

Pressemitteilung

Symantec Sicherheitsreport: Mit dem Breitband kamen die Bots...

23 Prozent aller Bot-infizierten Rechner Europas befinden sich in Deutschland/ Identitätsdiebstahl wird immer raffinierter/ Phishing-Webseiten gehen zurück/ Schattenwirtschaft mittlerweile milliardenschwer

München, 17. September 2007 – Phishing-Webseiten sind in Deutschland um fast ein Drittel zurückgegangen. Das zeigt die zwölfte Ausgabe des Internetsicherheitsreports von Symantec, der alle sechs Monate erscheint und auch diesmal wieder einen gesonderten Report zur Region EMEA (Europa, Mittlerer Osten, Afrika) umfasst. Die positive Nachricht wird allerdings durch die Tatsache getrübt, dass Angreifer über neue professionelle Angriffs-Tools verfügen. Diese ermöglichen, dass sie – auch ohne perfekte Betrugsseiten zu gestalten – in den Besitz vertraulicher Daten der Anwender kommen können. Bereits 65 Prozent der weltweiten Top-50 Schädlinge zielen auf Identitätsdiebstahl ab. Damit lässt sich Geld verdienen: so wird beispielsweise das Trojaner-Toolkit MPack für 1.000 Dollar auf Untergrundservern gehandelt. Der Professionalisierung und Kommerzialisierung einer mittlerweile milliardenschweren Schattenwirtschaft stehen viele Anwender unbedarft gegenüber: Allein in Deutschland stehen 23 Prozent der Bot-infizierten Computer in Europa.

Wie auch schon im Vorberichtszeitraum richten sich die Angriffe fast ausschließlich (99,4 Prozent bezogen auf EMEA, 95 Prozent weltweit) gegen Endanwender, von deren teilweise lückenhafter technischer Absicherung, aber auch Unbedarftheit die Angreifer zu profitieren hoffen. „Viele Anwender verwalten vertrauliche Informationen, wie beispielsweise Kontodaten, auf ihren Rechnern, was ein lukratives Ziel für die Angreifer darstellt und die finanziellen Interessen hinter den Aktivitäten unterstreicht,“ sagt Candid Wüest, Sicherheitsexperte bei Symantec.

Bots in Deutschland auf dem Vormarsch

In Deutschland sind 23 Prozent aller in EMEA infizierten Bot-Rechner zu finden. Der Grund für die führende Position ist in der hohen und stets wachsenden Zahl der vorhandenen Breitbandanschlüsse zu suchen. Viele neue Breitband-Nutzer sind sich der Notwendigkeit, sich gegen die Bedrohung aus dem Internet entsprechend zu schützen, noch nicht ausreichend bewusst. Weltweit liegt China mit 29 Prozent aller weltweiten Bots vorn.

Unter einem Bot (Abkürzung für Robot) versteht man ein ohne Wissen des Anwenders installiertes Computerprogramm, welches Angreifern den Fernzugriff auf das System über einen Kommunikationskanal (wie beispielsweise IRC) ermöglicht. Dabei infiziert in der Regel ein Angreifer zahlreiche Rechner mit einem Bot, der diese dann zu einem Netzwerk (Botnet) verbindet. Dieses Netzwerk kann zentral von einem Command-and-Control Server aus gesteuert werden, um koordinierte Angriffe zu starten. In der Region EMEA sind ein Viertel der Command-and-Control Server in Deutschland zu finden.

Bisher wurden Bots für massenhaften Spam- und Phishing-Versand oder für Denial of Service Attacken eingesetzt, aber die erweiterten Sicherheitskonzepte der Internet Service Provider blockieren diese Aktivitäten und so wenden sich die Angreifer unauffälligeren Techniken zu, mit denen sie schneller an vertrauliche Daten gelangen können, die sie dann zu Geld machen können.

Professionalisierung und Kommerzialisierung einer Schattenwirtschaft

Bereits im Frühjahr 2007 hatte der Internet Security Threat Report XI auf die Entstehung einer Schattenwirtschaft hingewiesen, die über IRC, Webseiten und Schwarzmarkt-Auktionen Zeroday-Schwachstellen und entsprechende Abgriffstools anbietet. Innerhalb kurzer Zeit hat sich diese Kommerzialisierung zu einem milliardenschweren kriminellen Zweig entwickelt und auch die Entwicklung, Verbreitung und Implementierung vieler Schadcodes und Aktivitäten zeugt von einer hochgradigen Professionalität.

