Pressemitteilung 11-02-2009

Neue Bedrohungen: Gumblar-Netzwerk nach 5 Monaten wieder aktiv

Signatur-basierte Malware-Erkennung hat hier kaum eine Chance

London - San Francisco - München, November 2009

Nach einer Pause von fünf Monaten ist ein Gumblar-Netzwerk wieder aktiv. Mary Landesman, Senior Security Researcher bei ScanSafe, warnt: im Mai dieses Jahres ist ein Netz von infizierten Webseiten gebildet worden, das jetzt diese Seiten als Host für seine Malware verwendet. *"In einer typischen Outbreak-Situation liegt die Malware auf einer gehackten Seite. In diesem Fall befindet sich die Malware jedoch auf tausenden legitimen - aber infizierten - Websites."*

Siehe http://blog.scansafe.com/journal/rss.xml

Die Mehrzahl der infizierten Sites sind „Tante Emma" Websites aus nicht englischsprachigen Ländern. Aber das ist hier unwichtig, denn die Attackierenden haben einen cleveren Trick, um den Internetverkehr direkt zur Malware zu führen, die auf diesen Seiten geparkt ist:

"Ein iframe, der zu dem Malware-Script auf der infizierten Seite führt, wird in diversen Foren abgelegt. Die betroffenen Foren, die wir uns bis jetzt angesehen haben, benutzen Feed Aggregatoren, um ihre Posts aus dem Forum zu Abonnenten zu bringen, die dann durch den iframe infiziert werden", so Landesman.

„Dieses infizierte Script, das im ersten Schritt der Gumblar-Attacke bestimmte unique Komponenten enthält, sucht die Version von AdobeReader und Adobe Flash und liefert dieselbe URL mit einer uniquen SID, die auf diesen Ergebnissen basiert."

Das Skript enthält auch ein Exploit für die Microsoft Office Web Komponenten, das im August 2009 gepatcht wurde (beschrieben in MS09-043). Erfolgreiche Exploit-Ergebnisse in einer durch Zufallsgenerator benannten Datei wurden im System abgelegt.

Genau wie bei der ursprünglichen Gumblar-Attacken modifiziert die Malware folgenden Registry Key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Drivers32

„Dadurch wird die Malware geladen, sobald eine x-beliebige Ton-fähige Anwendung bzw. irgendein Browser, gestartet wird. Die Malware liest auch sqlsodbc.chm, eine Datei, die bereits Ziel früherer von Gumblar verteilter Malware war", sagt Landesman.

ScanSafe meint, signature-basierte Sicherheitssoftware hat hier lt. dem VirusTotal Report kaum eine Chance.

Heute macht es für Unternehmen zunehmend Sinn, die URL gründlich und in Echtzeit zu analysieren, die von einem Nutzer gerade aufgerufen wird. Da die Überprüfung des gesamten Web-Traffics in der Internet-Wolke geschieht, kommt es weder zu

Verzögerungen noch zu Bandbreitenstau. Auch entfallen Kosten, wie sie bei traditionellen Verfahren entstehen, wenn etwa der Datenverkehr über ein Unternehmens-VPN an ein Internet-Gateway geleitet wird. Security-as-a-Service (SaaS) hat heute ein Funktionsspektrum, das internen Lösungen in nichts nachsteht und gewährleistet unendliche Skalierbarkeit. Organisationen - egal welcher Größe - sind einfach nicht in der Lage, ein solches Maß an Sicherheit selbst zu replizieren. Das gilt noch mehr im Falle einer verteilten Architektur, so wie für Roaming Users.

„Die Mehrzahl der SaaS-Kunden kostet die Security-Dienstleistung 30 bis 40 % weniger als eine gleichwertige Vor-Ort-Lösung“, meint Pim van der Poel, Regional Sales Manager DACH von ScanSafe.

Beim Vertriebsaufbau in Zentral-Europa wird ScanSafe durch Dienstleistungen der Inline Sales GmbH unterstützt.

Über ScanSafe

ScanSafe, Marktführer bei Managed Services für den Internetschutz, ermöglicht **mit seiner unabhängig von Signaturen arbeitenden Technologie** Outbreak Intelligence ™ proaktiven Schutz von Unternehmensnetzwerken über Web-Filtering, Virus-Scanning, Instant-Messaging-Kontrolle und Spyware-Screening. Außerdem können Kunden die Nutzung von Internet und Instant Messaging nach eigenen Vorstellungen kontrollieren. Der Sicherheitsdienstleister befreit seine Kunden von den Schwierigkeiten und Zusatzkosten, die aus der internen Einführung entsprechender Hard- und Software resultieren. **ScanSafe verarbeitet PRO TAG rund 1 Milliarde Web-Anfragen** und blockt 200 Millionen Bedrohungen für Kunden in über 100 Ländern. In 2009 wurde das Unternehmen im dritten Jahr in Folge als “Best Content Security” Lösung vom SC Magazine Europe ausgezeichnet.
ScanSafe unterhält Niederlassungen in London und San Mateo, Kalifornien. Das Unternehmen befindet sich in Privatbesitz, Risikokapitalgeber sind Benchmark Capital und Scale Venture Partners.

Über Inline Sales GmbH

Die Inline Sales GmbH mit Sitz in München ist Spezialist für Business Process Outsourcing in Vertrieb und Marketing. Die Inline Sales GmbH übernimmt für Unternehmen der unterschiedlichsten Branchen aus allen Kontinenten den strategischen und operativen Geschäftsaufbau durch die Bereitstellung von Services und Ressourcen in den Bereichen Vertrieb, Marketing und Business Development. Die Dienstleistungen der Inline Sales GmbH wurden in 2008 und 2009 als INNOVATIONSPRODUKT und in 2009 als qualifiziertes INDUSTRIEPRODUKT von der Initiative Mittelstand ausgezeichnet.
Die Inline Sales GmbH ist Bestandteil der Inline Sales International Group und verantwortlich für das Geschäft der Gruppe in Zentral- und Osteuropa. Weitere Niederlassungen der Gruppe befinden sich in London, Paris und Miami. Vertriebsbüros bestehen in Hannover, Moskau, Posen, Prag, San Francisco, Sofia, Valencia, Wien und Zürich.
In ihrer über 10-jährigen Tätigkeit hat die Inline Sales International Group namhafte Kunden betreut wie British Telecom, BBC, Motorola, COMPAREX, Samsung, EDS oder Laser 2000. Darüber hinaus wurden bereits hunderte von kleinen und mittelständischen Unternehmen erfolgreich aufgebaut.

Weitere Informationen: ScanSafe, Pim van der Poel, Tel. +49 (0) 8705 939 951, pim.vanderpoel@scansafe.com

Kontakt Inline Sales GmbH:
Presseabteilung
Hermann-Schaller-Strasse 24
81825 München
Deutschland
Tel: +49-89-3090-488-32
Fax: +49-89-3090-488-42
Email: presse@inline-sales.com
http://www.inline-sales.com