Bericht

McAfee Threat-Report: Erstes Quartal 2009

Von McAfee® Avert® Labs

Inhaltsverzeichnis

Der *McAfee Threat-Report* enthält aktuelle Statistiken und Analysen zu Gefahren aus dem Internet. Dieser vierteljährlich erscheinende Bericht wird von den Forschern der McAfee Avert Labs zusammengestellt, deren weltweit tätige Mitarbeiter einen einzigartigen Überblick über die Bedrohungslandschaft für Verbraucher und Unternehmen in den USA und in anderen Ländern der Welt bieten. Werfen wir gemeinsam einen Blick auf die wichtigsten Sicherheitsprobleme der vergangenen drei Monate. Nach der Lektüre dieses Textes können Sie weitere Informationen im McAfee Threat Center unter http://www.mcafee.com/us/threat_center/default.asp oder unter www.trustedsource.org erhalten.

Im ersten Quartal des Jahres 2009 haben wir, verglichen mit der Situation vor einem Jahr oder auch noch vor wenigen Monaten, erhebliche Veränderungen in der Bedrohungslandschaft wahrgenommen. Vor 12 Monaten hätte niemand vorhergesehen, dass der Umfang von Spam-E-Mails zurückgeht, aber nachdem das Unternehmen McColo im November 2008 aus dem Netz genommen wurde, ist genau das eingetreten. Noch immer liegt der Umfang an Spam-E-Mails 30 Prozent unter den bisherigen Spitzenwerten, und auch der normalerweise im Monat März festgestellte Anstieg blieb bislang aus. Aber die Frage lautet nicht, *ob* sich die vorherigen Spam-Levels wieder einstellen werden, sondern vielmehr *wann* genau das geschieht. Aktuelle Daten zu neuen Zombies und Botnets legen die Vermutung nahe, dass dieser Zeitpunkt in nicht allzu weiter Ferne liegt.

Die Kreation gefährlicher Webseiten nimmt ständig zu. Und auch zu Malware hostenden Webseiten kommen täglich Tausende hinzu. Jeden Tag werden neue Formen von Malware entwickelt. Dieser Bericht zeigt die Bedrohungen mit der höchsten Häufigkeit und Verbreitung auf.

Der offiziell mit „W32/Conficker.worm“ bezeichnete Conficker-Wurm hat genauso viel Aufmerksamkeit auf sich gezogen wie andere Sicherheitsbedrohungen in der jüngsten Vergangenheit auch. Dieser Bericht beleuchtet, ob dies nur Hysterie ist oder eine realistische Grundlage hat. Außerdem werden wir uns Bedrohungen ansehen, die in den Medien weniger stark in Erscheinung treten aber dennoch gefährlicher sein könnten, als bekanntere Vertreter ihrer Art.

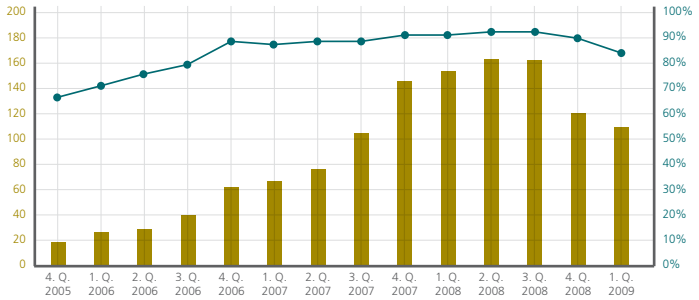
Die Geografie der Bedrohungslandschaft entwickelt sich weiter. Dieser Bericht bietet eine Analyse der geografischen Bedrohungsentwicklung, einschließlich der Herkunft von Spam-E-Mails, der Erstellung von Zombies und der Standorte von Malware-Webseiten. Außerdem werden die aufstrebenden Global Player des Bedrohungsgeschäfts benannt. Darüber hinaus enthält der Bericht einige interessante Details, aus denen hervorgeht, dass die Länder, in denen die Bedrohungen entwickelt werden, diese durchaus auch gegen Organisationen innerhalb der eigenen Grenzen einsetzen.

Abschließend portraitieren wir noch unsere eigene Leistung. So sehen wir uns unsere Vorhersagen genauer an, die wir in dem im Januar veröffentlichten Bericht *2009 Threat Predictions* („Bedrohungsvorhersagen 2009“) abgegeben haben und zeigen, ob und in welchem Umfang diese eingetreten sind. Zu den Highlights zählen die Nutzung aktueller Ereignisse und Social Networking-Webseiten, über die die Bedrohungen an nichtsahnende Benutzer weitergeleitet werden.

Spam: Noch immer eine globale Bedrohung

Welche Rezession?

Im ersten Quartal 2009 bewegt sich die Verbreitung von E-Mails und Spam auf einem Tiefstand, wie wir ihn seit fast zwei Jahren nicht gesehen haben. Sind auch die Spammer von der weltweiten Wirtschaftskrise betroffen und gehen schweren Zeiten entgegen? Das dürfte kaum der Fall sein. Es sieht vielmehr so aus, dass die Verbreitung von Spam nach der Abschaltung von McColo im November 2008 das bisherige Ausmaß noch nicht wieder erreicht hat. Gegenüber dem gleichen Quartal des Vorjahrs liegt der Umfang an Spam-E-Mails im Jahr 2009 um 20 Prozent niedriger und ist dabei sogar 30 Prozent unter den Zahlen vom dritten Quartal 2008, als die bislang höchsten Quartalswerte erreicht wurden. Seit dieser Spam-Host vom Netz genommen wurde, hat die Anzahl an Spam-E-Mails um etwa 70 Prozent zugenommen, aber die vorherigen Werte noch nicht wieder erreicht.



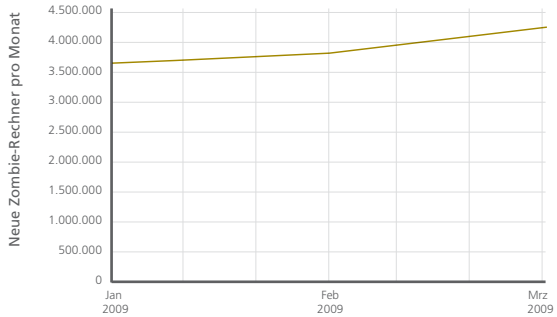
In den letzten Jahren hatte der Monat März immer die höchsten E-Mail-Zahlen ausgewiesen, aber in diesem März lagen die Werte weit darunter. Im vergangenen Jahr wurden im Durchschnitt 153 Milliarden E-Mails täglich festgestellt. Dagegen waren es in diesem März pro Tag nur etwa 100 Milliarden Nachrichten.

