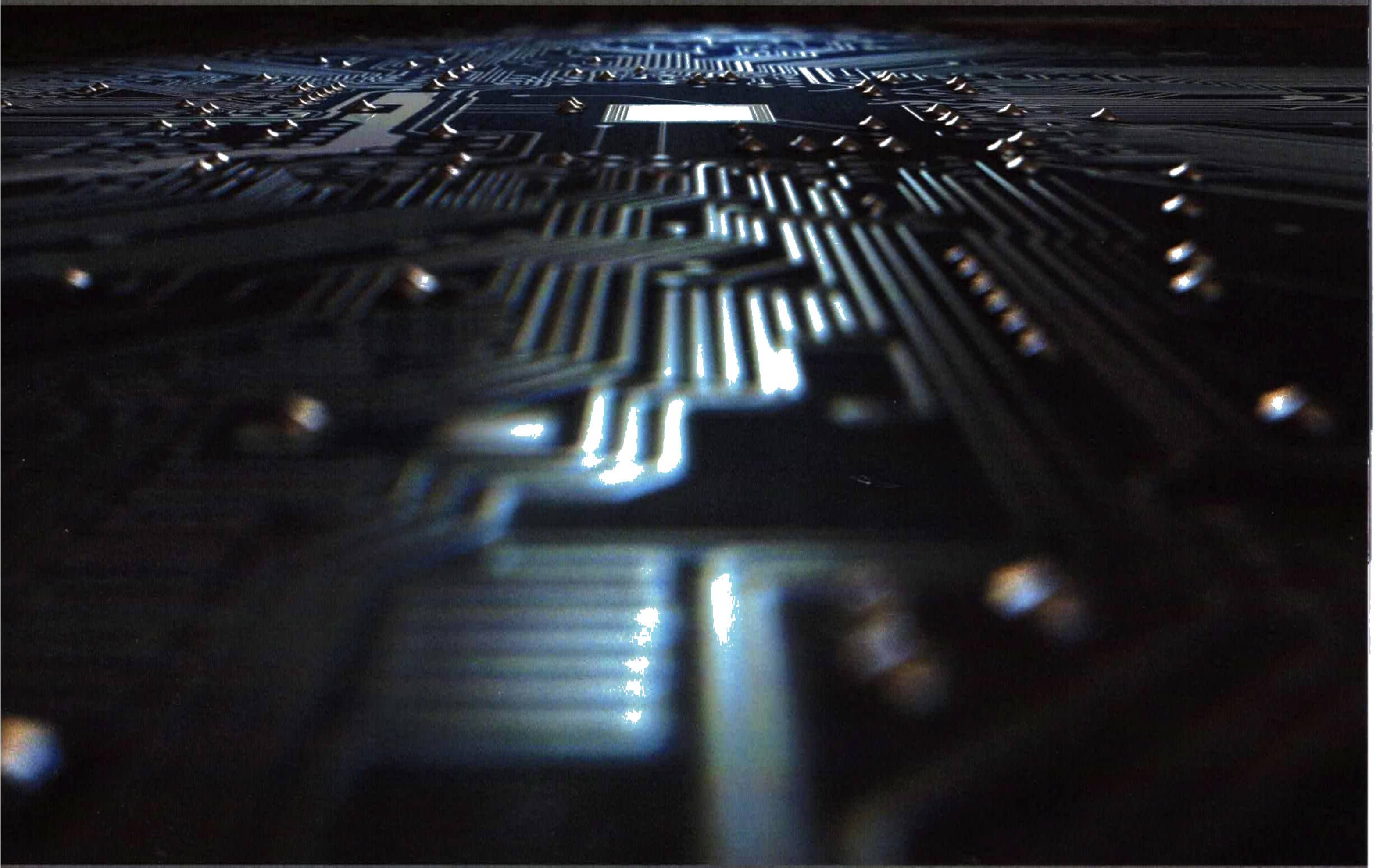
CYBER SOLUTIONS FOR THE FIGHT AGAINST CRIME

Founded in 2008 in Munich, Germany, we partner exclusively with Law Enforcement and Intelligence Agencies, being your reliable partner and trusted advisor to effectively prevent and investigate terror and crime. The company is privately owned with worldwide presence and proven track record serving top clients in the Law Enforcement and Investigation arena.



