PRESSEMITTEILUNG

Malicious Code Research Center von Finjan entdeckt Malware auf Storage- and Cache-Servern sowie akute Sicherheitsrisiken auf Web 2.0-Plattformen

Unternehmen gibt Malware-Trends im kürzlich veröffentlichten Web Security Report bekannt

München, 12. Oktober 2006 -- Finjan Inc., führender Anbieter von proaktiven webbasierten Sicherheitslösungen, hat heute seine aktuellen Web-Sicherheitstrends veröffentlicht, die vom unternehmenseigenen Malicious Code Research Center (MCRC) identifiziert wurden. In seinem Web Security Trends Report (Q3 2006) präsentiert Finjan neu entdeckte malicious Codes auf Storage- und Cache-Servern, sowie neue Gefahren, die auf Web 2.0 Plattformen und -Technologien abzielen. Der Report enthält außerdem eine weitere Folge der Reihe „Käufliche Werkzeuge für Attacken". Dieses Thema wurde bereits in Finjans vorhergehendem Web Security Trends Report vom Juli aufgegriffen und handelt vom käuflichen Angebot von Malware und einem sich immer rasanter ausbreitenden Schattenmarkt.

Malicious Code auf Storage- und Cache-Servern

Der neue Report beschreibt detailliert, wie Finjan mit malicious Code behaftete Inhalte auf Cache-Webseiten nachgewiesen hat. Diese befinden sich auf Storage- und Cache-Servern, wie sie beispielsweise von ISPs, Unternehmen und führenden Suchmaschinen eingesetzt werden. "Derartige Malware kann über Webseiten von Dritten bezogen und dazu genutzt werden, den Rechner des Anwenders zu missbrauchen", erklärt Yuval Ben-Itzhak, Finjan's Chief Technology Officer. "Selbst wenn die infizierte Seite geschlossen wurde, ist der Malware-verseuchte Inhalt nach wie vor auf den Cache-Servern gespeichert und einsatzbereit. Der Exploit kann zur Installation von Spyware, Trojanern und anderer Malware führen, die die Privatsphäre und die Identität des Nutzers gefährden."

Im Report sind verschiedene Belegstellen von Malware aufgelistet, die Finjans

Sicherheitsforscher auf öffentlichen Storage- und Cache-Speichern gefunden haben. “Das ist mehr als nur eine theoretische Bedrohung”, erklärt Ben-Itzhak. “Infolge dieses Exploits ist es vorstellbar, dass Storage- und Cache-Server unbeabsichtigt zu den größten, legitimen Speicherorten für Malware werden. Eine derartige Infektion über den Proxy stellt ein völlig neues Risiko für Unternehmen und Endkunden dar.” Ben-Itzhak bemerkte darüber hinaus, dass es zwingend notwendig ist, das Bewusstsein für die Gefahren, die möglicherweise auf im Cache gespeicherten Webseiten lauern, beim Nutzer zu schärfen.

Finjan hat die Suchmaschinenbetreiber und Service-Anbieter mit allen technischen Details der Entdeckung versorgt und führt mit all diesen Unternehmen einen offenen Dialog, um ihnen bei der Lösung des Problems unter die Arme zu greifen. Einige Beispiele der auf den Storage- und Cache-Servern entdeckten Malware sind unter dem folgenden Link zu finden: here. Details von MCRC’s disclosure policy sind auf Finjans MCRC-Webseite abrufbar.

Sicherheitslücken bei Web 2.0

Eine weitere erst kürzlich entdeckte Bedrohung der Websicherheit konzentriert sich auf die Nutzung von Web 2.0 und AJAX-Technologien (Asynchronous JavaScript and XML) zur Ausführung von Malware-Aktivitäten. Während Web 2.0 und AJAX eine Bereicherung und Verbesserung bei der Internetnutzung bieten, öffnet die Technologie gleichzeitig Tür und Tor für neue Methoden zur Verbreitung von Malware. “Dadurch, dass sie gerade auf viel besuchte Webseiten abzielen, haben die Hacker einen überaus einfachen Weg gefunden, um eine massenhafte Verbreitung zu erreichen”, sagt Ben-Itzhak. “Durch die Einbettung von Malware in gehostete Webseiten einerseits oder durch die Nutzung von AJAX andererseits, können Hacker quasi unsichtbare Angriffe fahren, da der Code auf der betroffenen Seite niemals sichtbar wird.”

