DSIRFWe unveil the “Subzero” state trojan from Austria

netzpolitik-org.translate.goog/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich

17. Dezember 2021

In August 2018 sent Florian Stermann , a "businessman with best Kremlin contacts" , an e-mail to Jan Marsalek, then still board the scandal company Wirecard, meanwhile, sought an international arrest warrant alleged economic criminal. Stermann sent Marsalek "as discussed the company description " of the DSIRF company, including information on their state Trojan product "Subzero".

In was first Focus reported . We have now received the original documents and are now publishing the company presentation as PDF , text and gallery . For legal reasons we had to remove some personal data.

According to the company description, DSIRF was founded "in June 2016" . This refers to the DSIRF GmbH in Vienna. This company belongs to DSR Decision Supporting Information Research Forensic GmbH at the same address. This in turn belongs to the Deep Dive Research Lab AG in Liechtenstein. Until recently there was another joint stock company in Switzerland. A company network.

According to its own statements , the story of DSIRF begins with analyzing “elections and election campaigning methods ” and “fraudulent hacking operations” as well as exposing “foreign information warfare tactics”. DSIRF used these skills to advertise the US presidential election in 2016, when Russia was accused of hacking operations and influencing the US election campaign.

In a next step, DSIRF developed “advanced biometrics” for “face, object and pattern recognition” for “commercial and public security”. At the same time, DSIRF devoted itself to “cyber warfare”.

Cyber warfare

The largest part of the company presentation revolves around the product Subzero, a “state-of-the-art computer monitoring tool” for “exfiltration of sensitive / private data” . Use cases are for example terrorism, crime and financial fraud . A state Trojan. Germany is also looking into buying and using Subzero .

According to self-promotion, Subzero can be stealthily installed on the target device via "multiple attack vectors " , both with physical access and remotely. Allegedly, the Trojan enables "invisible surveillance through the use of unique anti-virus bypassing techniques" .

Once installed, Subzero takes "full control of the target computer" and offers "full access to all data and passwords," claims DSIRF. The Subzero customers can via a Web interface to extract passwords , screenshots make , view current and past locations and "access files on the target computer, download them, edit and upload" .

DSIRF promotes Subzero as "next generation cyber warfare" , the tool was "developed for the cyber age" . However, when it was launched in 2018, the state trojan only supported target devices with Windows. Support for macOS as well as mobile devices with Android and iOS is a "next step" .

When asked by netzpolitik.org, the managing director Drazen Mokic did not want to say whether Subzero supports these devices today: "We do not provide any information on technical specifications."

Under zero

The company presentation from 2018 speaks of "a network of over 30 employees and contractors" and lists five employees as leaders in the Subzero team . Drazen Mokic was "Product Manager and Team Leader" for Subzero at the time, and is now the managing director of DSIRF GmbH.

Mokic succeeds Julian-Thomas Erdödy , the former managing director left DSIRF a year ago. According to the presentation, the developer Cem Baykam is responsible for machine learning and artificial intelligence.

The lead engineer Kuba G. is an experienced reverse engineer who advertises on various platforms to develop a machine-in-the-middle attack tool for phishing access data. Since it has not been publicly confirmed that he works for DSIRF, we are not allowed to give his last name. This also applies to security researcher Saša B., who has not updated his LinkedIn profile since DSIRF was founded.

None of the four people responded to our repeated questions about their roles and positions.

When asked, Managing Director Drazen Mokic said: “We do not provide any information about the company's precise personnel situation. In general, however, the following applies: The teams working on a topic are configured according to needs and requirements, so that the number of employees involved in a project changes frequently. "

Traces to Moscow

In the 2018 presentation, DSIRF also named five references for the company and its products . The company advertises with well-known and networked people from the international business world, the Focus describes it as a fairly illustrious company . Those who spoke to us know the company DSIRF, but not the state trojan product Subzero. Two of them did not know that they were named, it is quite possible that the other two were also not informed.