Der Anteil von Spam an allen E-Mail-Nachrichten ist erstmals seit 2006 unter die 90-Prozent-Marke gefallen. Wurden für 2008 vom gesamten E-Mail-Verkehr insgesamt 90 Prozent als Spam bewertet, lag der Spam-Anteil im letzten Quartal bei 86 Prozent. Auch wenn die Anzahl der E-Mail-Konten und die damit verbundenen Aktivitäten sehr stark schwanken, gehen wir davon aus, dass die Verbraucher, verglichen mit dem letzten Jahr, heute pro Tag sechs bis zwölf E-Mails weniger erhalten.

Natürlich erwarten wir, dass der Umfang des Jahres 2008 bald wieder erreicht sein wird, aber es dauerte länger als vielfach ursprünglich angenommen, bis die Kommandozentren und Botnets nach der Abschaltung von McColo wieder neu errichtet waren. Wie in jedem anderen Wirtschaftszweig auch, stellt dies für die Spammer letztendlich ein Renditeproblem dar.

Neue Zombies kurbeln Produktion an

In diesem Quartal entdeckten wir fast 12 Millionen neue IP-Adressen, die als „Zombies" betrieben, also von Spammern oder anderen gesteuert, werden. Dies stellt gegenüber dem letzten Quartal 2008 einen signifikanten Anstieg von fast 50 Prozent dar. Auch im dritten Quartal 2008 hatte es schon eine Rekordzunahme an neuen Zombies gegeben, aber diese Zahl wurde in diesem Quartal noch um 1 Million übertroffen. Und obwohl der Umfang von Spam-E-Mails nach der Trennung von McColo vom Netz noch nicht wieder den alten Stand erreicht hat, zeigen die Aktivitäten der neuen Zombies, dass die Spammer hart daran arbeiten, die verlorene Infrastruktur wiederherzustellen und dass der Spam-Umfang bald wieder das ursprüngliche Ausmaß annehmen wird.



Die infizierten Systeme können länderspezifisch aufgeschlüsselt werden. Im letzten Quartal konnten 63 Prozent der neuen Zombies den zehn Top-Ländern zugeordnet werden. Dieser Wert stellt gegenüber den beiden Quartalen zuvor eine geringfügige Abnahme dar. Es scheint, dass die Spammer nun auch Computer in anderen Ländern angreifen, um ihre Ziele zu erreichen.

1. Quartal 2009		4. Quartal 2008		3. Quartal 2008	
Land	**IP-Adressen in %**	**Land**	**IP-Adressen in %**	**Land**	**IP-Adressen in %**
USA	18,0	China	15,8	China	20,4
China	13,4	USA	15,4	USA	16,5
Australien	6,3	Deutschland	6,5	Deutschland	6,8
Deutschland	5,3	Großbritannien	6,0	Großbritannien	6,0
Großbritannien	4,7	Brasilien	4,9	Brasilien	4,8
Brasilien	4,0	Spanien	4,3	Spanien	3,7
Indien	3,1	Australien	4,1	Indien	2,5
Spanien	3,0	Italien	3,5	Russland	2,4
Südkorea	2,8	Russland	3,1	Südkorea	2,4
Russland	2,5	Südkorea	2,4	Italien	2,2
Gesamt	**63,3**	**Gesamt**	**66,0**	**Gesamt**	**67,5**

In den letzten drei Quartalen haben entweder China oder die USA den obersten Platz der Liste belegt. Sie liegen bei der Anzahl der von Spammern gesteuerten Computern an erster Stelle. Neu hinzu gekommen ist Australien, das im dritten Quartal 2008 noch nicht unter den ersten zehn Ländern war. Aber innerhalb von zwei Quartalen sprang dieses Land auf Platz drei und stellt nun 6 Prozent aller neuen Zombies. „Down Under" scheint ein fruchtbarer Boden für die Rekrutierer von Zombies zu sein.

1. Quartal 2009		4. Quartal 2008	
Land	**Spam in %**	**Land**	**Spam in %**
USA	35,0	USA	34,3
Brasilien	7,3	Brasilien	6,5
Indien	6,9	China	4,8
Südkorea	4,7	Indien	4,2
China	3,6	Russland	4,2
Russland	3,4	Türkei	3,8
Türkei	3,2	Südkorea	3,7
Thailand	2,1	Spanien	2,4
Rumänien	2,0	Großbritannien	2,3
Polen	1,8	Kolumbien	2,0
	70,0		**68,3**

Die wichtigsten Spam-Länder: Die USA haben weltweit die Führungsposition inne

Die US-Autobauer scheinen zwar Probleme mit der Produktion und dem Absatz zu haben, aber mit 35 Prozent des globalen Spam-Ausstoßes besetzen die USA auch weiterhin weltweit die Führungsposition. Die Steuer- und Überwachungsvorgänge von Spam-Aussendungen basieren zwar auf einer internationalen Infrastruktur, aber die Spammer bevorzugen noch immer Computer in den USA für die Produktion von Spam. Die 10 wichtigsten Länder dominieren die Spam-Produktion und sind für fast 70 Prozent des gesamten Spam-Vertriebs verantwortlich. Damit lassen sie die anderen 200 in der Skala folgenden Länder weit hinter sich.

Wenn wir uns die letzten beiden Quartale ansehen, stellen wir fest, dass Indien prozentual den größten Zuwachs zu verzeichnen hatte und nun mit fast 7 Prozent zum weltweiten Spam-Umfang beiträgt. Der Spam-Ausstoß dieses Landes hat sich gegenüber dem vorherigen Quartal verdoppelt. Möglicherweise ist Spam ja die neueste Branche, bei der ein Outsourcing nach Indien versucht wird.

Wir dürfen aber auch Thailand, Rumänien und Polen unter den Top 10 begrüßen. Diese Daten legen die Vermutung nahe, dass Spammer einfach überall nach neuen Quellen suchen, um ihre Spam-Engines zu stärken.

