

Cyberbit: Spyware aus Israel gegen äthiopische Oppositionelle eingesetzt

Originalartikel

Backup

<html> <p class=„printversionback-to-article printversion-hide“><a href=„<https://www.heise.de/newsticker/meldung/Cyberbit-Spyware-aus-Israel-gegen-aethiopische-Positionelle-eingesetzt-3910109.html>“>zurück zum Artikel</p><figure class=„printversionlogo“><img src=„<https://1.f ix.de/icons/svg/logos/svg/heiseonline.svg>“ alt=„heise online“ width=„180“ height=„40“></figure><figure class=„aufmacherbild“><figcaption class=„akwa-caption“><p class=„source akwa-captionsource“>(Bild: WOCinTech Chat, <a href=„<https://www.flickr.com/photos/wocintechchat/25926572291/>“ target=„_blank“ rel=„external“>wocintech (microsoft) - 14, <a href=„<https://creativecommons.org/licenses/by/2.0/>“ target=„_blank“ rel=„external“>CC BY 2.0)</p> </figcaption></figure><p>Dass autoritative Staaten vermehrt Spyware kaufen, um Dissidenten auszuspionieren, ist kein neues Phänomen. Das kanadische Citizen Lab hat dank besonders schlecht abgesicherter Infrastruktur nun einen weiteren Hersteller solcher Software in Israel gefunden.</p> <p>Aktivisten in Nordamerika und Europa sind das Ziel ausgeklammelter Spyware geworden, die aus Israel stammt und offenbar von Äthiopien gekauft wurde. Zu diesem Schluss kommen die Überwachungs-Analysten des Citizen Lab[1], die von einem Betroffenen auf die Kampagne aufmerksam gemacht wurden. Bei der anschließenden Untersuchung haben sie dann nach eigenen Angaben eine öffentlich zugängliche Log-Datei gefunden, über die sie nicht nur die Zielpersonen sondern auch die Überwacher selbst aufspüren konnten. Demnach stammt die Software von der israelischen Firma Cyberbit, die bei der Auswahl ihrer Kunden damit wohl ebenso wenig zimperlich ist, wie die NSO Group[2], das Hacking Team[3] und die Gamma Group.</p> <p>Wie Citizen Lab zusammenfasst, konnten aufgrund dieser schlecht eingerichteten Infrastruktur Computer in 20 Ländern ermittelt werden, die mit der Spyware infiziert waren. Die Software selbst kommt demnach ohne Exploits aus und heißt PC Surveillance System. Der Hersteller Cyberbit ist eine Tochter von Elbit, jener Firma, die die bewaffneten Drohne Heron TP baut. Über die öffentlich zugängliche Log-Datei seien offenbar aber auch infizierte Laptops von Cyberbit-Mitarbeitern selbst beobachtet worden. Diese hatten ihre Spyware in Thailand, Usbekistan, Sambia, den Philippinen, Vietnam, Kasachstan, Ruanda aber auch europäischen Staaten präsentiert.</p> <h3 class=„subheading“ id=„nav_gefährliches1“>Gefährliches Flash-Update</h3> <p>Immer wieder oft richtete sich die Cyber-Spionage demnach aber wohl einmal mehr gegen Oppositionelle[4] der autoritären Führung Äthiopiens. Die Zielpersonen darunter der Chef eines einflussreichen Medienunternehmens erhielten demnach Mails mit Links zu einem mutmaßlichen Video. Vorher sollten sie aber ein Update von Adobes Flash Players installieren, das über eine ebenfalls verlinkte Seite heruntergeladen werden sollte. In diesem Update war die Spyware für Windows verpackt, die etwa Audio- und Videoaufnahmen anfertigen, die Browser-History und Tastatureingaben abgreifen und Screenshots anfertigen konnte. Infizierte Geräte gab es demnach in Eritrea, Kanada, Deutschland, Australien, den USA und Südafrika. (mho[5])<br class=„clear“></p> <hr/><p>URL dieses Artikels:
<small>

<http://www.heise.de/-3910109>

</small></p> <p>Links in diesem Artikel:
<small>

[1] <https://citizenlab.ca/2017/12/champing-cyberbit-et-hiopian-dissidents-targeted-commercial-spyware/>

</small>
<small>

[2] <https://www.heise.de/meldung/Mexiko-Mit-staatlich-finanzierter-Spyware-gegen-Gesundheitsaktivisten-3623095.html>

</small>
<small>

[3] <https://www.heise.de/meldung/Hacking-Team-Was-ist-schon-Wassenaar-2764292.html>

</small>
<small>

[4] <https://www.heise.de/meldung/33C3-Mit-Zero-Days-gegen-Dissidenten-3583194.html>

</small>
<small>

[5] <mailto:mho@heise.de>

</small>
</p> <p class=„printversion__copyright“>Copyright © 2017 Heise Medien</p> </html>

From:
<https://schnipsl.qgelm.de/> - Qgelm

Permanent link:
<https://schnipsl.qgelm.de/doku.php?id=wallabag:cyberbit -spyware-aus-israel-gegen-thiopische-oppositionelle-eingesetzt>

Last update: 2021/12/06 15:24

