

DSIRF: Wir enthüllen den Staatstrojaner „Subzero“ aus Österreich

By Andre Meister

Published: 2021-12-17 · Archived: 2026-04-05 22:55:29 UTC

Im August 2018 schickte [Florian Stermann](#), ein „[Geschäftsmann mit besten Kreml-Kontakten](#)“, eine E-Mail an Jan Marsalek, damals noch Vorstand der Skandal-Firma Wirecard, mittlerweile [mit internationalem Haftbefehl gesuchter](#) mutmaßlicher Wirtschaftskrimineller. Stermann sendete Marsalek „wie besprochen die Firmenbeschreibung“ des Unternehmens [DSIRF](#) inklusive Informationen zu ihrem Staatstrojaner-Produkt „Subzero“.

Darüber hatte [zuerst Focus berichtet](#). Wir haben jetzt die Original-Dokumente erhalten und veröffentlichen an dieser Stelle die Firmen-Präsentation als [PDF](#), [Text](#) und [Galerie](#). Aus juristischen Gründen mussten wir einige personenbezogene Daten entfernen.

Laut Firmenbeschreibung wurde DSIRF „[im Juni 2016](#)“ [gegründet](#). Das bezieht sich auf die [DSIRF GmbH](#) in Wien. Diese Firma gehört der [DSR Decision Supporting Information Research Forensic GmbH](#) an der selben Adresse. Die wiederum gehört der [Deep Dive Research Lab AG](#) in Liechtenstein. [Bis vor kurzem](#) gab es [eine weitere Aktiengesellschaft](#) in der Schweiz. Ein Firmengeflecht.

Die Geschichte von DSIRF [beginnt laut Eigenaussage damit](#), „Wahlen und Wahlkampfmethoden“ und „betrügerische Hacking-Operationen“ zu analysieren sowie „ausländische Taktiken der Informationskriegsführung“ zu entlarven. Mit diesen Fähigkeiten warb DSIRF genau zur Präsidentschaftswahl in den USA 2016, als Russland Hacking-Operationen und Einflussnahme auf den US-Wahlkampf vorgeworfen wurde.

In einem nächsten Schritt entwickelte DSIRF „[fortgeschrittene Biometrie](#)“ zur „Gesichts-, Objekt- und Mustererkennung“ für „kommerzielle und öffentliche Sicherheit“. Parallel dazu widmete sich DSIRF der „Cyber-Kriegsführung“.

Cyber-Kriegsführung

Der größte Teil der Firmen-Präsentation dreht sich um das Produkt Subzero, ein „[hochmodernes Computerüberwachungs-Tool](#)“ zur „[Exfiltration sensibler/privater Daten](#)“. Anwendungsfälle sind zum Beispiel [Terrorismus, Kriminalität und Finanzbetrug](#). Ein Staatstrojaner. Auch Deutschland [prüft den Kauf und Einsatz von Subzero](#).

Laut Eigenwerbung kann Subzero über „[mehrere Angriffsvektoren](#)“ heimlich auf dem Zielgerät installiert werden, sowohl mit physischem Zugriff als auch aus der Ferne. Angeblich ermöglicht der Trojaner eine „[unsichtbare Überwachung durch die Verwendung einzigartiger Techniken zur Umgehung von Virenschutzprogrammen](#)“.

Einmal installiert übernimmt Subzero die „volle Kontrolle über den Zielcomputer“ und bietet [„vollständigen Zugriff auf alle Daten und Passwörter“](#), behauptet DSIRF. Die Subzero-Kunden können per Web-Interface [Passwörter extrahieren](#), [Screenshots anfertigen](#), [aktuelle und frühere Standorte anzeigen](#) sowie [„auf Dateien des Zielcomputers zugreifen, sie herunterladen, ändern und hochladen“](#).

DSIRF bewirbt Subzero als [„Cyber-Kriegsführung der nächsten Generation“](#), das Tool wurde [„für das Cyber-Zeitalter entwickelt“](#). Zur Markteinführung 2018 unterstützte der Staatstrojaner jedoch nur Zielgeräte mit Windows. Die Unterstützung für macOS sowie Mobilgeräte mit Android und iOS sei ein [„nächster Schritt“](#).

