Photo credit: Microsoft Word>Stock Images

HD TAT Success Story

Automatic Generation of Yara Rules to Target Malware

Customer:	National Security Agency's (NSA) Research Directorate
Challenge:	Yara is a technology using a set of statements to identify a collection of related malware samples, usually referred to as a malware family. Crafting a Yara rule by hand to identify a family of malware is often tedious and time consuming, yet this is the standard way to share information between organizations and agencies about discovered malware.
Approach:	Building on prior work, HD TAT leveraged a large n-gram capability to identify large byte sequences which are present in the malware family, and not present in other malicious or benign files. HD TAT 's automated approach enabled production of durable and accurate Yara rules in seconds.
Value:	HD TAT's solution saves time and effort in malware identification activities. The team presented this work at the 2020 AISec conference, where it won the 'Best Paper' award. Our method, AutoYara, is fast, allowing for deployment on low-resource equipment for teams that deploy to remote networks. Our results demonstrate that AutoYara can help reduce analyst workload by producing rules with useful true-positive rates while maintaining low false-positive rates, sometimes matching or even outperforming human analysts. In addition, real-world testing by malware analysts indicates AutoYara could reduce analyst time spent

	constructing Yara rules by 44-86%, allowing them to spend their time on the more advanced malware that current tools can't handle. Code will be made available at this https URL .

Booz Allen Hamilton supports HD TAT under contract FA8075-14-D-0002.