



So You've Decided to Use MITRE ATT&CK®: *Now What?*

November 30, 2022

PRESENTED BY:

Rich Struse, CTO

Scott Small, Director of CTI



Learning objectives

- Threat-informed defense and its applications
- The benefits and limitations of MITRE ATT&CK
- How to develop a threat-informed defense strategy

Note: All of the resources referenced in this presentation are freely-available community resources.

Threat-Informed Defense and its Applications

**What is "Threat-Informed
Defense"?**



Threat-Informed Defense

“The systematic application and deep understanding of adversary tradecraft and technology to assess, organize and optimize your defenses.”†

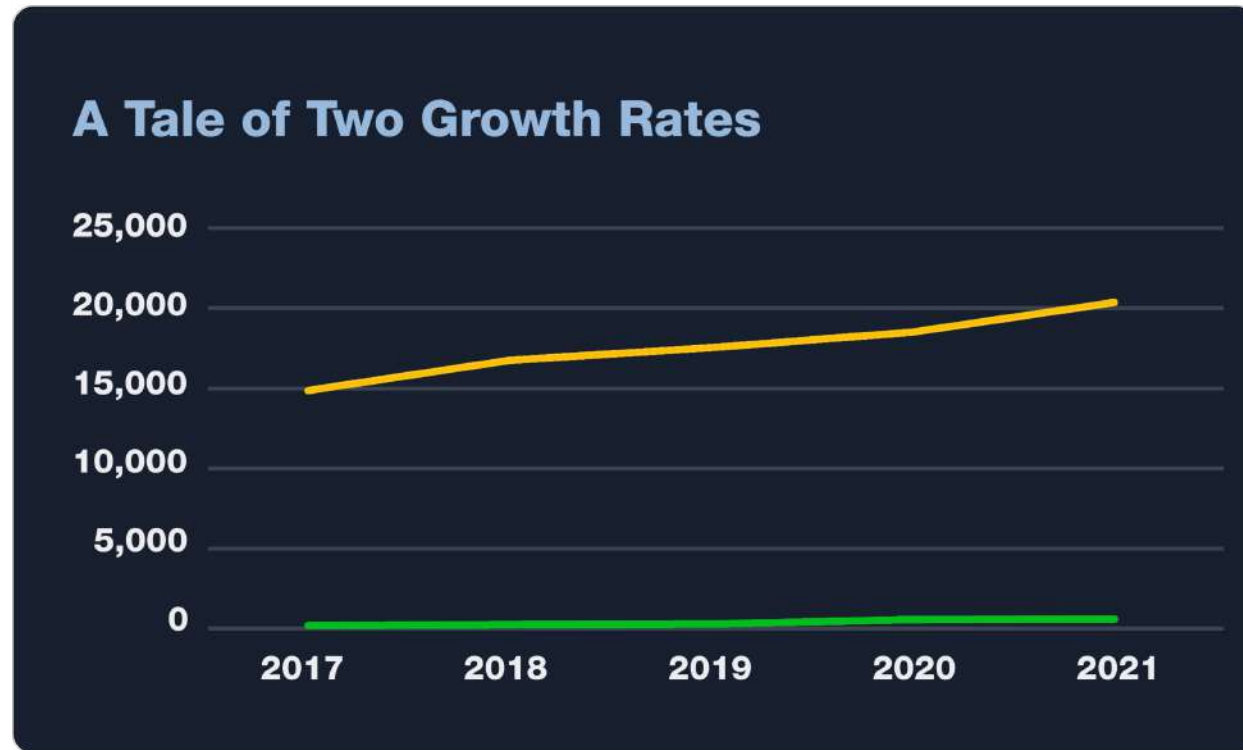
- Understanding adversary tactics, techniques and procedures is critical to effectively defending your systems
- Without this, you’re left with defending against anything and everything
- Threat-Informed Defense helps you to prioritize where to allocate time and resources for security

† <https://www.tidalcyber.com/blog/threat-informed-defense-what-is-it>

**Why is Threat-Informed
Defense so important?**



Because the Old Way Doesn't Work



- It is not feasible to ensure everything in your enterprise is always fully-patched against exploitable vulnerabilities

● Techniques
in Enterprise
ATT&CK

● CVEs
Issued

Supports Focus & Prioritization

- Threat-Informed Defense allows defenders to focus and prioritize their activities and investments, based on:
 - Specific threats they face including groups, software, campaigns – translated into the specific behaviors they employ
 - How existing defenses stack up against those behaviors
 - Identify key gaps



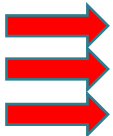
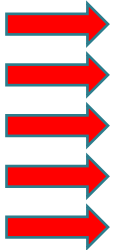
TIDAL

Mind the Gap(s)!

THREATS



BEHAVIORS



DEFENSES



GAPS



TIDAL

**What is the MITRE ATT&CK
knowledge base?**



MITRE ATT&CK

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.†

- ATT&CK is the globally-accepted encyclopedia of adversary behaviors
- ATT&CK serves as a common language to facilitate communication within and between organizations
- ATT&CK is made freely-available by the non-profit MITRE Corporation

† <https://attack.mitre.org/>

MITRE ATT&CK: The Basics

Tactics: the “why” of an adversary’s behavior – their technical objective

...

Persistence

Privilege Escalation

Credential Access

Lateral Movement

...

Techniques: the “how” of an adversary’s behavior – the actions they take to achieve their objective