Ben-Itzhak fügt hinzu, dass Unternehmen ihre Anwender vor den bösartigen AJAX-Abfragen schützen müssen und dazu Sicherheitslösungen benötigen, die in der Lage sind, jede einzelne Webanfrage oder –antwort gewissermaßen im Vorbeigehen zu analysieren. “Verhaltensbasierte Analysen von Web-Inhalten, die am Gateway zwischen Browser und Webserver stattfinden, sind eine sehr effektive Methode”, ergänzt er. “Ein wichtiger Vorteil der verhaltensbasierten Sicherheit ist, dass jedes Stückchen Inhalt überprüft wird, ganz egal, woher es ursprünglich stammt. Diese Technologie stellt sicher, dass bösartige Inhalte das Netzwerk nicht erreichen, selbst wenn der Ursprungsort eine absolut vertrauenswürdige Seite ist. ”

Wachsende Kommerzialisierung der Malware

Im vorangegangenen Web Security Trends Report, diskutierte Finjan die Entwicklung zur

Kommerzialisierung von Malware. Der Report legt einen neuen Trend hin zum Verkauf von Schwachstellen offen. Forscher von Finjan entdeckten eine Firma, die offen nach bislang noch unbekannten Fehlern und Schlupflöchern in Sicherheits-Produkten sucht (zum Beispiel bei ZoneAlarm Pro, Norton Personal Firewall).

Detaillierte Beschreibungen dieser neuesten Cyber-Bedrohung sind im Web Security Trends Report nachzulesen. Ben-Itzhak fasst zusammen: “Die Informationen, die von unserem MCRC zusammen getragen wurden und die unter Web Security Trends Report abgerufen werden kann, helfen unseren Kunden sowie der gesamten IT-Security-Gemeinschaft der wachsenden Bedrohung aus dem Cyberspace zu begegnen und Malware-verseuchten Inhalt entgegen zu treten.”

Über das MCRC
Das Malicious Code Research Center (MCRC) widmet sich der Ausforschung und Entdeckung von Sicherheitsschwachstellen im Internet, in E-Mail-Applikationen und anderen beliebten Anwendungen. Das Ziel des MCRCs ist es, den Hackern, die versuchen, öffentlich zugängliche Plattformen und Technologien für die Entwicklung von Malware wie beispielsweise Spyware, Trojaner, Phishing-Angriffe, Würmern und Viren zu missbrauchen, immer einen Schritt voraus zu sein. Die Forscher vom MCRC arbeiten mit den weltweit führenden Software-Anbietern zusammen. Weitere Informationen finden Sie auf der MCRC subsite.

Über Finjan
Die proaktiven, Security Lösungen von Finjan bieten höchst effektiven Schutz gegen alle Bedrohungen aus dem Web. Das Unternehmen nutzt dafür seine patentierte verhaltensbasierte Technologie um proaktiv all jene Bedrohungen abzuwehren, die über das Web kommen; so wird der Geschäftsbetrieb vor Spyware, Phishing, Trojaner und andere Malware und noch aufkommende Bedrohungen geschützt. Die Sicherheitslösungen von Finjan haben zahlreiche Industrieauszeichnungen erhalten und genießen die Anerkennung führender Analysten und Publikationen, eingeschlossen IDC, Bulter Group, SC Magazine, CRN, PCPro, ITWeek und Information Security. Weitere Informationen gibt es unter www.finjan.com.

Kontakt für Presseanfragen

Claudia Meisinger
Marketing Manager, EMEA
Tel: +49 89 673597-11
Fax: +49 89 673597-50
Mobile: +49 172 4545000
Email: cmeisinger@finjan.com
Visit us at: www.finjan.com