Ein aktuelles Beispiel hierfür ist MPack: Ein hochentwickeltes Angriffstoolkit, das anscheinend professionell programmiert und entwickelt wurde und im Internet für 1.000 US-Dollar angeboten wird.

Zu beobachten ist auch ein Paradigmenwechsel in der Angriffsmethodik: Angreifer legen sich heute auf die Lauer und warten, bis ihr Angriffsziel selbst auf sie zukommt. Hierfür wird die Schadsoftware auf einer präparierten Webseite hinterlegt. Besonders "Social Networking"-Webseiten haben sich für die Hacker als besonders ergiebig erwiesen, da sie Angreifern Zugang zu einer Vielzahl von Personen bieten, von denen viele blind darauf vertrauen, dass diese Webseiten sowie ihr Inhalt sicher sind. Dies hat ernste Konsequenzen für die Anbieter,

da das Vertrauen in die bekannten und beliebten Webseiten verloren geht. Der bislang gängige Rat, "schlechten Umgang" im Internet zu vermeiden, reicht heutzutage nicht mehr aus.

Sobald die infizierte Webseite vom Anwender besucht wird, wird Schadcode über eine Sicherheitslücke nachgeladen. Dabei braucht der Angreifer nicht lange nach einem Einfallstor in Web-Browsern und -Applikationen zu suchen, denn allein in diesem Berichtszeitraum wurden 237 Sicherheitslücken in Browser Plug-ins festgestellt.

Drei der Top-5 Schädlinge in der Region EMEA gehören bereits in die Kategorie der mehrstufigen Trojaner. Anwender sollten deshalb besonders bei Downloads aus dem Internet die Dateien vor dem Öffnen scannen lassen und regelmäßig ihre Sicherheitsprodukte aktualisieren.

Phishing-Tools im Baukastensystem

Zwar hat sich die Prozentzahl von Phishing-Webseiten in Deutschland von 32 auf 22 reduziert, dafür haben sich aber die Methoden professionalisiert, wie das enorme Auftreten von Phishing-Toolkits dokumentiert; hierbei handelt es sich um eine Reihe von Skripts, die einem Angreifer die automatische Einrichtung von Phishing-Webseiten ermöglichen, welche die Webseiten von Markenunternehmen vortäuschen – inklusive der zugehörigen Bilder und Logos. Parallel lassen sich über die Skripts korrespondierende Phishing-Mails generieren, um den Anwender auf die Webseite zu locken. In dem Berichtszeitraum stammten 86 Prozent der weltweiten Phishing-Webseiten von lediglich 30 Prozent der erfassten Absender IP-Adressen. Demnach kommen Phishing-Toolkits regelmäßig zum Einsatz.

Bei Spam-Mails befindet sich Deutschland mit einem Anteil von sieben Prozent auf Platz vier der EMEA-Liste – die allerdings von keinem konkreten Land, sondern von „Unbekannt“ angeführt wird. Dass der Spitzenreiter nicht klar bestimmt werden kann, liegt daran, dass die entsprechenden Provider oft in mehreren Ländern aktiv und daher nicht klar zuzuordnen sind. Allerdings existieren in Deutschland mit 17 Prozent die meisten Spam-Zombies. Ein Spam-Zombie ist – ähnlich wie bei einem Bot – ein ans Internet angeschlossener Computer, der durch verdeckte Installation entsprechender Schadprogramme eine „Fernsteuerung“ des Rechners zum Versand von Spam-Mails ermöglicht. Auch hier spielt wiederum die hohe Anzahl an Breitbandanschlüssen eine zentrale Rolle: die entsprechenden Rechner sind häufig online und in der Lage in kurzer Zeit viele Informationen zu verschicken.

Textumfang: 6.700 Zeichen (inclusive Leerzeichen)

Der "Symantec Internet Security Threat Report" bietet einen umfassenden Überblick über aktuelle Bedrohungen aus dem Internet und ist der einzige öffentlich zugängliche Bericht seiner Art, der nicht nur eine eingehende Analyse relevanter Daten und Trends veröffentlicht, sondern auch umfangreich Aufschluss gibt über die Verfahren und Methoden, mit denen diese Ergebnisse erzielt wurden. Aufgabe dieses Berichts ist es, alle Informationen bereitzustellen, die Privatpersonen und Unternehmen benötigen, um ihre Systeme jetzt und in Zukunft wirksam schützen zu können.

