

Ein gutes Jahrzehnt für Internetkriminalität

McAfees Rückblick auf zehn Jahre Internetkriminalität

Inhaltsverzeichnis

Einleitung	3
Ein Jahrzehnt Internetkriminalität	4
Internetkriminalität: Was kommt als Nächstes?	7
Top 5 Exploits – Verschiedene Zeitspannen von Internetkriminalität	9
Top 5 Scams – Die häufigsten Scams mit den meisten Opfern	9
Lexikon	10
Über McAfee	11

Einleitung

Trotz der weltweiten Rezession, der verbesserten Sicherheit und der internationalen Razzien ist Internetkriminalität im letzten Jahrzehnt gewachsen und Jahr für Jahr im zweistelligen Bereich angestiegen.

Um diesen Anstieg deutlich zu machen: Das vom FBI unterstützte Crime Complaint Center berichtete, dass sich Verluste für Verbraucher durch Internetkriminalität in den USA alleine von 2008 bis 2009 auf \$540 Mio. verdoppelt haben¹, während Beschwerden von Verbrauchern um mehr als 22 Prozent gestiegen sind. Es verwundert nicht, dass die Zahl an Beschwerden angestiegen ist, wenn man die Menge an heimtückischer Software bedenkt, der die Computer-Anwender gegenüberstehen, wenn sie online sind – von *Viren* und *Würmern* bis hin zu angeblicher Sicherheitssoftware. Tatsächlich entdeckte McAfee 2010 täglich durchschnittlich 60.000 neue *malware*-Programme. Viele dieser neuen Bedrohungen zielten auf die Stellen ab, an denen wir freizügiger sind und in Kontakt mit Freunden und Familie treten möchten - die sozialen Netzwerke. Aber leider haben Internetbetrüger auch dort ihre Krallen ausgefahren. McAfee² hat kürzlich berichtet, dass Malware, die über soziale Netzwerke verbreitet wird, heute schon die am schnellsten wachsende Gefahr im Internet ist.

Als wäre das noch nicht genug haben aktuelle Ereignisse darauf schließen lassen, dass Internetkriminalität ein neues Level an Reife und Verbreitung erreicht hat. Wir haben gezielte Angriffe gegen Regierungen und Organisationen gesehen, bei denen Internetkriminelle ihr Können nicht nur für Profit, sondern auch für Proteste eingesetzt haben. Ein aktuelles Beispiel für Online-Aktivismus oder auch „Hacktivismus“ von Hackern ist der Fall der Mediengruppe Wikileaks, die geheime Dokumente im Internet veröffentlicht. Die „Hacktivist“ haben eifrig Angriffe gestartet, um die Webseiten von Organisationen lahmzulegen, die ihrer Ansicht nach die kontroverse Nachrichtenplattform nicht unterstützen.

Wie sind wir also zu einer Welt gelangt, in der Proteste mittels Cyber-Krieg durchgeführt und Millionen³ von Internetnutzern Opfer von Online-Scams, Viren oder anderen Angriffen werden? Wo begann Internetkriminalität, und wo führt sie hin? Wir beantworten diese Fragen in „Ein gutes Jahrzehnt für Internetkriminalität“.

Ein gutes Jahrzehnt für Internetkriminalität

In den späten 90er Jahren formte Allen Pace, Angestellter bei Dunbar, einer Firma für Geldtransporte, einen Plan, der immer noch als größter Bargeldraub in der Geschichte der USA gilt. Pace, ein Sicherheitsinspektor bei Dunbar, nutzte seinen internen Zugriff zum Fotografieren und Ausforschen des Depots des Geldtransportunternehmens. Dann warb er fünf Freunde aus Kindertagen an, die ihm halfen, in die Einrichtungen von Dunbar in Los Angeles einzubrechen. Sie überfielen die Wachen aus dem Hinterhalt, durchstöberten einen Tresor und machten sich mit \$18,9 Mio. aus dem Staub. Zum Leidwesen von Pace konnten die Geldscheine auf das Verbrechen zurückgeführt werden. Er wurde festgenommen und zu 24 Jahren Haft verurteilt.

Heute müssen die erfolgreichsten Kriminellen ihr bequemes Zuhause nicht verlassen, um zehnmals größere Verbrechen als den Raub bei Dunbar zu begehen. Alles was sie brauchen ist eine Internetverbindung, etwas Technikverständnis und eine Menge an bösem Willen.

Nehmen wir das Beispiel von Albert Gonzalez, der mit einem Team an Hackern, genannt Shadowcrew, zwischen 2005 und 2007 in die Datenbanken von gut bekannten Einzelhandelsgiganten einschließlich TJ Maxx, Barnes and Nobles und BJ's Wholesale Club einbrach, um Zugriff auf mehr als 180 Millionen Geldkartenkonten zu erhalten. Es wird geschätzt, dass er und sein Team einen Schaden bei den Unternehmen von insgesamt mehr als \$400 Mio. an Entschädigungszahlungen, Gerichts- und Anwaltskosten verursacht haben.

Oder sehen wir uns den kürzlich aufgefliegenen „*scareware*“ -Ring an, der angebliche Sicherheitssoftware im Wert von \$180 Mio. an Nutzer verkauft hat, indem ihnen vorgegaukelt wurde, ihr Computer sei bedroht. Lesen Sie mehr über McAfees Bericht über Scareware [hier](#).