Create Account

Cloud Account

Domain Account

Local Account

Brute Force

Input Capture

Network Sniffing

Procedures: commands/APIs and parameters used

Sub-Techniques: more specific versions of some techniques

† <https://attack.mitre.org/>

MITRE ATT&CK: The Basics

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 10 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 10 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Scheduled Task/Job	Valid Accounts	Modify Authentication Process	Network Sniffing	System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Gather Victim Host Information	Compromise Accounts	Replication Through Removable Media											
Gather Victim Identity Information	Compromise Infrastructure	Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts	Rootkit	Direct Volume Access	Input Capture	Discovery	Replication Through Removable Media	Data Staged	Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Supply Chain Compromise	Shared Modules	Create or Modify System Process	Event Triggered Execution	Rootkit	Brute Force	System Network Configuration Discovery	Internal Spearphishing	Input Capture	Proxy	Data Transfer Size Limits	Inhibit System Recovery
Gather Victim Org Information	Establish Accounts	Hardware Additions	User Execution	Event Triggered Execution	Boot or Logon Autostart Execution	Obfuscated Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery	Use Alternate Authentication Material	Screen Capture	Communication Through Removable Media	Exfiltration Over C2 Channel	Defacement
Phishing for Information	Obtain Capabilities	Exploit Public-Facing Application	Exploitation for Client Execution	Account Manipulation	Process Injection	Process Injection	Exploitation for Credential Access	System Network Connections Discovery	Lateral Tool Transfer	Email Collection	Web Service Multi-Stage Channels	Exfiltration Over Physical Medium	Firmware Corruption
Search Closed Sources	Stage Capabilities	Phishing	External Remote Services	External Remote Services	Access Token Manipulation	Access Token Manipulation	Steal Web Session Cookie	Permission Groups Discovery	Taint Shared Content	Clipboard Data	Ingress Tool Transfer	Exfiltration Over Web Service	Resource Hijacking
Search Open Technical Databases		External Remote Services	System Services	Office Application Startup	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Unsecured Credentials	Discovery	Automated Collection	Automated Collection	Web Service Multi-Stage Channels	Endpoint Denial of Service	Network Hijacking
Search Open Websites/Domains		Drive-by Compromise	Command and Scripting Interpreter	Create Account	Domain Policy Modification	Domain Policy Modification	Credentials from Password Stores	File and Directory Discovery	Video Capture	Man in the Browser	Data Encoding	System Shutdown/Reboot	Account Access Removal
Search Victim-Owned Websites			Native API	Browser Extensions	Escape to Host	Indicator Removal on Host	Steal or Forge Kerberos Tickets	Peripheral Device Discovery	Man in the Browser	Repositories	Traffic Signaling	Automated Exfiltration	Disk Wipe
			Inter-Process Communication	Traffic Signaling	Exploitation for Privilege Escalation	Trusted Developer Utilities Proxy Execution	Forced Authentication	Network Share Discovery	Remote Service Session Hijacking	Data from Information Repositories	Remote Access Software	Exfiltration Over Alternative Protocol	Data Manipulation
			Container Administration Command	Server Software Component		Traffic Signaling	Signed Script Proxy Execution	Password Policy Discovery		Man in the Middle	Dynamic Resolution	Transfer Data to Cloud Account	
			Deploy Container	Pre-OS Boot		Trusted Developer Utilities Proxy Execution	Man-in-the-Middle	Browser Bookmark Discovery		Forge Web Credentials	Non-Standard Port		
				Compromise Client Software Binary		Rogue Domain Controller	Forge Web Credentials	Virtualization/Sandbox Evasion			Protocol Tunneling		
				Implant Container Image		Indirect Command Execution		Cloud Service Dashboard			Encrypted Channel		
				Modify Authentication Process		Execution		Software Discovery			Non-Application Layer Protocol		
						BITS Jobs		Query Registry					
						XSL Script Processing		Remote System Discovery					
						Template Injection		Network Service Scanning					
						File and Directory Permissions Modification		Process Discovery					
						Virtualization/Sandbox Evasion		System Information Discovery					
						Unused/Unsupported Cloud Regions		Account Discovery					
						Use Alternate Authentication Material		System Time Discovery					
						Impair Defenses		Domain Trust Discovery					
						Hide Artifacts		Cloud Service Discovery					
						Masquerading		Container and Resource Discovery					
						Decfuscate/Decode Files or Information		Cloud Infrastructure Discovery					
						Signed Binary Proxy Execution		System Location Discovery					
						Execution							
						Exploitation for Defense Evasion							
						Execution Guardrails							
						Modify Cloud Compute Infrastructure							
						Pre-OS Boot							
						Subvert Trust Controls							
						Build Image on Host							
						Deploy Container							
						Modify System Image							
						Network Boundary Bridging							
						Weaken Encryption							

= Has sub-techniques

MITRE ATT&CK[®]
Enterprise Framework

attack.mitre.org

† <https://attack.mitre.org/>



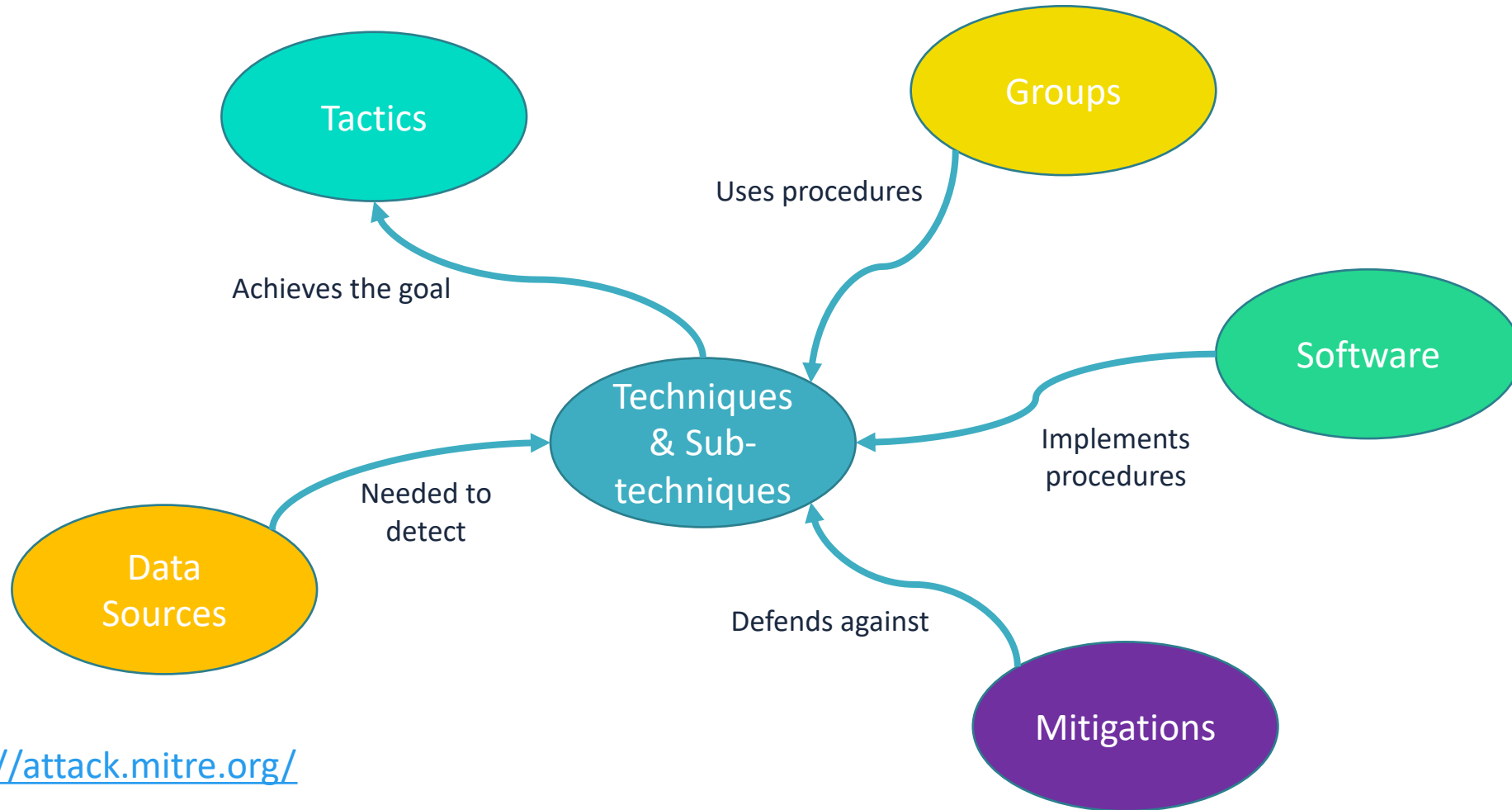
TIDAL

MITRE ATT&CK: Additional Data Resources

- **Groups:** Adversary groups linked to the techniques and software they employ
 - **Procedures:** specific examples of adversary implementations of techniques
- **Software:** Both malware and tools that adversaries use to achieve their objectives
- **Data Sources/Components:** Classification of data types mapped to the techniques they can be used to detect
- **References:** Published reporting cited to support inclusion in ATT&CK

