heise online

Subzero: Staatstrojaner-Software laut Microsoft missbräuchlich genutzt

02.08.2022 08:54 Uhr Daniel AJ Sokolov

(Bild: Kurt Bauschardt CC BY-SA 2.0 (Paparazzi Statue nahe Paparazzi Cafe in Pressburg, Slowakei))

Mehrere 0-Day-Exploits soll eine Wiener Firma für Malware genutzt haben, die gegen Anwälte und Banken losging. Die Wiener erkennen "nichts Missbräuchliches".

Microsofts Sicherheitsabteilung stellt die Wiener DSIRF GmbH unter dem Codenamen Knotweed an den Pranger: Das Unternehmen habe Schadsoftware namens Subzero entwickelt, feilgeboten und selbst genutzt, die mehrere 0-day-Lücken (bislang unbekannte Bugs) in Windows und Adobe Reader ausnutzt. Mit Subzero seien seit Februar 2020 mehrere Ziele gehackt und überwacht worden: Anwälte, Banken und Strategieberater in Österreich, Panama und Großbritannien sind bekannte Opfer. DSIRF stellt das nicht in Abrede, verneint aber "missbräuchlichen" Einsatz.

Im Dezember hat netzpolitik.org eine **Werbepräsentation der DSIRF GmbH veröffentlicht [1]**, die im E-Mail-Konto des nach Russland geflüchteten Wirecard-Managers Jan Marsalek gefunden worden sein soll. Darin beschreibt DSIRF die eigenen Geschäftsfelder Biometrie, IT-Beweissicherung, Analyse von Wahlen und Wahlkämpfen, sowie Cyber Warfare. Subzero wird als Waffe für die "nächste Generation der Online-Kriegsführung" beworben.

Gegenüber heise online zeigt sich DSIRF weniger martialisch. Bei Subzero handle es sich um

Software, die "zur behördlichen Anwendung in Staaten der EU entwickelt worden ist. Sie wird gewerblich weder angeboten, verkauft, noch zur Benutzung bereitgestellt." Missbräuchliche Verwendung stellt DSIRF in Abrede, ohne darzulegen, wie so eine IT-Waffe korrekt und legal eingesetzt werden könnte, beispielsweise gegen Anwälte.

So arbeitet Subzero

Laut Microsoft [2] hat DSIRF die Software nicht bloß weitergegeben, sondern auch Command-and-Control-Server für ihren Einsatz betrieben und digitale Zertifikate zur Verfügung gestellt. 2021 hat Subzero einen Bug im Adobe Reader (**CVE-2021-28550 [3]**), in Verbindung mit zwei Windows-Fehlern (CVE-2021-31199 und CVE-2021-31201) ausgenutzt, um sich Rechte auf fremden Windows- und Windows-Server-Rechnern zu verschaffen. Gegen diese Lücken schützen Updates aus dem Mai (Adobe) und Juni 2021 (Microsoft). Im August 2021 folgte ein Update gegen CVE-2021-36948, das ebenfalls von Subzero ausgenutzt wurde.

Im Mai 2022 hat Microsoft schließlich ein manipuliertes PDF-Dokument gefunden, das eine weitere Lücke (wahrscheinlich 0-day) im Adobe Reader als Hebel einsetzt, um eine 0-day-Lücke auf Windows oder Windows Server zur Ausführung von Schadcode auszunutzen. Der Windows-Bug kann inzwischen durch ein Update behoben werden (**CVE-2022-22047 für Windows 7 bis Windows Server 2022 [4]**). Subzero gelingt es demnach, aus der Sandbox des Adobe Reader oder des Chromium-Browsers auszubrechen und eine schädliche Bibliotheksdatei (DLL) auf den lokalen Datenspeicher zu schreiben und später aufzurufen.

Neben PDF-Dateien nutzt Subzero laut Microsoft auch Excel-Dateien mit schädlichen Visual-Basic-Makros, um fremde Systeme zu kapern. Neben verschlüsseltem Schadcode lädt Subzero auch ein präpariertes Bild (JPEG) herunter. Im JPEG ist ein Schlüssel versteckt, mit dem Schadcode entschlüsselt wird. Der Sinn der Sache: Solange Programmcode verschlüsselt ist, kann er von Antiviren-Software nicht untersucht werden. Ein Alarm bleibt aus.

Ein wichtiger Teil des Schadcodes bleibt immer im flüchtigen Arbeitsspeicher, um keine Spuren zu hinterlassen. Legitime Softwarebibliotheken (DLL-Dateien) und Registry-Einträge werden manipuliert, unter anderem um das Auslesen gespeicherter Passwörter zu erleichtern. Die Malware-verbreitenden Server wurden laut Microsoft meist von den Firmen Digital Ocean und Choopa gehostet; die einschlägigen IP-Adressen waren wiederum mit mehreren DSIRF-Domains verbunden.

Geheimdienst ermittelt jetzt

Subzero-Entwickler DSIRF gibt an, eine interne Untersuchung der Betriebsabläufe eingeleitet zu haben. Außerdem will die Wiener Firma, dass Microsoft mit einem von DSIRF bestellten unabhängigen Gutachter zusammenarbeitet, um die "aufgeworfenen Fragen" zu untersuchen.