Diese Beispiele zeigen uns, dass wir uns zweifelsfrei in einer neuen Ära der Kriminalität befinden - einer Ära, in der erfolgreiche Betrüger *hunderte Millionen Dollar* einnehmen können mit weniger Risiko als bei konventionellen Verbrechen. Das ist die Ära der Internetkriminalität.

1. <http://scamfraudalert.wordpress.com/2010/03/13/fbi-2009-cybercrime-statistics/>

2. <http://www.mcafee.com/us/about/news/2010/q3/20100810-02.aspx>

3. Javelin Strategy's 2010 Identity Theft Survey

Was ist im letzten Jahrzehnt geschehen, dass sich das Aussehen der Kriminalität so dramatisch verändert hat? Zunächst einmal nahm die Internetnutzung im letzten Jahrzehnt nach einem langsamen Start in den 90ern explosionsartig zu. Der Anstieg belief sich auf das Fünffache - von 361 Millionen Nutzern im Jahr 2000 auf 2 Milliarden Nutzer im Jahr 2010⁴. Auch das Internet selbst ist hinsichtlich seiner Raffinesse und der Profitmöglichkeiten gewachsen. Mit seinem reichhaltigen Angebot an E-Commerce-Seiten, bezahlten Diensten und Online-Banking ist das Internet zu einer Schatzkammer voller Geld und Informationen geworden, die für Internetbetrüger unwiderstehlich ist. Auf einmal wurden Bank- und Kreditkarteninformationen von Milliarden von Menschen potentiell zugänglich für jene, die den richtigen Exploit oder Scam anwenden. Die Entstehung der Webseiten sozialer Medien später in diesem Jahrzehnt eröffnete Dieben, die auf Personen- und Identitätsinformationen zielen, weitere unglaubliche Möglichkeiten.

Während die Reize der Internetkriminalität exponentiell anwuchsen, so wuchsen auch die Fertigkeiten der Internetbetrüger. Technische Fortschritte haben es den Betrügern erlaubt, ihre Malware einfacher zu verbreiten und ihre eigenen Identitäten besser zu verbergen.

Für Internetnutzer war es ein Jahrzehnt aufregender Online-Fortschritte, die es ermöglichen, auf nie da gewesene Weise zu kommunizieren, sich auszudrücken und Geschäfte zu machen. Es war auch ein Jahrzehnt von steigenden Online-Gefahren, die unser Geld und unsere Identität gefährden.

Um die Landschaft der Internetkriminalität besser zu verstehen und zu sehen, wie sie sich entwickelt hat, wollen wir einen Blick zurück werfen auf das *Jahrzehnt der Internetkriminalität*.

Ein Jahrzehnt Internetkriminalität

2000–2003—Bekanntheit und persönliche Herausforderung

Nach der unspektakulären Lösung des Jahr-2000-Problems, suchten Internetbetrüger nach Wegen, die Aufmerksamkeit auf wahrhaftige Computerbedrohungen zu lenken – sich selbst. Sie gaben mit ihren Fertigkeiten an, indem sie populäre Webseiten wie z.B. CNN, Yahoo und Ebay zeitweise durch hohe Auslastungen außer Betrieb setzten. Das wird *Distributed Denial of Service (DDoS)-Angriff* genannt. Sie starteten auch umfassende Angriffe, um die Computer von Nutzern zu lähmen.

Eine beliebte Methode war das Versenden von Spam-Mails, die den Empfänger aufforderten, auf einen Link oder Anhang zu klicken, was zur Installation von Malware führte. Dies geschah im Jahr 2000 mit dem berühmten „I love you“-Wurm, der sich als Spam-Mail mit der Betreffzeile „I love you“ und einem Anhang, der behauptete ein „Liebesbrief für dich“ („love letter for you“) zu sein, verbreitete. Das war verführerisch genug, dass einige Millionen von Windows-Nutzern darauf hereinfielen.

Scammer lernten auch „Makroviren“ zu programmieren, die in gängigen Dokumenten wie Microsoft Word DOC-Dateien eingebaut werden konnten. Wenn der Nutzer die infizierte Datei einfach nur öffnete, startete der Virus automatisch.

Diese Angriffe gaben den Internetbetrügern die Aufmerksamkeit, nach der sie sich gesehnt hatten – Überschriften verkündeten lauthals Nachrichten von neuen Angriffen auf Webseiten und den neuesten schnell verbreiteten Viren – aber sie brachten nicht das große Geld, das Scammer in den folgenden Jahren im Auge hatten.

In der Zwischenzeit...

WLAN-Hotspots wurden attraktiv und digitale Musik wurde mit der Einführung des iPod und Musikdiensten wie Napster ein zentrales Medium.

Diese Fortschritte sollten Internetbetrügern später Möglichkeiten eröffnen, Informationen von Nutzern in ungesicherten Drahtlosnetzwerken zu stehlen. Sie brachten Nutzer auch dazu, gefährliche Dateien von Musik-Sharing-Services herunterzuladen, indem sie diese als In-Demand Songs deklarierten.

Bis 2009 stellte McAfee einen Anstieg um 40 Prozent bei Webseiten fest, die entweder infizierte MP3-Dateien lieferten oder Malware unter denen verbreiteten, die online nach MP3s suchten.

2004–2005—Der Reiz des Geldes und Professionalität

Bis dahin hatten Internet-Scammer ihre Fertigkeiten unter Beweis gestellt und es war an der Zeit, einen Schritt weiter zu gehen - vom Verursachen von Schäden zu wahrem Geldgewinn.

