TLP: GREEN

21. Juli 2015

RISIKOFAKTOR: HOCH

Analyse der DDoS-Erpressung durch DD4BC

Seit Ende Juni 2015 ist die cyberkriminelle Gruppierung DD4BC in Deutschland und Österreich mit Erpressungsversuchen mittels DDoS-Attacken vermehrt aktiv. Das Link11 Security Operation Center (LSOC) hat bereits zahlreiche Attacken abgewehrt und die Angriffsmuster, sowie die Gefährdung analysiert. Die vorliegende Link11 Sicherheitsanalyse „DDoS-Erpressung durch DD4BC" fasst die Ergebnisse zusammen.

Zentrale Erkenntnisse

Ziel:	DDoS-Erpressung zur Erlangung von Bitcoins.
Täter:	DD4BC agiert bereits seit 2014 auf internationaler Ebene. Bei den Erpressern DD4BC könnte es sich um einen Einzeltäter, aber auch um eine vernetzte Gruppe handeln. Die Korrespondenz erfolgt in Englisch.
Opfer:	DD4BC hat ihre DDoS-Erpressungen von Bitcoin-Plattformen und Gaming-Webseiten auf Enterprise-Kunden im Finanzsektor sowie SaaS- und Hosting-Unternehmen ausgeweitet und attackiert gezielt entsprechende Großunternehmen. Zuerst waren nur Unternehmen in den USA betroffen. Inzwischen ist die Erpressungswelle in Europa angekommen. Nach Großbritannien und der Schweiz konzentrieren sich die die Erpresser aktuell auf Unternehmen in Deutschland.
Strategie:	In einer Erpresser-E-Mail fordert DD4BC branchenabhängig bis zu 50 Bitcoins. Parallel dazu erfolgt eine erste DDoS-Attacke als Warnung, um die Forderung zu untermauern. Bleibt die Zahlung aus, startet DD4BC eine anhaltende DDoS-Attacke und erhöht die Forderung.
Methode:	Das Angriffsmuster der DDoS-Attacken ähnelt sich jeweils stark. Zu Beginn erfolgt eine UDP-Flood auf die Webserver, worauf in den meisten Fällen eine TCP-SYN-Flood folgt. Insgesamt dauert der Angriff in der Regel zirka eine Stunde und erreicht Peak-Bandbreiten nahe 100 Gbps.
Gefährdung:	Insbesondere durch die unangekündigte erste DDoS-Attacke und die vermehrten Vorfälle in der DACH-Region ist die Gefahr für ungeschützte Unternehmen in Deutschland momentan sehr hoch.

1. Das Profil von DD4BC

DD4BC (DDoS for Bitcoins) ist eine cyberkriminelle Gruppierung, die DDoS-Attacken gezielt gegen Unternehmen einsetzt, um Bitcoins zu erpressen. Die Attacken erreichen ein Volumen, das Web-basierte Services und Prozesse sowie Unternehmensnetzwerke meist vollständig zum Erliegen bringt. Die Erpresser haben dabei keine Angst vor Strafverfolgung. Sie fühlen sich scheinbar sicher und rühmen sich „keine Amateure zu sein".

> „If you are thinking about reporting this to authorities, feel free to try. But it won't help. We are not amateurs."

Bild1: Auszug aus einem Original-Erpresserschreiben von DD4BC

Basierend auf einer Open Source Intelligent Analyse (OSINT) sind die DDoS-Erpressungen von DD4BC schon seit Februar 2014 aktiv. Zu den ersten öffentlichen Erwähnungen der Gruppe zählt die Erpressung des Bitalo Bitcoin Exchange am 1. November 2014.

Drei Prinzipien kennzeichnen dabei das Vorgehen von DD4BC:

1. An der Ernsthaftigkeit ihrer Forderungen lassen die Erpresser keine Zweifel. Wer nicht zahlt, der wird mit einer großvolumigen DDoS-Attacke angegriffen.

2. Im Gegensatz zu verbreiteten „Massenerpressungen" setzt DD4BC die Opfer einzeln unter Druck. Mögliche Kontaktpersonen auf Unternehmensseite werden dabei gezielt recherchiert und gemeinsam kontaktiert.

3. Die Erpresser gehen länderweise vor. Nach Erpresserwellen in den USA, Australien und Neuseeland hat DD4BC nun auch Europa im Blick. Im Mai warnten sowohl das britische Cyber Security Information Sharing Partnership (CISP), als auch das Schweizer Swiss Governmental Computer Emergency Response Team vor DD4BC. Beide staatlichen Organisationen veröffentlichten Guidelines. Auch in Skandinavien sind die Erpresser seit Juni 2015 aktiv.

