

Bedrohungsprognosen für 2012

McAfee® Labs™

Inhaltsverzeichnis

Bedrohungen für die Industrie	3
Bedrohung von innen: Eingebettete Hardware	4
Hacktivismus	4
Virtuelle Währungen	5
Internetkrieg	6
DNSSEC	7
Spam wird „legitim“	8
Bedrohungen für Mobilgeräte	9
Botnets + Rootkits = Bedrohungen auf niedriger Ebene	9
Mobile-Banking-Angriffe	9
Gefälschte Zertifikate	10
Fortschritte bei Betriebssystemen	10
Informationen zu den Autoren	11
Über McAfee Labs	11
Über McAfee	11

Wenn Sicherheitsunternehmen zukünftige Bedrohungen vorhersagen, hat das oft große Ähnlichkeit mit einem Glücksspiel. Es macht zwar Spaß, gelegentlich in die Glaskugel zu schauen und eine Prognose über den Verlauf der nächsten Monate zu erstellen, doch wer kann schon mit Sicherheit sagen, was sich von Jahr zu Jahr wirklich ändert? Die vergangenen 12 Monate waren durchaus von großen Entwicklungen gekennzeichnet, doch handelte es sich dabei eher um eine Revolution oder eine Evolution? Wir erlebten große Veränderungen bei Mobilgerätebedrohungen, Haktivismus, Client-seitigen Exploits, Ausnutzungen sozialer Medien sowie gezielten Angriffen. Diese Entwicklungen werden in den nächsten Jahren eine noch größere Rolle spielen.

Mit welchen Veränderungen rechnet McAfee Labs im kommenden Jahr? Wir gehen von verschiedenen neuen Szenarien sowie von bedeutsamen evolutionären Weiterentwicklungen selbst bei den etabliertesten Bedrohungsvektoren aus.

- Bedrohungen für die Industrie werden ausgereifter und spezialisierter
- Angriffe auf eingebettete Hardware werden umfassender und tiefergehender
- Haktivismus und Anonymous werden gestärkt und entwickeln sich weiter
- Virtuelle Währungssysteme erleben weiter gefasste und häufigere Angriffe
- Das neue Jahr wird das „Jahr für (nicht „der“) Internetkriege“
- DNSSEC führt zu neuen Netzwerk-Angriffsvektoren
- Herkömmlicher Spam wird „legitim“, während sich Spearphishing zu gezielten Messaging-Angriffen ausweitet
- Mobilgeräte-Botnets und -Rootkits werden ausgereifter und konsolidieren sich
- Gefälschte Zertifikate und illegale Zertifizierungsstellen untergraben das Vertrauen der Benutzer
- Fortschritte bei Betriebssystemen und Sicherheitsmaßnahmen werden die Entwicklung neuartiger Botnets und Rootkits antreiben

Die Karten liegen auf dem Tisch, gehen wir nun ins Detail!

Bedrohungen für die Industrie

Aus aktuellem Anlass erhalten Bedrohungen für industrielle und nationale Infrastrukturnetzwerke in letzter Zeit besondere Aufmerksamkeit. Schließlich ist dies einer der wenigen Bereiche, in denen Internetangriffe echte Schäden oder den Verlust von Menschenleben nach sich ziehen können. SCADA-Industriesysteme (Supervisory Control and Data Acquisition, Systeme zur Überwachung, Steuerung und Datenerfassung) sind genauso gefährdet wie jedes andere vernetzte System. Der große Unterschied besteht jedoch darin, dass viele dieser Systeme nicht für die Netzwerkumgebungen entwickelt wurden, in denen sie immer häufiger eingesetzt werden. Die zunehmende Interkonnektivität von Systemen und Geräten, die niemals für diese Zugangsart ausgelegt wurden, schreit geradezu nach Ärger. Das ist vor allem deshalb dramatisch, weil SCADA-Systeme oft in Umgebungen eingesetzt werden, in denen keine Informationssicherheitstechnologien vorhanden sind. Kritische Infrastruktursysteme werden offenbar häufig an das Internet angeschlossen und mit handelsüblicher Software verwaltet. Jede Software besitzt Schwachstellen, doch IT-Industrieleitsysteme erfordern größere Sorgfalt bei Architektur, Design und Implementierung. Die Angreifer werden diese Nachlässigkeit im kommenden Jahr immer häufiger und erfolgreicher ausnutzen – und sei es nur für Drohung und Erpressung. Angesichts der Ziele vieler Haktivisten-Gruppen lohnt es sich, *ernsthaft* über mögliche Auswirkungen auf Industrieleitsysteme nachzudenken.

Stuxnet ist der beste Beweis dafür, dass böswilliger Code reale, spürbare Auswirkungen haben kann.¹ Die kürzlich stattgefundenen Vorfälle bei Wasserversorgern in den USA zeigen, dass diese Einrichtungen für Angreifer zunehmend von Interesse sind. Je mehr Aufmerksamkeit SCADA und den Infrastruktursystemen zuteil wird, desto größere Sicherheitsschwachstellen kommen zutage. Wir erwarten, dass diese fehlende Sicherheit zu größeren Bedrohungen durch Exploit-Toolkits und -Frameworks sowie zu häufigeren Angriffen auf Versorger – und insbesondere die Leitsysteme von Stromanbietern – führen wird. Sobald ein angegriffener Bereich eine Schwachstelle zeigt, werden die Angreifer gnadenlos zuschlagen.

Angreifer konzentrieren sich meist auf Systeme, die erfolgreich kompromittiert werden können. Industrieleitsysteme haben sich als Umgebung mit einer reichen Auswahl leichter Beute erwiesen. Die zuständigen Administratoren sollten aus den jüngsten Ereignissen ihre Lehren ziehen. Es ist an der Zeit, umfassende Penetrationstests durchzuführen und Notfallreaktionspläne einzuführen, die alle Internetkomponenten und Netzwerkgeräte abdecken und auch die Strafverfolgungsbehörden vollständig einbinden. Sie müssen sich fragen: Was geschieht, wenn wir angegriffen werden?

