DEKENEAS

securing tomorrow

DESCRIPTION

Dekeneas APT Hunter is a *unique product*, being the only publicly available tool able to *identify with great accuracy both known and unknown browser exploits ("0day") and attacks* by the means of artificial intelligence algorithms, instead of traditional signature scanning. Our approach is mainly focused on *detection of unknown attack vectors for the vast majority of existing desktop browsers, such as Chrome, Edge, Firefox or Safari, but also mobile devices browsers for Android and iPhone*. Our artificial intelligence algorithms understand the code of the website (HTML, Javascript, etc.) before actually executing it, and try to understand if the encountered code constructs are malware specific or they are benign, even if they are heavily obfuscated. Also it tries to figure out if there are *special conditions* for certain code to run, such as specific User-Agent strings, language settings or IP addresses. All this information is later used during the *instrumentation performed by Dekeneas Sandbox*, which comes as a double check, actually executing the suspicious code in a real environment according to the special conditions requested by the analyzed code, launching a specific browser with specific language or country settings in a specific environment (desktop or mobile), and analyzing how the code interacts with the browser. In addition to code instrumentation Dekeneas Sandbox also analyzes the traffic generated looking for exploitation gadgets, therefore maximizing the chances of identifying unknown attacks. *Dekeneas APT Hunter is able to scan hundreds of websites simultaneously searching for locally or remotely included implants*.

KEY FEATURES

- **Signature less scanning** – one of the defining characteristics of browser attacks is the fact that code rarely looks similar between infections, therefore signature scanning is most of the times useless. In Dekeneas it is replaced by smart analysis of website code using artificial intelligence to classify the code as malicious or benign.
- **In-depth scanning** of websites is a very useful feature as most malware usually lurks beyond the first page of the website. The user can specify if they want a rapid scan or a more extensive or complete scan (which usually takes more time).
- **Detection of 0day attacks**, as new browser exploits appear almost weekly, more and more victims are infected with malware without even knowing
- **Detection of attacks in early stage** as opposed to other traditional detection methods who focus on post-exploitation stage of the compromise.
- **Detection of cryptojacking or skimming operations** who mine cryptocurrency while users browse the website, without user's consent or knowing, or credit card compromise operations such as Magecart.
- **Complex system of proprietary sandboxes for popular desktop and mobile browsers** performing smart analysis on suspicious HTML code, according to the special requirements of the code (e.g. specific User-Agent, or specific country or language settings)
- **Complex system of network traffic analysis** to identify network artefacts specific to attacks.
- **Heavy anti-analysis evasion** techniques guarantee that even the most cunniving malware is detected before producing any damage.
- **Scanning frequency** can be specified by the user as *monthly, weekly, daily* or *continuous*