Newsletter

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Informationen für betriebliche Datenschutzbeauftragte
und IT-Verantwortliche in kirchlichen Dienststellen

Nr. 04/2016

Infizierte Joomla-Server verbreiten TeslaCrypt

Heise berichtet über einen weiteren Verteilungsweg des Verschlüsselungstrojaners „TeslaCrypt“, der den durch die Kriminellen betriebenen Aufwand bei der Verbreitung des Schadcodes deutlicher werden lässt.

Bisher wurde im Zusammenhang mit Verschlüsselungstrojanern vor allem über die übliche Verbreitung von Schadcode über E-Mails mit präparierten Dateianhängen (z.B. Word- und PDF-Dateien) berichtet und gewarnt. Mittlerweile wurde durch Ermittlungen in mehreren Fällen des LKA Niedersachsen festgestellt, dass verschiedene Joomla-Server den Verschlüsselungstrojaner verbreiten.

Die Besonderheit: Die betroffenen Server mit dem CMS Joomla waren allesamt auf dem aktuellen Stand, d.h. es waren alle aktuellen Sicherheitsupdates eingespielt worden. Trotzdem war es den Angreifern möglich die Server zu infizieren. Dies ist ihnen aufgrund einer Sicherheitslücke Ende letzten Jahres gelungen. Diese wurde durch ein Update vom 14. Dezember 2015 geschlossen, zu diesem Zeitpunkt jedoch bereits einige Tage aktiv ausgenutzt. Während dieses Zeitraums erfolgte eine sog. „Zero-day“-Attacke, die Systeme kompromittiert bevor überhaupt ein Schutz möglich ist.

Eine durch die Kompromittierung eingebaute Hintertür wurde durch das Installieren des Updates nicht geschlossen. So ist es den Angreifern möglich gewesen auch lange nach dem Schließen der Sicherheitslücke Zugriff auf die Server zu erhalten und schließlich Schadcode auf die Server zu laden. Es ist davon auszugehen, dass es sich bei den Joomla-Servern die TeslaCrypt verteilen um genau solche Fälle handelt.

In den bekannten Fällen befand sich der Schadcode, der Funktionsaufrufe wie „decrypt_url“ enthielt, in folgenden Dateien:

/administrator/includes/defines.php
/includes/defines.php

Betreiber und Administratoren von Webseiten bzw. Servern die das CMS Joomla einsetzen wird dringend empfohlen ihre Systeme auf Anzeichen derartiger Infektionen hin zu überprüfen. Heise weist weiter darauf hin, dass davon auszugehen ist, dass die Kriminellen auch Server mit Wordpress, Drupal und anderen CMS angreifen oder angegriffen haben und sich diese durchaus brisante Problematik nicht auf Joomla beschränkt.

→ http://www.heise.de/security/meldung/Infizierte-Joomla-Server-verteilen-Erpressungs-Trojaner-TeslaCrypt-3114184.html

Javascript-Variante von Verschlüsselungstrojaner Locky

Nachdem in unseren vorherigen Newslettern bzgl. Verschlüsselungstrojanern bereits auf Mail-Anhänge mit präparierten Word- und PDF-Dateien hingewiesen wurde, möchten wir an dieser Stelle auf eine weitere Datei-Variante hinweisen. Der Trojaner Locky wird aktuell mittels JavaScript-Dateien verteilt. Diese verstecken sich in einem als Rechnung getarnten ZIP-Archiv.

Hierbei ist ein Wursthersteller aus Ludwigslust unfreiwilliger Helfer gewesen, da in seinem Namen massenhaft infizierte E-Mails versendet wurden. Der Betreff etwa „Rechnung Nr. 2016_131“ oder ähnlich mit einer anderen Zahlenkombination in Zusammenhang mit dem Absender, der beispielsweise fueldner6D@lfw-ludwigslust.de lautete, suggeriert zunächst eine

authentische E-Mail eben jenes Wurstfabrikanten. In einwandfreiem Deutsch wird der Empfänger dazu aufgefordert die der Mail angehängte Rechnung zu öffnen und den Adressaten zu korrigieren. Im Anhang befindet sich oben erwähnte ZIP-Datei, die nach dem Muster „RG843841155137-SIG.zip, benannt und eine JavaScript-Datei enthält. Jeder der das Skript ausführt infiziert in diesem Augenblick das System mit dem Verschlüsselungstrojaner.

Das Skript enthält einen Downloader, der den eigentlichen Schadcode nachlädt, ausführt und anschließend alle Festplatten, Netzwerkfreigaben und über USB angeschlossenen Speichermedien durchsucht und verschlüsselt. Von den Kriminellen wird in diesem Fall ein Lösegeld in Höhe von 0,5 Bitcoin (etwa 190 €) gefordert.

Auch in diesem Fall wird dringend empfohlen eine Backup-Strategie auszuarbeiten und regelmäßig Sicherungen seiner Dateien anzufertigen. Explizit hinzuweisen ist darauf, dass auch Dateien auf USB-Geräten und Netzwerkfreigaben von dem Trojaner verschlüsselt werden. Gleiches gilt für einen eingebundenen Cloud-Speicher im Falle einer automatischen Synchronisierung. Es ist daher darauf zu achten, dass das Backup-Medium mit dem System nicht dauerhaft verbunden ist.

Der Wurstfabrikant hat mit der Verbreitung des Trojaners nichts zu tun. Die Angreifer bedienten sich des sog. „Mail-Spoofings“ um eine falsche Absenderadresse vortäuschen zu können.

→ http://www.heise.de/security/meldung/Neue-Masche-Krypto-Trojaner-Locky-ueber-Javascript-Dateien-verbreitet-3113689.html

Heise weist auf einen weiteren Artikel hin, in dem die Frage behandelt wird, was man im Falle der Verschlüsselung seiner Dateien durch einen Trojaner möglicherweise noch retten kann, ohne das Lösegeld zu zahlen.

→ http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-Was-tun-gegen-den-Windows-Schaedling-3112408.html