



CYBERSECURITY  
EXPERTS ON YOUR SIDE

# RDP: SECURITY CONFIGUREREN VOOR EEN TOEKOMST OP AFSTAND

RDP gebruiken om uw netwerk te beheren tijdens een crisis? Zorg er dan voor dat u uw risico's beperkt middels goede hygiëne, authenticatietools en het gebruik van een bestaande kennisbank.

De coronapandemie heeft enterprises wereldwijd ertoe gedwongen hun medewerkers thuis te laten werken waar mogelijk. Dit betekent ook dat het gebruik van RDP-technologie, welke in de laatste jaren vaak werd misbruikt. Meerdere situaties hebben zich voorgedaan waarbij aanvallers slecht geconfigureerde instellingen of zwakke wachtwoorden hebben misbruikt om toegang te krijgen tot bedrijfsnetwerken.

Enmaal binnen hebben aanvallers vrij spel om bijna alles te doen, waaronder bijvoorbeeld het stelen van intellectueel eigendom of andere gevoelige gegevens en deze versleutelen tot er losgeld is betaald.

AUTEUR: Aryeh Goretsky  
BIJDRAGE DOOR: James Shepperd  
VERTAALD DOOR: Christa Tjadens

April 2020

# 1.

## Wat doen aanvallers met RDP?

In de afgelopen jaren heeft ESET een groei gezien in het aantal incidenten waarbij aanvallers op afstand via het internet verbinding maakten met Windows-servers en inlogden als beheerder. Dit omvat meerdere aanvalsvectoren, waaronder: kwetsbaarheden (zoals BlueKeep CVE-2019-0708), phishing, credential stuffing, password spraying, brute force aanvallen of slecht geconfigureerde services die toegang bieden tot interne systemen.

Wanneer aanvallers op een server zijn ingelogd als beheerder zullen zij doorgaans het netwerk verkennen om te bepalen met wat voor bedrijf zij te maken hebben, waar de server voor wordt gebruikt en wanneer. Vervolgens kunnen ze beginnen met het uitvoeren van hun kwaadaardige acties.

Dit is geen volledige lijst van alle aanvalsmogelijkheden. Het betekent ook niet dat alle kwaadwillenden altijd al deze acties gaan uitvoeren. De exacte frequentie, volgorde en het aanvalspatroon zullen elke keer anders zijn.

### ENKELE VAN DE VEELVOORKOMENDE KWAADAARDIGE ACTIVITEITEN DIE WIJ HEBBEN GEZIEN:

- Het wissen van logbestanden met daarin bewijs van hun aanwezigheid in het systeem
- Het uitzetten van geplande back-ups en schaduwkopieën
- Het uitzetten van securitysoftware of het instellen van uitzonderingen in, bijvoorbeeld, de firewall)
- Het downloaden en installeren van verscheidene programma's op de server
- Het wissen of overschrijven van oude back-ups indien deze toegankelijk zijn
- Het exfiltreren van data van de server

### DE DRIE MEEST VOORKOMENDE ACTIVITEITEN ZIJN:

- Het installeren van coin-miningprogramma's om cryptocurrency, zoals Monero, te genereren
- Het installeren van ransomware om de organisatie af te persen voor geld, vaak betaald in cryptocurrency als bitcoin
- In sommige gevallen kunnen aanvallers aanvullende software installeren om toegang te behouden tot servers en deze te compromitteren in het geval dat hun RDP-activiteiten worden ontdekt en onderbroken

## NOEMENSWAARDIGE, RECENTE RDP-ACTIVITEITEN

Een bekende ransomware, [GandCrab](#), die tot mei 2019 actief was, gebruikte Ransomware-as-a-Service (RaaS) als verdienmodel waarbij de ontwikkelaars een aantal gerelateerde kwaadwillenden inzetten om malware te distribueren. GandCrab richtte zich specifiek op MSP's en gebruikten [RDP](#) om verbinding te maken met hun remotemanagementtools en zo meerdere klanten tegelijk af te persen.

