AKTUELLES, BRANCHE - geschrieben von dp am Donnerstag, Juli 4, 2019 22:08 - noch keine Kommentare

APT33: Cyber-kriminelle Gruppe nutzt CVE-2017-11774

Tags: Advanced Practices Team, APT33, CVE-2017-11774, FireEye, Outlook, USA

Bereits seit 2017 bestehende „Outlook"-Sicherheitslücke noch immer virulent

[datensicherheit.de, 04.07.2019] Im Kontext der aktuellen Berichterstattung über die **bereits seit 2017 bestehende „Outlook"-Sicherheitslücke** CVE-2017-11774 kommentiert das „Advanced Practices Teams" von **FireEye**: *„FireEye hat im vergangenen Jahr mehrere iranische Hacker beobachtet und Beweise dafür veröffentlicht, wie sie die ‚Outlook'-Schwachstelle CVE-2017-11774 ausnutzen. FireEye weist die Merkmale in der Warnung des US Cyber Command, eine US-amerikanische Behörde für Internetsicherheit, zu CVE-2017-11774 der Gruppe ‚APT33' zu."*

VERWENDETE TECHNIKEN IM EINKLANG MIT VERHALTEN VON APT33

Die verwendeten Techniken stehen demnach *„im Einklang mit dem Verhalten von ‚APT33', wie es FireEye im veröffentlichten ‚OVERRULED'-Blogpost im Dezember 2018 beschrieben habe – sowie der aktuellen Kampagne von ‚APT33', die **im Juni identifiziert** wurde und eine verstärkte Ausrichtung auf viele in den USA ansässige Institutionen aufweist."*

CVE-2017-11774 VERWIRRT VIELE SICHERHEITSEXPERTEN

Die Ausnutzung von CVE-2017-11774 führe weiterhin zu Verwirrung bei vielen Sicherheitsexperten. Wenn „Outlook" von bösartigen Anwendungen befallen ist, werde häufig davon ausgegangen, dass der betroffene Nutzer Opfer einer Phishing-Attacke wurde – was hier jedoch nicht der Fall sei. *„Das Unternehmen kann **wertvolle Zeit verschwenden**, ohne sich auf die eigentliche Ursache zu konzentrieren."*

APT33 NUTZT „PASSWORD SPRAYING"

Bevor ein Gegner eine Schwachstelle ausnutzen könne, benötige er **gültige Anmeldeinformationen eines Nutzers**. Bei „APT33" würden diese oft durch sogenanntes *„Password Spraying"* erlangt. Dabei versuchten Bedroher Zugriff zu erlangen, indem sie wenige, häufig verwendeten Passwörtern bei einer großen Anzahl von Konten ausprobierten.

OFT FEHLENDE GEEIGNETE ZUGRIFFSKONTROLLEN IN UNTERNEHMEN

Seit mindestens **einem Jahr** nutzten die Gruppen „APT33" und „APT34" diese Technik mit Erfolg – aufgrund der fehlenden geeigneten Zugriffskontrollen in Unternehmen für E-Mails wie Multi-Faktor-Authentisierung und Patches für E-Mail-Anwendungen in Bezug auf CVE-2017-11774.

Weitere Informationen zum Thema:

twitter, 02.07.2019
USCYBERCOM Malware Alert

FIREEYE,21.12.2018
Threat Research / OVERRULED: Containing a Potentially Destructive Adversary

datensicherheit.de, 26.06.2019
Zscaler: Warum Office 365 für Stau im Netzwerk sorgen kann

datensicherheit.de, 19.05.2019]
Account Takeover-Angriffe: Wie Unternehmen ihre Office 365-Konten schützen können

datensicherheit.de, 22.04.2019
Proofpoint: Kommentar zu Sicherheitsvorfällen bei Office 365

datensicherheit.de, 17.04.2019
Office 365: Zunehmendes Risiko von Cloud-Account-Attacken

datensicherheit.de, 15.04.2019
Hackerangriff auf Outlook.com: Schwachstelle Privileged Account

datensicherheit.de, 03.03.2019
FireEye: Zehnter M-Trends Report veröffentlicht

datensicherheit.de, 03.02.2019
Microsoft 365-Nutzer konnten keine Links mehr öffnen

datensicherheit.de, 22.04.2013
FireEye-Studie belegt die zunehmend globale Natur von Cyber-Attacken

Kommentieren

Name - benötigt

Email - benötigt, wird nicht veröffentlicht.

