Mandiant

HOW COLLECTIONS WORK - DEFAULT TASKS

Each Seed type has a different set of default tasks that are run through the workflow. The following list includes the most common tasks that are applied to various seed types. This list is not all-inclusive and is subject to change due to the evolution in the individual tasks and sophistication of collection machines. A list of tasks and their capability are available in the **Library (https://asm.advantage.mandiant.com/library/tasks)**.

AwsS3Bucket

- aws_s3_put_file

Domain

- enumerate_nameservers
- dns_nsec_walk
- dns_transfer_zone
- dns_lookup_dkim
- search_crt
- search_certspotter
- dns_search_sonar
- search_threatcrowd
- email_brute_gmail_glxu
- dns_recurse_spf
- dns_morph
- dns_brute_sub
- saas_google_groups_check
- saas_jira_check
- search_grayhat_warfare
- aws_s3_brute

DnsRecord

- search_cleanbrowsing_dns
- search_comodo_dns
- search_opendns
- search_quad9_dns
- search_yandex_dns

EmailAddress

- saas_google_calendar_check

GithubAccount

- gitrob

IpAddress

- whois_lookup
- search_shodan

- common_tcp_port_scan

Nameserver

- security_trails_nameserver_search

NetBlock

- masscan_scan

NetworkService

- rdpscan_scan

Organization

- whois_lookup
- search_bgp
- search_grayhat_warfare
- saas_jira_check
- web_account_check
- aws_s3_brute

Uri

- wordpress_enumerate_users (if fingerprinted as wordpress)
- wordpress_enumerate_plugins (if fingerprinted as wordpress)
- uri_brute_focused_content
- uri_gather_ssl_certificate
- uri_check_subdomain_hijack
- uri_spider
- [many vulnerability checks]