Onze experts denken dat de sourcecode van GandCrab mogelijk aan een andere groep die nu actief is, namelijk Sodinokibi, is verkocht. Dit ondanks dat GandCrabs beheerders hun 'pensioen' [aankondigden](#) nadat de FBI sleutels had gepubliceerd om hun ransomware te ontsleutelen. Dit vermoeden wordt gewekt door veranderingen in de code, diens structuur en updates die volgden. [Sodinokibi-ransomware](#) werd voor het eerst gedetecteerd toen GandCrab zijn activiteiten stillegde – zo [verving](#) Sodinokibi GandCrab als het ware. Sodinokibi gebruikt soortgelijke tactieken, technieken en procedures als eerste stap om [MSP's](#) via RDP aan te vallen.

## RDP-KWETSBAARHEID OPENT DE DEUR WAGENWIJD VOOR RISICO'S

Aanvallen via RDP worden langzaamaan vaker uitgevoerd en worden aan overheidsbeleid onderworpen door overheidsinstanties als de Amerikaanse FBI, de Britse NCSC, Canadese CCCS en het Australische ACSC.

In mei 2019 werden deuren wagenwijd opengezet door de komst van [CVE-2019-0708](#), oftewel "BlueKeep", een kwetsbaarheid in RDP van Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server R2, Windows Server 2008 en Windows Server 2008 R2\*.

Al zijn deze besturssystemen al verouderd, in de meeste gevallen niet langer of beperkt ondersteund door de vendor, suggereert telemetrie dat er nog steeds veel kwetsbare systemen in gebruik zijn.

De [BlueKeep-kwetsbaarheid](#) stelt aanvallers in staat programmacode op de computers van slachtoffers te draaien. Al kunnen individuele aanvallers een grote dreiging vormen door geautomatiseerde tools te gebruiken bij een aanval, is deze kwetsbaarheid ook een "worm": een aanval zou zichzelf automatisch over verschillende netwerken kunnen verspreiden zonder tussenkomst van gebruikers, net als bij Win32/Diskcoder.C (ook bekend als NotPetya) en Conficker-worms in het verleden.

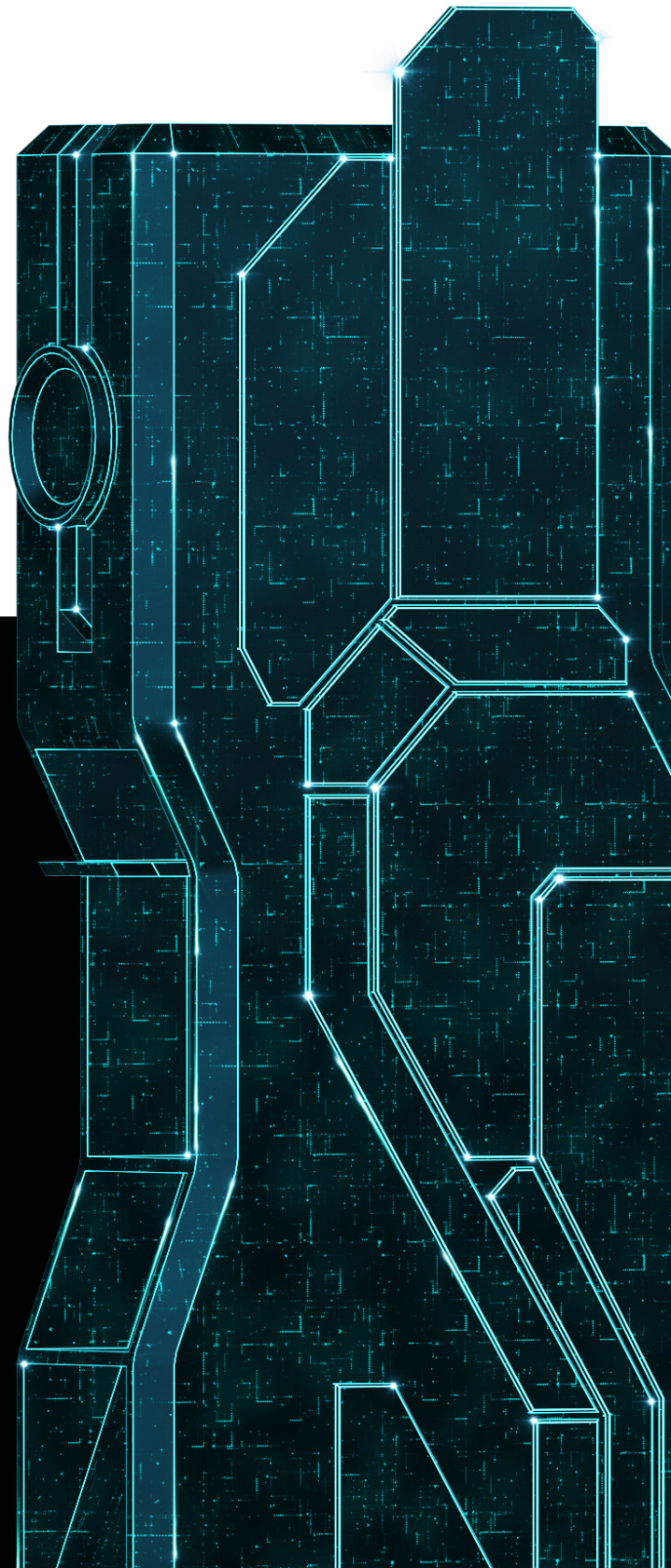
**ESET BIEDT EEN GRATIS DETECTIETOOL VOOR BLUEKEEP (CVE-2019-0708) OM SYSTEMEN TE DETECTEREN DIE KWETSBAAR ZIJN VOOR MISBRUIK VIA RDP. CLIJK OP DE KNOP HIERONDER VOOR GEBRUIKSIJSTRUCTIES EN DOWNLOAD.**

