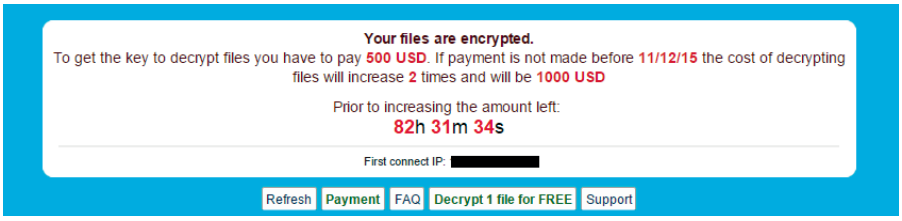
HILFE – MEINE DATEN SIND VERSCHLÜSSELT

von Andreas Wisler

Praktisch wöchentlich berichten diverse Medien über neue Varianten von Schädlingen, die die Festplatte bzw. die vorhandenen Daten verschlüsseln. Oft so, dass es nicht mehr möglich ist, an die eigenen Daten zu kommen. Der Hilfeschrei ist laut: Wie komme ich wieder an meine Daten?

Immer wieder hört und liest man von Software, die die lokalen Daten auf dem Rechner verschlüsselt. Inzwischen gibt es sogar Schädlinge, die auf verbundene Serverlaufwerke oder gar auf eine NAS, die oft als Backup verwendet wird, zugreift. Dann sind nicht nur die eigenen Daten auf dem Rechner verloren, sondern auch gleich noch das Backup mit. Nur gegen Bezahlung wird das Kennwort zum Entschlüsseln der Daten herausgegeben. Diese Art von Schädlingen wird Ransomware genannt. Wer genau hinter diesen Angriffen steht, ist in der Regel nicht nachvollziehbar. Dieses Jahr sind zudem erstmalig Mietmodelle aufgetaucht. Eine Ransomware kann für eine bestimmte Zeit gemietet werden, der Betreiber des Netzwerkes verdient an jeder Erpressung eine gewisse Anzahl an Prozenten mit.

Einer der ersten dieser Art war CryptoWall, der zum ersten Mal im September 2013 im Internet entdeckt wurde. Die Verteilung erfolgt über E-Mails und ein Botnet. Ein Botnet sind von Hackern übernommene Rechner, die für die Verteilung des Schädlings genutzt werden. Wird CryptoWall ausgeführt, sucht er bestimmte Dateitypen wie DOC / DOCX (Microsoft Word) und verschlüsselt diese mit einem mathematischen Verfahren (RSA, 2048 Bit). Das identische Verschlüsselungsverfahren wird auch für Webseiten genutzt, zum Beispiel, wenn Sie auf Ihr Online-Banking zugreifen. Es gilt somit als sehr sicher oder eben als nicht knackbar, eine Entschlüsselung der Daten ist somit nicht mehr möglich. Der Benutzer wird in der Folge zu einer Webseite gelotst und erhält in einem Fenster die Anweisung, 500 Dollar in Bitcoins (eine virtuelle Währung im Internet, die anonym von einem Ort an einen anderen transferiert werden kann) zu bezahlen.



