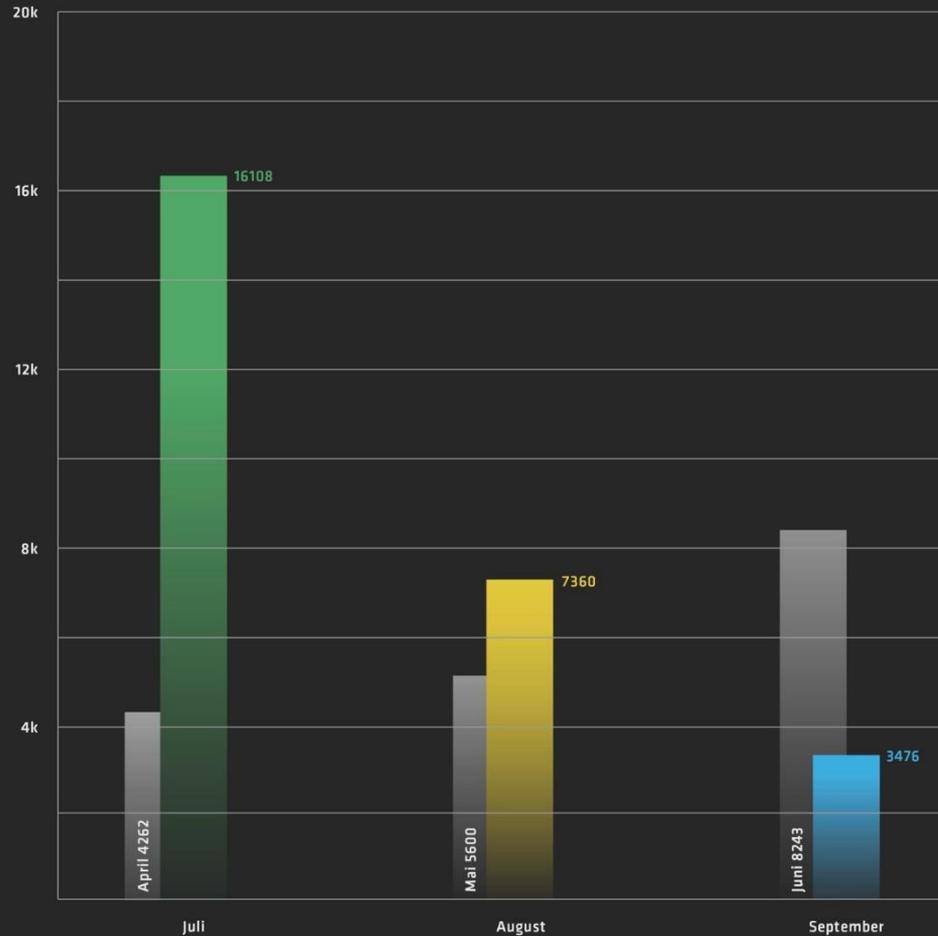


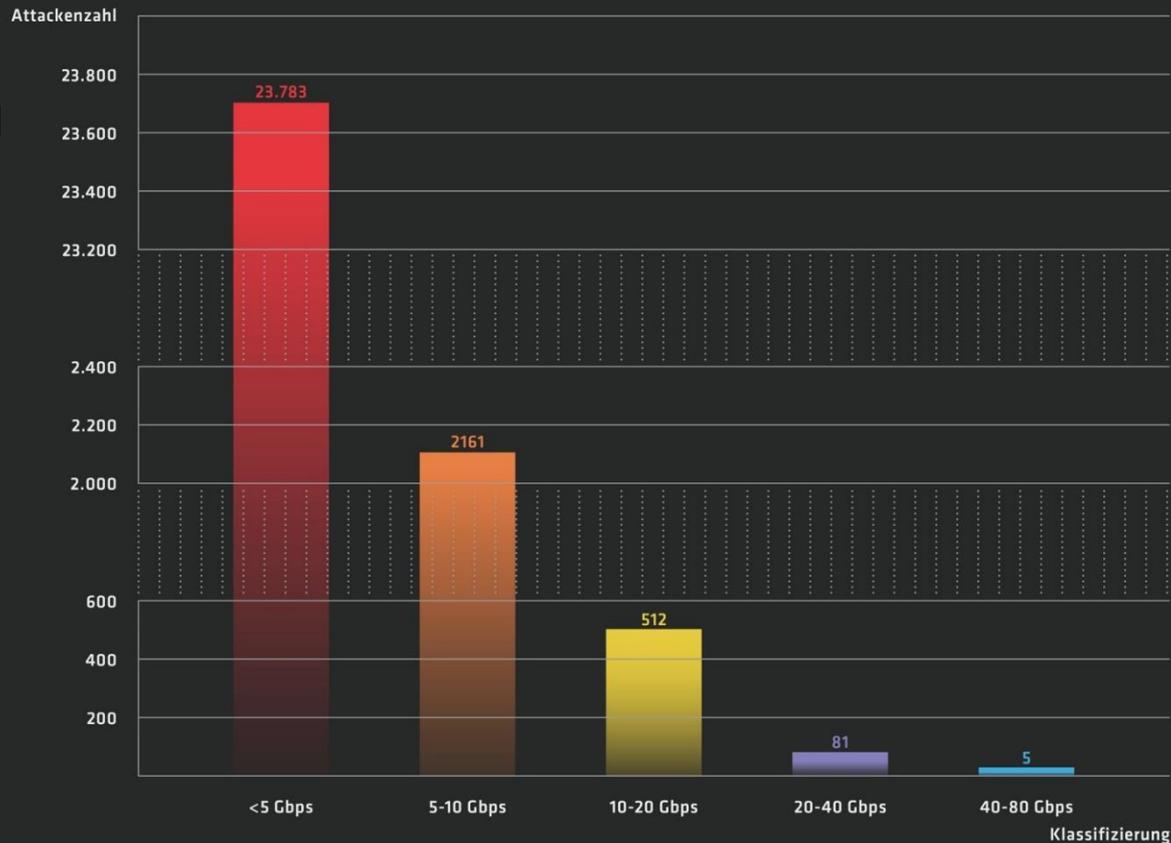
DDoS DDoS DDoS

DDoS-Gefahr in Deutschland

Verteilung der DDoS-Attacken in Q3 2017



Verteilung der Angriffsbandbreiten In Q3 2017



Die häufigsten Angriffsvektoren

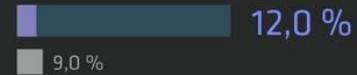
UDP Floods



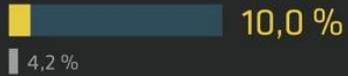
TCP SYN Floods



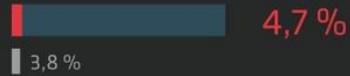
UDP Fragments



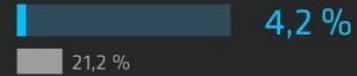
Gaming Server Reflection



DNS Reflection



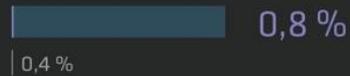
SSDP Reflection



NTP Reflection



ICMP Floods



Chargen



DDoS-Erpressungen seit Januar 2017

Unter dem Namen ‚Stealth Ravens‘
erpressen DDoS-Angreifer Online-
Shops in Deutschland und setzen dafür
auf ein Mirai-Botnetz.

01/17

----- Original Message -----

Subject: DDoS Attack (26-Jan-2017)

From: Stealth Ravens <stealth.ravens2@...>

Hi!

If you dont pay 5 bitcoin until 1. february you will be hardly ddosed! Our attacks are super powerfull (Mirai botnet). And if you don't pay until 1. february ddos attack will start and price to stop will double!

We are not kidding and we will do small demo now on just one of your servers xxx.xx.xxx.xxx to show we are serious. It will not be strong, we dont want damage now we hope you cooperate, just small flood to show we are not hoax.

DDoS-Erpressungen seit Januar 2017

Unter dem Namen „Stealth Ravens“
erpressen DDoS-Angreifer Online-
Shops in Deutschland und setzen dafür
auf ein Mirai-Botnetz.

01/17

04/17

XMR-Squad verlangen für DDoS
Protection Test je Unternehmen 250€.

DDoS-Erpressungen durch XMR_Squad



XMR @xmr_squad

We have successfully ddos dhl.de

#XMR #DHL #DDoS #Internet #notpayed #Downtime @DHLPaket



XMR @xmr_squad

wir "prüfen" ihre Protection :=) & dafür verlangen wir eben 250€ Win-Win.



