Der jüngste Anstieg von Web-DDoS-Angriffen und wie man sich schützen kann

Hintergrund: Entwicklung der jüngsten Angriffskampagnen

Mit dem Einmarsch Russlands in die Ukraine am 24. Februar 2022 begann eine neue Ära des Cyberkriegs. Als Reaktion auf die angebliche russische Cyber-Aggression gegen die Ukraine gründete die Ukraine die IT-Armee der Ukraine und rekrutierte westliche Hacker, die freiwillig Angriffe gegen russische Ziele durchführten. Zunächst beschränkten sich die Cyberangriffe auf die beiden Konfliktparteien, doch schon bald wurden sie auf weitere Ziele ausgedehnt.

Pro-russische Hacktivistengruppen - darunter NoName057, der KillnetCluster, Anonymous Russia, die Passion-Gruppe und andere - begannen mit Angriffen auf Ziele in Ländern, die die Ukraine unterstützen. In jüngster Zeit kamen religiöse Gruppen wie Anonymous Sudan, Mysterious Team Bangladesch und andere hinzu, die Cyberangriffe gegen Ziele starteten, die Muslime beleidigten.

Diese Cyberangriffe konzentrieren sich auf die Unterbrechung von Diensten und die Verunstaltung von Webseiten und betreffen Krankenhäuser, Flughäfen, Versorgungsunternehmen, Behörden, Finanzdienstleistungen und Medien auf der ganzen Welt. Niemand ist immun.

Die Angriffstaktiken begannen mit netzbasierten Flood-Angriffen in großem Umfang. Später entwickelten sie sich zu ausgefeilteren Multi-Vektor-Angriffen auf Anwendungsebene, die nur schwer zu erkennen und zu entschärfen sind.

OpIsrael ve OpsPetir

Laut der am 12. April veröffentlichten Warnung DragonForce Malaysia: OpsPetir, ist DragonForce Malaysia, eine pro-palästinensische Hacktivistengruppe mit Sitz in Malaysia, ist im dritten Jahr mit umbenannten Operationen gegen Israel zurückgekehrt.

Abbildung 1: DragonForce Malaysia OpsPetir

Nachdem die Bedrohungsgruppe während der Rückkehr von OpIsrael 2023 abwesend war, veröffentlichte sie am 11. April in ihrem Forum eine Pressemitteilung, in der sie alle muslimischen Cyberkrieger, Menschenrechtsaktivisten, Journalisten und Malaysier gleichermaßen aufrief, sich ihrer Operation anzuschließen, die sich gegen Israel richtet. OpsPetir begann offiziell am 12. April um 21.30 Uhr (MEZ), 14.30 Uhr israelischer Zeit, und die Liste der Opfer umfasst große Banken, Universitäten, Regierungsseiten, die israelische Post, Krankenhäuser und andere wichtige Ziele.

Angriffsmethoden

Der Benutzer Pari Malam, alias Night Pari, hat ein Denial-of-Service-Tool namens Cyber-Troopers für OpsPetir veröffentlicht. Das verschleierte Python-Programm enthält Funktionen zum Herunterladen von Listen freier und offener Proxy- und SOCKS-Dienste im Internet von freeproxy-list[.]net und proxyscrape[.]com.

Abbildung 2: Cyber Troopers Angriff Vektoren und Proxy Scraper Merkmal (Quelle: Radware)

Die gesammelten Proxy- und SOCKS-Dienste werden genutzt, um den Ursprung der Angriffe zu verschleiern und zu randomisieren und die Komplexität der Erkennung und Eindämmung von Angriffen auf Layer-7-Anwendungen zu erhöhen. Unter Ausnutzung der TCP-, UDP- und HTTP/HTTPS-Flooding-Fähigkeiten des Tools gelang es der Gruppe, Online-Dienste und Websites in vielen Banken, Universitäten, kritischen Infrastrukturen und Regierungsstellen zu stören und vorübergehend zu deaktivieren, um auf ihre politische Aussage aufmerksam zu machen.

Pro-russische Hacktivisten setzen ausgefeilte Techniken ein

Seit gut einem Jahr sind die pro-russischen Hacktivisten immer erfahrener und ihre Werkzeuge immer ausgefeilter. NoName057(16) ist wohl einer der raffiniertesten Angreifer. NoName verbreitet Bots, die von Freiwilligen betrieben werden und die Websites der Opfer mit vordefinierten GET- und POST-Anfragen angreifen, wobei für jede Anfrage bestimmte Variablen zufällig ausgewählt werden. Die Angriffsvektoren verwenden zufällige Informationen, nutzen aber auch legitime Argumente und Parameter, die von der Website erkannt werden. Die Unterscheidung zwischen legitimen und illegitimen Anfragen ist viel schwieriger als die Erkennung von Angriffsvektoren mit zufällig angehängten Argumenten, die Angreifer in der Regel verwenden, um CDNs zu umgehen.