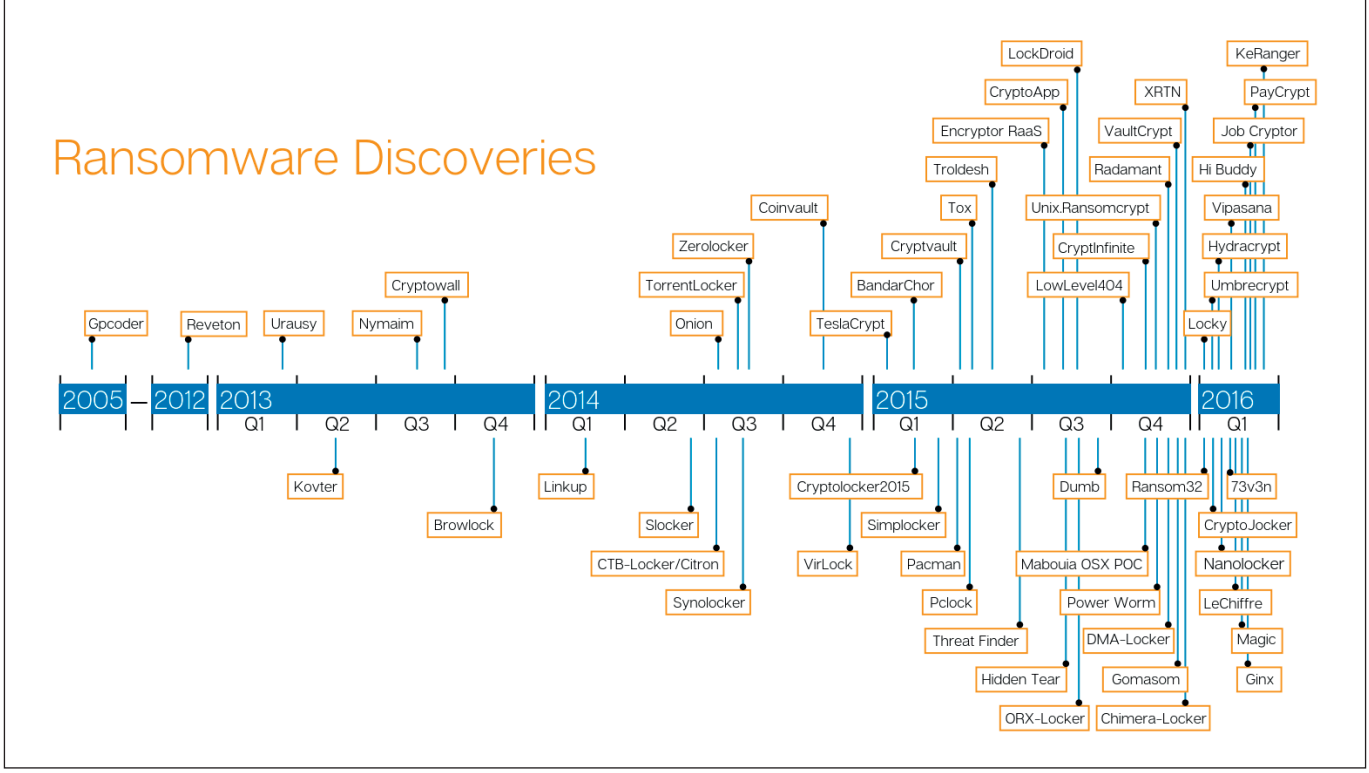
Ein Counter weist darauf hin, wie lange dies noch möglich ist. Nach Ablauf der Frist verdoppelt sich zwei Mal der Betrag, danach ist eine Entschlüsselung der eigenen Daten nicht mehr möglich, der dazu passende Wiederherstellungsschlüssel wird gelöscht. Verschiedene Quellen berichten, dass einige der betroffenen Personen bezahlen. Unter anderem war in der Tagespresse von einem Spital zu lesen, welches als einzige Lösung aus der Misere bezahlt hat. Je nach Quellen ergibt dies eine stolze Summe von bis zu drei Millionen US Dollar. Dies alleine ist ein grosser Antrieb, weiterhin auf diese Art Geld zu verdienen und eine Reduktion der Angriffe ist nicht zu erwarten. Dies zeigen auch aktuelle Varianten, die noch intelligenter geworden sind: zuerst wird überprüft, wer das Opfer ist. Handelt es sich dabei um eine grössere Firma oder gar um eine Behörde, wird der zu bezahlende Betrag massiv erhöht.

Die folgende Auswertung von Symantec (s. Grafik, rechte Seite) zeigt, dass es nicht bei CryptoWall geblieben ist. Eine Vielzahl von Varianten sind aktiv und versuchen, das «Business-Modell» zu übernehmen und ebenfalls viel Geld zu verdienen. Gerade in den vergangenen Monaten sind eine Vielzahl von weiteren Versionen entdeckt worden.

Doch bekommt der Benutzer nun tatsächlich seinen Schlüssel, um die Daten wiederherzustellen? Bei einigen Opfern war dies tatsächlich der Fall, nach wenigen Stunden wurde das überwiesene Geld abgeholt und der Wiederherstellungsschlüssel mitsamt eines Programms übergeben. Damit konnten die Daten wiederhergestellt werden. Doch ob dies immer der Fall ist, ist nicht garantiert. Je nachdem wer hinter dem Schädling steht, kann dies auch ins Leere führen und die Daten sind mitsamt des Geldes für immer verloren.