Auf Anfrage von netzpolitik.org wollte der Geschäftsführer Drazen Mokic nicht sagen, ob Subzero diese Geräte heute unterstützt: „Zu technischen Spezifikationen geben wir keine Auskunft.“

Unter Null

Die Firmen-Präsentation von 2018 spricht von [„einem Netzwerk von über 30 Mitarbeitern und Auftragnehmern“](#) und listet [fünf Mitarbeiter als Leiter im Subzero-Team](#). [Drazen Mokic](#) war damals „Produktmanager und Teamleiter“ für Subzero, er ist heute [Geschäftsführer](#) der DSIRF GmbH.

Mokic folgt auf [Julian-Thomas Erdödy](#), der ehemalige Geschäftsführer hat DSIRF vor einem Jahr verlassen. Der Entwickler [Cem Baykam](#) ist laut Präsentation zuständig für maschinelles Lernen und Künstliche Intelligenz.

Der leitende Ingenieur Kuba G. ist erfahrener Reverse-Engineer, der auf diversen Plattformen damit wirbt, ein Machine-in-the-Middle-Angriffswerkzeug zum Phishing von Zugangsdaten zu entwickeln. Da nicht öffentlich bestätigt ist, dass er für DSIRF arbeitet, dürfen wir seinen Nachnamen nicht nennen. Das gilt auch für den Sicherheitsforscher Saša B., der sein LinkedIn-Profil seit der Gründung von DSIRF nicht aktualisiert hat.

Alle vier Personen haben auf unsere wiederholten Presseanfragen nach ihrer Rolle und Position nicht geantwortet.

Geschäftsführer Drazen Mokic sagt auf Anfrage: „Über die genaue Personalsituation des Unternehmens geben wir keine Auskunft. Generell gilt aber: Die an einem Thema arbeitenden Teams werden jeweils entsprechend des Bedarfs und der Anforderungen konfiguriert, so dass die Zahl der mit einem Projekt befassten Mitarbeiterinnen und Mitarbeiter sich häufig ändert.“

Spuren nach Moskau

In der Präsentation von 2018 nennt DSIRF auch fünf [Referenzen für die Firma und ihre Produkte](#). Die Firma wirbt mit bekannten und vernetzten Personen der internationalen Geschäftswelt, der Focus bezeichnet sie als [ziemlich illustre Gesellschaft](#). Diejenigen, die mit uns gesprochen haben, kennen zwar die Firma DSIRF, aber nicht das Staatstrojaner-Produkt Subzero. Zwei davon wussten nichts von ihrer Nennung, es ist gut möglich, dass auch die anderen beiden nicht informiert waren.

Als Referenz für „Politik und Handel“ nennt DSIRF [Michael Harms](#), Geschäftsführer des Vereins [Ost-Ausschuss der Deutschen Wirtschaft](#). Harms kommentiert gegenüber netzpolitik.org: „Die DSIRF GmbH ist ein Mitgliedsunternehmen im Ost-Ausschuss. Die Nennung des Ost-Ausschusses als Referenz war nicht mit uns abgesprochen. Kontakte zu DSIRF bestehen im üblichen Rahmen einer Mitgliedschaft. Der Ost-Ausschuss selbst nutzt keine Produkte des Unternehmens und kennt das Produkt ‚Subzero‘ nicht.“

DSIRF nennt für den Bereich „Handel“ [Stephan Fanderl](#), damals Vorstandsvorsitzender des Warenhauskonzerns [Galeria Karstadt Kaufhof](#), der mal die Einzelhandelskette, [Walmart nach Russland bringen](#) sollte. Auch Fanderl teilt mit, er „kennt diese Firmen-Präsentation nicht“ und „einer wie auch immer gearteten ‚Referenz‘ hat er nicht zugestimmt“. Es gab zwar „zwischen einem früheren Arbeitgeber und DSIRF einen Kontakt, in dessen Rahmen das Unternehmen mit der Implementierung von Datensicherheit beauftragt wurde“. Fanderl kennt aber keine Einzel-Produkte von DSIRF, auch nicht Subzero.

[Christian Kremer](#) dient DSIRF als Referenz für den Bereich „Produktion“. Er war früher [Präsident von BMW in Russland](#) und zur Zeit der Präsentation stellvertretender Geschäftsführer von [Russian Machines](#). Die US-Regierung hat im Januar 2018 – sieben Monate vor der Nennung von DSIRF – [Sanktionen gegen Russian Machines verhängt](#). [Laut LinkedIn](#) ist er dort seit März 2019 nicht mehr. Christian Kremer hat auf unsere Anfrage nicht geantwortet.

