Bericht

Bedrohungsprognosen für 2011

McAfee® Labs™

Die Bedrohungen haben sich im vergangenen Jahr erheblich geändert. McAfee Labs stellte spürbare Weiterentwicklungen bei Malware und der Ausrichtung von Angriffen sowie einen weiteren Anstieg des täglichen Gesamtaufkommens bei Malware-Bedrohungen fest. Außerdem gab es wichtige Veränderungen bei den Bedrohungen, die auf Apple iPhones und andere Mobilgeräte abzielen. Es gibt jedoch auch gute Neuigkeiten. Die wichtigste lautet: Die Anzahl der täglich verbreiten Spam-E-Mails ist erheblich gesunken. Diese Schwankungen werfen die Frage auf, in welche Richtung sich Bedrohungen bewegen.

Genau wie in den vergangenen Jahr, wagt McAfee Labs Voraussagen über die Bedrohungen im nächsten Jahr und darüber hinaus. Wir empfehlen Ihnen, diese Informationen für Ihre Vorbereitung auf die sich verändernden zukünftigen Bedrohungen zu berücksichtigen.

Inhaltsverzeichnis

Ausnutzung von Social-Media-Tools

Im Jahr 2010 beobachteten wir einige bedeutende Veränderungen bei der Art und Weise, wie Schadcode und gefährliche Links verbreitet werden. Zum Ende dieses Jahres erlebten wir ein so geringes weltweites Spam-Aufkommen wie schon seit Jahren nicht mehr. Dies liegt darin begründet, dass immer mehr Benutzer von vergleichsweise „langsamen" Kommunikationsmethoden wie E-Mails zu direkteren Methoden wie Sofortnachrichten und Twitter wechselten. Dieser Mediumwechsel wird 2011 zu einem vollständigen Wandel der Bedrohungslandschaft führen.

„Social-Media-Verbindungen werden früher oder später E-Mails als Hauptmedium zur Verbreitung von böswilligem Code und Links ersetzen."

Da sowohl Verbraucher als auch Geschäftsnutzer weiterhin in Scharen zu Social-Media- und Networking-Webseiten strömen, um die Möglichkeiten zur sofortigen Kommunikation und zum Datenaustausch zu nutzen, wird es wahrscheinlich zu immer mehr gezielten Versuchen zum Missbrauch von Identitäten und Daten kommen. Social-Media-Verbindungen werden früher oder später E-Mails als Hauptmedium zur Verbreitung von böswilligem Code und Links ersetzen. Einerseits sind gewaltige Mengen persönlicher Informationen online verfügbar. Zudem haben Internetnutzer nur unzureichende Kenntnisse über den Schutz dieser Daten. Diese Kombination wird Internetkriminellen den Identitätsdiebstahl und das Anlegen von Benutzerprofilen erheblich erleichtern. Internetkriminelle setzen in Twitter und bei ähnlichen Technologien „Spear-Phishing"-Angriffe (gezielte Phishing-Angriffe) ein, da die Auswahl geeigneter Opfer unter den Benutzern und Gruppen auf diesen Plattformen sehr einfach ist.

Im nächsten Jahr werden außerdem zwei weitere verwandte Technologien die Aufmerksamkeit der Kriminellen auf sich ziehen: Kurz-URLs und Technologien zur Standortbestimmung.

Missbrauch von Kurz-URL-Diensten: Kurz-URLs sind für Social-Media-Tools und andere Kommunikationsmedien sinnvoll, da sie einfach eingefügt oder eingegeben werden können. Das Problem – und der Grund für den einfachen Missbrauch – dieses Dienstes liegt darin, dass die Benutzer erst beim Klicken auf die URL erfahren, wohin er führt. Diese Tatsache stellt eine hervorragende Gelegenheit zum Missbrauch dar. Spammer setzen Kurz-URLs bereits zur Umgehung traditioneller Spam-Filter ein. McAfee Labs erwartet, dass der Missbrauch von Kurz-URLs in allen Varianten der Internetkommunikation Einzug halten wird. Derzeit überwachen und analysieren wir – über mehrere Social-Media-Anwendungen und alle Anbieter von Kurz-URLs – mehr als 3.000 gekürzte URLs pro Minute. Diese werden zunehmend für Spam, Betrugsversuche und andere böswillige Zwecke eingesetzt. Die Tatsache, dass Kurz-URLs außerordentlich bequem sind, trägt erheblich zum Erfolg der Internetkriminellen und Spammer bei, da sie die Unmittelbarkeit von Social-Media-Tools im Vergleich zu E-Mails optimal nutzen können.

