„State of the Internet“-Sicherheitsbericht

Zusammenfassender Bericht für das
2. Quartal 2017

Akamai

Akamai verarbeitet auf seiner global verteilten Intelligent Platform™ – der weltweit größten und bekanntesten Plattform für die Cloudbereitstellung – täglich mehrere Billionen Webtransaktionen. Somit erfasst Akamai riesige Datenmengen mit Kennzahlen zur Breitbandkonnektivität, Cloudsicherheit und Medienbereitstellung. Mit dem *State of the Internet* möchten wir diese Daten gezielt einsetzen und es Unternehmen und Regierungen dadurch erleichtern, intelligente und strategische Entscheidungen zu treffen. In jedem Quartal veröffentlicht Akamai auf Basis dieser Daten einen *State of the Internet*-Bericht, in dem es vorrangig um Breitbandkonnektivität und Cloudsicherheit geht.

Redaktionsübersicht / In dem *„State of the Internet"-Sicherheitsbericht* sprechen wir über die ständige Weiterentwicklung der technologischen Umgebung. Im zweiten Quartal 2017 stellten wir deutliche Veränderungen des Traffics fest: Unter anderem gibt es weniger IP-Adressen, die an volumetrischen Angriffen beteiligt waren, und außerdem blieben umfangreiche Angriffe aus. Hingegen häufen sich Angriffe auf Webanwendungen, wobei SQL-Injections (SQLi) am zahlreichsten auftreten.

Die Anzahl der von Akamai verzeichneten DDoS-Angriffe liegt in diesem Quartal höher. Auffällig ist, dass die größten Angriffe mit mehr als 100 Gbit/s, die in der Vergangenheit immer öfter auftraten, zum ersten Mal seit drei Jahren nicht auftreten. Die Malwares „WannaCry" und „Petya" haben Unternehmen weltweit getroffen und Schäden in Höhe von über vier Milliarden US-Dollar verursacht. Das Mirai-Botnet wird auch weiterhin für Angriffe auf Organisationen eingesetzt und auch ältere Versionen der Malware werden für neue Zwecke wiederverwendet. Dazu gehört z. B. das PBot-Botnet, das das Akamai Security Intelligence Response Team (SIRT) im aktuellen Bericht untersucht.

Darüber hinaus untersuchten Akamai-Forscher den Traffic eines Malware-Prozesses namens „Domain Generation Algorithm" (DGA). Botnets nutzen den DGA, um eine Vielzahl von Domänen zu erstellen und diese als CnC-Kanäle (Command and Control) zu nutzen. Darunter werden eine Handvoll echter Kanäle versteckt – wie die sprichwörtliche Nadel im Heuhaufen. Wir haben außerdem einen ersten Blick auf Mirai-CnC-Traffic aus über neun Monaten geworfen, um zu ermitteln, wie die Bots miteinander verbunden sind. Damit haben wir unsere Forschungsaktivitäten noch weiter ausgebaut und vertieft.

Laden Sie hier den vollständigen *„State of the Internet"-Sicherheitsbericht* herunter: www.akamai.com/stateoftheinternet-security

DDoS-Update / Die Anzahl der DDoS-Attacken (Distributed Denial of Service) stieg im zweiten Quartal um 28 Prozent an, nachdem der Wert zuvor drei Quartale lang gefallen war. Der Wert der durchschnittlichen DDoS-Angriffe pro angegriffenem Kunden stieg auf ein Hoch von 32 pro Quartal – also jeden dritten Tag eine neue Attacke. Ein einziger Gaming-Kunde wurde allein in diesem Quartal 558 Mal angegriffen.

Das Mirai-Botnet nutzt auch weiterhin eine Vielzahl ungesicherter IoT-Geräte. In diesem Quartal wurde jedoch eine ältere Version der Malware namens „PBot" so umgerüstet, dass Ziele statt mit Zehntausenden mit Hunderten infizierter Nodes angegriffen werden können. Dieses Botnet wurde im größten Angriff des Quartals eingesetzt: eine Attacke mit 75 Gbit/s auf ein Finanzunternehmen.

Der Umfang von DoS-Angriffen schwankt mit der Beliebtheit und Verfügbarkeit neuer Malwarevarianten und Angriffstools. Die größten DDoS-Angriffe 2016 erreichten 500 bis 600 Gbit/s oder sogar mehr – ein deutlicher Anstieg im Gegensatz zu den 2014 und 2015 erreichten 100 Gbit/s. Obwohl die größte bisherige Attacke dieses Quartals mit 75 Gbit/s verhältnismäßig gering war, mahnt uns die Erfahrung zur Vorsicht.