Our solutions and know-how can be applied to different operational scenarios as individual modules or as a full offensive cyber security portfolio. Along the way, the end user will be provided with excellent support and maintenance services.

TACTICAL GATHERING

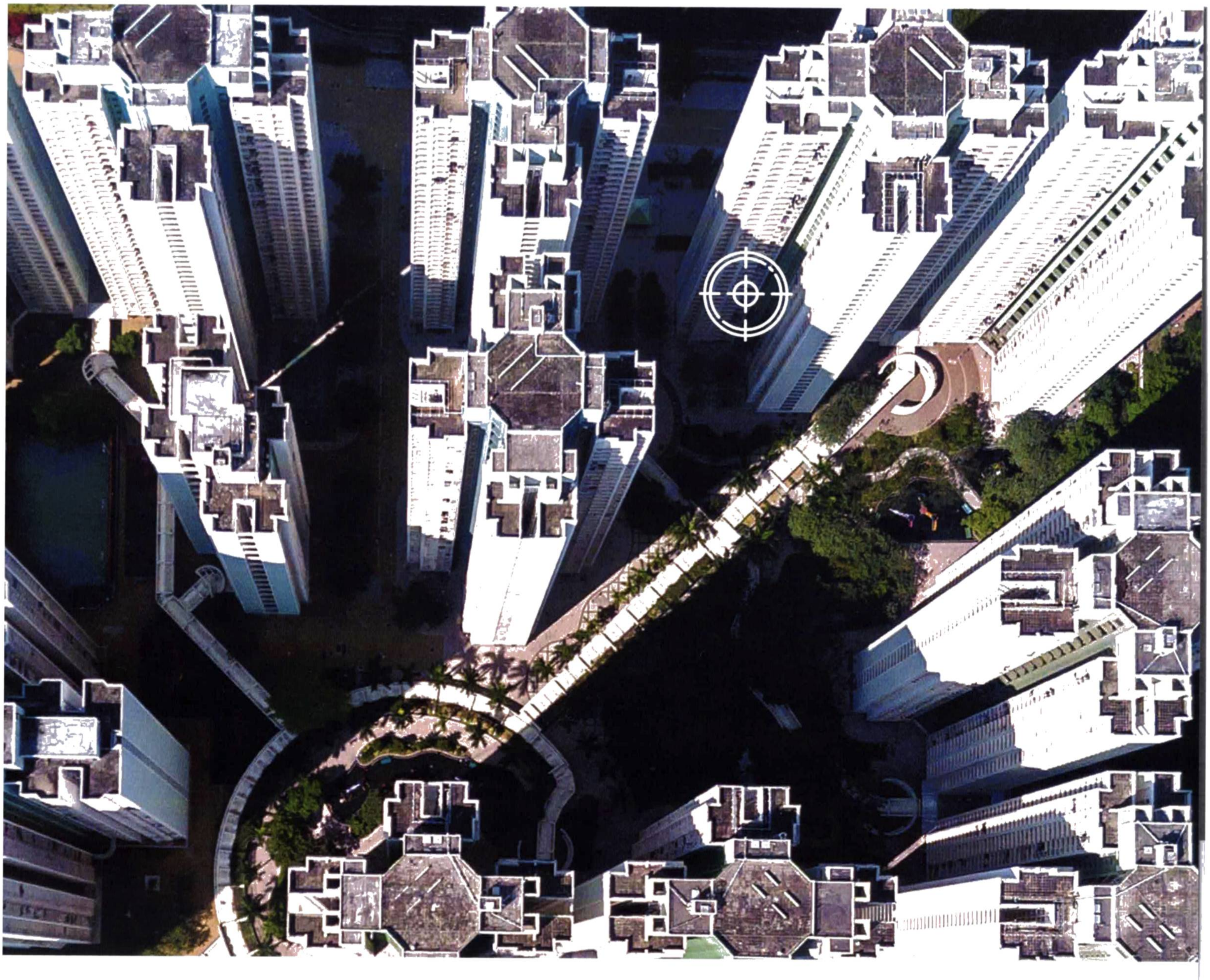
Easy to-to-use tool set that helps your organisation in profiling serious criminals and assists in the collection of target related information. A wide range of stationary, portable and nano sensors will support the investigation when applied to Wi-Fi and Local Area Networks. This can be combined into one package providing a diverse set of functionalities.

