TeleTrusT
Pioneers in IT security.

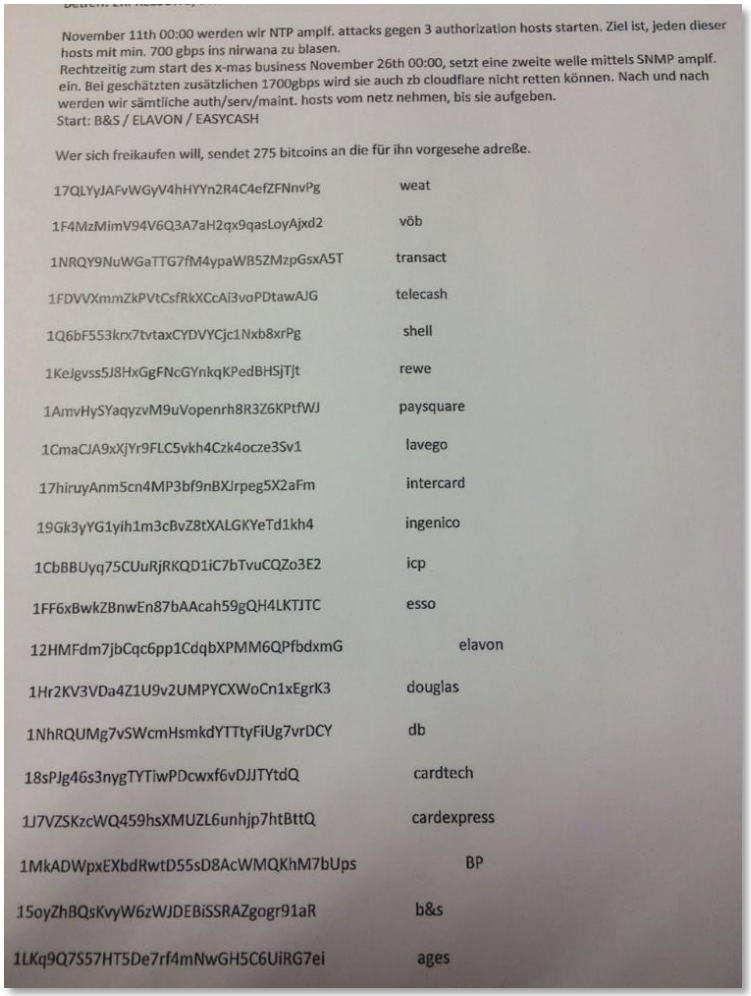
TeleTrusT-interner Workshop

Bochum 18./19.06.2015

DDoS-Erpressung

Raymond Hartenstein, Link11 GmbH

Erpresser-Emails



November 11th 00:00 werden wir NTP amplf. attacks gegen 3 authorization hosts starten. Ziel ist, jeden dieser hosts mit min. 700 gbps ins nirwana zu blasen.
Rechtzeitig zum start des x-mas business November 26th 00:00, setzt eine zweite welle mittels SNMP amplf. ein. Bei geschätzten zusätzlichen 1700gbps wird sie auch zb cloudflare nicht retten können. Nach und nach werden wir sämtliche auth/serv/maint. hosts vom netz nehmen, bis sie aufgeben.
Start: B&S / ELAVON / EASYCASH

Wer sich freikaufen will, sendet 275 bitcoins an die für ihn vorgesehe adreße.