*N.B.: Versies Windows 8 en Windows Servers 2012 en latere versies zijn op het moment van schrijven ongeraakt door de kwetsbaarheid.*



Exploitatie/misbruik van wormbare kwetsbaarheden wordt veelal gezien als een ernstig probleem. Microsoft heeft de kwetsbaarheid het hoogste securityniveau, Critical, toegekend in die gids die zij voor klanten publiceerden; in de Amerikaanse National Vulnerability Database ontvangt CVE-2019-0708 een score van 9,8 op een schaal van 10. Microsoft heeft een [blog](#) gepubliceerd waarin gebruikers worden aangeraden om hun patches te installeren, inclusief die voor besturingssystemen, zoals Windows XP en Windows Server 2003, die niet langer ondersteund worden. Zorgen over een wormbaar exploit waren zo groot dat in juni 2019 de Amerikaanse National Security Agency een advies publiceerde met de aanbeveling om Microsofts patches tegen de kwetsbaarheid te installeren.

Al wordt de kwetsbaarheid nog wel eens gedetecteerd bij pentesten, werden er tot november 2019 geen escalaties in BlueKeep-activiteit gerapporteerd tot november 2019. In november maakten ZDNet en WIRED publiek bekend dat het exploit weer gebruikt werd. De aanvallen waren naar verluidt minder succesvol; ongeveer 91% van de kwetsbare computers crashten met een stop-error (oftewel een bug check of het blauwe scherm) op het moment dat de aanvaller poogde de BlueKeep-kwetsbaarheid te misbruiken. De aanvallers slaagden er wel in om op de overige 9% van de kwetsbare computers Monero-cryptominingsoftware te installeren. De groep criminelen maakten gebruik van geautomatiseerde exploitatie, dus niet middels een gevreesde worm-aanval, maar zonder veel succes.



# 2.

## Verdediging tegen RDP-aanvallen

Dus, wat kunt u doen? Ten eerste is het belangrijk om niet meer direct verbinding via RDP te maken met uw servers, of dit op z'n minst te beperken waar mogelijk. Dit kan problematisch zijn voor veel organisaties, vooral nu veel werknemers waarschijnlijk thuiswerken wegens quarantainemaatregelen.

