Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | **VORFALL** | IT-ASSETS

DDoS-Entwicklungen vor Black Friday und Cyber Monday

CSW-Nr. 2021-269757-1132, Version 1.1, 15.11.2021

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Der Jahreszeit entsprechend, beobachtet das BSI auch dieses Jahr einen Anstieg der Aktivitäten im DDoS-Bereich vor den anstehenden umsatzstarken Onlineaktivitäten im E-Commerce-Bereich (Black Friday, Cyber Monday, Vorweihnachtsgeschäft, Weihnachtsgeschäft).

Hierbei wurden in zwei Bereichen herausragende Entwicklungen beobachtet:

1. Entwicklung von DDoS-Angriffsinfrastrukturen:

Bereits Ende August / Anfang September 2021 kamen DDoS-Angriffsinfrastrukturen zum Einsatz, mit denen seit mehreren Monaten bestehende Rekordwerte von DDoS-Parametern übertroffen wurden.

Beim Angriff auf die Microsoft Azure-Cloud wurde ein neuer Rekordwert bei der Spitzenangriffsbandbreite (Einheit: bits per second, bps) von 2,4 Tbps erreicht. Der Angriffsvektor war ein UDP-Reflection-Angriff, die Angriffsdauer erstreckte sich über mehr als zehn Minuten, mit sehr kurzlebigen Bursts, die jeweils innerhalb von Sekunden auf Terabit-Volumen anstiegen. Insgesamt wurden drei Spitzenwerte beobachtet, den ersten mit 2,4 Tbps, den zweiten mit 0,55 Tbps und den dritten mit 1,7 Tbps. [MIC2021]

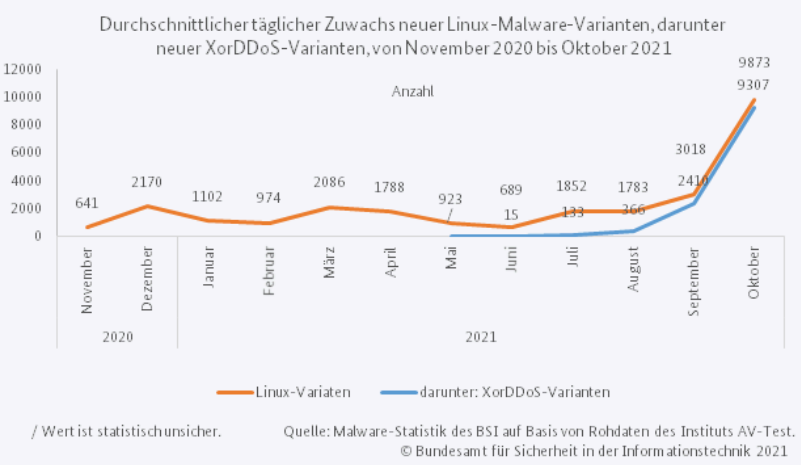
Beim Angriff gegen Yandex kam das Meris-Botnetz zum Einsatz, mit welchem ein neuer Anfrageraten-rekordwert (Einheit: requests per second, rps) mit nahezu 22 Mrps erreicht wurde. Das Meris-Botnetz besteht zum großen Teil aus zahlreichen Home-Routern des lettischen Herstellers MikroTik. [REU2021]

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

BSI IT-Sicherheitsinformation

Auch in anderen DDoS-Angriffsinfrastrukturen konnten ungewöhnliche Entwicklungen beobachtet werden:

Im Oktober 2021 wurden mit durchschnittlich 9307 neuen Varianten pro Tag rund 286 Prozent mehr neue Varianten der XorDDoS-Malware bekannt, als noch im Vormonat. Als Malware-Variante zählt hierbei jede im Hinblick auf ihren Hashwert einzigartige Variante einer Malware.XorDDoS ist ein Linux-Trojaner, der auf Docker Server zielt [TREN2020]. Das XorDDoS-Botnetz wurde bereits vor Jahren für großvolumige DDoS-Angriffe genutzt.



2. Entwicklung von DDoS-Schutzgelderpressungen:

Die Anzahl der Vorfälle im Zusammenhang mit DDoS-Schutzgelderpressung erfahren weiterhin einen stetigen Zuwachs. Seit Oktober 2019 stehen sie verstärkt in der öffentlichen Wahrnehmung, als Erpressergruppen begannen, im Namen von bekannten APT-Gruppierungen DDoS-Angriffe mit Lösegeldforderungen auszuführen. Im Laufe der Zeit verlagerten sich die Aktivitäten der Angreifer auf unterschiedliche Branchen. Aktuelle Kampagnen richten sich vornehmlich gegen Telekommunikationsanbieter / VoIP-Provider und E-Mail-Provider im nationalen und internationalen Raum.

2a. Beispiele für bekannt gewordene Schutzgelderpressungen gegen Telekommunikationsanbieter / VoIP-Provider:

1. August 2021 britische VoIP-Anbieter Voip Unlimited & Voipfone [DAB2021a]
2. September 2021 bis 16. September 2021 Belgisches Telekommunikationsunternehmen Edpnet [ISU2021]
3. September 2021 Kanadischer Voice-over-IP Provider VoIP.ms [BLE2021a]
4. September bis 29. September 2021 U.S. Unternehmen Bandwith [TWI2021]
5. Oktober bis 08. Oktober 2021 britische VoIP-Anbieter VoIP Unlimited [TREG2021]
6. Oktober 2021 britische VoIP-Anbieter Voipfone [DAB2021b]
7. November 2021 U.S. Unternehmen Telnyx [BLE2021b]

2b. Beispielhafte bekannt gewordene Schutzgelderpressungskampagne gegen E-Mail-Provider:

Zwischen Donnerstag, dem 21.10.2021 und Montag, dem 25.10.2021 fand eine DDoS-Schutzgelderpressungskampagne gegen mindestens sieben E-Mail-Serviceprovider statt, welche E-Mail-Dienste mit Sicherheitsfunktionen anbieten. Neben dem deutschen Provider Posteo waren im internationalen Umfeld die Unternehmen Runbox, Fastmail, TheXYZ, Guerilla Mail, Kolab Now, und RiseUp betroffen.