Missbrauch von Diensten zur Standortbestimmung: Immer mehr Internetnutzer aus allen Bereichen fügen in ihren Social-Media-Plattformen GPS-Informationen (Global Positioning System) hinzu, damit ihre Freunde und Kollegen stets wissen, wo sie sich befinden. Zudem bieten viele Standortbestimmungsdienste ihren Benutzern zur Erhöhung der Popularität Plaketten und Auszeichnungen an. Es bedarf wenig Fantasie, um zu erkennen, wie diese Informationen von Internetkriminellen und Betrügern ausgenutzt werden können: Dank Standortbestimmungsdiensten wie foursquare, Gowalla und Facebook Places ist es sehr einfach, die Position von Freunden und Fremden zu suchen, zu überwachen und genau zu bestimmen. Mit der Unterstützung der Bing-Kartenfunktion lassen sich beispielsweise die Positionen aller Tweet-Ersteller, die GPS-Daten veröffentlichen, in einem bestimmten Bereich genau bestimmen. Es ist leicht, diese Daten Themen oder Interessensbereichen zuzuordnen. Mit nur wenigen Mausklicks können Internetkriminelle in Echtzeit feststellen, wer wo Tweets veröffentlicht, was diese Personen sagen, wofür sie sich interessieren und mit welchen Betriebssystemen und Anwendungen sie arbeiten. Anschließend ist es kinderleicht, mithilfe der auf diese Weise erfassten Informationen einen gezielten Angriff zu starten.

Die Tatsache, dass diese Dienste die Suche und Überwachung einzelner Personen und Personengruppen (einschließlich ihrer Vorlieben und Abneigungen, Mitgliedschaften und Interessen) und die anschließend Reaktion darauf ermöglichen, sorgt dafür, dass sich Internetkriminelle und Betrüger im Jahr 2011 und darüber hinaus für diesen Ansatz interessieren werden.

Mobilgeräte

Bedrohungen für Mobilgeräte sind seit Jahren ein heißes Thema in der Sicherheits-Community. Wir erwarten, dass die Angriffe jederzeit losgehen können – was bisher jedoch noch nie der Fall war. Dennoch sagt McAfee Labs voraus, dass das Jahr 2011 einen Wendepunkt für Bedrohungen für Mobilgeräte darstellen wird. In diesem Jahr beobachteten wir viele neue, aber nur wenig verbreitete Bedrohungen für Mobilgeräte: Rootkits für die Android-Plattform, Remote-Jailbreaking-Exploits für das iPhone und nun auch Zeus (einen gut bekannten Bank-Trojaner mit Botnet). Der weit verbreitete Einsatz von Mobilgeräten in Geschäftsumgebungen wird in Kombination mit diesen und weiteren Angriffen wahrscheinlich zu der längst erwarteten Explosion führen. Aufgrund der empfindlichen Netzinfrastruktur und der zögerlichen Einführung von Verschlüsselungen sind Benutzer- und Unternehmensdaten ernsthaften Risiken ausgesetzt.