Für den Bereich „Recht“ nennt DSIRF eine weitere Person aus Moskau: [Florian Schneider](#), Partner bei der großen [Wirtschaftskanzlei Dentons](#). Auch Schneider hat auf unsere wiederholten Anfragen nicht geantwortet. Die Referenz zum Bereich „Bankwesen“ wird nicht namentlich genannt, laut Präsentation gibt es einen Geheimhaltungsvertrag.

Alle namentlich genannten Referenzen haben gute Verbindungen nach Russland, laut Focus führen [alle Spuren nach Moskau](#).

Meistgesuchter Mann der Welt

Mittlerweile gibt es eine ganze Reihe an Firmen, die Staatstrojaner anbieten. Mit dem Branchenprimus [NSO Group](#) aus Israel [mit 700 Angestellten](#) und Firmen wie [FinFisher](#) aus Deutschland kann DSIRF mit Subzero noch nicht mithalten.

Doch mindestens die deutsche Hacker-Behörde ZITiS [prüft den Kauf und Einsatz von Subzero](#) durch Polizei und Geheimdienste.

Ob DSIRF Subzero überhaupt schon verkauft hat, konnten wir nicht in Erfahrung bringen. Geschäftsführer Drazen Mokic sagt auf Anfrage: „Bis zum heutigen Tage wurde Subzero weder operativ noch kommerziell eingesetzt.“

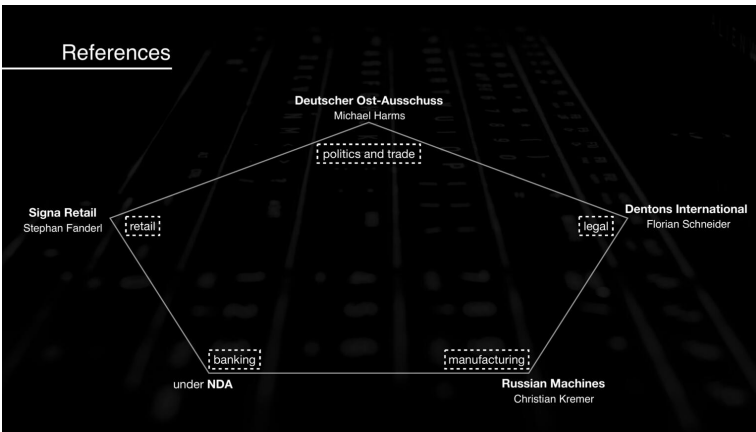
Vermarktet wird der Staatstrojaner trotzdem. Dass der ehemalige Wirecard-Manager Jan Marsalek dabei mitmischt, ist nur auf den ersten Blick seltsam. Schon 2013 [hat Marsalek offenbar versucht](#), den Staatstrojaner der italienischen Firma [Hacking Team](#) an den Karibikstaat Grenada zu verkaufen. Das berichteten [Spiegel](#) und [Motherboard](#) mit Bezug auf [E-Mails von Hacking Team bei WikiLeaks](#).

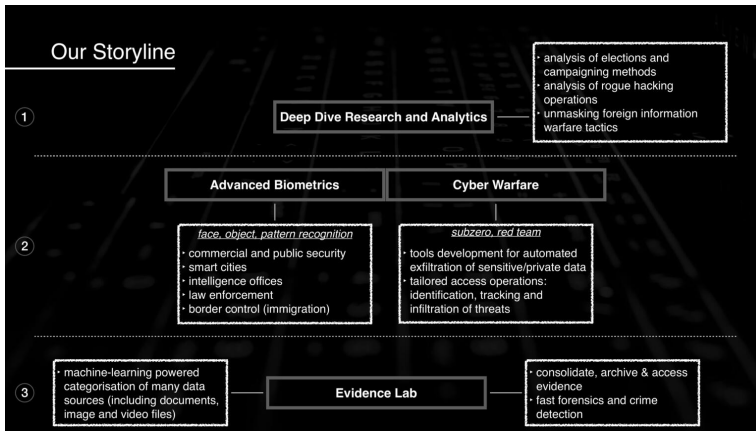
Leider können wir Jan Marsalek nicht zu seiner Rolle befragen. Der mutmaßliche Wirtschaftskriminelle ist [der meistgesuchte Mann der Welt](#), nach ihm wird [mit internationalem Haftbefehl gefahndet](#). Laut [Bellingcat](#) und [Handelsblatt](#) versteckt er sich in Moskau.