Sind nur Windows-Benutzer davon betroffen? Nein, inzwischen sind auch Schädlinge für den Mac im Internet aufgetaucht. Die sicheren Zeiten für Mac-Benutzer sind damit definitiv vorbei und es ist grosse Vorsicht geboten.

Wie verbreiten sich diese Schädlinge? Oft ist es der Weg via E-Mail. Aus irgendwelchen dubiosen Quellen oder dem Absuchen von Webseiten, analog wie dies Google für das Indexieren von Webseiten macht, werden E-Mail-Adressen beschafft. Diese erhalten dann die Aufforderung, eine beiliegende Datei zu öffnen. Immer öfters ist auch von perfekt und fehlerfrei geschriebenen Bewerbungsschreiben, als manipuliertes Word-Dokument getarnt, zu hören. Auch eine E-Mail mit einem Link zu einer Datei auf Dropbox wurde schon entdeckt – die Kreativität der Ransomware-Entwickler ist dabei unerschöpflich, um nicht aufzufallen oder das Antivirenprogramm zu täuschen. Mitte Februar 2016 wurden auch Webseiten, die mit Content-Management-System (CMS) Wordpress betrieben werden, infiziert. Durch eine



Quelle: Symantec Internet Security Threat Report 2016

vorhandene Schwachstelle kopiert sich der Schädling auf die Webseite. Besucht nun jemand eine solche verseuchte Webseite, kann es sein, und der Schädling beginnt ohne Ihr Dazutun mit der Verschlüsselung der erreichbaren Daten.

Wie schütze ich mich? Halten Sie Ihr System immer auf dem aktuellsten Stand. Installieren Sie die Updates (auch Patches genannt), die Microsoft, Apple und die vielen Software-Entwickler herausgeben. Vergessen Sie dabei nicht die anderen Programme, wie Office, Google Chrome, Firefox, Adobe Reader, Flash usw. Da sammelt sich doch einiges mit der Zeit an. Eine oft mühsame, aber enorm wichtige Aufgabe. Weiter gilt es, das Antivirenprogramm aktuell zu halten. Trotz dem aktuellen Antivirenprogramm ist Vorsicht geboten, nicht immer werden neue Varianten sofort erkannt! Daher gilt als dritter Punkt: klicken Sie nicht alles an, auch wenn es noch so spannend erscheint.

Was ist, wenn es doch mal passiert? Da hilft oft nur eines, das Wiederherstellen des Backups, Restore genannt. Daher gehört zu den wichtigen Aufgaben das Erstellen von regelmässigen Datensicherungen. Das reine Synchronisieren mit einem Netzwerkspeicher (NAS genannt) hat sich dabei als trügerische Sicherheit erwiesen. Ist dieser Speicher ständig verbunden oder über das Netzwerk erreichbar, verschlüsseln aktuelle Versionen der Schädlinge auch diese Daten. Sie benötigen daher ein Backup an einer externen Stelle. Dies kann zum Beispiel eine Wechselplatte oder ein grosser USB-Stick sein, den Sie wieder vom Rechner entfernen. Sollten Sie den Schädling auf dem Rechner haben, entfernen Sie diesen, bevor Sie die Festplatte anhängen. Erst wenn Sie ganz sicher sind, dass alles in Ordnung ist, spielen Sie Ihre vorher gesicherten Daten zurück.

Die Betrüger im Internet haben neue Wege gefunden, viel Geld zu verdienen. Da es mit den heutigen technischen Möglichkeiten nicht mehr möglich ist, die verschlüsselten Daten zu retten, ist es enorm wichtig, im Vorfeld für eine umfassende und geschützte Datensicherung zu sorgen. Im Internet gilt es Vorsicht walten zu lassen, und nicht jedes E-Mail oder jede Webseite anzuklicken und zu überlegen, will ich das wirklich? Nur so können Sie sich optimal vor den aktuellen Gefährdungen schützen.

DIENSTLEISTUNGEN

Die weiteren Dienstleistungen der goSecurity GmbH umfassen Penetration Tests, hersteller- und produkteneutrale Sicherheitsberatungen, ISO 27001 Zertifizierungsbegleitungen sowie Schulungen rund um die IT-Sicherheit.

Andreas Wisler ist Dipl. Ing. FH, CISSP, CISA, ISO 22301 und 27001 Lead Auditor. Bei der goSecurity GmbH ist er als Senior IT-Security Auditor für verschiedene Unternehmen tätig.