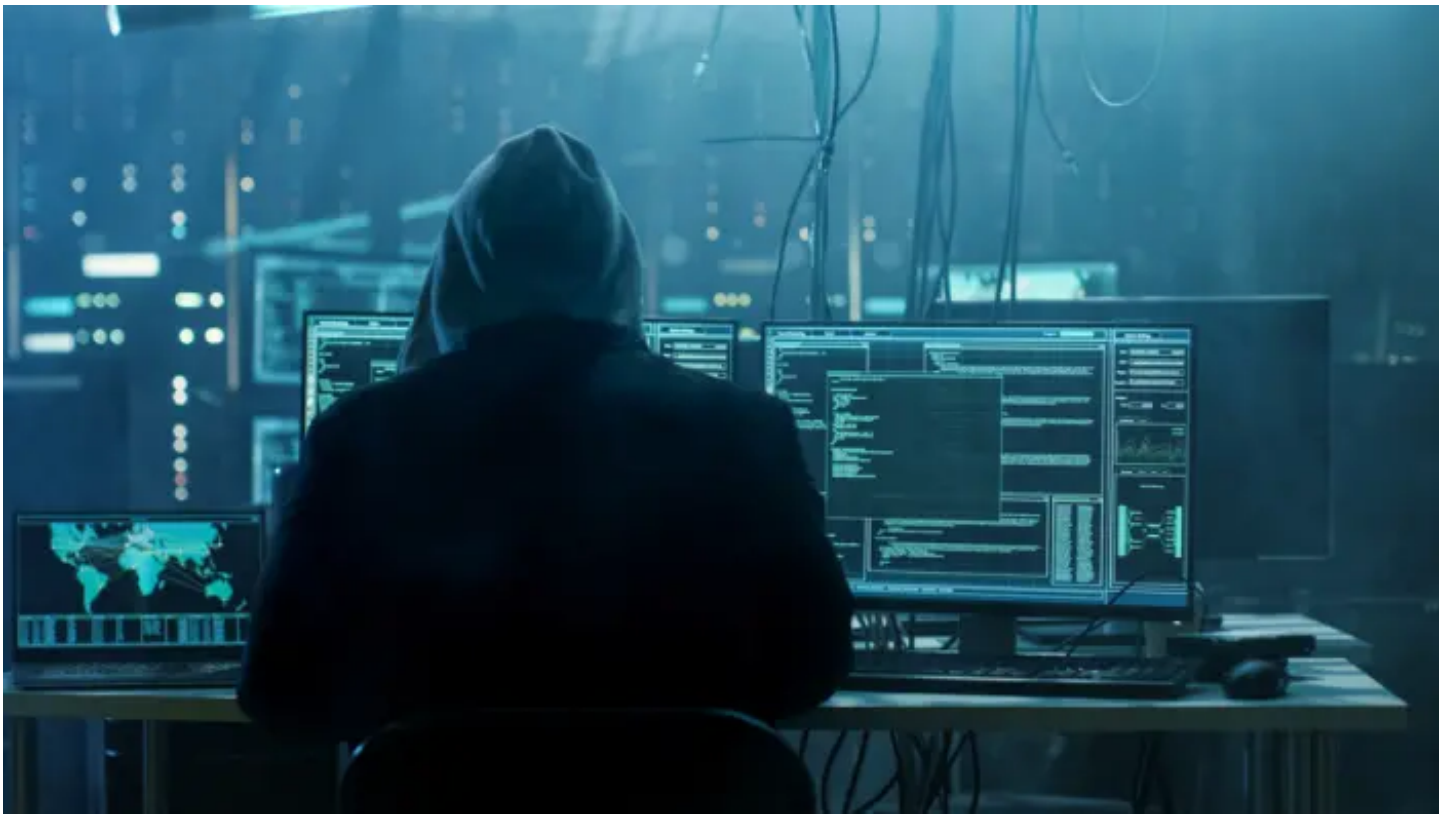
22.03.2019 09:39 Uhr

Vor der Europawahl: Russische Hacker verstärken angeblich Angriffe

Zwei russische Hackergruppen, denen Verbindungen zum Staat nachgesagt werden, haben ihre Angriffe in jüngster Zeit wohl verstärkt. Das hat FireEye beobachtet.

