Mandiant

JUNE 25, 2024 MANDIANT ADVANTAGE THREAT INTELLIGENCE RELEASE

YARA Rule naming update

To improve the organization and clarity of our threat intelligence, we are standardizing the naming of our YARA rules. This change will make it easier for you to identify, manage, and use the rules in your security workflows.

What to expect

- **Date of Change**: 25th June 2024
- **Impact**: All existing YARA rules will be republished under new names that adhere to our updated naming convention. For customers who are downloading the latest updated to yara rules from our API then you should expect that you will download all rules again with their updated names.
- **Action Required**: If you currently use MATI YARA rules, please review the updated rule names on June 25th. Update any references to the old rule names in your systems or integrations.

Why we're making this change

The current YARA ruleset has various naming inconsistencies, making it difficult to navigate and understand. This update will ensure a consistent, professional, and user-friendly experience for all MATI customers. We appreciate your understanding and cooperation as we enhance the quality and usability of our threat intelligence offerings.

Naming convention

The following naming convention aims to provide you with more specific information about the rule's purpose and the type of threat it is intended to detect. Incorporating these rules into security tools allows you to easily understand the Mandiant intelligence associated with each rule based on its name.

Malware

Prefix	Designation	Type	Name	Iteration
M	Tracked Group Category	Malware Role	Malware Family Name	Number to differentiate similarly named rules (not a version)

Examples

- `M_APT_Backdoor_SOGU_1`
- `M_APT_Dataminer_AZORULT_V2_1`
- `M_APTFIN_Downloader_SHELLTEA_1`
- `M_APTFIN_Downloader_SHELLTEA_2`

Exploit

Prefix	Designation	Name	Iteration
M	Exploit	CVE Number	Number to differentiate similarly named rules (not a version)

Example

- `M_Exploit_CVE20213156_3`

Other names (such as M_HUNTING) will be phased out in later releases and some will be changed (such as M_AUTOPATT), as they are folded into the new naming convention.