AlienVault-Analyse: Hacker greifen über Bitcoin an

AlienVault-Analyse: Hacker greifen über Bitcoin an

Malware speziell für virtuelle Währungen konzipiert
In den vergangenen Wochen diskutierte die IT-Welt vermehrt virtuelle Währungen wie Bitcoin und Co. Sie kommen zu Kaufzwecken, für Spenden oder als Umtauschwährung für Realgeld zum Einsatz. Security-Experte AlienVault hat mit seinem Labs Team das digitale Geld bereits seit einiger Zeit im Blick und präzisiert die Beobachtungen nun für Bitcoins, die Hacker zunehmend missbrauchen. Sie klauen die digitalen Münzen oder nutzen kompromittierte Systeme, um eigenständig virtuelles Geld zu "minen", d.h. herzustellen. Zudem führen sie DoS(Denial of Service)-Attacken aus, um die Wechselrate zu destabilisieren und auf diese Weise von der digitalen Währung zu profitieren.
Bitcoin ist eine dezentralisierte, virtuelle Währung, basierend auf einem Open-Source-P2P-Protokoll. Die Erzeugung und Übertragung führen als "Miner" bezeichnete Rechner aus, die die Information über eine Bitcoin-Herstellung an eine dezentralisierte Datenbank übermitteln. Der Münztransfer läuft per Computer ohne Beteiligung eines Finanzinstituts ab. Den Besitz einer oder mehrerer Bitcoin-Adressen weist der User mittels des sogenannten "Bitcoin Wallet" nach. Über diese Adressen können Nutzer Münzen senden und von anderen empfangen. Da der Mining-Prozess sehr kompliziert und zeitaufwendig ist, haben sich Bitcoin-Pools gebildet, in denen mehrere User zusammen Münzen erzeugen und den Gewinn untereinander teilen. Das virtuelle Geld lässt sich an Online-Börsen wie MtGox, BTC-E oder Virtex tauschen.
Realer Dieb klaut virtuelles Portemonnaie
Mittlerweile haben Hacker die Herstellungs- und Transferprozesse als Ziel für ihre kriminellen Aktivitäten entdeckt. Laut AlienVault-Recherchen stehlen sie z.B. Wallets mittels der mit Malware infizierten Datei "wallet.dat". Ein Beispiel dafür ist eine Version des Schädlings "Khelios", der von infizierten Systemen Spam-Nachrichten verschickt und Daten sowie die Wallet-Datei stiehlt. Diese Datei lässt sich zwar mittels Passwort schützen, was aber AlienVault zufolge nicht ausreicht, da viele Threats Keylogging-Fähigkeiten besitzen und somit den Schutz aushebeln können.
"Andere Malware-Typen hingegen nutzen den Computer ihres Opfers, um Bitcoins zu minen", erklärt Jaime Blasco, Director AlienVault Labs. "Unsere Experten haben festgestellt, dass den meisten Bitcoins ein Stück Code hinzugefügt wird, das sich mit einem öffentlichen oder privaten Mining Pool verbindet, um neue Münzen zu generieren. Bekannte Bedrohungen wie Zeus/Zbot verfügen ebenfalls über Mining-Fähigkeiten, indem sie einen ?Bitcoin-Dämon auf einem infizierten System installieren und darüber das virtuelle Geld erzeugen." Auch die populärste Tauschbörse Mtgox gerät ins Visier: Wie die AlienVault-Spezialisten analysierten, hat z.B. ein Angreifer eine gefakte Website mit der Domain www[.]mtgox-chat[.]info aufgesetzt, die mit einem bösartigen Java Applet verseucht ist.
Für Unternehmen, die ihre Sicherheit gefährdet sehen, eignet sich als Rundumschutz eine Unified Security Management-Plattform wie die USM-Konsole von AlienVault. Sie kombiniert Open Source-Tools für Bestandsaufnahmen (Asset Discovery), Schwachstellenprüfung, Bedrohungserkennung, Verhaltensüberwachung und Sicherheitsinformationen (SIEM). Die neue Version 4.2 ist als virtuelle Appliance erhältlich und steht als kostenfreie 30-Tage-Testversion bereit.
Weitere Informationen zu den Bitcoin Hacks sind unter http://labs.alienvault.com/labs/index.php/2013/how-cybercriminals-are-exploiting-bitcoin-and-other-virtual-currencies/ verfügbar.
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.

AlienVault Deutschland GmbH
Gutenbergstraße 6
D-85737 Ismaning
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
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
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_=530612" 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