

[Security](#) > [News](#) > [7-Tage-News](#) > [2017](#) > [KW 30](#) > Cyber-Angriffe NotPetya: Unternehmen haben immer noch viel Arbeit mit dem Fallout des Angriffs

Cyber-Angriffe NotPetya: Unternehmen haben immer noch viel Arbeit mit dem Fallout des Angriffs

25.07.2017 15:50 Uhr – Fabian A. Scherschel

 vorlesen


Die [Emma Mærsk](#), eins der größten Containerschiffe der Welt, beim Einlaufen in den Hamburger Hafen. (Bild: Hummelhummel, CC BY-SA 3.0)

Mit Maersk ist die größte Containerschifflinie der Welt betroffen. Auch TNT Express und Reckitt Benckiser, Hersteller von Sagrotan und Durex, haben immer noch nicht alle Computer bereinigt. Bei TNT verzögert sich die Paketauslieferung.

Unternehmen wie das dänische Industrie-Konglomerat Maersk und der britische Hersteller von Haushaltprodukten Reckitt Benckiser leiden nach wie vor unter den Folgen des Angriffes durch den [NotPetya-Trojaner](#). Maersk betreibt mit der Maersk Line unter anderem die größte Übersee-Transportschiffahrtsgesellschaft der Welt und mit Maersk Oil und Maersk Drilling eine Reihe von Nordsee-Bohrinseln und Bergbau-Unternehmungen auf der ganzen Welt. Reckitt Benckiser vertreibt in Deutschland unter anderem Durex, Sagrotan, Calgonit und Produkte unter der Marke Scholl. Auch die niederländische FedEx-Tochter TNT Express, ein weltweit operierendes Transportunternehmen, ist nach wie vor betroffen.

Computer auf Bohrinseln außer Betrieb, Produktionsstätten stehen still

Nach Informationen von heise online legte der Trojaner bei Maersk Systeme auf Bohrinseln lahm und brachte das Beladen und Löschen von Containerschiffen zum Stocken. Auch die Herstellung von Nivea bei Beiersdorf in Hamburg-Billbrook war demnach betroffen. Maersk ist nach eigenen Angaben [nach wie vor mit der Beseitigung der Folgen des Angriffes befasst](#). Reckitt Benckiser [gab gegenüber ZDNet bekannt](#), man rechne erst gegen Ende August mit einer vollständigen Rückkehr zur Normalität in den eigenen Betriebsstätten. TNT meldet nach wie vor eine Störung der IT-Systeme und weist darauf hin, dass deswegen das Paket-Tracking verzögerte Informationen anzeige. Auch Auslieferungen und das Abholen von Lieferungen verzögern sich seit dem Trojaner-Angriff immer mal wieder.

Reckitt Benckiser geht für das laufende Jahr von einem [Umsatzrückgang von zwei Prozent](#) statt

Siehe dazu:

Verschlüsselung knackbar: Hoffnung für (manche) NotPetya-Opfer

Neue Einblicke in die perfide Verbreitungsmasche

[Angebliche Angreifer wollen 250.000 Euro für Datenrettung](#)

[Ukrainischer Geheimdienst vermutet Russland hinter Petya/NotPetya-Angriffe](#)

[Petya/NotPetya: Kein Erpressungstrojaner, sondern ein "Wiper"](#)

[Alles, was wir bisher über den Petya/NotPetya-Ausbruch wissen](#)

[Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm](#)

Dienste

Security Consulter Emailcheck
 Netzwerkcheck Browsercheck
 Anti-Virus Krypto-Kampagne

heise devSec

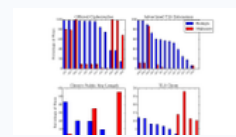
Im Oktober: Die Konferenz für sichere Software- und Webentwicklung



Artikel

[Cisco analysiert verschlüsselten Traffic, um Malware zu erkennen](#)

Mit Hilfe von Machine Learning gelang es einer Forschergruppe, den verschlüsselten Netzwerk-Verkehr von Malware von regulärem zu unterscheiden – und das, ganz ohne ihn zu entschlüsseln.



[Windows-Diagnose: Programme und Prozesse meistern](#)

Wer mehr über das wissen will, was unter der Haube von Windows so vorgeht, kommt weder am Task-Manager noch am Sysinternals-Tool ProcMon vorbei.



