen. Üblicherweise werden dabei auch offiziell aussehende Schriftstücke verwendet.

Phishing: Hierunter fallen alle E-Mails, die mit dem Ziel verschickt wurden, dem Opfer persönliche Informationen zu entlocken.

Produkte: Alle unerwünschten Spam-E-Mails, mit denen versucht wird, Produkte zu verkaufen. Meist handelt es sich dabei um Repliken von Handtaschen oder Schmuck.

Produkte für Erwachsene: Spam-E-Mails mit Werbung für Pornografie, meist Filme auf DVDs oder über Download-Webseiten.

Reisen: E-Mails, die zum Marketing legaler Reisebüros gehören.

Software: Hier wird versucht, OEM-Lizenzen (Großlizenzen für Comuputerhersteller und größere Unternehmen) als Einzellizenzen oder gehackte bzw. gecrackte Software-Versionen zu äußerst günstigen Konditionen zu verkaufen.

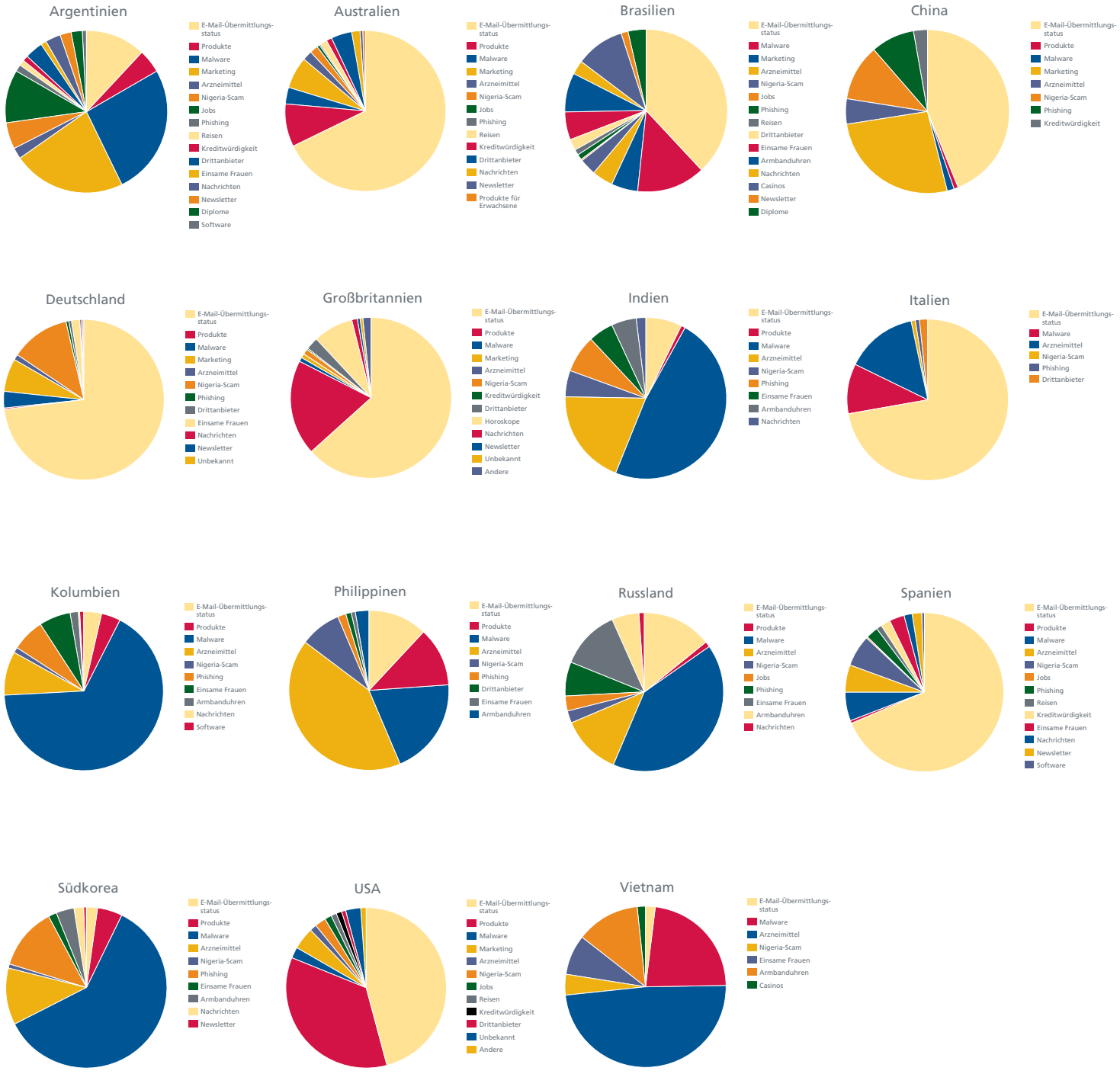


Abbildung 3: In den einzelnen Ländern werden bei Spam höchst unterschiedliche Themen angesprochen. In diesen Diagrammen werden unterschiedliche Anteile der häufigsten Themenbereiche in den jeweiligen Ländern gezeigt. Dabei erstreckt sich die Aufstellung jedoch nicht auf das gesamte Spam-Volumen, sondern nur auf die ersten Plätze.

Keine Überraschungen: Malware zeigt stetiges Wachstum

Die Malware-Landschaft in diesem Quartal unterscheidet sich von den vorherigen Quartalen. Beim letzten Mal verzeichneten wir eine Stabilisierung des gesamten Malware-Aufkommens und zum Teil sogar Rückgang bei einigen Malware-Typen.

Beim Gesamtaufkommen von Malware stellen wir nach dem langsamen Wachstum im ersten Quartal dieses Jahres im zweiten Quartal ein verstärktes Wachstum fest (siehe Abbildung 4). Malware-Entwickler sind wieder voll dabei. Wir haben in der ersten Hälfte dieses Jahres 10 Millionen neue Versionen katalogisiert! Im gleichen Zeitraum des vergangenen Jahres verzeichneten wir 9 Millionen Exemplare, sodass wir durchaus von einem starken Gesamtwachstum sprechen können. Damit sind die ersten sechs Monate des Jahres 2010 das aktivste Halbjahr bei Malware-Produktion überhaupt.

