Hacker Lexikon: Ein Leitfaden für Ransomware, der unheimliche Hieb, der im Steigen begriffen ist

Autor: Kim Zetter.Kim Zetter Sicherheit
TELEGRAPHIERTE | 2015-09-17

Ransomware ist malware, das Ihre Tastatur oder Ihren Computer abschließt, um Sie daran zu hindern, auf Ihre Daten zuzugreifen, bis Sie ein Lösegeld bezahlen, gefordert normalerweise in Bitcoin. Der digitale Erpressungsschläger ist nicht neu-es ist seit etwa 2005 gewesen, aber Angreifer haben das Schema sehr verbessert mit um die Entwicklung des Lösegelds cryptware herum, welches verschlüsselt Ihre Dateien mit Hilfe eines privaten Schlüssels, den nur der Angreifer besitzt statt Ihre Tastatur oder Ihren Computer einfach abschließend.

TL; DR: Ransomware ist malware, das Ihre Tastatur oder Ihren Computer abschließt, um Sie daran zu hindern, auf Ihre Daten zuzugreifen, bis Sie ein Lösegeld bezahlen, - normalerweise forderte in Bitcoin. Eine beliebtere und heimtückischere Variation von diesem ist Lösegeld cryptware, das Ihre Dateien verschlüsselt, die eine private Taste benutzen, die nur der Angreifer besitzt, statt Ihre Tastatur oder Ihren Computer einfach abschließen.

Und ransomware macht diese Tage nicht nur Wirkungsschreibtischmaschinen oder Laptops; es richtet auch Mobiltelefone. Letzte Wochennachrichten, die von einem Stück ransomware pleite sind, wenn sich die Wildnis als Porno app verkleidet. Der so genannte Porno Droid app richtet Androidenbenutzer und ermöglicht Angreifer, um während des Forderns eines $ 500 Lösegelds von Opfern das Telefon abzuschließen und seine PIN-Nummer zu ändern, um Zugang zurückzugewinnen.

Früher gab dieses Jahr, das FBI an einen Alarm aus und warnte, dass alle Arten von ransomware im Steigen begriffen sind. Personen, Geschäfte, Behörden, akademische Institutionen und sogar Vollstreckungsagenten sind alle Opfer gewesen. Das malware kann Sie über eine arglistige E-Mail oder Website infizieren, oder Angreifer können es direkt Ihrem Computer liefern, wenn sie es schon mit einer Hintertür infiziert haben, durch die sie eintreten können.

Das Lösegeldgeschäft blüht

Gerade wie lukrativ ist ransomware? Eigentlich. Im Jahr 2012, Symantec gewann Zugang zu einem Befehl-und-kontrolliert vom CryptoDefense malware benutzten Server und bekam einen Blick von der Ausbeute der Hacker basierend auf Geschäften für zwei Bitcoin Adressen, die die Angreifer zu erhalten pflegten Lösegelder. Aus an einem einzelnen Tag mit dem malware infizierten 5,700 Computern heraus legt etwa drei Prozent von Opfern, denen geschienen ist, für das Lösegeld hin. An einem Durchschnitt von $ 200 pro Opfer schätzte Symantec, dass die Angreifer diesen Tag in mindestens $ 34,000 (.pdf) zogen. Von diesem extrapolierend, hätten sie in einem Monat mehr als $ 394,000 verdient. Und dies basierte auf Daten von nur einer Befehlsserver und zwei, die Bitcoin anspricht; die Angreifer wurden wahrscheinlich mehrere Server und Bitcoin Adressen für ihre Operation benutzend.

Symantec hat konservativ geschätzt, dass mindestens $ 5 Millionen jedes Jahr ransomware Opfern abgepresst wird. Aber, Gelder zu blechen, um das Lösegeld zu bezahlen, garantiert nicht, dass Angreifer wahr zu ihrem Wort sein werden, und Opfer werden in der Lage sein, auf ihre Daten wieder zuzugreifen. In vielen Fällen bemerkt Symantec, dass dies nicht auftritt.

Ransomware ist ein langer Weg gekommen, da es zuerst auftauchte, in Russland und andere Teile zwischen 2005 und 2009 von Osteuropa. Viele dieser frühen Schemen hatten einen großen Nachteil für Übeltäter doch: eine zuverlässige Art, Geld bei Opfern abzuholen. Am Anfang waren Online-Zahlungsmethoden nicht beliebt die Art, wie sie heute sind, also wurden einige Opfer in Europa und die USA angewiesen, Lösegelder über Kurzmitteilungen oder mit vorausbezahlten Karten zu bezahlen. Aber das Wachstum an digitalen Zahlungsmethoden, besonders Bitcoin hat sehr zu ransomwares Ausbreitung beigetragen. Bitcoin ist die beliebteste Methode geworden für das Fordern auslösen, weil es anonymize hilft, die Geschäfte, um extortionists daran zu hindern, verfolgt zu werden.

Laut Symantec zeigten einige der ersten Versionen von ransomware, die Russland strichen, eine pornographische Abbildung auf den Maschine und geforderter Zahlung des Opfers an, um es zu entfernen. Das Opfer wurde angewiesen, Zahlungen eines durch eine SMStextnachricht zu machen, oder durch Anrufen einer Vorzugstariftelefonnummer würde das die Angreifereinnahmen verdienen.

Die Evolution von Ransomware

Es dauerte nicht lang, damit die Angriffe sich in Europa und die USA und mit neuen Zielen ausbreiten, kam neu Techniken, beinhalten, als Ortsrechtsdurchsetzungsagenturen zu posieren. Ein als Reveton bekannt ransomware Angriff, das an US-Opfer gerichtet ist, produziert eine automatische Nachricht, die sagt, dass Ihre Maschine an Kinderpornoaktivität oder irgendeinem anderen Verbrechen beteiligt worden ist und abgeschlossen gewesen ist beim FBI oder Justizministerium. Es sei denn, Sie bezahlen eine Geldstrafe-in Bitcoin, natürlich und sandte an eine Adresse, die die Angreifer kontrollieren, - die Regierung stellt keinen Zugang zu Ihrem System wiederher. Anscheinend ist die Geldstrafe deswegen, einen Bundesverstoß zu begehen, der Kinderporno einschließt, jedoch billig, weil Reveton Lösegelder nur $ 500 oder weniger sind. Opfern wird 72 Stunden gegeben, um zu zahlen, und eine E-Mail-Adresse, fines@fbi.gov bezweifelt, wenn sie irgendwelche haben. In einigen Fällen werden sie mit Verhaftung bedroht, wenn sie nicht zahlen. Jedoch unwahrscheinlich ist das Schema, Opfer haben wahrscheinlich gezahlt, weil das extortionists ihr malware dadurch verteilte, für Netze zu werben, die mit Pornostandorten liefen, das Herbeiführen von Schuld und Furcht bei Opfern, die bewusst Pornographie geprüft hatten ob es Kinderporno war oder nicht. ***Symantec determined that some 500,000 people clicked on the malicious ads over a period of 18 days.***

Im August 2013 nahm die Welt von ransomware einen großen Sprung mit der Ankunft von CryptoLocker, das Öffentlichkeit und private kryptographische Schlüssel benutzte, um die Akten eines Opfers zu sperren und aufzuschließen. Geschaffen von einem Hacker mit dem Namen Slavik, wie verlautet denselben Verstand, wurde CryptoLocker anfangs an Opfer über das Gameover ZeuS verteilt, das trojanische Kappe einzahlte. Die Angreifer würden zuerst ein Opfer mit Gameover Zeus infizieren, um Bankausweispapiere zu stehlen. Aber, wenn das nicht funktionierte, installierten sie die Zeus Hintertür auf der Maschine des Opfers, um sie einfach abzupressen. Spätere Versionen von CryptoLocker breiten sich über eine E-Mail aus, die angeblich ist, von UPS oder FedEx zu kommen. Opfer wurden gewarnt, die, wenn sie es nicht taten, innerhalb von vier Tagen zahlen, - eine Digitaljüngste Taguhr in der automatischen

Nachricht von den Angreifern zählte die Stunden herunter-der Entschlüsselungsschlüssel würde zerstört und Nein man wäre in der Lage, zu helfen, ihre Akten aufzuschließen.

In nur sechs Monaten wurden mehr als eine halbe Million Opfer zwischen dem September 2013 und dem Mai 2014 mit CryptoLocker infiziert. Der Angriff war hoch wirksam, obwohl nur etwa 1,3 Prozent von Opfern das Lösegeld bezahlte. Das FBI schätzte letztes Jahr, dass das extortionists einen $ 27 Millionen von Benutzern betrogen hatte, die zahlten.

Unter CryptoLockers Opfern? Ein Polizeicomputer in Swansea, Massachusetts. Die Polizeidirektion beschloss, dem Lösegeld von 2 Bitcoins (über $ 750 zur Zeit) anstatt Versuch zu bezahlen, um zu begreifen, wie das Schloss zu zerbrechen ist.

"(das Virus) ist so kompliziert und erfolgreich, dass Sie diese Bitcoins kaufen müssen, von denen wir nie gehört hatten," die Swansea Polizei Lt. Gregory Ryan sagte die *Vorbotennachrichten*.

Im Juni 2014 waren das FBI und die Partner in der Lage, Befehl zu ergreifen, - und-Kontrollserver verwendeten für die Gameover Zeus Kappe und das Gameover Zeus CryptoLocker. In Folge der Beschlagnahmung war die Sicherheitsfirma FireEye in der Lage, ein Werkzeug zu entwickeln, das DecryptCryptoLocker genannt wird, um die Maschinen der Opfer aufzuschließen. Opfer konnten Logdateien auf die FireEye Website hochladen und einen privaten Schlüssel erhalten, um sie zu entschlüsseln. FireEye war nur in der Lage, das Werkzeug zu entwickeln, nach dem Erhalten des Zugangs zu einer Anzahl der verschlüsselten Schlüssel, die auf den Angriffsservern gelagert worden waren.

Vor dem scharfen Vorgehen war CryptoLocker so erfolgreich gewesen, dass es mehrere Nachahmer ablegte. Unter ihnen war eine, die CryptoDefense genannt wird, das aggressive Taktik verwendete, um Opfer darin zusammenzuschlagen zu zahlen. Wenn sie nicht das Lösegeld innerhalb von vier Tagen darüber gabelten, verdoppelte es sich. Sie hatten auch dazu, dass Bezahlung das Bergnetz verwendete, so dass die Geschäfte anonymized waren, und nicht, wie leicht verfolgt. Die Angreifer lieferten sogar Benutzern ein praktisch wie-zu führen für das Herunterladen und das Installieren des Bergkunden. Aber sie machten einen größeren Fehler-sie überließen dem Entschlüsselungsschlüssel für das Aufschließen von auf der Maschine des Opfers gelagerten Opferdateien. Das ransomware generierte den Schlüssel, als die Maschine des Opfers die Windows verwendete, API, bevor ich es an die Angreifer sende, so dass sie konnten, speichere es, bis das Opfer zahlte. Aber sie versäumten, zu verstehen, dass beim Verwenden vom eigenen Betriebssystem des Opfers, um den Schlüssel zu generieren, eine Kopie davon auf der Maschine des Opfers blieb.

The "malware author's poor implementation of the cryptographic functionality has left their hostages with the key to their own escape," Symantec noted in a blog post.

Das Geschäft von ransomware ist hoch professionalisiert worden. Im Jahr 2012 identifizierte zum Beispiel Symantec etwa 16 verschiedene Varianten von ransomware, das von verschiedenen strafbaren Banden verwendet wurde. Alle malware Programme konnten jedoch zurück zu einer Einzelperson für Kunden auf Anfrage verfolgt werden, die anscheinend volle Zeit arbeitete, ransomware zu programmieren.

Das Ransomware zu achten zunächst

Vor kurzem täuscht-es katalogisierte, was sie annehmen, dass sie heute die obersten drei ransomware Familien in der Wildnis sind, das sie als CryptoWall, CTB Schließfach und TorrentLocker identifizieren. CryptoWall ist eine verbesserte Version von CryptoDefense abzüglich seines tödlichen Fehlers. Jetzt generieren es die Angreifer, statt die Maschine des

Opfers zu benutzen, um den Schlüssel zu generieren, auf ihrem Server. In einer Version von CryptoWall verwenden sie starke AES symmetrische Kryptographie, um die Dateien des Opfers und einen RSA -2048 Schlüssel zu verschlüsseln, um den AES Schlüssel zu verschlüsseln. Neue Versionen von CryptoWall präsentieren ihren Befehlsserver auf dem Bergnetz, um sie besser zu verdecken, und kommunizieren auch mit dem malware auf Opfermaschinen durch mehrere Vollmachten.

CryptoWall kann nicht nur Dateien auf dem Computer des Opfers, aber auch jeder Äußerlichkeit oder gemeinsamen Antrieben verschlüsseln, die an den Computer anschließen. Und die Probeforderung kann sich irgendwo von $ 200 bis zu $ 5,000 erstrecken. CryptoWalls Autoren haben auch ein Partnerprogramm eingeführt, das Verbrechern einen Schnitt des Gewinnes gibt, wenn sie helfen, das Wort über das ransomware über andere strafbare Käufer zu verbreiten.

Der Name des CTB Schließfachs steht für Kurvenberg Bitcoin, weil es ein elliptisches Kurvenverschlüsselungsschema, das Bergnetz für das Präsentieren seines Befehlsservers und seines Bitcoins für Lösegeldzahlungen verwendet. Es hat auch ein Mitgliedsverkaufsprogramm.

TorrentLocker Ernten E-Mail-Adressen von einem Opfer schicken Spam selbst Kunden zu anderen Opfern. Täuschen-es berechnete an einem Punkt, dass TorrentLocker etwa 2,6 Millionen E-Mail-Adressen auf diese Weise zusammengetragen hatte.

Gegen ransomware zu schützen, kann schwierig sein, da Angreifer ihre Programme aktiv ändern, um Antivirusentdeckung zu besiegen. Jedoch, ist eine der besten Methoden, um sich gegen bekanntes ransomware in der Wildnis zu schützen, Antivirusimmer noch? Es könnte nicht möglich sein, Ihr Risiko völlig zu entfernen, ein Opfer von ransomware zu werden, aber Sie können den Schmerz verringern, ein Opfer durch Machen von regelmäßigen Rückstaus Ihrer Daten und Speichern davon auf einem Gerät zu sein, das nicht online ist.

Quelle : read:https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/