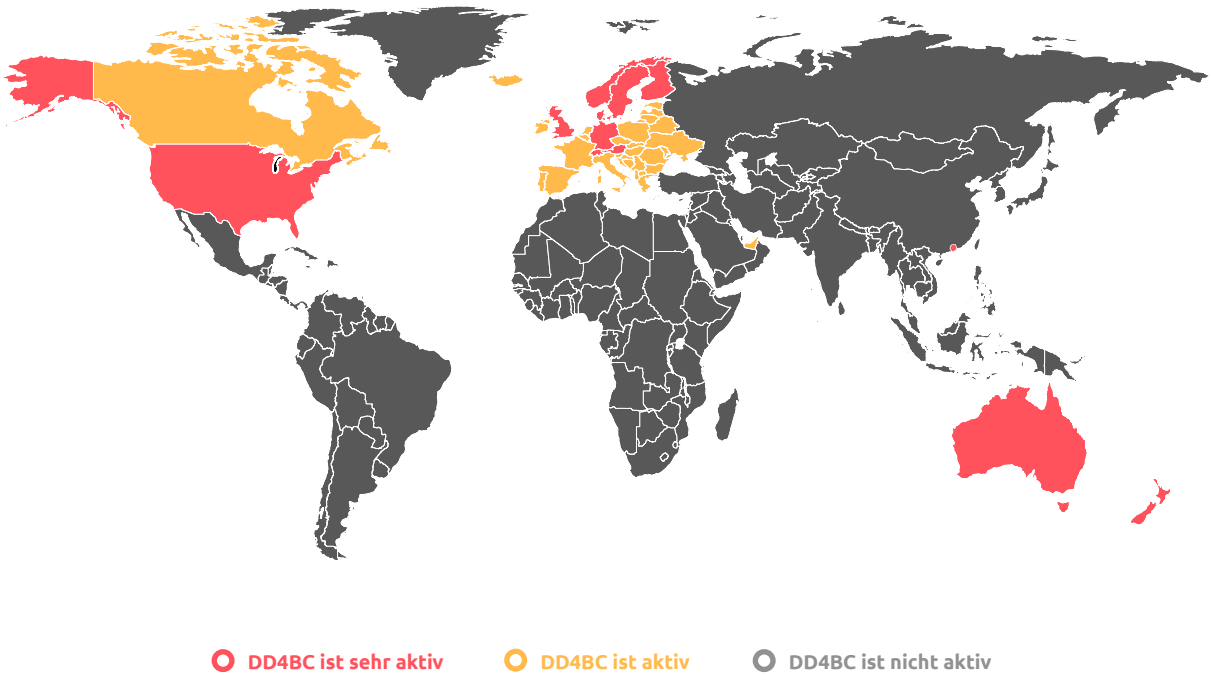

Bild2: Länder, in denen DD4BC bereits Unternehmen erpresst hat.

2. Das Vorgehen von DD4BC

In einer ersten E-Mail fordert DD4BC branchenabhängig zwischen 30 bis 50 Bitcoins (ca. 7.000 bis 11.500 Euro) innerhalb von 24 Stunden. Sollte die Zahlung ausbleiben, droht DD4BC mit anhaltenden DDoS-Attacken mit einem Volumen von 400 bis 500 Gbps und erhöht die Schutzgeldforderung auf 50 bis 100 Bitcoins. Die Forderung steigt weiter im Stunden-Takt.

DD4BC untermauert die Ernsthaftigkeit ihrer Forderungen mit einer ersten DDoS-Attacke als Warnung, welche bereits ein Volumen von mindestens 20 Gbps Bandbreite erreicht. In Folge-E-Mails erinnert DD4BC an die Zahlungsfrist und droht neben der DDoS-Attacke weitere Konsequenzen durch öffentliche Rufschädigung an.

> „And if, within 24 hours not paid, not only that attack will start and price will go up, but we will go publicly and say that we are ddosing you, that you are in capable of protecting your site and it's time for your members to move on to another casinos."

Bild3: DD4BC droht mit Rufschädigung.

Nach dem Auslaufen des Ultimatums startet der angekündigte DDoS-Angriff mit Peaks im zweistelligen Gbps-Bereich.

3. Beispiele der Erpresser-E-Mails

DD4BC richtet das Erpresserschreiben an möglichst viele öffentlich einsehbare Ansprechpartner des Unternehmens, welche vorher akribisch recherchiert werden. Link11 liegen Schreiben vor, welche an bis zu 12 Führungspersonen aus dem jeweiligen Unternehmen adressiert waren. Die Absender verwenden zur Verschleierung anonyme Mail-Dienste, wie openmailbox.org und tutanote.com. Neben der E-Mail-Adresse geben die Erpresser auch eine Bitmessage-Adresse für die Kontaktaufnahme an. Die Texte der aktuell vorliegenden Erpresserschreiben sind fast identisch.

Von: DD4BC Team [mailto:dd4bc@openmailbox.org]
Betreff: DDOS ATTACK !
Hello,
To introduce ourselves first:
http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks/
http://bitcoinbountyhunter.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info
Or just google "DD4BC" and you will find more info.

So, it's your turn!

You are going under DDoS attack unless you pay 30 Bitcoin.
Pay to xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.

Right now we are running small demonstrative attack on xxx.xx.xxx.xxx

Don't worry, it will not be hard (we will try not to crash it at this moment) and will stop in 1 hour. It's just to prove that we are serious.We are aware that you probably don't have 30 BTC at the moment, so we are giving you 24 hours to get it and pay us.

Find the best exchanger for you on howtobuybitcoins.info or localbitcoins.com You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet. Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 30 BTC to xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
– we will know it's you and you will never hear from us again. We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated.
If you need to contact us, feel free to use some free email service. Or contact us via Bitmessage: BM-xxxxxxxxxx

But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 50 BTC and will keep increasing for every hour of attack.

Many of our „clients" believe that if they pay us once, we will be back.
That's not how we work - we never attack the same target after we are paid.

If you are thinking about reporting this to authorities, feel free to try. But it won't help. We are not amateurs.

REMEMBER THIS: It's a one-time payment. Pay and you will not hear from us ever again!

We do bad things, but we keep our word.

Thankyou.

Bild4: Erpresserschreiben von DD4BC

Die Erpresser-E-Mail wird von einer DDoS-Attacke begleitet. Das Ende dieser Warnattacke kündigt DD4BC ebenfalls per E-Mail an.

Von: DD4BC Team
Betreff: Stopping now!
It looks that all your services went offline, so we are stopping the demonstration right now! if you need to contact us, please don't use email, but Bitmessage. It's safe and anonymous.
BM-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Bild5: DD4BC kündigt das Ende der Warn-Attacke an.

Nach Ablauf der Zahlungsfrist fasst DD4BC bei seinen Opfern per E-Mail nach. Diese Erinnerungs-Mails basieren auf demselben E-Mail-Verteiler wie die erste Erpresser-Mail. Die Nachfass-Mails sind jedoch kürzer und individueller. Neben der Ausweitung der Zahlungsfrist um weitere 24 Stunden formuliert DD4BC kundenspezifisch die Folgen einer ausbleibenden Bitcoin-Zahlung. Dabei beachtet DD4BC scheinbar sogar die Arbeitszeiten der Unternehmen: In einem Fall verlängerte DD4BC die Zahlungsfrist wegen des Wochenendes um zwei Tage.

You are ignoring us.
You probably believe that after some time we will give up. But we never give up.
Maybe you believe that if you pay us once, we will be back? But we never attack the same target twice.
Please note that there are 2 options:
- You pay us, you never hear from us again.
- You don't pay, your services go offline for a long time. Until you pay more.
Is it worth it?

We will give you more time and since it's weekend we will wait until the end of Monday - enough time for you to decide. Until the end of Monday, if not paid, attack will start. Understand that this is your last chance.

Bild6: In einer weiteren E-Mail räumt DD4BC dem Opfer zusätzliche Zeit zum Überweisen der Bitcoins ein.

3.2 Geldforderungen per Bitcoin

DD4BC nutzt Bitcoin-Transaktionen zum Verschleiern der Spuren. Jeder Erpresser-E-Mail ist eine individuelle Bitcoin-Adresse zugeordnet. Das erleichtert DD4BC die Überwachung des Zahlungseingangs. Den Ermittlungsbehörden wiederum erschwert diese Taktik die Strafverfolgung. Sie können über die Menge der eingesetzten Bitcoin-Adressen nur spekulieren. Wie viele Erpressungsversuche erfolgreich waren und wie viele Bitcoins dabei insgesamt schon gezahlt wurden, bleibt ebenfalls im Dunkeln.

Auf bereits veröffentlichten Bitcoin-Adressen von DD4BC lassen sich auch Zahlungseingänge feststellen. Diese wurden innerhalb kürzester Zeit über weitere anonyme Bitcoin-Konten bis hin zu Exchange Services und Bitcoin Casinos zur Verschleierung weitertransferiert.

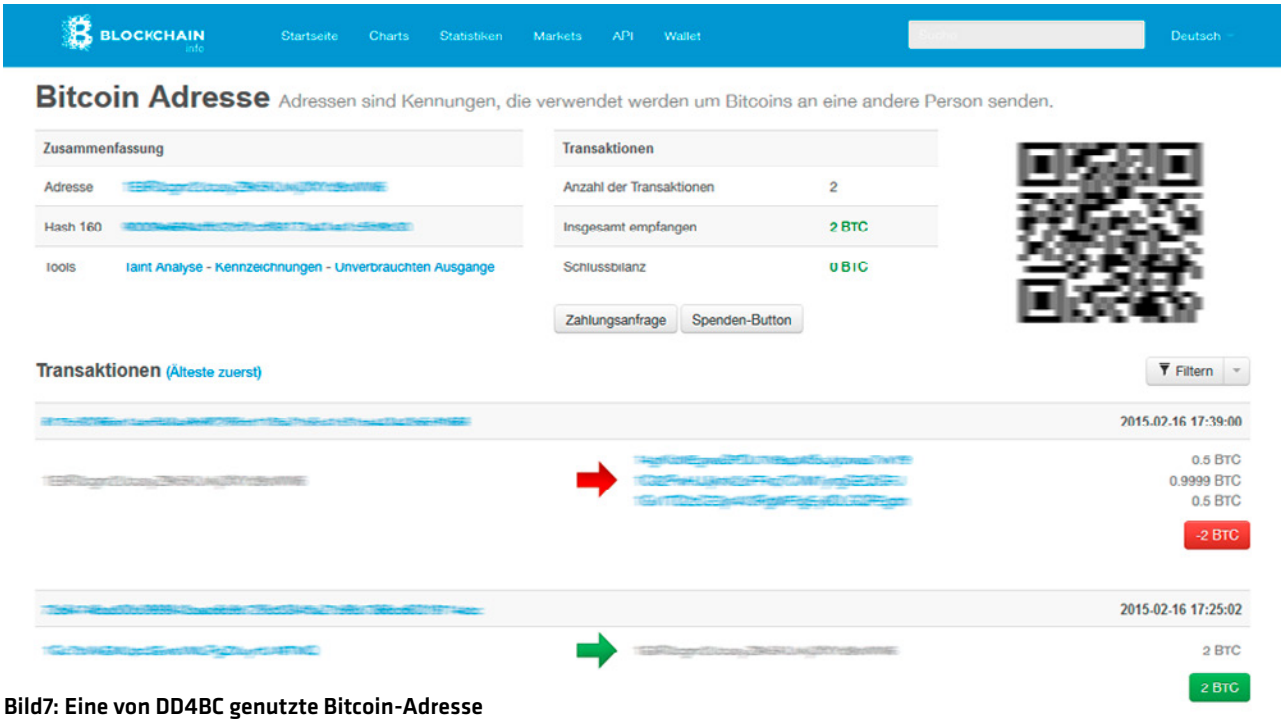

Bild7: Eine von DD4BC genutzte Bitcoin-Adresse

Die Schutzgeld-Summen von DD4BC sind im vergangenen halben Jahr stark angestiegen. Die Forderungen haben sich innerhalb weniger Monate um den Faktor 50 erhöht. Von Bitalo Bitcoin Exchange versuchte die Gruppe noch 1 Bitcoin zu erpressen. Derzeit verlangen die Erpresser bis zu 50 Bitcoins von deutschen Unternehmen. Link11 vermutet, dass aufgrund der bisherigen, für DD4BC positiven Entwicklung, die Schutzgeldforderungen zukünftig weiter steigen werden.