17QLYyJAFvWGyV4hHYYn2R4C4efZFNnvPg	weat
1F4MzMimV94V6Q3A7aH2qx9qasLoyAjxd2	vöb
1NRQY9NuWGaTTG7fM4ypaWB5ZMzpGsxA5T	transact
1FDVVXmmZkPVtCsfRkXCcAi3voPDtawAJG	telecash
1Q6bF553krx7tvtaxCYDVYCjc1Nxb8xrPg	shell
1KeJgvss5J8HxGgFNcGYnkqKPedBHSjTjt	rewe
1AmvHySYaqyzvM9uVopenrh8R3Z6KPtfWJ	paysquare
1CmaCJA9xXjYr9FLC5vkh4Czk4ocze3Sv1	lavego
17hiruyAnm5cn4MP3bf9nBXJrpeg5X2aFm	intercard
19Gk3yYG1yih1m3cBvZ8tXALGKYeTd1kh4	ingenico
1CbBBUyq75CUuRjRKQD1iC7bTvuCQZo3E2	icp
1FF6xBwkZBnwEn87bAAcah59gQH4LKTJTC	esso
12HMFdm7jbCqc6pp1CdqbXPMM6QPfbdxmG	elavon
1Hr2KV3VDa4Z1U9v2UMPYCXWoCn1xEgrK3	douglas
1NhRQUMg7vSWcmHsmkdYTTtyFiUg7vrDCY	db
18sPJg46s3nygTYTiwPDcwxf6vDJJTYtdQ	cardtech
1J7VZSKzcWQ459hsXMUZL6unhjp7htBttQ	cardexpress
1MkADWpxEXbdRwtD55sD8AcWMQKhM7bUps	BP
15oyZhBQsKvyW6zWJDEBiSSRAZgogr91aR	b&s
1LKq9Q7S57HT5De7rf4mNwGH5C6UiRG7ei	ages

Von: Raul Garcia [mailto:graul494@yahoo.com]
Gesendet: Mittwoch, 6. Mai 2015 10:47
An: vogelzubehoer.com ; fidi-didi.de ; feuerloescher-guenstig.de ; finlayswhiskyshop.de ; firestorm-games.de ; fliegfix.com ; flashlightshop.de ; flaggenmeer.de ; fitnessworld24.net ; foedoe-shop-ist-freu.de ; fotobantle.de ; fortknox.de ; forhouse.de ; freeride-mountain.com ; fotozack.de ; fotoversand24.de ; fun-sport-vision.com ; fussball2go.de ; fussballcompany.de ; fussballoutlet24.de ; gartenallerlei.de ; garten-und-freizeit.de ; gardelino.de ; gamingoase.de ; gabler24.com ; gaastraproshop.com ; geschenkeschmidt.com ; geraete-discount.de ; gelkamine.de ; gbk-shop.de ; gasherd.de ; gartenwelt-schneider.de ; global-kitchen.de ; gieger-versand.de ; getreidemuehlenshop.de ; gesundwerk.de ; gesundplus24.de ; gokart-profi.de ; grillstudio.de ; greenstars.de ; goodtires.de ; golfmeile.de ; gokarthof.de ; gw-werkzeuge.de ; gummistiefelprofi.de ; guenstixx.de ; guenstiger-bekommen.de ; guenstige-malerwerkzeuge.de
Betreff: DDOS Erpresserbrief

Sehr geehrte Damen und Herren,

hiermit fordere ich die Zahlung von 5 Bitcoins (ca. 1300€) an folgende Bitcoin-Adresse: 1NyrwLZm1L7KAAYwwaYmb764pqAXoFLSJL
Sollte die Zahlung nicht bis zum 13.05.2015 um 22.00 Uhr erfolgt sein, startet automatisch ein DDOS-Angriff auf Ihren Onlineshop, was zur Folge hat, dass dieser nichtmehr erreichbar sein wird. Um den Angriff zu beenden wäre dann eine Zahlung von 50 Bitcoins erforderlich.

Die Höhe der Forderung und die Zahlingsfrist sind NICHT VERHANDELBAR!

Bitcoins können Sie unter Anderem auf diesen Internetseiten kaufen: https://btc-e.com/
https://www.bitcoin.de/
https://www.kraken.com/

WICHTIG: Die erfassung Ihrer Zahlung erfolgt automatisch. Um eine erfolgreiche erfassung zu garantieren ist es erforderlich, dass Sie, sobald Sie die Zahlung getätigt haben, eine e-mail welche ausschließlich ihre Bitcoinadresse enthält an btcadresses@hmamail.com

Mit freundlichen Grüßen

Unless you pay 10 Bitcoin to [redacted] within 24 hours from now, your site is going under heavy DDoS attack.

Pay, and you will never hear from us again.

Usually, we attack first, then ask BTC to stop, but since your site is too big, we are giving you time to act first, because we are well aware that even 1 hour offline would cause much larger damage then 10 BTC.

24 hours, so you have enough time to read email, buy Bitcoin and act.