Von **Martin Holland**

92

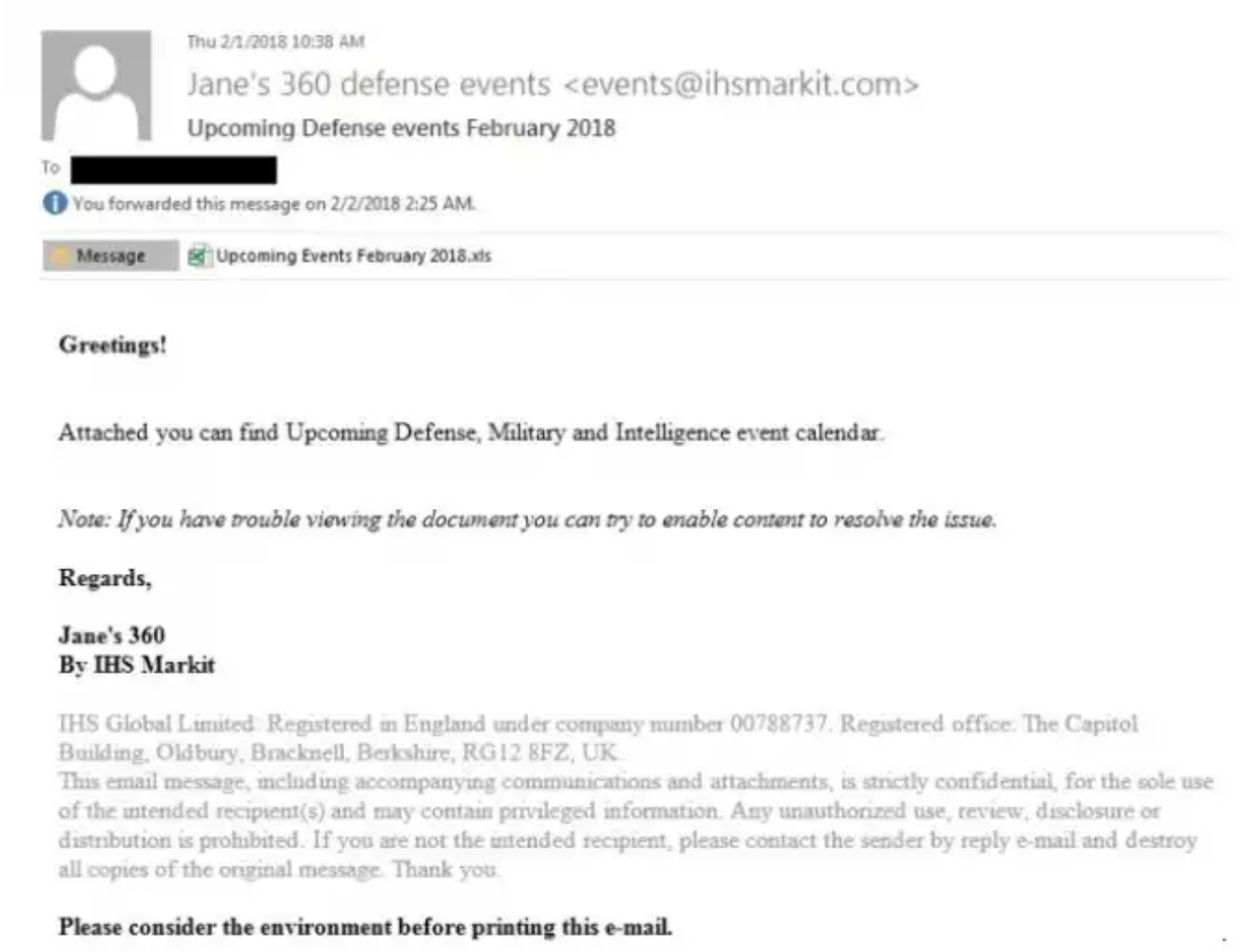


(Bild: Shutterstock)

Sicherheitsforscher haben Hinweise darauf gefunden, dass vom russischen Staat unterstützte Hacker vor der anstehenden Europawahl gezielt europäische Regierungsinstitutionen und Medien in Deutschland sowie Frankreich ins Visier genommen haben. Ihr Ziel sei es demnach, durch Spearphishing an Zugangsdaten für IT-Systeme zu gelangen, um damit dort dann Daten zu sammeln. Die sollten Russland bei politischen Entscheidungen helfen, oder als Leak politischen Parteien oder Kandidaten gezielt schaden, erklärt Mike Hart von FireEye.