[Analysiert: Alte Masche, neue Verpackung – Infektion durch PDFs](#)

Manipulierte Word-Dokumente sind bei Kriminellen beliebt, um Computer mit Malware zu infizieren. Dass auch PDF-Dateien ausführbaren Code enthalten können, ist hingegen ein wenig in Vergessenheit geraten. Eine unlängst grassierende Spam-Kampagne ist ein guter Grund, sich diese Gefahr anhand eines frischen Samples in Erinnerung zu rufen.



dem vorausgesagten Gewinn von drei Prozent aus – als Grund wurde eine nicht weiter spezifizierte "Cyberattacke" genannt. Allein bei dieser Firma geht man daher von [einem Verlust von über 111 Millionen Euro durch NotPetya](#) aus. Das Unternehmen musste wohl in einigen europäischen Standorten Produktion und zum Teil den Versand für bis zu zwei Wochen einstellen. Auch TNT und Maersk erwarten mehreren Quellen zu Folge erhebliche finanzielle Belastungen.

Erheblicher Schaden für die Weltwirtschaft

Das gesamte Ausmaß des Angriffes auf die Weltwirtschaft lässt sich nach wie vor nicht abschätzen, aber angesichts der bisher genannten Zahlen ist mindestens von hunderten Millionen, wenn nicht gar über einer Milliarde Euro auszugehen. Neben den genannten

Unternehmen waren ebenfalls Niederlassungen des deutschen Pharma-Großkonzerns Merck und die britische Werbeagentur WPP von der Malware betroffen. Unzählige kleinere Opfer finden sich in ganz Europa und den USA. In der Ukraine, dem Ausgangspunkt des Trojaners, waren neben der Zentralbank auch Einrichtungen zur Messung der Strahlung im havarierten AKW Tschernobyl betroffen.

Reckitt Benckiser und Maersk sprechen davon, dass Anti-Viren-Software, die in den Firmen im Einsatz war, die Infektion nicht habe aufhalten können. Maersk zufolge haben auch die eingespielten Windows-Updates den Ausbruch des Trojaners nicht verhindern können. Mittlerweile gehen viele Sicherheitsforscher davon aus, dass es sich bei NotPetya nicht um Ransomware, sondern einen [Wiper-Trojaner](#) gehandelt hat, der explizit viel Schaden anrichten sollte. Der Geheimdienst der Ukraine spricht von einem [Cyberangriff aus Russland](#). ([fab](#))

Kommentare lesen (149 Beiträge)

Forum zum Thema: **Politik & Gesellschaft**



<https://heise.de/-3782794>

Drucken

Mehr zum Thema [Ransomware](#) [Malware](#)



Bild: Fabian A. Scherschel, heise online

Neueste Forenbeiträge

Re: ISO 27001?

Hausbauer schrieb am 25.07.2017 20:16: Das kommt dabei raus, wenn man ein Zertifikat mit einem funktionierendem ISMS verwechselt... De Facto...

Forum: [Cyber-Angriffe NotPetya: Unternehmen h...](#)



von ubuntuX; 26.07.2017 13:21

Re: Nein! Bitte kein Linux!

Heilige drei Könige schrieb am 26.07.2017 08:55: In meinem Haushalt hat Linux eine Verbreitung von 75%. Mein Vater mag sich einfach nicht von...

Forum: [Cyber-Angriffe NotPetya: Unternehmen h...](#)



von cosinux; 26.07.2017 13:15

Re: Windows

Cyberneulandbingobuzzer schrieb am 25.07.2017 18:38: "Das Traumgeschehen handelt häufig von Dingen und Ereignissen, die theoretisch unmöglich..."

Forum: [Cyber-Angriffe NotPetya: Unternehmen h...](#)



von Apple_oder_nichts; 26.07.2017 13:08

Der Kommentar

1 2 3 4 5

Warum wir Forward Secrecy brauchen



Der SSL-GAU zeigt nachdrücklich, dass Forward Secrecy kein exotisches Feature für Paranoiker ist. Es ist vielmehr das einzige, was uns noch vor einer vollständigen Komplettüberwachung aller Kommunikation durch die Geheimdienste schützt.

News und Artikel
News
7-Tage-News
News-Archiv
Hintergrund-Artikel

Service
Newsletter
Tools
Foren
RSS
mobil

Dienste
Security Consulter
Netzwerkcheck
Anti-Virus
Emailcheck
Browsercheck
Krypto-Kampagne