Lumen veröffentlicht DDoS-Bericht für erstes Quartal 2021 / für Q1 2021

Bericht enthält neuen Blogbeitrag, der jüngste Angriffe auf belgisches Regierungsnetzwerk untersucht

Denver, 19. Mai 2021 – DDoS-Angriffe (Distributed Denial of Service) entwickeln sich in puncto Komplexität, Häufigkeit und Umfang weiter. **Lumen Technologies** (NYSE: LUMN) trackt und entschärft diese Threats – einschließlich der Botnet-Familien Gafgyt und Mirai – und hat hierzu kürzlich seinen DDoS-Bericht für das erste Quartal 2021 veröffentlicht. Der Bericht bietet einen Überblick über die DDoS-Landschaft und identifiziert aktuelle Trends.

Als Grundlage für den Bericht dienten dem Lumen Security Team die Informationen von **Black Lotus Labs** – der unternehmenseigenen Threat Research Unit – und Angriffstrends aus der **Lumen DDoS-Mitigation-Service**-Plattform, die Gegenmaßnahmen direkt in das umfangreiche, globale Netzwerk des Unternehmens einbettet.

„Unternehmen sind zur Einnahmengenerierung zunehmend auf Webanwendungen angewiesen und viele erkennen, dass sie es nicht länger riskieren können, auf grundlegende DDoS-Abwehrmaßnahmen zu verzichten. Die Informationen in diesem Bericht unterstreichen dies einmal mehr“, so Mike Benjamin, Vice President of Security und Black Lotus Labs bei Lumen. „Während sich IoT-DDoS-Botnets kontinuierlich weiterentwickeln, konzentrieren wir uns bei Lumen darauf, unsere tiefen Einblicke zu nutzen, um schädliche Infrastrukturen zu identifizieren und zu zerschlagen."

Zentrale Erkenntnisse:

Der DDoS-Bericht konzentriert sich auf die umfangreichsten Angriffe, die von der globalen DDoS-Scrubbing-Infrastruktur von Lumen gescrubbed wurden.

IoT-Botnets:

- Angesichts von 700 aktiven Command-and-Control-Servern (C2s) und Angriffen auf insgesamt 28.000 verschiedene Opfer sind bekannte IoT-Botnets wie Gafgyt und Mirai nach wie vor ernsthafte DDoS-Bedrohungen.
- Lumen trackte im ersten Quartal weltweit fast 3.000 DDoS-C2s. Die meisten wurden in Serbien (1.260) gehostet, gefolgt von den Vereinigten Staaten (380) und China (373).
- Bei den aktivsten C2s weltweit verzeichneten die Vereinigten Staaten die meisten (163), gefolgt von den Niederlanden (73) und Deutschland (70).

- Lumen trackte mehr als 160.000 globale DDoS-Botnet-Hosts. Mit fast 42.000 befanden sich die meisten davon in den Vereinigten Staaten.

DDoS-Angriffstrends

- Der umfangreichste von Lumen anhand der gescrubbten Bandbreite gemessene Angriff lag bei 268 Gbit/s; der umfangreichste Angriff, gemessen anhand der gescrubbten Packet Rate, lag bei 26 MPPS.
- Der längste DDoS-Angriff, den Lumen für einen einzelnen Kunden entschärfte, dauerte fast zwei Wochen.
- Multi-Vector-Mitigations machten 41 Prozent aller DDoS-Mitigations aus, wobei am häufigsten eine DNS-Query-Flood in Kombination mit einer TCP-SYN-Flood verwendet wurde.
- Finanzwesen, Software und Technologie sowie Regierungseinrichtungen waren die Bereiche, die am stärksten von den 500 umfangreichsten Angriffen im ersten Quartal 2021 betroffen waren.

Tracking von UDP-Reflektoren (User Diagram Protocol)

- Eines der wichtigsten Tools in den Händen von Cyberkriminellen, die die Bandbreite ihrer Angriffe erhöhen wollen, ist UDP-basierte Reflexion mit Hilfe von Services wie Memcached, CLDAP und DNS.
- Bei diesem Prozess fälscht ein Angreifer eine Quell-IP und verwendet dann einen Proxy-Server – oder Reflektor –, um große Antwortpakete an die IP des Opfers zu senden.
- Black Lotus Labs nutzt die über das umfangreiche globale Lumen Netzwerk möglichen tiefen Einblicke, um Services zu identifizieren, die potenziell für diese Art von Angriffen genutzt werden.
- Basierend auf den Daten aus dem ersten Quartal 2021 sind Memcached, CLDAP und DNS laut Black Lotus Labs die Services, die aktuell aktiv genutzt werden.
- Weitere Informationen zu UDP-Reflektoren finden Sie im neuesten Blogbeitrag von Black Lotus Labs: **Tracking von UDP-Reflektoren für ein sichereres Internet**.

Weitere Quellen:

- Lesen Sie den vollständigen **DDoS-Bericht für das erste Quartal 2021**.
- Eine Zusammenfassung der DDoS-Berichtsdaten finden Sie in **dieser Infografik**.
- Erfahren Sie mehr über **UPD-basierte Reflektoren** im neuesten Blogbeitrag von Black Lotus Labs.
- Lesen Sie mehr über den Lumen **DDoS Mitigation Service**.

Erfahren Sie, wie Unternehmen im Falle eines Angriffs mithilfe von **Lumen DDoS Hyper** innerhalb von Minuten ihre **DDoS Mitigation aktivieren** können.

Über Lumen Technologies:

Lumen wird von der Überzeugung geleitet, dass die Menschheit am besten ist, wenn Technologie die Art und Weise, wie wir leben und arbeiten, voranbringt. Mit ca. 450.000 Glasfasermeilen für Kunden in mehr als 60 Ländern liefern wir die schnellste und sicherste Plattform für Anwendungen und Daten, um Unternehmen, Behörden und Kommunen großartige Erfahrungen bereitzustellen. Mehr zu den Netzwerk-, Edge-Cloud-, Sicherheits- sowie Kommunikations- und Collaboration-Lösungen von Lumen und der Zielsetzung des Unternehmens, den menschlichen Fortschritt durch Technologie zu fördern, finden Sie auf **news.lumen.com/home**, LinkedIn: /lumentechnologies, Twitter: @lumentechco, Facebook: /lumentechnologies, Instagram: @lumentechnologies und YouTube: /lumentechnologies. Lumen und Lumen Technologies sind eingetragene Marken von Lumen Technologies, LLC in den Vereinigten Staaten. Lumen Technologies LLC ist eine hundertprozentige Tochtergesellschaft der Lumen Technologies Inc.

For further information: Pressekontakt: Suzanne K. Dawe Lumen Public Relations Connected Security | Black Lotus Labs 720.217.5476 suzanne.dawe@lumen.com

---

https://news.lumen.com/2021-05-28-Lumen-veroffentlicht-DDoS-Bericht-fur-erstes-Quartal-2021