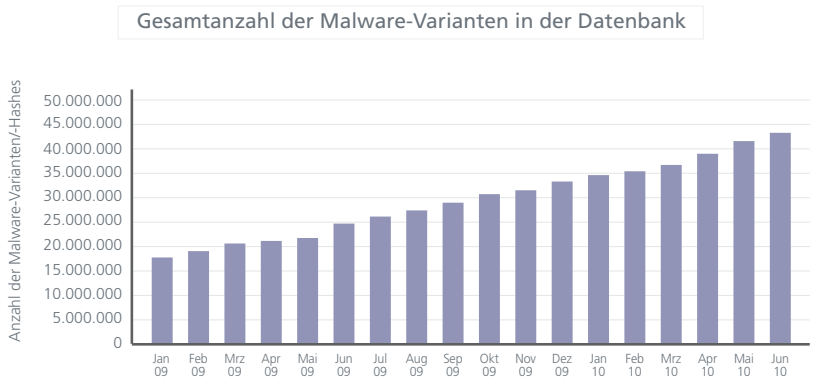


Abbildung 4: Die Gesamtzahl eindeutiger Malware-Exemplare (einschließlich Varianten) in der McAfee Labs-Datenbank.

In der Kategorie der unangenehmsten und häufigsten Malware-Typen in diesem Quartal stellten wir fest, dass Autostart-Angriffe (Malware, die sich über USB- und Wechseldatenträger verbreitet) im April und Mai einen Boom erlebten (siehe Abbildung 5). Derweil normalisierte sich das Wachstum bei gefälschten Antiviren-Programmen (Malware, die legale Software imitiert aber betrügerischen Charakter hat) etwas (siehe Abbildung 6).

Angesichts der riesigen Benutzerbasis von Facebook und ihrem fortgesetzten Wachstum als populärste Social-Networking-Webseite ist es kaum überraschend, dass Koobface (eine auf Facebook zugeschnittene Malware) auch weiterhin zu den häufigsten Bedrohungen gehört (siehe Abbildung 7). Zudem beobachten wir bei der häufigsten und wichtigsten Geldquelle für Internetkriminelle auf der ganzen Welt – Kennwort stehlenden Trojanern – eine unspektakuläre, aber stetige Zunahme bei der Verbreitung (siehe Abbildung 8).

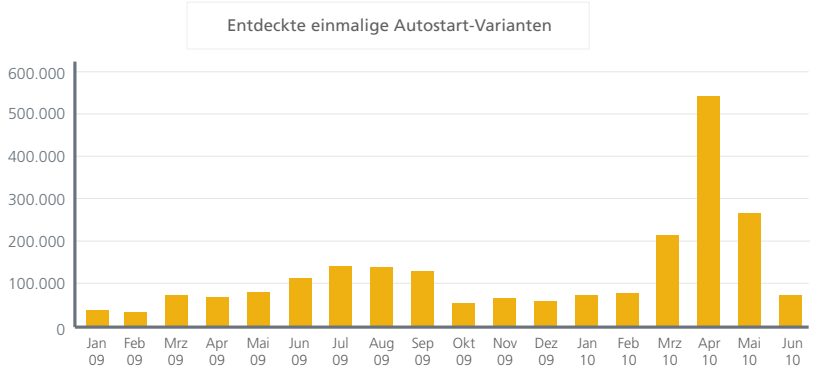


Abbildung 5: Autostart-Würmer zählten in diesem Quartal zu den aktivsten Malware-Kategorien. Sie erreichten im April Rekordzahlen und fielen dann in kurzer Zeit auf das übliche Niveau.

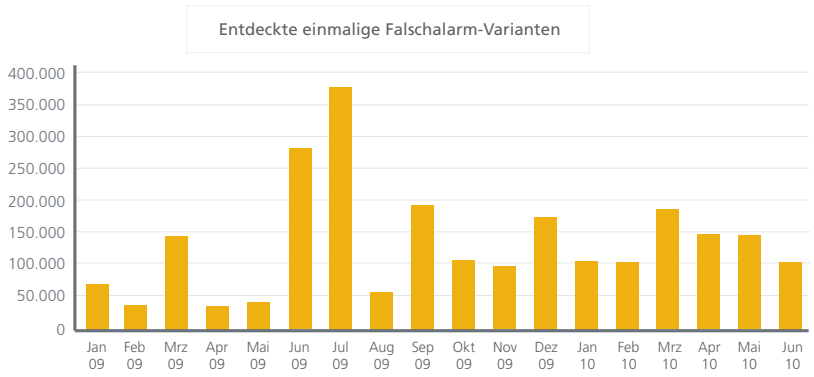


Abbildung 6: Im dritten Quartal 2009 gab es ein Rekordhoch bei neuen Varianten gefälschter Sicherheits-Software. Trotz eines Rückgangs ist diese lukrative Form der Internetkriminalität auch weiterhin stark verbreitet.

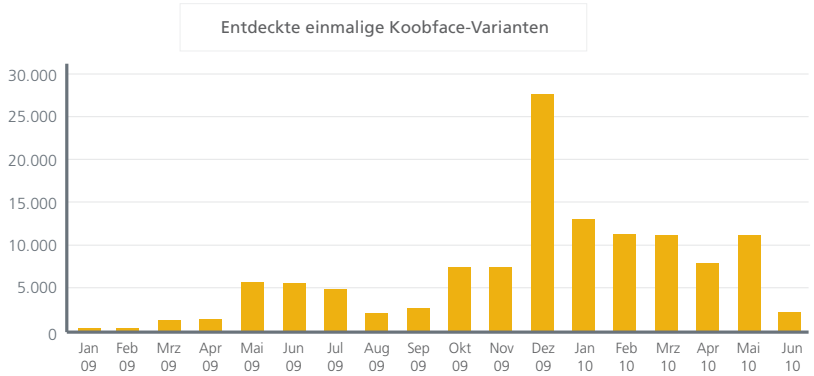


Abbildung 7: Die Anzahl neuer Koobface-Varianten ging nach einem Anstieg im Dezember drastisch zurück. Diese Malware plagt jedoch auch weiterhin die Facebook-Nutzer.

