Amazons Cloud-Service EC2 für Botnet missbraucht

In einem Interview mit CNET erklärte Don DeBolt von HCL Technologies, einem Unternehmen, das für CA Sicherheitsforschung betreibt, dass er das Botnet bei der Analyse von Spam entdeckte. In einem Malware-Code mit dem Namen xmas2.exe , eine Variante des Zeus-Trojaners, entdeckte er eine URL, die auf einen Rechner innerhalb von EC2 verwies. Über diese URL kommunizierte der Trojaner.

Zeus ist darauf abgestellt, Bankverbindungen zu stehlen und auch in diesem Fall war das das Ziel der Schadsoftware. Der Schädling meldete dann jeweils die IP-Adressen der infizierten Maschinen in die Kommandozentrale in EC2. Den Amazon-Service konnten die Kriminellen über eine Seite knacken, die auf diesem Dienst gehostet wird. Nachdem DeBolt den Vorfall gemeldet hatte, konnte Amazon das Leck schnell beheben.

“Wir nehmen alle Meldungen über Missbrauch des Dienstes sehr ernst und prüfen jeden Hinweis. Wenn wir tatsächlich auf Missbrauch stoßen, handeln wir schnell und unterbinden ihn, was wir auch in diesem Fall getan haben. Unsere Nutzerbedingungen sind klar und wir überwachen ständig die Vorgänge auf unserem Service, um illegale Aktivitäten zu unterbinden.” Zudem würde Amazon den Anwendern mit Best Practices zur Seite stehen, um damit die Anwender vor bösartigen Zugriffen innerhalb und außerhalb der Cloud zu schützen.

DeBolt erklärte, dass die Hacker wohl nicht über ein bestimmtes Sicherheitsleck auf den Amazon-Service zugreifen konnten. Bisher sei völlig offen, wie die Angreifer die Command and Control-Dateien auf den Amazon-Server bringen konnten.

Möglicherweise liegt das Leck in einer Anwendung oder die Hacker konnten der Loging-Dateien habhaft werden, die die Hacker berechtigte, auf den Service zuzugreifen.

Zwar ist dieser Angriff der erste bekannte Fall, bei dem EC2 als Malware-Hoster missbraucht wurde, doch sollte man es als eine klare Warnung auffassen. Denn die Komplexität nimmt für einen Anwender in einem Cloud-Dienst zu und damit wächst auch die Gefahr, dass Fehler gemacht werden, die den Angreifern ein Einfallstor bieten. Einzelne Dienste, die auf EC2 gehostet werden, waren hingegen schon häufiger Ziel von Attacken.

Neben der Botnet-Attacke musste Amazon außerdem mit einem Stromausfall in einem Datenzentrum in Virginia kämpfen. Der Ausfall dauerte rund eine Stunde. Anschließend waren die Administratoren mehrere Stunden beschäftigt, sämtliche Dienste und Instanzen wieder anzustoßen. Offenbar war nicht nur die primäre sondern auch die Notstromversorgung ausgefallen und damit waren einige Server in dem Rechenzentrum ohne Strom.