Eine smarte Wende vollzog sich mit der Einführung von *adware*, oder durch Werbung unterstützte Software, die Pop-ups automatisch öffnet oder Werbung auf den Computer des Nutzers herunterlädt, um ihn zum Kauf von Produkten oder Services zu bewegen. Zum Beispiel könnte ein Einkäufer, der online nach einer Autoversicherung sucht, ein Adware Pop-up erhalten, welches Werbung für ein Autoversicherungsunternehmen anzeigt und so versucht, den Nutzer zum Kauf dieser Versicherung zu verführen. Verbreiter von Adware förderten ihr Geschäft, indem sie ihre Software in so vielen Systemen installieren ließen, wie sie konnten. Eine Methode, die sie verwendeten, war das Pay-Per-Install-Model (Bezahlung pro Installation). Angreifer nutzten die Möglichkeit, verschiedene Adware-Pakete auf Millionen von Systemen zu installieren, während sie nebenbei dafür Schecks einsammelten.

Spyware, die aufzeichnet, welche Seiten wir besuchen oder erfasst, was wir eintippen, war eine weitere geläufige Bedrohung dieser Zeit. Sowohl mit Adware als auch mit Spyware zeigten die Internetkriminellen, dass es ihnen ernsthaft um Geldgewinn ging - und darum, unsere Privatsphäre auszuspienieren.

Ein weiterer bedeutsamer Fortschritt der Internetkriminalität zu dieser Zeit war die Entwicklung von Software, die vollen Zugriff auf einen Computer erhalten konnte, gleichzeitig aber vom eigentlichen Benutzer unerkannt blieb. Internetbetrüger nutzten diese Software, genannt *rootkits*, um Malware zu verstecken und sogar zu verhindern, dass sie durch Sicherheitschecks gefunden wurde. Mit diesem Trick konnten Internetbetrüger heimlich Passwörter und Kreditkarteninformationen stehlen und Viren verbreiten.

Andere Fortschritte hatten einen weitläufigeren Einfluss auf die allgemeine Sicherheit im Internet. Internetbetrüger konnten nun hunderte oder sogar tausende von Rechnern zur gleichen Zeit infizieren und sie aus der Ferne ohne das Wissen des Computernutzers steuern. Durch die Aktivierung einer Armee an sogenannten *Zombie-Computern* die ihren Befehlen blind gehorchten, hielten Cyber-Kriminelle eine enorme Rechnerleistung in der Hand, die sie verwendeten, um Angriffe auf andere Computer oder Webseiten zu starten oder Spam zu verbreiten. In beiden Fällen war das Ziel, Geld zu machen; entweder durch Erpresser-Mails (Bedrohung von Unternehmen, dass deren Computer und Webseiten angegriffen würden, wenn sie nicht zahlten) oder mittels Spam-Mails entstandener Verkäufe.

Tatsächlich sind botnets immer noch gängig - McAfee Labs™ berichtete 2010, dass es durchschnittlich sechs Millionen neue Botnet-Infizierungen jeden Monat registrierte und die spanische Polizei schaltete kürzlich ein Botnet mit Millionen von infizierten Computern ab. Es wurde angenommen, dass es sich dabei um das größte Botnet der Welt handelte. Das sogenannte Mariposa-Botnet war mit 13 Millionen eindeutigen Internet-Protokoll (IP)-Adressen verbunden, die zum Stehlen von Bankinformationen und DDoS-Angriffe genutzt wurden.

In der Zwischenzeit ...

Verletzungen von Kundendaten traten häufiger auf, da Internetkriminelle Datenbanken großer Unternehmen anzapften, um riesige Mengen an Kundeninformationen zu erhalten. Gleichzeitig begann der Diebstahl von Identitäten zu wachsen. Innerhalb von fünf Jahren sollte dies mit 1,1 Millionen betroffener Amerikaner ein Hauptproblem werden.

Facebook startete ebenso in dieser Zeit. Wie bei anderen Webseiten sozialer Netzwerke sollte es sich als ergiebiger Ort für Internetbetrüger herausstellen, an dem sie ihre Scams fortsetzen konnten.

2006–2008—Gangs und Diskretion

Als eine wachsende Geldmenge auf dem Spiel stand, begannen sich Internetkriminelle in Gangs zu organisieren. Einige hatten sogar eine Mafia-ähnliche Struktur mit bösartigen Hackern, Programmierern und Datenverkäufern, die Managern untergeben waren, die wiederum dem Boss untergeben waren, der für die Verbreitung von Malwarebaukästen im Internet verantwortlich war.

Um ihre wachsenden Unternehmensimperien zu schützen, gingen Angreifer diskreter mit ihren Methoden um, während sie nach wie vor mit ihrer technischen Klugheit angaben. Zum Beispiel nutzten Cyber-Betrüger ihre Fertigkeiten, um unbekannte Schwachstellen von Anwendungen zu finden. Dann versuchten sie diese Schwachpunkte auszunutzen, bevor sie ausgebessert werden konnten. Sie konnten Malware verbreiten oder sogar die komplette Kontrolle über die Computer der Nutzer übernehmen, indem sie einfach eine Sicherheitslücke, die der Hersteller der Software noch nicht geschlossen hatte, zu ihrem Vorteil nutzten.

Angriffe suchten auch nach Wegen, Software-Features für ihre eigenen Zwecke zu manipulieren. Zum Beispiel wurde ein Feature in der Microsoft Windows Software, genannt Autorun, entwickelt, um Programme von externen Geräten automatisch zu starten. Indem sie dieses Feature ausnutzten, konnten sie das führende Betriebssystem von Microsoft dazu bringen, bösartige Codes automatisch zu starten.