Volumenbasierte Angriffe auf Infrastrukturebene machten 99 Prozent der DDoS-Attacken im zweiten Quartal aus – hauptsächlich aufgrund der Verfügbarkeit von Botnets „zur Miete". Das liegt hauptsächlich daran, dass volumetrische Angriffe, die auf die Anwendungsebene abzielen, eher selten sind. Solche Angriffe greifen eher die Anwendung an, wie z. B. Schwachstellen im Web und in Datenbanken, als mithilfe Brute-Force-Methoden mehr Schlagkraft zu erzielen.

Der Großteil des DDoS-Traffics wird durch Reflection-Techniken generiert, bei denen mithilfe gespoofter IP-Adressen allgemeine Internetprotokolle wiederholt abgefragt und ihre Antworten an das Ziel des Angriffs umgeleitet werden. Die beliebtesten Reflektoren, Domain Name System (DNS) und Network Time Protocol (NTP), verstärken den Traffic um den Faktor 100 und stehen weltweit zur Verfügung.

DDoS-ANGRIFFE [Q2 2017 gegenüber Q1 2017]

- Anstieg der DDoS-Angriffe insgesamt um 28 %
- Anstieg der Angriffe auf Infrastrukturebene (L3 und L4) um 27 %
- Anstieg der Reflection-Angriffe um 21 %
- Anstieg der durchschnittlichen Angriffe pro Ziel um 28 %

GRÖSSTE DDoS-ANGRIFFE

- Q2 2017: 75 Gbit/s
- Q1 2017: 120 Gbit/s
- Q4 2016: 517 Gbit/s
- Q3 2016: 623 Gbit/s
- Q2 2016: 363 Gbit/s

Angriffe auf Webanwendungen / Die Anzahl der Attacken auf Webanwendungen nimmt mit jedem Quartal zu. Während volumetrische DDoS-Angriffe eine Website für einige Minuten, Stunden oder Wochen beeinträchtigen, können Angriffe auf Webanwendungen zur Infektion der Unternehmenssite führen. Damit können deutlich längerfristige und schwerwiegendere Folgen für das Unternehmen entstehen.

ANGRIFFE AUF WEBANWENDUNGEN [Q2 2017 gegenüber Q1 2017]

- Anstieg der Webanwendungsangriffe insgesamt um 5 %
- Anstieg der Angriffe aus den USA (führendes Ursprungsland) um 4 %
- Anstieg der SQLi-Attacken um 21 %

FÜHRENDE VEKTOREN FÜR WEBANWENDUNGSANGRIFFE (Q2 2017)

- SQL-Injection (SQLi): 51 %
- Local File Inclusion (LFI): 33 %
- Cross-Site-Scripting (XSS): 9 %

Attacken auf Webanwendungen unterscheiden sich von volumetrischen Angriffen, da sie nicht darauf abzielen, einen Service durch ein Übermaß an Traffic lahmzulegen. Stattdessen greifen sie Schwachstellen in den Servern an und versuchen, die zugrunde liegenden Services und Systeme zu gefährden. Die meisten Angriffe – SQLi, Local File Inclusion und Cross-Site-Scripting – dienen dazu, an Daten zu gelangen oder Schwachstellen von Webservern auszunutzen.

In vielen Fällen nutzt Akamai Techniken zur Verhaltensanalyse, um potenziell schädliche Aktivitäten zu erkennen und Angriffe auf Webanwendungen zu blockieren. Im zweiten Quartal untersuchten wir DNS-bezogenen Traffic unserer CSI-Plattform (Cloud Security Intelligence), um in infizierten Netzwerken abweichende Verhaltensmuster zu ermitteln. Einige beliebte Botnets nutzen Domain Generation Algorithms (DGA) – eine Technik, die täglich neue Domänennamen generiert und die CnC-Infrastruktur verschiebt, um die Malware-Bekämpfung zu verhindern. Anhand relevanter Eigenschaften und durch den Einsatz von Algorithmen für maschinelles Lernen können wir anormale Verhaltensmuster ermitteln und so die Malware-Aktivität erkennen und blockieren.