1. Quartal 2009		4. Quartal 2008		3. Quartal 2008	
Verschreibungs-pflichtige Medika-mente	25,0	Verschreibungs-pflichtige Medikamente	37,0	Stärkung der Männlichkeit	31,2
Werbung	21,9	Werbung	19,3	Werbung	19,3
Produktnachbil-dungen	18,8	Stärkung der Männlichkeit	16,8	Verschreibungs-pflichtige Medikamente	10,7
Stärkung der Männlichkeit	17,5	E-Mail-Übermitt-lungsstatus	9,5	Storm	8,0
E-Mail-Übermitt-lungsstatus	7,1	Dating	3,9	E-Mail-Übermitt-lungsstatus	7,7
Storm	1,6	Produktnachbil-dungen	2,6	Aktuelle Neuigkeiten	6,7
Diplome	1,1	Stellen-/ Arbeitsangebote	1,7	Produktnachbil-dungen	6,0
Software	1,1	Software	1,5	Kreditangebote	1,6
Kreditangebote	1,0	Kreditangebote	1,2	Bankwesen	1,1
Sonstige	4,9	Sonstige	6,5	Sonstige	7,7
	100,0		**100,0**		**100,0**

Die wichtigsten Spam-Arten: Sex, Drogen und vieles mehr

Zu den am häufigsten versendeten Spam-Arten zählen Werbungen für Produkte zur Stärkung der Männlichkeit und für verschreibungspflichtige Arzneimittel sowie allgemeine Werbung. Diese drei Arten machten für sich genommen bereits etwa 60 Prozent des gesamten Spam-Aufkommens in den vergangenen drei Quartalen aus. Es scheint, als habe der Kultslogan „Sex, Drugs and Rock'n'Roll" durch Spam noch immer Bestand. Na ja, fast. Vielleicht sind wir ja einfach nur erwachsener geworden, denn heute geht es vielmehr um Sex, Drogen und Geschäfte.

Spam zur Bewerbung von Produktnachbildungen (zumeist Fälschungen von Markenuhren) haben in diesem Quartal stark zugenommen und stellen fast 19 Prozent des gesamten Spam-Aufkommens dar. Diese Art von Spam war im ganzen letzten Jahr sehr häufig, hat aber in diesem Quartal noch einmal deutlich zugenommen. Das legt die Vermutung nahe, dass uns Spammer in wirtschaftlich schwierigen Zeiten bei der Stärkung unserer Kaufkraft unterstützen, indem sie auf scheinbar gute Geschäfte oder ganz besondere Angebote hinweisen.

Spam mit Hinweisen zum Übermittlungsstatus anderer E-Mails macht noch immer 8 Prozent allen Spams aus. Diese Nachrichten sind fast immer an Phishing-Angriffe gekoppelt und geben nach dem erfolgreichen Spoofing der E-Mail-Adresse des Opfers den Anschein, als handele es sich um die Benachrichtigung über eine nicht zustellbare E-Mail. Ganz offensichtlich werden Phishing-Bedrohungen noch immer ganz groß geschrieben. Viele dieser Nachrichten gehen mit einem finanziellen Betrug einher und versuchen, dem Empfänger persönliche Daten zu entlocken.

Spammer interessieren sich weder für ihre noch eine andere Staatshoheit

Einem Mythos aus der Gemeinschaft der Internetkriminellen zufolge, ziehen es diese zu einem Großteil mutmaßlich in Osteuropa beheimateten Online-Gangster vor, Ziele in der westlichen Hemisphäre anzugreifen und Verbraucher oder Unternehmen im Bereich der eigenen Strafverfolgung zu meiden.

Wir erhalten jedoch immer mehr Daten, die das als Irrglauben ausweisen. Im Internet gibt es keine geografischen Grenzen, und es ist offensichtlich, dass Internetkriminelle jedes beliebige Ziel angreifen, das Aussicht auf Erfolg verspricht. So haben wir den Nachweis, dass Cyberbetrüger auch in einige Regierungsstellen und Unternehmen in Russland und Osteuropa eingedrungen sind und hochrangige Personen dieser Organisationen angegriffen haben.

Die McAfee-Organisation TrustedSource™ hat unlängst Malware transportierende E-Mails und Spam aus einer Reihe von Regierungsstellen und Finanzinstituten in Russland beobachtet. Nach unserer Auswertung zählen die folgenden Unternehmen zu den betroffenen russischen Banken:

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

Darüber hinaus weisen unsere Daten darauf hin, dass die Computersysteme der folgenden russischen Regierungsstellen von Cybergangs gesteuert werden:

- Finanzministerium der Region Nazran
- Staatliches Internet-Netzwerk
- Regionales Finanz- und Wirtschaftsinstitut
- Vereinigtes Institut für Kernforschung
- Medical Center of Russian Federation President's Management Department
- Rentenkasse der Russischen Föderation
- Persönliches Netzwerk des Justizministeriums der Russischen Föderation
- JSC Chechen Cellular Communication

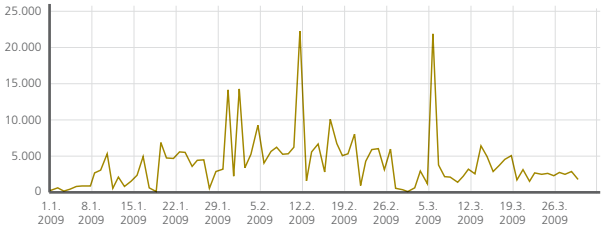
Diese sich auf Russland beziehenden Daten zeigen, dass Internetkriminelle bei ihren Zielpersonen und -institutionen keinen wirklichen Unterschied machen und im Grunde jede für sie interessante Organisation angreifen. Und auch wenn Russland bei diesen Aktivitäten eindeutig die Nase vorn hat (und hier der meiste Spam produziert wird), belegen unsere Auswertungen, dass auch in anderen Ländern der ehemaligen Sowjetunion wie der Ukraine, Weißrussland, Armenien, Aserbaidschan, Georgien, Kasachstan, Kirgisistan, Moldawien, Tadschikistan, Turkmenistan und Usbekistan derartige Spam-E-Mails produziert werden.

Web: Täglich neue Webseiten mit bedrohlichen Inhalten

Im Verlauf dieses Quartals beobachteten wir zahlreiche Bedrohungen, die bereits im letzten Quartal 2008 zu verzeichnen waren. Allerdings war ihre Intensität höher. Die Medien haben sich zwar in erster Linie auf Conficker konzentriert, aber dieser Wurm war beileibe nicht die einzige Bedrohung in diesem Quartal. Denn auch ohne die Aktivität von Conficker ist seit Jahren ein leichter Anstieg der Aktivitäten und, verglichen mit den vorherigen Quartalen, eine beträchtliche Zunahme zu beobachten. Gefälschte AV-Anwendungen stellten ein Problem dar, das im Internet einige Besorgnis sowie einen Anstieg der Scam- und Phishing-Aktivität auslöste.

