epicenter.works – Plattform Grundrechtspolitik,
Widerhofergasse 8/2/4, 1090 Wien, ZVR: 140062668
office@epicenter.works

An die
Staatsanwaltschaft Wien
Landesgerichtsstraße 11
1080 Wien

Wien, 28.07.2022

Betreff: Strafanzeige gegen die DSIRF GmbH wegen Widerrechtlichem Zugriff auf und Störung der Funktionsfähigkeit von Computersystemen, Missbrauch von Computerprogrammen und betrügerischem Datenverarbeitungsmissbrauch durch Herstellung von Angriffs-software , sowie gegen noch zu ermittelnde Unbekannte Täter bezüglich des Besitzes dieser Software

Sehr geehrte Damen und Herren,

Der Geschäftsführer der Firma DSIRF GmbH mit Sitz in Barichgasse 38/1/5, 1030 Wien, FN 455495x, Herrn Drazen M. sowie Mitarbeiter der Firma stehen im Verdacht mit Ihrer Firmentätigkeit gegen die Bestimmungen

§ 118a StGB Widerrechtlicher Zugriff auf ein Computersystem
§ 126a StGB Datenbeschädigung
§ 126b StGB Störung der Funktionsfähigkeit eines Computersystems
§ 148a StGB Betrügerischer Datenverarbeitungsmissbrauch
§ 278a StGB Kriminelle Organisation
sowie
§ 79 Abs. 1 Z 2 und § 80 Abs. 1 Z 1 Außenwirtschaftsgesetz[1] iVm Anhang I und Anhang IV der Dual Use Güter Verordnung 2021/821[2] in der Fassung der Verordnung 2022/1 [3]
sowie
§ 24 MedienG

verstoßen zu haben. Es ergeht folgende

SACHVERHALTSDARSTELLUNG

Wie aufgrund von Medienberichten[4] und Meldungen der Sicherheitsabteilung von Microsoft[5] öffentlich wurde, hat die in Wien ansässige Firma DSIRF GmbH Produkte für den unrechtmäßigen Zugriff auf fremde Computersysteme erstellt, vermarktet und gegen konkrete Ziele im In- und Ausland zum

1 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20007221
2 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:02021R0821-20220505&qid=1659001385255&from=de
3 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0001&from=DE
4 https://www.intelligenceonline.com/surveillance—interception/2022/04/06/after-finfisher-s-demise-berlin-explores-cyber-tool-options,109766000-art und https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich
5 https://blogs.microsoft.com/on-the-issues/2022/07/27/private-sector-cyberweapons-psoas-knotweed/

Einsatz gebracht. Es besteht weiters der Verdacht, dass diese Software entgegen geltenden Exportkontrollen an ausländische Abnehmer verkauft wurde, ohne dass die für Güter mit doppeltem Verwendungszweck gemäß AußWG notwendige Ausfuhrgenehmigung erteilt wurde.

Die Angriffssoftware „Subzero“ oder „KNOTWEED“ der wiener Firma DSIRF bediente sich laut den oben referenzierten internationalen Medienberichten und der technischen Analyse von Microsoft mehrerer bisher unbekannter Sicherheitslücken (0-day exploits) in Windows und Adobe Produkten. Die Angriffssoftware wurde zum unerlaubten Eindringen, Ausspionieren und potentiell auch Manipulieren fremder Computersysteme eingesetzt. Zu den Opfern der Angriffssoftware gehören Anwaltskanzleien, Banken und Beratungsfirmen in mehreren Ländern, darunter Österreich, Großbritannien und Panama. Die Analyse von Microsoft ergab eine direkte Verbindung der Verwendung der Angriffssoftware Subzero mit der Firma DSIRF (comand-and-control infrastructure, Github Repositories). Laut der Analyse von Microsoft war die Infrastruktur von DSIRF zumindest seit Februar 2020 und mindestens bis zum 27. Juli 2022 in der Infektion fremder Computersysteme beteiligt. [6]

Aufgrund der bisher unbekannten und dadurch weiterhin ungeschützten Sicherheitslücken, derer sich die Angriffssoftware von DSIRF bedient und der bis dato aufrechten Infrastruktur zur Verbreitung und Kontrolle der Angriffssoftware, besteht eine **aufrechte Gefährdung für die Computersysteme Dritter**. Ein **Einschreiten der Behörden** zur Unterbindung und Aufklärung dieser Angriffe ist deshalb aus unserer Sicht zeitnah geboten.

Laut internen Firmenpräsentation von DSIRF aus 2018 ist das Unternehmen in fünf Ländern innerhalb und außerhalb von Europa aktiv und hat ein Netzwerk von über 30 Mitarbeitern und Auftragnehmern. Die eigene Angriffssoftware wird dort als „Next Generation Cyber Warfare“ (Übersetzt: Cyberkriegsführung der nächsten Generation) beworben. Laut Produktbeschreibung ist die volle Kontrolle des Zielrechners, der Zugriff auf alle Daten des Zielsystems, inklusive Passwörter, dem Bildschirminhalt und Standortdaten möglich. Das Ändern von Dateien auf dem Zielsystem wird explizit als Funktion der Angriffssoftware beworben, wodurch ua. § 126a StGB erfüllt sein könnte.[7]

Der Firma DSIRF werden laut Medienberichten Kontakte zum Wirecard Umfeld und dem mit internationalem Haftbefehl gesuchten Ex-Wirecard-Chef Jan Marsalek[8] nachgesagt.[9] Laut parlamentarischer Anfragebeantwortung von Innenminister Karner vom 25. Jänner 2022 besteht keine Geschäftsbeziehung zum Innenministerium mit DSIRF und es wurde keine Aussage über eine etwaige Risikobewertung von DSIRF durch den DSN(ehem. BVT) geäußert[10].

Weiters erstatten wir **Anzeige gegen Unbekannt** im Bezug auf die Abnehmern der Angriffssoftware von DSIRF, welche diese laut Microsoft gegen in- und ausländische Ziele zum Einsatz gebracht haben könnten.

6 https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/
7 https://cdn.netzpolitik.org/wp-upload/2021/12/2018-08-28_DSIRF_Company-Profile-Gov.redacted.pdf
8 https://www.bka.de/DE/IhreSicherheit/Fahndungen/Personen/BekanntePersonen/Jan_Marsalek_wirecard/Sachverhalt.html
9 https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html
10 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_08753/index.shtml

Im Zuge der Recherche wurde auf der Website https://dsirf.eu/ festgestellt, dass das Impressum nicht den Bestimmungen des § 24 MedienG entspricht.[11]

Da es sich hierbei um eine Verwaltungsübertretung handelt, ergeht das Ersuchen, die Anzeige an die zuständige Bezirksverwaltungsbehörde weiter zu leiten.

Die Staatsanwaltschaft wird ersucht, den angeführten Sachverhalt strafrechtlich, insbesondere aufgrund der angeführten Bestimmungen, zu überprüfen.

Um Information über alle relevanten Verfahrensschritte wird ersucht.

Mit freundlichen Grüßen
epicenter.works (ZVR: 140062668)

11 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000719