Het is belangrijk om te benadrukken dat u ernstig risico loopt op een aanval als u nog steeds gebruikmaakt van Windows Server 2008 of Windows 7 (welke sinds januari 2020 niet meer ondersteund worden) en machines die op deze platformen draaien ook direct toegankelijk zijn via RDP. In dit geval dient u onmiddellijk stappen te ondernemen ter mitigatie. Door op deze platforms te draaien, wordt uw dreigingsoppervlak substantieel vergroot. De volgende aanbevelingen dienen lagere prioriteit te krijgen dan het updaten van uw organisatie

naar platformen die volledig ondersteund worden door hun leveranciers. Voor degenen die reeds gebruikmaken van up-to-date platformen betekent dat niet dat u direct moet stoppen met RDP gebruiken. U dient echter wel zo snel mogelijk aanvullende maatregelen te treffen. Om hierbij te helpen, hebben wij een tabel samengesteld met de Top 12 stappen die u kunt nemen om uw computers tegen RDP-gebaseerde aanvallen te beveiligen.



# 12 AANBEVELINGEN OM RDP TE BEVEILIGEN

Deze tabel is los gesorteerd op volgorde van belang en implementatiegemak, maar dit kan per organisatie verschillen. Sommige aanbevelingen zijn wellicht niet van toepassing of zijn mogelijk beter van toepassing in een andere volgorde. Mogelijk dient uw organisatie ook aanvullende stappen te ondernemen..

AANBEVELING	REDEN
1 Blokkeer externe verbindingen met lokale machines op port 3389 (TCP/UDP) op de perimeterfirewall*	Blokkeert toegang tot het internet voor RDP volledig.
2 Test en rol patches uit voor de BlueKeep-kwetsbaarheid (CVE-2019-0708) en stel Network Level Authentication zo snel mogelijk in.	Het installeren van Microsofts patch en het volgen van hun aanbevelingen helpt apparaten te beschermen tegen de BlueKeep-kwetsbaarheid.
3 Eis complexe wachtwoorden voor accounts waarop ingelogd kan worden via RDP; verplicht een lange wachtzin met 15+ karakters, exclusief woorden verwant aan het bedrijf, productnamen of gebruikers.	Beveilig uw organisatie tegen aanvallen waarbij (gelekte) wachtwoorden worden geraden en credential stuffing. Het is erg eenvoudig om deze aanvallen te automatiseren; het verlengen van wachtwoorden maakt ze exponentieel resistenter tegen zulke aanvallen.
4 Eis unieke wachtwoorden voor lokale accounts met beheerdersrechten om toegang te krijgen tot servers (bijv. door LAPS of een robuuste wachtwoordmanager te gebruiken). <i>*Beperk ook servertoegangsrechten tot een beperkte groep gebruikers of users.</i>	<i>(zie hierboven)</i> Het beperkt het aanvalsoppervlak van servers door het aantal gebruikers dat er toegang toe heeft te beperken..
5 Stel waar mogelijk het encryptieniveau van RDP-clientverbindingen in op " <b>hoog</b> ". Indien dat niet mogelijk is, gebruik dan het hoogst mogelijk beschikbare encryptieniveau voor verbindingen.	Gebruik waar mogelijk 128-bitsencryptie voor client-servercommunicatie.
6 Installeer een multifactorauthenticatie-oplossing (MFA), zoals <a href="#">ESET Secure Authentication</a> , en maak MFA verplicht voor alle accounts waarop ingelogd kan worden via RDP én voor beheerdersaccounts.	Eis een tweede authenticatielaag, die alleen toegankelijk is voor werknemers via hun mobiele telefoon, een hardware token of een ander mechanisme, om op computers in te loggen..

---

7

Installeer een virtueel privénetwerk (VPN)-toegang om RDP-verbindingen buiten uw lokale netwerk te bemiddelen.

Voorkomt RDP-verbindingen tussen het internet en uw lokale netwerk. Laat u sterkere identificatie- en authenticatie-eisen instellen voor toegang op afstand tot computers.

---

8

Zorg er, via uw securitydashboard, voor dat uw endpointsecuritysoftware een sterk wachtwoord gebruikt dat niet te herleiden is tot andere (administratieve, service-) accounts. [ESET Security Management Center \(ESMC\)](#) biedt eenvoudig instelbare en gedetailleerde policies en kan verschillende computergroepen creëren. ESMC is geschikt voor multitenancy en biedt beveiligde inlogmogelijkheden met MFA.

Biedt een extra laag beveiliging in het geval dat een aanvalleur beheerdersrechten tot uw netwerk krijgt.