Apple

Unter Sicherheitsexperten, die sich in Online-Foren für Informationssicherheit bewegen oder Konferenzen zu diesem Thema besuchen, ist bekannt, dass die Mac OS X-Plattform in den Whitehat- und Blackhat-Communities ein sehr beliebtes Ziel ist. Whitehats suchen bereits seit langem nach Schwachstellen in Mac-Betriebssystemen und -Anwendungen. Obwohl Mac-Computer in der Vergangenheit nur selten Ziel böswilliger Angreifer waren, wird das Mac-Betriebssystem sehr häufig eingesetzt. In diesem Jahr beobachtete McAfee Labs weiter entwickelte Malware, die auf Mac-Computer abzielte. Wir erwarten, dass sich diese Entwicklung im Jahr 2011 fortsetzen wird. Die Beliebtheit von iPads und iPhones in Geschäftsumgebungen und die einfache Übertragbarkeit von böswilligem Code zwischen diesen Geräten könnten für viele Benutzer und Unternehmen im nächsten Jahr und darüber hinaus Risiken bedeuten. Wir erwarten, dass die Bedrohungen für Daten und Identitäten zunehmen werden. Das fehlende Verständnis der Benutzer für die Gefährdung dieser Plattform und das Fehlen von eingesetzten Sicherheitslösungen öffnen Internetkriminellen weite Einfallstore. McAfee Labs rechnet damit, dass das Auftreten von Botnets und Trojanern auf Apple-Plattformen im Jahr 2011 keine seltenen Ereignisse, sondern häufige Tatsache sein werden.

Anwendungen

Wir leben in einer anwendungsorientierten Welt. Dabei spielt die Wahl der Plattform oder des Geräts keine große Rolle. Der Nachteil liegt dabei in der Übertragbarkeit der eingesetzten Anwendungen zwischen Mobilgeräten und zukünftigen Internet-TV-Plattformen. Daher werden uns böswillige und Schwachstellen enthaltende Anwendungen im Jahr 2011 große Sorgen bereiten. Neben böswilligem Code rechnet McAfee Labs mit Anwendungen, die darauf abzielen, persönliche und personenbezogene Daten offen zu legen und zu kompromittieren. Die Gefahr wird schließlich über Medienplattformen wie Google TV zu Datenkompromittierung und Bedrohungen führen.

„Wenn aufgrund von Zeitdruck unsichere Produkte verkauft werden, wird es im Jahr 2011 mehr Angriffe geben, die es auf persönliche Informationen und andere Daten abgesehen haben."

Da von zuhause, vom Arbeitsplatz und über das Gerät gesteuerte Apps immer beliebter werden, werden auch sie immer öfter im Fokus von Angriffen stehen. Diese Tools sind traditionell schlecht programmiert und unzureichend geschützt, sodass Internetkriminelle über kompromittierte oder gesteuerte Apps verschiedenste physische Geräte manipulieren können. Dies wird die Effektivität von Botnets erheblich verbessern.

McAfee Labs erwartet für 2011 einen Anstieg bei verdächtigen und böswilligen Apps für die meisten häufig eingesetzten mobilen Plattformen und Betriebssysteme. Schlecht entwickelte Apps führten bereits zur Kompromittierung personengebundener Daten. Wir erwarten, dass Entwickler und Vermarkter mit zunehmender Verbreitung dieser Apps dem Druck unterliegen, diese so schnell wie möglich auf den Markt zu bringen. Plattformen, bei denen neue Apps ohne Kontrolle des Gerätehersteller entwickelt und verbreitet werden, sind besonders gefährdet. Wenn aufgrund von Zeitdruck unsichere Produkte verkauft werden, wird es im Jahr 2011 mehr Angriffe geben, die es auf persönliche Informationen und andere Daten abgesehen haben.

In diesem Jahr beobachtete McAfee Labs in Twitter und LinkedIn bereits einen Trend zu anwendungs-gesteuerten Botnets. Dies wird im Jahr 2011 und in den Folgejahren wahrscheinlich die Norm sein, da die Entwicklung und der Einsatz von Anwendungen im verbreiteter werden. Wird dies das Jahr der mobilen Botnets, die über eine heruntergeladene App gesteuert werden?

Fortschritt imitiert Rechtmäßigkeit

In diesem Jahr stellten wir fest, dass sich einige Bedrohungen weiter entwickelten. „Signierte" Malware, die legitime Dateien imitiert, wird im Jahr 2011 weiter verbreitet sein. Dies wird zu einer höheren Zahl gestohlener Schlüssel sowie zu Technologien und Tools führen, mit denen Schlüssel für den Einsatz bei solchen Angriffen gefälscht werden können.