Website

Kommentar

KOMMENTAR ABSCHICKEN

KOOPERATION

TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V.

KOOPERATION

INITIATIVE DIGITAL Inspiration. Knowhow. Kontakte.

MITGLIEDSCHAFT

BISG Bundesfachverband der IT-Sachverständigen und -Gutachter e.V.

MULTIPLIKATOR

Allianz für Cyber-Sicherheit Multiplikator

PARTNER

ZIM Zentrum für innovatives Marketing Berlin Brandenburg

GEFRAGTE THEMEN

Beliebt Neu Kommentare Schlagwörter

AKTUELLES, BRANCHE, GASTBEITRÄGE - Mrz 6, 2020 16:55 - noch keine Kommentare

SCHATTEN-IOT: WIE MAN LICHT INS DUNKEL BRINGT

WEITERE BEITRÄGE IN EXPERTEN

Phishing-Mails: Auch Kleinanleger betroffen
Donnerstag, März 5, 2020 12:17 - noch keine Kommentare

Maschinenidentitäten: Drei Tipps und Tricks zur Erneuerung, Neuausstellung und Widerrufung
Mittwoch, Februar 19, 2020 16:13 - noch keine Kommentare

Industrie 4.0 braucht ganzheitliche IT-Sicherheit im Wertschöpfungsprozess
Montag, Februar 17, 2020 13:10 - noch keine Kommentare

bitkom: Kryptoverwahrer im Visier der Finanzaufsicht
Samstag, Februar 15, 2020 19:26 - noch keine Kommentare

Phishing-Angriffe nehmen Spender ins Visier
Freitag, Februar 14, 2020 19:02 - noch keine Kommentare

Aktuelles Branche Gastbeiträge

AKTUELLES, BRANCHE, PRODUKTE - Mrz 11, 2020 11:20 - noch keine Kommentare

NETWRIX BIETET DATENKLASSIFIZIERUNG FÜR GOOGLE DRIVE

WEITERE BEITRÄGE IN BRANCHE

Schatten-IoT: Wie man Licht ins Dunkel bringt
Freitag, März 6, 2020 16:55 - noch keine Kommentare

Phishing-Mails: Auch Kleinanleger betroffen
Donnerstag, März 5, 2020 12:17 - noch keine Kommentare

Palo Alto Networks warnt vor neuer Phishing-Kampagne
Sonntag, März 1, 2020 21:10 - noch keine Kommentare

BSI: 5 Jahre Sicherheitsupdates für Smartphones
Sonntag, März 1, 2020 21:05 - noch keine Kommentare

Mimecast Threat Intelligence Report – Emotet ist zurück
Donnerstag, Februar 27, 2020 4:41 - noch keine Kommentare

Aktuelles Branche

AKTUELLES, UMFRAGEN - Mrz 6, 2020 19:24 - noch keine Kommentare

CYBERSICHERHEIT: SANS-STUDIE ZU FRAUEN IN FÜHRUNGSPOSITIONEN

WEITERE BEITRÄGE IN SERVICE

SANS Institute: Cloud-Nutzung treibt die Ausgaben für Cybersicherheit
Mittwoch, Februar 19, 2020 22:18 - noch keine Kommentare

Warnung und Trost zugleich: Keine absolute Sicherheit
Mittwoch, Oktober 16, 2019 15:42 - noch keine Kommentare

Nährwertkennzeichnung: Große Mehrheit für Nutri-Score-Ampel
Mittwoch, August 14, 2019 16:05 - noch keine Kommentare

Datenschutz: Mehrheit fühlt sich durch die Gesetze sicher
Mittwoch, Juli 24, 2019 11:14 - noch keine Kommentare

Umfrage der Brabbler AG zum Thema Privatsphäre
Mittwoch, Juli 17, 2019 23:34 - noch keine Kommentare

Aktuelles Branche Umfragen

Datenschutzerklärung

© 2017 datensicherheit.de Informationen zu Datensicherheit und Datenschutz - RSS-Feeds der Einträge und Kommentare.