Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Office macro's

Een oude dreiging in een nieuw jasje

Factsheet FS-2014-01
versie 1.0 | 30 januari 2014

In de jaren '90 van de vorige eeuw verscheen veel malware die misbruik maakte van een functie in softwarepakket Microsoft Office: macro's. Macro's boden gebruikers de mogelijkheid om taken te automatiseren, maar waren voor virusschrijvers een dankbare zwakke plek via welke zij hun slachtoffers aanvielen en hun malware verder verspreidden. Microsoft heeft daar lering uit getrokken en de standaardconfiguratie van Office aangepast. Hierdoor waren gebruikers die hun instellingen lieten staan op de standaardconfiguratie niet meer kwetsbaar en verdwenen de grote aanvalsgolven van macrovirussen van het toneel.

Vooral thuisgebruikers zijn tegenwoordig niet meer kwetsbaar, maar grote organisaties maken soms gebruik van macro's en hebben de instellingen daarvoor daarom aangepast, afwijkend van de aanbeveling. Dit heeft hernieuwde aandacht getrokken van malware-auteurs en heeft langzamerhand geleid tot de terugkeer van macrovirussen. Eigenlijk zijn dit geen virussen meer in de vorm van massale uitbraken, maar andersoortige malware die zeer gericht en op maat gemaakt wordt, voor aanvallen op individuele organisaties. De oplossing is echter eenvoudig.

De belangrijkste feiten

- Macro's krijgen nieuwe aandacht; in plaats van de virusuitbraken van de jaren '90 worden ze nu misbruikt in gerichte aanvallen op individuele organisaties.
- Microsoft Office staat vaak onveilig ingesteld, om legitiem gebruik van macro's mogelijk te laten blijven.
- Met behulp van vertrouwde bestandslocaties kunnen een veilige configuratie en legitiem macrogebruik naast elkaar bestaan.

Wat zijn macro's?

In sommige kantoorapplicaties, in de praktijk vrijwel altijd Microsoft Office, kunnen zogenaamde macro's actief zijn. Een macro bestaat uit een reeks geautomatiseerde opdrachten die door de gebruiker kunnen worden aangeroepen met een bepaalde toetsencombinatie of muisklik. Macro's kunnen ook automatisch uitgevoerd worden, bijvoorbeeld bij het openen of sluiten van een bepaald document. Macro's worden bij veel organisaties gebruikt om de correspondentielay-out of huisstijl mee te maken.

Software die macro's ondersteunt is daartoe vaak uitgerust met een interne scripttaal. In Microsoft Office kan een macro worden gemaakt in de Microsoft Visual Basic (VBA) editor die vanuit Word, Excel en PowerPoint kan worden aangeroepen. Een gebruiker hoeft geen VBA-code te programmeren maar kan ook gebruik maken van de opnamefunctie. Daarbij kan een gebruiker een aantal muisbewegingen of toetsaanslagen voordoen en deze plaatsen in een macro. Ook macro's gemaakt met de opnamefunctie bestaan uit VBA-code, maar dit wordt door Office gegenereerd vanuit de handelingen van de gebruiker.

Een macro kan in een document zelf worden opgeslagen of in een ander document, bijvoorbeeld een documentsjabloon. Een macro wordt aangeroepen op naam; als dezelfde naam verschillende keren wordt gebruikt dan wordt de macro uitgevoerd die het dichtste bij is. Als dus een macronaam wordt aangeroepen die zowel in het document zelf is gedefinieerd als in een sjabloon dan wordt de macro in het document uitgevoerd.

Een macro kan pas worden uitgevoerd als de beveiligings-instellingen dit toestaan. Dit wordt op twee punten bepaald:

- de instellingen voor macro's in het Vertrouwenscentrum;
- de vertrouwde locaties in Bestandslocaties.

Wat zijn de risico's van macro's?