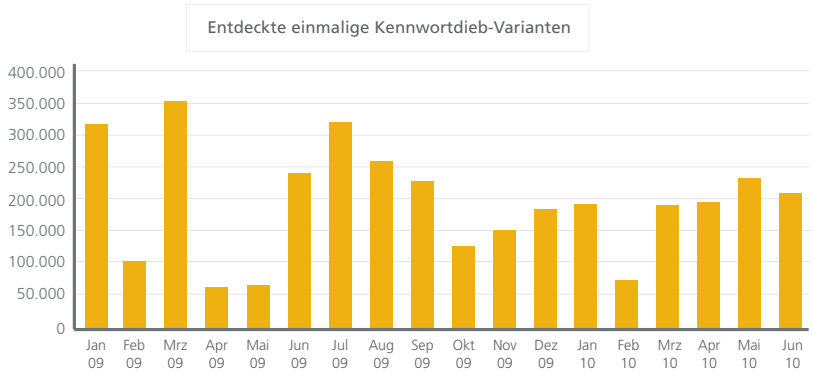


Abbildung 8: Kennwort stehlende Trojaner haben es hauptsächlich auf die Bankkontodaten der Opfer abgesehen.

Neue Zeiten für Mac-Benutzer?

Aus verschiedenen Gründen war Malware für Mac-Benutzer nur selten ein Problem. Diese Tage könnten jedoch schon bald vorbei sein. Im April entdeckte McAfee Labs den Mac-basierten Trojaner OSX/HellRTS, eine Fernzugriffs-Malware mit Client-, Server- und Server-Editor-Komponenten. OSX/HellRTS hat zahlreiche Funktionen, die auch Windows-Trojaner aufweisen:

- Prozessmanager (Auflisten und Beenden von Prozessen, die ausgeführt werden)
- Dateimanager (Auflisten, Hochladen, Herunterladen, Ausführen und Löschen von Dateien)
- Öffnen eines Chatfensters und Chat mit dem Opfer
- Streiche mit dem Opfer spielen (CD-Laufwerk öffnen/schließen, Videos und Audiodateien abspielen)
- Inhalt der Zwischenablage lesen oder ändern
- Benutzer abmelden, Computer neu starten oder herunterfahren

Wir möchten diese Gefahr keinesfalls überbewerten, da OSX/HellRTS bislang nur wenig Aktivität zeigte und McAfee-Produkte den Trojaner erkennen und davor schützen. Dennoch ist dies eine Erinnerung daran, dass im Zeitalter von Internetkriminalität, Datenkompromittierung und Identitätsdiebstahl kein Betriebssystem oder Gerät von Schutzmaßnahmen ausgenommen werden darf.

Globale und regionale Entdeckungen

Der Anstieg bei Malware-Beispielen, gegen die wir Schutz bieten, ist weiterhin stabil und auf relativ hohem Niveau: Täglich erscheinen ca. 55.000 neue Malware-Exemplare. Da es sich bei den meisten Exemplaren um statische und leicht abgewandelte Varianten bekannter Malware handelt, die lediglich mit verschiedenen Packprogrammen verschleiert wurden, können wir dank generischer Erkennungen die Größe der DAT-Dateien (Signaturen) gering halten. Dennoch ist die Menge an Malware immens.

Die meisten Bedrohungen sind nur kurze Zeit im Umlauf. Die Autoren erstellen die Malware, prüfen, ob Antiviren-Software sie erkennt, und verbreiten sie dann per E-Mail, Drive-by-Downloads oder indem sie Opfer dazu bringen, die Malware herunterzuladen und auszuführen. Am nächsten Tag wiederholen die Autoren diese Schritte, und die alte Malware verschwindet auf Nimmerwiedersehen. Die infizierten Computer bleiben jedoch infiziert. Für effektiven Schutz benötigen Privatanwender und Unternehmen Malware-Erkennung praktisch in Echtzeit. McAfee Artemis™ Technology bietet diesen Schutz.

Autostart weiterhin auf Platz 1

Der Trojaner Generic!atr ist immer noch die am häufigsten erkannte Malware und findet sich auf fast 9 Prozent aller Computer, die weltweit von McAfee gescannt wurden. (Wir erhalten diese Daten von den Nutzern unserer Produkte für Heimanwender, die einer Übermittlung der Erkennungsdaten zugestimmt haben. Informationen zu diesem Thema finden Sie unter http://home.mcafee.com/VirusInfo/RegionalVirusInformation.aspx.) Wir empfehlen Ihnen daher dringend, die Autostartfunktion nur dann zu aktivieren, wenn Sie sie wirklich benötigen.

Regionale Unterschiede bei Malware

Die häufigsten Erkennungen ähneln sich weltweit sehr stark. In den Top 10 gibt es jedoch einige interessante Unterschiede (siehe Abbildung 9). Die Top 5 werden angeführt von der Autostart-Malware Generic!atr, gefolgt von einem Kennworter stehlenden Trojaner, einer Autostartversion von Conficker, potenziell unerwünschten Programmen (PUPs) und einem Java-Applet-Trojaner. In Nordamerika ist FakeAlert, einer unserer Erkennungsnamen für gefälschte Virenschutzprodukte und Scareware, viel häufiger vertreten als im Rest der Welt. In Europa finden sich unter den Top 10 verschiedene generische PUP-Varianten. In den meisten Fällen handelt es sich dabei um gefälschte Virenschutzprodukte, jedoch nicht um die gleichen Varianten wie in Nordamerika.