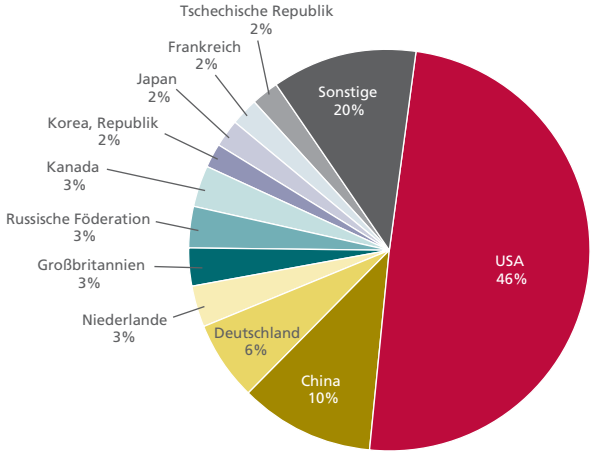
Die gefährlichen Domains, die mit Conficker infiziert wurden, tauchen auf keinen Karten oder in den Daten dieses Abschnitts nur in der Grafik „Verteilung von Webseiten mit schlechter Bewertung" auf. Die Daten von Conficker sind zwar ein wichtiger Bestandteil der Bedrohungslandschaft, zeigen aber nicht das ganze Bild der gefährlichen Aktivitäten. Denn es gibt noch viele andere Bedrohungen, die an Verbreitung und Bedeutung zunehmen. Die Malware-Autoren und Scammer nutzen die Besorgnis über die wirtschaftliche Situation aus, um zahlreiche neue Scam-Seiten zu erzeugen. In ihren E-Mails locken sie die Empfänger zum Beispiel mit der Vermeidung von Zwangsvollstreckungen, lenken Interessierte

aber zu Phishing-Webseiten um, auf denen alles Mögliche, bis hin zu Kundenkarten von Kaufhausketten, angeboten wird. Webseiten mit gefälschten Virenschutzangeboten werden ahnungslose Benutzer auch weiterhin ausnutzen. Die Methoden zum Anlocken von Benutzern auf solche Webseiten entwickeln sich stetig weiter. Auch ohne die gesamte Conficker-Aktivität ist die Anzahl der URLs, die die Empfehlungsstufe „Vorsicht" (rot) erhalten haben, gegenüber den letzten beiden Quartalen 2008 beträchtlich angestiegen.



Neue Webseiten mit schlechter Bewertung pro Tag

Wo werden diese URLs mit schlechter Internetbewertung gehostet? Auf keinen Fall da, wo die meisten Menschen glauben.



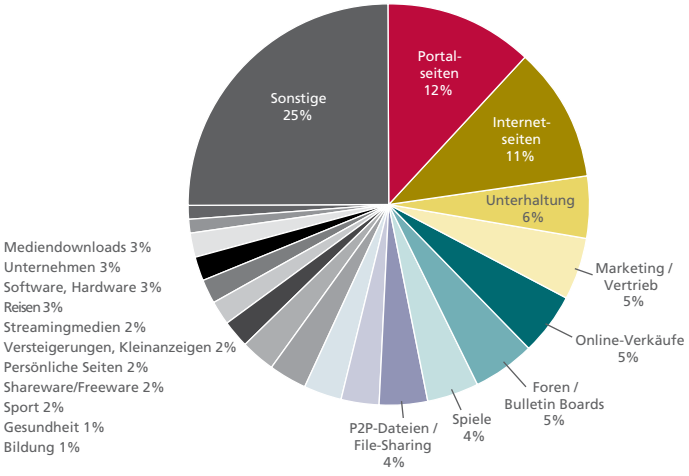
Verteilung von Webseiten mit schlechter Bewertung

Warum aber der plötzliche Wechsel weg von den bei gefährlichen Internetaktivitäten als Standard angesehenen Ländern, insbesondere den ersten drei, USA, China und Russland?[1] Es bedeutet nicht, dass es in diesen Ländern weniger URLs mit einer schlechten Bewertung gibt. Es heißt vielmehr, dass der Prozentsatz in anderen Ländern gestiegen ist. Ein Großteil dieses Wachstums hat mit den Domains zu tun, die Conficker infiziert hat bzw. es versuchte. Tatsächlich hat allein diese Bedrohung die Niederlande zusammen mit einem weiteren Land auf Platz 4 katapultiert. Dort wurden Phishing-URLs zwar schon über längere Zeit gehostet, aber Conficker verursachte einen beträchtlichen Anstieg der mit Malware und anderen gefährlichen Inhalten infizierten Webseiten. Allerdings geht diese Veränderung nicht allein auf das Konto von Conficker. So hat Kanada seinen Weg in die Top 10 dadurch geschafft, dass dort zahlreiche gefährliche Webserver gehostet werden. Die Zahl der unterschiedlichen Malware und Spyware, die auf diesen Webseiten lauert, ist in erster Linie für diese Bewertung verantwortlich.

1Im dritten Quartal 2008 wurde folgende Reihenfolge verzeichnet: USA mit 41 Prozent, China mit 12 Prozent, Russland mit 7 Prozent, Deutschland und die Niederlande mit je 5 Prozent, Südkorea mit 4 Prozent, Hongkong mit 3 Prozent, Taiwan, Kanada und Tschechien mit jeweils 2 Prozent und alle anderen mit zusammen 17 Prozent.

Eine wichtige Erkenntnis besteht darin, dass diese Länder in den Statistiken zu mehreren Angriffskomponenten auftauchen: Gefährliche Webseiten, Webseiten mit Spyware oder Adware, Phishing und Spam. Die 7 Länder mit den meisten Webseiten mit schlechter Internetbewertung sind auch in der Liste der 10 Länder mit den meisten Webseiten mit Phishing- und Spam-Bedrohungen sowie mit Malware bzw. Spyware vertreten.