† <https://attack.mitre.org/>

MITRE ATT&CK: Connecting the Dots



† <https://attack.mitre.org/>

MITRE ATT&CK: Benefits & Limitations

ATT&CK Benefits

- Provides a common foundation for threat-informed defense across geographic and sectorial boundaries
- Level of abstraction – tactics, techniques and sub-techniques balances specificity with manageable size/scope
- Vibrant community with many freely-available resources

ATT&CK Realities

- MITRE relies on open-source reporting and community contributions as their inputs
 - Implication: it isn't exhaustive (but nothing is) – think of it as a great starting point
- MITRE updates ATT&CK twice a year
 - Typically in April & October
- Level of abstraction – tactics, techniques and sub-techniques may not convey enough detail (i.e. procedures)
- Not all ATT&CK techniques are created equal
 - Some techniques are more important than others

ATT&CK Realities

TIDAL Search... QakBot Infectio... Shared By TropChaud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Exploit Public-Facing Application	Command and Scripting Interpreter (8)	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Deobfuscate/Decode Files or Information	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Browser Session Hijacking	Application Layer Protocol (4)	Exfiltration Over C2 Channel
Phishing (3)	JavaScript	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder	Hijack Execution Flow (12)	Credentials from Password Stores (5)	Local Account	Remote Services (6)	Data from Local System	DNS	
Spearphishing Attachment	PowerShell	Hijack Execution Flow (12)	Exploitation for Privilege Escalation	DLL Side-Loading	Credentials from Web Browsers	Application Window Discovery	VNC	Data Staged (2)	Web Protocols	
Spearphishing Link	Visual Basic	DLL Side-Loading	Hijack Execution Flow (12)	Impair Defenses (9)	Input Capture (4)	Domain Trust Discovery	Replication Through Removable Media	Local Data Staging	Data Encoding (2)	
Replication Through Removable Media	Windows Command Shell	Scheduled Task/Job (5)	DLL Side-Loading	Disable or Modify Tools	Keylogging	File and Directory Discovery	Use Alternate Authentication Material (4)	Email Collection (3)	Standard Encoding	
	Native API	Scheduled Task	Process Injection (12)	Indicator Removal (9)	OS Credential Dumping (8)	Network Share Discovery	Pass the Hash	Local Email Collection	Dynamic Resolution (3)	
	Scheduled Task/Job (5)		Dynamic-Link Library Injection	File Deletion	LSASS Memory	Peripheral Device Discovery		Input Capture (4)	Domain Generation Algorithms	
	Scheduled Task		Process Hollowing	Masquerading (7)	Steal Web Session Cookie	Permission Groups Discovery (3)		Keylogging	Encrypted Channel (2)	
	System Services (2)		Scheduled Task/Job (5)	Modify Registry		Domain Groups			Symmetric Cryptography	
	Service Execution		Scheduled Task	Obfuscated Files or Information (9)		Local Groups			Ingress Tool Transfer	
	User Execution (3)			Binary Padding					Non-Application Layer Protocol	
	Malicious File			HTML Smuggling					Non-Standard Port	
	Malicious Link			Indicator Removal from Tools					Protocol Tunneling	
	Windows Management Instrumentation			Software Packing					Proxy (4)	
				Process Injection (12)					External Proxy	
				Dynamic-Link Library Injection					Multi-hop Proxy	
				Process Hollowing					Remote Access Software	



Implementing Threat- Informed Defense

Step One: Identify your threats: Groups

The screenshot shows the TIDAL interface for identifying threat groups. The top navigation bar includes the TIDAL logo, a search bar, and a user profile icon. Below the navigation bar, there is a breadcrumb trail 'Home > Groups' and a 'Groups' section. The 'Groups' section features a search bar and several filter dropdowns: 'Motivation', 'Suspected Attribution' (set to 'Russia'), 'Observed Sectors' (set to 'Energy'), and 'Observed Countries'. Below the filters is a table of threat groups. The 'APT29' group is highlighted with a red circle. The table columns are: Name, Associated Groups, Motivation, Suspected Attribution, Observed Sectors, Observed Countries, and Add to Matrix.

Name	Associated Groups	Motivation	Suspected Attribution	Observed Sectors	Observed Countries	Add to Matrix
APT28	SNAKEMACKEREL, Swallowtail, Group 74 ...		Russia	Aerospace, Chemical, Defense ...	Afghanistan , France ...	<input type="checkbox"/>
APT29	IRON RITUAL, IRON HEMLOCK, Dark Halo ...	Cyber Espionage	Russia	Aerospace, Education, Energy ...	Austria , Brazil ...	<input checked="" type="checkbox"/>
Dragonfly	TEMP.Isotope, DYMALLOY, TG-4192 ...	Cyber Espionage	Russia	Energy, Government, Travel Services	France , Germany ...	<input type="checkbox"/>
Sandworm Team	ELECTRUM, IRON VIKING, BlackEnergy (Group) ...	Destruction	Russia	Energy, Government	France , Georgia ...	<input type="checkbox"/>
Wizard Spider	UNC1878, TEMP.MixMaster, Grim Spider	Financial Gain	Russia	Aerospace, Agriculture, Automotive ...	Australia , Belgium ...	<input type="checkbox"/>

Step One: Identify your threats: Groups

The screenshot shows the TIDAL interface for the APT29 group. The top navigation bar includes the TIDAL logo, a search bar, and a user profile icon. Below the navigation bar, there is a breadcrumb trail: Home > Groups > APT29. The main content area is titled 'Groups' and features a large 'APT29' header with a 'REMOVE FROM MATRIX' button. Below the header, there are several sections: 'Suspected Attribution: Russia', 'Motivation: Cyber Espionage', 'Observed Countries: Austria, Brazil, China, France, Germany, Hungary, Japan, Republic of Korea, Mexico, Netherlands, New Zealand, Norway, Portugal, Spain, Turkey, Ukraine, United Kingdom, United States, Uzbekistan', 'Observed Sectors: Aerospace, Education, Energy, Financial Services, Government, Insurance, Legal, Manufacturing, Media, NGOs, Non Profit, Pharmaceuticals, Technology, Telecommunications, Think Tanks', and 'Sources: MITRE, Tidal Cyber'. A detailed paragraph follows, starting with 'APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR)...'. Below the paragraph, there are four links: 'Associated Groups (11)', 'Techniques (106)', 'Software (47)', and 'References (49)'. The 'Software (47)' link is circled in red. Below these links is a table with two columns: 'Name' and 'Description'. The first row of the table shows 'AADInternals' and '[MSTIC Nobelium Oct 2021]'. The TIDAL logo is visible in the bottom right corner of the page.