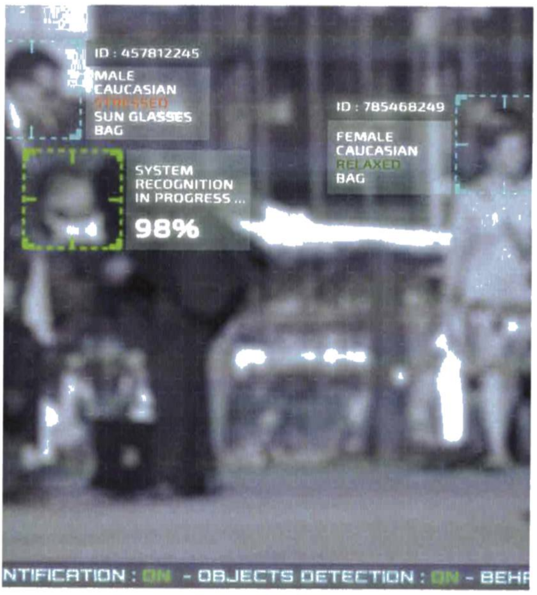
STRATEGIC MONITORING

High-end remote monitoring solutions capable of accessing data and communication from target devices – tailored to individual customer requirements. With full access to target systems, agencies can obtain locally stored information to the point of capturing encrypted data, location of suspects and messaging apps.

DEPLOYMENT METHODS

In many real-life operations, physical access to targeted systems cannot be achieved. To solve this, a covert installation of a remote monitoring solution is available. Our deployment methods and exploitation solutions cover PCs, smartphones, tablets and most common operating systems.





CYBER ACADEMY AND CONSULTANCY

Our Cyber Investigation Academy and Consultancy offers certified customised trainings and qualified support, thus setting the foundation for every successful investigation. With our Academy, we will transfer our vast knowledge in the different fields of intrusion. We will ensure that your team has a solid foundation in the cyber world.

SUPPORT AND MAINTENANCE PROGRAMME

The Support and Maintenance Programme provides upgrades and updates of our product line in combination with an annual support contract. Professional back office assistance for trouble resolution and technical queries are also part of the package. Furthermore, within the programme you will periodically be informed about our new features and functionalities.

TACTICAL GATHERING

Easy-to-Use Profiling Solution

This solution is the latest innovational step in investigation systems created by us. It is a tactical monitoring solution for Wi-Fi and Local Area Networks, combined into one package providing a diverse set of functionalities. This system has been built to seamlessly integrate with the Remote Monitoring Solution architecture, to support, improve and complement the wide range of tasks that are essential to Law Enforcement in their day-to-day operations.

Our product brings you the capability of acquiring a vast array of important data, collected from in-field deployed sensors that can be remotely controlled by operatives from a Command and Control Center. The Suite provides three types of sensor devices which are different in size and performance, thus offering the same basic functionality.

As with all our products, we made sure that all complex current techniques have been implemented to provide a simple and efficient user experience. This helps the client to focus on what matters: discovering and recording evidence to locate and convict criminals.

