ProtonMail bewältigt raffinierten erpresserischen DDoS-Angriff

ProtonMail

Über ProtonMail

- 2013 gegründeter verschlüsselnder Gratis-E-Mail-Dienst mit rund 500.000 Nutzern weltweit (Stand 2015)
- Das Unternehmen wurde Ziel eines Angriffs durch die Hacker-Gruppe „Armada Collective“, bei dem eine Bitcoin-Zahlung in Höhe von rund 6.000 US $ erpresst wurde.
- Eine Welle weiterer, komplexerer Angriffe veranlasste ProtonMail zur Implementierung neuer Prozesse und Lösungen für Erkennung und Abwehr.

Der E-Mail-Serviceprovider ist Ziel einer Vielzahl von DDoS-Attacken, die jeweils über eine Woche andauern.

Große Aufmerksamkeit in den Medien erregten die Angriffe der neuen Hackergruppe „Armada Collective“ auf das Schweizer Unternehmen ProtonMail, einen Anbieter verschlüsselter E-Mail-Services. Nach Eingang einer Lösegeldforderung trafen das Unternehmen mehrere aufeinanderfolgende Angriffswellen. In der Hoffnung, die Attacken stoppen zu können, griff ProtonMail in den Geldbeutel. In Folge kam es jedoch zu weiteren volumetrischen und Burst-Attacken, bei denen mehrere Anwendungs- und Netzwerkvektoren kombiniert wurden.

ProtonMail war als sichere Kommunikationsplattform für Aktivisten, Journalisten, Whistleblower und andere Risikogruppen gegründet worden. Doch mit der Erpressung durch das „Armada Collective“ wurde das Unternehmen selbst in seiner Sicherheit bedroht.

Der Schweizer E-Mail-Provider war fortgesetzten Attacken aus zwei verschiedenen Quellen ausgesetzt – die erste Angriffswelle hatte finanzielle Hintergründe, mit der zweiten sollte die grundlegende Mission von ProtonMail unterminiert werden. Da die Attacken nach Eingang des Erpresserschreibens anfingen, entschloss sich ProtonMail schließlich unter Druck zur Zahlung der geforderten Summe in Bitcoins. Jedoch gingen die volumetrischen und Burst-Attacken, bei denen mehrere Anwendungs- und Netzwerkvektoren kombiniert wurden, unvermindert weiter.

Der Fall ProtonMail zeigt einmal mehr, wie sehr sich die Motivation für Cyberangriffe inzwischen verändert hat. Publicity und Vandalismus sind nicht länger die Hauptanreize, stattdessen stehen finanzielle oder ideologische Gründe im Vordergrund – oder ganz einfach die Absicht, einem Gegenspieler einen möglichst großen Schaden zuzufügen. Im Global Application & Network Security Report 2015–2016 stellte Radware fest, dass Schutzgeldforderungen als Hauptmotiv von Cyberangriffen von 16 % im Jahr 2014 auf 25 % im Jahr 2015 zugenommen hatten.

Der Angriffsverlauf und die vom Radware Emergency Response Team (ERT) ergriffenen Gegenmaßnahmen sind in den folgenden Abschnitten zusammengefasst.

Angriffe auf ProtonMail: zeitlicher Ablauf

4. November 2015

Kurz vor Mitternacht erhält ProtonMail per E-Mail ein Erpresserschreiben vom „Armada Collective“. Ähnlich wie DD4BC erpresst diese Gruppierung unter Androhung einer DDoS-Attacke von Unternehmen Lösegeldzahlungen in Bitcoins. Entsprechend ihrem üblichen Modus Operandi lässt sie dem Erpresserschreiben einen ersten DDoS-Angriff folgen, der ProtonMail etwa 15 Minuten lang offline nimmt.

Um 11 Uhr am Folgetag trifft eine weitere Welle von DDoS-Attacken das Rechenzentrum von ProtonMail. Der ISP des Unternehmens beginnt mit Abwehrmaßnahmen. Innerhalb weniger Stunden erreichen die Angriffe jedoch eine beispiellose Raffinesse.