(Bild: Tatiana Popova/Shutterstock.com)

Seinen Kunden empfiehlt Microsoft, den Patch gegen CVE-2022-22047 schnell einzuspielen, und sicherzustellen, dass Microsoft Defender Antivirus mindestens mit Update 1.371.503.0 versorgt ist. Wer MS Excel hat, soll die Makro-Einstellungen überprüfen. Wenn das Antimalware Scan Interface (AMSI) aktiviert ist, können Macros zusätzlich in Echtzeit überprüft werden. Konten sind bitte durch Multifaktor-Authentifizierung zu schützen, was illegal kopierte Passwörter weitgehend nutzlos macht. Welche bekannten Spuren eine bereits erfolgte Kompromittierung durch Subzero hinterlässt, verrät Microsoft [5] ebenfalls.

Nachdem die europäische Datenschutzorganisation **Epicenter Works eine Sachverhaltsdarstellung [6]** bei der Staatsanwalt eingebracht hat, führt inzwischen auch der österreichische Geheimdienst DSN (Direktion Staatsschutz und Nachrichtendienst) eine Untersuchung. Epicenter Works verweist auf das Strafgesetzbuch, sowie darauf, dass die Ausfuhr der "Cyberwaffe" ohne Genehmigung rechtswidrig wäre. Das österreichische Innenministerium gibt an, die Spyware selbst nicht eingesetzt zu haben.

Russland-Verbindungen

Die Stellungnahme der DSIRF gegenüber heise online ist mit "DSIRF Geschäftsleitung" gezeichnet, ohne Namensnennung. Laut österreichischem Firmenbuch ist Drazen Mokic seit September 2020 alleiniger Geschäftsführer der DSIRF GmbH. Damals ist sein Co-Geschäftsführer Christian Hauer ausgeschieden. Mokic ist zudem Geschäftsführer der Guardian GmbH sowie der DSIRF-Tochter MSL Machine Learning Solutions Gmbh.

An MSL ist auch die B&C Privatstiftung beteiligt. Die milliardenschwere Stiftung hat sich der Förderung des Unternehmertums in Österreich verschrieben. Ihren Sitz haben DSIRF GmbH, Guardian und MSL in einem Gemeinschaftsbüro in Wien. Ironie der Geschichte: Im selben Gebäudekomplex logiert auch die Datenschutzbehörde der Republik.

Haupteinfahrt zum Gebäudekomplex Barichgasse 38-42/Ungargasse 59-61 in Wien III. Hier hat neben DSIRF unter anderem auch die österreichische Datenschutzbehörde ihren Sitz.
(Bild: Daniel AJ Sokolov)

Gegründet wurde die DSIRF GmbH im Jahr 2016. Julian-Thomas Erdödy war bis zum Valentinstag 2020 ihr erster Geschäftsführer, laut Linkedin-Profil sogar bis Ende 2020. (Eine weitere Geschäftsführerin währte nur ein halbes Jahr.) Erdödys Linkedin-Profil erzählt, dass er gleichzeitig (2017-2020) auch "Solutions Architect, Computer Vision" bei einer Moskauer Firma war, die keine offensichtliche Webpräsenz unterhält.

200 Millionen Euro Finanzanlagen

In Erdödys Zeit bei DSIRF fällt ein erstaunlicher Geldregen für das Unternehmen: Bis inklusive 2018 zeigen die Jahresabschlüsse null Euro Finanzanlage und Bilanzsummen von deutlich unter einer Million Euro. 2019 explodieren die Finanzanlagen plötzlich auf 200,5 Millionen Euro, die Bilanzsumme auf über 206 Millionen Euro. Und das bei nur sechs Millionen Euro Verbindlichkeiten, die im Jahr darauf komplett getilgt werden. Woher eine kleine Firma in einem Gemeinschaftsbüro in einem Jahr so viel Geld bekommt, verraten die öffentlichen Jahresabschlüsse nicht.

Heute arbeitet Erdödy offenbar für die Zürcher Holding Zühlke, die laut ihrer Webseite "nachhaltige Lösungen für die Zukunft" durch "Innovationen und technologischen Fortschritt" erarbeitet. Dort, in der Schweiz, saß auch der ursprüngliche Eigentümer der DSIRF GmbH, eine

gewisse DSR Decision Supporting Information Research and Forensic AG. Inzwischen ist das Firmengeflecht komplexer: Die DSIRF GmbH gehört heute der DSR Decision Supporting Information Research Forensic GmbH (DSR) mit Sitz im selben Wiener Gemeinschaftsbüro.

Verschleierte Eigentümer

Auch hier gibt es eine Russlandverbindung: DSR-Geschäftsführer Stefan Gesslbauer war von 2004 bis Ende 2016 in Russland in Managerfunktionen tätig, und zwar für die deutschen Konzerne REWE und MediaSaturn. Zwei Jahre lang war Gesslbauer nach eigenen Angaben auch Vorstandsmitglied der Deutsch-Russischen Auslandshandelskammer AHK.

Die DSIRF-Mutter DSR gehört wiederum der Deep Dive Research Lab AG. Sie unterhält ihren Firmensitz im selben Briefkastenfirmenbüro in Liechtenstein, wie die Guardian AG, Eigentümerin der Guardian GmbH. So bleiben die wahren Eigentumsverhältnisse im Dunkeln.

(**ds [7]**)

URL dieses Artikels:

https://www.heise.de/-7199360

Links in diesem Artikel:

[1] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/

[2] https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

[3] https://www.heise.de/news/Patchday-Attacken-auf-Adobe-Acrobat-und-Reader-6044528.html

[4] https://www.heise.de/news/Microsoft-kuemmert-sich-um-84-Sicherheitsluecken-7177806.html

[5] https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

[6] https://epicenter.works/document/4236

[7] mailto:ds@heise.de