Erkennungen weltweit Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic!atr	8,9
Generic.dx	5,8
W32/Conficker.worm!inf	4,3
Generic PUP.x	3,2
Downloader-BCS	3,0
GameVance	2,8
FakeAlert-FakeSpy!env.a	2,1
Adware-BDSearch	1,9
Adware-WinAd	1,8
FakeAlert-FakeSpy.a	1,7

Erkennungen in Nordamerika Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic!atr	8,0
Generic.dx	4,1
GameVance	4,0
Downloader-BCS	3,6
W32/Conficker.worm!inf	3,2
Generic PUP.x	3,0
FakeAlert-FakeSpy!env.a	3,0
FakeAlert-FakeSpy.a	2,4
Adware-WinAd	2,3
Adware-HotBar.b	1,7

Erkennungen in Südamerika Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic!atr	13,8
W32/Conficker.worm!inf	6,7
Generic.dx	5,8
W32/Autorun.worm.zf.gen	5,5
Downloader-BCS	5,4
Generic PWS.ak	3,0
W32/Conficker.worm.gen.a	2,6
Generic.dx!ssz	2,3
W32/Sality.gen	2,3
W32/Autorun.worm.ev	2,2

Erkennungen in Europa Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic!atr	9,7
Generic.dx	5,6
W32/Conficker.worm!inf	4,2
Generic PUP.x	3,7
Adware-Url.gen	2,9
Downloader-BCS	2,8
Generic PUP.x!dz	2,6
Generic PUP.x!dx	2,4
Adware-GameSpyArcade	2,3
Exploit-ByteVerify	2,1

Erkennungen in Afrika Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic!atr	19,6
Generic.dx	11,9
W32/Sality.gen	7,4
PatchedSFC	5,1
W32/YahLover.worm.gen	5,1
Spyware-AdaEbook	4,9
Generic PUP.x	4,1
W32/Autorun.worm.ev	4,1
W32/Mabezat	3,8
W32/Fujacks.remnants	3,2

Erkennungen in Asien Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic.dx	12,7
Generic!atr	10,8
W32/Conficker.worm!inf	8,5
Adware-BDSearch	6,8
Generic Dropper!cqt	5,6
WebThunder	4,8
Generic PUP.x	3,8
Generic Downloader.ac	3,8
Spyware-AdaEbook	3,7
W32/Autorun.worm.bx	3,6

Erkennungen in Australien Top 10 im Juni	Anteil bei gescannten Computern (in %)
Generic!atr	10,5
Generic.dx	3,3
W32/GetCodec	3,2
W32/Conficker.worm!inf	2,9
Generic.dx!tal	2,9
Generic PUP.x	2,5
Adware-GameSpyArcade	2,1
CasOnline	2,1
FakeAlert-FakeSpy.a	1,9
Adware-Url.gen	1,8

Abbildung 9: Top 10 bei Malware-Erkennungen – weltweit und nach Region

Klassische Viren sind immer noch im Umlauf und verursachen Probleme. In Südamerika und Afrika erreicht W32/Sality eine Platzierung in den Top 10, weltweit lediglich Platz 19 (1,1 Prozent aller Computer). Sality gehört zur Familie der polymorphen und sehr weit entwickelten Viren. Ein Ausbruch innerhalb eines Netzwerks hat zwangsläufig große Probleme zur Folge. Durch die derzeitige Vorherrschaft von Trojanern, Downloadern und Scareware wird die Bedrohung durch Viren schnell unterschätzt.

Botnets erleben Comeback

In diesem Quartal kehrten mit Storm Worm und Kraken zwei alte Bedrohungen zurück. Im April wurde eine neue Variante des Botnet-Trojaners Storm Worm beobachtet. Diese neue Variante basiert zwar auf dem ursprünglichen Trojaner, ihr fehlen jedoch einige Funktionen, insbesondere die Peer-to-Peer-Funktion, die die Bekämpfung von Storm Worm so schwer gemacht hatte. Nach anfänglicher Aufregung legte sich dieser Sturm recht schnell. In den letzten Juni-Tagen schien ein weiteres Botnet von den Toten wiederzukehren. Kraken galt zu seinen Spitzenzeiten im Jahr 2008 als eines der weltweit größten Botnets und war für sehr viel Spam verantwortlich. Die ursprüngliche Variante wurde 2009 deaktiviert. Doch jetzt ist ein neues Botnet auf dem Vormarsch. Es bleibt abzuwarten, ob diese Version die gleichen Ausmaße wie sein Vorgänger erreichen wird. In diesem Fall werden wir im nächsten *McAfee Threat-Report* sicher mehr darüber berichten.

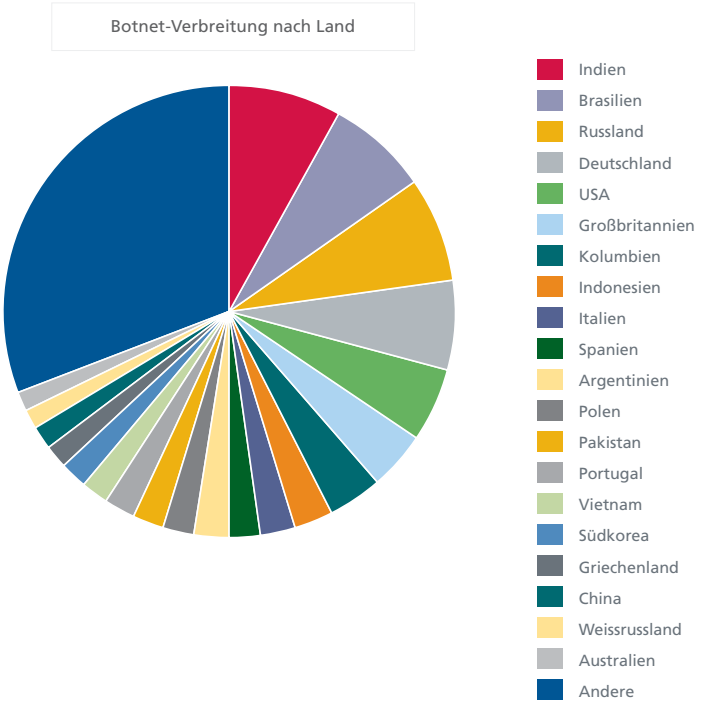


Abbildung 10: McAfee Labs erkannte in Indien mit fast 1,5 Millionen Erkennungen mehr Botnet-Infektionen als in irgendeinem anderen Land. In Brasilien, Russland und Deutschland gab es ebenfalls mehr als eine Million Infektionen.