---

9

Stel het [blokkeren van exploits](#) in op uw endpointsecuritysoftware, waarbij [non-signature-based anomaly detection-technologie](#) het gedrag van applicaties die vaak worden aangevallen.

Veel endpointsecurity-oplossingen kunnen ook exploitatietechnieken blokkeren. Ga na of deze functionaliteit is ingesteld

---

10

Isoleer onbeveiligde computers in uw netwerk die toegang tot het internet via RDP nodig hebben

Implementeer netwerkisolatie om kwetsbare computers te blokkeren van de rest van het netwerk.

---

11

Vervang onbeveiligde computers.

Als een computer niet gepatcht kan worden (tegen de BlueKeep-kwetsbaarheid), zorg dan tijdig voor vervanging.

---

12

Overweeg het instellen van GeoIP-blokkade bij VPN-toegang.

Als werknemers en leveranciers in hetzelfde land gevestigd zijn, overweeg dan om toegang vanuit andere landen te blokkeren om verbindingen van onbekende aanvallers te blokkeren.

*\*RDP opereert standaard op port 3389. Indien u deze port gewijzigd heeft naar een andere waarde, dan is dat de port die geblokkeerd dient te worden..*



# 3.

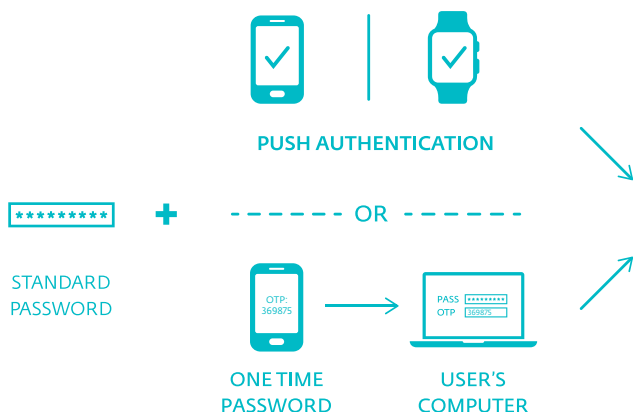
## Hoe ESET helpt uw RDP te beveiligen

Een goede eerste stap is ervoor te zorgen dat uw endpointsecuritysoftware 1. up-to-date is en 2. de BlueKeep-kwetsbaarheid detecteert. Gelaagde technologie heeft vervolgens een granulaire rol. BlueKeep wordt gedetecteerd als RDP/Exploit.CVE-2019-0708 door [ESETs Network Attack Protection-module](#), welke een verlenging is van de firewalltechnologie die wordt gebruikt in ESETs endpoint-beveiligingsoplossingen vanaf versie 7.

Een andere belangrijke technologielaag voor het beschermen van RDP is [ESET Exploit Blocker](#), die veel misbruikte applicaties (onder andere browsers, documentlezers, e-mailclients, Flash en Java) monitort. In plaats van alleen te letten op specifieke CVE-kenmerken, wordt er ook op exploitatietechnieken gelet. [Gedetecteerde dreigingen](#) worden direct geblokkeerd op de machine.

Naast de juiste technologie adviseren wij het gebruik van duidelijke, gebruiksvriendelijke processen die gesterkt worden door tools die eenvoudig in gebruik zijn. Omdat er voor het beveiligen van RDP verschillende (procedurele) stappen nodig zijn, is gebruiksvriendelijke multifactorauthenticatie (MFA) mogelijk de meest cruciale stap omdat het als beveiliging dient tegen eenvoudige of gekraakte wachtwoorden. Door op toegang tot een systeem of platform, in dit geval RDP, te focussen, beveilt u één van de meest belangrijke systemen voor het waarborgen van de veiligheid van uw netwerk en diens individuele gebruikers.