Home > Groups > APT29

Groups

APT29

REMOVE FROM MATRIX

Suspected Attribution: Russia

Motivation: Cyber Espionage

Observed Countries: Austria, Brazil, China, France, Germany, Hungary, Japan, Republic of Korea, Mexico, Netherlands, New Zealand, Norway, Portugal, Spain, Turkey, Ukraine, United Kingdom, United States, Uzbekistan

Observed Sectors: Aerospace, Education, Energy, Financial Services, Government, Insurance, Legal, Manufacturing, Media, NGOs, Non Profit, Pharmaceuticals, Technology, Telecommunications, Think Tanks

Sources: MITRE, Tidal Cyber

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).^{[White House Imposing Costs RU Gov April 2021][UK Gov Malign RIS Activity April 2021]} They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.^{[F-Secure The Dukes][GRIZZLY STEPPE JAR][Crowdstrike DNC June 2016][UK Gov UK Exposes Russia SolarWinds April 2021]}

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.^{[NSA Joint Advisory SVR SolarWinds April 2021][UK NSCS Russia SolarWinds April 2021]} Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.^{[FireEye SUNBURST Backdoor December 2020][MSTIC NOBELIUM Mar 2021][CrowdStrike SUNSPOT Implant January 2021][Volatility SolarWinds][Cybersecurity Advisory SVR TTP May 2021]}

Associated Groups (11) Techniques (106) **Software (47)** References (49)

↑ Name	Description
AADInternals	[MSTIC Nobelium Oct 2021]



Step One: Identify your threats: Software

The screenshot shows the TIDAL interface. At the top, there is a dark blue header with the TIDAL logo on the left, a search bar in the center, and a user profile icon on the right. Below the header is a light blue navigation bar containing a 'Draft' dropdown, two active threat cards labeled 'GR APT29' and 'SW Cobalt S...', a plus sign, and a notification icon with the number '2'. The main content area has a breadcrumb trail: 'Home > Software > Cobalt Strike'. The title 'Software Cobalt Strike' is displayed, with a 'REMOVE FROM MATRIX' button to its right. Below the title, the following details are listed: 'Type: malware', 'Platform(s): Linux, macOS, Windows', and 'Source: MITRE'. A descriptive paragraph follows: 'Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system. [cobaltstrike manual]'. Another paragraph states: 'In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz. [cobaltstrike manual]'. Below this is a filter bar with 'Associated Software (0)' selected, and other filters for 'Techniques (115)', 'Groups (28)', and 'References (63)'. A message reads 'There are no items to display'. At the bottom, a table shows the following data: ID: S0154, Version: 1.8, Created Date: 14 December 2017, Last Modified: 25 February 2022, 06:58 PM GMT. The footer contains the copyright notice: '© 2022 Tidal Cyber Inc. All rights reserved. | Terms of Service | MITRE ATT&CK® is a registered trademark of The MITRE Corporation.' The TIDAL logo is also present in the bottom right corner.

Home > Software > Cobalt Strike

Software

Cobalt Strike

REMOVE FROM MATRIX

Type: malware
Platform(s): Linux, macOS, Windows
Source: MITRE

Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system. [cobaltstrike manual]

In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz. [cobaltstrike manual]

Associated Software (0) Techniques (115) Groups (28) References (63)

There are no items to display

ID: S0154	Version: 1.8	Created Date: 14 December 2017	Last Modified: 25 February 2022, 06:58 PM GMT
-----------	--------------	--------------------------------	---

© 2022 Tidal Cyber Inc. All rights reserved. | Terms of Service | MITRE ATT&CK® is a registered trademark of The MITRE Corporation.



Step One: Identify your threats: Combined

The screenshot displays the TIDAL threat intelligence platform interface. At the top, there is a navigation bar with the TIDAL logo, a search bar, and user profile icons. Below the navigation bar, there are tabs for 'Draft', 'GR APT29', and 'SW Cobalt S...', along with a plus sign and a notification icon showing '2'.

The main content area is a grid of 12 columns, each representing a threat category. Each category contains a list of sub-techniques or methods, with some items having a count in parentheses next to them. The categories and their sub-techniques are:

- Reconnaissance**: Active Scanning (3), Vulnerability Scanning, Gather Victim Identity Information (3), Credentials.
- Resource Development**: Acquire Infrastructure (6), Domains, Web Services, Compromise Accounts (2), Email Accounts, Compromise Infrastructure (6), Domains, Develop Capabilities (4), Digital Certificates, Malware, Obtain Capabilities (6), Tool.
- Initial Access**: Exploit Public-Facing Application, External Remote Services, Phishing (3), Spearphishing Attachment, Spearphishing Link, Spearphishing via Service, Supply Chain Compromise (3), Compromise Software Supply Chain, Trusted Relationship, Valid Accounts (4), Cloud Accounts, Domain Accounts, Local Accounts.
- Execution**: Command and Scripting Interpreter (8), JavaScript, PowerShell, Python, Visual Basic, Windows Command Shell, Exploitation for Client Execution, Native API, Scheduled Task/Job (5), Scheduled Task, System Services (2), Service Execution, User Execution (3), Malicious File, Malicious Link, Windows Management Instrumentation.
- Persistence**: Account Manipulation (5), Additional Cloud Credentials, Additional Cloud Roles, Additional Email Delegate Permissions, Device Registration, BITS Jobs, Boot or Logon Autostart Execution (14), Registry Run Keys / Startup Folder, Shortcut Modification, Create Account (3), Cloud Account, Create or Modify System Process (4), Windows Service, Event Triggered Execution (15), Domain Trust.
- Privilege Escalation**: Abuse Elevation Control Mechanism (4), Bypass User Account Control, Sudo and Sudo Caching, Access Token Manipulation (5), Make and Impersonate Token, Parent PID Spoofing, Token Impersonation/Theft, Boot or Logon Autostart Execution (14), Registry Run Keys / Startup Folder, Shortcut Modification, Create or Modify System Process (4), Windows Service, Domain Policy Modification (2), Domain Trust.
- Defense Evasion**: Abuse Elevation Control Mechanism (4), Bypass User Account Control, Sudo and Sudo Caching, Access Token Manipulation (5), Make and Impersonate Token, Parent PID Spoofing, Token Impersonation/Theft, BITS Jobs, Deobfuscate/Decode Files or Information, Domain Policy Modification (2), Domain Trust Modification, Hide Artifacts (10), Process Argument Spoofing, Impair Defenses.
- Credential Access**: Brute Force (4), Password Spraying, Credentials from Password Stores (5), Credentials from Web Browsers, Forge Web Credentials (2), SAML Tokens, Web Cookies, Input Capture (4), Keylogging, Multi-Factor Authentication Request Generation, OS Credential Dumping (8), DCSync, LSASS Memory, Security Account Manager, Steal or Forge Kerberos Tickets (4).
- Discovery**: Account Discovery (4), Cloud Account, Domain Account, Domain Trust Discovery, File and Directory Discovery, Network Service Discovery, Network Share Discovery, Permission Groups Discovery (3), Domain Groups, Local Groups, Process Discovery, Query Registry, Remote System Discovery, Software Discovery (1).
- Lateral Movement**: Remote Services (6), Distributed Component Object Model, Remote Desktop Protocol, SMB/Windows Admin Shares, SSH, Windows Remote Management, Use Alternate Authentication Material (4), Application Access Token, Pass the Hash, Pass the Ticket, Web Session Cookie.
- Collection**: Archive Collected Data (3), Archive via Utility, Browser Session Hijacking, Data from Information Repositories (3), Code Repositories, Data from Local System, Data Staged (2), Remote Data Staging, Email Collection (3), Remote Email Collection, Input Capture (4), Keylogging, Screen Capture.
- Command and Control**: Application Layer Protocol (4), DNS, Web Protocols, Data Encoding (2), Standard Encoding, Data Obfuscation (3), Protocol Impersonation, Steganography, Dynamic Resolution (3), Encrypted Channel (2), Asymmetric Cryptography, Symmetric Cryptography, Ingress Tool Transfer, Non-Application Layer Protocol.