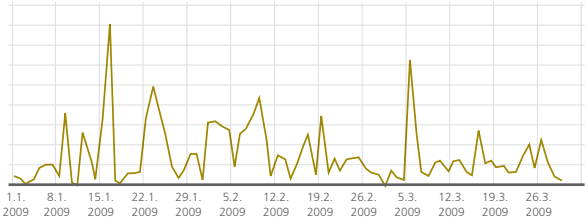
Dabei sind die Absichten der Webseiten mit einer schlechten Bewertung sehr unterschiedlich. Sie reichen von seriösen Zielen über zweifelhafte Angebote bis hin zu eindeutigem Betrug. Natürlich ist das Risiko immer noch höher, wenn man Porno- oder Casino-Seiten besucht, die nicht mit anerkannten, seriösen Unternehmen in Zusammenhang stehen. Aber im Grunde sind alle Webseiten verwundbar und jeder beliebige Inhalt, auf den ein Benutzer zugreifen möchte, bietet einem Malware-Verteiler eine Angriffsmöglichkeit.



Die 20 wichtigsten, seriösen Kategorien von Webseiten, die von TrustedSource eine schlechte Bewertung erhalten haben

In diesem Quartal wenden sich die Malware-Verteiler eher den Inhaltsservern als Mittel zur Weitergabe gefährlicher und illegaler Inhalte zu. Wir sehen diesen Trend genauso bei Webseiten, die von respektablen und hoch angesehenen Anbietern betrieben werden, wie bei weniger bekannten und fragwürdigeren Providern. In Kombination mit der weit verbreiteten Nutzung von Blogs und Suchmaschinenoptimierern stellt diese Bedrohung eine noch kritischere Gefährdung der Sicherheit aller Computer dar.

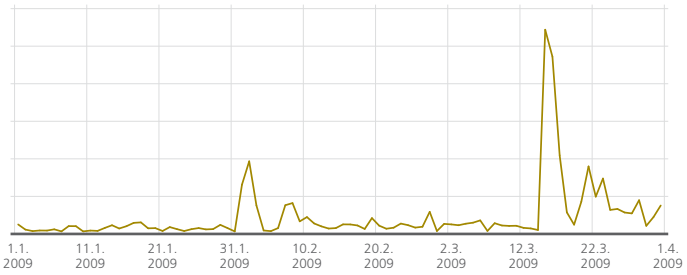
Die Frage des *Wo* haben wir erklärt, sehen wir uns nun noch die *Arten* der Bedrohungen an, die wir registrierten. Abgesehen von Conficker gab es in diesem Quartal auch noch zahlreiche andere Aktivitäten im Hinblick auf neue Malware und Bedrohungen im Internet.



Neue Websites, die Malware und PUPs liefern

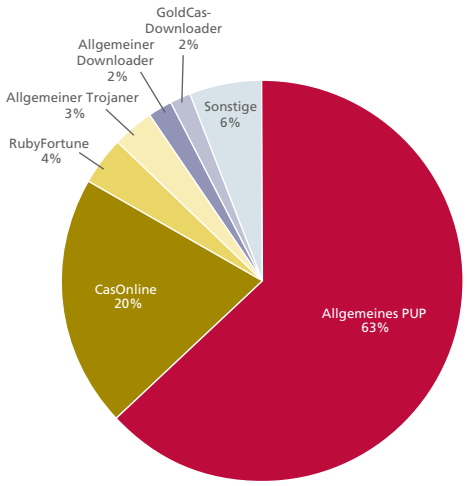
Die Grafik oben zeigt die Anzahl der Webseiten, von denen Malware und potenziell unerwünschte Programme (PUPs) ausgehen und die in diesem Quartal vom McAfee TrustedSource-Netzwerk entdeckt wurden. (Die Grafik zeigt Webseiten, auf denen Malware gehostet wird, und stellt den Datenverkehr zwischen Benutzern und diesen Seiten dar. Bei dieser Grafik geht es nicht um seriöse Seiten, über welche die Benutzer auf Malware-Seiten umgeleitet werden. Außerdem wurde aus den Daten unsere präventive Forschungsaktivität herausgerechnet, um ein echtes Bild der einzelnen neuen Gefahren zu zeichnen, die bei normalen Suchvorgängen im Internet in der Schule, am Arbeitsplatz oder zu Hause drohen.)

Dagegen zeigen die Grafiken unten die Daten, die unsere präventive Methodik fand hinsichtlich neuer einzelner Malware-Downloads, die von mehreren Webseiten verwendet werden. Es gibt einige interessante Spitzen durch neue Bedrohungen oder wahre „Goldgruben" mit gefährlichen Downloads oder PUPs, die wir entdeckten.



Malware- und PUP-Downloads, präventive Erkennung pro Tag

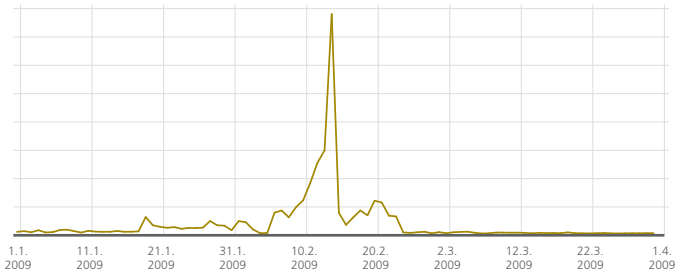
Unsere präventiven Beobachtungen (regelmäßige Durchsuchung und Verifizierung von Webseiten sowie einmalige Verfahren zum Auffinden bedrohlicher Daten) zeigten eine riesige Spitze bei neuen mit Online-Casinos in Zusammenhang stehenden Malware-Downloads etwa gegen Ende Januar/Anfang Februar, sowie eine weitere Spitze bei allgemeinen PUPs gegen Ende des Quartals. Diese Aktivität bezog sich auf die vier häufigsten Malware-Download-Typen im Quartal (siehe nächste Grafik). Eine weitere interessante Malware ist der dauerhaft festgestellte Trojaner Vundo, der in den vergangenen drei Monaten eine größere Aktivität verzeichnete.



Häufigkeit von Malware- und PUP-Downloads, nach Typ

Eine der nur schlecht zu erfassenden Internetbedrohungen, denen wir derzeit ausgesetzt sind, ist der sogenannte *Exploit* (Ausnutzung), ein Begriff, der bei Forschern und Benutzern mehrere, häufig unterschiedliche Sachverhalte bezeichnet. Avert Labs spürt bei der Durchsuchung und Überwachung des Internets neue Seiten auf, auf denen Browser-Exploits gehostet werden. Dabei werden ständig neue Sicherheitslücken festgestellt. Wenn Browser (und ihre Plug-Ins) nicht regelmäßig aktualisiert werden, können diese „Spielwiesen" sehr leicht zum Betätigungsfeld von Malware-Autoren werden. Sobald sich einer dieser Autoren eines solchen Bereichs bemächtigt, erhalten die Computer der Benutzer unter Umständen einen Programmcode, der eine Infektion mit Adware, einem Tastaturprotokollierer und anderen gefährlichen Aktivitäten ermöglicht.