Aanvallers kunnen macro's schrijven die kwaadaardige code bevatten en automatisch uitgevoerd worden. Omdat Office toestaat dat systeembronnen worden aangeroepen is een macro een krachtig uitgangspunt om malware te plaatsen die het hele systeem van de gebruiker infecteert. Er wordt dan van oudsher gesproken van een macrovirus, zij het dat nu hier nieuwe aandacht voor is, er andere vormen van malware worden gebruikt. Het is zelfs mogelijk een compleet programma (zoals een programma om een werkplek op afstand over te nemen) te plaatsen in een Office-document dat vervolgens wordt uitgepakt en aangeroepen vanuit de macro.

Veel organisaties hebben in de beveiligingsinstellingen toegestaan dat macro's worden uitgevoerd, omdat macro's bijvoorbeeld worden gebruikt om gebruik van de huisstijl te ondersteunen. Soms ontwikkelen gebruikers binnen een organisatie zelf macro's – buiten het zicht van de ICT-afdeling – die door hele afdelingen worden gebruikt. Hierdoor ontstaat een onbekende afhankelijkheid met (soms kritische) bedrijfsprocessen.

Het bestand dat in macro's verstopte malware bevat kan door aanvallers worden verspreid via onder meer e-mailbijlagen, webpagina's en verwisselbare media zoals USB-schijfstations. Omdat het geïnfecteerde bestand zich gedraagt als een normaal document verloopt een infectie vaak onopgemerkt. Antivirusprogramma's herkennen bekende malware op basis van de unieke 'vingerafdruk', maar zijn niet vaak in staat kwaadaardig gedrag te herkennen in individueel aangepaste (en dus onbekende) malware.

Wie zijn het slachtoffer?

Omdat de standaardinstellingen van Microsoft Office macro's tegenwoordig niet meer toestaan zijn veel thuisgebruikers niet kwetsbaar voor malware in macro's. Om die reden leent deze aanvalsmethode zich niet meer voor grootschalige verspreiding.

Automatische macro's

Macro's kunnen automatisch worden uitgevoerd bij bepaalde gebeurtenissen wanneer de beveiligingsinstellingen dit toestaan. Deze gebeurtenissen zijn gekoppeld aan bepaalde macronamen, waarbij er verschillen zijn tussen Word, Excel en PowerPoint. In Word zijn de volgende mogelijkheden:

- **AutoExec** werkt alleen in sjablonen en wordt gestart wanneer het sjabloon wordt geladen (bij een als standaard ingesteld sjabloon zal dit direct bij het starten van Word zijn).
- **AutoNew** wordt gestart bij het aanmaken van een nieuw document.
- **AutoOpen** wordt gestart bij het openen van het document.
- **AutoClose** wordt uitgevoerd vóór het sluiten van het document.
- **AutoExit** wordt uitgevoerd vóór het afsluiten van Word of wanneer het sjabloon wordt gesloten.

Oud nieuws

Macrovirussen bestaan sinds het midden van de jaren '90. Het eerste zichzelf verspreidende macrovirus was WM.Concept in 1995. Dit virus richtte geen schade aan, maar was vermoedelijk slechts een experiment van de maker om de technische mogelijkheid te demonstreren.

Een bekendere uitbraak is die van Melissa in 1999. Melissa verspreidde zich via een Word-document als bijlage in een e-mail met een korte tekst die gebruikers moest verleiden de bijlage te lezen. Eenmaal geopend verspreidde het virus zich naar andere documenten en paste die aan door er citaten uit The Simpsons in te plaatsen. Sommige documenten werden ongemerkt ge-e-maild. Het virus liet ook zichzelf via Outlook e-mailen naar de eerste vijftig contactpersonen.

Melissa ontving enige media-aandacht omdat het het snelst verspreidende virus tot dan toe was. In de ochtend werd het ontdekt, en nog diezelfde avond meldden vele organisaties grote aantallen besmettingen. Ook Microsoft zelf zag zich genoodzaakt al hun interne e-mailverkeer op te schorten om verspreiding tegen te gaan.