Step Two: Inventory your defenses: Detections


The screenshot shows the TIDAL interface. At the top, there is a search bar and a navigation menu. Below the search bar, there are several product cards: 'Draft', 'GR APT29', 'SW Cobalt S...', and 'PR Sysmon...'. The main content area displays the 'Sysmon-Modular' product page. The product name is 'Sysmon-Modular' and it features a fox head icon. The page includes a 'REMOVE FROM MATRIX' button and a notification that the item has been added to the matrix. Below the product name, there is a list of tactics covered, capability types, vendor, product version, and source. A detailed description of the product is provided, along with a link to the MIT License. At the bottom, there are filters for 'Capabilities (142)' and 'Product Data Source (105)', and a table with columns for Capability, Type, Technique, Platform, Description, and Availability.

Home > Product Registry > Olaf Hartong > Sysmon-Modular

Product

This item has been added to the matrix

REMOVE FROM MATRIX

 Sysmon-Modular

Tactic(s) Covered: [Initial Access](#), [Execution](#), [Persistence](#), [Privilege Escalation](#), [Defense Evasion](#), [Credential Access](#), [Discovery](#), [Lateral Movement](#), [Collection](#), [Command and Control](#), [Impact](#)

Capability Type(s): Detect

Vendor: [Olaf Hartong](#)

Product Version:

Source: Olaf Hartong

Sysmon-modular is a configuration repository, mapped to MITRE ATT&CK, to be used with [Sysinternals Sysmon](#). The project has been set up in a modular fashion which allows for easier maintenance and the generation of specific configs. For instance, one for servers, one for workstations and one to only to be used in an Incident Response scenario. Please note this is a possible log entry that might lead to a detection, not in all cases will this be the only telemetry for that technique. Additionally there might be more techniques related to that rule, there is only one mapped, this is the one deemed most likely by the author.

This product is licensed under the [MIT License](#)

[Capabilities \(142\)](#) [Product Data Source \(105\)](#)

Filter By: [Detect](#)

Capability	Type	Technique	Platform	Description	Availability
------------	------	-----------	----------	-------------	--------------

Step Two: Inventory your defenses: Tests

The screenshot displays the TIDAL web application interface. At the top, there is a dark blue header with the TIDAL logo on the left, a search bar in the center, and a user profile icon on the right. Below the header, a navigation bar shows a 'Draft' dropdown and several product cards with colored status indicators: 'GR APT29', 'SW Cobalt S...', 'PR Sysmon...', and 'PR Invoke-...'. A '4' notification badge is visible on the right side of the navigation bar.

The main content area is titled 'Atomic Red Team'. It features a red circular logo with a white atomic symbol and a red bird. The text includes 'Atomic Red Team', 'Last Updated: July 14, 2022', 'Source: Atomic Red Team', and a description: 'Atomic Red Team™ is a library of tests mapped to the MITRE ATT&CK® framework. Security teams can use Atomic Red Team to quickly, portably, and reproducibly test their environments.' Below this, the 'Capability Type' is listed as 'Test'. On the right side, there are two buttons: 'ADD TO MATRIX' and 'VISIT WEBSITE'.

Below the main content, there is a search bar labeled 'Search in products' and a dropdown menu for 'Capability Type'. The 'Products' section is titled 'Products' and contains a card for 'Invoke-Atomic'. This card has the same red atomic logo and includes the following information: 'Invoke-Atomic', 'Last Updated: 14 July 2022, 01:16 PM GMT', 'Product Version: v1.0.2', and 'Tactics Covered: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact'. At the bottom of the card, the 'Capability Type' is 'Test' with a '1065' badge. To the right of the card are two buttons: 'REMOVE FROM MATRIX' and 'VIEW DETAIL'.