Durch die Ausnutzung von Software-Schwachstellen und von diversen anderen Features erhielten Internetkriminelle diskret Zugriff auf Nutzersysteme, während sie zur gleichen Zeit die normalen Software-Programmierer verhöhnten.

In der Zwischenzeit ...

Einzigartige Services wie Skype und Twitter starteten und boten Computer-Nutzern neue Wege in Kontakt zu bleiben und Daten auszutauschen. Zusammen mit Facebook sollte Twitter bald eine unwiderstehliche Plattform für Betrüger werden, um mit Nutzern zu interagieren und zu versuchen, Geld und Informationen von ihnen zu bekommen.

Das war auch die Zeit, als das iPhone auf den Markt kam und zu mehr und mehr mobilen Apps und kriminellen Möglichkeiten führte.

2009–2010—Soziale Netzwerke und Manipulation

Als die Webseiten sogenannter sozialer Netzwerke wie Facebook und Twitter im späteren Abschnitt des Jahrzehnts starteten, merkten Internetbetrüger, dass sie eine reichhaltige Menge an persönlichen Informationen erlangen konnten, wenn sie das Spiel nur richtig spielten.

Da Nutzer alles vom aktuellen Standort bis hin zum Heimatort und der Arbeitsstätte bekannt gaben, mussten Internetbetrüger nur noch virtuell mit ihnen interagieren, um Zugriff auf diese Informationen zu erlangen.

Sie tun dies noch immer, indem sie *soziale Manipulation*, anwenden, d.h. sie finden heraus, welche Themen die Internetnutzer interessieren und entwickeln dann Angriffe mit populären Betreffzeilen als Köder. Zum Beispiel kann ein Internetbetrüger angesagte Themen auf Twitter verfolgen und dann eine Nachricht veröffentlichen, in der er das aktuell beliebte Thema aufgreift und einen Link zu einer gefährlichen Webseite integriert, die darauf abzielt, Kreditkarteninformationen und andere persönliche Informationen zu stehlen.

In einem aktuellen Spam, bei dem soziale Manipulation angewendet wurde, nutzten Internetbetrüger die Neugier von Facebook-Nutzern aus, indem sie ihnen eine gefälschte Anwendung auf Facebook anboten, die zeigen sollte, wer ihr Profil angesehen hatte. Anstelle der gewünschten Anwendung luden die Opfer ein bösartiges Programm herunter, das auf deren Nachrichten in Facebook zugriff, um Spam-Mails zu versenden, einschließlich Nachrichten mit einer Werbung für genau den Scam, auf den sie reingefallen waren.

Geschichte einer Internetgang

2006 stellte sich ein Kreditkartendieb mit dem Online-Namen John Dillinger als Hauptverdächtiger in der Operation CardKeeper des FBI heraus. Diese Operation war eine Initiative, um herauszufinden, wer hinter den Diebstählen von zehntausenden an Kreditkartennummern aus Konzerndatenbanken steckte. Dillinger und eine Reihe anderer Amerikaner wurden beschuldigt, gestohlene Kreditkartennummern von Komplizen im Ausland erhalten zu haben und mit diesen Nummern Waren eingekauft zu haben, die sie später weiter verkauften.

Wie sich herausstellte, war Dillinger Teil einer internationalen Internetbande, die sich von den USA über Polen bis nach Rumänien erstreckte. Dillinger und die anderen amerikanischen Staatsbürger kauften Informationen, die elektronisch vom Magnetstreifen auf der Rückseite der gestohlenen Kredit- oder Bankkarte kopiert wurden. Dann fügten sie diese Informationen auf gefälschten Karten ein, so dass sie diese für Einkäufe und zum Geldabheben verwenden konnten. Währenddessen verkauften Mitglieder der Bande persönliche Daten wie Sozialversicherungsnummern in Online-Foren. Diese persönlichen Informationen wurden später verwendet, um Kreditkarten zu erhalten, die den Namen des Opfers trugen.

Es wurde angenommen, dass der Anführer der Internetbande aus Polen stamme und den Nickname „Blindroot“ trug. Blindroot und seine Komplizen hackten sich in Webserver von Dritten und vermieteten den Platz auf den Servern dann für illegale Aktivitäten wie das Hosten von Phishing-Seiten für Kreditkartenbetrug an andere Internetkriminelle.

Dillinger und 16 weitere Hacker und Verkäufer von Informationen in den USA und Polen wurden am Ende während ihrer Aktionen verhaftet. Obwohl das wahre Ausmaß ihres Netzwerkes nie entdeckt wurde, sagten Behörden, dass mehr als 100.000 Kreditkartennummern allein in Virginia gestohlen wurden; mehrere Tausend Identitäten wurden über das Internet verbreitet.

Ein weiterer aktiver Facebook-Scam beinhaltet, dass Internetbetrüger Zugriff auf die Konten der Nutzer erhalten und dann Nachrichten vom Kontoinhaber an seine Freunde versenden. Diese Nachrichten sagen aus, dass der Freund im Ausland ausgeraubt wurde und sie nun Geld an ihn senden sollten, damit er nach Hause kommen könne. Dieser „Ich wurde ausgeraubt!“-Scam ist ein weiteres gutes Beispiel für soziale Manipulation, die vielen unwissenden, gutherzigen Freunden hunderte oder tausende Dollar gekostet hat.