Der Bericht bietet einen halbjährlich aktualisierten Überblick über Internet-Bedrohungen; die aktuelle Ausgabe XII deckt den Zeitraum vom 1. Januar 2007 bis zum 30. Juni 2007 ab.

Um dem neuen Trend zu regionalen Bedrohungsmustern Rechnung zu tragen, gibt Symantec neben dem genannten Hauptbericht drei weitere Berichte heraus:

- den "EMEA Internet Security Threat Report" (für die Regionen Europa, Mittlerer Osten und Afrika)
- den "APJ Internet Security Threat Report" (für die Region Asien/Pazifischer Raum/Japan)
- den "Government Internet Security Threat Report", der sich in erster Linie mit Bedrohungen und Trends befasst, die speziell für Regierungsorganisationen und Behörden sowie kritische Infrastrukturbereiche wie die Öl- und Gasbranche, Energie- und Stromversorger und Finanzdienstleister interessant sind.

Weiterführende Informationen zur Datenerhebung

Die im 12. Internet Security Threat Report analysierten Daten stammen aus verschiedenen Informationsquellen von Symantec und sind zusammen genommen die weltgrößte Ressource für Datensicherheit:

- Symantec DeepSight Threat Management System und Symantec Managed Security Services – mehr als 40.000 Sensoren, die die Netzwerkaktivitäten in 180 Ländern überwachen.
- Symantec Virenschutzlösungen – mehr als 120 Millionen Installationen auf Clients, Servern und Gateways erfassen Schadcodes, Spyware und Adware.
- Schwachstellen-Datenbank – mehr als 22.000 erfasste Sicherheitslücken aus mehr als 50.000 Technologien von über 8.000 Anbietern seit mehr als zehn Jahren.
- BugTraq – Forum mit über 50.000 Abonnenten, die täglich neue Gefahrenpotenziale diskutieren und Lösungsansätze austauschen.
- Symantec Probe Network – ein System mit mehr als zwei Millionen E-Mail Accounts, als Köder in 20 Ländern installiert, um weltweite Spam- und Phishing-Aktivitäten zu analysieren.
- Symantec Phish Report Network – eine umfangreiche Community, deren Mitglieder, Unternehmen und Endkunden, betrügerische Webseiten aufdecken, indem sie Informationen zu Phishing-Webseiten an das Netzwerk weiterleiten und im Gegenzug weiterführende Daten zu aktuellen Phishing-Aktivitäten erhalten.

Weitere Details, Grafiken sowie den kompletten Sicherheitsbericht finden Sie im Symantec Online-Pressezentrum unter:

http://www.symantec.com/de/de/about/theme.jsp?themeid=threat_report

Umfassendes Hintergrundmaterial zum Symantec Global Intelligence Network ist unter folgendem Link erhältlich:

http://www.symantec.com/about/news/resources/press_kits/securityintelligence/

Über Symantec

Symantec ist ein weltweit führender Anbieter von Software, mit der sich Unternehmen und Privatpersonen sicher und vertrauensvoll in einer vernetzten Welt bewegen können. Das Unternehmen unterstützt Kunden mit Software und Dienstleistungen beim Schutz ihrer Infrastrukturen, Informationen und Interaktionen. Symantec hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in 40 Ländern. Mehr Informationen unter www.symantec.de

Hinweis für Redakteure:

Wenn Sie mehr über Symantec und seine Produkte erfahren möchten, dann besuchen Sie unser Online-Pressezentrum unter www.symantec.com/presse
Dort liegt auch Bildmaterial von Personen und Produkten für Sie bereit.

Symantec und das Symantec Logo sind Warenzeichen oder eingetragene Warenzeichen der Symantec Corporation in den USA und ihrer Tochtergesellschaften einigen anderen Ländern. Andere Firmen- und Produktnamen können Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen sein und werden hiermit anerkannt.

*Symantec (Deutschland) GmbH, Humboldtstraße 6, 85609 Aschheim
Telefon: +49 (0) 89 / 94302 - 100
Telefax: +49 (0) 89 / 94302 - 950*

Ihr Ansprechpartner (NUR PRESSE!) für Rückfragen:

*Corinna Spohr
PR Manager*

*Symantec (Deutschland) GmbH
Telefon +49 (0) 89-94302-620
Fax: +49 (0) 89-94302-450*

E-Mail: corinna_spohr@symantec.com

*Suemer Cetin
PR Consultant*

*Trimedia Communications Deutschland GmbH
Telefon +49 (0) 211-96485-54
Fax +49 (0) 211-96485-45*

E-Mail: suemergetin@dus.trimedia.de