10.01.2019 19:01 Uhr

Massen-Doxxing: Täter hat sich wohl schon 2016 verraten

Gegen den Verdächtigen lief bereits seit 2016 ein Verfahren, als Beamte seine Wohnung durchsuchten und Hardware beschlagnahmten.

Von **Fabian A. Scherschel**

329

Avatar des Doxxers auf Twitter: Er hielt sich anscheinend für allmächtig, beging aber grobe Fehler. (Bild: Fabian A. Scherschel)

Der 19-jährige IT-Experte Jan Schürlein hat dem BKA nach eigenen Angaben entscheidende Hinweise auf den Promi-Doxxer 0rbit geliefert, die kurz darauf zu dessen Verhaftung führten. Die Wohnung Schürleins war von Strafverfolgern durchsucht worden, nachdem er öffentlich zu Protokoll gegeben hatte, dass er wisse, wer der Urheber des Datenskandals sei. Wie er jetzt über Twitter bekannt gab, hatte Schürlein das BKA auch auf die Fährte eines anderen Ermittlungsverfahrens gegen 0rbit aus dem Jahr 2016 gebracht.

Damals war der Doxxer demnach unter dem Pseudonym Nullr0uter unterwegs – Verbindungen zwischen beiden Pseudonymen konnte auch heise online in der vergangenen Woche noch feststellen. Durch das alte Verfahren sollte es den Beamten leicht gefallen sein, 0rbit aufzuspüren. Denn 2016 hatte er seine IP-Adresse und damit den Internetanschluss seiner Eltern verraten.

MEHR INFOS

Im Gespräch mit heise online sagte Schürlein, er habe den geständigen Tatverdächtigen über Twitter kennengelernt. Als Teil der Security-Szene rund um YouTube und Gamer-Chatnetzwerke wie Discord fiel ihm das Doxxing und die Account-Übernahmen von 0rbit schon vor Jahren auf. Nach eigenen Angaben hatte er über die Jahre immer wieder Kontakt mit dem Hacker. Schürlein sagt in einer Stellungnahme, er habe seine Informationen über 0rbit nur den Strafverfolgern preisgegeben, weil er keine andere Wahl gehabt habe. Ein Bekannter habe das BKA darauf hingewiesen, dass er mit dem Hacker in Kontakt stehe.

Er habe es nicht riskieren wollen, ins Visier der Ermittler zu geraten, und nachher als Komplize dazustehen. In einem Interview mit *Spiegel Online* spricht Schürlein davon, nun um seinen Ruf zu kämpfen. In der Szene stehe er wie ein Verräter da. Dabei habe er einen Datenklau von dem Ausmaß, wie er nun die Republik erschüttert hat, nie decken können oder wollen.

Der entscheidende Fehler des Promi-Hackers

0rbit verriet sich wohl schon 2016 durch Logins auf gehackte Konten der YouTuber PietSmiet und ApeCrime. Nach Aussage Schürleins funktionierte dabei das zur Anonymisierung genutzte VPN des Hackers nicht richtig und gab seine tatsächliche IP-Adresse preis, die in den Logs der gehackten Konten landete. Nachdem die betroffenen YouTuber Anzeige erstattet hatten, kam es demnach am 6. Oktober 2016 zu einer Hausdurchsuchung bei 0rbit beziehungsweise bei dessen Eltern – der Tatverdächtige lebt laut BKA auch heute noch dort. Die beschlagnahmten Rechner sollen zum Teil verschlüsselt gewesen sein, was dazu führte, dass die Ermittlungen wohl im Sande verliefen beziehungsweise bis vergangene Woche nicht von Erfolg gekrönt waren.

Erst als Schürlein die beiden Untersuchungen für das BKA verknüpfte, sollen die Beamten auf die Fährte des Doxxers gelangt sein, meint der Sicherheitsexperte. Er ist sich sicher, dass seine Aussage maßgeblich zu der schnellen Ergreifung des Tatverdächtigen geführt hat. Bei seinen aktuelleren Hacking-Aktivitäten hat sich 0rbit demnach viel besser geschützt, unter anderem durch die Verwendung des Anonymisierungsnetzwerkes Tor.

Ob Schürleins Aussagen stimmen, lässt sich nur schwer bestätigen. Die Behörden halten sich nach wie vor zum Ablauf der Ermittlungen bedeckt. Seine Angaben scheinen allerdings plausibel und decken sich in einigen Punkten mit unabhängigen Recherchen von heise online.

Ein Armutszeugnis für die Ermittler

Stimmt der von dem unabhängigen IT-Experten dargelegte zeitliche Ablauf und die Details zur ersten Hausdurchsuchung beim Verdächtigen, so werden sich die beteiligten Institutionen fragen lassen müssen, wieso die Ermittlungen 2016 im Sande verlaufen sind und ob ein rigoroseres Vorgehen damals den Datenskandal nicht hätte verhindern können. Angesichts der Kritik, die seit vergangener Woche auf das Bundesamt für Sicherheit in der Informationstechnik (BSI) einprasselt, weil es nach eigenen Aussagen schon im Dezember von 0rbits Twitter-Konto mit den Leaks wusste, sollten sich die Strafverfolgungsbehörden auf einiges gefasst machen.

