AlienVault analysiert SSH-Zone.net: Account buchen und Zombie-PC-Armeen ins Leben rufen

AlienVault analysiert SSH-Zone.net: Account buchen und Zombie-PC-Armeen ins Leben rufen

Gerootete Server für jedermann
München/San Mateo, 09. Juli 2013 - Einen gehackten Server kaufen und darüber Malware verbreiten, Spammails absetzen oder ein Botnetz einrichten? Das ist nur eine Frage des Geldes. Im Untergrund-Store "SSH-Zone.net" sind derartige Server-Käufe möglich. Kürzlich haben die Spezialisten von AlienVault diese Seite genauer untersucht, um festzustellen, wer hinter diesem Geschäft steht und wie die Kriminellen in die Server einbrechen. Überwiegend machen sich die Cybergangster die Server per IP-Scanning und Brute-Force-Attacken zu eigen.
Die Domain "SSH-Zone.net" des Store ist seit dem 07. April 2013 registriert, die Website ist laut Vermutungen der AlienVault-Experten kurz darauf veröffentlicht worden. Zum Zeitpunkt der Analyse waren etwa 400 Kunden angemeldet, Anzahl täglich steigend. Um den Standpunkt des eigenen Servers zu verschleiern sowie digitale Attacken abzuwehren, haben die Inhaber die Site hinter dem Schutzwall des Security-Tools CloudFlare aufgezogen. Im Store findet der User verschiedene, international aufgestellte Server-Typen inklusive detaillierter technischer Informationen. Der Großteil der gerooteten Server ist den Labs-Spezialisten zufolge eher überholt und läuft mit alter Software. Den Kauf kann der Interessierte mittels der Online-Bezahlsysteme Perfect Money oder WebMoney tätigen.
Erst gescannt, dann gehackt
Außerdem hat AlienVault ermittelt, wie die Seitenbetreiber die Kontrolle über die betroffenen Server erlangen: Hauptsächlich hacken sie Nutzerkonten von SSH und dem Serververwaltungs-Tool Plesk. Als Secure Shell oder kurz SSH werden u.a. Programme bezeichnet, die Remote-Zugriffe per verschlüsselte Netzwerkverbindung auf andere Geräte ermöglichen. Vor den Brute-Force-Attacken scannen die Kriminellen mittels eines portablen Scanners namens Fever offene 8443- und 22-Ports. Es gibt Indizien dafür, dass manche "Mitarbeiter" der Site russisch sprechen, da auf dem Server installierte Software auf russische Sprache eingestellt war. Auf demselben Server werden außerdem gehackte PayPal-Accounts und Kreditkarten verkauft.
Fazit der AlienVault-Experten: Gerootet zu werden kann jedem Server bevorstehen, der nicht ausreichend abgesichert oder mit einem schwachen Passwort geschützt ist. Das Unternehmen rät Systemadministratoren verbeugend dazu, unnötige Services auszufiltern, die Software stets upzudaten sowie starke Passwörter oder besser: Authentifizierungsschlüssel zu verwenden. Des Weiteren empfiehlt sich das Monitoring aller Kommunikationsstrukturen, wie es die AlienVault Unified Security Management-Plattform ermöglicht. Mit ihrer Hilfe lassen sich forensische Daten nach Cyberangriffen analysieren und künftige Attacken abwehren.
Weitere Informationen zum Underground Store stehen im Blog der AlienVault Labs bereit.
Über AlienVault:
Die Unified Security ManagementTM-Plattform AV-USM von AlienVault ebnet Unternehmen mit eingeschränktem Security-Personal und Budget einen schnellen und kostengünstigen Weg, Anforderungen an Compliance und Threat Management zu erfüllen. Da alle essenziellen Kontrollfunktionen bereits integriert sind, verschafft die AV-USM gerade kleinen Security-Teams eine Enterprise-Class-mäßige Security-Umgebung. AlienVaults Open Threat ExchangeTM, ein System für den Austausch zum Thema Threat Intelligence zwischen OSSIM-Nutzern und AlienVault-Kunden, stellt dabei sicher, dass AV-USM den Bedrohungen stets einen Schritt voraus ist. AlienVault ist ein Privatunternehmen mit Hauptsitz in Silicon Valley (Kalifornien/USA) und wird von Kleiner Perkins Caufield
 Byers, Sigma, Trident Capital und Adara Venture Partners unterstützt. Die Märkte in Deutschland, Österreich und der Schweiz werden von der AlienVault Deutschland GmbH mit Sitz in Ismaning betreut. Für weitere Informationen besuchen Sie www.alienvault.com oder folgen Sie uns auf Twitter.

Weitere Informationen:
AlienVault Deutschland GmbH
Gutenbergstraße 6
D-85737 Ismaning
 www.alienvault.com
Ansprechpartner:
Oliver Bareiss
Regional Director DACH and Central Europe
Tel.: +49 (0) 89-32 60 70 91
Fax: +49 (0) 89-97 89 93 42
E-Mail: obareiss@alienvault.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Ansprechpartner:
Fabian Sprengel
Tel.: +49 (0) 26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: alienvault@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=538492" width="1" height="1">

Pressekontakt

AlienVault Deutschland GmbH

85737 Ismaning

obareiss@alienvault.com

Firmenkontakt

AlienVault Deutschland GmbH

85737 Ismaning

obareiss@alienvault.com

Weitere Informationen finden sich auf unserer Homepage