WannaCry nicht überall erfolgreich

Hornetsecurity ATP wehrt globalen Ransomware-Angriff ab der ersten Schadmail ab

Hannover, 15.05.2017 – In über 150 Ländern verursachte WannaCry teils schwere Schäden: Bei der weltweit laufenden Angriffswelle, der unter anderem der englische NHS, der Autobauer Renault, aber auch einige Systeme der Deutschen Bahn zum Opfer fielen, nutzten die Angreifer gleich mehrere Schwachstellen aus. Hornetsecurity Advanced Threat Protection konnte die gefährliche Ransomware-Attacke allerdings von der ersten Schad-E-Mail an erkennen und unterbinden.

WannaCry ist eine Erpressersoftware, die per E-Mail in dem Umlauf kommt und darüber verbreitet wird. Ist sie auf einem lokalen Gerät aktiviert, verschlüsselt sie die dort befindlichen Dateien. Anschließend werden Benutzer dazu aufgefordert, eine Lösegeldzahlung zu leisten, um den Entschlüsselungscode zu erhalten, wovon Sicherheitsexperten jedoch abraten. Im Fall von WannaCry nutzt die Malware einen Exploit aus, der ursprünglich vom amerikanischen Geheimdienst NSA entwickelt wurde und den eine Hackergruppe namens „Shadow Broker“ entdeckte und veröffentlichte.

Das Perfide an WannaCry ist, dass die Schadsoftware eine Schwachstelle in Microsofts „Server Message Block (SMB) Protocol“ ausnutzt, um sich wurmartig weiter zu verbreiten und etliche andere Computersysteme zu infizieren. Auf diese Weise erreichte WannaCry erst den sehr hohen, weltweiten Verbreitungsgrad. WannaCry setzt auf das veraltete Windows XP Betriebssystem, das immer noch häufig anzutreffen ist. Ursprünglich stellte Microsoft als Hersteller keine Sicherheitsupdates mehr für Windows XP bereit, änderte dies jedoch hastig, nachdem WannaCry einen solchen Erfolg aufweisen konnte.

Hornetsecurity Advanced Threat Protection (ATP) hat die neuartig auftretende Ransomware bereits beim ersten Auftreten durch dynamische Pattern Analysen in der Sandbox erkannt und unter Quarantäne gestellt. Weitere Analysen von WannaCry durch die Security-Spezialisten von Hornetsecurity ergaben, dass die Software eine DOUBLEPULSAR Backdoor Variante installiert, mit der sie schadhaften Code einschleust. Anschließend verschlüsselt das Programm die unterschiedlichsten Dateien und versieht diese mit der zusätzlichen Dateiendung ".wncry", also zum Beispiel die Datei *finanzen.xlsx* in *finanzen.xlsx.wncry*. Die Dateien sind für den Benutzer damit unbrauchbar. Gleichzeitig werden Infizierte Hosts Teil eines Botnetzes, das aus dem TOR Netzwerk gesteuert wird.

Hornetsecurity empfiehlt die folgenden Maßnahmen, um sich vor einer Infektion zu schützen: Unternehmen und Personen, die noch das Betriebssystem Windows XP nutzen, sollten unbedingt den von Microsoft bereitgestellten Patch verwenden und das System aktualisieren. Besser noch ist ein Schwenk auf neuere Betriebssysteme mit aktiven Sicherheitsupdates (mindestens MS17-010). Zudem sollten Unternehmen ihre Firewall dahingehend anpassen, um den eingehenden SMB Traffic an Port 445 sowie den ausgehenden

TOR Traffic im Unternehmensnetz zu blockieren. Generell raten die Sicherheitsexperten von Hornetsecurity, E-Mails mit Rechnungen genauestens zu überprüfen und und in solchen E-Mails verlinkte Office-, Skript- oder ausführbare Dateien (portable executable, PE) vor dem Öffnen mindestens mit dem Virusscanner zu überprüfen. Mit dem URL Rewriting und URL Scanning bietet Hornetsecurity ATP einen Service für die tiefgehende Analyse von URLs in E-Mails – als Rundumschutz vor neuartigen Gefahren.

Über Hornetsecurity:
Der führende deutsche Cloud-Security-Provider Hornetsecurity schützt die IT-Infrastruktur, Kommunikation und Daten von Unternehmen und Organisationen jeglicher Größenordnung. Seine Dienste erbringt der Sicherheits-Spezialist aus Hannover über redundante, gesicherte Rechenzentren in Deutschland und nach deutschem Datenschutzrecht. Das Lösungsportfolio beinhaltet Services in den Bereichen Mail Security, Web Security und File Security. Alle Services des Unternehmens sind in kurzer Zeit implementierbar und rund um die Uhr verfügbar. Bis Anfang 2015 firmierte Hornetsecurity unter dem Namen antispameurope. Zu den Kunden von Hornetsecurity zählen unter anderem KONICA MINOLTA, Bitburger Braugruppe, LVM Versicherung, DEKRA, Melitta und Otto Group.

Mehr Informationen finden Sie unter www.hornetsecurity.com.

Pressekontakt:
Hornetsecurity
Christoph Maier
Am Listholze 78
30177 Hannover
Tel.: +49 (511) 260 905-25
Fax: +49 (511) 260 905-99
E-Mail: presse@hornetsecurity.com