Hier die Slides aus [dem PDF](#) befreit:



Cover: DSIRF





The Rationale

Evidence is becoming primarily digital.

Technical obstacles make it increasingly difficult for governments and law enforcement agencies to de-anonymise and access data from suspects.

Encrypted channels allow criminals to exchange information and hide from law enforcement surveillance.



Perfected Investigations

Rapid Forensic Analysis

100 hours of accessible CCTV footage can be analysed for faces of criminals in just 10 hours by our algorithms

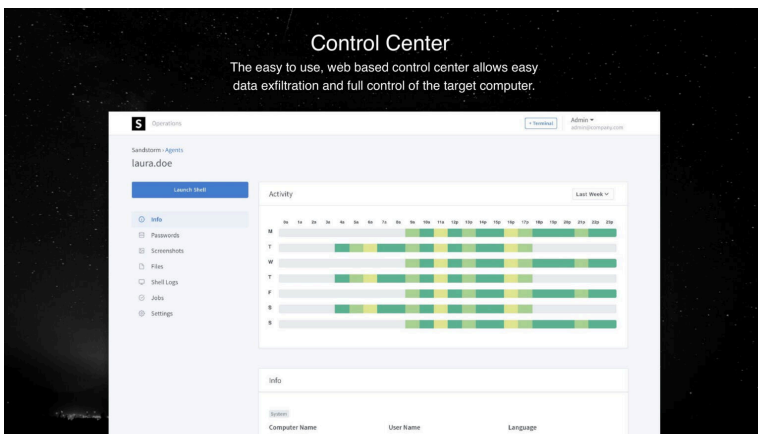
Offline to Online

images of terrorists or of any person of interest can be checked against social networks, blogs and other digital sources and databases

Predictive Policing

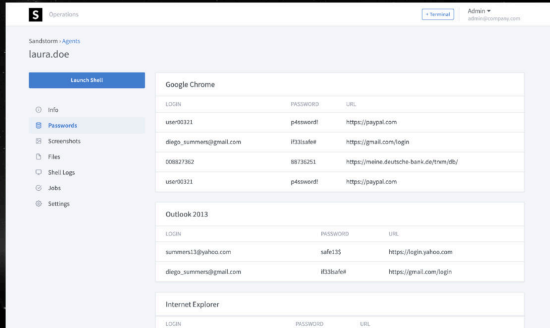
learning from criminal activities in the past, our algorithms derive risky areas and predict strategies of outlaws to make police work more effective

real-world demonstration video: <https://bit.ly/2MzpV2I>



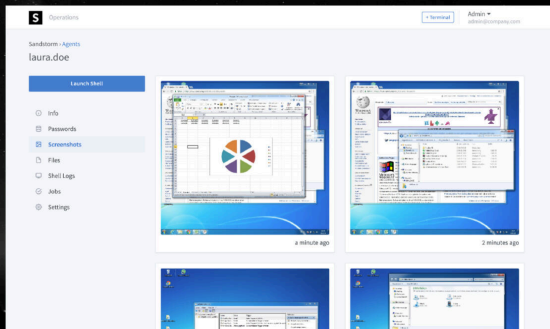
Passwords

Extract credentials from the target PC with a single click.



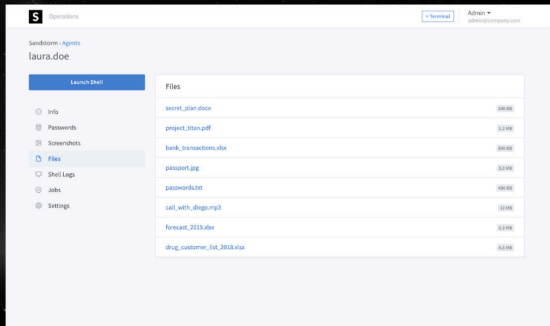
Screenshots

Easily take screenshots from the target PC for intelligence and evidence collection.