Neue und störende Web-DDoS-Angriffe

Wie in den jüngsten Angriffskampagnen zu sehen war, nutzen Angreifer mehrere Angriffsarten und -vektoren als Teil einer Kampagne, wobei sie sowohl Angriffsvektoren der Netzwerk- als auch der Anwendungsebene kombinieren und neue Tools einsetzen, um ausgeklügelte Angriffe zu erstellen, die mit herkömmlichen Methoden schwerer und manchmal sogar unmöglich zu erkennen und zu entschärfen sind.

Mit diesen neuen Angriffswerkzeugen generieren Angreifer neue Arten von HTTPS Flood-Angriffen - auch als Web-DDoS-Tsunami-Angriffe bezeichnet -, die noch ausgefeilter und aggressiver sind.

Diese einzigartigen Angriffe haben ein höheres Volumen mit sehr hohen Anfragen pro Sekunde (RPS). Sie sind verschlüsselt und erscheinen als legitime Anfragen. Sie nutzen ausgefeilte Umgehungstechniken, um herkömmliche Anwendungsschutzmechanismen zu umgehen, wie z. B. die Zufallsgenerierung von HTTP-Methoden, Headern und Cookies, die Imitation beliebter eingebetteter Dienste von Drittanbietern, das Spoofing von IPs und andere wichtige Ziele. Zu den Angriffsmethoden auf Anwendungsebene, die in den jüngsten Kampagnen beobachtet wurden, gehörten HTTPS-Get-, Push- und Post-Request-Angriffe mit wechselnden Parametern, hinter Proxies und dynamischen IP-Angriffen. Alle sehen wie legitime Anfragen aus.
HTTP/S Floods und insbesondere Web-DDoS-Tsunami-Angriffe sind komplex zu entschärfen. Die Angriffe erfolgen auf Schicht 7, was bedeutet, dass die meisten Maßnahmen zur Angriffsabschwächung, insbesondere die Überprüfung des Datenverkehrs, nach dem Beenden der Verbindung und der Überprüfung des Inhalts durchgeführt werden müssen. Die Prozesse zur Angriffsabschwächung, die nach dem Datenverkehr stattfinden, werden verschlüsselt und sind allesamt relativ aufwändig und teuer in der Wartung, vor allem im großen Maßstab. Dies macht diese Angriffe zu einer sehr attraktiven Technik für potenzielle Angreifer, um Online-Unternehmen und Dienste zu stören oder zu beeinträchtigen.

Warum die derzeitigen Schutzmaßnahmen unwirksam sind

Der Trend zu verschlüsselten Angriffen und die Zunahme des Umfangs und der Raffinesse dieser Angriffe legt die Messlatte für die Erkennung höher.
Diese Veränderungen machen netzwerkbasierte DDoS-Minderungs-Tools sowie herkömmliche On-Premise- und Cloud-basierte WAF-Lösungen im Wesentlichen unwirksam gegen diese Angriffe. Netzwerkbasierte DDoS-Schutzlösungen sind einfach nicht in der Lage, DDoS-Angriffe auf der Anwendungsebene zu erkennen und genau zu entschärfen. Die Erkennung und Eindämmung solcher Angriffe erfordern die Entschlüsselung des Angriffsverkehrs und eine genauere Untersuchung der L7-Header. Daher würden diese Angriffe von netzwerkbasierten DDoS-Schutzlösungen unentdeckt bleiben.
Eine Standard-WAF - ob vor Ort oder in der Cloud - ist ein effektives Tool zum Schutz von Anwendungen vor webbasierten Standardbedrohungen (hauptsächlich OWASP Top-10). Aus den folgenden Gründen bietet sie jedoch keinen Schutz vor diesen L7 DDoS-Bedrohungen:

- **Ausmaß:** Die Geschwindigkeit einiger dieser Angriffe, gemessen an der Anzahl der Anfragen pro Sekunde (Requests Per Second, RPS), erreicht neue Dimensionen. Im vergangenen Jahr wurden mehrere Angriffe mit mehreren Millionen Anfragen pro Sekunde (RPS) von mehreren Dritten beobachtet und öffentlich bekannt gegeben. Die Raten und das Volumen des Datenverkehrs liegen um mehrere Größenordnungen über der Kapazität der On-Premise-Lösung. Wenn es sich bei der vor Ort installierten WAF um eine ADC mit integrierter WAF handelt, ist die Aufgabe sogar noch komplexer. Dies liegt daran,
dass der ADC mit der Beendigung und Entschlüsselung von Millionen neuer Anfragen pro Sekunde an seine Grenzen stößt, ganz zu schweigen von der Durchführung von Sicherheitsüberprüfungen. Infolgedessen ist die WAF/ADC selbst mit dem Angriff überfordert und ALLE dahinter liegenden Dienste fallen aus - nicht nur die angegriffene URL/Domäne/Anwendung. In diesem Fall hilft es nicht, die WAF mit mehr Kapazität auszustatten, da die Angreifer mit verschiedenen Mitteln immer mehr RPS-Leistung erlangen können.

- **Raffinesse des Angriffs:** Diese Layer-7-DDoS-Angriffe erscheinen als legitime Verkehrsanfragen und werden ständig randomisiert (dynamische IPs und andere Parameter). Daher gibt es keine vordefinierte Signatur oder einen regelbasierten Mechanismus, der auf einer Verbindung basiert, da die Anfragen legitim erscheinen und keine spezifischen schlechten Argumente enthalten. Daher können nur verhaltensbasierte Algorithmen mit Selbstlernfunktion und automatischer Abstimmung solche Angriffe erkennen und abwehren.

- **Morphing-Angriffe: D**ie Dynamik dieser neuen Bedrohungen, d. h. die Häufigkeit, mit der sie Vektoren, Quell-IPs und andere Parameter ändern und randomisieren und diese Änderungen über einen langen Zeitraum aufrechterhalten, ist beispiellos. Um sich vor solchen Angriffen zu schützen, benötigen Unternehmen Lösungen, die sich schnell und in Echtzeit an die Angriffskampagne anpassen können. Eine standardmäßige On-Premise- oder Cloud-basierte WAF ist dazu nicht in der Lage.

- **Der Faktor Mensch:** Die Komplexität von Angriffskampagnen erfordert Sicherheitsexperten, die mit der Komplexität der Angriffe umgehen können und sicherstellen, dass die Qualität des Schutzes während eines Angriffs nicht beeinträchtigt wird. Selbstverwaltete Teams, die nur über begrenztes Personal, Tools und Budgets verfügen, können eine Angriffskampagne nicht rund um die Uhr bewältigen. Außerdem sind On-Prem-Tools hauptsächlich regelbasiert und erfordern die Definition neuer Regeln zur Abwehr von Angriffen. Die Zeit, die für die Analyse des Angriffs und die Bereitstellung einer Regel benötigt wird, bedeutet bei jeder Iteration des Angriffs erhebliche Ausfallzeiten, die von Minuten bis zu Stunden dauern können. All dies und die ständige Veränderung des Angriffs führen zu ständigen Ausfallzeiten.

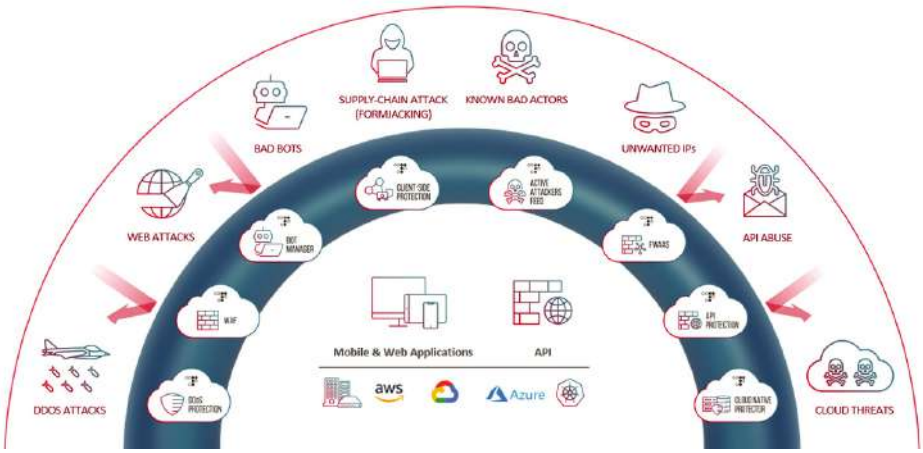
Hinzu kommt, dass zusätzliche herkömmliche Methoden zur Eindämmung dieser Angriffe nicht erfolgreich sein werden. Lösungen, die auf Techniken zur Ratenbegrenzung zurückgreifen, sind nicht in der Lage, den Angriffsverkehr genau vom legitimen Verkehr zu unterscheiden und blockieren den legitimen Verkehr. Auch das Blockieren von Datenverkehr auf der Grundlage des geografischen Standorts seiner Quelle (auch als Geoblocking bekannt) wäre unwirksam, da die Angriffe Botnets nutzen, die weltweit verteilt sind und sich oft im selben Land wie das Ziel selbst befinden.