Tegenwoordig zijn voor macrovirussen dergelijk grote uitbraken niet meer haalbaar. Maar wanneer een kwaadwillende het op een specifieke organisatie gemunt heeft, bijvoorbeeld voor bedrijfsspionage, kan een onveilige macro-instelling dikwijls als zwakste schakel van de keten in het vizier komen.

De afgelopen jaren hebben zich enkele incidenten voorgedaan waarbij macro's werden ingezet bij gerichte aanvallen op individuele organisaties, de zogeheten Advanced Persistent Threats.[1] Sommige van deze gerichte aanvallen startten met een medewerker van de organisatie die een bijlage in een e-mail opende. Er is geen volledig beeld te krijgen van hoe vaak dit voorkomt; individueel ingezette malware wordt door antivirusbedrijven niet opgemerkt en organisaties zijn zeer terughoudend in het communiceren wanneer dergelijke aanvallen zich hebben voorgedaan.

Van in macro's verstopte malware voor andere applicaties dan die uit het Microsoft Office-pakket zijn geen praktijkvoorbeelden bekend, al is het hiervoor ook mogelijk dat in het kader van een Advanced Persistent Threat specifieke malware voor een doelwit op maat gemaakt wordt.

[1] Voor meer informatie over Advanced Persistent Threats, zie het NCSC-factsheet 'De aanhouder wint' op https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-de-aanhouder-wint-advanced-persistent-threats.html.

Ben ik kwetsbaar?

Om te controleren of Microsoft Office macro's toestaat of tegenhoudt kunnen de instellingen in het Vertrouwenscentrum worden nageslagen.

Staat mijn Microsoft Office goed ingesteld?
Instructie geldt voor versies 2007, 2010 en 2013

- Start een Microsoft Office-applicatie.
- Ga naar:
  - de Office-knop of menu Bestand (linksboven);
  - Opties (rechtsonder (2007) of in linkermenu (2010, 2013));
  - Vertrouwenscentrum (onderste menu-item);
  - Instellingen voor het Vertrouwenscentrum;
  - Macro-instellingen.
- Controleer of macro's zijn uitgeschakeld, of dat er een melding voor wordt gegeven.
- De laatste optie schakelt alle macro's in en wordt niet aanbevolen. Wanneer die optie is geselecteerd, is deze Office-applicatie kwetsbaar voor kwaadaardige macro's.

Let op dat voor iedere Office-applicatie de instellingen onafhankelijk zijn. Herhaal daarom bovenstaande controle voor alle Office-applicaties (Word, Excel, PowerPoint, etc.).

Naast Microsoft Office zijn er andere applicaties die macro's ondersteunen. Raadpleeg de handleiding of website van die applicaties om te controleren of de veilige instellingen zijn gekozen.

Wat kan ik doen?

Om besmetting met malware via macro's te voorkomen zijn de volgende maatregelen nodig. Zie het kader Handelingsperspectief voor een concrete uitwerking van de voorgestelde maatregelen.

- **Inventariseer het legitiem gebruik van macro's** in uw organisatie. Sommige beveiligingsmaatregelen kunnen bedrijfsprocessen hinderen. Om te voorkomen dat plotselinge klachten van gebruikers leiden tot het terugdraaien van maatregelen is het belangrijk om eerst een goed overzicht te hebben van alle mogelijke afhankelijkheden.

- **Gebruik vertrouwde bestandslocaties** of digitale handtekeningen voor documenten met legitieme macro's. Blokkeer het uitvoeren van alle andere macro's in alle applicaties die het ondersteunen.

- **Configureer de server voor inkomende e-mail** zodat inkomende e-mail met macro's in de bijlagen wordt tegengehouden. Houd er rekening mee dat ook in dit geval legitieme documenten kunnen worden geblokkeerd. Laat de geadresseerde dit weten zodat de afzender kan worden geïnstrueerd een bestand zonder macro's aan te leveren.