As a reference for "politics and trade", DSIRF names Michael Harms , managing director of the Association for the East Committee of German Business . Harms comments to netzpolitik.org: “DSIRF GmbH is a member company in the Eastern Committee. The naming of the Eastern Committee as a reference was not discussed with us. Contacts to DSIRF exist within the usual framework of membership. The Eastern Committee itself does not use any of the company's products and does not know the product 'Subzero'. "

DSIRF names for the area “retail” is the name of Stephan Fanderl , at that time chairman of the board of directors of the department store group Galeria Karstadt Kaufhof , who was supposed to bring Wal-Mart to Russia . Fanderl also states that he “does not know this company presentation” and “he did not agree to any kind of 'reference'”. There was “a contact between a previous employer and DSIRF, in the context of which the company was commissioned with the implementation of data security.” Fanderl does not know any individual products from DSIRF, not even Subzero.

Christian Kremer serves DSIRF as a reference for the "Production" area. He was formerly President of BMW in Russia and, at the time of the presentation, Deputy General Manager of Russian Machines . The US government imposed sanctions on Russian Machines in January 2018 - seven months before DSIRF was named . According to LinkedIn , he has not been there since March 2019. Christian Kremer did not respond to our request.

DSIRF names another person from Moscow for the area of "law": Florian Schneider , partner at the large business law firm Dentons . Schneider did not respond to our repeated inquiries either. The reference to the "banking" area is not named, according to the presentation there is a confidentiality agreement.

All references mentioned by name have good connections to Russia, according to Focus all traces lead to Moscow .

Most wanted man in the world

There are now a number of companies that offer state Trojans. With the industry leader NSO Group from Israel with 700 employees and companies like FinFisher from Germany, DSIRF cannot keep up with Subzero.

But at least the German hacker authority ZITiS is examining the purchase and use of Subzero by the police and secret services.

We couldn't find out whether DSIRF had already sold Subzero at all. When asked, Managing Director Drazen Mokic said: "To this day, Subzero has not been used either operationally or commercially."

The state Trojan is still being marketed. That the former Wirecard manager Jan Marsalek is involved is only strange at first glance. As early as 2013 Marsalek apparently tried to sell the state Trojan from the Italian company Hacking Team to the Caribbean state of Grenada. This is what Spiegel and Motherboard reported with reference to emails from the Hacking Team at WikiLeaks .

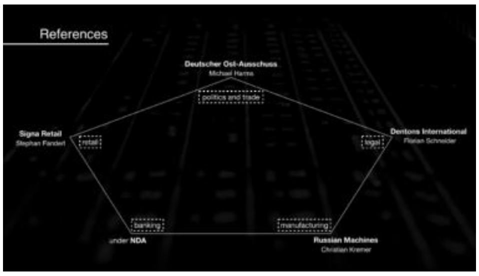
Unfortunately we cannot ask Jan Marsalek about his role. The alleged white-collar criminal is the most wanted man in the world and is being searched for with an international arrest warrant . According to Bellingcat and Handelsblatt , he is hiding in Moscow.

Here are the slides freed from the PDF :

DSIRF

About Us

- established in June, 2016
- spanning a network of over 30 employees and contractors
- operating in 5 countries in and around Europe
- dedicated to deeptech and security



References

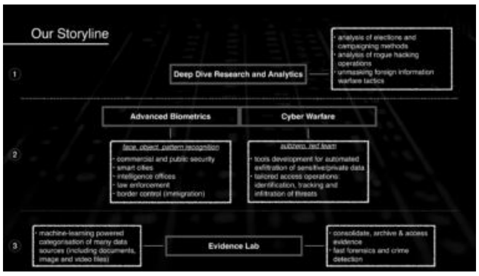
Deutscher Ost-Ausschuss
Michael Harms
politics and trade

Dentons International
Florian Schneider
legal

Russian Machines
Christian Kremer
manufacturing

under **NDA**
banking

Signa Retail
Stephan Fandert
retail



Our Storyline

1 **Deep Dive Research and Analytics**
- analysis of elections and campaigning methods
- analysis of rogue hacking operations
- unmasking foreign information warfare tactics

2 **Advanced Biometrics**

face, object, pattern recognition
- commercial and public security
- smart cities
- intelligence offices
- law enforcement
- border control (immigration)

Cyber Warfare

subzero, red team
- tools development for automated exfiltration of sensitive/private data
- tailored access operations: identification, tracking and infiltration of threats

3 **Evidence Lab**
- machine-learning powered categorisation of many data sources (including documents, image and video files)
- consolidate, archive & access evidence
- fast forensics and crime detection

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.

