

SPARK

SPARK is 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 9000 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 and macOS. It is smaller, faster and more flexible than THOR but lacks some features, modules and checks on the Windows platform.

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

- Threat intel reports and threat exchanges
- 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 IOCs like hashes, C2 servers, file names and YARA rules. 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

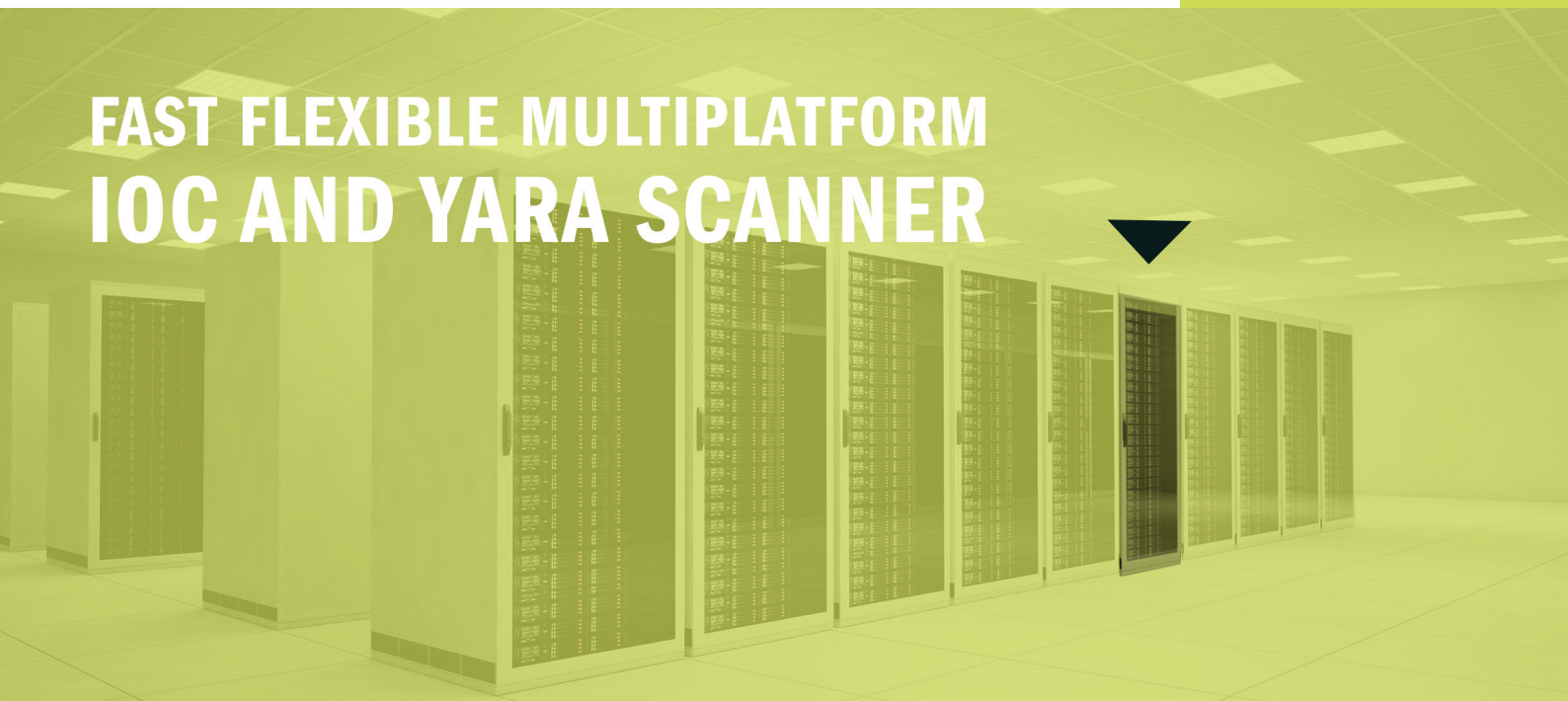
Fast, Lightweight and Multiplatform

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 in Text or JSON form 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.