Auswirkungen auf Unternehmen / In diesem Quartal stellten wir eine Zunahme der DDoS-Angriffe und Attacken auf Webanwendungen fest, die auf von Akamai geschützte Unternehmen abzielten. Die Zahlen zeigen im Vergleich zu den letzten drei Quartalen einen Rückgang der DDoS-Angriffe. Bedeutet das, dass wir künftig mit einer Zunahme der Angriffe rechnen müssen? Das lässt sich nicht mit Sicherheit sagen. Wir wissen jedoch, dass sowohl Angriffe auf Webanwendungen als auch DDoS-Attacken zyklisch auftreten und dass sie mit jeder Wiederkehr an Stärke gewinnen. Und ohne eine grundlegende Veränderung der Natur des Internets wird sich an dieser Tatsache auch nichts ändern. Deshalb müssen wir uns auf die nächste Angriffswelle vorbereiten.

Wenn wir ermitteln, mit welchen Tools die Angreifer arbeiten, wie z. B. Mirai und PBot, können wir Schlüsse darüber ziehen, was uns in Zukunft erwarten könnte. Auch die Erforschung der Methoden, mit denen sich Malware versteckt (z. B. Domain Generation Algorithms), trägt zur Entschleierung des Traffics bei, der die Malware steuert. Je besser wir wissen, was bei einem Angriff hinter den Kulissen vor sich geht, desto besser können wir Systeme schützen und damit unseren Auftrag erfüllen.

Weitere Analysen und Forschungsergebnisse finden Sie im vollständigen Bericht.

Der *„State of the Internet"-Sicherheitsbericht* für das zweite Quartal 2017 kombiniert Angriffsdaten aus der globalen Infrastruktur von Akamai und spiegelt die Forschung verschiedenster Teams im gesamten Unternehmen wider.

„State of the Internet"-Sicherheitsbericht

***State of the Internet / Sicherheit* – Das Team**
Jose Arteaga, Leiter Akamai SIRT, Data Wrangler – Angriffe im Fokus
Dave Lewis, Global Security Advocate – DDoS-Aktivität, Angriffe auf Webanwendungen
Chad Seaman, Akamai SIRT – Angriffe im Fokus, Mirai-CnC-Cluster (Command and Control)
Wilber Mejia, Akamai SIRT – Angriffe im Fokus
Alexandre Laplume, Akamai SIRT – Angriffe im Fokus
Elad Shuster, Security Data Analyst, Threat Research Unit
Or Katz, Principal Lead and Security Researcher – Domain Generation Algorithm (DGA)
Jon Thompson, Custom Analytics
Shrijita Bhattacharya, Praktikant – Mirai-CnC-Cluster

Redaktionsteam
Martin McKeay, Senior Security Advocate, Senior Editor
Amanda Fakhreddine, Senior Technical Writer, Editor

Entwurf
Shawn Doughty, Creative Direction
Brendan O'Hara, Art Direction/Design

Kontakt
sotisecurity@akamai.com
Twitter: *@akamai_soti* / *@AkamaiDACH* / *@akamai*
www.akamai.com/stateoftheinternet-security

Vollständigen Bericht herunterladen

„State of the Internet"-Sicherheitsbericht

Vollständiger Sicherheitsbericht
für das 2. Quartal 2017

Über Akamai
Als weltweit größte und renommierteste Plattform für die Cloudbereitstellung unterstützt Akamai seine Kunden dabei, ein optimales und sicheres digitales Erlebnis bereitzustellen – auf jedem Gerät, an jedem Ort und zu jeder Zeit. Die stark verteilte Plattform von Akamai weist mit über 200.000 Servern in 130 Ländern eine beispiellose Skalierbarkeit auf und bietet Kunden somit eine überragende Performance sowie einen umfassenden Bedrohungsschutz. Das Akamai-Portfolio für Website- und App-Performance, Cloudsicherheit sowie Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice und Rund-um-die-Uhr-Überwachung begleitet. Führende Finanzinstitute, E-Commerce-Unternehmen, Medien- und Unterhaltungsanbieter sowie Behörden vertrauen auf Akamai. Die Gründe dafür erfahren Sie unter *www.akamai.de*, im Blog *blogs.akamai.com/de* oder auf Twitter unter *@AkamaiDACH* sowie *@Akamai*. Unsere globalen Standorte finden Sie unter *www.akamai.de/locations*. Veröffentlicht: August 2017