Wenn Browser (und ihre Plug-Ins) nicht regelmäßig aktualisiert werden, können diese „Spielwiesen" sehr leicht zum Betätigungsfeld von Malware-Autoren werden.

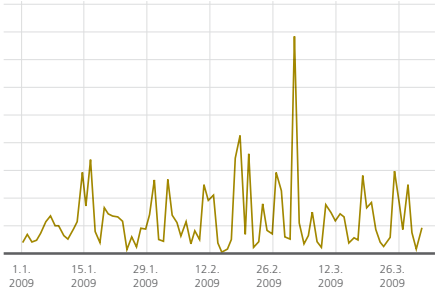


Festgestellte Webseiten mit Browser-Exploits

Anonymizer-Aktivität

Malware-Autoren setzen verstärkt URL-Umleitungen ein. Sie nutzen dabei entweder einen Anonymizer oder die Web 2.0-Schnittstelle eines Inhaltsservers. Dies geschieht entweder, um eine Standard-erkennung zu verhindern (Verwendung einer eingebetteten URL statt einer Quell-URL) oder um die Internetbewertung der Seiten auszunutzen, die angezeigt wird und die Malware übermittelt.

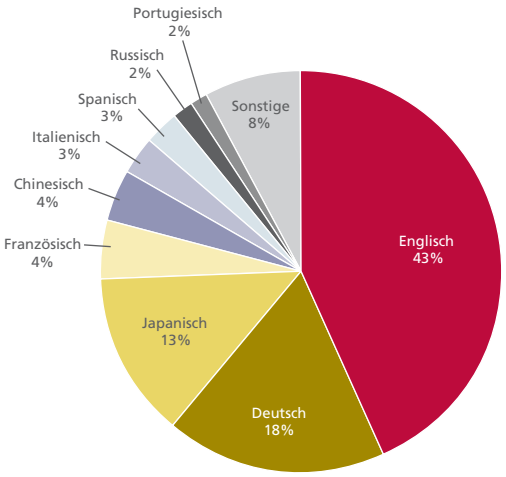
Bei einem Anonymizer handelt es sich um ein Programm, das die Identität eines Benutzers verschleiert, während er online ist. Da die meisten Anonymizer nicht gefährlich sind, werden sie in unseren früheren Darstellungen zu den bestehenden Sicherheitsrisiken nicht erwähnt. Allerdings kann die Nutzung eines solchen Programms leicht zu einem MITM (Man In The Middle)-Angriff führen, bei dem siche ein gefährlicher oder entführter Anonymizer Code in zwischen Benutzer und Server übertragene Mitteilungen einfügt. Dies gefährdet nicht nur den Benutzer sondern auch die Hosts und Netzwerke, die ansonsten geschützt wären. Insgesamt betrachtet, hat die Anonymizer-Aktivität in diesem Quartal gegenüber dem letzten zugenommen. Aber auch über die Jahre gesehen ist in diesem Quartal ein leichter Anstieg zu verzeichnen.



Neue Anonymizer pro Tag

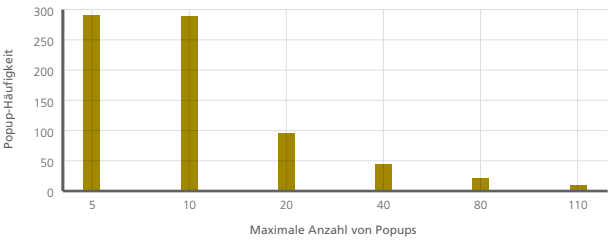
Allgemeine Trends bei Internetbedrohungen

Das Internet ist eine weltweite Gemeinschaft. Das lässt sich gut anhand der zahlreichen Querverbindungen von berufsbezogenen oder Social Networkung-Webseiten darstellen. Ständig werden Webseiten erweitert, um weitere Sprachen zu unterstützen. Die gleichen Blog-Angriffe, die auf stark frequentierten Webseiten in den USA festgestellt werden, verbreiten sich neben zahlreichen anderen Sprachversionen auch über chinesische und brasilianische Blogs. Hinzu kommt, dass die heutigen Angriffe Netze mit einem großen Verbreitungsgebiet nutzen. Außerdem nutzen die Malware-Verteiler das Markenbewusstsein der Benutzer aus (wie z.B. bei führenden Sportereignissen mithilfe von in Turnierpläne oder Spielerfotos eingebettete Malware) und nutzen weltweite Markennamen, um Benutzer in allen Sprachen zu ködern.



Sprachverteilung von Webinhalten

Noch immer stellen Popups ein Ärgernis dar. Interessant ist dabei, dass trotz des Einsatzes von Popup-Blockern und ähnlichen Tools die meisten Webseiten weiterhin Popups einsetzen. Die höchste bei einer Website festgestellte Anzahl von Popups betrug 116.



Verteilung von Popups in Webseiten (mit wenigstens 5 Popups)

Die sich im Internet präsentierenden Unternehmen müssen mit der gleichen Sorgfalt behandelt werden, wie ein Vertreter an der Haustür.

Wir stellen noch immer fest, das seriöse Web 2.0- und unternehmensbezogene URLs zur Verbreitung von Malware genutzt werden. Noch bis vor 10 Jahren konnte man davon ausgehen, dass man relativ sicher war, wenn man sich nur von bestimmten Inhalten fernhielt. Heute sehen wir uns dagegen überall Bedrohungen ausgesetzt, unabhängig davon, wo wir suchen. Alle Webseiten, die ausgenutzt werden können, werden auch ausgenutzt (über eine der zahllosen Schwachstellen, die es gibt). Die Administratoren sehen sich regelmäßig Scans ihrer Server an, um festzustellen, ob ein Exploit vorhanden ist. Interessant ist dabei, dass viele dieser Scans Webseiten und Server betreffen, die mit allen möglichen

Angeboten von illegaler Software über gefährliche Inhalte bis hin zu Anonymizern in Zusammenhang stehen. Wenn bestimmte stark frequentierte Webseiten Sicherheitslücken aufweisen, dann ist es keine Frage, ob diese Seiten ausgenutzt werden, sondern nur, wann dies geschieht.

