SPARK

SPARK is, like his big brother THOR, a portable scanner that detects hack tools, backdoors and traces of hacker activity on end points.

While everyday Anti-Virus scanners recognize malware such as viruses, trojans and exploit codes, SPARK uses more than 7000 special signatures to examine systems for typical attacker tools, activities in logs, system manipulations, and other elements that can expose attacker activities.

The major differences to THOR is the completely different code base that allows us to compile SPARK for any desired platform like Windows, Linux, macOS and even AIX or other Unix derivatives. It is smaller, faster and more flexible than THOR but lacks many features, modules and checks on the Windows platform.

Security analysts, forensic experts and security monitoring specialists at Nextron Systems, HvS and BSK Consulting regularly update SPARK with information from various sources on attack patterns and hack tools. These sources include:

- Threat Intel Reports and Threat Feeds
- Internal Research
- Ongoing monitoring of attackers tool sets
  (e.g. disclosed tools, hack tools from underground forums)
- Forensic analyses of compromised systems in customer APTs

SPARK can be easily extended to handle individual, client-specific attack patterns. IOCs like hashes, C2 servers, file names and YARA rules can be added easily. We use a simple to write and read CSV format that many users have come to appreciate from LOKI, our Open Source scanner.

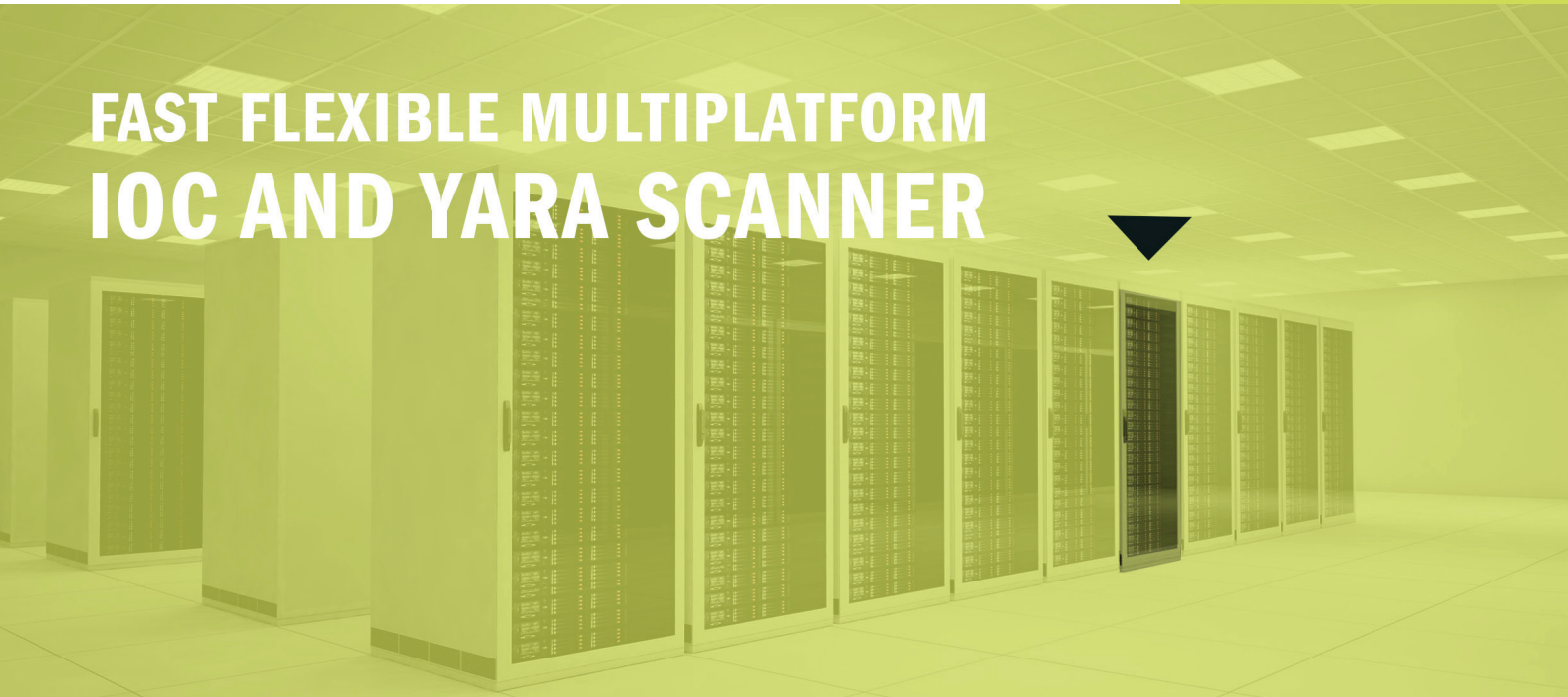
Focus on APTs

Fast, Lightweight and Multiplatform

Signatures maintained by security researchers

Specific indicator and signature sources

Custom case-related attack patterns



FAST FLEXIBLE MULTIPLATFORM
IOC AND YARA SCANNER

SPARK

SPARK generates different output types: a text log and SYSLOG output that can be send to remote systems.

The well-known CEF format, used by ArcSight, is also supported. Therefore it is an easy task to integrate SPARK's logs into any major SIEM system.

