+ + + Pressemitteilung + + +

Trustwave SpiderLabs: Fast jede 5. Spam-Mail enthält den Krypto-Trojaner Locky

München, 15. März 2016 - Der Verschlüsselungs-Trojaner Locky verbreitet sich scheinbar ungebremst. Das Team von Trustwave SpiderLabs, das aus Sicherheits-Experten, Forschern und ethischen Hackern besteht, hat alleine in den letzten sieben Tagen über vier Millionen Spam-Mails aufgespürt, die den gefährlichen Krypto-Trojaner Locky enthalten. Das entspricht etwa 18% des gesamten Spam-Mail-Volumens. Doch gegen Locky ist ein Kraut gewachsen. Die Experten des Trustwave SpiderLabs zeigen, wie Locky arbeitet und wie man den Krypto-Trojaner mit wenigen Handgriffen daran hindern kann, sich auf den Rechner einzunisten.

Die Zahlen basieren auf den von Trustwave verbreiteten Web Honeypots. Diese digitalen Honigtöpfe wirken von außen wie ein regulärer Bestandteil einer Webseite, sie sind aber vom restlichen IT-System isoliert und werden von den Trustwave SpiderLabs überwacht. So lässt sich Schadsoftware anlocken und ausgiebig analysieren.

Obwohl Locky in den letzten Wochen so etwas wie eine Art zweifelhafter Berühmtheit erlangt hat, ist die Vorgehensweise des Verschlüsselungs-Trojaner keineswegs neu oder innovativ. Ransomware, wie diese Art von Trojanern auch genannt wird, wird von Cyber-Kriminellen schon seit Jahren eingesetzt. Weil die Urheber von Locky auf das gleiche Botnetz Zugriff haben, das für den Versand der Banking-Malware Dridex verantwortlich war, ist Locky besonders erfolgreich. Zur Erinnerung: Der Banking-Trojaner Dridex hat im letzten Jahr mindestens einen Schaden in zweistelliger Millionenhöhe verursacht.

Zudem weist Locky eine Besonderheit auf, die seinen Siegeszug bisher so unaufhaltbar machte: Wie ein Virus mutiert Locky und wird immer wieder den veränderten Abwehrmechanismen angepasst. Anfänglich waren es Office-Makros, die Locky nutzte, um sich auf einem System auszuführen. Jetzt sind es größtenteils Java-Script-Dateien, die für die Installation von Locky verantwortlich sind.

In den Spam-Mails befindet sich als Anhang eine ausführbare Java-Script-Datei. Wird diese angeklickt, lädt sie den Trojaner auf die Festplatte herunter. Sobald Locky auf der Festplatte ist, legt der Trojaner einen neuen Registrierungsschlüssel an (Registrierungsschlüssel HKEY_CURRENT_USER \ Software \Locky) und verschlüsselt die Daten auf dem infizierte System, auf Netzlaufwerken sowie auf allen ins System eingebundenen Cloud-Speichern. Bisher war es nicht möglich, Krypto-Trojaner mit herkömmlichen Sicherheitsprogrammen wieder vom System zu entfernen. Hat sich Locky oder ein anderer Krypto-Trojaner erst einmal auf dem System eingenistet, bleibt den Betroffenen nichts anderes übrig, als das von den Cyber-Kriminellen geforderte "Lösegeld" - bei Locky in Form von Bitcoins - zu zahlen, um wieder Zugriff auf ihre Daten zu bekommen.

Besonders in den letzten sieben Tagen hat Locky noch einmal mit aller Vehemenz zugeschlagen. Fast jede fünfte Spam-Mail hat den gefährlichen Krypto-Trojaner im Gepäck, insgesamt sind das vier Millionen Mails alleine in den letzten sieben Tagen. Dabei erreicht der Versand so extreme Spitzenwerte wie 200.000 Spam-Mails pro Stunde.

So kann man Locky ausbremsen

Hat Locky erst einmal den Rechner erreicht, ist es für eine Bekämpfung also zu spät. Wer sich gegen Locky wirksam schützen will, sollte also grundsätzlich keine Mailanhänge mit ausführbaren Java-Script-Dateien oder Office-Dokumenten anklicken. Firmenkunden empfehlen die Trustwave SpiderLabs

außerdem, eingehende JavaScript-Anhänge und Office-Dokumente die Makros enthalten, direkt am Gateway zu blockieren.

IT-Administratoren, die sich die Arbeit etwas vereinfachen wollen, können zum Beispiel auf Trustwave Secure Email Gateway zurückgreifen. Die Security-Lösung bietet einen Echtzeit-Schutz gegen aktuelle Bedrohungen unter Berücksichtigung aller Datenschutz- und Compliance-Anforderungen. Weitere Informationen bekommen Sie hier.

Druckfähiges Bildmaterial finden Sie hier:
http://www.laubstein-media.de/News/Trustwave_201603II.zip

Pressemitteilung zum Download:
http://www.laubstein-media.de/News/PM_Trustwave_201603II.pdf

Über Trustwave
Trustwave hilft Unternehmen die Cyberkriminalität zu bekämpfen, Daten zu schützen und Sicherheitsrisiken zu reduzieren. Mit Cloud- und Managed Security Services, integrierten Technologien und dem Trustwave SpiderLabs, einem Team von Sicherheitsexperten, bestehend aus ethischen Hackern und Forschern, unterstützt Trustwave die Unternehmen bei der Verwaltung und Umsetzung der IT-Sicherheit und den Compliance-Programmen. Mehr als drei Millionen Unternehmen sind auf der Trustwave TrustKeeper® Cloud-Plattform registriert, über die Trustwave ein automatisiertes, effizientes und kosteneffektives Schwachstellen-, Bedrohungs- und Compliance-Management anbietet. Trustwave ist in Chicago ansässig und verfügt über Kunden in 96 Ländern. Für weitere Informationen zu Trustwave, besuchen Sie bitte https://www.trustwave.com und https://www.info-point-security.com/hersteller/ueber-trustwave.

Pressekontakt:
Laubstein Media
Anja Eichelsdörfer
Untere Parkstr. 42
85540 Haar

Tel.: +49-89-41 85 84 85
Fax: +49-89-41 85 84 86
Mobil: +49-151-41 20 22 32

Mail: presse@laubstein-media.de
Web: http://www.laubstein-media.de