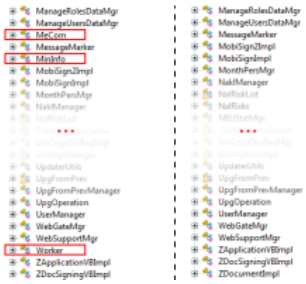
Cyber-Attacke Petya/NotPetya: Neue Einblicke in die perfide Verbreitungsmasche

05.07.2017 10:39 Uhr – Ronald Eikenberg

vorlesen

Durch die Verbreitung ihres Schädlings über die Auto-Update-Funktion einer weit verbreiteten Steuersoftware trafen die Angreifer viele Unternehmen mitten ins Herz. Ein Eset-Bericht liefert neue Details zu diesem spannenden Teil der Geschichte.

Eine Analyse des Antiviren-Herstellers Eset zeigt interessante Hintergründe zu der perfiden Verbreitungsmasche hinter dem Petya/NotPetya-Angriff auf: Bekanntlich missbrauchten die Täter die Steuersoftware MeDoc, die in der Ukraine bei Unternehmen eine große Verbreitung hat. Die Analyse offenbart, dass die Täter modifizierte Versionen des legitimen Moduls „ZvitPublishedObjects.dll“ über die Update-Funktion des Programms verteilten. Sie ergänzten die rund fünf MByte große Bibliothek um Backdoor-Funktionen, durch welche die Täter nicht nur Informationen über das infizierte System, sondern auch Dateien abziehen können. Zudem führt die modifizierte Bibliothek auf Zuruf beliebige Befehle auf dem Rechner des Opfers aus.



Auf der linken Seite befindet sich die trojanisierte Bibiliothek, rechts das Original. Die Angreifer haben die rot markierten Funktionen ergänzt.

Bild: Eset

Hin und her

Der Angriff war offenbar keine Hauruck-Aktion, sondern gut vorbreitet: Die Täter verteilten mindestens drei trojanisierte Versionen der Bibliothek; die erste am 14. April, die zweite am 15. Mai und die dritte schließlich am 22. Juni. Zwischenzeitlich erhielten die MeDoc-Nutzer mehrere Versionen ohne Trojaner-Code – offenbar von den legitimen Entwicklern. Dabei kam es anscheinend zu für die Angreifer unerwarteten Überschneidungen: So erschien nur zwei Tage nach einer trojanisierten Fassung schon wieder eine saubere Kopie der Bibliothek, einen weiteren Tag später versuchten die Täter den Schädling Win32/Filecoder.AESNI.C durch die Backdoor zu verbreiten. Dass diese Malware nur eine geringe Verbreitung erzielte, könnte nach Einschätzung von Eset daran liegen, dass viele Nutzer zu diesem Zeitpunkt mit der sauberen Version der Bibliothek ausgestattet waren. Ein größerer Schlag gelang den Angreifern erst Ende Juni, als sie

Siehe dazu:

Ukrainischer Geheimdienst vermutet Russland hinter Petya/NotPetya-Attacke

Petya/NotPetya: Kein Erpressungstrojaner, sondern ein "Wiper"

Alles, was wir bisher über den Petya/NotPetya-Ausbruch wissen

Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm

Dienste

Security Consulter Emailcheck
Netzwerkcheck Browsercheck
Anti-Virus Krypto-Kampagne

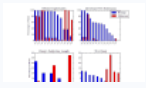
heise devSec

Im Oktober: Die Konferenz für sichere Software- und Webentwicklung

// heise devSec()

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

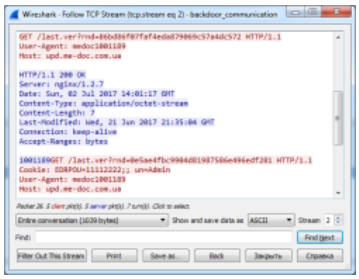
Wer mehr über das wissen will, was unter der Haube von Windows so vorgeht, kommt weder am Task-Manager noch am Sysinternals-Tool ProcMon vorbei.