Internetbetrüger begannen auch, Scareware zu verbreiten. Sie bleibt bis heute eine der häufigsten Internetbedrohungen, die eine signifikante Evolution in der Internetkriminalität darstellt, da sie demonstriert, wie erfolgreich Angreifer sein können, wenn sie wissen, wie sie ihrer Opfer psychologisch manipulieren können. Durch das Spiel mit den Ängsten der Internetnutzer, dass Computer und Informationen bedroht sein könnten, waren Internetbetrüger in der Lage, ungehindert Zugriff auf Computer zu erlangen, während sie hundert Millionen von Dollar einnahmen.

Schließlich, nach den Angriffen auf Nutzer und Konsumenten, richteten sie sich die Angriffe auch gegen Unternehmen, Regierungen und Organisationen, wobei sie als Form des sozialen Protests und Rebellion genutzt wurden. Der Fall des WikiLeaks „Hacktivist“, der DDoS-Angriffe gegen Webseiten wie MasterCard und Visa startete, nachdem sich diese Unternehmen von der Nachrichtenplattform distanziert hatten, ist ein Beispiel. Der Stuxnet-Wurm, der auf Versorgungsunternehmen und Kontrollsysteme und sogar nukleare Einrichtungen abzielte, ist ein weiteres. Nach und nach wurde Internetkriminalität von einem Akt der persönlichen Herausforderung und Bekanntheit zu einem lukrativen Vorhaben sowie einem politischen Werkzeug.

In Anbetracht dessen, wie weit Kriminalität in den letzten 10 Jahren gekommen ist, kann man sich nur fragen, was noch vor uns liegt.

Internetkriminalität: Was kommt als Nächstes?

Soziale Scammer & App Spoiler

Wenn man auf zukünftige Trends der Internetkriminalität blickt, prophezeit McAfee Labs eine Weiterführung der Scams in sozialen Netzwerken und Tricks wie infizierte Links, angebliche Freundeseinladungen und *phishing*-Versuche. Zum Beispiel haben Sie eine Nachricht erhalten, die von einem Freund zu sein scheint, in der er Sie um Geld oder Informationen bittet. Scams werden wahrscheinlich intelligenter und persönlicher zugeschnitten, insbesondere dann, wenn Nutzer weiterhin eine große Menge an Informationen preisgeben.

McAfee Labs sieht auch einen verstärkten Missbrauch von Twitter, wo Internetbetrüger Tweets zu angesagten Themen posten, die einen infizierten Link enthalten und so Nutzer zum anklicken verlocken sollen.

Identitätsdiebstahl im Detail

Im Jahr 2000 gab die Bundeskommission für Identitätsdiebstahl ihr Identitätsdiebstahlprogramm bekannt, welches Verbrauchern eine kostenfreie Nummer und eine Informations-Webseite bot, um ein wachsendes Problem zu bekämpfen, das 600.000 bis 700.000 Amerikaner jährlich bedroht. Viele der Gefahren treten zu Hause auf - durch gestohlene Post, *Dumpstern* und Diebstahl durch dem Opfer bekannte Personen, sogar Freunde und Verwandte.

Zehn Jahre später war Identitätsdiebstahl so verbreitet, dass schätzungsweise im Jahr 2009 11,1 Millionen amerikanische Erwachsene Opfer von Identitätsdiebstählen wurden, während sich der Geldbetrag der Betrügereien auf \$59 Mia. erhöhte. Sogar der Vorsitzende der US-Notenbank Ben Bernanke und seine Frau wurden Opfer eines raffinierten Identitätsdiebstahlsrings mit dem Namen „Big Head“. Ein Betrüger stahl die Handtasche der Ehefrau, die ihr Scheckbuch für ein gemeinsames Konto enthielt.

Während Identitätsdiebstahl immer noch oft mit althergebrachten Methoden wie Taschendiebstahl verübt wird, so wird doch eine wachsende Menge an Diebstählen online durch Phishing, gefälschte Webseiten und Einbrüche in Unternehmensdatenbanken vollzogen.

Die Wahrheit ist, dass es heute eine Vielzahl an weiteren Wegen für die Diebe gibt, unsere persönlichen Daten zu stehlen – mehr als vor dem Internetboom. Doch während sich die Methoden des Identitätsdiebstahls ständig verändern haben sich die Auswirkungen nicht geändert. Opfer von Identitätsdiebstahl verlieren nicht nur Geld, sondern auch ihre Kreditwürdigkeit und ihr Ansehen. In dieser Ära der Internetkriminalität ist Identitätsdiebstahl die häufigste und ernsthafteste Bedrohung.

Ortsabhängige Services wie Foursquare, Google Placed und Gowalla stellen weitere Risikobereiche dar. Wenn mehr und mehr Nutzer bekanntgeben, wo sie sich in der richtigen Welt aufhalten, haben Betrüger ausgiebige Möglichkeiten, typische Verhaltensmuster und den momentanen Aufenthaltsort von Nutzern herauszufinden. Zudem erfahren sie, wann sie nicht zu Hause sind. Zusammen mit anderen Informationen, die online zugänglich sind, wie deren Adresse, können diese Online-Daten zu ernsthaften Verbrechen wie Raubüberfällen oder Einbrüchen in der echten Welt führen.

Letztlich stellt die Verbreitung von mobilen Geräten und Anwendungen eine weitere Möglichkeit für Internetbetrüger dar. Sie haben ihre Aufmerksamkeit bereits dahin gelenkt—McAfee Labs⁵ berichtete, dass mobile Gefahren wachsen und zielgerichteter im dritten Quartal des Jahres 2010 ausgeführt wurden. Es wird auch vorausgesagt, dass 2011 eine Wende bei Gefahren für mobile Geräte eintreten wird. Durch das Abzielen auf mobile Anwendungen können Betrüger enorme Mengen von persönlichen Daten oder auch Bankdaten von Nutzern stehlen.