Bedrohung von innen: Eingebettete Hardware

Die Beliebtheit und Bedeutung eingebetteter Systeme hat in den vergangenen Jahren zugenommen. Diese Systeme werden im Allgemeinen für eine bestimmte Kontrollfunktion innerhalb größerer Systeme entwickelt und müssen ihre Aufgaben häufig in Echtzeit erfüllen. Meist sind sie Bestandteil eines kompletten Geräts, das aus Hardware und anderen mechanischen Teilen besteht. Bisher wurde diese Architektur im Industriebereich eingesetzt, beispielsweise in der Luftfahrtelctronik, dem Transportsektor sowie bei Energieversorgern, aber auch im Automobilbereich und in medizinischen Geräten. Die Technologie erobert jedoch immer mehr Unternehmens- und Privatkundenbereiche. So nutzen GPS, Router sowie Netzwerkbrücken und – seit Neuestem – auch Verbrauchergeräte eingebettete Funktionen und Geräte.

Zur Ausnutzung eingebetteter Geräte ist Malware erforderlich, die auf Hardware-Ebene angreift. Das Wissen, das hinter erfolgreichen Angriffen steckt, hat auch Auswirkungen, die über eingebettete Plattformen hinausgehen.

Malware-Autoren entwickeln zunehmend Malware, die auf die tiefer gelegenen Ebenen des Betriebssystems zugreift. Vielfach versuchen die Angreifer, ein System auf der untersten Ebene („Root“) anzusprechen. Dazu gehören der Master Boot Record und sogar das BIOS. Wenn Angreifer Code einschleusen können, der die Boot-Reihenfolge oder die Ladereihenfolge des Betriebssystems verändert, erhalten sie umfassendere Kontrolle und können langfristigen Zugang zu System und seinen Daten aufrecht erhalten. Die Kontrolle über die Hardware ist das gelobte Land kompetenter Hacker.

Durch diese Entwicklung werden Systeme mit eingebetteter Hardware für diese Art von Angriffen anfälliger. Uns ist Konzept-Code bekannt, der die eingebettete Hardware von Automobil-, Medizin- und Versorgungssystemen angreift. Solcher Proof-of-Concept-Code wird in den nächsten Jahren wahrscheinlich effektiver.

Hacktivismus

Obwohl Hacktivismus beileibe kein neues Phänomen ist, erlangte er im Jahr 2010 dank der Medienpräsenz von WikiLeaks größere Bekanntheit, Akzeptanz und Verwendung als je zuvor. Insgesamt war 2011 ein gemischtes Jahr für Online-Aktivisten, da einzelne Akteure vielfach gegeneinander arbeiteten und oft klare Ziele fehlten. Häufig war es alles andere als einfach, politisch motivierte Kampagnen und die Albernheiten von Skript-Kiddies auseinander zu halten. Eines wurde jedoch schnell klar: Wenn Hacktivismus ein Ziel auswählten, wurde es durch einen Dateneinbruch oder eine Denial-of-Service-Angriff kompromittiert. Deshalb sollten diese Gruppierungen ernstgenommen werden. Ganz gleich, ob man mit ihren Zielen einverstanden ist oder nicht, Anonymous und andere Hacktivismus-Gruppen haben sich bei der Wahl ihrer Ziele und Vorgehensweisen als zielstrebig, einfallsreich und flexibel erwiesen.

Das kommende Jahr wird für den Hacktivismus entscheidend sein. Dabei werden die Geschichten um Anonymous nur eine Seite dieser Medaille darstellen.

- Das „echte“ Anonymous (also der historische Kern) wird sich entweder neu ordnen oder eingehen. Wenn sich die einflussreichen Kreise innerhalb der Anonymous-Bewegung nicht durch konzertierte und verantwortungsbewusste Aktionen organisieren können, laufen alle, die sich als Anonymous ausgeben, letztendlich Gefahr, marginalisiert zu werden. Wir rechnen in jedem Fall mit einer starken Zunahme solcher Angriffe. Politisch motivierte DDoS-Angriffe (Distributed Denial-of-Service) und Kompromittierungen persönlicher Daten werden weiter zunehmen.
- Die Menschen, die digitale Störungen initiieren, werden besser mit den Initiatoren von physischen Demonstrationen verbunden sein. Wir werden erleben, wie Social-Media-Hacktivismus immer häufiger mithilfe von Social Media koordiniert wird. Wir erwarten in Zukunft viele Operationen, die physische und digitale Komponenten vereinen. Gemeinsame und koordinierte Aktionen in der Real- und Online-Welt werden gleichzeitig geplant. Es fällt nicht schwer, sich die Evolution der Occupy-Bewegung und anderer Protestgruppen hin zu direkten digitalen Aktionen vorzustellen. Wie wir bereits bei anderen Vorhersagen deutlich gemacht haben, ist das Umschwenken von Hacktivismus auf Industrielleit- oder SCADA-Systeme eine sehr reale Möglichkeit. Wir erwarten, dass Hardliner unter den Hacktivismus, die die Occupy-Bewegung unterstützen, sich bald von der Anonymous-Bewegung freimachen und eigenständig als „Cyberoccupiers“ auftreten.
- Aus politischen und ideologischen Gründen wird das Privatleben öffentlicher Personen wie Politiker, Unternehmensführer, Richter sowie Strafverfolger und Sicherheitsbeamter im neuen Jahr öfter als bisher öffentlich gemacht. Die Protestierenden werden sich kaum aufhalten lassen, wenn es darum geht, Daten von sozialen Netzwerken oder Web-Servern zu erlangen, um ihre unterschiedlichen Aktionen zu unterstützen.

