**Persbericht**

**“De *ram*, *zwerm* en *egel* ontleed”**

*Sophos-onderzoek identificeert drie ‘hackeraanvalspatronen’*

Oosterhout, 17 juli 2019 - **Sophos lanceert vandaag het meest recente onderzoek** [**RDP Exposed: The Threat That's Already at your Door**](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers.aspx?url=%2fen-us%2fmedialibrary%2fPDFs%2ftechnical-papers%2fsophos-rdp-exposed-the-threats-thats-already-at-your-door-wp.pdf)**. Het onthult hoe cybercriminelen meedogenloos organisaties proberen aan te vallen via het gebruik van Remote Desktop Protocol (RDP).**

RDP blijft voor system administrators een regelrechte nachtmerrie. Sophos rapporteert al sinds 2011 over cybercriminelen die RDP uitbuiten, en in het afgelopen jaar hebben deze bendes achter twee van de grootste gerichte ransomwareaanvallen (Matrix en SamSam) gezeten en RDP hierbij ingezet.

Matt Boddy, securityspecialist bij Sophos, en nauw betrokken bij het onderzoek, stelt: *"Onlangs heeft een fout in de remote RDP-code BlueKeep (CVE-2019-0708) alle media gehaald. Deze kwetsbaarheid is zo ernstig is dat het kan worden gebruikt om ​​ransomware-uitbraken in gang te zetten die zich in no-time over de hele wereld kunnen verspreiden. Beveiliging tegen RDP-dreigingen gaat echter veel verder dan patchen tegen Blue Keep; het is slechts het topje van de ijsberg. Naast de ‘zorg’ om BlueKeep moeten IT-managers veel meer tijd besteden aan RDP. Uit ons onderzoek blijkt namelijk dat cybercriminelen bezig zijn met het onderzoeken van alle potentieel kwetsbare computers die RDP 24/7 met aanvallen met wachtwoordschattingen blootlegt."*

Het recente RDP-onderzoek van Sophos laat zien hoe aanvallers RDP-apparatuur vinden zodra deze apparaten online komen. Om dit te demonstreren, heeft Sophos tien geografisch verspreide honeypots ingezet om RDP-gebaseerde risico's te meten en te kwantificeren. De voornaamste bevindingen in het onderzoek laten dat zien dat

* Alle tien honeypots binnen één dag hun eerste RDP-inlogpoging ontvingen
* Remote Desktop Protocol pc's in slechts 84 seconden blootstellen
* De tien RDP-honeypots gecombineerd 4.298.513 mislukte inlogpogingen hebben bijgehouden gedurende een periode van 30 dagen (ofwel: één poging elke zes seconden)
* De industrie van mening is dat cybercriminelen sites zoals Shodan gebruiken om naar open RDP-bronnen te zoeken. Sophos’ onderzoek laat zien hoe cybercriminelen hun eigen technieken hebben om open RDP-bronnen te vinden en niet noodzakelijkerwijs alleen op sites van derden vertrouwen

**Hackergedrag ontleed**

Sophos heeft op basis van het onderzoek drie aanvalspatronen geïdentificeerd.

* De **ram** is een strategie ontworpen om het wachtwoord van de systeemadministrator te onthullen. Een voorbeeld uit het onderzoek is dat binnen tien dagen, een aanvaller 109.934 inlogpogingen bij de Ierse honeypot deed met slechts drie gebruikersnamen om toegang te krijgen;
* De **zwerm** is een strategie die gebruikmaakt van sequentiële gebruikersnamen en een eindig aantal van de slechtste wachtwoorden. Een voorbeeld uit het onderzoek werd in Parijs gezien met een aanvaller die de gebruikersnaam Abrown negen keer gebruikte binnen veertien minuten, gevolgd door negen pogingen met de gebruikersnaam BBrown, vervolgens CBrown, gevolgd door DBrown, etc. Het patroon werd herhaald met A.Mohamed, AAli, ASmith en anderen;
* De **egel** kenmerkt zich door uitbarstingen van activiteiten gevolgd door langere perioden van inactiviteit. Een voorbeeld in Brazilië zag elke ‘spike’ gegenereerd met één IP-adres, duurde ongeveer vier uur en bestond uit tussen 3.369 en 5.199 wachtwoord-gissingen.

Boddy legt uit wat de reikwijdte van deze POP-exposure voor bedrijven betekent: *"Op dit moment zijn er via RDP wereldwijd meer dan drie miljoen apparaten toegankelijk, en het is nu een zeer gewild point of entry door cybercriminelen. Sophos ziet dat criminelen die doelgerichte ransomware inzetten (waaronder BitPaymer, Ryuk, Matrix en SamSam) bijna alle andere methoden achterwege laten – ten gunste van RDP. Alle honeypots werden binnen een paar uur ontdekt, alleen maar omdat ze via RDP aan het internet werden blootgesteld. Waar mogelijk zou het gebruik van RDP verminderd moeten worden en goede wachtwoordbeleid binnen organisaties van kracht moeten zijn. Bedrijven moeten dienovereenkomstig handelen om het juiste beveiligingsprotocol in te voeren teneinde zich te beschermen tegen meedogenloze aanvallers."*

RDP Exposed: The Threat That's Already at your Door is [hier](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers.aspx?url=%2fen-us%2fmedialibrary%2fPDFs%2ftechnical-papers%2fsophos-rdp-exposed-the-threats-thats-already-at-your-door-wp.pdf) te downloaden.

**Over Sophos**   
Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK) en in Boston (VS). Meer informatie over Sophos op: [www.sophos.com](http://www.sophos.com).

**Voor meer informatie, contacteer:**Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.