Kontrolle der Suchmaschinen

Kriminelle greifen die breite Masse der Computernutzer weiterhin gezielt mithilfe besonders beliebter Suchbegriffe an. Sie überwachen regelmäßig Google Trends-Daten, um Ziele zu identifizieren. Dabei weben sie ein Netz aus speziell erstellten Webseiten mit Querverweisen und hacken Webseiten mit Schwachstellen, um diese zum Starten ihrer böswilligen Aktivitäten auszunutzen.

Abbildung 11: Top 50 der in diesem Quartal am häufigsten missbrauchten Suchbegriffe

In diesem Quartal gehörten die Namen bekannter Persönlichkeiten zu den am häufigsten missbrauchten Suchbegriffen (siehe Abbildung 11). Die Frage „Wie alt ist Prince?" führte mit der größten Wahrscheinlichkeit zu böswilligen Ergebnissen. Wenn Sie auf eines der Ergebnisse klicken, landen Sie wahrscheinlich auf einer gefälschten YouTube-Seite, auf der Sie aufgefordert werden, eine Datei mit einem Namen wie „download.exe" oder „install.#####.exe" herunterzuladen. Bei diesen Dateien handelt es sich um Downloader-Trojaner, die gefälschte Software installieren.

Die Suche nach „ynn news rochester", „valmeticulous", „val meticulous", „justine musk" oder 52 anderen Top-Begriffen kann zu der gleichen gefälschte Webseite führen.

Das Seltsame daran ist, dass es sich bei den Begriffen *valmeticulous* und *val.meticulous* um erfundene Begriffe zu handeln scheint. Bereits in der Vergangenheit fanden sich ungewöhnliche Wörter oder Phrasen unter den am häufigsten missbrauchten Begriffen. In diesem Fall stellten Beobachter von Google Trends diese ungewöhnliche Tatsache fest. Mindestens eine Person ging sogar so weit, ein Profil einer fiktiven Val zu erfinden. Es ist nicht genau bekannt, warum und wie solche Begriffe in die Listen gelangen. Möglicherweise handelt es sich um eine Art Google-Tracer, der in die Reihe der Suchbegriffe eingeschleust wurde, um Suchergebnismanipulierer zu entlarven.

Wir waren überrascht, das Öl-Leck von BP im Golf von Mexiko nicht unter den täglichen Top-20-Suchbegriffen dieses Quartals zu finden.

Anzahl an Malware-Webseiten nimmt dramatisch zu

Im letzten Quartal berichteten wir vom hohen Anteil böswilliger URLs, die in den USA gehostet wurden. Möglicherweise verursachte diese Information etwas Verwirrung darüber, dass wir und andere häufig über Webrisiken auf Domänenebene berichten, obwohl der Blick auf die Domänen allein nicht mehr zum Verständnis dieser Bedrohungen genügt. Es gibt durchaus böswillige Server und Domänen, wir entdecken jedoch immer öfter URLs, die auf legitimen Domänen gehostet werden und lediglich auf Pfadebene böswillig sind. Dazu gehören beispielsweise Malware, die in JPG-Dateien auf Wikipedia oder Bildern in Facebook-Profilen enthalten sind, gefährliche Downloads, die über Webseiten zum Medienaustausch oder für persönlichen Netzwerkspeicher veröffentlicht werden, sowie böswillige Inhalte in Foren oder Diskussionsplattformen. Die Liste kann endlos weitergeführt werden. Im Jahr 2009 waren 6 Prozent der von McAfee identifizierten böswilligen URLs auf Pfadebene schädlich. Im Jahr 2010 stieg deren Anteil bereits auf 16 Prozent. Da Registrare versuchen, ihre Domänen sicher zu halten, wird sich dieser Trend voraussichtlich fortsetzen.

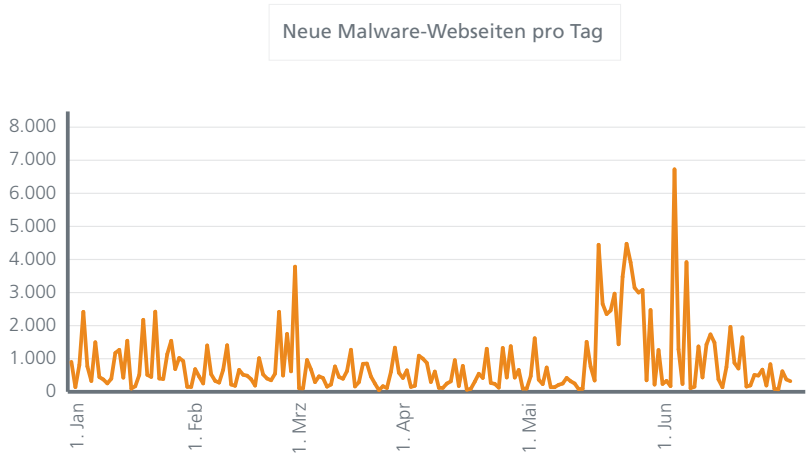


Abbildung 12: McAfee Labs-Sensoren entdecken täglich hunderte bis tausende neuer Webseiten, die Malware hosten. Zeus und andere Botnet-Aktivitäten sorgten Ende Mai und Anfang Juni für die Spitzenwerte.

Abbildung 12 zeigt den Trend bei böswilligen Webseiten im Verlauf der ersten Jahreshälfte. Diese Webseiten verbreiten Malware, werden für Exploits verwendet, aktualisieren und koordinieren Botnets, fungieren als Proxy für böswilligen Datenverkehr oder werden für andere böswillige Zwecke genutzt. Im Zeitraum vom 13. Mai bis 4. Juni stellten wir einen erheblichen Anstieg fest. Unsere Untersuchungen ergaben, dass die Ursache vor allem in verschiedenen gezielten Angriffen und gesteigerten Aktivitäten von Zeus und anderen Botnets zu finden war. Das Diagramm zu neuen Phishing-Webseiten zeigt ein ähnliches Muster – jedoch ohne Rückgang der Zahlen (siehe Abbildung 13).