„Friendly Fire"-Angriffe durch Koobface und VBMania, bei denen die Bedrohungen von Ihren Freunden zu kommen scheinen, werden auf Social-Media-Plattformen weiter zunehmen. Dies geht mit gleichzeitiger Zunahme des Missbrauchs sozialer Netzwerke einher und wird schließlich dazu führen, dass E-Mails als ehemals führender Angriffsvektor weit zurückfallen.

Wir erwarten zudem eine Zunahme von Angriffen mit „intelligenten Bomben", die nur unter bestimmten Bedingungen zünden. Bei diesen Bedrohungen müssen die Opfer einem festgelegten Angriffspfad folgen. Dadurch bleiben Honeypots, Crawler und Sicherheitsforscher außen vor, während verwundbare Opfer gezielt angegriffen werden können. Bei diesen Bedrohungen kommt Global Threat Intelligence eine noch größere Bedeutung zu, um einen Schutz vor Angriffen zu bieten, die nur unter bestimmten Umständen gestartet werden.

Persönliche Angriffe werden damit erheblich persönlicher.

Überleben der Botnets

Wie bereits im Abschnitt über Apps erwähnt, gehören Botnets weiterhin zu den größten und am weitesten entwickelten Bedrohungen, die von McAfee Labs beobachtet werden. Wir rechnen für die nächste Jahre mit einer Zunahme bei Datenexfiltrationen. In diesem Jahr setzten Internetkriminelle immer mehr gezielte Angriffe ein. Botnets werden sich wahrscheinlich mehr darauf konzentrieren, Daten von den angegriffenen Computern und Unternehmen zu entfernen und weniger Spam einsetzen. Botnets werden erweiterte Datenerfassungsfunktionen einsetzen und sich mehr auf den Missbrauch sozialer Netzwerke konzentrieren.

Gleichzeitig erleiden Botnets ebenfalls Verluste. Strafverfolgungsbehörden in aller Welt setzten Mariposa, Bredolab und einige Zeus-Botnets außer Kraft. Botnets entwickeln sich jedoch ebenfalls weiter. Der Zusammenschluss von Zeus und SpyEye wird zu ausgeklügelteren Bots führen, die Sicherheitsmechanismen und die Überwachung der Strafverfolgungsbehörden noch besser umgehen. Zusammenschlüsse und Übernahmen sind nun auch in der Malware-Welt angekommen.

Botnets, die Facebook und Twitter nutzen, erweitern ihren Tätigkeitsbereich um beliebte Social-Networking-Webseiten wie foursquare, Xing, Bebo, Friendster und andere. Internetkriminelle können die zunehmende Nutzung dieser Webseiten durch Privatpersonen und Unternehmen einfach nicht ignorieren. McAfee Labs erwartet zudem, dass mit der weiteren Verbreitung von GPS-Funktionen Standortbestimmungsfunktionen stärker in Botnets integriert werden.

Hacktivismus

Politisch motivierte Angriffe sind nicht neu. Die Häufigkeit nimmt jedoch immer weiter zu und wird 2011 noch erheblich wachsen. Zusätzlich zu den unter Hacktivisten besonders beliebten Webseiten-verunstaltungen sowie den in jüngster Zeit ebenfalls häufig eingesetzten DDoS-Angriffen (Distributed Denial of Service) kommen neue raffinierte Angriffsmethoden ins Spiel. So wird Informationsdiebstahl wahrscheinlich zunehmen, da auf diese Weise politische Gegner in Miskredit gebracht werden können. Weitere Gruppen werden dem Beispiel von Wikileaks folgen, da Hacktivismus von Personen betrieben wird, die sich als von bestimmten Regierungen oder Bewegungen unabhängig betrachten. Es wird noch darüber diskutiert, ob in Wirklichkeit Regierungen hinter diesen Manipulationen und Aktivitäten stehen oder diese heimlich unterstützen. Es ist jedoch wahrscheinlich, dass Staaten private Hacker dafür einsetzen werden. Hacktivismus könnte als Ablenkung zu Beginn eines Internetkriegs dienen. Alle Beteiligten der Informationssicherheitsbranche – Journalisten ebenso wie Forscher – müssen wachsam sein, um den Unterschied zwischen Hacktivismus und dem Beginn eines Internetkriegs erkennen zu können.

