To: (10)(2e) [(10)(2e)@rivm.nl]
From: (10)(2e)
Sent: Wed 5/20/2020 1:19:03 PM
Subject: FW: Antw: DDOS aanval op RIVM.NL
Received: Wed 5/20/2020 1:19:04 PM

Zie het antwoord van (10)(2e) hieronder.

Van: (10)(2e) <(10)(2e)@rivm.nl>
Verzonden: woensdag 20 mei 2020 13:37
Aan: (10)(2e) <(10)(2e)@rivm.nl>
Onderwerp: Antw: DDOS aanval op RIVM.NL

Hi,

Ik blijf het netwerk monitoren zoals ik al deed. Ik besteed veel tijd aan het mailfilter omdat ik vermoed dat men in eerste instantie een lid van het OMT (vreemde mogendheid of journalist) of een beheerder (vreemde mogendheid of op geld belaste ransomware verspreider) zal verleiden om op een link te klikken waarmee malware wordt geïnstalleerd.

Als een dergelijke ddos aanval langer duurt is de kans aanwezig dat er een andere bedoeling dan RIVM pesten achter zit. Het tijdstip (vlak voor de bekendmaking van nieuwe Covid cijfers) doen vermoeden dat het dit keer "pesten" was.

De enige twee relaties ik nu zie mogelijk zijn :

(10)(2g)

Groeten (10)(2e)

(10)(2g)

Van: (10)(2e) <(10)(2e)@rivm.nl>
Datum: 20 mei 2020 om 13:00:37 CEST
Aan: (10)(2e) <(10)(2e)@rivm.nl>
Onderwerp: FW: DDOS aanval op RIVM.NL

Hi (10)(2e)

Zie de vraag van (10)(2e) hieronder. En daarnaast: Hebben we (RIVM) er last van gehad? En zo ja, op welke manier.

Groet
(10)(2e)

Van: (10)(2e) <(10)(2e)@rivm.nl>
Verzonden: woensdag 20 mei 2020 12:55
Aan: (10)(2e) <(10)(2e)@rivm.nl>
Onderwerp: RE: DDOS aanval op RIVM.NL

(10)(2e)
Dit klinkt niet fijn en ook al is het ter info hoop ik wel dat dit opgepakt wordt. Overigens heb ik de ervaring dat een dergelijke aanval soms gebruikt wordt om een andere zwaardere inbruik te maskeren. Is de algemene alertheid ook verhoogd??

Mvg,
(10)(2e)
(10)(2e)

Rijksinstituut voor Volksgezondheid en Milieu
Antonie van Leeuwenhoeklaan 9 | Postbus 1 | 3720 BA Bilthoven

T +31 (10)(2e) / 06 (10)(2e)
M (10)(2e) @rivm.nl
W http://www.rivm.nl
Secr: (10)(2e) @rivm.nl 030 (10)(2e)

RIVM *De zorg voor morgen* begint vandaag!

Van: (10)(2e) < (10)(2e) @rivm.nl>
Verzonden: woensdag 20 mei 2020 08:53
Aan: (10)(2e) < (10)(2e) @rivm.nl>
Onderwerp: FW: DDOS aanval op RIVM.NL

Te info

Van: (10)(2e) < (10)(2e) @rivm.nl>
Verzonden: woensdag 20 mei 2020 08:02
Aan: (10)(2e) < (10)(2e) @rivm.nl>; (10)(2e) < (10)(2e) @rivm.nl>
CC: (10)(2e) < (10)(2e) @rivm.nl> (10)(2e) (10)(2e) @rivm.nl>; (10)(2e) < (10)(2e) @rivm.nl>; (10)(2e) < (10)(2e) @rivm.nl>
Onderwerp: DDOS aanval op RIVM.NL

All,

Ter info:

Gisteren, 19-05-2020 is RIVM.NL even naar 1300 uur het slachtoffer geweest van de DDOS aanval. Kenmerk van deze aanval is dat die niet te voorkomen is, de "aanstichter" niet te achterhalen is en dat die door het gebruik van veel resources (bijvoorbeeld veel reacties uitlokken van de webserver waardoor deze geen nieuwe verbindingen meer accepteert) of door het gebruik van veel bandbreedte van de verbindingen de bereikbaarheid van de website verstoort.

Mogelijk mitigerende preventieve maatregelen zijn:

1. Beperkt: een filter door Surfnet laten instellen zodat alleen verkeer naar port 443 en 80 wordt doorgelaten richting de websites.
2. Full blown: een proxydienst gebruiken zodat de originele website niet meer zichtbaar is. Cloudflare en Akamai bieden deze diensten aan. Zie hiervoor ook het op 15-5-2020 gestuurde aanbod van Akamai.

Ik kan hier helaas verder niets aan doen, behalve signaleren dat -conform verwachting- RIVM.NL wordt aangevallen en jullie in overweging te geven om preventieve maatregelen te nemen.

(Note: CC aan (10)(2e) omdat die graag op de hoogte wil blijven van acties met het doel de bedrijfsvoering van het RIVM te verstoren, informatie te stelen etc. etc.)

Met vriendelijke groeten,
(10)(2e), RIVM
Gebouw (10)(2e) Kamer (10)(2e)
Mobiel: 06 (10)(2e)