Um 14 Uhr werden die Infrastruktur der Upstream-Provider von ProtonMail und das Rechenzentrum selbst angegriffen. Der Angriff auf den ISP von ProtonMail übersteigt 100 Gbit/s. Betroffen sind nicht nur das Rechenzentrum, sondern auch Router in Zürich, Frankfurt und an anderen Standorten des ISPs. Der koordinierte Angriff auf zentrale Infrastrukturelemente legt sowohl das Rechenzentrum als auch den ISP lahm. Neben ProtonMail werden Hunderte anderer Unternehmen in Mitleidenschaft gezogen.

Auf massiven Druck Dritter hin zahlt ProtonMail schließlich widerwillig das Lösegeld in Form von Bitcoins. Im Blog von ProtonMail wurde dies später wie folgt kommentiert: „Das war eine kollektive Entscheidung aller betroffenen Unternehmen, und obwohl wir anderer Ansicht waren, haben wir die Entscheidung respektiert. Berücksichtigt haben wir dabei auch die Schäden in Höhe von Hunderttausenden Schweizer Franken, die anderen betroffenen Unternehmen entstanden waren. Durch die Zahlung hofften wir, die anderen Firmen schützen zu können, doch die Angriffe gingen unvermindert weiter. Die Entscheidung war eindeutig falsch, deshalb sagen wir es zukünftigen Angreifern ganz klar: ProtonMail wird NIEMALS wieder Lösegeld bezahlen.“

5.-7. November 2015
In den nächsten drei Tagen hat ProtonMail erneut mit komplexen, großvolumigen Angriffen aus einer zweiten unbekannten Quelle zu kämpfen.

8. November 2015
ProtonMail nimmt die Zusammenarbeit mit dem Radware Emergency Response Team auf und implementiert die Lösung zur Angriffsabwehr. Kurz darauf kann der Dienst wieder hergestellt werden.

„Zur Abwehr der DDoS-Angriffe gegen uns sind wir eine Partnerschaft mit Radware eingegangen, einem der weltweit führenden DDoS-Schutz-Anbieter. Mit Radware fanden wir eine Lösung, welche den Schutz von ProtonMail ohne Abstriche bei der E-Mail-Sicherheit gewährleisten konnte“, so Andy Yen, CEO von ProtonMail. „Angesichts der massiven Angriffe war uns klar, dass wir mit den Besten der Besten arbeiten müssten. In der BGP-Redirection-Lösung von Radware haben wir genau das gefunden, worauf es uns ankam. In der Stunde der Not boten uns viele Unternehmen Hilfe zu exorbitanten Kosten, aber Radware machte uns ein angemessenes Angebot, um uns möglichst schnell wieder online zu bringen. Mit Radware DefensePipe konnten wir dann die fortdauernden Angriffe endgültig abwehren.“

9.-15. November 2015
Die Angriffe werden mit einem hohen Volumen, zu Spitzenzeiten 30 bis 50 Gbit/s, fortgesetzt, können aber durch Radware erfolgreich eingedämmt werden.

Am 15. November um 14.34 Uhr wird eine kurze UDP-Spitze von 2 Gbit/s verzeichnet, diese wird aber erfolgreich blockiert. Minuten später geht der UDP-Angriff weiter. Der Traffic erreicht 7 Gbit/s, kann aber erneut mitigiert werden. Um 11.01 Uhr steigt der Traffic auf zunächst 17 Gbit/s an, später auf bis zu 40 Gbit/s. Abermals können die Attacken durch ProtonMail und Radware abgewehrt werden. Der Angriffsvektor ändert sich: Auf die DP2-Infrastrukturrichtlinien prasseln ca. 10 Gbit/s ein. Zum Teil geht dies mit einer verteilten DNS-Amplifikations-Attacke einher; beides kann erfolgreich mitigiert werden.

Am 16. November wird um 3.20 Uhr morgens ein kurzzeitiger Angriff mit 150 Mbit/s Traffic erkannt. Radware kann diesen vereiteln.