FEATURES

- Profiling of target devices
- Collection of data
- Controlled from Command and Control Centre
- Discovery and recording of incriminating evidence
- Data analysis and reporting
- Multiple wireless cards available in sensors
- Bypasses encryption
- Extraction of social media credentials
- Network Monitoring
- Correlation of target's habits and movements
- Unified GUI integrated with strategic monitoring solution
- SSL/TLS interception
- Possibility to combine with exploitation tools
- Wi-Fi Scanner
- Wi-Fi Jammer
- Wi-Fi Catcher
- Wi-Fi IMSI Grabber
- Bluetooth scanning and Bluetooth exploit

Tactical Solutions:

Leo5 Suite

- Leo5 Mobile
- Leo5 NANO
- Leo5 MAX

Leo5 Use Case Scenario

Local Intelligence received news on a suspect entering the country via the capital's airport. The only available information was the suspect's way of entering the country and his hotel. To locate the suspect, local intelligence correlated the obtained phone's MAC addresses and locations from the airport and hotel. This activity allowed the investigator to monitor his traffic throughout his whole stay. This resulted in visited websites, credentials used and metadata of encrypted messenger chats.

STRATEGIC MONITORING

High-End Remote Monitoring Solution

Our field-proven remote monitoring solution enables governments to overcome the current challenges of monitoring mobile and security-aware targets that regularly change location, use encrypted and anonymous communication channels and travels internationally. When the solution is installed on a computer system or mobile system, it can be remotely controlled and accessed as soon as it is connected to the Internet, no matter where in the world the system is located.

The system's modular architecture will allow the operator to adapt the system to their specific requirements and as their operational need arises. Modules such as OCR, case management and intelligence gathering modules, to cite a few, can be easily added. All used combinations in one defined operation can be controlled on a "per-case" or "per-mission" basis. This enhanced user experience will allow the investigator to analyse, combine, export and manage the collected evidence in a highly intuitive fashion.

FEATURES

- **Mission based**
- **Messenger Interception: chats, files, video**
- **Live recordings**
- **Global tracking and location of targets**
- **Integration of exploitation solutions**
- **Integration of tactical solutions**
- **Integration of advanced analysis tools**
- **Geofencing/proximity modules**
- **Analyse, combine, export and manage collected evidence**
- **Delivers valid evidence in compliance with international laws and regulations**
- **Integration into other systems via LEMF interface**

The strategic solution provides a high-performance infrastructure, which thoroughly increases the security of all components, automates monitoring of the whole system and enhances overall capacity. This will provide the end user a way for fast and efficient evidence collection and analysis. The hardware architecture is optimised to support higher availability, display system health status, allow for faster backup and restore and enhance processing speed. Also, thanks to the virtualisation approach, additional infrastructure resources can be simply added to the system.

Strategic Solution:

RMS NEO

RMS NEO Use Case Scenario

In a terrorism case, the solution's multiple layer approach was used to provide a reliable and secure way to install the RMS payload on the suspect's devices. This ensures that the payload is deployed at the right time. Security software did neither prevent nor notify about the installation, which was compliant with a given warrant. This technology ensured that the payload remained stealth and undetected.

With this solution, a whole terrorist organisation was monitored and compromised at the end of the operation.

DEPLOYMENT METHODS

Advanced Deployment Tools for Different Scenarios

There are various different products to cater for a covert installation of the remote monitoring solution that can be deployed in a "friendly" network environment like ISPs, hotel LANs, hotspots, or company LANs. The end user can select several sophisticated passive methods of target and traffic identification. Each method can be used either stand-alone or combined, to provide maximum success in identifying the targets of interest. Furthermore, deployments can be achieved through websites or with direct deployments into binary downloads.

In addtion, you will have access to our sophisticated deployment system to easily select, configure and use exploits as well as useful intrusion tools. Exploits are useful against software such as office applications, browsers or file readers. In addition, we also provide stand-alone tools against protocols such as Telegram, Bluetooth or Skype. Furthermore, they can contain remote exploits for example, routers, servers and content management systems. The exploits are meant for usage against laptops, computers and mobile phones. The infrastructure is implemented with high security in mind and resides at customer location.