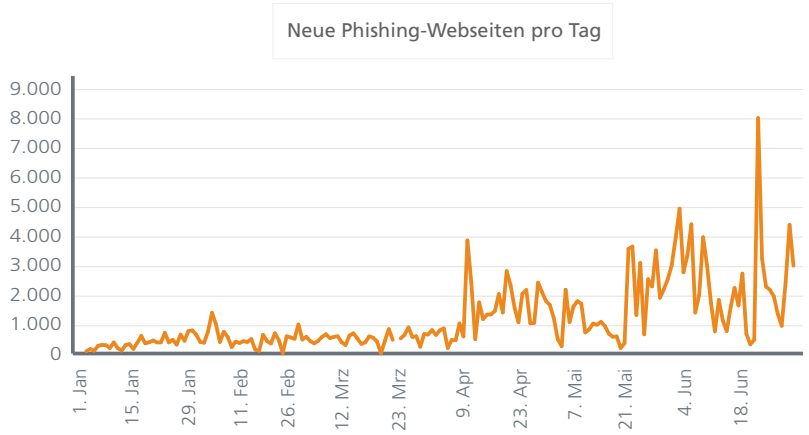


Abbildung 13: Von McAfee Labs erfasste neue Phishing-Webseiten folgen im Großen und Ganzen dem gleichen Trend wie neue Malware-Webseiten.

Eine Analyse der neuen Phishing-Webseiten ergab ähnliche Spitzenwerte wie bei Malware-Webseiten, wobei das Wachstum der Phishing-Webseiten etwas hinter den Malware-Webseiten hinterherhinkte. Viele Phishing-Webseiten wurden scheinbar mit einem Toolkit erstellt, das dem Toolkit zur Erstellung von Malware-Webseiten sehr ähnlich ist. Zudem folgt es Standardmustern. Angreifer nahmen in der letzten Phase erhöhten Aufkommens zahlreiche Marken und Kunden ins Visier. Zu den größten Zielen gehörten PayPal, Bank of America sowie Halifax Bank Großbritannien. Jedoch gehörten nicht nur Banken zu den Opfern, sondern auch Messenger- und E-Mail-Anbieter sowie Anbieter von Spielen, Pornographie-Abonnements, Benzinkarten, Online-Shopping sowie Luftfahrt- und andere Reiseplandienste. Außerdem sind auch Plattformen für Social Networking und Online-Interaktionen betroffen.

Zu den größten Nachrichten Anfang Juni gehörte ein massiver SQL-Injektionsangriff. Ein „Splitterangriff" auf zehntausende Webseiten fügte einen Iframe ein, der Benutzer auf eine böswillige Seite weiterleitete, über die eine Datei heruntergeladen und anschließend ausgeführt wurde. Solche Angriffe treten regelmäßig auf – mindestens einmal im Quartal. Sobald die böswillige Domäne deaktiviert wurde, geraten die Meldungen und die Beunruhigung über den jeweiligen Angriff schnell in den Hintergrund. Wir erfahren jedoch nicht, wie viele Webseiten nach einem solchen Angriff nicht richtig bereinigt werden. Ein Monat nach dem Juni-Angriff mit dem Namen ww.robint.us zählten wir 51.900 Webseiten, die noch mit dieser SQL-Injektion infiziert waren. Dies ist kein Sonderfall. Der Angriff 2677.in leitet Benutzer weiterhin auf 26.800 Webseiten weiter, yahoosite.ru betrifft noch 1.380 Webseiten, das killpp.cn-Exploit aus dem Jahr 2008 lässt sich noch auf 680 Webseiten nachweisen und die k.18xn.com-Infektion ist immer noch auf 538 Webseiten präsent. Diese Probleme werden sich wahrscheinlich weiter verschärfen, da das Internet durch seine Dynamik und seinen ständigen Wandel Injektionen und das Verbergen von Angriffen erleichtert.

In den Medien wurde außerdem darüber berichtet, dass böswillige Webangriffe und Bedrohungen zunehmend von Freitag bis Sonntag erfolgen. McAfee Labs kann diesen Trend bisher nicht bestätigen. An Freitagen kommen tatsächlich die meisten neuen Bedrohungen in Umlauf. Dieser Trend ist jedoch nicht neu. Stattdessen nahm die Anzahl der böswilligen Webseiten – unabhängig vom Wochentag ihres Erscheinens – erheblich zu.

Viele Patches

Die vergangenen drei Monate stellten das bisher aktivste „Patch-Quartal" dar. Microsoft und Adobe, die beiden größten Software-Anbieter, sendeten umfangreiche Aktualisierungen. Adobe behob 87 Fehler, die in der Common Vulnerabilities and Exposures-Datenbank verzeichnet waren. Microsoft veröffentlichte Patches für 61 weitere CVEs. Außerdem veröffentlichte Microsoft sieben Sicherheitshinweise. Sechs dieser Hinweise wurden als Reaktion auf die öffentliche Bekanntmachungen von Problemen in Windows und anderen Anwendungen herausgegeben.

Im Folgenden finden Sie eine Zusammenfassung einiger der bemerkenswertesten Schwachstellen, die McAfee Labs in diesem Quartal analysierte:

- *Windows Help and Support Center (Windows Hilfe- und Supportcenter) – CVE-2010-1885:* Diese Schwachstelle betrifft Windows XP und Windows 2003. Zur Ausnutzung dieser Schwachstelle auf ungepatchten Systemen ist Interaktion seitens des Benutzers erforderlich. Der Autor veröffentlichte Proof-of-Concept-Code, was das Risiko dieses Problems erhöht. Für diese Schwachstelle stand bis zum Verfassen dieses Berichts noch kein Patch zur Verfügung. McAfee Labs fordert alle Windows-Nutzer eindringlich auf, ihre Sicherheits-Software auf dieses Problem hin zu aktualisieren und strenge Kontrollen innerhalb des Netzwerks einzuführen, um die böswillige Verwendung des HCP-Handlers zu blockieren, bis ein Hersteller-Patch bereitgestellt wird.
- *Adobe Flash Memory Corruption Vulnerability (Schwachstelle in Adobe Flash aufgrund eines Speicherfehlers) – CVE-2010-1297:* Am 4. Juni gab Adobe bekannt, dass eine schwerwiegende Schwachstelle in Adobe Flash ausgenutzt werden und zu Remotecodeausführung führen kann. Adobe veröffentlichte am 10. Juni einen Patch, der dieses Problem behob.[1] McAfee Labs ist Malware bekannt, die diesen Fehler aktiv ausnutzt.
- *PDF /Launch Attack (PDF-Startangriff) – CVE-2010-1240:* Am 29. März zeigte ein Sicherheitsforscher, wie Code ausgeführt werden kann, indem er in eine PDF-Datei eingebettet über Social Engineering gestartet wird. Diese Angriffsmethode betrifft einige Versionen der PDF-Betrachter Adobe Acrobat, Adobe Reader und Foxit und wird vielfach diskutiert. McAfee Labs kennt aktive Ausnutzungen dieses Problems. Der Angriff auf Foxit war noch etwas schwerwiegender, da keine Warnung angezeigt wurde, die Anwender auf das verdächtige Verhalten hingewiesen hätte. Sowohl Adobe[2] als auch Foxit[3] haben Patches veröffentlicht.
- *Oracle Java Toolkit Insufficient Validation of Parameters (Unzureichende Parameter-Validierung im Oracle Java-Toolkit) – CVE-2010-0887:* Im April veröffentlichte ein Sicherheitsforscher zusammen mit Proof-of-Concept-Code Details zu einem Exploit, der eine Schwachstelle im Plug-In für die Java Virtual Machine in Java 6 Update 10 ausnutzte. Durch diesen Fehler können beliebige Parameter übergeben werden, die zu Codeausführung führen. Oracle hat eine Sicherheitswarnung zu diesem Problem veröffentlicht.

1. Adobe Systems. http://www.adobe.com/support/security/bulletins/apsb10-14.html
2. Adobe Systems. http://www.adobe.com/support/security/bulletins/apsb10-15.html
3. Foxit. http://www.foxitsoftware.com/pdf/reader/security_bulletins.php

SQL-Injektionsangriffe

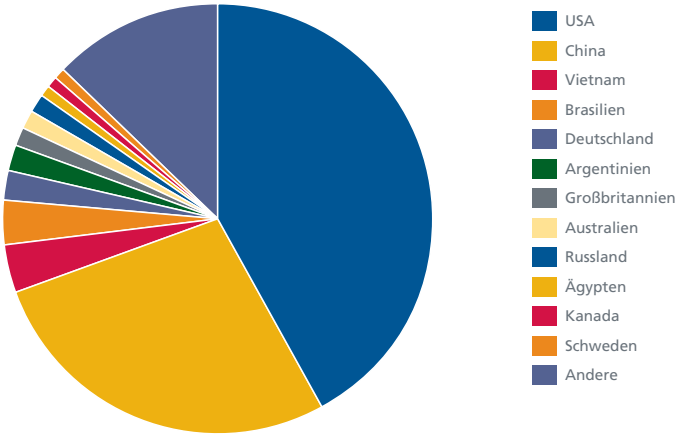


Abbildung 14: McAfee Labs-Sensoren registrierten zahlreichen Angriffsversuche von Clients auf Server mithilfe von SQL-Injektion. Die Quellen dieser Angriffe lagen vor allem in den USA und in China.

Internetkriminalität

Im April gab die rumänische Polizei die Verhaftung von 70 Mitgliedern dreier voneinander unabhängiger Gruppen organisierter Internetkrimineller bekannt. Laut Anklage hatten diese Gruppen seit 2006 Bürger in Spanien, Italien, Frankreich, Neuseeland, Dänemark, Schweden, Deutschland, Österreich, den USA, Kanada und der Schweiz bei Online-Auktionsbetrug finanziell geschädigt. Die internationalen Behörden ermittelten mehr als 800 Opfer, die insgesamt um mehr als 800.000 EUR betrogen wurden.[4]

Den Kriminellen wird vorgeworfen, fiktive Elektronikartikel, Luxusautos, Jachten, Villen und sogar Flugzeuge verkauft zu haben. Zu den „verkauften" Produkten gehörten Pkws der Marken BMW X5, Lexus und Infiniti. Zudem verkauften sie einem reichen Amerikaner ein Privatflugzeug für 67.000 EUR.[5]

CallService geschlossen

Später im April gab das FBI bekannt, dass gegen Dmitri M. Naskowets, den weißrussischen Gründer und Betreiber von CallService.biz, Anklage erhoben wird.[6] Diese Webseite soll Identitätsdiebe bei der Ausnutzung gestohlener Finanzdaten wie Kreditkartennummern unterstützt haben.

Um ihre nur Russisch sprechenden Kunden zu unterstützen, boten Naskowets und sein Komplizen an, die betrügerischen Transaktionen auf Deutsch und Englisch durchzuführen.

Die Manager von CallService.biz warben für ihre Dienste auf anderen Webseiten, die von Identitätsdieben frequentiert wurden. Dazu gehörte die Webseite CardingWorld.cc, die von Sergej Semashko, einem in der Anklageschrift genannten Mitwisser, betrieben wurde. In der Werbung wurde behauptet, dass sie mit „mehr als 2.090 Personen zusammenarbeiten" würden und bereits „mehr als 5.400 Bestätigungsanrufe" an Banken getätigt hätten.

Naskowets wurde am 15. April von den tschechischen Strafverfolgungsbehörden nach einer Anfrage aus den USA und auf Grundlage bilateraler Verträge zwischen beiden Ländern verhaftet. Am gleichen Tag fand eine gemeinsame Operation ihren Abschluss: Während Semashko in Weißrussland von weißrussischen Strafverfolgungsbehörden verhaftet wurde, beschlagnahmten litauische Behörden die Computer, auf denen die Webseiten von CallService und CardingWorld.cc gehostet waren.

4. DIICOT. http://www.diicot.ro/index.php?option=com_content&view=article&id=298
5. Gandul. http://www.gandul.info/news/ce-vand-infractorii-romani-pe-internet-avioane-de-agrement-si-masini-de-lux-5825091
6. FBI (Federal Bureau of Investigation), New York. http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo041910b.htm

Bandenkrieg

Carder.cc ist ein deutsches Online-Forum für Kriminelle, die mit gestohlenen Kreditkarten- und Anmeldedaten handeln, die sie im Rahmen von Carding- oder Phishing-Aktivitäten erbeutet haben. Solche Foren sind die Haupteinnahmequelle für ihre Administratoren (die sich an diesem Schwarzmarkt beteiligen), so dass sich die bekanntesten Untergrund-Plattformen im permanenten Kampf um die Vorherrschaft befinden. Wenn ein Wettbewerber beweisen kann, dass ein Konkurrenzforum unsicher ist, steigt sein Marktanteil.