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.

die Malware DiskCoder.C (auch als ExPetr, PetrWrap, Petya und NotPetya bekannt) über die zu diesem Zeitpunkt abermals verseuchte Steuersoftware verbreiteten.

Angreifer identifizierten Unternehmen

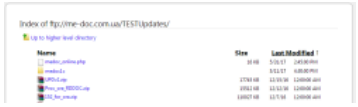


Als Cookie getarnt sendet das trojanisierte Modul die Informationen übers infizierte System an den MeDoc-Server.

Bild: Eset

Offensichtlich ist es den Tätern ein Anliegen, zu erfahren, in welche Unternehmen ihre Backdoor vorgedrungen ist: Die trojanisierte MeDoc-Bibliothek fragt gezielt die EDRPOU-Nummer ab, die vergleichbar mit der Umsatzsteuer-Identifikationsnummer (USt-IdNr.) eingesetzt und einem Unternehmen eindeutig zuzuordnen ist. Mit dieser Information können die Angreifer entscheiden, wie sie nach der Infektion weiter vorgehen – etwa, ob es sich lohnt, gezielt Unternehmensgeheimnisse abzugreifen, ehe der Erpressungs-Trojaner zuschlägt. Neben der EDRPOU-Nummer saugt das Backdoor-Modul dem Bericht zufolge die Mail- und Proxy-Konfiguration aus der MeDoc-Software ab. In beiden Fällen können auch Zugangsdaten darunter sein, weshalb Eset den betroffenen Nutzern dringend rät, die Passwörter für Mail-Accounts und Proxy-Zugänge zu ändern.

Beute als Cookie getarnt



Eset stieß auf dem MeDoc-Server auf eine Webshell, über die welche die Täter möglicherweise Zugriff erlangten.

Bild: Eset

Die ausspionierten Daten sendet das Backdoor-Modul nicht etwa an ein System der Angreifer, sondern an den Server der MeDoc-Entwickler. Im Rahmen der routinemäßigen Nachfrage, ob eine neue Software-Version zum Download bereitsteht, sendet die Bibliothek das Diebesgut als vermeintliches Cookie im HTTP-Request mit.

Offenbar gelang es den Angreifern, die Kontrolle über den offziellen MeDoc-Server zu gewinnen. Der Einstiegspunkt könnte eine PHP-Webshell mit dem Dateinamen medoc_online.php gewesen sein, die Eset auf dem FTP-Server der MeDoc-Entwickler fand. Das Verzeichnis, in dem sich die Datei befand, war über den HTTP-Server öffentlich zugänglich. (rei)

Kommentare lesen (153 Beiträge)

Forum zum Thema: **Viren & Würmer**

https://heise.de/-3763750 Drucken

Mehr zum Thema **Malware** **Ransomware**

Neueste Forenbeiträge

Re: Und wer möchte noch immer sein Leben Riskieren

aleggo schrieb am 05.07.2017 15:16: Dann leg dir schon mal 2-3 zur Seite, denn solche Autos wird es nicht mehr geben. Die Reichen wissen…

Forum: Cyber-Attacke Petya/NotPetya: Neue Ein…

von Moody; 06.07.2017 06:01

Re: Was ist daran denn nun "perfide"?

flack schrieb am 05.07.2017 17:02: "Irgendwie muß man das doch verflixt noch mal hingedreht bekommen, daß der Angegriffene Schuld hat, damit…

Forum: Cyber-Attacke Petya/NotPetya: Neue Ein…

von 7eggert; 06.07.2017 02:31

Re: Erinnert sich noch wer an den Reiserfs-Hype?

Sven Sasse schrieb am 05.07.2017 21:16: Daran wurde ich bei dieser Neuerung in der Tat ebenfalls erinnert. Damals jubelten meine Kollegen, die…

Forum: Aufregung über angebliche Sicherheitslü…

von Systemverwalter; 06.07.2017 02:07

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.