Wir haben eine beträchtliche Zunahme an Betrugsversuchen über das Internet festgestellt. Wir gehen davon aus, dass diese Zahlen noch weiter steigen werden, da Internetkriminelle- die Ängste der Verbraucher über Spam-E-Mails und das Internet ausnutzen. Es ist häufig schwierig festzustellen, ob ein Unternehmen seriös ist oder nicht. Daher müssen die sich im Internet präsentierenden Unternehmen mit der gleichen Sorgfalt behandelt werden, wie ein Vertreter an der Haustür. Den Benutzern muss klar sein, dass ihre Daten weg sind, sobald sie einem Betrüger ihre Kreditkartendaten für eine Online-Zahlung oder eine gefälschte Dienstleistung übermitteln.

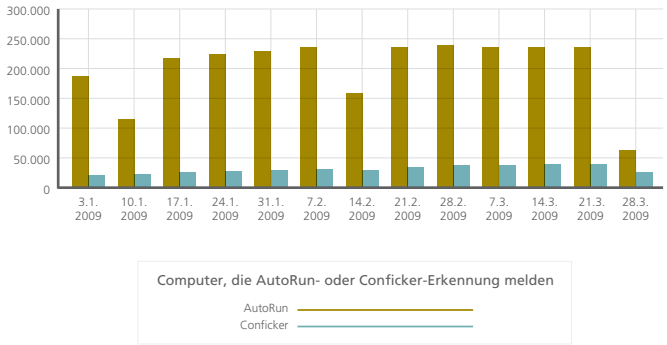
Allerdings bringen unsere Forschungen auch einen Funken Hoffnung für die Wirtschaft. Webseiten mit Immobilienangeboten weisen in diesem Quartal einen beträchtlichen Anstieg auf. Sie stehen rangieren nun unter den 10 bedeutendsten Inhaltskategorien, die Nutzern zur Verfügung stehen (der Bereich Sport wurde dabei aus dieser Liste verdängt).

Bedrohungen durch Malware: Conficker-Hysterie gegen AutoRun-Wirklichkeit

In den vergangenen Monaten war Conficker ständig in den Schlagzeilen. Man konnte leicht annehmen, es wäre die einzige Bedrohung gewesen, über die man sich Gedanken machen müsste. Die vorhandenen Zahlen sagen jedoch etwas anderes aus. Conficker ist nicht wirklich ein Schicksalsschlag.

In vielerlei Hinsicht war Conficker natürlich eine ernst zu nehmende Malware. Dieser Wurm infizierte zahlreiche Hosts. Er wurde konsequent entwickelt, verwaltet und diskutiert. Aber die Anzahl an tatsächlich erfolgten Erkennungen ist nicht so hoch, wie man dies von einer Malware erwarten würde, der ein solches Maß an Aufmerksamkeit zuteil wurde.

Auf der anderen Seite sahen wir in diesem Quartal auch Malware, die uns echte Sorgen bereitet. Denn AutoRun-basierte Malware, die sich in erster Linie über USB-Laufwerke oder Flash-Speicher selbst repliziert und verbreitet und dazu in diesem Quartal viel häufiger auftritt als Conficker, ist ein ganz anderes Kaliber. Sehen wir uns beide einmal im direkten Vergleich an:



Während der letzten 30 Tage waren weniger als 10 Prozent aller gemeldeten Erkennungen AutoRun-Würmer. Conficker begann mit einem Prozent und arbeitete sich auf das 12-Fache hoch, machte aber zu den Spitzenzeiten der AutoRun-Würmer zahlenmäßig immer noch weniger als 15 Prozent der AutoRun-Erkennungen aus.

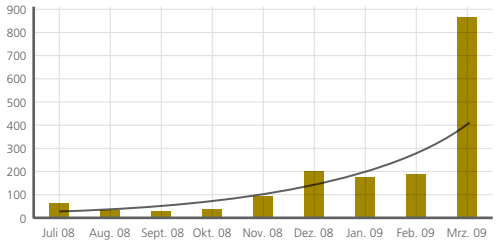
Aktualisierte Vorhersage

Anfang des Jahres veröffentlichten die McAfee Avert Labs ihren Bericht *2009 Threat Predictions („Bedrohungsvorhersagen 2009").*[2] Einige unserer wohlbegründeten Vermutungen bewahrheiteten sich in diesem Quartal tatsächlich.

2. McAfee Avert Labs Threat Center. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_de.pdf

Beschuss durch eigene Truppen fordert Opfer

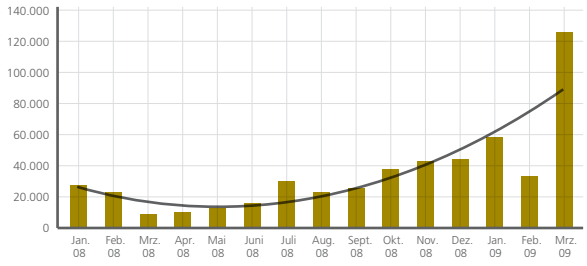
Eine weit verbreitete Bedrohung des letzten Jahrzehnts war, von Freunden oder Bekannten Viren zu erhalten. Diese Bedrohung ist wurde fast unbedeutend. Aber durch Web 2.0 nahm diese althergebrachte Angriffsmethode wieder etwas an Bedeutung zu. In diesem Quartal überraschten zahlreiche Koobface-Varianten Tausende Benutzer, als sie von Freunden über Facebook einen Virus erhielten. Von den Opfern unerkannt, wurden sie durch Links in einer vom Virus versendeten Mitteilung auf Webseiten umgeleitet, die diesen Wurm verbreiteten. Kurz darauf wurden ihre Computer mit dem Virus infiziert, und sie gaben die infizierten Mitteilungen dadurch wiederum an ihre Freunde weiter. Social Networkung-Seiten bieten Angreifern noch immer Möglichkeiten für eine Social Engineering-Attacke.