Daher hackten sich einige in das Carder.cc-Forum und veröffentlichten die Ergebnisse – einschließlich der Daten tausender Forumsmitglieder, häufig einschließlich der zugehörigen Kennwörter. Von besonderem Interesse ist ein RAR-Archiv mit einem Auszug des Forums und einem Tool zu dessen Wiederherstellung. Diese Datei enthält Daten zu den vier Administratoren, deren E-Mails und ihrem Beitrittszeitpunkt zur Gruppe. Zu diesen Daten gehören auch die (tatsächlichen oder anonymen) IP-Adressen, die bei der Anmeldung im Forum verwendet wurde, sowie die Aufgabenbereiche der Administratoren.

Zusätzlich zu den Administratordaten enthält diese Datei folgende Informationen:

- 4.121 einfache Mitglieder
- 5 globale Moderatoren
- 258 Mitglieder der Ebene 2
- 7 Mitglieder der Ebene 3
- 4 Moderatoren
- 17 bestätigte Anbieter
- 497 gebannte Mitglieder

Die Datei enthält Informationen zum Alter, zur Nationalität sowie weitere persönliche Daten. Wir können jedoch nicht mit Sicherheit sagen, dass diese Daten korrekt sind. Weiterhin werden Webseiten und Kontaktinformationen für ICQ, AOL Messenger, Yahoo Messenger und MSN genannt.

Abbildung 15: Veröffentlichte Daten einiger Carder.cc-Forumsmitglieder.

Das Beispiel Carder.cc beweist, dass der Markt für Identitätsdiebstahl boomt. Dies wird durch die Anzahl der kostenlosen Zahlungskonten deutlich, die zur Gewinnung neuer Kunden angeboten werden und die volle Identität der Opfer preisgeben.

Hacktivismus

Der kürzlich erfolgte israelische Angriff auf die Gaza-Flotte führte zu Aktionen unterschiedlicher politischer Hacktivisten-Gruppen. Einige als Türken auftretende Hacker verunstalteten israelische Webseiten wie die der Stadtverwaltung von Tel Aviv. Wir registrierten mehrfach Protestnachrichten mit einem Video des Nachrichtendiensts Al Jazeera, das an Bord der Flotte aufgenommen wurde.

Türkische Hacker verunstalteten auch mehrere Facebook-Konten israelischer Bürger.[7] Dabei wurde in einigen Fällen das tatsächliche Profil durch die gleiche Botschaft ersetzt, bevor der Protest an eine Gruppe gesendet wurde (siehe Abbildung 16).

Abbildung 16: Türkische Hacktivisten verunstalteten Webseiten und Facebook-Konten, um gegen Israels Angriff auf die Gaza-Flotte zu protestieren.

Israelische Hacker konterten, indem sie unter anderem die Webseite der türkischen Hilfsorganisation IHH unterwanderten, die auch das Schiff Mavi Marmara der Gaza-Flotte sponsorten.[8] Die Hacker tauschten das große Foto der Marmara durch das Bild eines israelischen Kampfflugzeugs mit der Unterschrift „Yes, we can" (Doch, wir können) aus.

Der Fall von Gilad Shalit, einem israelischen Soldaten, der im Juni 2006 gefangen genommen wurde und noch immer von militanten Hamas-Mitgliedern gefangen gehalten wird, schlug auch im Internet Wellen. Im April veröffentlichte die Hamas ein animiertes Comic mit Noam Shalit, dem Vater des Soldaten.[9] Als Reaktion verunstalteten israelische Hacker die arabischen, englischen und französischen Webseiten der libanesischen Nachrichtenagentur NNA.[10]

Abbildung 17: Der Gaza-Konflikt inspirierte politische Comics und führte zu verunstalteten Webseiten.

7. „Turkish Hackers Defacing Israeli Facebook Accounts" (Türkische Hacker verunstalten israelische Facebook-Konten), Dark Reading. http://www.darkreading.com/blog/archives/2010/06/facebook_accoun.html
8. „Israeli hacker hits IHH terrorist website: 'The real war today is online'" (Israelischer Hacker trifft IHH-Terroristenwebseite: Der echte Krieg wird heute online geführt). JIDF. http://www.thejidf.org/2010/06/israeli-hacker-hits-ihh-terrorist.html
9. „Hamas Release Animated Gilad Shalit Cartoon" (Hamas veröffentlichen animiertes Comic mit Gilad Shalit), Sabbah Report. http://sabbah.biz/mt/archives/2010/04/26/hamas-release-animated-gilad-schalit-cartoon-video/
10. „Lebanon news agency: Website hacked by Israel to post Ron Arad message" (Libanesische Nachrichtenagentur: Webseite von Isreal zur Veröffentlichung von Ron Arad-Meldung gehackt). http://www.haaretz.com/news/diplomacy-defense/lebanon-news-agency-website-hacked-by-israel-to-post-ron-arad-message-1.285018

Informationen zu den Autoren

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

Über McAfee Labs™

McAfee Labs ist das globale Forschungsteam von McAfee, Inc. Hierbei handelt es sich um die einzige Forschungsorganisation, die sich mit allen Bedrohungsbereichen befasst: Malware, Internet, E-Mails, Netzwerk und Schwachstellen. McAfee Labs erfasst Daten mithilfe von Millionen Sensoren und cloudbasierter Bewertungstechnologien wie McAfee Artemis™ Technology und McAfee TrustedSource™. 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, Inc.

McAfee (NYSE: MFE) ist der weltweit größte dedizierte Spezialist für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze 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 einer preisgekrönten Forschungsabteilung, 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. Weitere Informationen über McAfee finden Sie unter www.mcafee.com/de.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

10104rpt_quarterly-threat-q2_0710_fnl_ETMG