News von Proofpoint

Carbanak-Bande plant neue Anschläge

Forscherteam von Proofpoint deckt Vorbereitungen zu Angriffen auf Banken und Finanzinstitutionen auf

Ein Forscherteam von Proofpoint hat entdeckt, dass die berüchtigte Carbanak-Bande wieder aktiv ist und es auf Banken in Europa, dem Mittleren Osten und den USA abgesehen hat. Proofpoint beobachtete Vorbereitungen zu diversen Angriffen und warnt nun davor, dass die Bande wieder einige Milliarden Dollar erbeuten wird, wenn ihr nicht schnell Einhalt geboten wird.

Die Carbanak-Bande attackiert seit 2013 Banken und Finanzinstitutionen

Proofpoint veröffentlichte einen Blogbeitrag und einen Forschungsbericht zu dieser Entdeckung auf der Website. Hier die Zusammenfassung der wichtigsten Ergebnisse aus beiden Berichten:

Die Carbanak-Bande

Die Carbanak-Bande ist bekannt dafür, dass sie Finanzunternehmen infiltriert und Millionen Dollar erbeutet, indem sie die Netzwerke interner Zahlungsprozesse, ATM-Netzwerke und Transaktionen ausspioniert und missbraucht. Im aktuellen Fall wurden Kampagnen im Mittleren Osten, USA und Europa aufgedeckt, die auf die obere Management-Ebene in Finanzunternehmen oder auf finanzielle Entscheider abzielten. Dabei setzten die Kriminellen Spear-Phishing-Mails ein, die URLs, Dokumente mit Makros oder Exploits enthielten. Sie unterstützten die Aktionen mit der Carbanak-spezifischen Malware Spy.Sekur und gewöhnlichen Remote-Acess-Trojanern (RATs) wie jRAT, Netwire und Cybergate.

Eskenzi PR Germany
fon + 49.241.43 53 74 84

Sabine Faltmann
faltmann@eskenzipr.com

Abdruck kostenfrei. Wir freuen uns über ein Belegexemplar!

News von Proofpoint

Neue Anschläge in Vorbereitung

Am 1. März entdeckte Proofpoints Forschungsteam eine E-Mail, die an handverlesene Bankangestellte und Mitarbeiter von Finanzorganisationen, professionellen Dienstleistern sowie Software-Händlern gerichtet war. Die Zielpersonen waren aus der oberen Führungs- und Entscheidungsebene: Direktoren, Führungskräfte, regionale und überregionale Manager und Betriebsleiter. Die meisten Zielpersonen arbeiten im Mittleren Osten in Ländern wie Libanon, Kuweit, Vereinigte Arabische Emirate und Jemen.

Am 4. März entdeckte Proofpoint noch mehr zielgerichtete E-Mails, die an Einzelpersonen und Abteilungen wie Support und Verwaltung aus den Branchen Finanzwesen, Massenmedien und andere, scheinbar zufällige Zielpersonen in Brandschutz, Heizungs-, Lüftungs- und Klimatechnik adressiert waren. Diese Personen arbeiteten in Finanz- und Helpdesk-Positionen als Account Manager, Kreditprüfer und IT-Support. Anders als in der oben beschriebenen Kampagne arbeiten die meisten Zielpersonen in Unternehmen, die ihren Sitz in USA und Europa haben.

Hersteller und Lieferanten als Hintertür

Die Carbanak-Bande steckt seit 2013 hinter einer Reihe von Anschlägen, die meist auf Kampagnen im APT-Modus basieren und unterschiedliche Zielgruppen mit vielfältiger Malware bombardieren. In den beschriebenen Fällen nutzte die Bande neue Exploits, Dokumente mit Makros und Remote-Access-Trojaner, um neue Ziele außerhalb ihrer gewöhnlichen russischen Domains zu attackieren. Sie setzten Kampagnen mit Dateianhängen, URLs, die zu Exploit-Dokumenten verlinken, und raffinierte Malware ein, um Unternehmen in den USA und dem Mittleren Osten zu attackieren. Außerdem dehnte sie ihre Zielgruppe von Finanz-Institutionen zu scheinbar zufälligen Branchen wie Brandschutz, Heizungs-, Lüftungs- und Klimatechnik aus.

Auf jeden Fall zeigte sich durch die Datenschutzverletzungen, dass Hersteller und Lieferanten den Angreifern als Hintertür zu ihrem wirklichen Ziel dienen können.

Weiterführende Links

- Bank robbery in progress: **New attacks from Carbanak group target banks in Middle East and US** https://www.proofpoint.com/uk/threat-insight/post/carbanak-cybercrime-group-targets-executives-of-financial-organizations-in-middle-east
- **Carbanak Group Targets Executives of Financial Organizations in the Middle East** https://www.proofpoint.com/sites/default/files/proofpoint-threat-insight-carbanak-group-en.pdf

465 Worte, 3421 Zeichen

Eskenzi PR Germany
fon + 49.241.43 53 74 84

Sabine Faltmann
faltmann@eskenzipr.com

Abdruck kostenfrei. Wir freuen uns über ein Belegexemplar!