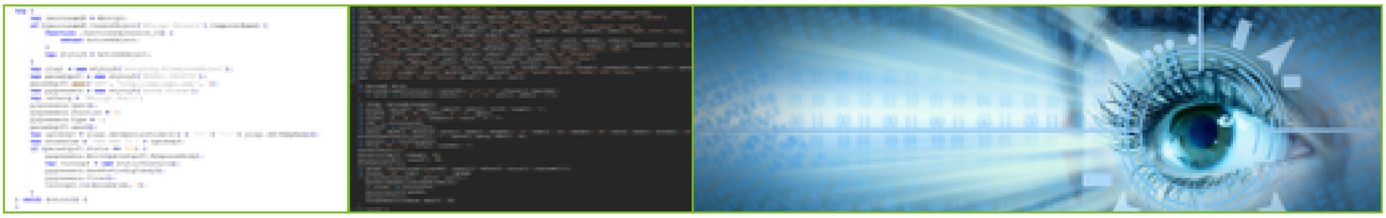
Detect malicious software and **recognize** it with the **CSPi Deobfuscation algorithm**

Malicious Software has come to a point, where not a single sample, but thousands of unique variations are being delivered every day. This is not a result of excessive malware development, but of heavy and automated obfuscation.

SECURITY IS BECOMING HARDER TO MAINTAIN

Today's threats are not about single attack vectors anymore. Developing malicious software has become an art of obfuscation, to disclose malicious behavior from Antivirus solutions and malware analysts. Especially Antivirus software can not maintain high quality endpoint security, because the detection capabilities are being scrambled by obfuscation. Especially JavaScript is a very satisfying language to provide an obfuscation that is by 100% unreadable for humans or machines. As a result of these weaknesses, there is a much higher requirement for dynamic techniques, like sandboxing, which have an even lower cost efficiency.

The consequence: High amount of costs to detect a very small percentage of actual malware.



Sebastian Rosenkranz, Malware Analyst at **CSPi Germany,** has taken a scientific approach to automatically detect and remove statically obfuscated code.

JavaScript, Office documents, PDF files, Websites. Repeating obfuscation patterns can be found everywhere. Obfuscation is always an attempt of adding an enormous amount of code, utilizing dynamic functionality, to distract the analyzer and disclose malicious behavior. Anyway, the origin of the code base will always be reassembled as a result of executing the obfuscated code pieces. The challenge is to reassemble the obfuscated code into the malicious code base, to reenable existing and high speed signature algorithms.

Sebastian Rosenkranz, Malware Analyst at CSPi Germany, has taken a scientific approach to automatically detect and remove statically obfuscated code. The patented algorithm, in a practical use case, is able to provide a clean malware sample, which only contains dynamic functionality. The consequence: Existing malware detection and analysis solutions can analyze actual behavior, instead of unreliable obfuscation detection.

ADVANTAGES OF USING THE CSPI **DEOBFUSCATION ALGORITHM**

- **Fully automatically deobfuscate** different types of malicious software
- **Read malicious URLs and related files within droppers** to automatically determine IOCs (Indicators of Compromise)
- **Assist your security- and malware analysts,** which often have to take hours or days to deobfuscate samples, to focus on the actual malware and zeroday exploits
- **Enhance the effectiveness** of existing signature algorithms
- **Decrease the amount of** false-positives by rating behavior, instead of obfuscation techniques

Why CSPi?

DATA PROTECTION KNOW-HOW

IT SECURITY COMPETENCE

INDIVIDUEL SOLUTIONS

REGULAR AUDITS

INTERNATIONAL

CSPi
Technology Solutions

CSPi (NASDAQ:CSPI) is a multinational IT service provider with a long history of success as an IT systems integrator. We can assist you with: APT & Malware Defense, Application Firewalling, Data Leakage Prevention, Database Security, Governance & Risk Management, Threat Services, SIEM & Security Intelligence and Managed Service or On Premise.

A single point of contact for your digital immune system. To learn more about **CSPi Technology Solutions** security services and receive an analysis of your business, contact us on **+44 (0) 118 9893843 or uk-ts-sales@cspi.com.** We will be happy to give you a detailed overview of our services.

LOCATIONS EUROPE

United Kingdom
12A Oaklands Business Centre Oaklands Park
Wokingham, Berkshire RG41 2FD
Phone: +44 (0) 118 989 3843

Germany
Oskar-Jäger-Str. 173 / K4
D-50825 Cologne, Germany
Phone: +49 (0) 221 9 54 46 60
www.cspi.com