- Einige Hacktivismus werden sich der gleichen Mittel bedienen wie „Internetarmeen“, die vor allem in nicht-demokratischen oder religiös geprägten Staaten gedeihen. Dazu zählen die iranische sowie die pakistanische Internetarmee und die chinesische Honker-Gruppe. Nachdem sie in den vergangenen zwei Jahren mit Verunstaltungen auf sich aufmerksam gemacht haben, werden sich diese Armeen im neuen Jahr immer öfter auf Unterbrechungsaktionen konzentrieren. Einige dieser Gruppen werden einander bekriegen und dabei möglicherweise Schäden verursachen, die noch nicht abzuschätzen sind (beispielsweise Palästinenser gegen Israelis, Inder gegen Pakistaner, Nordkoreaner gegen Südkoreaner). Im Jahr 2011 gingen Gerüchte um, dass Internetarmeen von den jeweiligen Regierungen gesteuert oder unterstützt würden. Totalitäre Staaten werden im nächsten Jahr noch weiter gehen und die Aktionen ihrer Internetarmeen offen gutheißen.

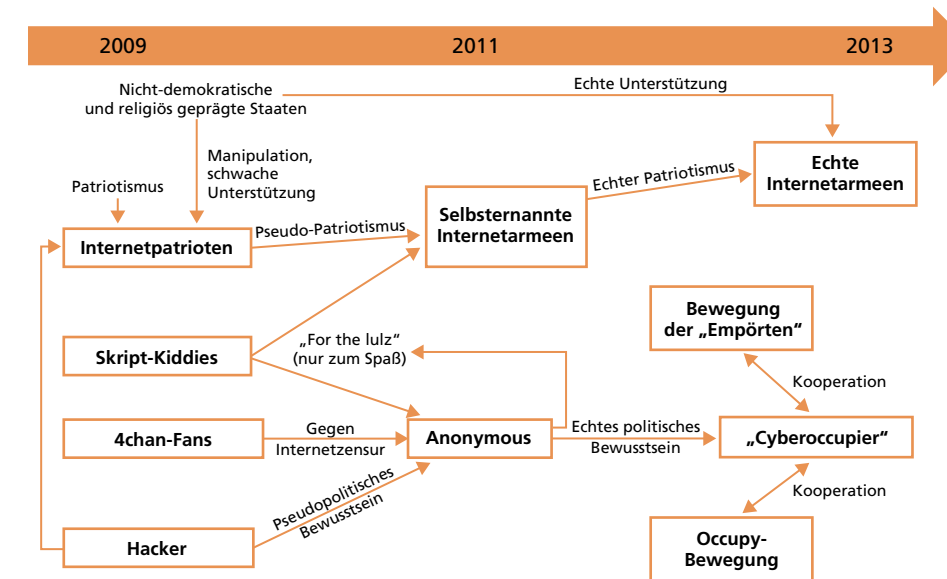


Abbildung 1. Die verschiedenen Verbindungen und Motivationen von Hacktivismus.

Virtuelle Währungen

Virtuelle Währungen, sogenannte Internetwährungen, werden immer häufiger für den Online-Transfer von Geld genutzt. Obwohl dieses Geld nicht von greifbaren Ressourcen oder Waren gestützt wird, können Benutzer dank Diensten wie Bitcoin mithilfe eines dezentralisierten Peer-to-Peer-Netzwerks Transaktionen durchführen. Im Grunde genommen handelt es sich dabei also um elektronisches Geld, das für direkte Zahlungen im Internet genutzt werden kann. Nutzer benötigen lediglich eine Client-Software sowie einen Online-Geldbörsendienst, um die „Coins“ (Münzen) zu empfangen, die in der Geldbörse gespeichert und als Bezahlung für Waren oder Dienstleistungen übertragen werden können. Zum Versand und Empfang dieser Coins ist nur eine Geldbörsen-Adresse erforderlich. Sehen Sie das Problem und die Möglichkeiten?

Trojaner-Malware fügt sich nahtlos in diese Architektur ein. Da die Geldbörsen nicht verschlüsselt und die Transaktionen öffentlich sind, sind sie für Internetkriminelle außerordentlich interessant. Im Jahr 2011 fanden mehrere Ereignisse im Umfeld von virtuellen Währungen statt:

- Die Mt. Gox Bitcoin Exchange-Datenbank wurde von Kriminellen angegriffen, die tausende Bitcoins erbeuteten.
- Es wurde Spam mit Werbung für gefälschte Bitcoin-Mining-Tools (Programme zur Bitcoin-Generierung) verbreitet. Diese Tools enthielten in Wirklichkeit Malware, die die Geldbörsen-Dateien der Opfer an eine Internetadresse sendete. Auf diese Weise konnten andere Miner die infizierten Computer zur Generierung weiterer Bitcoins missbrauchen.
- Es wurden aktive Bitcoin-Miner-Botnets entdeckt. Durch die Nutzung unzähliger infizierter Computer konnten diese Botnets das Mining (Generieren) von Bitcoins beschleunigen und zudem noch DDoS-Angriffe durchführen.

Virtuelle Währungen und Technologien wie Bitcoin haben konzeptionelle Eigenschaften, die sie zu einem verlockenden Ziel für Internetkriminelle machen. Im Jahr 2011 registrierten wir erhebliches Wachstum bei Malware, die diese Technologien angreift. In dieser Grafik finden Sie eine Übersicht von Bitcoin-Malware:

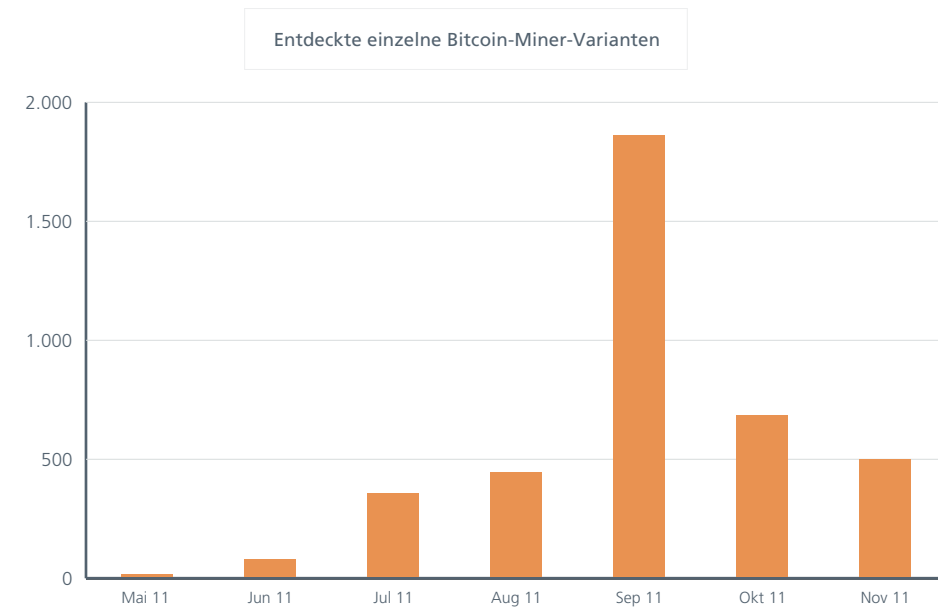


Abbildung 2. Das Stehlen (Mining) der virtuellen Währung Bitcoin erreichte im September seinen Höhepunkt. Wir gehen davon aus, dass diese Betrugsmasche 2012 zunehmen wird.

Diese Art von Bedrohung wird sich wahrscheinlich zu einer internetkriminellen Heimindustrie entwickeln, wobei für den Diebstahl virtueller Währungen Spam, Datendiebstahl, Tools, Support-Netzwerke sowie andere Dienste zum Einsatz kommen. Internetkriminelle haben also ein Bezahlungssystem gefunden, das ihnen entgegen kommt.

Internetkrieg

Wird 2012 das „Jahr des Internetkriegs“ sein, oder lediglich die Macht und das Potenzial offensiver Internetwaffen demonstrieren? Es ist natürlich zu hoffen, dass höchstens der letztere Fall eintritt. Doch die Entwicklung der letzten Jahre deutet darauf hin, dass ein ausgewachsener Internetkrieg nur noch eine Frage der Zeit ist. Wir erleben häufig, dass Internettechniken die traditionellen Geheimdienst- oder Spionage-Operationen ergänzen, wobei viele der Akteure einander beschuldigen und dabei nicht zwischen Verbündeten und Gegnern unterscheiden. Internetspionage ist billig, lässt viele Möglichkeiten zum Abstreifen einer Mittäterschaft offen, gefährdet keine Menschenleben und – viel wichtiger – scheint höchst effektiv zu sein. Bislang beobachteten wir nur wenige Einsätze von Internetwaffen als Teil eines bewaffneten Konflikts. Solche Angriffe erfolgten in einem relativ kleinen Rahmen und mit geringer Raffinesse, beispielsweise während des Georgien-Konflikts.

Die Situation hat sich jedoch geändert. Viele Länder erkennen das Bedrohungspotenzial von Internetangriffen auf wichtige Infrastrukturen sowie die Schwierigkeiten eines zuverlässigen Schutzes. Dieses Bedrohungspotenzial eröffnet kleinen Ländern oder Organisationen Angriffsmöglichkeiten und ist vor allem dann interessant, wenn sich keine Ziele für einen Gegenangriff bieten. Der Stuxnet-Angriff änderte in vielerlei Hinsicht die Spielregeln. So beseitigte er jegliche Zweifel daran, dass die Bedrohung real ist und gravierende Auswirkungen haben kann.

Die USA haben ihre Verwundbarkeit vermutlich besser als jedes andere Land erkannt. Dies liegt zum Teil sicherlich am massiven Einsatz von Computersystemen und einer Internetverteidigung, die sich in erster Linie auf Regierungs- und Militärnetzwerke konzentriert. (Stellen Sie sich einmal eine Armee vor, die lediglich andere Militärbasen schützt, anstatt den Schutz des gesamten Landes zu gewährleisten.) Nachdem aufgrund des Fehlens entsprechender Strategien scharfe Kritik laut geworden war, reagierte der Staat endlich.

Im Juli veröffentlichte das Department of Defense Strategy for Operating in Cyberspace (US-Verteidigungsministerium ein Strategiepapier zu Internetfragen).² Der Bericht besagt Folgendes (Anm. d. Übers.: frei übersetzt): „Strategische Initiative 1: Das Verteidigungsministerium betrachtet das Internet als Medium, in dem es sich organisiert, Schulungen durchführt und ausrüstet, sodass es das Potenzial des Internet vollständig nutzen kann.“ Sie werden jedoch in diesem Papier ein bestimmtes zuvor diskutiertes Thema vergeblich suchen: dass Internetangriffe ab einem bestimmten Schweregrad mit einem Gegenangriff beantwortet werden. Stattdessen bereitet das US-Verteidigungsministerium eine neue Richtlinie zur Ergänzung der bisher geltenden Internetstrategie vor, die konkrete Vorgehensweisen für das für Internetkriegsführung zuständige Personal enthält. Selbst wenn diese Richtlinie bestimmt, unter welchen Umständen eine Reaktion im Internet erfolgt, sind wir noch weit von der „drohenden Massenvernichtung“ entfernt, die im Kalten Krieg als Möglichkeit angesehen wurde.

Niemand wird von einem Angriff abgehalten, wenn die möglichen Gegenreaktionen aufgrund der Geheimhaltung unbekannt sind.

Laut Medienberichten wurde der Einsatz von Internetwaffen bei der Revolution in Libyen zwar erwogen, letztendlich jedoch aufgrund der unvorhersehbaren Auswirkungen abgelehnt. Vielleicht boten sich aber einfach nicht genügend attraktive Ziele an. Zumindest bisher kennen wir keine öffentliche Demonstration offensiver Internetkriegsführung, die Schäden anrichten kann. Es werden jedoch immer mehr Stimmen laut, die eine Veröffentlichung solcher Informationen fordern. Wir müssen also damit rechnen, dass eine wie auch immer geartete Demonstration (die mehr beinhaltet als Videos von lahmgelegter Technik, die ausländischen Diplomaten vorgeführt werden) stattfinden wird. Gleichzeitig kann eine effektive Demonstration der Auslöser für andere Staaten sein, zu Abschreckungszwecken ihre eigenen offensiven Möglichkeiten vorzuführen.