Advanced Biometrics

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

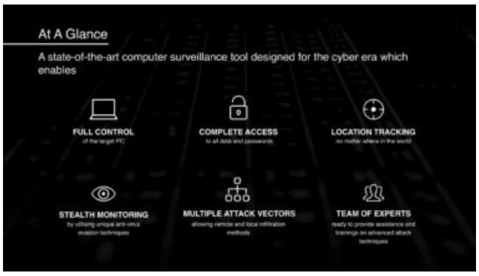
learning from criminal activities in the past, our algorithms derive risky areas and predict strategies of outlaws to make police work more effective

real-world demonstration video: https://bit.ly/2MzpV2T

SUBZERO

NEXT GENERATION CYBER WARFARE

DSIRF



At A Glance

A state-of-the-art computer surveillance tool designed for the cyber era which enables

FULL CONTROL
of the target PC

COMPLETE ACCESS
to all data and passwords

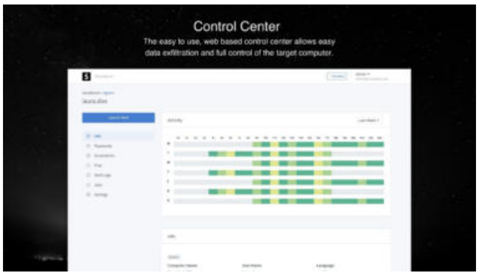
LOCATION TRACKING
no matter where in the world

STEALTH MONITORING
by utilising unique anti-virus evasion techniques

MULTIPLE ATTACK VECTORS
allowing remote and local infiltration methods

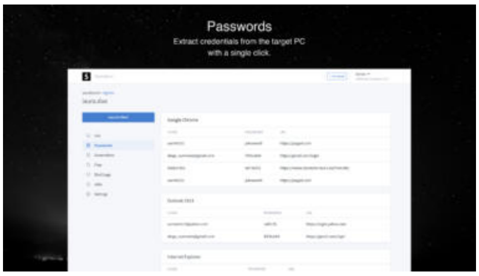
TEAM OF EXPERTS
ready to provide assistance and trainings on advanced attack techniques

THE PRODUCT



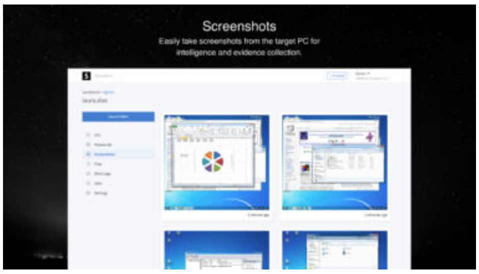
Control Center

The easy to use, web based control center allows easy data exfiltration and full control of the target computer.



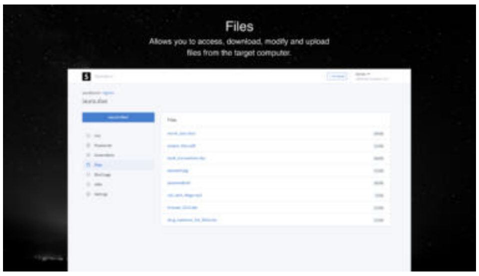
Passwords

Extract credentials from the target PC with a single click.