„Hacktivismus wird im nächsten Jahr zur neuen Methode, seine politische Meinung zu demonstrieren.“

Wir erwarten, dass soziale Netzwerke bei Hacktivismus eine größere Rolle spielen werden. Ebenso wie sich Internetkriminalität von Aktionen einzelner Personen, die Malware erstellen, zu unstrukturierten Gruppen verlagerte, die einen DDoS-Angriff starten können, rechnen wir im nächsten Jahr mit strafferen Organisationen und Strukturen unter den Hacktivistengruppen.

Hacktivismus wird im nächsten und in den Folgejahren zur neuen Methode, seine politische Meinung zu demonstrieren. Die politischen Organisatoren verlagern ihre Aktivitäten von der Straße ins Internet, um in Echtzeit Angriffe zu starten und Botschaften zu senden. Hacktivisten werden wie auch in der realen Welt Menschen zu Protesten und Demonstrationen anregen.

Hoch entwickelte hartnäckige Bedrohungen

Die Nachrichten über Operation Aurora und Google, die im Januar um die Welt gingen, führten zu einer neuen Bedrohungskategorie, den hoch entwickelten hartnäckigen Bedrohungen (Advanced Persistent Threats, APT). Diese werden seitdem unter Experten und in der Presse heiß diskutiert. Bis heute ist das wahre Ausmaß dieser Angriffe noch nicht vollständig geklärt.

Die allgemein akzeptierte Definition von APT beschreibt einen gezielten Internetspionage- oder -sabotageangriff, hinter dem Staaten oder Organisationen stehen, die nicht ausschließlich aus finanziellen/kriminellen oder politischen Interessen handeln. Nicht alle APT-Angriffe sind raffiniert und hoch entwickelt. Ebenso handelt es sich nicht bei jedem komplexen und gut geplanten gezielten Angriff um einen APT-Angriff. Nicht die Raffinesse oder die Auswirkungen, sondern das Motiv des Angreifers unterscheidet einen APT-Angriff von Angriffen durch Internetkriminelle oder Hacktivisten.

Der Angriff auf RBS WorldPay, der zum Diebstahl von 9 Millionen US-Dollar durch organisierte osteuropäische Internetkriminelle führte, war trotz des hohen Niveaus und der hervorragenden Koordination kein APT-Angriff. Diese Art von Angriffen werden nicht von Einzelpersonen durchgeführt. Weltweit gibt es zahlreiche APT-Angriffsteams, die sich in ihren Möglichkeiten und Fähigkeiten unterscheiden. Ebenso wie bei organisierten Internetkriminellen gibt es A-Teams und B-Teams. Einige haben Zugriff auf erhebliche Ressourcen (Hardware, Software und Personal) und sogar auf traditionelle Geheimdienst- und Überwachungsinformationen. Andere nutzen, stehlen oder kaufen vorgefertigte Tools, die von etablierten internetkriminellen Organisationen angeboten und häufig eingesetzt werden. Sie verhalten sich wie traditionelle Banden und unterscheiden sich nur durch die Daten, auf die sie es abgesehen haben. Unternehmen aller Größen, die im Bereich der nationalen Sicherheit beschäftigt sind oder großen wirtschaftlichen Einfluss besitzen, sollten mit hartnäckigen und fortgesetzten APT-Angriffen auf ihre Archive für E-Mails, Dokumente, geistiges Eigentum und andere Datenbanken rechnen. Dies gilt auch für Unternehmen, die nur zum Teil in diese Tätigkeitsfelder fallen, z. B. Wirtschaftsberatungsunternehmen, die Konzerne beim Aufbau von Präsenzen in anderen Ländern beraten.

Informationen zu den Autoren

Dieser Berichte wurde von Dmitri Alperovitch, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget und Craig Schmugar 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 des cloudbasierten Dienstes 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.

Über McAfee, Inc.

McAfee, Inc., mit Hauptsitz in Santa Clara, Kalifornien, ist der weltweit größte auf IT-Sicherheit spezialisierte Anbieter der Welt. 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. 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. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

17800rpt_threat-predictions_1110_fnl_ETMG