Wir hoffen, dass das kommende Jahr höchstens Demonstrationen anstelle echter Vorfälle von Internetkriegsführung bringen wird!

DNSSEC

Bei DNSSEC (Domain Name System Security Extensions, Domain Name System-Sicherheitserweiterungen) handelt es sich um eine Technologie zum Schutz von Namensauflösungsdiensten vor Spoofing und Cache Poisoning (Speicherfälschung), indem ein „Vertrauensnetz“ auf Grundlage von Kryptographie mit öffentlichen Schlüsseln eingesetzt wird. Auf diese Weise sollen Client-Computer vor der unbeabsichtigten Kommunikation mit einem Host durch einen Man-In-The-Middle-Angriff geschützt werden, bei dem der Verkehr vom Ziel-Server (z. B. Webseite oder E-Mail) auf einen anderen Server umgeleitet wird. Diese Maßnahme ist ein wichtiger Schritt in der Entwicklung des Internet: Sie dient dem Schutz der Internetnutzer und legt Hackern größere Hürden in den Weg.

Allerdings verhindert DNSSEC auch, dass Behörden Internetverkehr zu Webseiten, die illegale Software oder Medien bereitstellen, manipulieren oder umleiten können. Wenn eine Regierung die Absicht hätte, Datenverkehr umzuleiten, müsste diese Maßnahme von Root-Domänen anerkannt werden. Diese Art von Vertrauen wird spätestens dann entzogen, wenn die zuständigen Stellen den Verdacht hätten, dass Inhalte aufgrund von Partikularinteressen ausländischer Regierungen unterdrückt werden sollen.

Aktuelle Gesetzgebungsvorhaben zur Verhinderung der Verbreitung geistigen Eigentums basieren auf dem Modell heutiger DNS-Dienste, berücksichtigen jedoch nicht das zukünftige DNSSEC. Diese Diskrepanz kann zu weiteren Anforderungen an die Verwaltung der aktuellen DNS-Infrastruktur führen, die möglicherweise nicht mit der DNSSEC-Infrastruktur kompatibel sind. Sollten diese Anforderungen implementiert werden, könnte die Aufwertung der Sicherheit unserer DNS-Infrastruktur blockiert werden, während Expertengremien einen Mittelweg zwischen rechtlichen Vorgaben und DNSSEC zu finden versuchen.

Wenn Regierungsstellen auf der ganzen Welt ihr Interesse für die Festlegung von „Straßenverkehrsregeln“ auf der Datenautobahn entdecken, müssen wir damit rechnen, dass zukünftige Lösungen durch juristisches Tauziehen um gestrige Probleme gebremst werden. Dadurch würde das Internet von morgen sehr stark dem Internet der Vergangenheit ähneln – eine Aussicht, die vor allem Sicherheitsexperten nicht begeistert.

Spam wird „legitim“

In den vergangenen vier Jahren konnten wir zunehmend internationale Abmachungen und Kooperationen beim Kampf gegen Botnet-Spam beobachten. Diese Kooperation führte zu zahlreichen weithin beachteten Abschaltungen von Infrastruktur zur Botnet-Steuerung (wie dem Zugangsanbieter McColo), zum Web-Hosting von Spam-Domänen (Glavmed), zur Verarbeitung von Kreditkartendaten im Zusammenhang mit gefälschten Medikamenten und außerdem zu Gerichtsverfahren gegen große Internet-Unternehmen, die Werbung für illegale Angebote schalteten. Aufgrund dieser Aktionen ging das weltweite Spam-Aufkommen Mitte 2009 dramatisch zurück und trieb die Schwarzmarkt-Kosten für den Spam-Versand über Botnets in die Höhe.

Obwohl diese Maßnahmen – anders als von einigen Experten erwartet – Spam natürlich nicht endgültig den Riegel verschieben werden, ändern sie die Lage doch erheblich. Mittlerweile sehen wir immer mehr unerwünschte Spam-E-Mails, die nicht von Botnet-Hosts, sondern von „legitimen“ Werbeagenturen versendet werden, die von der Anti-Spam-Community heftig abgelehnte Techniken einsetzen. Dabei gelangen die E-Mail-Adressen von Internetnutzern ohne deren Wissen oder Einverständnis auf Werbungs-Mailinglisten. Zu den Vorgehensweisen gehört der offene Kauf von E-Mail-Adressenlisten, bei dem die enthaltenen Adresseninhaber angeblich dem Erhalt von Werbung zugestimmt hätten – eine äußerst fragwürdige Behauptung. Eine andere Möglichkeit bietet das „E-Pending“. Hierbei werden mithilfe von Algorithmen die E-Mail-Adressen von Benutzern gesucht, die sich wahrscheinlich für Werbung registrieren würden. Anschließend werden diese Benutzer ohne ihre vorherige Zustimmung in die Liste aufgenommen. Attraktiv ist auch der Kauf von Kundendatenbanken von Unternehmen, die den Geschäftsbetrieb eingestellt haben. Dabei werden einstmals geltende Datenschutzregelungen schlichtweg ignoriert. Nicht zu vergessen wäre zudem noch eine „Partnerschaft“ mit anderen Werbeagenturen oder Mailinglisten-Anbietern, um an deren E-Mail-Listen zu gelangen.

Den Werbeagenturen, die diese Maßnahmen einsetzten, ist natürlich bewusst, dass sie Spam versenden. Aus diesem Grund setzen sie die gleichen Techniken ein wie Botnet-Betreiber, um einer Entdeckung zu entgehen. Täglich werden Tausende neuer E-Mail-Domänen registriert, wobei Datenschutzeinstellungen getroffen werden, die eine Identifikation der Besitzer verhindern. Gleichzeitig werden für wenige Stunden Tausende neuer IP-Adressen in den Subnetzen von Hosting-Anbietern aktiviert, und Spam-Kanonen beschließen die Posteingänge von Internetnutzern mit schlecht formatierten E-Mails voller Rechtschreib- und Grammatikfehler. Die meisten E-Mails enthalten einen Abmeldelink, der nur eine Aufgabe hat: die Spammer wissen zu lassen, dass Ihre E-Mail-Adresse aktiv ist und Sie die E-Mail gelesen haben. Außerdem gibt es meist noch eine Postadresse, an die Sie eine schriftliche Aufforderung schicken können, um sich aus der Liste austragen zu lassen. Wenn Sie diese Postanschrift jedoch nachschlagen, werden Sie feststellen, dass es sich meist um eine Adresse in der Wildnis Kanadas oder in der Wüste Arizonas handelt. In einigen Fällen erhielten einzelne E-Mail-Adressen innerhalb eines Tages mehr als 9.000 fast identische Spam-Nachrichten mit Werbung für eine wunderheilsame magnetische Kette.