Was Sie brauchen, um sich zu schützen

Umfassender 360-Grad-Schutz für Cloud-Anwendungen
Um sich vor diesen neuen Kampagnen zu schützen, müssen sich Unternehmen für einen umfassenden, anpassungsfähigen Cloud-Anwendungsschutzdienst entscheiden - einen Dienst, der sie vor Bedrohungsvektoren schützt, während das Unternehmen wächst und die Anwendungen sich weiterentwickeln, und der gleichzeitig den Verwaltungsaufwand eliminiert und die schnellste Schutzzeit ermöglicht.

Der Cloud Application Protection Service von Radware ist eine Komplettlösung für alle Ihre Anforderungen an den Anwendungsschutz. Er kombiniert Best-of-Breed-WAF, Bot-Management, API-Schutz, Client-seitigen Schutz und Web-DDoS-Schutz in einer einzigen Lösung. Der Cloud Application Protection Service von Radware wird durch das Emergency Response Team (ERT) von Radware unterstützt, um einen vollständig verwalteten, umfassenden Schutz bei Angriffen zu bieten.

Abbildung 3: Radware 360-Grad-Schutzdienst für Cloud-Anwendungen



Neuer erweiterter Schutz für Web-DDoS-Angriffe
Als Teil seines Cloud Application Protection Service ist Radwares neuer Cloud Web DDoS Protection-Lösung wurde speziell für den Schutz vor groß angelegten, neu aufkommenden Web-DDoS-Tsunami-Angriffen entwickelt und bietet Kunden einen fortschrittlichen Schutz in dem Umfang, der für die Bekämpfung dieser Bedrohungen erforderlich ist. Die Lösung bietet:

1. Automatisierte, präzise Erkennung und Eindämmung mit minimalen Fehlalarmen

Die Lösung nutzt dedizierte, verhaltensbasierte Algorithmen mit fortschrittlichen Lernfunktionen, um L7-DDoS-Angriffe schnell zu erkennen und chirurgisch zu blockieren, während Fehlalarme minimiert werden und legitimer Datenverkehr nicht blockiert wird. Im Gegensatz zum üblichen volumetrischen Ansatz der meisten Anbieter kann der verhaltensbasierte L7-Schutz von Radware genau zwischen einem legitimen Anstieg des Datenverkehrs (auch Flash Crowd genannt) und einer Flut von Angriffsdaten, die von Angreifern generiert werden, unterscheiden und sicherstellen, dass nur bösartiger Datenverkehr blockiert wird - selbst bei Web-DDoS-Tsunami-Angriffen.

2. Umfassendste Angriffsabdeckung zum Schutz vor den fortschrittlichsten Zero-Day-Angriffen

Einzigartige Algorithmen bieten Schutz vor einer Vielzahl von L7-DDoS-Bedrohungen, einschließlich kleinerer, raffinierter Angriffe, neuer L7-Angriffs-Tools und -Vektoren sowie groß angelegter, raffinierter Web-DDoS-Tsunami-Angriffe. Die Lösung analysiert die fortschrittlichen Bedrohungen sowie ihre zahlreichen Varianten und passt sich an alle Angriffsmuster, Randomisierungsmethoden und Angriffstechniken (Verwendung von Proxys, Imitation legitimer Bots usw.) an.

3. Bester Schutz für DDoS-Tsunami-Attacken im großen Stil

Eine Kombination aus automatisierten Algorithmen und einer groß angelegten Infrastruktur ist erforderlich, um diese hochentwickelten L7-DDoS-Bedrohungen mit hohen RPS-Werten (Anfragen pro Sekunde) präzise abzuwehren.