FEATURES

- **Can be installed in an ISP/LAN/WAN environment**
- **Identifies targets**
- **Deploys a remote monitoring solution as a software update**
- **Installs monitoring solution through websites**
- **Relays for secure and anonymised deployment**
- **Encrypted communication for all data exchange**
- **Maximum security given to the transmission channel**
- **Portal with exclusive client access**
- **User-friendly GUI**
- **Provisioning of secure relay software for communication**

Deployment Solutions:

XPL DIVER

NET DIVER

XPL DIVER Use Case Scenario

A high-tech crime unit was investigating a cyber crime and needed to deploy a remote monitoring solution on a target system. They used an Adobe Acrobat Reader exploit and sent the target a prepared file via e-mail. The RMS was automatically downloaded and installed from the XPL DIVER Portal once he opened the file.

NET DIVER Use Case Scenario

Secret Service deployed NET DIVER in a hotel's LAN in front of the DSL modem before the IP-traffic was transmitted to the ISP network. Targets of interest could be identified in the IP-traffic by various passive profiling and identification methods and the RMS was deployed on the positively identified target systems.

CYBER ACADEMY AND CONSULTANCY

Know-How Transfer and Consulting from World-Class Experts

Faced with the unique challenges of the Law Enforcement and Intelligence space, we believe that our cyber intelligence solutions should be constantly supported and enhanced with technical know-how and the ability to operate under real-life conditions. Anticipating the client's needs, we have created the Cyber Investigation Academy and Consultancy. Sharing with you our vast knowledge in the different fields of intrusion, we will ensure that your team will have a solid foundation in the cyber world, in order to achieve excellent investigative results.

In the Consultancy, our seasoned experts will be supporting your team in topics like formation of a cyber unit, evaluating your current team and providing advice for operational situations.

FEATURES

- **Wide range of training modules**
- **Customised trainings**
- **Operational know-how**
- **Customised investigation scripting**
- **World class trainers to assist team build-up**
- **Seasoned experts**
- **Evaluation of current set-up to assist with identifying current strength and areas for development**
- **Assistance in the recruitment of team members including recommendation of training and defining the roadmap**
- **Broad catalogue of courses for all levels of previous knowledge and experience**

Example courses:

NET101: Intrusion professionals need to know a wide spectrum of disciplines. Networks can be very complex and mastering networking can make the difference between failure and success in intrusion operations (not only for tactical reasons, but specially for technical motives related to a tool's efficiency, interaction and configuration). In this course the trainees will be presented with the following topics:

- How network works
- All network media
- Network hardware, topologies and standards
- Routing / DNS
- Internet: Web and Cloud
- Analysing small corporate networks

BIN201: Scripting skills are not the only ingredient for the exploiting formula. Binaries must be understood from the development and debugging perspective, before starting the reverse engineering process. This specific online training introduces you to the complex world of:

- Programming fundamentals
- Compilers and C/C++ syntax
- Operating systems overview
- Understanding Windows API
- Binaries static / dynamic analysis
- Practical applications of reverse engineering

The above are only two examples of the 12 specialised courses we can offer to end users. We are able to mix topics depending on clients request and offer advanced consultancy and operational services.

SUPPORT AND MAINTENANCE PROGRAMME

Staying Up-to-Date with Professional Support

The Support and Maintenance Programme contains upgrades and updates of our product line in combination with an annual support contract. Our team offers the following services:

- In our Support Programme, we provide professional back office assistance for trouble resolution and technical queries. It also takes care of software bug fixes and hardware replacements under warranty. Furthermore, within the programme the client periodically receives new features and functionalities. We offer the possibility to contract our emergency On-Site Assistance module in case a rapid deployment of our experts is needed to solve any issue related to the systems.

- The Maintenance Programme offers regular software upgrades to the existing system with software patches provided via system updates. You will also get to choose how these updates are received. These updates include new features, new enhancements and new functionalities that are in line with our solutions roadmap.

FinFisher GmbH
Munich
Germany

info@finfisher.com

www.finfisher.com

Products/services described in this brochure are subject to Dual Use Regulations - Export permit required.
All information contained is strictly confidential and subject to change without notice.