Voorblad casus mondeling college-examen

Examenvak en niveau	**informatica vwo**
Naam kandidaat	
Examennummer	
Datum	
Voorbereidingstijd	**20 minuten**
Titel casus	**Nieuwe versie Dorifel-virus gesignaleerd**

Instructie

Bestudeer bijgevoegde voorbereidingsopdracht. Uw mondeling examen begint straks met een gesprek over deze casus.

Toelichting:

- Het is toegestaan om op deze kopie te schrijven/markeren.
- Aan de hand van deze casus of dit artikel wordt een aantal vragen gesteld over informaticabegrippen die in dit artikel genoemd of besproken worden.
- Misschien komen niet alle vragen aan bod.

Hulpmiddelen

Bij deze voorbereidingsopdracht mag u gebruik maken van:

- Een woordenboek

Aan het eind van de voorbereidingstijd haalt een van de examinatoren u op.

College voor Toetsen en Examens

Nieuwe versie Dorifel-virus gesignaleerd

Er is een nieuwe versie gesignaleerd van het Dorifel-virus, dat vorige maand schade aanrichtte bij een aantal organisaties in Nederland, waaronder ministeries en provincies. De nieuwe versie van het virus is moeilijk te detecteren.

Het nieuwe Dorifel-virus is ontdekt door beveiligingsonderzoeker Mark Loman, CEO bij Surfright. De nieuwe versie is versleuteld, in tegenstelling tot het originele virus. Daardoor is het moeilijker te herkennen voor virusscanners; slechts 3 van 42 geteste virusscanners zouden de nieuwe versie herkennen. Volgens Loman heeft het virus op elke pc die het infecteert een andere *hash*; dat maakt het lastig voor antivirusbedrijven om definities uit te brengen waarmee de malware wordt gedetecteerd.
Circa twintig minuten na installatie downloadt de nieuwe versie van Dorifel volgens Loman een rootkit die verwijdering verder bemoeilijkt. Ook wordt *ransomware* gedownload. Gebruikers krijgen een venster te zien dat zogenaamd van Buma/Stemra afkomstig is, waarin wordt gemeld dat ze illegaal hebben gedownload en daarom een boete van 100 euro moeten betalen. Doet een gebruiker dat niet, dan krijgt hij geen toegang tot zijn computer en bestanden.
De vorige versie van Dorifel deed iets vergelijkbaars; onder meer Word- en Excel-documenten werden ontoegankelijk gemaakt. Daarbij werd, om onduidelijke redenen, echter geen vergelijkbare melding getoond. Het was daarom lang onduidelijk waarom de malware de documenten verminkte. Misschien is de waarschuwing toen per abuis niet getoond.
Volgens Loman heeft de ontwikkelaar van de malware zijn code opgeschoond en wordt er nu bijvoorbeeld minder vaak gecommuniceerd met de command-and-control-server, die de malware nieuwe instructies kan sturen. Die instructies zitten in de nieuwe versie verstopt in een afbeelding van Mohammed Ali.
Hoeveel mensen al zijn besmet met de nieuwe Dorifel-versie, is onduidelijk.

"Ik heb het Nationaal Cyber Security Centrum er al over ingelicht", zegt Loman. Hij onderzoekt nog of er in Nederland infecties zijn. Woordvoerster Mary-Jo van de Velde van het NCSC zegt dat er nog geen meldingen binnen zijn gekomen over besmette pc's bij de overheid.
Beveiligingssoftware die Lomans bedrijf heeft ontwikkeld, HitmanPro, kan de malware verwijderen. Eerder dook al een nieuwe versie van de malware op in de Verenigde Staten. Volgens beveiligingsbedrijf Digital Investigation is het aan te raden om het IP-adres 91.220.35.61 in de firewall te blokkeren, evenals de domeinnamen open-consulting-company.com en oianowifna.ru. Die worden waarschijnlijk gebruikt om de malware te verspreiden of dienen als command-and-controlserver.

***Bron**: https://tweakers.net/nieuws/84629/nieuwe-versie-dorifel-virus-gesignaleerd.html*
Door Joost Schellevis

Vragen

1. Geef een samenvatting van bovenstaande tekst.
2. Wat is een virusscanner en hoe werkt deze software (2)?
3. Dit virus werkt met een hash en een command-and-controlserver. Hoe werkt dat?
4. Waarom moet het IP-adres 91.220.35.61 geblokkeerd worden?
5. In de tekst wordt gesproken over malware. Noem een aantal voorbeelden.
6. Leg van 3 van deze uit hoe het werkt.
7. Welke andere maatregelen moet je als computergebruiker nemen om veilig met op internet te werken?
8. Wat is een rootkit en waarom is dit zo moeilijk te verwijderen?
9. Waarom wordt er in de benaming van een rootkit verwezen naar root?

Uitwerking bij casus Dorifel-virus

1.	I	Ter beoordeling aan de examinator.
2.	I	Software die virussen probeert te detecteren. Dit doet de software door te scannen naar bestanden volgens een lijst en door verdacht gedrag op te merken.
3.	I	De hash is een verborgen bestand dat pas iets doet als het contact maakt met de control server. Dit werkt dan als een Trojaans paard.
4.	I	Het IP-adres is gekoppeld aan een domeinadres en dus een website. Het IP-adres betreft dus een server waar de control is.
5.	R	adware, worm, virus, rootkit, keylogger, etc.
6.	R	ter beoordleing
7.	T	besturingssysteem updaten als dat nodig is. Software zoals Flash en drivers updaten, maak een herstelpunt.
8.	I	Een rootkit is een set softwaretools die wordt gebruikt door een derde partij (meestal een hacker) na toegang te hebben verkregen tot een (computer)systeem. De rootkit nestelt zich diep in het besturingssysteem, zodat het mogelijk is dat het besturingssysteem instabiel wordt. De rootkit is bijna niet te verwijderen zonder de functie van het besturingssysteem te beschadigen.
9.	R/I	De root is waar de administrator van een systeem volledig toegang heeft, en bij een rootkit heeft de hacker dat dus ook.