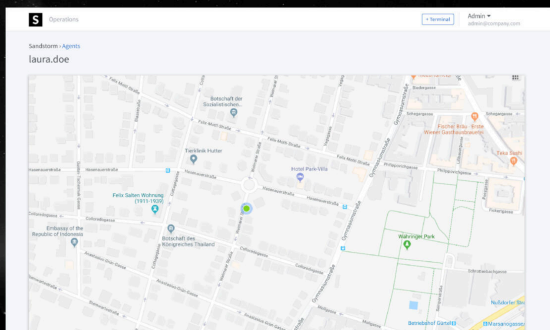
Files

Allows you to access, download, modify and upload files from the target computer.



Location Tracking

View the current and past geo-location of your target. Worldwide.

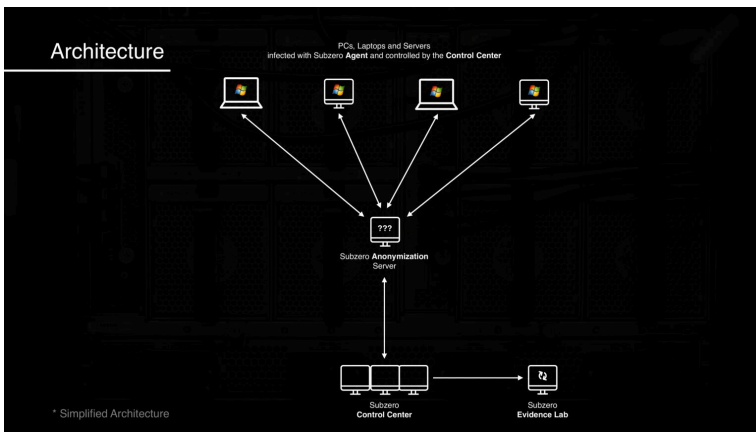


Evidence Lab

Next Big Feature

A dedicated place to securely store, organise and search collected evidence using state-of-the-art AI technology.

- Secure**
Evidence is stored encrypted. Permissions can be easily applied to restrict who can see what.
- Smart**
Using cutting edge technologies like machine learning, large amounts of data can be quickly searched and automatically categorised.
- Advanced**
An advanced biometric recognition feature which allows to quickly search and categorise image and video files looking for objects, faces or patterns.



Mit Folien wie dieser wirbt DSIRF für seinen Staatstrojaner „Subzero“.

Use Cases

- ANTI TERRORISM
- FINANCIAL FRAUD
- CYBER CRIME
- HUMAN TRAFFICKING & CHILD PORNOGRAPHY RINGS
- DARKNET CRIMES



Leadership

Our leadership works with contracted specialists around the globe. Our intellectual property remains exclusively in our hands.

JULIAN ERDOEDY
Managing Director

DRAZEN MOKIC
Product Manager & Team Lead

SASA B [redacted]
Cyber Security Expert & Security Researcher

KUBA G [redacted]
Lead Engineer & Security Researcher

CEM BAYKAM
Machine Learning & AI Lead Engineer

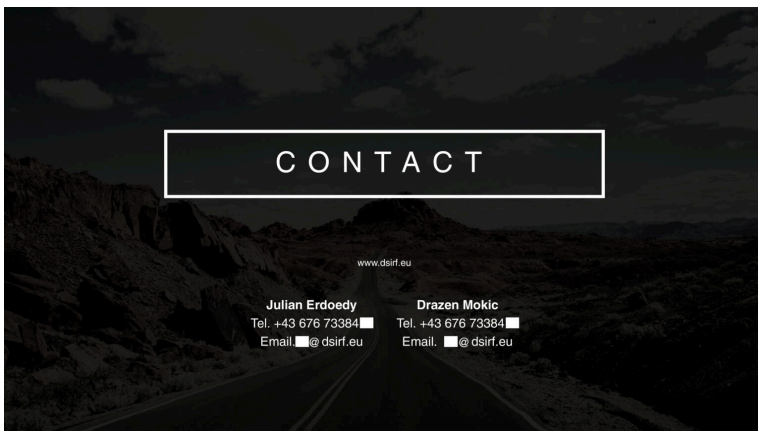


Next Steps


Ready-to-Ship
Market introduction supporting Windows OS & Windows Server.


macOS
Add support for the macOS operating system.


Mobile Devices
Add support for Android and iOS mobile devices.



Source: <https://netzpolitik.org/2021/dsif-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/>