Erstes Ziel: Login-Daten

Das beschriebene Vorgehen ist nicht neu, vor den US-Präsidentschaftswahlen 2016 war es in den Blickpunkt der Öffentlichkeit geraten. Kernstück der Taktik sind E-Mails, mit denen Zielpersonen dazu gebracht werden sollen, auf einen schädlichen Link zu klicken oder einen bösartigen Anhang zu öffnen. Die Erfolgschancen dieser Angriffe könnten durch den Rückgriff auf Internetadressen erhöht werden, die eine Ähnlichkeit mit vertrauten Webseiten aufweisen. "So erhielten Ziele in europäischen Regierungsorganisationen Links, die scheinbar zu echten staatlichen Webseiten führen", erklärt FireEye. Die Ziele werden dazu verleitet, Angreifern ihre Login-Daten zu übermitteln.



Thu 2/1/2018 10:38 AM

Jane's 360 defense events <events@ihsmarkit.com>

Upcoming Defense events February 2018

To [redacted]

You forwarded this message on 2/2/2018 2:25 AM.

Message | Upcoming Events February 2018.xls

Greetings!

Attached you can find Upcoming Defense, Military and Intelligence event calendar.

Note: If you have trouble viewing the document you can try to enable content to resolve the issue.

Regards,

Jane's 360
By IHS Markit

Eine Spearphishing-Email von APT28 die bei der rumänischen Botschaft in Moskau einging. (Bild: FireEye)

Hinter den Angriffen stecken demnach zwei verschiedene Gruppen, die unter Sicherheitsforschern als APT28 und Sandworm Team bekannt sind. Beide scheinen zwar die gleichen Ziele zu verfolgen, erklärt FireEye, aber ihre Werkzeuge und Methoden seien unterschiedlich. Das Sandworm Team nutzt demnach vor allem

öffentlich verfügbare Hacking-Tools, während APT28 auf selbst programmierte Software zurückgreift und auch über Zero-Day-Exploits verfügt. FireEye hat die Ziele der Angriffe "nach Möglichkeit" informiert, versichert das Unternehmen.

Keine Unbekannten

APT28 waren schon vorher unter anderem Angriffe auf den Bundestag, die Konrad-Adenauer-Stiftung, die Friedrich-Ebert-Stiftung, die Demokratische Partei im US-Präsidentschaftswahlkampf, die NATO und die Wahlkampagne von Emmanuel Macron angelastet worden. Das Ziel der Hackergruppe ist Analysten zufolge Spionage. Im Unterschied dazu wird dem Sandworm Team auch noch nachgesagt, Sabotageakte durchzuführen. Die Gruppe wird unter anderem verantwortlich gemacht für Hackerangriffe auf Kraftwerke in der Ukraine sowie auf Medienhäuser. Dabei ging es wohl nicht um Ausspähung, sondern die Zerstörung der Infrastruktur. (*mit Material der dpa*) / (mho)

Kommentare lesen (92)

Zur Startseite

MEHR ZUM THEMA

HACKING

TEILE DIESEN BEITRAG

Kurzlink: https://heise.de/-4342383

Abonnieren

Top-News der Redaktion von heise online »

Urheberrechtsreform

EU-Parlament winkt Upload-Filter und Leistungsschutzrecht durch

Mit knapper Mehrheit haben die Abgeordneten die neue Urheberrechtsrichtlinie beschlossen. Alle Warnungen vor Zensur im Netz hab...

1797

Huawei P30 Pro: Vier Kameras mit Nachtsicht im Kurztest

91

Keine Zukunft mit Oracles Cloud: Hunderten Mitarbeitern gekündigt

38

Apple TV+ ist viel heiße Luft

124

---

nach oben

Alle Angebote