Naast deze specifieke maatregelen blijven ook de algemene aanbevelingen voor malwarepreventie staan. Train gebruikers om geen ongevraagd toegestuurde bestanden te openen, ook al lijken ze van een bekende afzender te komen.

Handelingsperspectief

1. Maak alle gebruikers bewust van het risico van malware in bestanden en de manieren waarop dit wordt verspreid.
2. Inventariseer legitiem gebruik van macro's. Wees kritisch op de noodzaak en kijk of er alternatieven mogelijk zijn.
3. Pas in het Vertrouwenscentrum van Microsoft Office de macro-instellingen aan. De volgende opties zijn mogelijk:
   - Bij de eerste instelling "Alle macro's uitschakelen, zonder melding" worden de macro's niet uitgevoerd zonder dat de gebruiker daarover wordt geïnformeerd of de gelegenheid krijgt hiervan af te wijken.
   - De tweede instelling "Alle macro's uitschakelen, met melding" is de standaardinstelling van Microsoft Office. Als een gebruiker een macro wil uitvoeren (of als een automatische macro dreigt te worden uitgevoerd) dan krijgt de gebruiker een waarschuwing maar met de optie om de macro toch uit te voeren.
   - De derde optie laat alleen macro's toe die voorzien zijn van een digitale handtekening van een "Vertrouwde uitgever", waardoor macro's van andere partijen worden geblokkeerd.
   - De vierde optie "Alle macro's inschakelen (wordt niet aanbevolen omdat mogelijk schadelijke programmacode kan worden uitgevoerd)" laat toe dat alle macro's zonder restricties of waarschuwingen worden uitgevoerd.
4. Bedenk per applicatie het benodigde veiligheidsniveau. Zo is het voor bijvoorbeeld PowerPoint niet waarschijnlijk dat hier macro's gebruikt worden. Deze kunnen dan geheel uitgeschakeld worden.
5. Vervang macro's in losse documenten door documentsjablonen en verplaats al deze bestanden naar centrale locaties.
6. Stel de centrale locaties in als vertrouwde locaties. Mochten (sommige) gebruikers toch documenten met macro's willen toepassen, maak dan een speciale vertrouwde locatie voor hen waar zij deze documenten kunnen plaatsen en daarvandaan kunnen opstarten.
7. Laat leveranciers van macro-applicaties de documenten digitaal ondertekenen zodat die uitgever als vertrouwd kan worden ingesteld.
8. Configureer de e-mailserver of de virusscanner die het e-mailverkeer filtert om bijlagen met macro's tegen te houden, eventueel met een waarschuwing aan de geadresseerde.
9. Overweeg Excel-bestanden met macro's te verbieden als zij niet een specifieke extensie daarvoor (.xlsm) hebben.[2]
10. Blokkeer bestanden met specifieke macro-extensies (.docm, .pptm, .xlsm) voor externe bronnen (e-mail, internet, cd-rom, etc.).

[2] Zie hiervoor http://support.microsoft.com/kb/948615/.

Tot slot

Voorbeelden van gerichte aanvallen op grote organisaties zijn er in overvloed. Helaas worden er in veel gevallen weinig details vrijgegeven over de aanval; vooral technische informatie wordt niet gepubliceerd. Hierdoor is het moeilijk om een goed beeld te krijgen van de omvang van dit specifieke probleem en de grootte van de daadwerkelijke dreiging. Toch is er een duidelijke reden om de macro-instellingen goed te zetten: wanneer een aanvaller op zoek is naar de zwakste schakel, dan zal die in de macro-kwetsbaarheid snel zijn gevonden.

Dit factsheet is mede tot stand gekomen met hulp van prof. dr. E.R. Verheul, Radboud Universiteit Nijmegen.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55 | F 070-888 75 50
Publicatienr: FS-2014-01 1.0 | Aan deze informatie kunnen geen rechten worden ontleend.