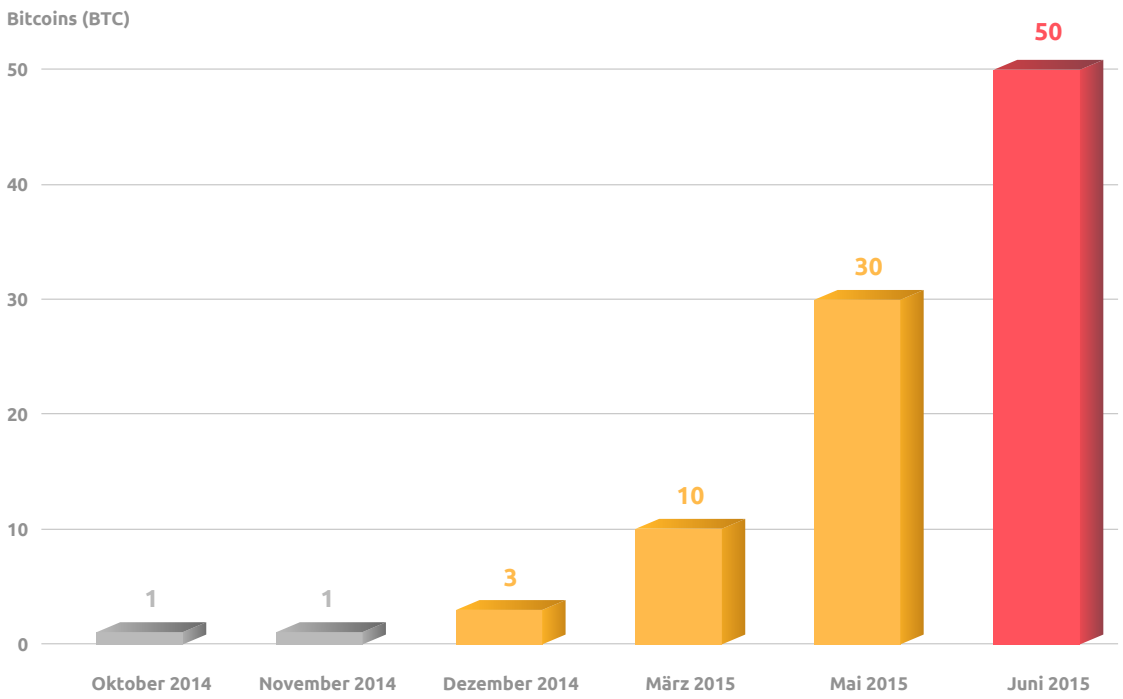

Bild8: Entwicklung der Schutzgeld-Forderungen

4. Analyse der DDoS-Attacken

4.1. Dauer und Stärke der DDoS-Attacken

Die von DD4BC angekündigten DDoS-Attacken von 400 bis 500 Gbps wurden bisher nie erreicht. Link11 liegen auch keine Indizien dafür vor, dass DD4BC über solche Kapazitäten verfügt. Jedoch weisen einzelne vom LSOC abgewehrte Attacken eine Peak-Bandbreite von knapp 100 Gbps auf.

DD4BC setzt für die Angriffe verschiedene Stärken und Taktiken ein. In den vom LSOC abgewehrten Fällen verwendet DD4BC großvolumige Reflection Amplification-Attacken. DNS Amplification-, NTP Amplification- sowie die seit diesem Jahr stark verbreiteten SSDP Amplification-Attacken kommen in verschiedenen Bandbreitenstärken und Längen zum Einsatz. In einigen Fällen wechseln die Angreifer dann aber abrupt zu TCP-SYN Flood-Attacken.

Um ihre Angriffsbandbreite zu erhöhen und die DDoS-Abwehr zu erschweren, werden die Attacken simultan als kombinierte Reflection-Attacken ausgeführt und mehrere Systeme des Opfers gleichzeitig angegriffen. Die daraus resultierenden Bandbreiten liegen im Bereich von 30 bis 50 Gbps und 80 bis 100 Gbps. Aufgrund der gewählten Uhrzeiten und der unterschiedlichen Verteilung der Angriffsbandbreite könnte die reduzierte Bandbreite ein Indiz für simultane Angriffe auf mehrere Opfer sein.

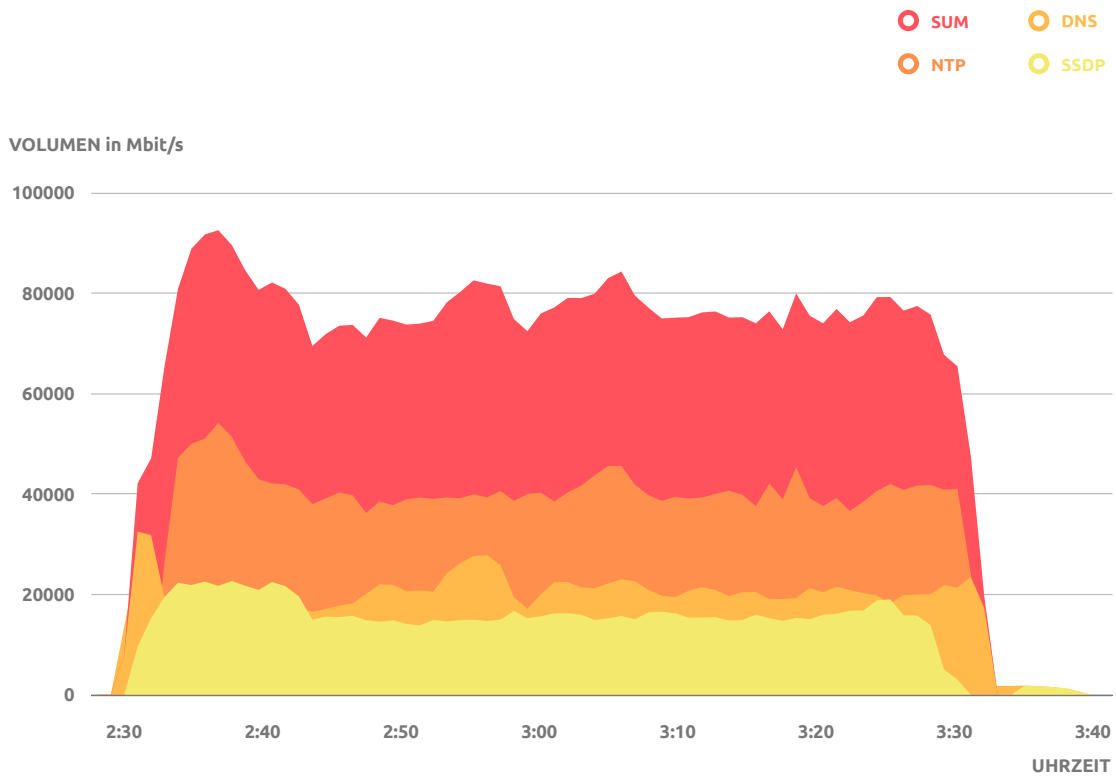

Bild9: Verlauf einer von DD4BC durchgeführten DDoS-Amplification-Attacke, die vom LSOC abgewehrt wurde

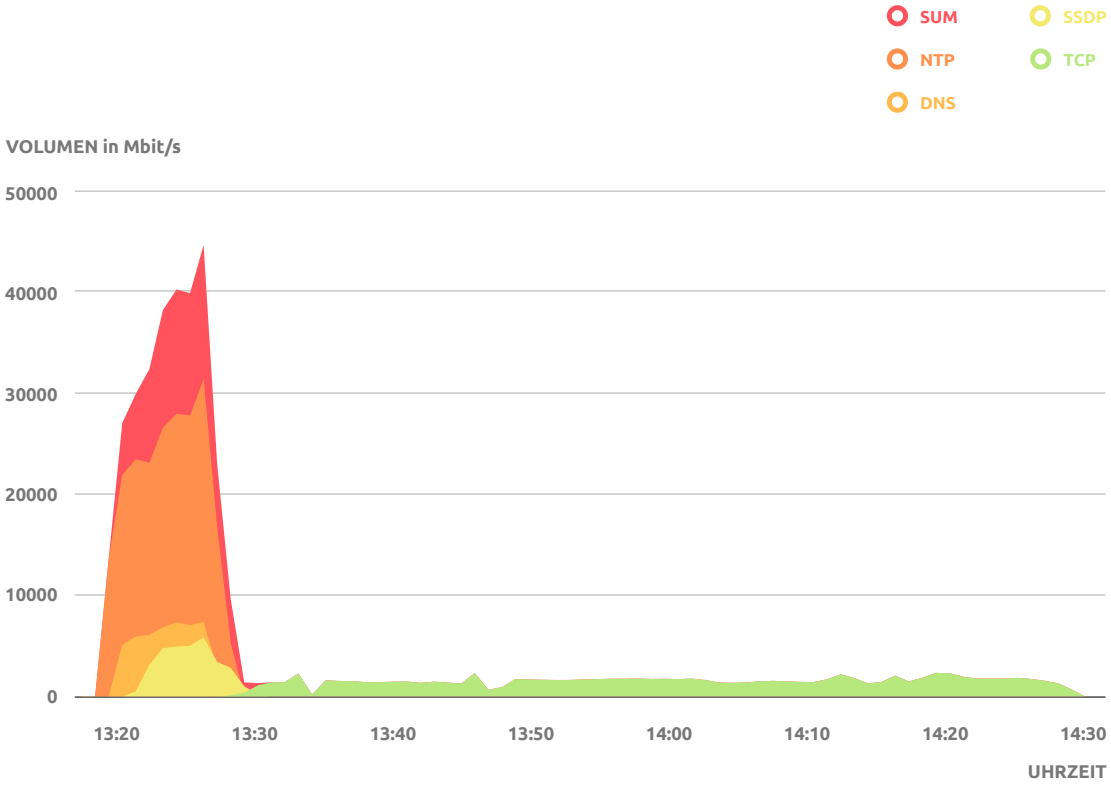

Bild10: Verlauf einer DD4BC-DDoS-Attacke mit TCP-SYN Flood

Den höchsten Anteil bei den Reflection-Attacken haben SSDP-Attacken mit knapp 62 Prozent. DNS- und NTP-Attacken kommen auf ca. 21 und 14 Prozent. Die von DD4BC ausgeführte SYN-Flood-Attacke erreicht im Peak knapp 1 Gbps.

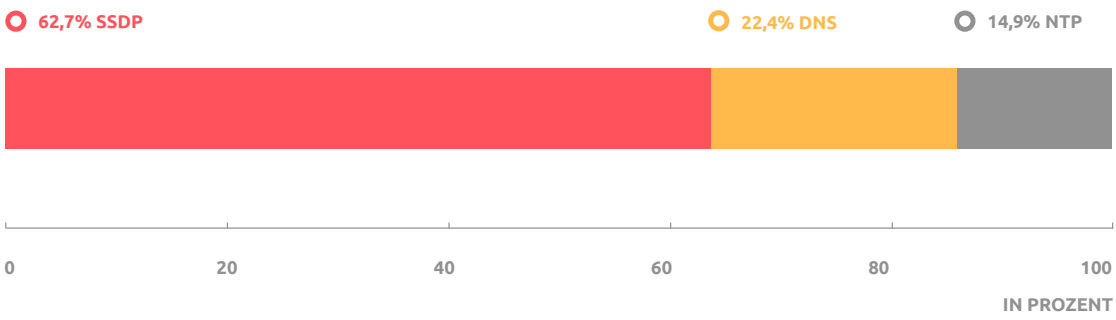

Bild11: Verteilung der Reflection-Attacken-Methoden

4.2 DDoS-Quellen

Die DDoS-Quellen der Attacken sind weltweit verteilt. Der Großteil des DDoS-Traffics (53 Prozent) stammt aus den USA und China. DDoS-Pakete lassen sich auch in andere typische Quellländer wie Russland und Brasilien zurückverfolgen.

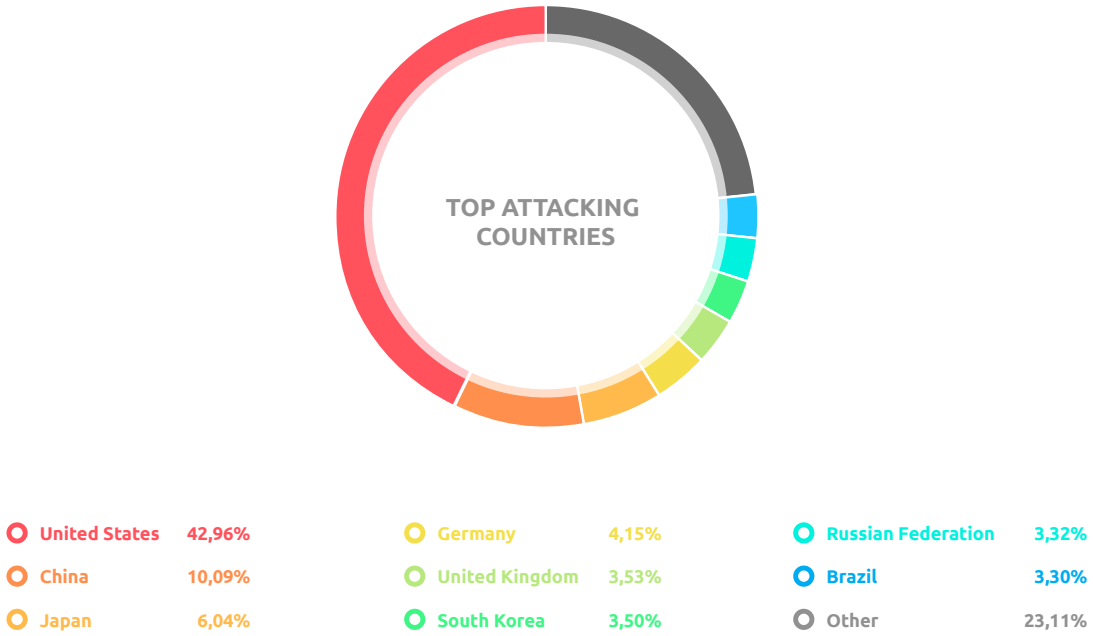

Bild12: Verteilung der DDoS-Quellen von DD4BC

4.5. Attacken-Know-how

Die Angriffswerkzeuge von DD4BC sind überschaubar und nach Faktenlage für Deutschland auf Reflection-Attacken und SYN-Floods beschränkt. Die Angreifer nutzen - im Unterschied zu bekannten Attacken in anderen Ländern - keine Applikations-Attacken.