	SPARK	THOR
Main Use Case	Preventive Scanning / Triage	Incident Response / Live Forensics
Platform	Windows, Linux, macOS	Windows
Size (Binaries)	9 MB	16 MB
Language	Go	Python
Modules	9	26
Special Extras	JSON output SYSLOG (tcp/udp/ssl) Scan Throttling	... a lot, see comparison

There are three major use cases for SPARK:

- **Triage Sweep**
Scan run on all systems in a system environment, 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

```
THOR SPARK
Fast IOC, YARA and Sigma Scanner
Copyright by Nextron Systems GmbH, 2018
SPARK Version: 1.17.26
THOR Signature Revision: c27025c
Sigma Signature Revision: 9ef3144

Scan Info
Info Init SPARK Version: 1.17.26
Info Init Run on system: prometheus.local
Info Init Running as user: neo
Info Init User has admin rights: no
Info Init Argument list: [/spark-macosx-x64]
Info Init Platform: darwin (Darwin prometheus.local 18.2.0 Darwin Kernel Version 18.2.0:
Thu Dec 20 20:46:53 PST 2018; root:xnu-4903.241.1~1/RELEASE_ARM_T8020)
Info Init CPU Count: 8
Info Init Writing report file to: prometheus.local_spark_2019-03-04.log
Info Init Syslog export: disabled
Info Init Scanning system drive only
Info Init IP Address 1: 192.168.14.162
Info Init IP Address 2: 192.168.56.1
Info Init IP Address 3: 10.255.249.14
Info Init Maximum runtime in hours: 72
Info Init Reading assets from working directory /Users/neo/Downloads/spark-macosx-pack
Info Init License File: thor.lic
Info Init License Owner: CI Testing
Info Init License Type: enterprise
Info Init License Start Date: 0001/01/01
Info Init License Expiration Date: 2021/12/31
Info Init Reading file type signatures 'signatures/file-type-signatures.cfg'
Info Init Reading IOCs ...
Info Init Reading encrypted keyword IOCs 'signatures/keywords.dat'
Info Init Reading encrypted file name IOCs 'signatures/filename-characteristics.dat'
Info Init Reading encrypted hash IOCs 'signatures/custom-evil-hashes.dat'
Info Init Reading encrypted file name IOCs 'custom-signatures/filename-iocs.dat'
Info Init Reading false positive hash IOCs 'custom-signatures/falsepositive-hashes.txt'
Info Init Reading YARA rule sets ...
Info Init Adding rule set from thor-log-sigs.yas as 'log' type
Info Init Adding rule set from thor-keywords.yas as 'keyword' and 'log' type
Info Init Ignoring rule set from thor-registry.yas due to operating system type
Info Init Adding rule set from spark-process-memory.yas as 'process' type
Info Init Adding rule set from thor-all.yas as 'default' type
Info Init Adding rule set from new_rules.yas as 'default' type
Info Init Rule Set Sizes default: 2, log: 2, reg: 0, key: 1, prc: 1
Info Init Reading STIXv2 indicators ...
Info Init Successfully compiled 0 / 0 STIXv2 indicators

Initializing Active Modules
Info Init Active modules: RegistryScan, LogScan, EventLog, Rootkit, FileScan, ProcessScan,
SHIMCachesScan, Autoruns, AtJobs
Info Init Active features: Bifrost, RegistryWalk, YARA, DumpScan, STIX
```

Further advantages / features are:

- Quick scan mode for fast analysis of the most important elements within minutes
- Sigma rule application on endpoints
- Extensive STIXv2 support
- Free Splunk App / Add-on
- Resource control feature provides high stability and ensures low CPU load during the scan
- Encrypted signatures (bundled with encrypted rule set, encrypt custom rules with 'thor-util')
- Data protection option to remove personal information from scan results
- Direct contact to the developers / quick feature integration / security made in Germany

SPARK

Scan your systems with SPARK to gain certainty about their integrity and detect possible attackers.

Contact us today via the following address: