Petya-Attacke oder "NotPetya": Erstes Angriffsziel offenbar in der Ukraine

28.06.2017 10:54 Uhr – Martin Holland

vorlesen

Nachdem die aktuelle Cyberangriffswelle zuerst Opfer in der Ukraine und Russland fand, schält sich heraus, dass die Malware wohl von dort in den Rest der Welt schwappte. Ob es wirklich darum ging, viel Lösegeld zu scheffeln, scheint jetzt zweifelhaft.

Die massive Angriffswelle mit einem Verschlüsselungstrojaner, der an den Kryptotrojaner Petya erinnerte, nutzte offenbar eine Software aus der Ukraine. Das haben verschiedene Sicherheitsforscher ermittelt, die geschlossen das Programm MeDoc verdächtigen. Auch die ukrainische Polizei gab bekannt, dass in diese Richtung ermittelt würde. Die Software ist mehreren Sicherheitsforschern zufolge Voraussetzung für eine Zusammenarbeit mit der Regierung der Ukraine, beispielsweise um dort Steuern zu bezahlen. Das würde erklären, warum internationale Großkonzerne von der Attacke auf Windows-Rechner betroffen waren. Die Entwickler von MeDoc haben einer Mitschuld an der Angriffswelle aber widersprochen.

Geld scheffeln oder Chaos stiften?

Während der Verbreitungsweg noch ermittelt wird, weisen Sicherheitsexperten außerdem darauf hin, dass die Malware höchstens ein sehr schlechter Erpressungstrojaner ist. Der Bezahlvorgang ist auffallend kompliziert. Nötig war beispielsweise eine E-Mail-Adresse, die rasch gesperrt wurde. Den Machern der Software ging es offenbar anders als denen hinter der ersten Petya-Welle vergangenes Jahr nicht darum, schnell viel Geld zu machen. Naheliegend wäre dann, dass es eher darum ging, möglichst viel Chaos zu erzeugen. In einer Zusammenfassung zitiert der Sicherheitsforscher Brian Krebs seinen Kollegen Nicholas Weaver mit der Einschätzung, dass es sich wohl um einen "absichtlichen, bösartigen und destruktiven Angriff" handelte oder vielleicht um einen als Erpressungstrojaner getarnten Test. Immerhin haben die Erpresser bisher knapp 8000 Euro an dem Angriff verdient.

Unterdessen hat Kaspersky die Angriffswelle und die verwendete Malware untersucht. Dabei seien genug Unterschiede zu Petya gefunden worden, um zu erklären, dass es sich hierbei nicht um eine Variante des Kryptotrojaners handelt. Deswegen spricht das Unternehmen von "NotPetya" und das haben sich mehrere

In diesem Zusammenhang:

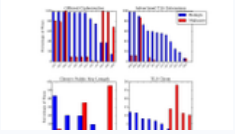
- Allgemeine Tipps gegen Erpressungs-Trojaner
- Backup statt Lösegeld Update: Daten Trojaner-sicher speichern

Dienste

Security Consulter Emailcheck
Netzwerkcheck Browsercheck
Anti-Virus Krypto-Kampagne

Artikel

Cisco analysiert verschlüsselten Traffic, um Malware zu erkennen



Mit Hilfe von Machine Learning gelang es einer Forschergruppe, den verschlüsselten Netzwerk-Verkehr von Malware von regulärem zu unterscheiden – und das, ganz ohne ihn zu entschlüsseln.

Windows-Diagnose: Programme und Prozesse meistern

Wer mehr über das wissen will, was unter der Haube von Windows so vorgeht, kommt weder am Task-Manager noch am Sysinternals-Tool ProcMon vorbei.

Analysiert: Alte Masche, neue Verpackung – Infektion durch PDFs

Manipulierte Word-Dokumente sind bei Kriminellen beliebt, um Computer mit Malware zu infizieren. Dass auch PDF-Dateien ausführbaren Code enthalten können, ist hingegen ein wenig in Vergessenheit geraten. Eine unlängst grassierende Spam-Kampagne ist ein guter Grund, sich diese Gefahr anhand eines frischen Samples in Erinnerung zu rufen.

Sicherheitsforscher inzwischen zu eigen gemacht. Weiterhin scheinen die meisten betroffenen Organisationen ihren Sitz in Russland und der Ukraine zu haben. Wie andere auch, rät Kaspersky dringend dazu, umgehend alle Updates auf Windows-Rechner aufzuspielen. Solange der genaue Verbreitungsweg aber noch nicht ergründet ist, ist aber nicht klar, ob das als Schutzmaßnahme ausreicht. (mho)

Backups vom Fließband: Mit Duplicati in fünf Minuten zum Trojaner-sicheren Backup

Kommentare lesen (18 Beiträge)

Forum bei heise online: **Sicherheit**

Neueste Forenbeiträge

Re: Nimm doch gleich Qubes

speete schrieb am 28.06.2017 12:56: Und warum? Um die Nachteile eines anfälligen OS mit denen einer schlechten Linux-Distro zu vereinen?

Forum: Petya-Attacke oder "NotPetya": Erstes A…

von racor05; 28.06.2017 13:22

Re: Selbst Schuld?

Es wird leider immer schwerer. Um Geld zu sparen, werden z.B. Telefone in Firmen durch Skype ersetzt. Wenn alles funktioniert, ist dies…

Forum: Rückkehr von Petya – Kryptotrojaner leg…

von MAB2003; 28.06.2017 13:20

Re: Warum hacken alle auf MS rum?

Ein Gewohnheitssache. Wie die Malware-Wellen auf MS Windows auch.

Forum: Rückkehr von Petya – Kryptotrojaner leg…

von sys3; 28.06.2017 13:17

Der Kommentar

1 2 3 4 5

Warum Google uns echte Verschlüsselung verweigert

Warum haben wir eigentlich immer noch keine einfach zu nutzende Ende-zu-Ende-Verschlüsselung? Die Standardantwort lautet: Viel zu kompliziert! Doch das ist Unsinn; Apple zeigt längst, wie einfach das sein kann.