In einer der analysierten SYN-Floods stellte das LSOC-Team eine Schwäche fest: Die Länge der TCP-Pakete war auffallend klein. TCP-SYN-Pakete sind gewöhnlich 50bis 64 Bytes groß und enthalten TCP Options. Die Pakete von DD4BC beschränkten sich hingegen durchgehend auf die Minimalgröße von 40 Bytes und wiesen keine TCP Options auf. Dies machte eine Filterung der TCP-SYN Flood-Attacke sehr einfach. Unklar ist daher, wie viel eigenes Know-how in den DDoS-Tools von DD4BC steckt. Einiges spricht dafür, dass die Gruppierung eigene Skripte und IP-Listen entwickelt hat. Es finden sich aber auch Anzeichen dafür, dass sie Dienstleistungen von Untergrund-Bootern und IP-Stressern anmietet.

5. Zusammenfassung

DD4BC ist eine der aktivsten cyberkriminellen Gruppierungen, die mit DDoS-Attacken Bitcoins von Unternehmen erpressen. Ihr Vorgehen dabei ist geplant und folgt strukturierten und bewährten Prozessen aus dem Bereich der DDoS-Erpressung. Im Gegensatz zu vielen vorherigen DDoS-Erpressungen erfolgt bei DD4BC fast immer konsequent die angekündigte DDoS-Attacke. Bleibt eine DDoS-Attacke jedoch wegen der Abwehr durch eine professionelle Schutzlösung erfolglos und verspricht keine Einnahmen, geben die Angreifer ihr Ziel umgehend auf und konzentrieren sich auf das nächste Opfer.

Das Geschäftsmodell der DDoS-Erpressung scheint für DD4BC lukrativ zu sein. Die Lösegeldforderungen sind innerhalb weniger Monate gestiegen. Das legt die Vermutung nahe, dass genügend Opfer den Forderungen nachgegeben und gezahlt haben. Die zügige Erschließung neuer Märkte und weiterer Branchen lässt keine Zweifel daran, dass DD4BC auch weiterhin aktiv bleiben wird. Was mit Attacken gegen Bitcoin Exchanges und Gaming-Plattformen begann, welche oft keine Strafverfolgung bemühen, hat inzwischen auch börsennotierte Unternehmen erreicht. Nach Erpresserwellen in den USA, Australien und Neuseeland sowie in Großbritannien und der Schweiz steht aktuell Deutschland im Fokus von DD4BC.

Jedes Unternehmen, das eine Erpresser-E-Mail von DD4BC erhält, sollte diese unbedingt ernst nehmen. Schon die Warn-Attacke kann ein Unternehmensnetzwerk empfindlich treffen. Die Gefahr durch DD4BC ist daher hoch. Den attackierten Unternehmen bleibt daher nur die Option, innerhalb der 24-Stunden-Zahlungsfrist einen geeigneten DDoS-Schutz aufzusetzen.

Über Link11

Die Link11 GmbH mit Sitz in Frankfurt am Main ist ein deutsches IT Unternehmen mit Kernkompetenzen in den Bereichen DDoS-Schutz und Serverhosting. Mit der DDoS-Protection-Cloud hat die Link11 im Jahr 2011 ein neues und innovatives Produkt erfolgreich am Markt etabliert. Dieser Link11 DDoS-Schutz ist bereits zum Patent angemeldet und ermöglicht, jede Webseite, oder ganze Serverinfrastrukturen vor DDoS-Angriffen zu schützen. Mit seinen Netzwerkstandorten und eigenen Glasfaserstrecken zwischen Frankfurt, Amsterdam und London gehört die Link11 heute zu den großen DDoS-Filter-Anbietern weltweit. Der kontinuierliche Ausbau des Netzes umfasst aktuell weitere Standorte in Asien und den USA. Zu seinen Kunden zählt Link11 führende Unternehmen aus den Bereichen E-Commerce, Finanzen & Versicherung, Medien und Produktion.