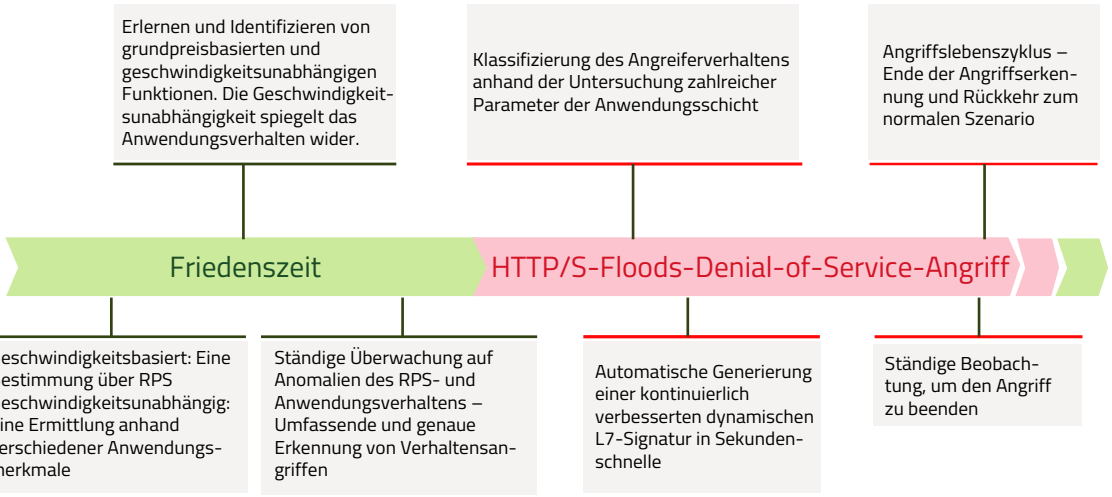


Abbildung 4: Der Lebenszyklus von Radwares Web-DDoS-Schutz zur Angriffsabwehr

Zusammenfassung

Web-DDoS-Angriffe werden immer umfangreicher und raffinierter. Wie bei den jüngsten Angriffskampagnen zu beobachten war, beginnen die Angriffstaktiken mit großvolumigen netzbasierten Flutangriffen und entwickeln sich dann zu ausgefeilteren Multi-Vektor-Angriffen auf Anwendungsebene, die schwer zu erkennen und abzuschwächen sind.

Diese neuen Arten von Web-DDoS-Tsunami-Fluten sind schwerer zu erkennen und abzuschwächen, was sie für potenzielle Angreifer, die Online-Unternehmen und Dienste stören oder beeinträchtigen wollen, äußerst attraktiv macht. Herkömmliche WAF- oder netzwerkbasierte DDoS-Schutzlösungen sind nicht in der Lage, diese L7-DDoS-Bedrohungen zu entschärfen.

Um sich vor diesen neuen Kampagnen zu schützen, müssen sich Unternehmen für einen umfassenden, anpassungsfähigen Cloud-Anwendungsschutzdienst entscheiden - einen Dienst, der sie vor Bedrohungsvektoren schützt, während das Unternehmen wächst und die Anwendungen sich weiterentwickeln, und der gleichzeitig den Verwaltungsaufwand eliminiert und die schnellste Schutzzeit ermöglicht.
Radwares neue Cloud-Web-DDoS-Schutzlösung wurde speziell für die Abwehr dieser
Angriffe entwickelt und nutzt spezielle, verhaltensbasierte Algorithmen, um L7-DDoSAngriffe schnell zu erkennen und zu blockieren, ohne den legitimen Datenverkehr zu behindern.

Die neue Lösung wird als Teil des Cloud Application Protection Service von Radware angeboten, der End-to-End-Anwendungsschutz bietet und es Unternehmen ermöglicht, die Anwendungssicherheit zu verwalten und zu skalieren, wenn das Unternehmen wächst, Anwendungsarchitekturen weiterentwickelt und Cloud-Umgebungen und -Dienste erweitert werden. Sie umfasst:

- **Umfassender Schutz:** Eine zentrale Anlaufstelle für Anwendungsschutzlösungen: WAF, API-Schutz, L7 DDoS-Abwehr und Bot-Management.

- **Sicherheit auf dem neuesten Stand der Technik:** Umfassender Schutz vor bekannten Bedrohungen und Zero-Day-Angriffen auf der Grundlage einer fortschrittlichen, patentierten, auf maschinellem Lernen basierenden Verhaltensanalysetechnologie, die für L3- bis L7-Bedrohungen implementiert ist.

- **Reduzierter Aufwand:** Adaptiver Schutz mit automatischer Richtlinienerstellung und 24x7-Support durch Radwares ERT.

- **Zentralisierte Verwaltung und Berichterstattung:** Verwalten und überwachen Sie die Sicherheit Ihrer Anwendungen von einer Stelle aus, unabhängig davon, wo sie eingesetzt werden.