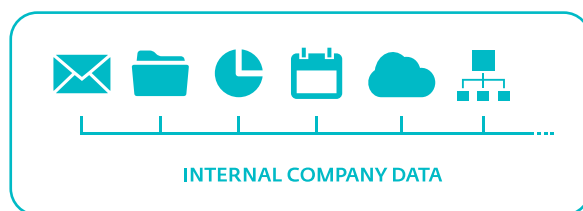
Oplossingen als [ESET Secure Authentication \(ESA\)](#) ondersteunen VPN's (op zichzelf ook belangrijk voor het beveiligen van toegang), toegang op belangrijke apparaten met gevoelige data en clouddiensten als Office365, Google Apps of Dropbox en andere diensten die [ADFS 3.0](#) of [SAML](#) gebruiken.



ESA kan centraal beheerd worden vanuit de browser en is ontworpen om op alle iPhones en Android-apparaten te werken. De oplossing werkt ook goed met meerdere andere authenticators, waaronder gebruiksvriendelijke pushnotificaties, mobiele applicaties, hardwaretokens, FIDO security keys en andere gepersonaliseerde methoden (via de ESA SDK). Daarnaast helpt ESA zowel bedrijfsgegevens al de cloud te beveiligen op een eenvoudige, maar krachtige manier, die bijdraagt aan het voldoen aan compliance-eisen voor reguleringen als de AVG.

**OM BEDRIJVEN TIJDENS DE COVID-19-PANDEMIE HUN KRITIEKE SYSTEMEN EN GEVOELIGE GEGEVENS VOLDOENDE TE LATEN BEVEILIGEN, HEEFT ESET HAAR PROEFPERIODE VOOR ESA VERLENGD TOT 90 DAGEN.**

Tenslotte is [volledige schijfversleuteling](#) een goede vervolgstap op MFA. ESET Full Disk Encryption biedt krachtige versleuteling van systeemschijven, partities of volledige schijven. Deze kunnen beheerd worden vanuit ESET beheerconsole, [ESET Security Management Center](#) en [ESET Cloud Administrator](#), om de datasecurity van uw organisatie verder te verbeteren.





## KENNIS IS MACHT – VOLLEDIGE SECURITY OOK

Verschillende [RDP-technieken en -tactieken kunnen ook geanalyseerd worden aan de hand van de MITRE ATT&CK-kennisbank](#). ATT&CK en (EDR-)tools gebruiken kan erg nuttig zijn om dreigingen voor uw netwerk uitvoerig te analyseren. Tools als [ESET Enterprise Inspector \(EEI\)](#) stelt beheerders en securityteams in staat detecties te analyseren, rechtstreeks aan de ATT&CK-kennisbank te refereren voor meer informatie en detectieregels te maken die op de organisatie van toepassing zijn.

Een andere mogelijkheid voor RDP-dreigingen is (gedeeltelijke) detecties, terwijl u onbeschermd blijft. EDR kan ook een rol spelen in scenario's waarbij [duidelijke detecties](#) niet plaatsvinden. In sommige gevallen crashte het aangevallen systeem direct door gebruik van de BlueKeep-kwetsbaarheid. Om de RDP-exploit te laten functioneren moet deze het mogelijk gecombineerd worden met een andere exploit, bijvoorbeeld een information disclosure-kwetsbaarheid in Adobe Flash of PHP die aanvallers in staat stelt geheugenadressen in de kernel te achterhalen. Op deze manier wordt de kans op crashes verminderd, aangezien de huidige exploit heap spraying gebruikt.

Dit gerelateerde gedrag kan gesignaleerd worden middels gepersonaliseerde regels in EEI die een alarm af laten gaan om de aandacht van de beheerder te trekken. Aanvullende netwerkinformatie kan verkregen worden via reguliere pentesten en door via SIEM, [IPS](#) en [IDS](#) verdacht gedrag in de gaten te houden.

## CONCLUSIE

**COVID-19 heeft voorgoed veranderd hoe organisaties werken. Werkgevers moeten zich aanpassen aan zowel de eisen en behoeften van hun medewerkers thuis als die van de toekomst.**

**De pandemie heeft ons aangetoond dat veel banen en taken vanuit huis uitgevoerd kunnen worden, terwijl voorheen werd gedacht dat aanwezigheid op kantoor daarvoor essentieel was. Om deze verandering te faciliteren, hebben thuiswerkers veilige toegang tot kantoor nodig. ESET biedt meerdere oplossingen die kunnen helpen veilige toegang te bieden tot bedrijfsmiddelen.**