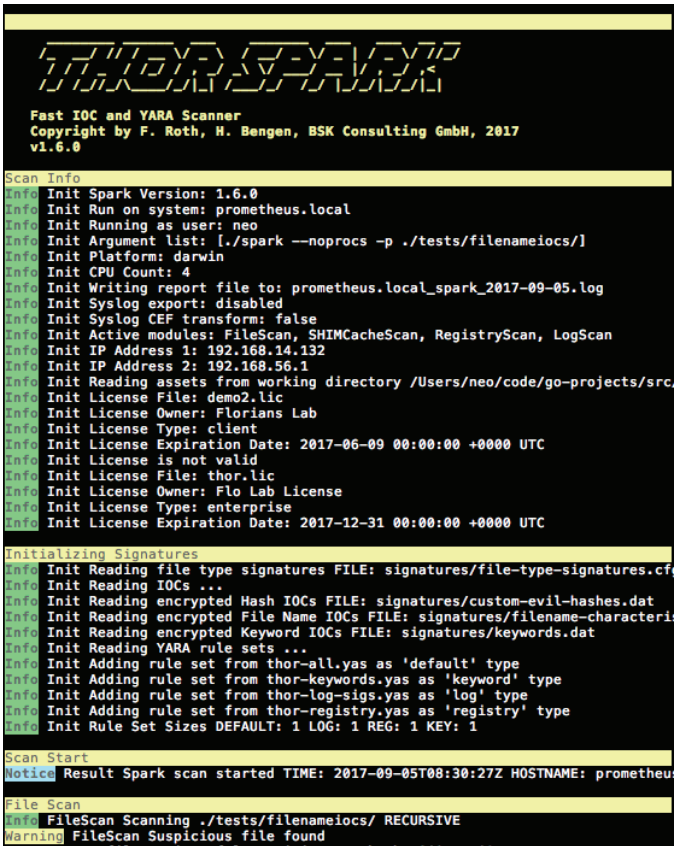
SPARK can operate completely offline. The scope of application is therefore very flexible. You can easily scan separated network segments like DMZs, collect and merge the generated log data afterwards.

	THOR	SPARK
Preferred Use Case	Incident Response / Live Forensics	Preventive Scanning / Triage
Keywords	Intense, Sensitive	Fast, Determined
Platform	Windows	Windows, Linux, OpenBSD, FreeBSD, macOS (Solaris, Android)
Size	15 MB	4 MB
Modules	26 Modules	6 Modules
Language	Python	Golang

Beside the hard indicators SPARK uses a scoring-system that evaluates a score for files based on attributes, contents and meta data. It allows SPARK to report suspicious files and detect malware that is yet unknown.

There are three major use cases for SPARK:

- **Triage Sweep**
  Scan run on all systems in a system einvironment, reporting to a central SIEM to identify compromised systems
- **Single System Live Forensics**
  Scan run on a single running system reported as suspicious to falsify or verify a possible threat
- **Image Scan im Lab**
  Scan run on a mounted drive image in the Lab to identify known indicators of compromise and speed up forensic analysis



SPARK scans can be scheduled and controled from a central location, the ASGARD server (optional). With ASGARD, you can run distributed SPARK scans on thousands of end points and all possible platforms like Windows, Linux, macOS and AIX.

Further advantages / features are:

- Central scan control via ASGARD appliance
- Free Splunk App / Add-on
- Resource control feature provides high stability and ensures low CPU load during the scan
- Encrypted signatures
- Data protection option to remove personal information from the scan results
- Quick scan mode for fast analysis of the most important elements within minutes
- Direct contact to the developers / quick feature integration / security made in Germany