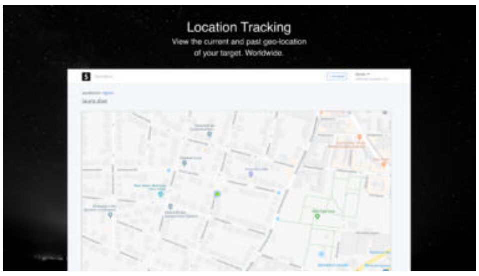
Screenshots

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



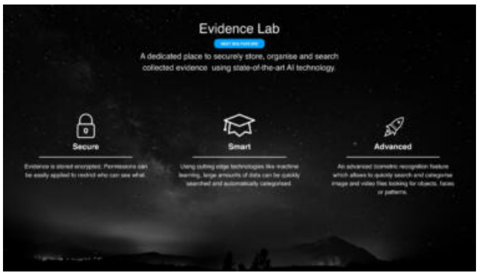
Files

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

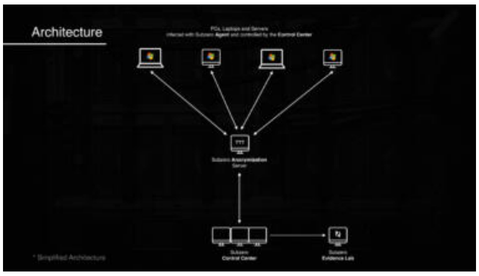
Evidence is stored encrypted. Permissions can be easily applied to restrict who can see what.

Smart

Using cutting edge technologies like machine learning, large amounts of data can be quickly searched and automatically categorised.

Advanced

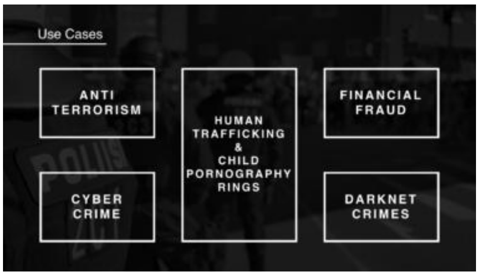
An advanced biometric recognition feature which allows to quickly search and categorise image and video files looking for objects, faces or patterns.



Architecture

PCs, Laptops and Servers
infected with Subzero **Agent** and controlled by the **Control Center**
Subzero **Anonymization** Server
Subzero **Control Center**
Subzero **Evidence Lab**

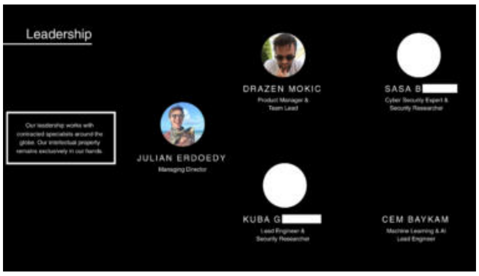
* Simplified Architecture



Use Cases

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

THE TEAM



Leadership

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

JULIAN ERDOEDY
Managing Director

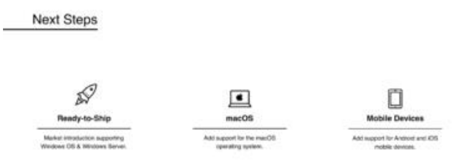
DRAZEN MOKIC
Product Manager &
Team Lead

SASA B[redacted]
Cyber Security Expert &
Security Researcher

KUBA G[redacted]
Lead Engineer &
Security Researcher

CEM BAYKAM
Machine Learning & AI
Lead Engineer

NEXT STEPS



Next Steps

Ready-to-Ship

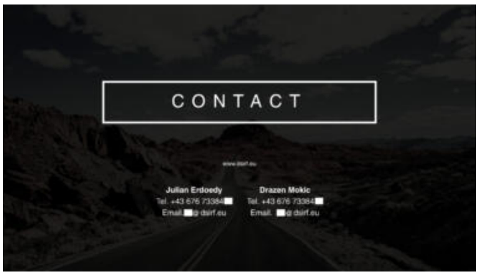
Market introduction supporting Windows OS & Windows Server.

macOS

Add support for the macOS operating system.

Mobile Devices

Add support for Android and iOS mobile devices.



CONTACT

www.dsirf.eu

Julian Erdoedy
Tel. +43 676 73384[redacted]
Email [redacted]@ dsirf.eu

Drazen Mokic
Tel. +43 676 73384[redacted]
Email. [redacted]@ dsirf.eu