



AUGUST 10-11
MANDALAY BAY / LAS VEGAS



Sandbox Scryer

Greg Dalcher

Joel Spurlock

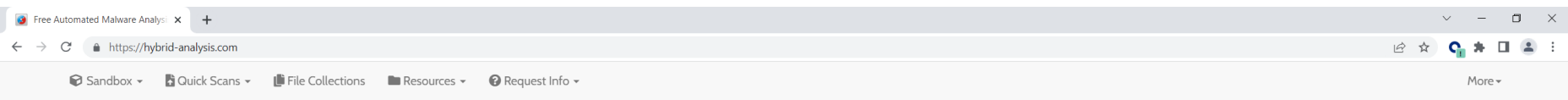
Problem Statement, and Solution


- Defending against Advanced Persistent Threats requires answering “what’s next?” after an initial detection
 - How will threat try again?
 - What is threat after?
 - How can defenses be improved to thwart next attack attempts and stages?
- Sandbox can help provide the signal to communicate focused answers to the above questions
 - Can be integrated into SoC and SOAR operations at scale
 - Can enhance intelligence and threat hunting operations
 - Allows for prioritization of important IOCs and ATT&CK behaviors
 - Sandbox solutions generate a lot of data, which needs post processing to be effective

Sandbox Scryer – What is it?

- Open-source tool for producing threat-hunting and intelligence data from sandbox output
 - Initial integration is with the free and public Hybrid Analysis (HA) sandbox
 - <https://hybrid-analysis.com/>
 - <https://hybrid-analysis.com/docs/api/v2>
- Leverages MITRE ATT&CK framework to organize and prioritize findings, facilitating assembly of IOCs


Hybrid Analysis Sandbox - Web UI





File/URLFile CollectionReport SearchYARA SearchString Search

This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology.



Drag & Drop For Instant Analysis

or

Analyze

Maximum upload size is 100 MB.
Powered by **CrowdStrike Falcon® Sandbox**.
Interested in a free trial?

Removal Notice
API v1 has been removed as of August 2021.
Please use API v2, [click here to learn more](#).

Latest News

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell
Chris Nguyen - Eric Loui - March 7, 2022

Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities
CrowdStrike Intelligence Team - March 1, 2022

CrowdStrike Falcon Protects from New Wiper Malware Used in Ukraine Cyberattacks
William Thomas - Adrian Liviu Arsene - Farid Hendi - February 25, 2022

Access Brokers: Who Are the Targets, and What Are They Worth?
CrowdStrike Intelligence Team - February 23, 2022

CrowdStrike Research Investigates Exploit Behavior to Strengthen Customer Protection
Joseph Goodwin - Aspen Lindblom - February 22, 2022

[See More!](#)

Output

- Primary output: Layer file for import into MITRE ATT&CK Navigator
 - Collates data from set of sandbox submissions' report summaries
 - Includes metadata and ranking of ATT&CK techniques
- Supplemental output
 - Individualized output for each sandbox report summary
 - Graphical file showing triggered techniques in MITRE ATT&CK Framework
 - Text file for human readability. Includes ranking of techniques
 - .csv file for import into collating tools. Used to assemble the collated data placed in the Navigator layer file

