



Technologie

20/10/2009

De dimensies van het open web



Loopbaan

20/10/2009

IT'ers en hun managers



De sysadmin

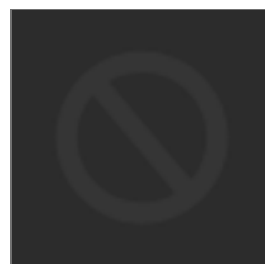
14/10/2009

Bastiaan Hungerink:
Eigenlijk twee
omgevingen tegelijk

[DATACENTER](#)
[CLIENT](#)
[NETWERK](#)
[BEVEILIGING](#)
[OPSLAG](#)
[OS](#)
[TOOLS](#)
[CLOUD COMPUTING](#)

U bent nu hier: » [Home](#) » [Technologie](#) » 'Dode hackkit is springlevend'

'Dode hackkit is springlevend'



Gepubliceerd: 26 september 2008 om 15:40 uur

Auteur: Michiel van Blommestein

Het beruchte hackerspakket NeoSploit lijkt weer te zijn opgedoken. Onderzoekers zijn op een relatief nieuwe versie gestuit van de toolkit voor zware cybercriminaliteit.

"NeoSploit is terug", beweert Ian Amit, directeur van de onderzoeksdienst van beveiligingsbedrijf [Aladdin](#). Het bericht dat afgelopen zomer door de makers de wereld in is geholpen was een afleidingsmanoeuvre, zo pleit de onderzoeker. "Als een dergelijk pakket zo veel aandacht krijgt van onderzoekers en autoriteiten, dan willen ze daarvan af", zegt Amit [tegenover Computerworld](#). "Door geruchten de wereld in te helpen dat ze ermee ophouden, duiken ze verder onder de radar."

Aladdin zegt deze week een nieuwe versie van de toolkit te hebben opgedoken op een Argentijnse [server](#). Het zou gaan om versie 3.1, met een build-datum van 9 augustus, ruim een maand na [het bericht](#) van beveiliging van RSA dat de groep ermee ophield. RSA had toen een bericht gevonden waarin de makers hun afscheid aankondigden.

De onderzoekers waren toen al sceptisch over het idee dat de criminelen hun operaties helemaal zouden staken. In dit nieuwe geval zou het gaan om ongeveer twintig 'klanten', die gezamenlijk duizenden succesvolle exploits per dag logden, aldus Amit. Dat zou via twee- a driehonderd besmette websites gaan. Amit zegt verder dat een recente golf van aanvallen op PDF-kwetsbaarheden een lijntje hebben met de terugkeer van NeoSploit.

Infectie

NeoSploit is een toolkit waarmee criminelen bezoekers van websites kunnen infecteren met malware. Programma's die met het pakket gebouwd zijn, moeten via een bestaand lek in een website worden gesmokkeld, waarna bezoekers van die website kunnen worden geïnfecteerd. Daarnaast biedt het allerlei tools waarmee statistieken worden bijgehouden en de malware kan worden beheerd, evenals [uitgebreide databasemogelijkheden](#) voor gestolen informatie.

Het pakket dook voor het eerst op in 2007 en wordt gezien als een voortzetting van [MPack](#). Voor het pakket moet grof geld worden neergelegd (tot in de duizenden dollars), waarna de klanten kunnen rekenen op ondersteuning en regelmatige updates om beveiligingsleveranciers voor te blijven. Een van de redenen dat NeoSploit 'de handdoek gooide' zou dan ook zijn dat het programma het slachtoffer werd van piraterij, ondanks dat het in principe alleen aan 'vertrouwde' klanten in de onderwereld wordt verstrekt.

Daar is nu wel paal en perk aan gesteld: de al draconische 'DRM' in de software is verder aangescherpt. Zo is bijvoorbeeld de login gekoppeld aan een ip-adres.