XMR @xmr_squad

Vielleicht könnten Sie auch erwähnen, dass DHL keine 250€ bezahlen wollte und sie die Kunden so vernachlässigt haben.



DDoS-Erpressungen seit Januar 2017

Unter dem Namen „Stealth Ravens“ erpressen DDoS-Angreifer Online-Shops in Deutschland und setzen dafür auf ein Mirai-Botnetz.

01/17

XMR-Squad verlangen für DDoS Protection Test je Unternehmen 250€.

04/17

Die DDoS-Erpresser von XMR-Squad rufen Copycats auf den Plan.

05/17

Mit technischer Expertise und unübersehbaren Folgen attackiert ZZb00t vornehmlich deutsche Unternehmen

05/17

DDoS-Erpressungen durch ZZb00t



ZZb00t

@zzb00t

Mentally disturbed gray hat | Former IT-Security Consultant | [#freetheweb](#) | [#vulnerabilities](#) hunter | [#DDoS](#) | [#zzb00t](#) | LOVED & HATED.

Islamic Republic of Iran

tinyurl.com/mzpxrap

Joined April 2017

TWEETS
186

FOLLOWING
11

FOLLOWERS
600

LIKES
15

MOMENTS
2

Tweets

Tweets & replies

Media

Pinned Tweet



ZZb00t @zzb00t · 16h

New customer: [m-net.de](#) | [#stresstest](#) on 16/05/2017 12:00 CEST



ZZb00t @zzb00t · 4h

[#cooldown](#) [m-net.de](#) , have to go



ZZb00t @zzb00t · 17h

DDoS-Erpressungen seit Januar 2017

Meridian Collective, Team Xball, Collective Amadeus: drei neue DDoS-Erpresser sind parallel in der DACH-Region aktiv und bluffen.

06/17

Unter dem Namen Phantom Squad werden 1.000-fach DDoS-Erpresser-Mails verschickt.

09/17

XMR-Squad ist wieder auf Twitter aktiv und berichtet von Attacken auf Unternehmen in Deutschland.

08/17

Aktuell berichten Unternehmen von DDoS-Erpressungen mit dem Absender Fancy Bear.

11/17

Weitere Zahlen und Fakten zu DDoS in Deutschland



Link11 DDoS-Report für die DACH-Region
<https://www.link11.com/ddos-report/>



Warnmeldungen zu akuten DDoS-Vorfällen
<https://www.ddos-info.de>