Einzelne festgestellte Koobface-Varianten

Das World Wide Schurken-Web

Im Februar wurde Facebook von Angreifern ausgenutzt, die mithilfe dieser Plattform eine schädliche Anwendung erstellten. Viele Benutzer schluckten den Köder und installierten diese Anwendung. Der Angriff wurde in den Medien mit viel Aufmerksamkeit bedacht, was dazu führte, dass die McAfee Avert Labs einen sehr umfangreichen Suchmaschinen-Optimierungsring aufdeckte, der sich gegen die am häufigsten bei Google eingegebenen Suchbegriffe richtete. Die Angreifer stahlen nicht nur durch Copyright geschützte Daten von bekannten Webseiten, sondern nutzten auch andere bekannte Webseiten wie Democrats.org, um ihre eigene Bewertung bei Google zu steigern. Das Ziel der Angreifer bestand dabei darin, über diese Suchergebnisse gefälschte Virenschutz-Software zu installieren. Insgesamt führte die schädliche Facebook-Anwendung zu falschen Suchergebnissen und diese wiederum zu einer schädlichen Sicherheits-Software. Diese Zusammenhänge verdeutlichen die Notwendigkeit für mehr Sicherheit beim Surfen im Internet.

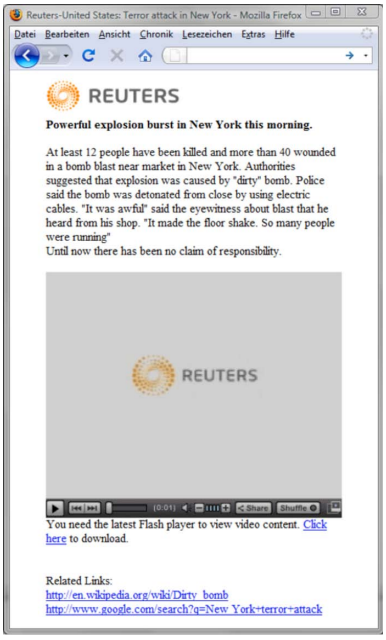


Festgestellte einzelne gefälschte Virenschutz-Codes

Die Bedrohungen sprechen Ihre Sprache

Die Angreifer wissen, dass ein Benutzer viel leichtsinniger reagiert, wenn der Angriff relevant und kontextbezogen ist: Klick auf einen Link, Eingabe eines Benutzernamens und eines Kennworts, Installation einer Anwendung. Berichte von Ereignissen in Ihrer Nähe ziehen viel leichter Ihre Aufmerksamkeit auf sich als Dinge, die sich auf der anderen Seite des Globus abspielen. Im Februar

und März nutzten Internetkriminelle dieses Konzept im Zusammenhang mit dem Waledac-Virus. Nichtsahnende Benutzer wurden auf Webseiten gelockt, die entsprechend ihrer jeweiligen Standorte angepasst waren und einen Hauch von Authentizität vermittelten. Während die Benutzer dann örtliche oder regionale Nachrichten lasen, versuchten die Webseiten mithilfe eines Drive-By-Codes heimlich, einen Virus zu installieren.



McAfee Avert Labs-Blog

Google und der Mißbrauch von Suchmaschinen

Google. Allein dieser Begriff hat für Nutzer unterschiedlichste Bedeutungen. Arbeitssuchende finden hier die aktuellen Stellenangebote. Arbeitgeber können unter Umständen qualifizierte Mitarbeiter online finden. Für Verbraucher ist es ein wirksames Instrument um, die Waren, die sie benötigen, zu einem attraktiven Preis zu erhalten. Und Malware-Autoren und Internetkriminelle sehen darin eine effiziente Möglichkeit zur Verbreitung von Malware und zur Ausübung von Internetverbrechen. Bei der aktuellen Bedeutung dieser Suchmaschinen für die Internetaktivitäten erscheint es nur logisch, dass Malware-Autoren deren Leistungsfähigkeit ausnutzen, um ihre Schadprogramme zu verbreiten. Wenn Sie Interesse an Blogs zu dieser Thematik haben, sollten Sie die folgenden Einträge im McAfee Avert-Blog lesen:

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

Die Kombination aus Indexierung und häufig benutzten Suchbegriffen auf der einen Seite und dem für Internetkriminelle leicht verdientem Geld auf der anderen, gehen wir davon aus, dass diese Art des Missbrauchs auch weiterhin Bestand hat.

Wirtschaft und Angst

Die weltweite wirtschaftliche Situation ängstigt weiterhin viele Menschen. Andere wiederum machen sich Sorgen über Sicherheitsprobleme und Terror. Malware-Autoren und Internetkriminelle schlagen aus diesen Ängsten Profit. Der Wirtschaftstrend, den wir auch in unserer Bedrohungsvorhersage für 2009 ansprachen, wurde in diesem Quartal auf unterschiedlichste Weise ausgenutzt. Angst ist ein mächtiger Motivator, wenn sie von Internetkriminellen als Lockmittel in einem Social Engineering-Umfeld eingesetzt wird:

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/

- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Betrug, Spam und Phishing funktionieren schon in guten Zeiten gut, in schlechten erst recht. Denken Sie immer daran, dass Kriminelle dieselben Nachrichten lesen wie wir alle. Sie nutzen die Schlagzeilen und Ereignisse gegen uns, wenn wir nicht wachsam bleiben.

Info über McAfee Avert Labs

McAfee Avert Labs ist das globale Team zur Bedrohungsforschung von McAfee Inc. Mit speziellen Teams für die Erforschung von Malware, potenziell unerwünschten Programmen, Host und Network Intrusion, mobiler Malware sowie ethischer Schwachstellenoffenlegung deckt Avert Labs ein breites Sicherheitsspektrum ab. Diese umfassende Sicht ermöglicht es den Forschern von McAfee, Sicherheitstechnologien kontinuierlich zu verbessern und Verbraucher besser zu schützen.

Info über McAfee, Inc.

McAfee (NYSE: MFE) ist einer der weltweit größten dedizierten Spezialisten für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Das Unternehmen bietet präventive und bewährte Lösungen und Dienstleistungen an, die weltweit sowohl Systeme als auch Netzwerke schützen und Anwendern beim Surfen, Browsen und Shoppen mehr Sicherheit im Internet geben. Dank seines preisgekrönten Forschungsteams entwickelt McAfee innovative Produkte, die es Privatanwendern, Unternehmen, dem öffentlichen Sektor und Service-Providern ermöglichen, gesetzliche Vorschriften einzuhalten, Daten zu schützen, Ausfälle zu vermeiden, Schwachstellen zu erkennen und ihre Sicherheit fortlaufend zu überwachen und zu verbessern. www.mcafee.com/de.

McAfee GmbH
Ohmstr. 18
5716 Unterschleißheim
Deutschland
Telefon: +49 (0)89 3707 0
www.mcafee.com/de