1-year anniversary to SentinelOne 1.8.4 release

March 12, 2018
by Migo Kedem

We've just celebrated a year since launching 1.8.4 release. Here's a post sharing some interesting facts about the version. **1.8.4 will reach End of Support on June 15th**. Before, please update to 2.0, 2.1, or 2.5.

Features

It was the first release including our Static AI engine, exclusions, Windows Security Center integration (so Windows does not claim there is no malware protection if SentinelOne installed), auto mitigation for PUP on macOS and many more features.

Our Static AI module:

Adding Static AI to our list of engines had a magnificent impact on the amount of malware we prevent before it had the chance to run, as most of the mitigation before this release happening on or post-execution. Starting 1.8.4, every file that is copied to disk is immediately scanned against SentinelOne static AI module, if classified either as a threat (and mitigated immediately), as a suspicious file (mitigation depends on the policy) or a benign, allowing other engines to examining it before it can make its impact.

One of the major benefits of static-based detection is that it can be performed *before the file is executed* (or pre-execution). This is obviously useful because it's much easier to remediate malware if it's never allowed to execute. An ounce of prevention is worth a pound of cure. A corollary of this benefit is that even corrupt and malformed executables which won't execute can still be detected statically. Of course, any sort of detection which is mostly based on behavioral analysis will fail to detect these same samples because they don't generate any behavior. It's questionable if these types of files should even be considered malicious. Even still, there may be some value in detecting and removing malware which can't actually harm you simply because it brings peace of mind and suits existing policies and procedures.

Releasing the Static AI module also helped us in two aspects:

1. SentinelOne has decided to contribute to the community by offering it to VirusTotal. It's important to highlight that we've shared SentinelOne Static AI engine with VirusTotal, and not other modules available on SentinelOne agents. To test a malware against SentinelOne technology, we recommend using a deployed agent and not rely on VirusTotal score for SentinelOne Static AI.
2. Although SentinelOne technology does not depend on scanning for detection, some of our customers asked for the ability to scan their endpoint, to cover the case of dormant malware and due to compliance reasons. Adding Static AI enabled us to offer Full Disk Scan to our customers.

Policy

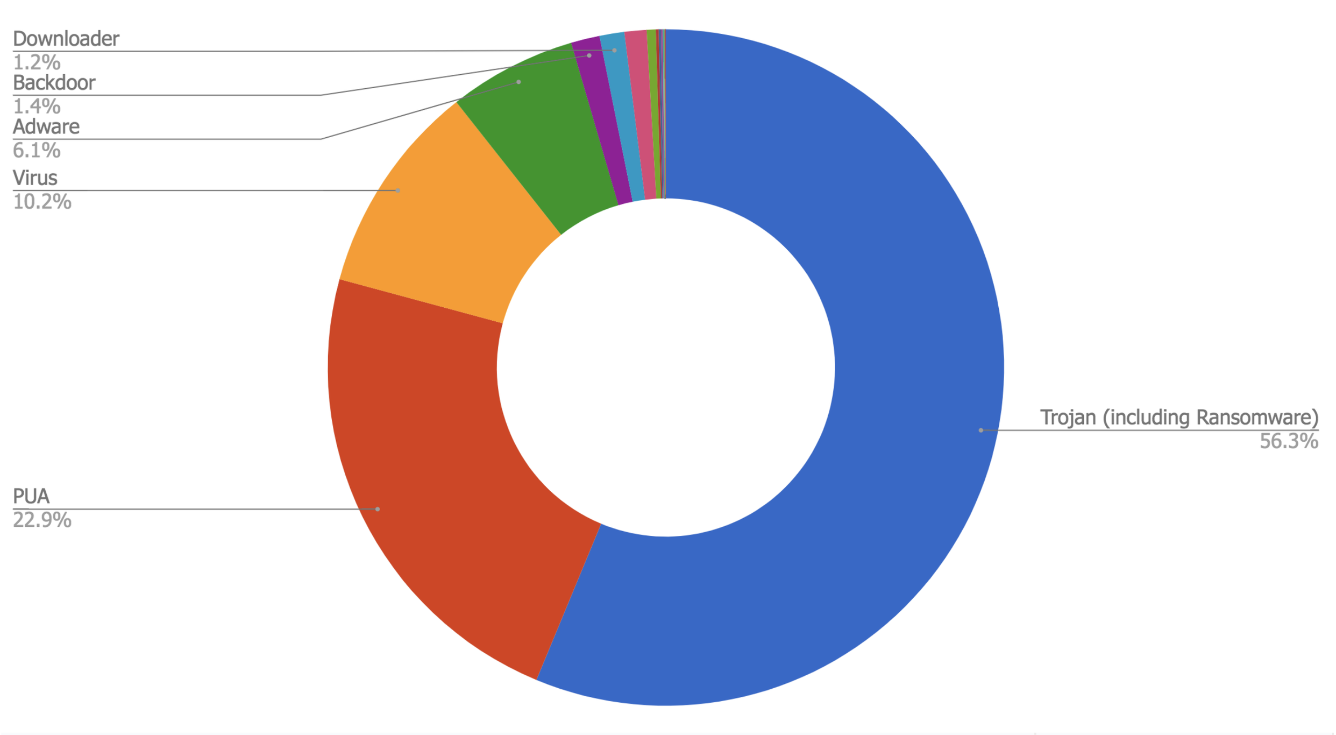
The policy was reasonably simple, but we needed to change the concept of cloud validation to the internal logic that uses the cloud when needed. Our default policy used to require cloud connectivity for mitigation.

Remember this?

Detection

From detection side, we added our Anti exploit capabilities, with ROP detection, Stack Pivot, and Shellcode detection.

1.8.4 prevented many different malware attempts. Find their classification:



Type	
Trojan (including Ransomware)	56.26%
PUA	22.95%
Virus	10.16%
Adware	6.12%
Backdoor	1.37%
Downloader	1.18%
Hacktool	1.06%
Exploit	0.43%
Rootkit	0.14%
Spyware	0.10%
Packed	0.10%
Browser	0.06%
Infostealer	0.03%
Keylogger	0.03%
Network	0.02%
Dialer	0.01%

Recognised by 3rd parties

NSS labs

1.8.4 earns NSS Labs' coveted 'Recommended' rating scoring a 99.79% in effectiveness, achieving the highest ROI out of 15 competing endpoint protection solutions and Leading TCO rating.

AV-Comparatives

1.8.4 has been named an Approved Business Product in an independent test from AV-Comparatives.

Conclusions

1.8.4 was a game changer for SentinelOne, as it marked the prevention, detection and response era. It was the first time SentinelOne technology was deployed to large enterprises, covering 100K and above organizations that were geographically dispersed. We do recommend all our customers to upgrade with an ease of a click to 2.x versions.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- In Pursuit Of Perfection – A Console Rewrite
- Feature Spotlight | Introducing Singularity Dark Mode
- Introducing the New Singularity XDR Process Graph
- Feature Spotlight | Combating Email Threats Through AI-Driven Defenses with Armorblox Integration
- Feature Spotlight | Announcing General Availability (GA) of Linux and K8s Agents v22.3 for Cloud Workload Security
- Feature Spotlight | Integrated Mobile Threat Detection with Singularity™ Mobile and Microsoft Intune