Das Verlangen der Nutzer nach universellen Anwendungen, die auf mehreren ihrer Geräte funktionieren, bedeutet, dass Internetbetrüger Schaden auf vielen Plattformen anrichten können, indem sie nur eine App angreifen. Dabei spielt es keine Rolle, ob es das iPhone, Android oder Windows-basierte Telefone sind.

Während viele Arten der Angriffe gleich bleiben werden (also Phishing, gefährliche Webseiten und Downloads sowie Spam), werden die Methoden der Internetbetrüger zielgerichteter und intelligenter werden. Die Zeiten der Zerstörung sind vorüber – nun geht es nur noch um Geld und Diskretion.

Wachstum der Internetkriminalität: Sind die Computernutzer teilweise mit Schuld?

Bei Internetkriminalität ist es einfach, mit dem Finger auf die Bösewichte zu zeigen. Aber wie stark hängt ihr Erfolg von unseren Aktivitäten oder unserer Untätigkeit ab? Beachten Sie dies: Trotz umfassender Informationen zur Verbreitung und Gefahr von Internetangriffen ergab eine kürzlich durchgeführte Umfrage, dass nur 58 Prozent der Nutzer sagten, sie hätten ein umfassendes, komplettes Sicherheitsprogramm. Als die Experten dann deren Computer tatsächlich untersuchten entdeckten sie, dass nur 37 Prozent vollständig geschützt waren. Das bedeutet, dass fast zwei Drittel der Nutzer ungeschützt sind und sie es so den Internetbetrügern einfacher machen. In Anbetracht dieser Tatsachen ist es nicht verwunderlich, dass 545.000 Haushalte ihren PC während einer 6-monatigen Zeitspanne im Jahr 2009 ersetzen mussten, nachdem er mit Malware infiziert wurde.

Der Grund dafür, dass in der Umfrage gezielt nach einem kompletten Sicherheitspaket gefragt wurde ist, dass sich Bedrohungen ständig verändern und raffinierter werden, so dass ein einfacher Schutz einfach nicht ausreicht. Trotzdem nutzen 25 Prozent der Verbraucher kostenlose Sicherheitsprogramme, die normalerweise nicht gegen alle aufkommenden Bedrohungen schützen und oft verwendet werden, um dem Verbraucher ein umfassenderes aber kostenpflichtiges Programm zu verkaufen.

Zusätzlich dazu, dass wir unseren Computer nicht so sorgfältig schützen wie wir es sollten scheint es auch so, als müssten wir unsere Daten besser sichern.

Allein in den letzten zwei Jahren gaben sieben Millionen US-Verbraucher - das bedeutet einer von 13 Haushalten - zu, ihre persönlichen Daten an Phishers weitergegeben zu haben. Phishers sind Betrüger, die Nutzer dazu bringen Informationen preiszugeben, indem sie sich als legitime Unternehmen oder Organisationen ausgeben. Zudem richten nun Betrüger ihre Angriffe auf soziale Netzwerke, in denen besonders jüngere Leute ihren Schutz fallen lassen und sich anderen mitteilen. Leider funktioniert das auch. Eine andere Studie zeigt, dass Nutzer sozialer Netzwerke zwischen 18 und 24 Jahren im Vergleich zu anderen Gruppen verstärkt Opfer von Betrug und Datenweitergabe wurden.

Es ist ganz klar, dass wir beim Schutz unserer Computer und persönlichen Informationen besser werden müssen, wenn wir den Erfolg der Internetbetrüger ausbremsen möchten. Technologie kann uns ein großes Stück voranbringen aber für den restlichen Teil des Weges benötigen wir Aufklärung und Wachsamkeit von Seiten der Computernutzer.

Quellen: NCSA-Study 2010 ; Consumer Reports State of the Net report in 2010; Javelin Strategy & Research, 2010.

Top 5 Exploits – Verschiedene Zeitspannen von Internetkriminalität

1. MyDoom's Masseninfektion: Geschätzter Schaden \$38 Mia.

Dieser sich rasch ausbreitende Wurm schlug erstmals 2004 zu und ist Spitzenreiter was den verursachten monetären Schaden angeht. Der Wurm war darauf programmiert Computer zu infizieren und Spam-Mails zu versenden. Durch die Menge an versendeten Spams verlangsamte er den weltweiten Internetzugriff um 10 Prozent und verringerte den Zugriff auf einige Webseiten um 50 Prozent. Dadurch wurde ein Schaden von Milliarden Dollar durch Produktivitätseinbußen und entgangene Online-Verkäufe verursacht.

2. Die falsche Zuneigung des „I LOVE YOU“-Wurms: Geschätzter Schaden \$15 Mia.

Der „I love you“-Wurm (benannt nach der Betreffzeile der E-Mail, mit der er versendet wurde) stellte sich 2000 als unwiderstehlich heraus, denn Millionen von Nutzern öffneten die Spam-Mail und luden die angehängte Datei, einen „Liebesbrief“, herunter. Leider erhielten sie statt süßen Nichtigkeiten einen bösen Virus. Der berüchtigte Wurm kostete Unternehmen und Regierungsbehörden \$15 Mia., da sie ihre Computer herunterfahren und die Infizierung entfernen mussten.