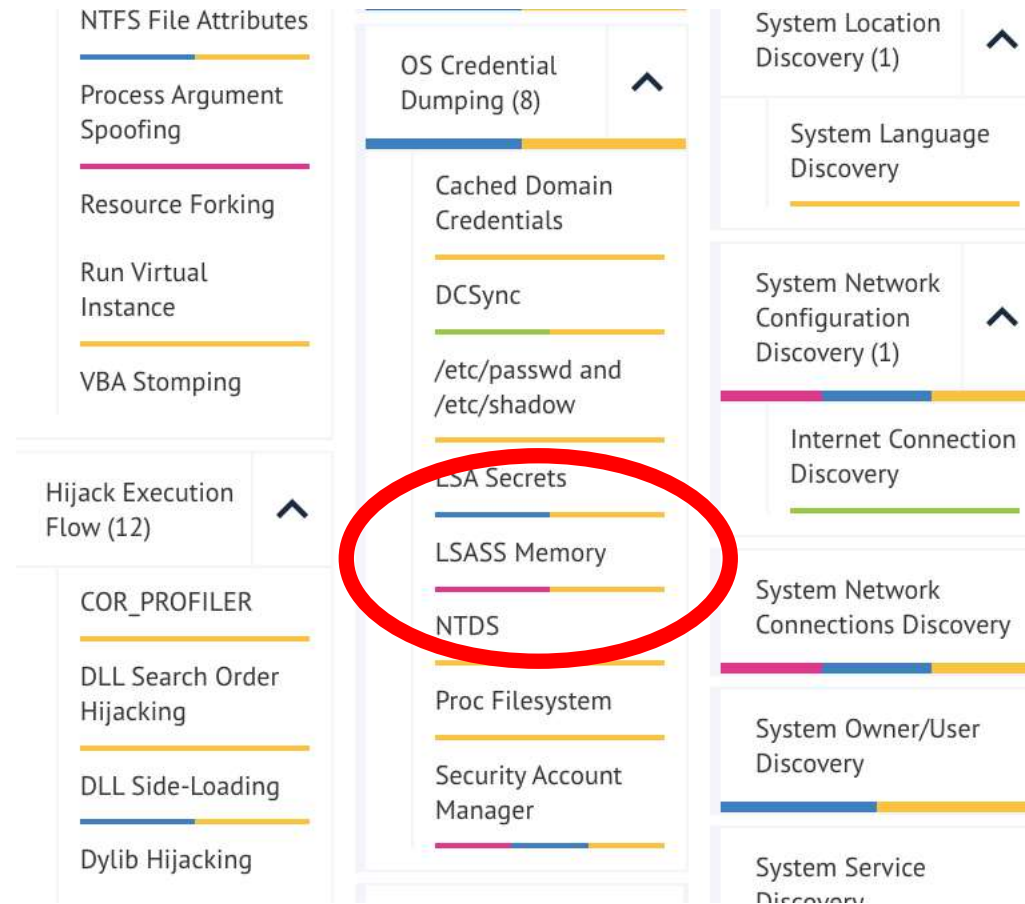
Step Three: Assess your Coverage

The screenshot displays the TIDAL Cybersecurity Dashboard interface. At the top, there is a search bar and a navigation menu with a 'Draft' dropdown and several project tabs: 'GR APT29', 'SW Cobalt S...', 'PR Sysmon...', and 'PR Invoke...'. Below the navigation, the dashboard is organized into a grid of 12 columns, each representing a different phase of the cyber attack lifecycle. Each column contains a list of specific techniques with associated progress bars and status indicators.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
Active Scanning (3) Scanning IP Blocks Vulnerability Scanning Wordlist Scanning Gather Victim Host Information (4) Gather Victim Identity Information (3) Credentials Email Addresses Employee Names Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (5)	Acquire Infrastructure (6) Botnet DNS Server Domains Server Virtual Private Server Web Services Compromise Accounts (2) Email Accounts Social Media Accounts Compromise Infrastructure (6) Botnet DNS Server Domains Server Virtual Private Server Web Services Develop Capabilities (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Spearphishing Attachment Spearphishing Link Spearphishing via Service Replication Through Removable Media Supply Chain Compromise (3) Compromise Hardware Supply Chain Compromise Software Dependencies and Development Tools Compromise Software Supply Chain	Command and Scripting Interpreter (8) AppleScript JavaScript Network Device CLI PowerShell Python Unix Shell Visual Basic Windows Command Shell Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Component Object Model Dynamic Data Exchange XPC Services	Account Manipulation (5) Additional Cloud Credentials Additional Cloud Roles Additional Email Delegate Permissions Device Registration SSH Authorized Keys BITS Jobs Boot or Logon Autostart Execution (14) Active Setup Authentication Package Kernel Modules and Extensions Login Items LSASS Driver Port Monitors Print Processors Registry Run Keys / Startup Folder	Abuse Elevation Control Mechanism (4) Bypass User Account Control Elevated Execution with Prompt Setuid and Setgid Sudo and Sudo Caching Access Token Manipulation (5) Create Process with Token Make and Impersonate Token Parent PID Spoofing SID-History Injection Token Impersonation/Theft Boot or Logon Autostart Execution (14) Active Setup Authentication Package Kernel Modules and Extensions	Abuse Elevation Control Mechanism (4) Bypass User Account Control Elevated Execution with Prompt Setuid and Setgid Sudo and Sudo Caching Access Token Manipulation (5) Create Process with Token Make and Impersonate Token Parent PID Spoofing SID-History Injection Token Impersonation/Theft BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information	Adversary-in-the-Middle (3) ARP Cache Poisoning DHCP Spoofing LLMNR/NBT-NS Poisoning and SMB Relay Brute Force (4) Credential Stuffing Password Cracking Password Guessing Password Spraying Credentials from Password Stores (5) Credentials from Web Browsers Keychain Password Managers Securityd Memory Windows Credential Manager Exploitation for Credential Access	Account Discovery (4) Cloud Account Domain Account Email Account Local Account Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Domain Trust Discovery File and Directory Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Services (6) Distributed Component Object Model Remote Desktop Protocol SMB/Windows Admin Shares SSH VNC Windows Remote Management Remote Service Session Hijacking (2) RDP Hijacking SSH Hijacking Replication Through Removable Media Software Deployment Tools	Adversary-in-the-Middle (3) ARP Cache Poisoning DHCP Spoofing LLMNR/NBT-NS Poisoning and SMB Relay Archive Collected Data (3) Archive via Custom Method Archive via Library Archive via Utility Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2)	Application Layer Protocol (4) DNS File Transfer Protocols Mail Protocols Web Protocols Communication Through Removable Media Data Encoding (2) Non-Standard Encoding Standard Encoding Data Obfuscation (5) Junk Data Protocol Impersonation Steganography Dynamic Resolution (3) DNS Calculation Domain Generation



Step Four: Address Gaps – LSASS



Step Four: Address Gaps – OSS Analytics

Technique Preview ×

LSASS Memory




[VIEW DETAILS](#)

ID: T1003.001
Tactic(s): [Credential Access](#)
Platform(s): Windows
Parent-Technique: [OS Credential Dumping](#)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](#) using [Use Alternate Authentication Material...](#)



Vendors

Filter By: [Test](#)