Diese Praktiken werden tatsächlich vom Gesetz geschützt. Das US-Gesetz CAN-SPAM wurde so weit verwässert, dass Werbetreibende für den Versand von Werbung kein Einverständnis der Empfänger mehr benötigen. Da Werbung erheblichen Profit verspricht und darum auch eine starke Lobby hinter sich hat, ist es sehr unwahrscheinlich, dass diesen Praktiken so bald ein Riegel vorgeschoben wird.

Wir gehen davon aus, dass „legalisierter“ Spam unter diesen Bedingungen auch weiterhin mit alarmierender Geschwindigkeit zunehmen wird. Es ist billiger und weniger riskant, Internetnutzer über eine Werbeagentur mit Spam zu belästigen, als ein Botnet einzusetzen. Diese Aktivitäten, die auch als Snowshoe Spamming (Schneeschuh-Spam) bekannt sind, haben derart zugenommen, dass zum Zeitpunkt der Erstellung dieses Berichts die 10 häufigsten Spam-E-Mails eine Benachrichtigung über den Zustellstatus, eine Botnet-Spam-Nachricht für gefälschte Rolex-Uhren, einen Nigeria-Betrug und ganze sieben Snowshoe-Spam-Nachrichten umfassten. Solcher Datenverkehr wird schneller wachsen als Phishing und Nigeria-Betrug, während Botnet-Spam zurückgehen wird, weil die Botnet-Betreiber bessere und sicherere Mittel und Wege finden werden, aus ihren Armeen ferngesteuerter Computer Profit zu schlagen. Es ist nur eine Frage der Zeit, bis der größte Teil des weltweiten Spam-Aufkommens von kriminell agierenden, aber technisch gesehen „legalen“ Unternehmen stammt.

Bedrohungen für Mobilgeräte

In den vergangenen zwei Jahren beobachteten wir eine Zunahme bei Angriffen auf Smartphones und Mobilgeräte. Dabei wurden Rootkits, Botnets und andere Malware eingesetzt. Die Angreifer schwenkten von destruktiver Malware auf Spyware und finanziell motivierte Malware um, die hohe Profite versprechen. Sie nutzten Schwachstellen aus, um Systemschutzmaßnahmen auszuhebeln und größere Kontrolle über die Mobilgeräte zu erlangen. Wir gehen davon aus, dass die Angreifer im Jahr 2012 ihren bisherigen Kurs fortsetzen und ihre Angriffe vervollkommen werden. Außerdem rechnen wir mit einer Konzentration auf Mobile-Banking-Angriffe.

Botnets + Rootkits = Bedrohungen auf niedriger Ebene

Auf PCs blenden Rootkits und Botnets Werbung ein und stehlen ihren Opfern Geld. Auch auf Mobilgeräten werden diese Malware-Formen für diesen Zweck eingesetzt. Rootkits ermöglichen die Installation zusätzlicher Software oder Spyware, und Botnets können Werbungs-Klicks generieren oder Premium-SMS versenden.

Wir kennen Mobilvarianten von Malware-Familien wie Android/DrdDream, Android/DrdDreamLite und Android/Geinimi sowie Android/Toplank und Android/DroidKungFu. Einige dieser Malware-Varianten setzen Root-Exploits – die einst dazu entwickelt wurden, Benutzern das Entsperren ihrer eigenen Smartphones zu ermöglichen – dazu ein, Zugriff auf und die Kontrolle über die Telefone ihrer Opfer zu erlangen. Im kommenden Jahr werden Entwickler und Forscher neue Methoden zum Rooting von Telefonen austüfteln und Malware-Autoren die Lektionen, die sie bei der Entwicklung von PC-Malware gelernt haben, für umfangreichere Angriffe auf Mobilgeräte-Hardware nutzen. PC-basierte Malware bewegt sich zunehmend zu den unteren Ebenen des Betriebssystems, bis auf die Hardware-Ebene. Es ist damit zu rechnen, dass die Entwicklung bei Mobilgeräte-Malware in die gleiche Richtung geht.

Bootkits, also Malware-Formen, die Systemstartfunktionen ersetzen oder umgehen, bedrohen auch Mobilgeräte. Obwohl das Rooten des eigenen Telefons oder eBook-Lesegeräts weitere Funktionen ermöglicht oder das Ersetzen des Betriebssystems erlaubt, können Angreifer darüber auch ihr eigenes verändertes Betriebssystem laden. Während ein Mobilgeräte-Rootkit nur das Betriebssystem verändert, um einer Entdeckung zu entgehen, kann ein Bootkit dem Angreifer erheblich größere Kontrolle über ein Gerät ermöglichen.

Das Toolkit „Weapon of Mass Destruction“ für Penetrationstests von Mobilgeräten ist auf alten Windows Mobile-Telefonen lauffähig. WMD installiert sich selbst mithilfe von Tools, die zum Laden von Linux auf Windows Mobile-Telefonen entwickelt wurden und den Benutzern den Start des originalen Betriebssystems erlauben. Die Angreifer haben bereits alte Root-Exploits zum Verbergen verwendet. Wenn neue Exploits entwickelt werden, können die Angreifer irgendwann ihre eigene angepasste Firmware installieren.

Mobile-Banking-Angriffe

PC-Benutzer kennen bereits Angriffe von Kriminellen, bei denen mithilfe der Crimeware-Kits Zeus und SpyEye Geld von Online-Banking-Konten gestohlen werden soll. Sowohl Zeus als auch SpyEye setzen mittlerweile Mobilgeräte-Apps als Unterstützungsprogramme ein, um die zweistufige Authentifizierung zu umgehen und Zugriff auf das Geld des Opfers zu erlangen.