3. Die schleichende Zerstörung von Conficker: Geschätzter Schaden \$9,1 Mia.

Dieser Wurm aus dem Jahr 2007 infizierte Millionen von Computern und führte seine Infizierung dann weiter als die ersten beiden Würmer in unserer Liste, denn Internetverbrechern ging es nicht mehr nur darum, berühmt zu werden sondern um Professionalität. Conficker ist darauf ausgelegt Malware von Webseiten herunterzuladen und zu installieren, die von Virenprogrammierern kontrolliert werden. Die Malware enthielt einen *keystroke logger* und andere PC-Kontrollsoftware, durch die die Internetbetrüger Zugriff auf persönliche Daten des Computernutzers sowie den Computer erhielten.

4. Stuxnet Wurm – Zielgerichtet und gefährlich: Schaden unbekannt

Der neueste Wurm zielt auf entscheidende Infrastrukturen wie beispielsweise Versorgungsunternehmen und Kontrollsysteme, indem er etliche Schwachstellen von Windows vorteilhaft ausnutzt.

Stuxnet hat Berichten zufolge Schäden bei Regierungseinrichtungen in Indien, den USA und Indonesien sowie nuklearen Einrichtungen im Iran verursacht. Die Schöpfer des Wurms sind nach wie vor unbekannt, aber die Welt ist sich ihrer Gegenwart und der Gefahr zielgerichteter Angriffe bewusst.

5. Zeus Botnet – Gewandter Informationsdieb: Schaden unbekannt

Internetbetrüger benannten dieses Botnet nach einem griechischen Gott und auch wenn es nicht allmächtig ist, ist es Computernutzern seit 2007 ein Dorn im Auge.

Eines seiner wesentlichen Fähigkeiten ist es persönlichen Daten zu stehlen, indem es den Computer infiziert und beim Online-Banking eingegebene Daten inklusive Passwörtern erfasst. Das Botnet kann infizierte Computer auch kontrollieren und persönliche Informationen erbeuten. Und kürzlich hat Zeus seine Raffinesse gezeigt, als pro Tag 700 Varianten entdeckt wurden, darunter auch solche für mobile Endgeräte.

Top 5 Scams – Die häufigsten Scams mit den meisten Opfern

1. *Scareware*—Der Verkauf von falscher Antivirus-Software ist einer der heimtückischsten und erfolgreichsten Scams der vergangenen Jahre. Internetbetrüger spielen mit der Angst der Anwender, ihre Computer oder Daten seien gefährdet, indem sie irreführende Pop-up-Fenster auf dem Rechner des Nutzers anzeigen, die ein angebliches Malware-Problem auf dem Computer melden. Die Betrüger fordern dann die Opfer auf, gefälschte Antiviren-Software zu kaufen, um das Problem zu beheben. Wenn das Opfer dem Kauf zustimmt, überträgt es sein Geld und seine Kreditkarteninformationen an diejenigen, die hinter dem Scam stecken.

2. *Phishing Scams*—Phishing oder der Versuch, Nutzer dazu zu bringen, persönliche Informationen weiterzugeben, ist eine der häufigsten und beständigsten Online-Bedrohungen. Tatsächlich wurden über 49.000⁶ Phishing-Seiten Ende des Jahres 2009 entdeckt. Phishing-Versuche können auf viele verschiedene Weisen auftreten, z. B. durch Spam-Mails, Spam-Sofortnachrichten, falsche Freundeseinladungen und Posts in sozialen Netzwerken. Normalerweise geben Internetbetrüger vor, ein legitimes Unternehmen oder eine Organisation zu sein und fragen dann nach Ihren Daten.

3. *Gefälschte Webseiten*—In den letzten Jahren sind Internetbetrüger immer geschickter in der Erstellung von gefälschten Webseiten geworden, die wie die originalen aussehen. Von angeblichen Bankseiten zu Auktionsseiten und E-Commerce-Seiten – Betrüger legen immer wieder Online-Fallen und hoffen, dass Nutzer darauf hereinfallen und ihre Kreditkarten- oder persönlichen Daten angeben. Oft sind diese trügerischen Webseiten Teil eines

Phishing-Versuchs, bei dem Internetbetrüger Nachrichten mit einem Link zur gefälschten Seite verschicken. Wenn man bedenkt, dass laut einer kürzlich durchgeführten Studie die Zahl der Webseiten (darunter viele gefälschte), die mit bösartiger Software oder Werbung infiziert sind die Marke von 1,2 Millionen⁷ erreicht hat, dann sollten sich Nutzer vor dieser Gefahr in Acht nehmen.

4. *Online-Partnervermittlungsbetrug*—Wie der "I love you"-Virus zielt diese Masche auf die innersten Gefühle der Opfer, um ihr Ziel zu erreichen. Der typische Betrug bei der Online-Partnervermittlung beginnt damit, dass der Betrüger ein attraktives Bild auf eine Online-Partnervermittlungsbörse stellt. Der Betrüger versendet dann Nachrichten an andere Mitglieder der Seite, die Interesse bekunden. Der nächste Schritt ist, eine persönliche Unterhaltung normalerweise per E-Mail oder Instant Messenger mit dem Opfer zu beginnen, wobei sie eine anrührende Geschichte erzählen. Der Betrüger baut eine persönliche Beziehung auf, um dann um Bargeld, Waren oder andere Gefälligkeiten zu bitten.

