

## 1. ZIP- und RAR-Archive

Cyberkriminelle lieben es, Malware in Archiven zu verbergen. So wurden beispielsweise ZIP-Dateien mit dem verlockenden Namen „Love\_You0891“ (die jeweilige Endziffer variierte) von Angreifern verwendet, um die Ransomware [GandCrab](#) am Vorabend des Valentinstags unter den Nutzern zu verbreiten. Einige Wochen später wurden weitere Betrüger gesichtet, die [Archive mit dem Qbot-Trojaner](#) (spezialisiert auf den Datendiebstahl) versendeten.

Darüber hinaus wurde in diesem Jahr ein interessantes WinRAR-Feature entdeckt. Beim Erstellen eines Archivs können Regeln festgelegt werden, um den Inhalt im Systemordner zu entpacken. Insbesondere können Inhalte in den Windows-Startordner verschoben werden, sodass sie beim nächsten Neustart unweigerlich ausgeführt werden. Wir empfehlen WinRAR-Nutzern daher, das [Packprogramm umgehend zu aktualisieren](#), um dieses Problem zu beheben.

## 2. Microsoft-Office-Dokumente

Microsoft-Office-Dateien, insbesondere Word-Dokumente (.doc, .docx), Excel-Tabellen (.xls, .xlsx, .xlsm), Präsentationen und Vorlagen sind bei Cyberkriminellen besonders beliebt; Diese Dateien können sogenannte [Makros](#) – kleine Programme, die innerhalb der Datei ausgeführt werden – enthalten, die Cyberkriminelle als Scripts verwenden, um Malware herunterzuladen.

Am häufigsten richten sich derartige Anhänge an Büroangestellte und werden als Verträge, Rechnungen, Steuermeldungen oder dringende Nachrichten der Geschäftsleitung getarnt. Zum Beispiel wurde ein Banking-Trojaner namens [Ursnif](#) unter dem Deckmantel einer Zahlungsaufforderung italienischen Nutzern untergeschoben. Sobald das Opfer die Datei öffnete und sich dazu bereit erklärte, die benötigten Makros zu aktivieren (aus Sicherheitsgründen standardmäßig deaktiviert), wurde ein Trojaner auf den Computer heruntergeladen.

## 3. PDF-Dateien

Tatsächlich kennen viele Nutzer die Gefahren von Makros in Microsoft Office-Dokumenten, sind sich jedoch häufig nicht der möglichen Fallen in PDF-Dateien bewusst. Doch auch hinter scheinbar harmlosen PDFs kann sich Malware verbergen – das Dateiformat kann nämlich zum Erstellen und [Ausführen von JavaScript-Dateien](#) verwendet werden.

Zudem haben Cyberkriminelle ein besonderes Faible dafür, Phishing-Links in PDF-Dokumenten zu verstecken. In einer Spam-Kampagne forderten Betrüger die Nutzer beispielsweise dazu auf, eine „sichere“ Seite aufzurufen, auf der sie dann zur Anmeldung bei ihrem American-Express-Konto aufgefordert wurden. An dieser Stelle ist es vermutlich unnötig zu erwähnen, dass ihre Anmeldeinformationen umgehend an die Betrüger weitergeleitet wurden.

## 4. ISO- und IMG-Disk-Images

Im Vergleich zu den vorherigen Arten von Anhängen, werden ISO- und IMG-Dateien nur sehr selten verwendet. Cyberkriminelle haben ihnen in letzter Zeit allerdings deutlich mehr Aufmerksamkeit gezollt als zuvor. Bei diesen sogenannten Disk-Images handelt es sich im Grunde genommen um die Kopie einer CD oder DVD.

Angreifer verwendeten ein Disk-Image, um Malware – wie den auf Datendiebstahl spezialisierten Trojaner *Agent Tesla* – auf die Computer der Opfer zu schleusen. In dem Image befand sich eine böswillige ausführbare Datei, die dann Spyware auf dem Rechner aktivierte und installierte. In einigen Fällen verwendeten die Cyberkriminellen kurioserweise sogar zwei Anhänge (einen ISO-Anhang und einen DOC-Anhang); Vermutlich, um auf Nummer sicher zu gehen.

## So gehen Sie richtig mit potenziell bösartigen Anhängen um

Alle Nachrichten mit einem angehängten Archiv oder einer .docx bzw. .pdf-Datei in den Spam-Ordner zu verschieben, wäre tatsächlich zu viel des Guten. Um Betrüger zu überlisten, sollten Sie sich stattdessen ein paar einfache Regeln merken:

- Öffnen Sie keine verdächtigen E-Mails von unbekannten Absendern. Wenn Sie nicht wissen, weshalb eine Nachricht mit einem spezifischen Betreff in Ihrem Postfach gelandet ist, sollten Sie diese ganz einfach ignorieren.
- Wenn Sie bei Ihrer Arbeit mit Korrespondenzen von Fremden zu tun haben, sollten Sie zunächst die E-Mail-Adresse des Absenders und den Namen der angehängten Datei überprüfen. Wenn Ihnen etwas komisch vorkommt, sollten Sie den Anhang unter keinen Umständen öffnen.
- Lassen Sie das Ausführen von Makros in Dokumenten, die Sie per E-Mail erhalten, nur dann zu, wenn Sie sich sicher sind, dass dies unbedingt erforderlich ist.
- Behandeln Sie alle Links innerhalb einer Nachricht oder Datei mit Vorsicht. Wenn Sie nicht ganz verstehen, weshalb Sie zum Öffnen eines Links aufgefordert werden, ignorieren Sie diesen einfach. Ansonsten können Sie den Link der Website auch ganz einfach manuell in Ihren Browser eingeben.
- Verwenden Sie eine zuverlässige [Sicherheitslösung](#), die Sie über gefährliche Dateien informiert, diese blockiert und Ihnen darüber hinaus eine Warnmeldung zukommen lässt, sobald Sie versuchen eine verdächtige Seite zu öffnen.