MITRE ATT&CK Navigator – View of Collated Data

ATT&CK Navigator

https://mitre-attack.github.io/attack-navigator/

collated_080122

selection controls layer controls technique controls

TA0001 Initial Access 9 techniques	TA0002 Execution 10 techniques	TA0003 Persistence 18 techniques	TA0004 Privilege Escalation 13 techniques	TA0005 Defense Evasion 13 techniques	TA0006 Credential Access 15 techniques
T1189 Drive-by Compromise	T1106 Native API	T1547.001 Registry Run Keys / Startup Folder	T1134.001 Token Impersonation/Theft	T1134.001 Token Impersonation/Theft	T1056.001 Keylogging
T1190 Exploit Public-Facing Application	T1047 Windows Management Instrumentation	T1547.014 Active Setup	T1134.002 Create Process with Token	T1134.002 Create Process with Token	T1056.004 Credential API Hooking
T1133 External Remote Services	T1059.003 Windows Command Shell	T1547.002 Authentication Package	T1134.003 Make and Impersonate Token	T1134.003 Make and Impersonate Token	T1056.002 GUI Input Capture
T1200 Hardware Additions	T1059.002 AppleScript	T1547.006 Kernel Modules and Extensions	T1134.004 Parent PID Spoofing	T1134.004 Parent PID Spoofing	T1056.003 Web Portal Capture
T1566 Phishing (0/3)	T1059.007 JavaScript	T1547.015 Login Items	T1134.005 SID-History Injection	T1134.005 SID-History Injection	T1158 Software Discovery (1/1)
T1091 Replication Through Removable Media	T1059.001 PowerShell	T1547.008 LSASS Driver	T1548.002 Bypass User Account Control	T1140 Deobfuscate/Decode Files or Information	T1157 Process Discovery
T1195 Supply Chain Compromise (0/2)	T1059.006 Python	T1547.010 Port Monitors	T1548.004 Elevated Execution with Prompt	T1070.004 File Deletion	T1109 System Network Connections Discovery (1/4)
T1199 Trusted Relationship	T1059.004 Unix Shell	T1547.012 Print Processors	T1548.001 Setuid and Setgid	T1070.003 Clear Command History	T1108 File and Directory Discovery
T1078 Valid Accounts (0/3)	T1059.005 Visual Basic	T1547.007 Re-opened Applications	T1548.003 Sudo and Sudo Caching	T1070.002 Clear Linux or Mac System Logs	T1057 Process Discovery
	T1203 Exploitation for Client Execution	T1547.005 Security Support Provider	T1547.001 Registry Run Keys / Startup Folder	T1070.001 Clear Windows Event Logs	T1212 Exploitation for Credential Access
	T1559 Inter-Process Communication (0/3)	T1547.009 Shortcut Modification	T1547.014 Active Setup	T1070.005 Network Share Connection Removal	T1187 Forced Authentication
	T1053 Scheduled Task/Job (0/4)	T1547.003 Time Providers	T1547.002 Authentication Package	T1070.006 Timestamp	T1606 Forge Web Credentials (0/2)
	T1129 Shared Modules	T1547.004 Winlogon Helper DLL	T1547.006 Kernel Modules and Extensions	T1548.002 Bypass User Account Control	T1556 Modify Authentication Process (0/4)
	T1072 Software Deployment Tools	T1547.013 XDG Autostart Entries	T1547.015 Login Items	T1548.004 Elevated Execution with Prompt	T1111 Multi-Factor Authentication Interception
	T1569 System Services (0/2)	T1574.010 Services File Permissions Weakness	T1547.008 LSASS Driver	T1548.001 Setuid and Setgid	T1621 Multi-Factor Authentication Request Generation
	T1204 User Execution (0/2)	T1574.012 COR_PROFILER	T1547.010 Port Monitors	T1548.003 Sudo and Sudo Caching	T1040 Network Sniffing
		T1574.001 DLL Search Order Hijacking	T1547.012 Print Processors	T1574.010 Services File Permissions Weakness	T1615 Group Policy
		T1574.002 DLL Side-Loading	T1547.007 Re-opened Applications	T1574.001 DLL Search Order Hijacking	
		T1574.004 Dylib Hijacking	T1547.005 Security Support Provider	T1574.002 COR_PROFILER	
		T1574.006 Dynamic Linker Hijacking	T1547.009 Shortcut Modification	T1574.003	

MITRE ATT&CK Navigator v4.6.5

legend

Operation

- Sample(s) submitted to Hybrid Analysis sandbox for analysis
 - Submission of samples and retrieval of results normally handled separately from the Scryer tool. Optionally, Scryer tool can be used to submit sample
- Scryer tool run with 'parse' command against each collected sandbox report
 - Input includes technique ranking, generated using MITRE ATT&CK Top Techniques calculator
- Scryer tool run with 'collate' command against set of collected sandbox reports
 - Generates MITRE ATT&CK Navigator layer file using collated data from set of sandbox reports
 - Viewable within Navigator
 - Includes metadata for ATT&CK techniques noted by HA sandbox
- Scryer operation governed by command-line parameters, enabling scripting

Using Results

- Viewing within MITRE ATT&CK Navigator – Primary usage
 - Allows view of techniques and tactics affected by set of samples, with prevalence and prioritization shown via heat map
 - Metadata available for techniques observed within sample set's detonation and analysis in sandbox
 - File and Windows Registry paths, command-line arguments, network addresses and URLs, user/system account used, etc.
 - Using metadata, responses can be developed:
 - Prioritized vulnerability scanning and software update management
 - Security posture adjustments: accounts locked, authentication policies adjusted, systems isolated, ...
- Other usages: importing .csv files into other tools

Input and Dependencies

- Sample report summaries: result from submissions to sandbox, using the free and public HA Sandbox at: <https://hybrid-analysis.com/>
- MITRE ATT&CK definitions CTI data from <https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json>
- MITRE ATT&CK top techniques ranking data, generated using their calculator at <https://top-attack-techniques.mitre-engenuity.org/>

For more info

- Open-source will be released under github repo
https://github.com/PayloadSecurity/Sandbox_Scryer
- Input and collaboration welcome!

Demo

- Set of samples previously submitted to HA sandbox and reports collected
 - Brief overview of collected report summaries
- Show Scryer tool invoked for set of reports, via simple script
 - Walk through output Scryer tool generates after parsing sandbox reports
- Show Scryer tool invoked against prior step's output
 - Walk through collated data and generated Navigator layer file
- Invoke MITRE ATT&CK Navigator, loading generated layer file
 - Walk through displayed ATT&CK framework. Discuss usage of data shown