5. *Nigerianischer Scam*—Diese Form des Betrugs, auch bekannt als der „Vorauszahlungsbetrug“ besteht in der Regel aus einer Spam-Nachricht von einem Ausländer, der Hilfe dabei benötigt, Millionen von Dollars aus seinem Heimatland zu bringen und der dem Empfänger einen Prozentsatz seines Vermögens für die Unterstützung bei dieser Überweisung bzw. Transaktion anbietet. Auch wenn diese Geschichte zu unglaublich klingt, fielen leider viele Empfänger darauf herein und einige verloren dabei tausende Dollars, da die Betrüger eine Gebühr im Voraus verlangten die diese Transaktion erst ermöglichen sollte.

Lexikon

Adware—Software, die Gewinne erwirtschaftet indem sie auf den Nutzer abgestimmte Werbeanzeigen einblendet. Der Entwickler der Adware erhält seine Einnahmen entweder vom Händler oder dessen Partnern. Bestimmte Arten von Adware sind in der Lage, persönliche Daten zu sammeln oder zu übertragen.

Botnet—Eine Ansammlung von Zombie-PCs. Botnet ist die Abkürzung für Robot Network (Roboternetzwerk). Ein Botnet kann aus bis zu hunderttausende einzelnen Computern bestehen. Ein einziger PC in einem Botnet ist in der Lage automatisch tausende von Spam-Nachrichten pro Tag versenden. Die am meisten verbreiteten Spam-Nachrichten stammen von Zombie-Computern.

DDoS-Angriffe—DDoS, oder Denial-of-Service-Angriffe, zielen auf einen Computerserver oder ein Netzwerk und überfluten es mit Zugriffsverkehr. Ein DDoS-Angriff überhäuft sein Ziel mit falschen Verbindungsanfragen, so dass das Ziel echte Anfragen ignoriert.

Dumpstern—Das Durchsuchen von Müll in der Hoffnung, wertvolles Material einschließlich sensibler Daten zu finden.

Keystroke logger—Ein Programm, das versteckt aufzeichnet, was Sie mit Ihrer Tastatur schreiben, einschließlich Passwörter und anderer sensibler Daten.

Makroviren—Ein Programm oder Codesegment, das in der internen Makrosprache der Anwendung programmiert ist. Einige Makroviren vervielfältigen oder verbreiten sich, andere manipulieren einfach Dokumente oder andere Dateien auf dem Computer des Nutzers ohne sich zu vervielfältigen.

Malware—Malware, kurz für malicious (böartige) Software, zielt darauf ab, Computersysteme ohne die Zustimmung des Nutzers zu infizieren.

Phishing—Eine Methode, auf betrügerische Weise an persönliche Informationen wie Passwörter, Sozialversicherungsnummern und Kreditkartendetails zu gelangen, indem gefälschte E-Mails versendet werden, die aussehen, als stammen sie von einem vertrauenswürdigen Absender. Phishing-Nachrichten fordern den Empfänger typischerweise dazu auf, einem Link in der E-Mail zu folgen, um ihre Kontaktdaten oder Kreditkarteninformationen zu aktualisieren.

Rootkits—Ein Set an Software-Tools, das Dateien oder Prozesse in einem infizierten Computer verändern kann, während es dabei unerkannt bleibt.

Scareware—Eine Art der Malware, die entwickelt wurde, um Nutzer zum Kauf oder Download nutzloser oder möglicherweise gefährlicher Software zu bewegen, normalerweise angeblich nötiger Antivirus-Programme. Es wird Scareware genannt, weil Nutzern Angst eingejagt wird, dass etwas mit ihrem Rechner nicht stimmen könnte, so dass sie die Software herunterladen.

7. Malware is Everywhere, Report Says (PCMag, November 2010)

Soziale Manipulation—Der Internetbetrüger nutzt nicht nur rein technische Mittel um das zu bekommen was er möchte sondern manipuliert das Verhalten des Computernutzers so, dass dieser bestimmte Dinge macht oder persönliche Daten preisgibt.

Virus—Eine Computerprogrammdatei, die in der Lage ist, sich auf Festplatten oder anderen Dateien festzusetzen und sich mehrmals selbst zu vervielfältigen, normalerweise ohne das Wissen oder die Erlaubnis des Nutzers.

Wurm—Ein Virus, der sich verbreitet, indem er Duplikate von sich selbst auf anderen Festplatten, Systemen oder Netzwerken anfertigt. Ein Massen-Mail-Wurm ist einer, der das Eingreifen eines Nutzers zur Verbreitung benötigt (z.B. das Öffnen eines Anhangs oder Herunterladen einer Datei). Die meisten der heutigen E-Mail-Viren sind Würmer.

Zombie computer—Ein Computer, der infiziert wurde und aus der Ferne von einem Internetbetrüger gesteuert werden kann.

Über McAfee

McAfee (NYSE: MFE) ist der weltgrößte dedizierte Spezialist für IT-Sicherheit. Das Unternehmen mit Hauptsitz im kalifornischen Santa Clara hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von der einzigartigen Global Threat Intelligence entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen und Behörden helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. Weitere Informationen über McAfee finden sich unter www.mcafee.com/de

Bei Fragen wenden Sie sich bitte an:

McAfee

Isabell Unseld

PR-Managerin Mittel-, Ost- und Westeuropa

Ohmstraße 1

85716 Unterschleißheim

089 3707-1535

isabell_unseld@mcafee.com

Harvard Public Relations

Felix Laubenthal

Guillermo Luz-y-Graf

Implerstraße 26

81371 München

089 532957-46

089 532957-30

mcafee@harvard.de

felix.laubenthal@harvard.de

guillermo.luz-y-graf@harvard.de