Falls die Aussagen von Schürlein stimmen, wurde hier seit Mitte 2016 nicht gehandelt. Und dass, obwohl 0rbit in der YouTuber-Szene seit Jahren bekannt war und mehrere Videoproduzenten offensichtlich mit dem Hacker Kontakt hatten. Ob Schürleins Aussagen nun stimmen oder nicht, die ganze Geschichte entblößt eine Doppelmoral beim Umgang mit Angriffen auf Politiker und Promis auf der einen Seite und auf Netz-Subkulturen wie YouTuber auf der anderen. (fab)

Kommentare lesen (329)

Zur Startseite

MEHR ZUM THEMA

DATENKLAU | DATENSCHUTZ | HACKING

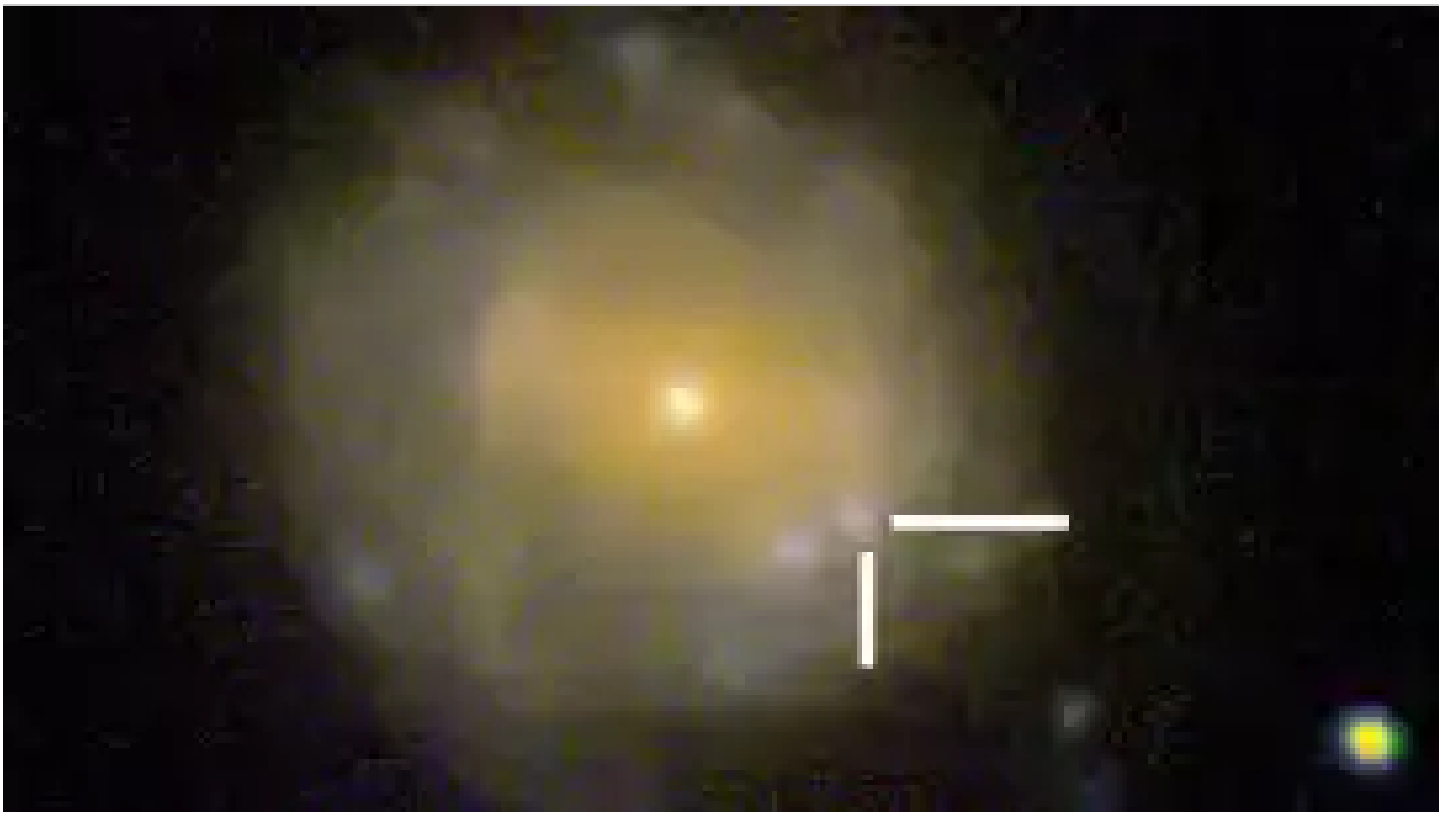
Forum zum Thema: Sicherheit

TEILE DIESEN BEITRAG

Kurzlink: https://heise.de/-4271251

Abonnieren

Top-News der Redaktion von heise online »



Supernova oder Sternentod?

Mysteriöse Explosion verblüfft Astronomen

Rund 200 Millionen Lichtjahre entfernt gab es vergangenen Sommer eine ungewöhnlich helle Explosion. Astronomen nähern sich der ...

Das Fahrrad mit einem Dach und vier Rädern

Auf dieses Headset hat die VR-Welt gewartet

Virtueller Außenspiegel in einem Serienfahrzeug

nach oben

Alle Angebote