„Nach mehreren Tagen intensiver Arbeit ist es uns gelungen, die DDoS-Angriffe gegen uns weitgehend zu entschärfen“, schrieb das Unternehmen am 10. November in seinem Blog. „Durch diese Angriffe war ProtonMail offline und der Zugriff auf E-Mails unmöglich, aber die Sicherheit unserer Infrastruktur und Daten wurde nicht verletzt. Aktuell gehen die Angriffe weiter, sind aber nicht mehr in der Lage, ProtonMail für längere Zeit offline zu nehmen. Während der Wiederherstellung unserer Infrastruktur kann es in den nächsten Tagen weiterhin zu kurzzeitigen Service-Unterbrechungen kommen. Alle Dienste sind jedoch weitgehend wieder-hergestellt. Dieser Erfolg war nur dank des beherzten Einschreitens von IP-Max und Radware möglich, und wir möchten uns dafür bei ihnen ganz herzlich bedanken.“

Analyse der Angriffe

Nach den Angriffen tauschte ProtonMail in Zusammenarbeit mit MELANI, einer Abteilung der schweizerischen Bundesregierung, Informationen mit anderen ebenfalls betroffenen Firmen aus. Dabei wurde klar, dass die Attacke gegen ProtonMail in zwei Phasen abgelaufen war und es sich mit ziemlicher Sicherheit um zwei separate Kampagnen handelte. In der ersten Phase fand ein volumetrischer Angriff auf die IP-Adressen des Unternehmens statt. In der zweiten, komplexeren Phase wurden Schwachstellen in der Infrastruktur des ISPs von ProtonMail angegriffen.

Im Blog von ProtonMail wurde das wie folgt kommentiert: „Diese zweite Phase wurde bei den anderen jüngsten Angriffen auf Schweizer Unternehmen nicht beobachtet und war technisch wesentlich anspruchsvoller. Das heißt, dass ProtonMail wahrscheinlich von zwei unabhängigen Gruppen angegriffen wurde, wobei die zweite Hackergruppe Fähigkeiten zeigte, die man eher bei staatlich finanzierten Akteuren erwarten würde. Und es belegt, dass die zweite Gruppe keinerlei Bedenken hatte, massive Kollateralschäden zu verursachen, nur um uns zu schaden.“

Schlussfolgerungen

Wer das nächste Opfer einer Erpressung werden könnte, lässt sich nicht vorhersagen. Unternehmen sollten deshalb ihre Netzwerke proaktiv vorbereiten und geeignete Notfallpläne in der Tasche haben. Bei einem Erpressungsversuch ist es von großer Bedeutung, die richtigen Abwehrmaßnahmen zu ergreifen. Die Erfahrungen von ProtonMail zeigen, was für angegriffene Unternehmen wichtig ist:

- Eine Sicherheitslösung zum Schutz der Infrastruktur vor Multi-Vektor-Attacken – sowohl vor netzwerk- und applikationsbasierten DDoS-Angriffen als auch vor volumetrischen Angriffen, deren Ziel eine Überlastung des Internetzugangs ist

- Eine Hybridlösung, die eine Vor-Ort-Erkennung und einen cloudbasierten Schutz bei volumetrischen Angriffen beinhaltet. Dies ermöglicht eine schnelle Erkennung, sofortige Eindämmung und Schutz der Netzwerke vor volumetrischen Angriffen auf den Internetzugang.

- Ein Cyber-Security-Notfallplan einschließlich Notfallteam und Notfallprozesse. Dabei sollten auch Bereiche ermittelt werden, in denen Unterstützung durch Dritte erforderlich ist.

- Sorgfältige Überwachung von Sicherheitswarnungen und Untersuchung von Triggern. Bestehende Richtlinien und Schutzmaßnahmen sollten dahingehend optimiert werden, dass Fehlalarme vermieden und auftretende echte Bedrohungen sicher identifiziert werden können.

Weitere Informationen: DDoS Warriors

Mehr zu den heutigen Angriffsvektoren, den wirtschaftlichen Folgen von Cyber-Attacken sowie neu entwickelten Angriffsmethoden und -Tools erfahren Sie unter DDoSWarriors.com. Auf dieser vom Radware Emergency Response Team (ERT) betriebenen Website finden Sicherheitsexperten alles, was man über DDoS-Angriffe und Cybersicherheit wissen muss.