Zitmo (Zeus-in-the-Mobile) und Spitmo (SpyEye-in-the-Mobile) sind zwei Familien von Mobilgeräte-Spyware, die SMS-Nachrichten an die Angreifer weiterleiten. Beim Einsatz dieser Spyware mussten sich die Angreifer manuell anmelden, um das Geld des Benutzers zu stehlen.

Im vergangenen Juli diskutierte der Sicherheitsforscher Ryan Sherstobitoff über Möglichkeiten zur Erfassung der Aktionen, die Kriminelle mithilfe von Zeus und SpyEye durchführten – schließlich glichen diese in keinster Weise den Aktionen legitimer Nutzer. Im vergangenen Monat demonstrierte er, wie sehr sich die Kriminellen angepasst haben und ihre Opfer mittlerweile programmunterstützt bestehlen können, während diese noch angemeldet sind. Auf diese Weise täuschen die Kriminellen vor, dass ihre Aktionen vom legitimen Benutzer stammen. Durch eingebaute Verzögerungen erscheinen die Eingaben wie von einem echten Menschen getätigt. Die Angreifer haben sich schnell an Veränderungen angepasst, die die Sicherheit von Online-Banking auf PCs verbessern sollen. Da wir unsere Mobilgeräte immer öfter auch für Finanztransaktionen nutzen, können wir damit rechnen, dass Angreifer den PC ignorieren und sich direkt auf Mobile-Banking-Apps konzentrieren werden. Angriffe, die solche programmgesteuerten Techniken, werden wahrscheinlich immer häufiger auftreten, da Anwender ihre Finanzen zunehmend über ihre Mobilgeräte verwalten.

Gefälschte Zertifikate

Wenn Dateien und Dokumente digital signiert wurden, halten wir sie meistens für echt – schließlich wurden sie mit digitalen Signaturen von Zertifizierungsstellen signiert. Viele Whitelist- und Anwendungskontrollsysteme können ohne gültige digitale Signaturen nicht funktionieren. Dank dieser Lösungen können wir Richtlinien und Kontrollen für Dienste, Anwendungen und sogar Dateien mit digitaler Signatur einrichten. Sicheres Web-Browsen und geschützte geschäftliche Transaktionen sind ebenfalls von vertrauenswürdigen digitalen Signaturen abhängig. Diese Zertifizierungsstellen und ihre Zertifikate bestätigen dem Betriebssystem im Grunde genommen, dass dieses ihnen vertrauen kann, da sie gültig und überprüft sind.

Wenn wir dieser Technologie so viel Vertrauen entgegen bringen, welche Auswirkungen hätten dann nicht autorisierte oder gefälschte digitale Zertifikate? Mehr noch: Welche Implikationen hätte die Kompromittierung einer Zertifizierungsstelle? Dank digitalen Zertifikaten können wir Dateien, Prozessen oder Transaktionen ein gewisses Vertrauen entgegen bringen. Durch die Erstellung und Verbreitung gefälschter oder nicht autorisierter Zertifikate können Angreifer Aktionen durchführen, die durch fast nichts erkennbar sind. Im Browser werden damit Man-in-the-Middle-Angriffe möglich. Dabei wird normalerweise verschlüsselter und für den Angreifer unsichtbarer Datenverkehr für den Angreifer zum Klartext, da dieser den Schlüssel besitzt. Im Host ignoriert Sicherheits-Software Dateien, die mit einem gültigen Schlüssel signiert sind, da dieser nun zulässig zu sein scheint. Die Datei erhält aufgrund der vorgelegten Zertifikate Zugriff.

Bei aktuellen Angriffen mithilfe von Stuxnet und Duqu wurden nicht autorisierte Zertifikate eingesetzt, um die Entdeckung zu verhindern. Obwohl wir dieses Verhalten nicht zum ersten Mal sehen (gefälschte Virenschutz-Software, einige Zeus-Varianten, Conficker und selbst einige alte Malware-Varianten für Symbian nutzen diese Technik), erwarten wir eine Zunahme dieses Trends für das Jahr 2012 und darüber hinaus.

Angriffe auf Zertifizierungsstellen, bei denen nicht autorisierte Zertifikate generiert werden sollen, stellen auch für die Zukunft eine Bedrohung dar – schließlich können Angreifer auf diese Weise unterschiedliche Schlüssel erstellen, die vielfach im Web und auf Hosts verwendet werden können. Dadurch wäre das Vertrauen in diese Technologie effektiv beschädigt. Wir machen uns große Sorgen über die Auswirkungen umfassender unauthorisierter Zertifikate für Whitelist- und Anwendungssteuerungstechnologien, die auf solchen Zertifikaten aufbauen. Die niederländische Zertifizierungsstelle DigiNotar, die bereits zuvor mit Problemen zu kämpfen hatte, meldete kürzlich Insolvenz an, nachdem ein Sicherheitseinbruch zur Ausstellung gefälschter Zertifikate geführt hatte. Bedeutete dieser Angriff das endgültige Aus? Untersuchungen ergaben, dass DigiNotar insgesamt 531 gefälschte Zertifikate ausgestellt hatte. Angesichts unseres zunehmenden Wissens um die Sicherheitslücken in dieser Branche ist der Niedergang des Unternehmens sehr wahrscheinlich nur der Anfang. Unsere Aufmerksamkeit muss nun der Beantwortung der Frage gehören, wie stark das Vertrauen beschädigt wurde.

Die großmaßstäblichen Angriffe auf Zertifizierungsstellen und die weit reichende Verwendung betrügerischer, aber dennoch gültiger digitaler Zertifikate haben Auswirkungen auf die Public-Key-Infrastruktur (PKI), sicheres Browsen und Transaktionen sowie hostbasierte Technologien wie Whitelisting und Anwendungssteuerung. Durch die Ausnutzung unseres Vertrauens in dieses System ziehen die Angreifer große Vorteile. Daher rechnen wir mit einer verstärkten Konzentration ihrer Bemühungen in diesem Bereich.

