BlueShield

Wenn DNS zum Spielplatz wird

Doom als Warnschuss für die Unternehmenssicherheit

DNS ist das Telefonbuch des Internets. Doch was passiert, wenn Angreifer dieses Telefonbuch nutzen, um ganze Programme einzuschleusen? Ein aktuelles Experiment des Entwicklers Adam Rice sorgt derzeit in der Tech-Welt für Aufsehen: Er schaffte es, den Spieleklassiker **Doom vollständig in DNS-TXT-Records zu speichern und direkt aus dem DNS-Speicher zu laden.**

Was wie eine technische Spielerei klingt, ist ein massives Alarmsignal für die Cybersicherheit. Hier erfahren Sie, warum herkömmliche Lösungen in so einem Fall versagen und wie Blue Shield Ihre Kunden vor dieser neuen Dimension der Infiltration schützt.

Die Story: 3,8 MB „Fileless“ Payload über Port 53

Adam Rice zerlegte das Spiel in rund 2.000 einzelne TXT-Einträge. Mittels Base64-Kodierung und einem PowerShell-Skript reassemblierte er die Daten direkt im Arbeitsspeicher, ohne dass jemals eine Datei auf die Festplatte geschrieben wurde.

Das Problem

Wäre dieser Code kein harmloses Videospiel, sondern eine Ransomware-Payload oder ein verschlüsselter C2-Kanal, hätten die meisten Sicherheitsarchitekturen keine Chance.

Warum herkömmliche Security-Lösungen blind sind

1

Die Vertrauensfalle (Port 53)

DNS-Verkehr ist essenziell und wird an Firewalls fast universell erlaubt. Da herkömmliche Filter nur bösartige Domains blockieren, aber nicht den Inhalt der TXT-Antworten prüfen, schlüpft der Schadcode als „legitimer Text“ hindurch.

2

Dateilose Angriffe (Fileless Malware)

Da die Payload im Arbeitsspeicher zusammengesetzt wird, schlägt kein klassischer Antivirus-Scanner Alarm – es gibt schlicht keine Datei auf der Festplatte, die gescannt werden könnte.

3

Verschlüsselungs-blindheit

Mit der Zunahme von DNS-over-HTTPS (DoH) verschwinden diese Abfragen in verschlüsselten Strömen, die für Standard-Gateways unsichtbar sind.

BlueShield

Der BlueShield-Schutzwall: Advanced DNS Infiltration & Exfiltration Detection

Blue Shield Umbrella wurde genau für diese Szenarien entwickelt. Die Lösung sieht nicht nur, wohin eine Anfrage geht, sondern versteht, was übertragen wird. Dank der neuesten Release-Features bietet Blue Shield einen Schutz, der weit über herkömmliches Filtering hinausgeht:

- **Score-basiertes Erkennungsmodell:** Blue Shield bewertet jede DNS-Transaktion dynamisch und kombiniert die Erkennung von High-Entropy TXT-Records (ungewöhnlich komplexe Zeichenfolgen) mit der Reassembly von Base64-Chunks. Das System erkennt sofort, wenn jemand versucht, über hunderte Abfragen hinweg einen Datenstrom aufzubauen.
- **File-Magic Byte Fingerprints:** Wie ein digitaler Röntgenscan prüft Blue Shield die reassemblierten Daten auf bekannte Dateiformate. Wenn ein TXT-Record plötzlich die Signatur einer ausführbaren Windows-Datei (4D 5A) enthält, wird die Verbindung unterbrochen – noch bevor der erste Byte-Schadcode ausgeführt werden kann.
- **Passive Infrastructure Checks:** Blue Shield erkennt verdächtige Infrastrukturen. Domains, die ausschließlich massenhaft TXT- oder SRV-Records ausliefern und keine Web- oder Maildienste bereitstellen, werden automatisch als Hochrisiko eingestuft.
- **Keine Fehlalarme (Whitelisting):** Um den Betrieb nicht zu stören, nutzt Blue Shield eine umfassende Whitelist für legitime TXT-Präfixe wie SPF, DKIM oder DMARC. Sicherheit und Produktivität gehen Hand in Hand.

Ihr Business-Vorteil als Reseller

Mit Blue Shield bieten Sie Ihren Kunden eine Lösung, die das „DNS-Vakuum“ schließt. Während andere noch über Blocklisten diskutieren, sichern Sie die Protokollebene selbst ab. Helfen Sie Ihren Kunden, DNS von einer potenziellen Schwachstelle in die erste Verteidigungslinie zu verwandeln.