

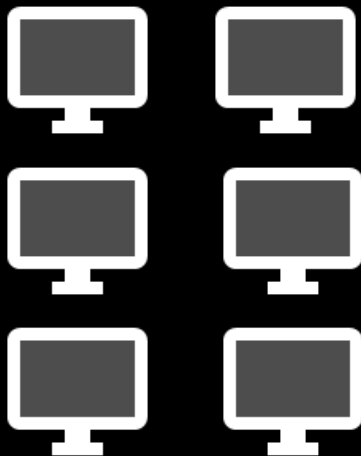
Applying ATT&CK to Web Applications

...

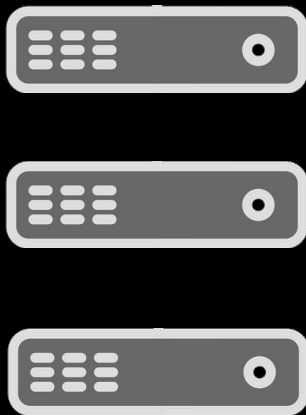
EU ATT&CK Community, May 19th

Current state of monitoring

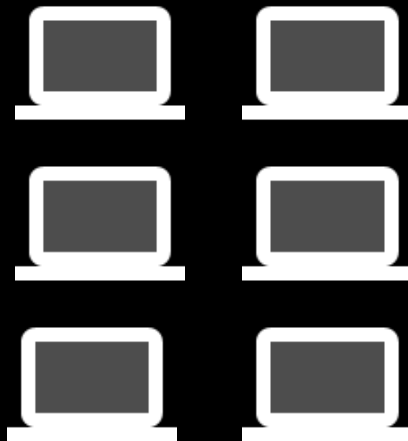
ATT&CK Windows



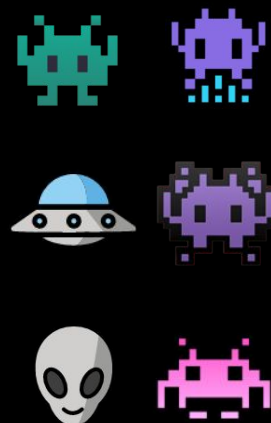
ATT&CK Linux



ATT&CK macOS



Web Applications



ATT&CK Navigator For Web Applications

MITRE ATT&CK® Navigator

ATT&CK for Web Applications x +

selection controls layer controls technique controls

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
4 items	4 items	5 items	3 items	10 items	5 items	9 items	6 items	6 items	8 items	3 items	9 items
Drive-by Compromise	Scripting	Account Manipulation	Exploitation for Privilege Escalation	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Automated Collection	Data Encoding	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Space after Filename	Create Account	Valid Accounts	Compile After Delivery	Brute Force	Cloud Service Dashboard	Exploitation of Remote Services	Data from Cloud Storage Object	Data Obfuscation	Exfiltration Over Command and Control Channel	Data Destruction
Spearphishing Link	Third-party Software	Server Software Component	Web Shell	Exploitation for Defense Evasion	Cloud Instance Metadata API	File and Directory Discovery	Internal Spearphishing	Data from Information Repositories	Domain Generation Algorithms	Transfer Data to Cloud Account	Defacement
Valid Accounts	User Execution	Valid Accounts		File Deletion	Steal Application Access Token	Network Service Scanning	Remote Services	Data from Local System	Remote Access Tools		Endpoint Denial of Service
		Web Shell		Obfuscated Files or Information	Steal Web Session Cookie	Password Policy Discovery	Third-party Software	Data Staged	Standard Application Layer Protocol		Network Denial of Service
				Scripting		Remote System Discovery	Web Session Cookie	Email Collection	Standard Cryptographic Protocol		Resource Hijacking
				Space after Filename		Software Discovery			Uncommonly Used Port		Runtime Data Manipulation
				Valid Accounts		System Information Discovery			Web Service		Stored Data Manipulation
				Web Service		System Owner/User Discovery					Transmitted Data Manipulation
				Web Session Cookie							

MITRE ATT&CK® Navigator v2.3.2

#fcf3a2	Manual URL mapping
#74c476	Default CRS detection
#c6dbef	Behavior based detection

Demo

ATT&CK Navigator for Web Applications

Why are custom web applications so hard?

They are SO CUSTOM!?!>

Normalize URLs to ATT&CK

Users behave differently>

Use statistics to learn normal

They change DAILY!?!>

Involve Dev for DevSecOps

Developer triage required>

Find similar requests in SIEM

Outsourced applications>

Forward logs for correlation

Let's be in touch

Ruben van Vreeland

Open Source Hacker at Securely

OWASP Slack (OWASP Core Rule Set)

owasp-slack.herokuapp.com

Mail ruben@securely.ai

PGP 3700 C0A7 31F4 54BC 420F
8E30 10D3 EA7B DFFE F5A0