Die Unternehmen erhielten nach den DDoS-Angriffen (Spitzen bis zu 256 Gbps) eine Schutzgeldforderung in Höhe von 0,06 BTC (ca. $4.000). [TREC2021]

Bewertung

Besonders die rekordbrechenden DDoS-Angriffsinfrastrukturen verfügen über ein hohes Angriffspotenzial, mit welchem sich im Falle eines Angriffs auch bei bisher ausreichenden Schutzmaßnahmen entsprechende Auswirkungen erzielen lassen könnten.

Es kann davon ausgegangen werden, dass die aktuell entwickelten DDoS-Angriffsinfrastrukturen sowohl im nationalen als auch im internationalen Umfeld bei den genannten umsatzstarken Onlineaktivitäten im E-Commerce-Bereich so oder in ähnlicher Form zum Einsatz kommen werden.

Im Vorfeld von Black Friday und Cyber Monday sowie des Vorweihnachtsgeschäfts könnten die neuen Varianten des XorDDoS-Botnetz den Angreifern insbesondere dazu dienen, das Botnetz weiter zu vergrößern, d.h. mehr Systeme zu infizieren und damit mehr Ressourcen für DDoS-Angriffe verfügbar zu machen.

In diesem Jahr wird besonders bei den DDoS-Schutzgelderpressungen ein signifikanter Zuwachs erwartet.

Maßnahmen

Organisationen wird empfohlen, ihre DDoS-Schutzmaßnahmen gegen aktuelle DDoS-Angriffstechniken zu evaluieren, um der aktuellen Bedrohungslage begegnen zu können. Hierbei sollte besonderes Augenmerk auf UDP-Reflection-Angriffe und Angriffe mit hohen Anfrageraten gelegt werden. Prüfen Sie zudem, welche Folgen der Ausfall verschiedener angreifbarer Komponenten sowie Nebenwirkungen "benachbarter" Systeme auf ihre Institution haben kann.

Weiterhin wird empfohlen, zeitnah Handlungspläne im Falle von DDoS-Erpressungsversuchen zu erstellen. Das BSI empfiehlt, nicht auf Schutzgeldforderungen einzugehen.

Eine Liste von qualifizierten DDoS-Mitigations-Dienstleistern finden Sie unter [BSI2021a]. Weitere Informationen zu DDoS-Abwehrmaßnahmen finden Sie unter [BSI2021b].

Als Präventivmaßnahme gegen XorDDoS empfiehlt es sich, Telnet zu deaktivieren und SSH mindestens mit einem starken Passwort oder asymmetrischem Key abzusichern. Gegen SSHBruteforcing kann fail2ban eingesetzt werden; ein Python-Programm, das Serverdienste absichern kann.

Links

[BLE2021a] - VoIP.ms phone services disrupted by DDoS extortion attack
https://www.bleepingcomputer.com/news/security/voipms-phone-services-disrupted-by-ddos-extortion-attack/

[BLE2021b] -Telnyx is the latest VoIP provider hit with DDoS attacks
https://www.bleepingcomputer.com/news/security/telnyx-is-the-latest-voip-provider-hit-with-ddos-attacks/

[BSI2021a] - Qualifizierte DDoS-Mitigation Dienstleister
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf

[BSI2021b] -DDoS-Angriffe im Cyber-Raum
https://www.bsi.bund.de/ddos

[DAB2021a] - UK telecom firms under ddos-attacks
https://www.databreachtoday.com/2-uk-telecom-firms-under-ddos-attacks-a-17458

[DAB2021b] - Voipfone ddos-attacks raise specter protection racket
https://www.databreachtoday.com/voipfone-ddos-attacks-raise-specter-protection-racket-a-17805

[ISU2021] -Outage: General DDoS on edpnet services
https://issues.edpnet.be/?p=3507

[MIC2021] -Business as usual for Azure customers despite 2.4 Tbps DDoS attack
https://azure.microsoft.com/en-us/blog/business-as-usual-for-azure-customers-despite-24-tbps-ddos-attack/

[REU2021] -Russia's Yandex says it repelled biggest DDoS attack in history
https://www.reuters.com/technology/russias-yandex-says-it-repelled-biggest-ddos-attack-history-2021-09-09/

[TEC2021] -VoIP.ms Faces DDoS Attack, Hackers Demand 100 Bitcoin
https://techdator.net/voip-ms-faces-ddos-attack-hackers-demand-100-bitcoin/

[TWI2021] - Twitter Beitrag von Potomac Pediatrics

https://twitter.com/potomackids/status/1442880833765978113

[TREG2021] -UK's VoIP Unlimited hit by DDoSes again, weeks after ransom-linked attacks KO'd it
https://go.theregister.com/feed/www.theregister.com/2021/10/08/voip_unlimited_limited_by_outage/

[TREC2021] -DDoS attacks hit multiple email providers
https://therecord.media/ddos-attacks-hit-multiple-email-providers

[TREN2020] -XORDDoS, Kaiji Variants Target Exposed Docker Servers
https://www.trendmicro.com/en_us/research/20/f/xorddos-kaiji-botnet-malware-variants-target-exposed-docker-servers.html

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.