Fortschritte bei Betriebssystemen

Informationssicherheit bedeutet immer ein Geben und Nehmen sowie Maßnahmen und Gegenmaßnahmen. Die Angreifer schreiben böswilligen Code – wir finden ein Gegenmittel. Die Betriebssystemanbieter integrieren Sicherheitsfunktionen in den Betriebssystemkern – die Angreifer finden einen Weg, sie zu umgehen. Das ist der natürliche Kreislauf der dynamischen Bedrohungssituation, der uns stets begleiten wird. Wäre es jedoch möglich, dass die Fortschritte in der Informationssicherheitsbranche und bei den Betriebssystemherstellern die Malware-Autoren dazu treiben, das Betriebssystem zu umgehen und die Hardware direkt anzugreifen?

Aktuelle Windows-Versionen besitzen Funktionen zur Datenausführungsverhinderung sowie Funktionen zur zufälligen Vergabe von Adressbereichen (Address Space Layout Randomization). Diese Sicherheitsmethoden erschweren Angreifern die Kompromittierung der Computer ihrer Opfer. Der Schutz von Betriebssystemen wurde in den letzten Jahren auch durch Verschlüsselungstechnologien vorangetrieben. Wie bei den meisten internen Betriebssystem-Sicherheitsmaßnahmen fanden auch hier Angreifer schnell Mittel und Wege, diese Maßnahmen zu umgehen. Beim kommenden Windows 8 wird Microsoft viele neue Sicherheitsfunktionen integrieren. Dazu gehört der sichere Kennwortspeicher, sichere Boot-Funktionen, Malware-Schutzmaßnahmen sowie erweiterte Reputations-Funktionen. Wohin wird diese neue Sicherheitsarchitektur die Angreifer treiben?

Die Antwort ist: „Runter und raus“ – runter in die Hardware-Ebene und raus aus dem Betriebssystem.

In den vergangenen Jahren beobachtete McAfee Labs bei Angreifern und Malware-Autoren große Fortschritte in Bezug auf Rootkits und Bootkits. Mithilfe von Rootkits werden das Betriebssystem und die Sicherheitssoftware unterwandert, während Bootkits die Verschlüsselung angreifen und legitime Boot-Loader ersetzen können. Dabei handelt es sich um hochentwickelte Techniken zum Abfangen von Verschlüsselungsschlüsseln und Kennwörtern sowie zur Umgehung der Treibersignierung, die in manchen Betriebssystemen eingesetzt wird.

Angriffe auf Hardware und Firmware sind alles andere als trivial. Ein Erfolg versetzt die Angreifer jedoch in die Lage, Malware dauerhaft in Netzwerkkarten, Laufwerken und sogar im System-BIOS zu verankern. Im Jahr 2012 und darüber hinaus wird voraussichtlich mehr Energie in Hard- und Firmware-Exploits sowie ihre Realwelt-Entsprechungen investiert.

Die Fortschritte beim Windows 8-Bootloader führten bereits dazu, dass Sicherheitsforscher demonstrierten, wie diese Funktion mithilfe eines alten BIOS umgangen werden kann. Die Ironie dabei: Windows 8 ist noch nicht einmal erschienen. Angesichts der weiteren Entwicklungen rund um die einheitlichen erweiterbaren Firmware-Schnittstellenspezifikationen (EFI) von Intel, die als Software-Schnittstelle zwischen Betriebssystem und Plattform-Firmware fungieren und sicheres Booten sowie das veraltete BIOS ersetzen sollen, rechnen wir damit, dass noch mehr Angreifer ihre Energie in die Entwicklung von Umgehungsmaßnahmen investieren werden.

Wir werden weiterhin genau beobachten, wie Angreifer diese Funktionen auf niedriger Ebene zur Botnet-Steuerung ausnutzen und möglicherweise auf Funktionen im Grafikprozessor, BIOS oder gar Master Boot Record ausweiten. Gleichzeitig rechnen wir damit, dass Angreifer „neue“ Protokollstandards wie IPv6 nutzen, da sich die Netzwerkimplementierungen der Betriebssysteme weiterentwickeln.

Trotz unserer Bemühungen, den Aktivitäten der Angreifer entgegen zu wirken, sehen diese es als lohnend und Erfolg versprechend an, die Hardware anzugreifen und die ausgetretenen Wege bisheriger Betriebssystemangriffe zu verlassen.

Informationen zu den Autoren

Dieser Bericht wurde von Zheng Bu, Toralv Dirro, Paula Greve, David Marcus, François Paget, Ryan Perme, Craig Schugar, Jimmy Shah, Peter Szor, Guilherme Venere und Adam Wosotowsky von McAfee Labs vorbereitet und geschrieben.

Über McAfee Labs

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

Über McAfee

McAfee ist ein hundertprozentiges Tochterunternehmen der Intel Corporation (NASDAQ: INTC) und der weltweit größte auf IT-Sicherheit spezialisierte Anbieter. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer, ITK-Netze und Mobilgeräte auf der ganzen Welt vor Angriffen schützen und es den Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von der einzigartigen Global Threat Intelligence-Technologie entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. McAfee ist stets auf der Suche nach neuen Möglichkeiten, seine Kunden zu schützen.

<http://www.mcafee.com/de>



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

¹ <https://blogs.mcafee.com/mcafee-labs/stuxnet-update>

² Sie finden die frei zugängliche Version unter <http://www.defense.gov/news/d20110714cyber.pdf>.

Die hier enthaltenen Informationen werden McAfee-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern und werden wie besehen zur Verfügung gestellt, ohne Garantie oder Gewährleistung auf die Richtigkeit oder Anwendbarkeit der Informationen zu einem bestimmten Zweck oder für eine bestimmte Situation.

McAfee, das McAfee-Logo, McAfee Labs und McAfee Global Threat Intelligence sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind alleiniges Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2011 McAfee, Inc.

40302rpt_threat-predictions_1211_fnl_ETMG