Tags: [aladdin](#) [hacken](#) [rsa](#) [tool](#) [neosploit](#)

[Categorie]: [Beveiliging](#)

IT ARCHITECT '09

Bent u de IT architect van 2009?
Meld u nu aan en maak kans op een Sony
Vaio VGN t.w.v. € 1149,-

prijzen ter beschikking
gesteld door

sponsored by

PEILING

Ga je binnen een jaar migreren naar Windows 7?

- Ja, we zijn al bezig met testen
- Ja, we gaan binnenkort testen
- Ja, maar we wachten nog even met testen
- Nee, we wachten met testen op SP1
- Nee, daar hebben we geen geld voor
- Nee, we draaien helemaal geen Windows

GERELATEERDE PERSBERICHTEN POWERED BY **itworld**

- Ministerie van Justitie kiest ook voor...
- Lean IT-denkwijze populair onder...
- MKB netwerk vaak onvoldoende beveiligd...
- SafeNet introduceert eSafe SmartSuite...
- TelecityGroup verlicht security-eisen...

NU OP NGN.NL

- NGN op LinkedIn
- SharePoint 2010 gelanceerd in Las Vegas
- Team players: Wireshark en CACE Pilot
- Windows 7 Resource Kit
- DNS, DNSSEC, IPv6 en meer
- Waarom je niet onder Windows 7 uitkomt, deel 3

Relevante berichten

- 12-01 [De 25 gevaarlijkste programmeerfouten op een rij](#)
- 03-05 [FireEye virtualiseert netwerkbeveiliging](#)
- 17-04 [Microsoft bouwt Forefront uit tot SaaS-bewaker](#)
- 31-10 [Stration-worm evolueert razendsnel](#)
- 03-08 ['Groffe tactiek hackers maakt mkb kwetsbaar'](#)



UITREIKING VAN DE OORKONDE AAN JOHN EIJGENSTEIJN

Reageer

Reageer als:
Gast

Nickname (verplicht):

URL:

Stuur reacties naar e-mail:
(e-mail zal niet worden getoond of gedeeld)

Reactie:

Voeg afbeeldingen toe

(Powered by JS-kit)
(Spam filtering by Akismet)

NU OP COMPUTERWORLD

5 Manieren waarop de Linux desktop zich de das om doet

Infoworld loopt ten einde, Computerworld begint!

Tips voor tijdens sollicitaties: kijk goed rond!

Bescheiden herstel in ICT-markt

Crisis in je datacentrum (5 wijze lessen)

10 Ideeën die Apple afkeek van Microsoft

NU OP WEBWERELD

ADV: Wil jij ook 85.000.000 klanten?

EC tekent deal met online muziekindustrie

ICT Roddels 280: Snow Leopard Server (podcast)

Linux-bestrijder SCO ontslaat ceo

Computerworld.nl volgt Infoworld.nl op

Batterij voorkomt exploderende telefoons (video)

NU OP ITWORLD

Celesio benoemt COLT als enige leverancier voor...

Qwise wordt NetApp Gold Partner

VelligMobiel vereenvoudigt beheer mobiele...

Wereldwijde samenwerkingsovereenkomst voor...

Geef uw mening en maak kans op een Netbook van...

Scholten Awater gekozen tot HP Authorised...

INTERNATIONAAL NIEUWS

Mobile WAN operators raise 'openness' bar

There's no such thing as a 'business cell phone'

Oracle fined by TPC over benchmarking claims

Microsoft Covers the Basics With Security Essentials

Cisco to buy videoconferencing vendor Tandberg for \$3B

Google Wave boasts twin power

CONTACT

ADVERTEREN

MOBIEL

RSS

TWITTER

NIEUWSBRIEF



Privacyverklaring. © 2009 IDG Nederland. Alle rechten voorbehouden.

IDG Nederland is uitgever van: [ChannelWorld](#), [CIO](#), [Computer!Totaal](#), [GameZ](#), [Gadget](#), [Computerworld](#), [ITworld](#), [Techworld](#), [Tips & Trucs](#), [Webwereld](#), [Zoom.nl](#) en [ADSL!Totaal.nl](#)

Meer informatie: [IDG Nederland](#), [IDG.com](#), Hosting by [Terremark](#).