  
Atomic Red Team AttackIQ SCYTHE

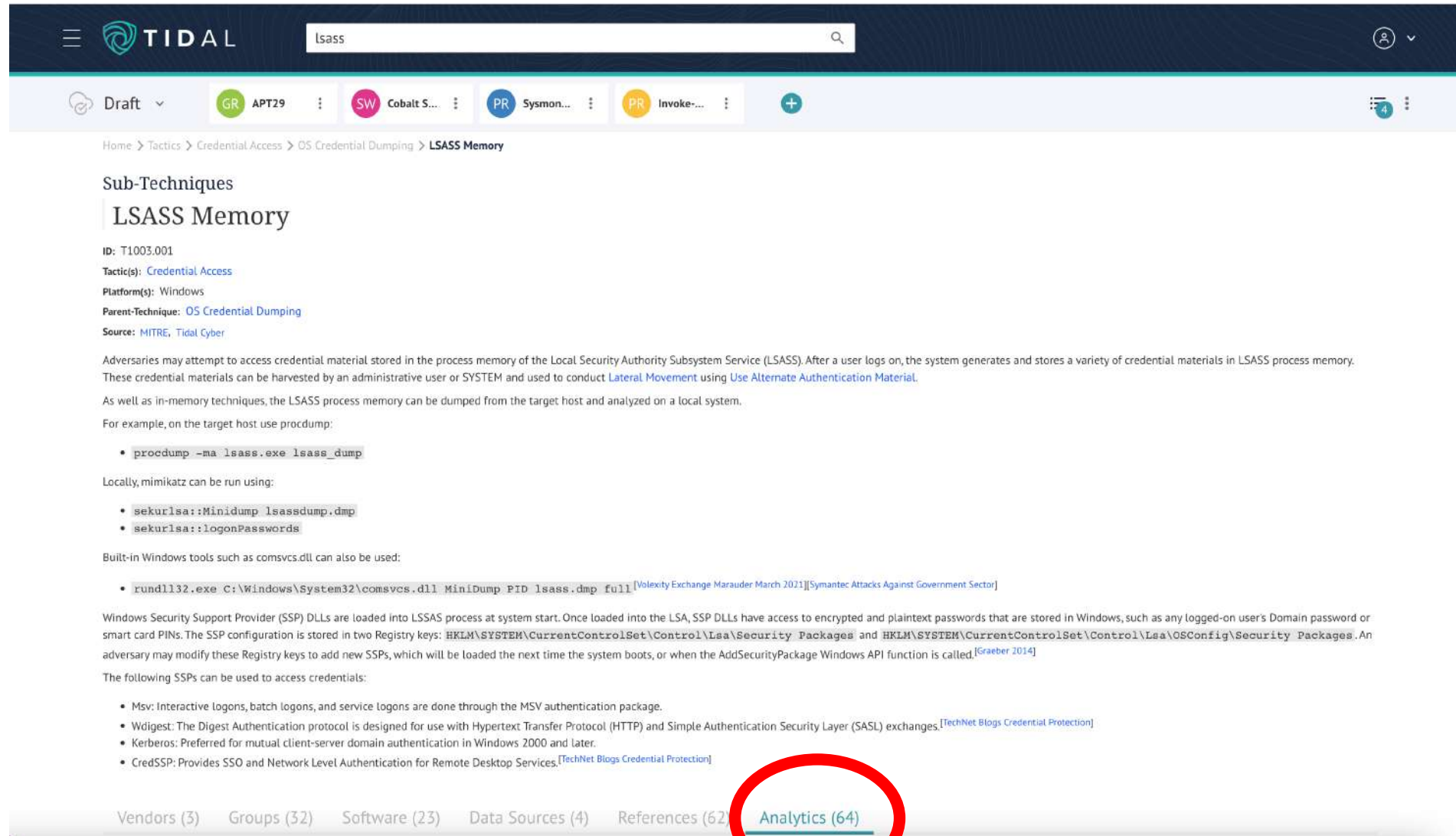
Labels

Filter By: [All\(2\)](#) [Software\(1\)](#) [Product\(1\)](#)

 [Cobalt Strike](#)  [Invoke-Atomics](#)

Category	Count
Groups	32
Software	23
Data Sources	4
Analytics	64

Step Four: Address Gaps – OSS Analytics



Home > Tactics > Credential Access > OS Credential Dumping > LSASS Memory

Sub-Techniques

LSASS Memory

ID: T1003.001
Tactic(s): [Credential Access](#)
Platform(s): Windows
Parent-Technique: [OS Credential Dumping](#)
Source: [MITRE](#), [Tidal Cyber](#)

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](#) using [Use Alternate Authentication Material](#).

As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system.

For example, on the target host use procdump:

- `procdump -ma lsass.exe lsass_dump`

Locally, mimikatz can be run using:

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonpasswords`

Built-in Windows tools such as comsvcs.dll can also be used:

- `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full` [Volexity Exchange Marauder March 2011][Symantec Attacks Against Government Sector]

Windows Security Support Provider (SSP) DLLs are loaded into LSSAS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the `AddSecurityPackage` Windows API function is called. [Graeber 2014]

The following SSPs can be used to access credentials:

- MsV: Interactive logons, batch logons, and service logons are done through the MSV authentication package.
- Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. [TechNet Blogs Credential Protection]
- Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later.
- CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services. [TechNet Blogs Credential Protection]

Vendors (3) Groups (32) Software (23) Data Sources (4) References (62) **Analytics (64)**



Step Four: Address Gaps- Add Sigma rules

github.com/SigmaHQ/sigma/blob/7853f93862304e65310e0c292ebb211f715857cb/rules/windows/process_access/proc_access_win_cred_dump_lsass_access.yml

SigmaHQ / sigma Public Sponsor Notifications Fork 1.6k Star 5.5k

<> Code Issues 76 Pull requests 24 Discussions Actions Wiki Security Insights

7853f93862 sigma / rules / windows / process_access / proc_access_win_cred_dump_lsass_access.yml Go to file

phantinuss fix: FPs found in testing environment Latest commit 9475153 on Jun 20 History

3 contributors

Executable File | 130 lines (130 sloc) | 4.56 KB Raw Blame

```
1 title: Credentials Dumping Tools Accessing LSASS Memory
2 id: 32d0d3e2-e58d-4d41-926b-18b520b2b32d
3 status: experimental
4 description: Detects process access LSASS memory which is typical for credentials dumping tools
5 author: Florian Roth, Roberto Rodriguez, Dimitrios Slamaris, Mark Russinovich, Thomas Patzke, Teymur Kheirkhabarov, Sherif Eldeeb, James Dickenson, Aleksey Pota
6 oscd.community (update)
7 date: 2017/02/16
8 modified: 2022/06/20
9 references:
10 - https://onedrive.live.com/view.aspx?resid=D026B4699190F1E6!2843&ithint=file%2cpptx&app=PowerPoint&authkey=!AMVCRtKB_V1J5ov
11 - https://cyberwardog.blogspot.com/2017/03/chronicles-of-threat-hunter-hunting-for_22.html
12 - https://www.slideshare.net/heirhabarov/hunting-for-credentials-dumping-in-windows-environment
13 - http://security-research.dyndns.org/pub/slides/FIRST2017/FIRST-2017_Tom-Ueltschi_Sysmon_FINAL_notes.pdf
14 tags:
15 - attack.credential_access
16 - attack.t1003.001
17 - attack.s0002
18 - car.2019-04-004
19 logsource:
20 category: process_access
21 product: windows
22 detection:
23 selection:
24 TargetImage|endswith: '\\lsass.exe'
25 GrantedAccess|startswith:
26 - '0x40'
27 # - '0x1000' # minimum access requirements to query basic info from service
28 # - '0x1400'
29 - '0x100000'
```



Step Five: Verify Defenses – run ART tests

Invoke-Atomic

Tactic(s) Covered: [Credential Access](#)

Capability Type(s): Test

Vendor: [Atomic Red Team](#)

Product Version: v1.0.2

Source: Atomic Red Team

Invoke-AtomicRedTeam is a PowerShell module to execute tests as defined in the atomics folder of Red Canary's Atomic Red Team project. Visit the [GitHub repository](#) for Invoke-Atomic for installation and usage instructions.

This product is licensed under the [MIT license](#)

Capabilities (12) Product Data Source (0)

Filter By: Test Capabilities shown for "LSASS Memory"

Capability	Type	Technique	Platform	Description	Availability
Create Mini Dump of LSASS.exe using ProcDump	Test	LSASS Memory	Windows	The memory of lsass.exe is often dumped for offline c...	Default-Off
Dump LSASS with .Net 5 createdump.exe	Test	LSASS Memory	Windows	This test uses the technique describe in this tweet (ht...	Default-Off
Dump LSASS.exe Memory using comsvcs.dll	Test	LSASS Memory	Windows	The memory of lsass.exe is often dumped for offline c...	Default-Off

Step Six: Go To Step 1

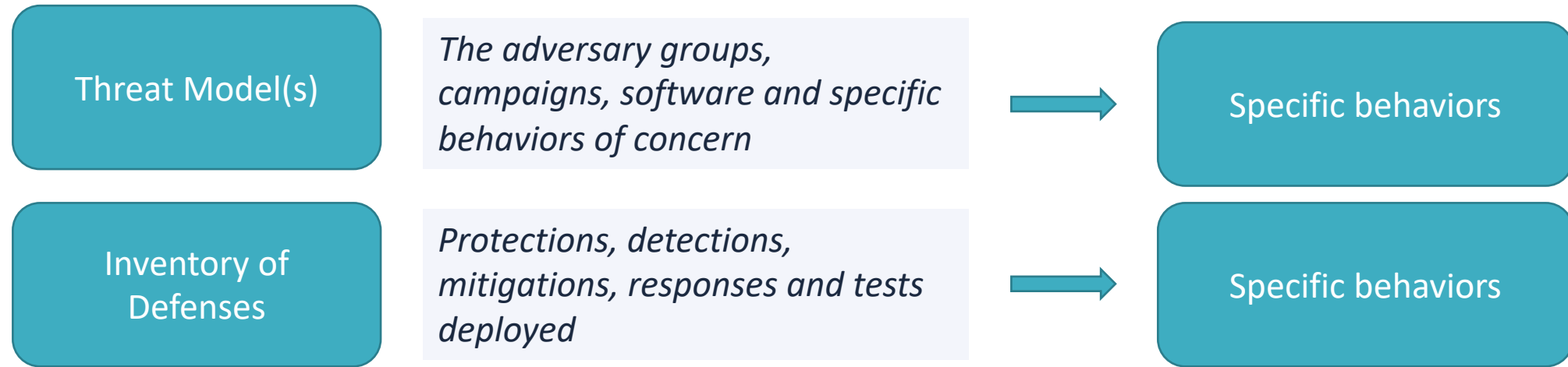
- Threat-Informed Defense is an iterative, continuous process
- The environment is always changing
 - Evolution in threats – new groups, new behaviors, new malware
 - Evolution in defenses – new detections, new tests, new analytics
 - New public reporting of both



TIDAL

Putting it All Together into a Threat-Informed Strategy

Foundational Elements



Building a Threat Model

- Goal: Identify the threats to your organization and map those to specific behaviors you can defend against
- Sources of intelligence to drive threat modeling:
 - OSINT / Commercial threat intel sources – based on targeting of sector, geography and technology platforms
 - ISACs/ISAOs
 - Internal knowledge – past incidents, ongoing reconnaissance and probing, etc.



TIDAL

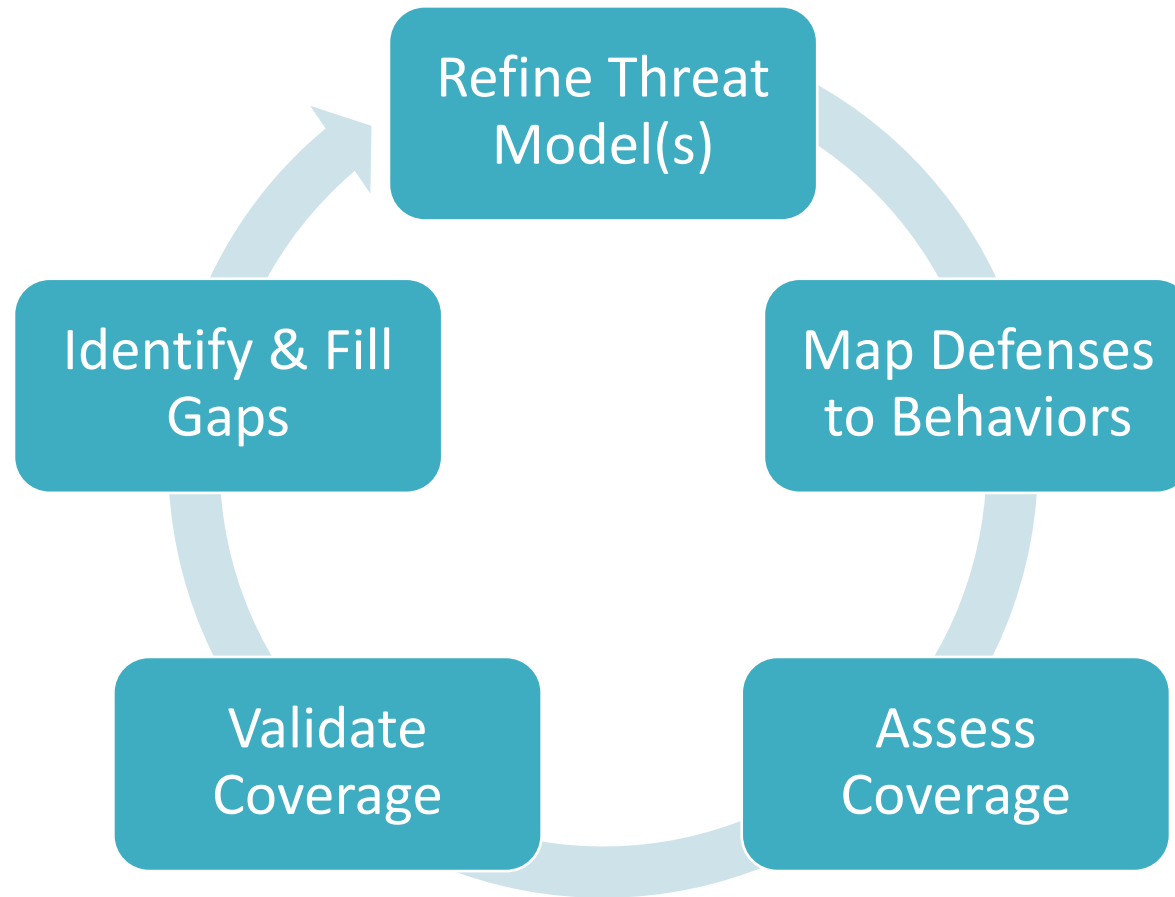
Inventory your Defenses

- Goal: Identify the security policies, controls and technologies deployed and map those to the specific behaviors they are effective against
- Helpful to segment by the type of defense:
 - **Mitigation:** prevents a behavior from being employed
 - **Protection:** blocks a specific behavior from achieving its objective
 - **Detection:** alerts when a behavior is seen in use
 - **Response:** takes corrective action when a behavior is detected
 - **Test:** verify if a specific defense is operating normally



TIDAL

Continuous Evaluation & Adaptation



Closing Thoughts

ATT&CK is a *Means*, not an *End*.

- Don't try to achieve 100% coverage of the entire ATT&CK matrix – you will fail
- ATT&CK isn't a checklist to be blindly followed
- Focus on ATT&CK as the glue that helps you connect and organize your understanding of what adversaries do IRL
- Understand that ATT&CK isn't exhaustive and embrace the fact that you'll want to extend it for yourself



TIDAL

Threat-Informed Defense is a Journey

- Embrace the iterative and continuous nature of threat-informed defense
- Align people, processes and technology to support this ongoing set of activities
- Measure your progress and use that to course correct



Select Community Resources

- MITRE ATT&CK: attack.mitre.org
- Tidal Cyber Community Edition: app.tidalcyber.com
- Atomic Red Team: atomicredteam.io
- SIGMA: github.com/SigmaHQ/sigma
- Sysmon Modular: github.com/olafhartong/sysmon-modular



Inventory your Defenses

- Goal: Identify the security policies, controls and technologies deployed and map those to the specific behaviors they are effective against
- Helpful to segment by the type of defense:
 - **Mitigation:** prevents a behavior from being employed
 - **Protection:** blocks a specific behavior from achieving its objective
 - **Detection:** alerts when a behavior is seen in use
 - **Response:** takes corrective action when a behavior is detected
 - **Test:** verify if a specific defense is operating normally



TIDAL

Thank You!

