THREAT INTELLIGENCE

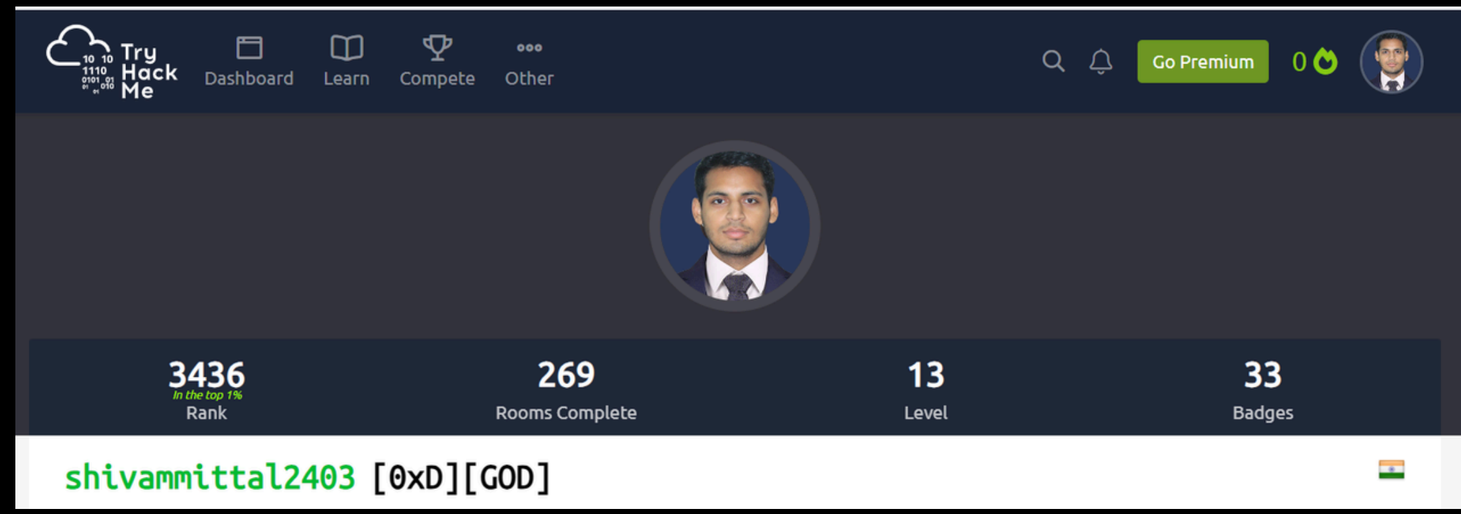
Presented By Shivam

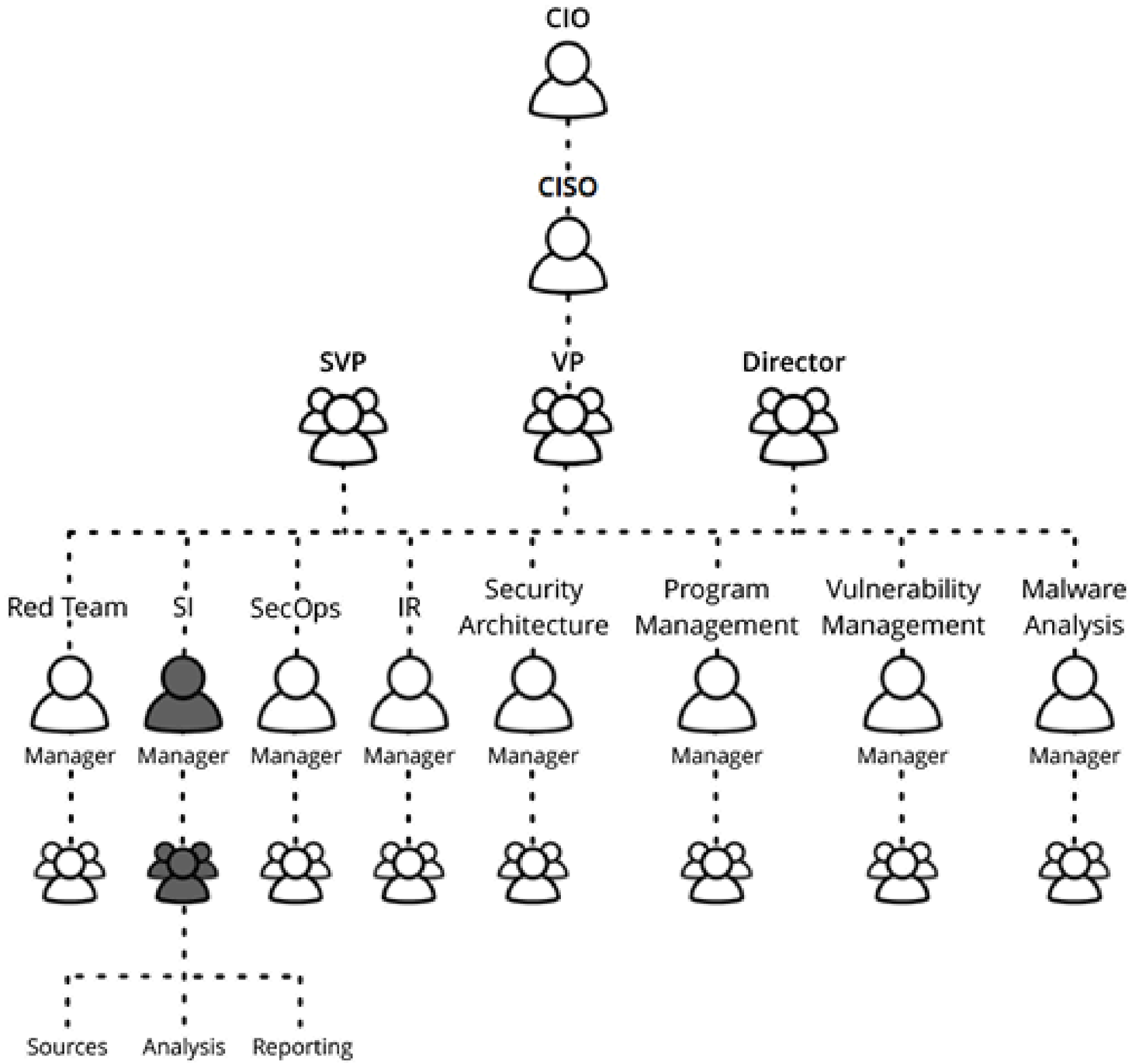
“IMAGINE AN INVISIBLE ENEMY CAPABLE OF BRINGING DOWN COMPANIES, GOVERNMENTS, AND ENTIRE INFRASTRUCTURES—ALL FROM THE SHADOWS. THESE ARE THE THREAT ACTORS IN THE CYBER WORLD.”

WHO AM I

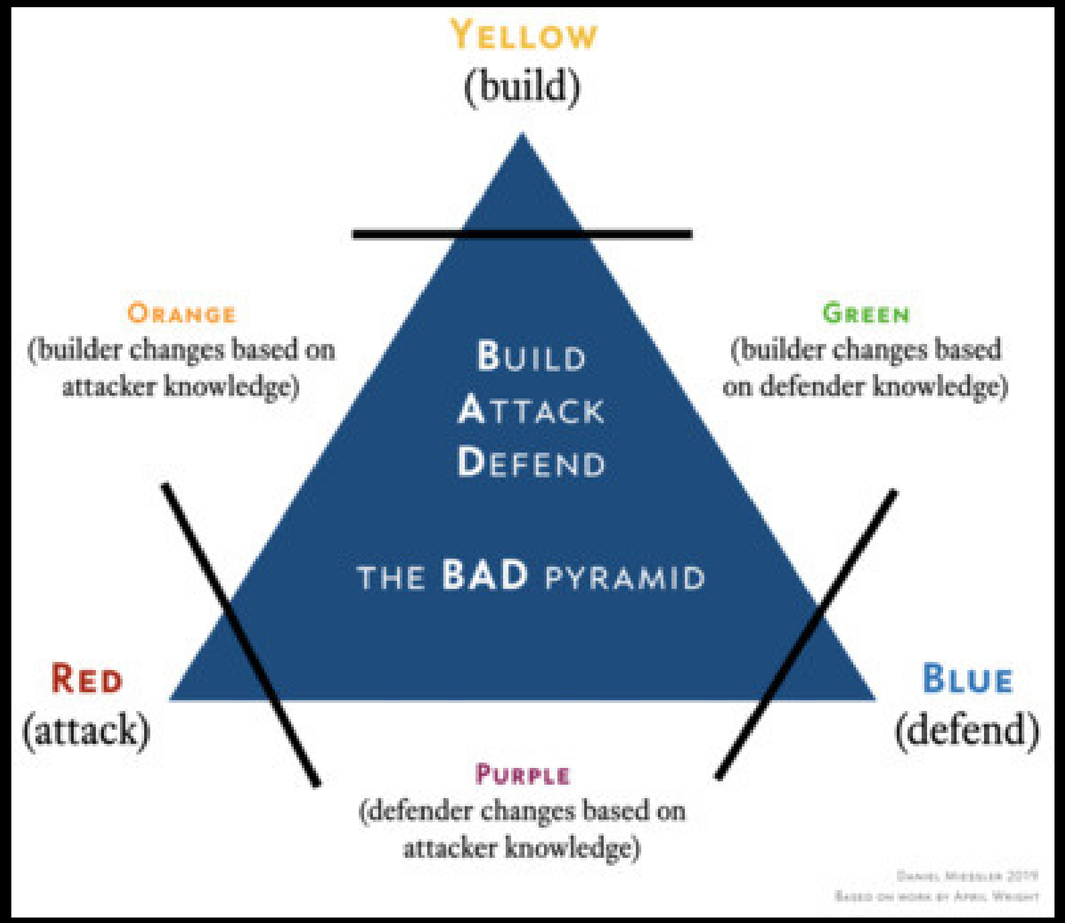
Co-founder,President
DigiSuraksha Parhari Foundation
Former Gurugram cyber police Intern
Technical Content Manager at BSides Pune
Ethical Hacker & Malware Analyst
Intern at Cyber Secure India
Threat Hunter && Open Source Intelligence Analyst
Public Speaker
Car Hacking

https://github.com/shivammittal2403
https://medium.com/@shivammittal2403
https://www.linkedin.com/in/shivam-mittal2023/




CIO
CISO
SVP
VP
Director
Red Team
SI
SecOps
IR
Security Architecture
Program Management
Vulnerability Management
Malware Analysis
Manager
Manager
Manager
Manager
Manager
Manager
Manager
Manager
Sources
Analysis
Reporting

Total Cve :-280720 CVE



WHO IS THREAT ACTOR

"Threat actors are individuals or groups responsible for malicious activities against systems, networks, or organizations."

- **Hacktivists: Driven by political or social ideologies.**
- **Cybercriminals: Motivated by financial gain.**
- **State-Sponsored Groups: Conduct cyber espionage or sabotage on behalf of governments.**
- **Insiders: Employees or associates who misuse access for personal or financial reasons.**

Key Points to notice

DIRECT CYBERCRIME:

1. FREQUENTLY INVOLVES INDIVIDUAL OR AMATEUR HACKERS.
2. MAY EXHIBIT SHORT-TERM PLANNING OR IMPULSIVE BEHAVIOR.
3. USUALLY DONE BY YOUNGER PEOPLE OR THOSE WHO ARE EXPERIMENTING WITH OTHER SYSTEMS.

INDIRECT CYBERCRIME:

1. EXHIBITS A GREATER DEGREE OF TECHNICAL EXPERTISE AND PATIENCE.
2. CENTERED ON PRESERVING ANONYMITY AND REDUCING DANGER.
3. THE LIKELIHOOD OF PERPETRATORS HAVING A TECHNICAL OR PROFESSIONAL BACKGROUND IS HIGHER.

ORGANIZED CYBERCRIME:

1. OFFENDERS OPERATE IN WELL-ORGANIZED GROUPS WITH DESIGNATED RESPONSIBILITIES, SUCH AS DISTRIBUTORS, NEGOTIATORS, AND PROGRAMMERS.
2. FREQUENTLY SUPPORTED BY BIGGER STATES OR ORGANIZATIONS.
3. EXHIBIT A HIGH DEGREE OF INTELLIGENCE AND LONG-TERM STRATEGIC PLANNING.

Trigent event or Motivation

Trigger Category	Trigger	Description
Emotional Triggers	Curiosity	Desire to explore systems or test boundaries.
	Revenge	Personal vendetta against an individual, company, or institution.
	Greed	Driven by financial gain through theft, ransomware, or fraud.
	Pride/Ego	Desire to prove skills or achieve recognition in hacking communities.
	Fear/Paranoia	Hacking to cover tracks, avoid detection, or preemptively attack a perceived threat.
Psychological States	Thrill-Seeking	Enjoyment of the adrenaline rush from risky activities.
	Sense of Power	Gaining control over systems, data, or individuals.
	Empathy or Altruism	Ethical hacking or hacktivism to expose corruption or fight injustice.
	Isolation/Loneliness	Using hacking as a coping mechanism or to gain social interaction in online communities.
	Obsession	Persistent focus on breaking into a specific system or network, often due to a fixation or grudge.
External Motivations	Ideology	Political, religious, or social beliefs driving hacktivism.
	Financial Necessity	Economic hardships leading to crimes like fraud or identity theft.
	Peer Pressure	Influence from groups or online forums encouraging hacking.
	Professional Ambition	Testing or enhancing skills for career advancement or self-promotion.
	External Provocation	Being provoked by a challenge or perceived insult.

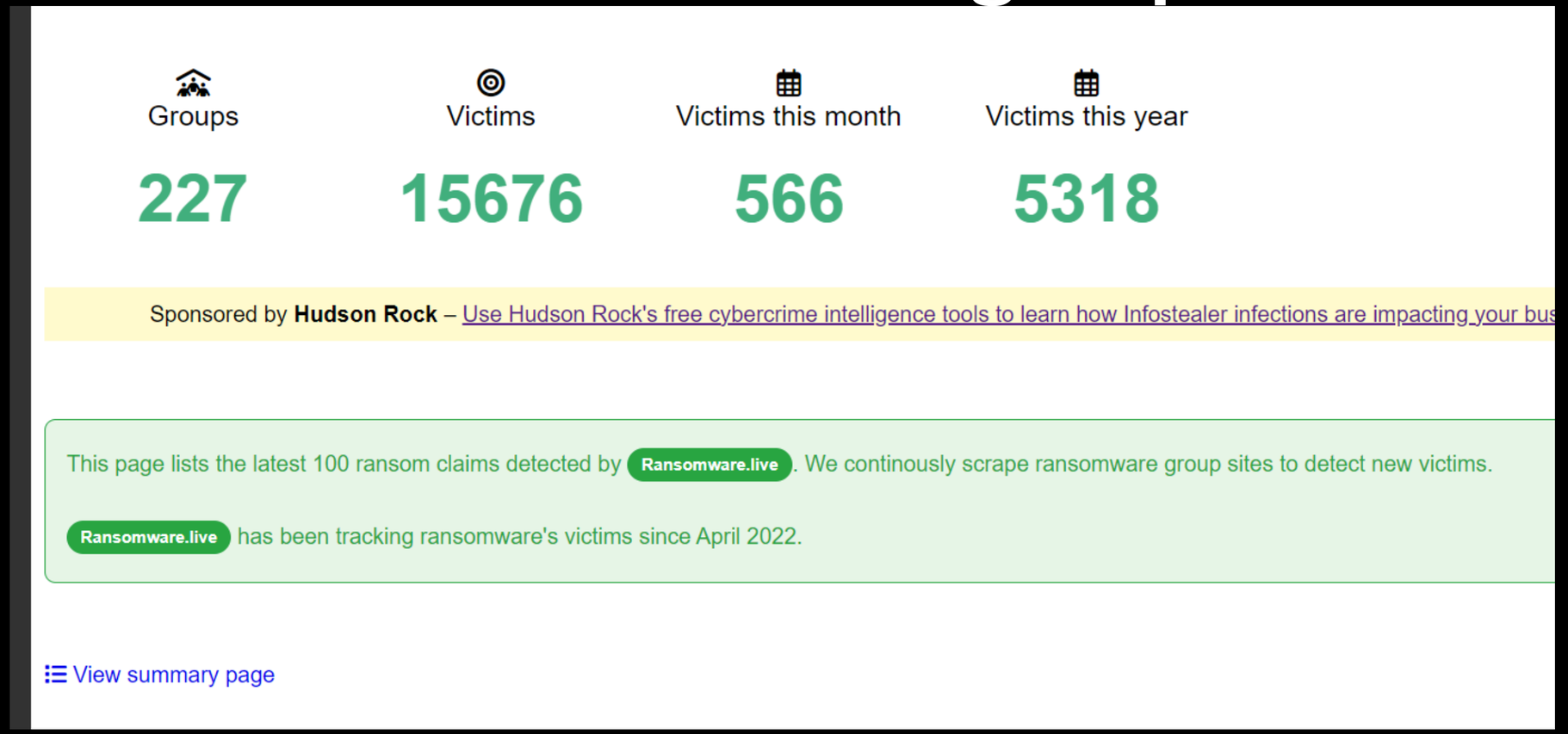
IDENTIFING THREAT ACTOR GROUP

Critical Infrastructure	Cyber Threat Actor Pattern/Focus	
Energy (Electricity & Power)	Targeting SCADA systems, power grids, and renewable energy management systems. Attacks could disrupt power supply or cause damage to critical equipment (e.g., Stuxnet-like attacks).	11+
Water Supply Systems	Exploiting IoT devices, PLCs, or SCADA systems. Potential for contamination of water supplies or shutting down treatment plants.	4+
Telecommunications	Hacking network infrastructures, disrupting services, or spying on communications. Cyber espionage is common, targeting sensitive communication channels.	263+
Transportation Systems	Disrupting air traffic control systems, railway signals, or logistics networks. Could lead to massive disruptions in transportation and supply chains.	28+
Financial Services	Targeting online banking, payment systems, and financial data. Cybercriminals may seek financial theft through ransomware, fraud, or data breaches.	150+
Healthcare	Ransomware attacks, data breaches, and attacks on medical devices. Aimed at stealing patient data, causing service disruption, or extorting hospitals.	180+
Government Facilities	Espionage, data exfiltration, and cyber warfare. Attackers might target government websites, classified databases, or communication channels for intelligence gathering or disruption.	295+
Food Production and Supply	Disrupting supply chains, stealing data, or causing operational shutdowns. Cyber threats could cause food shortages, price hikes, or contamination.	9+

IDENTIFING THREAT ACTOR GROUP

Chemical Industry	Targeting chemical plants, industrial control systems (ICS), and hazardous materials management. Attacks could lead to environmental disasters or mass casualties.	3+
Nuclear Facilities	Attacks on nuclear power plants' safety systems or data exfiltration. Similar to attacks on power grids but with far higher consequences in terms of radioactive material.	
Public Safety	Ransomware, denial of service attacks, or compromising 911 systems. Aimed at disabling emergency response systems, which can cause significant harm to public welfare.	3+
Space Systems	Cyber espionage, satellite jamming, or hacking space-based communication systems. Attacks may disrupt navigation systems, surveillance, and military communications.	14+
Information Technology (IT)	Targeting data centers, cloud services, and software vulnerabilities. Exploiting unpatched systems or data breaches to steal sensitive information or disrupt services.	150+
Defense and Military	Cyber warfare, espionage, and sabotage of military equipment. Attacks on defense infrastructure can impair national security, including targeting missile defense, troop coordination, or military secrets.	4+
Critical Manufacturing	Attacks on industrial control systems (ICS), intellectual property theft, or sabotage of production lines. Can disrupt manufacturing processes, destroy intellectual property, or cause supply chain breakdowns.	292+

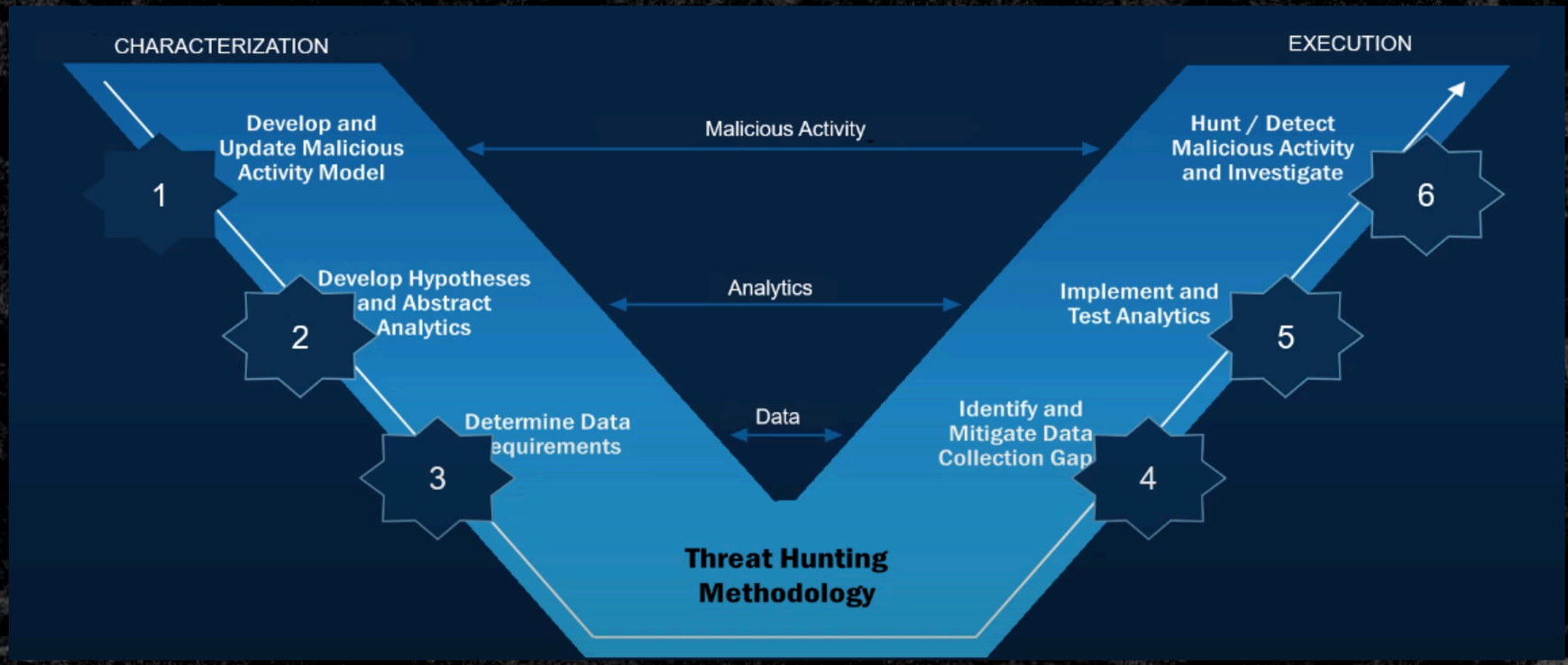
list of Rensomeware group



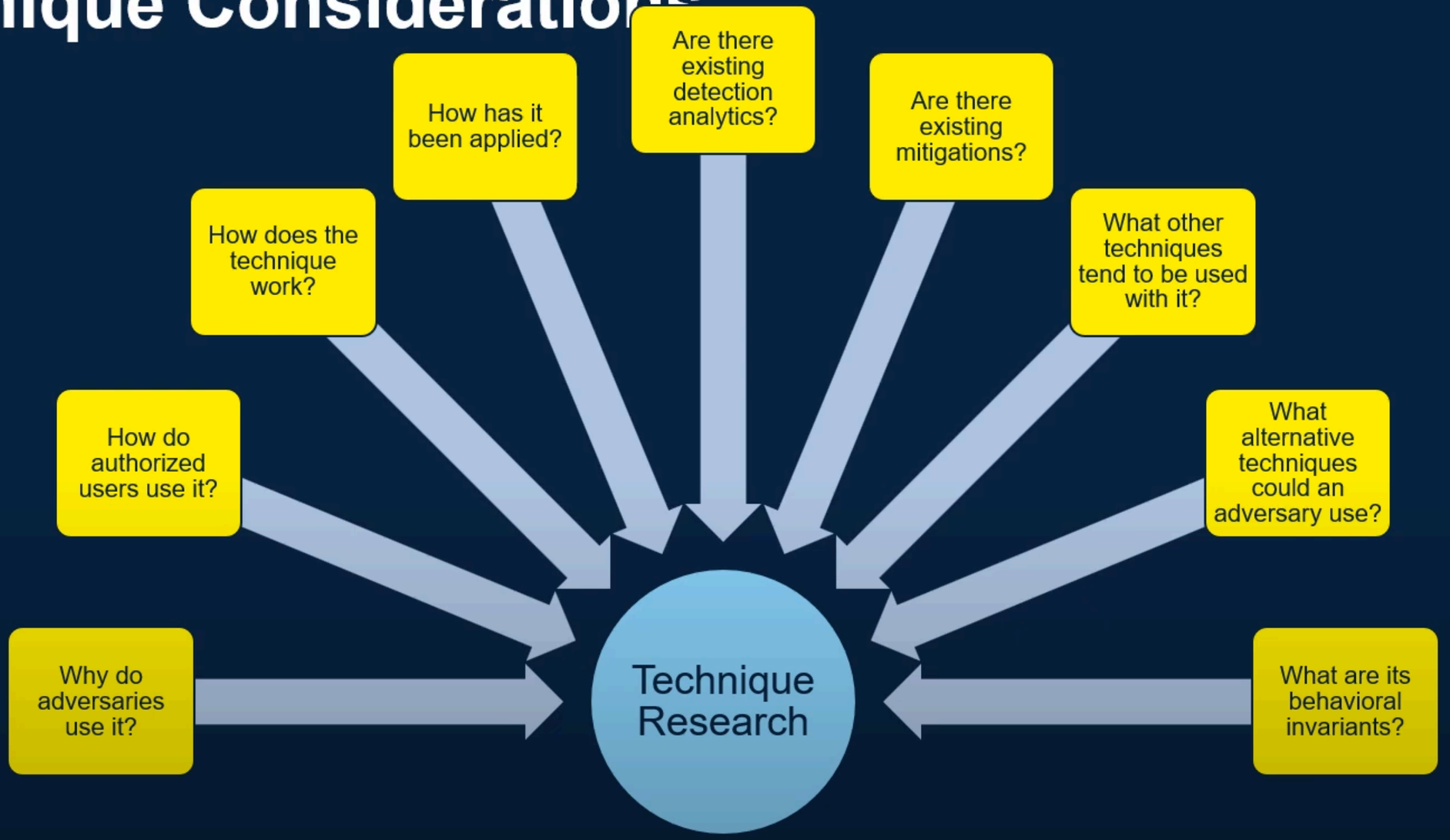
There are more than 73 active ransomware groups out of 227 total.

What is threat intelligence

Threat intelligence, also known as cyber threat intelligence (CTI), is the process of gathering, analyzing, and interpreting data regarding potential or existing cyber threats. This intelligence is crucial for organizations to understand the motives, behaviors, and capabilities of threat actors, thereby enabling them to proactively defend against cyber attacks.



Technique Considerations



What is threat intelligence

Type of Threat Intelligence	Focus	Purpose	Use Case
Strategic	High-level overview of threats and trends.	Guide decision-making and long-term security planning.	Board-level decisions, long-term cybersecurity strategy.
Tactical	Tactics, techniques, and procedures (TTPs) of attackers.	Inform security teams about attack methods and behaviors.	Attack detection, response tactics, security operations.
Operational	Real-time, detailed intelligence on specific attacks.	Provide actionable data for immediate defense or response.	Incident response, monitoring ongoing attacks.
Technical	Specific indicators like IPs, file hashes, and URLs.	Provide actionable data to detect and block known threats.	SIEMs, endpoint protection, firewall integration.

Helps of threat intelligence

Benefit	Explanation
Proactive Threat Detection	Identifies threats before they become attacks.
Enhanced Incident Response	Accelerates response time and minimizes damage during an attack.
Reduced False Positives	Helps focus on real threats, improving detection efficiency.
Improved Risk Management	Informs decisions and improves defenses based on emerging trends.
Protection Against APTs	Detects and defends against long-term, sophisticated attacks.
Compliance	Helps organizations meet regulatory requirements.
Competitive Advantage	Strengthens security posture and builds trust with customers.
Threat Collaboration	Enables sharing of intelligence to strengthen community defenses.
Strengthened Security Operations	Automates threat detection and optimizes resource use.

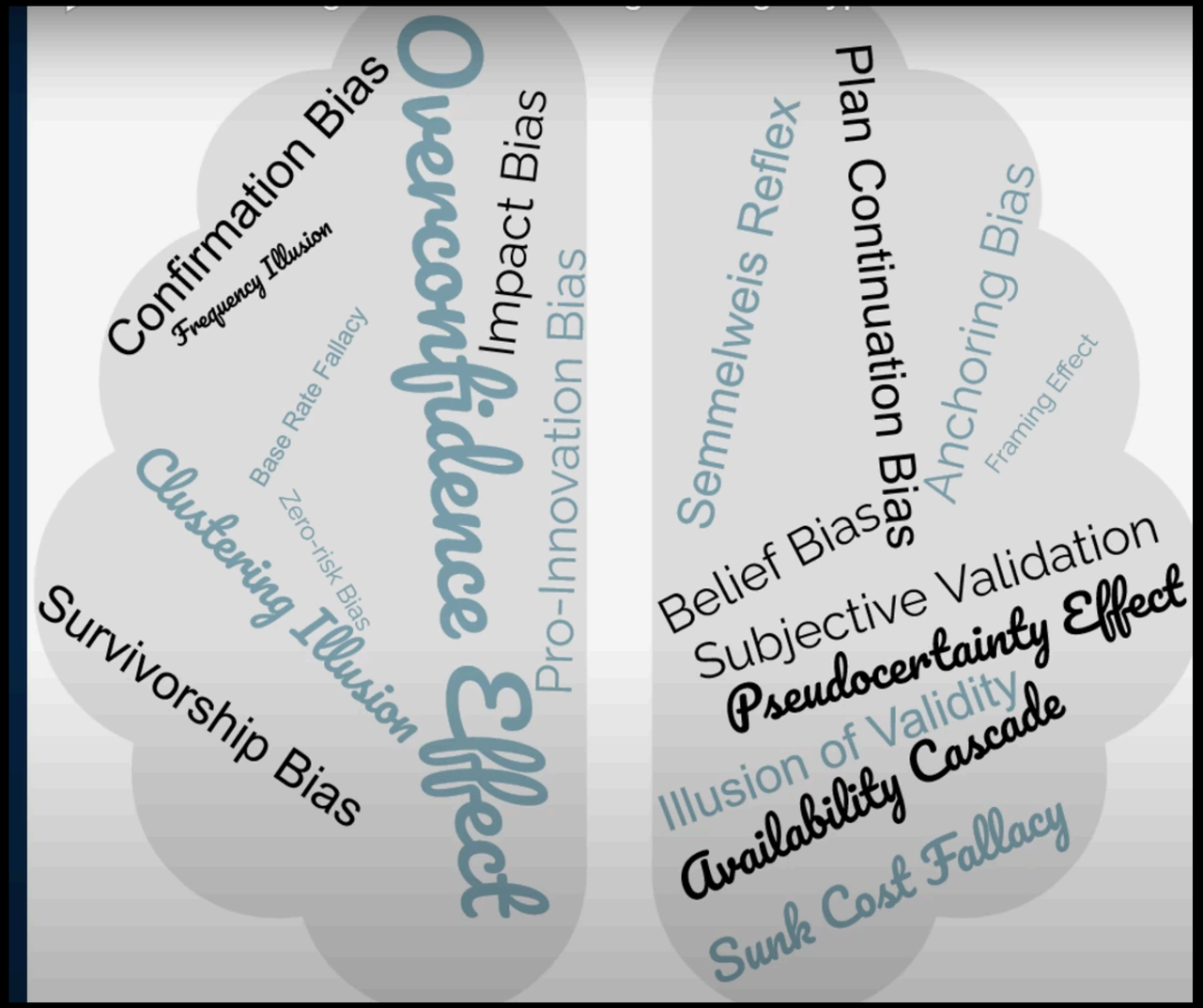
OSINT (Open Source Intelligence)
Description:
Open Source Intelligence involves collecting publicly available data to gather insights into cyber threats. OSINT methods focus on gathering data from various sources like social media, websites, and the Dark Web.

- Sources:
  - Social Media (Twitter, Reddit, Telegram): To identify emerging threats and hacker activities.
  - Dark Web: Anonymized forums and marketplaces where threat actors trade tools, stolen data, or discuss exploits.
  - Websites: Monitoring threat reports, breach data, and security advisories.
- Benefits:
  - Cost-effective and easy to access.
  - Real-time data from global discussions.
  - Identifies trends and potential vulnerabilities.

CSINT (Closed Source Intelligence)
Description:
Closed Source Intelligence focuses on gathering data from closed, proprietary sources, such as paid threat feeds, intelligence vendors, or private threat-sharing groups.

- Sources:
  - Threat Intelligence Platforms (TIPs): Services like ThreatConnect or FireEye provide curated, expert-driven intelligence.
  - Private Threat Sharing Networks: Information sharing with trusted partners or through ISACs (Information Sharing and Analysis Centers).
- Benefits:
  - Specialized and targeted data relevant to your environment.
  - Curated feeds from reliable, vetted sources.
  - Quick access to new threats, vulnerabilities, and advisories.

Problems When Threat intelligence



- Effects of Bias in a Hypothesis
- Distorted Conclusions
  - The research might lead to incorrect conclusions, as the hypothesis is skewed by preconceived notions or preferences.
- Lack of Generalizability
  - Biased hypotheses often fail to account for diverse perspectives or variables, limiting the applicability of the results.
- Confirmation Bias
  - Researchers may seek evidence that supports the biased hypothesis while ignoring contradictory data.
- Erosion of Credibility
  - If identified, bias can diminish the credibility of the research and the researcher.

Best Practices for Implementing Cloud Native DevSecOps in Azure

The adoption of Cloud computing has come with its set of security challenges and risks. Here are some eye-opening cloud security statistics and breach examples from 2018 to 2023 : As organizations...

Medium / Sep 10, 2023

Malware Analysis Workflow

Static Analysis:Tool: VirusTotal (hash lookup, community insights).
Example: Malware.exe (SHA-1: 839a6e6678e9b...).
Dynamic Analysis Tool: Valkyrie (sandbox behavior report).
Graph Intel:
Tool: Maltego (infrastructure mapping).
Visual: Step-by-step flowchart.

What we know about the Hezbollah device explosions

20 September 2024

Share Save

Matt Murphy BBC News
Joe Tidy Cyber Correspondent

LIVE UPDATE → FROM THE LIVEBLOG OF WEDNESDAY, NOVEMBER 27, 2024

Report: US 'side letter' to Israel pledges to share intelligence on Hezbollah activity after ceasefire, cooperate against Iranian threat

27 November 2024, 1:24 am

7

Israel's Channel 12 news outlet shares details from a side letter that it says the US is providing to Israel as part of the Israel-Hezbollah ceasefire deal, in which it affirms and details Israel's right to defend itself against renewed threats from the Iran-backed terror group in Lebanon.

According to the report, the US will commit to providing Israel with intelligence information pertaining to violations of the terms of the ceasefire deal, and in particular, regarding any indication that Hezbollah is attempting to infiltrate the ranks of the Lebanese Armed Forces, which will be deployed to southern Lebanon.

What the Five Eyes Alliance Means for the Public

The Five Eyes alliance might sound like a plot out of a riveting spy novel, but its implications for the public are far from fictional. In essence, this intelligence network is a double-edged sword. It represents a compelling power to uphold national security and tackle global threats, which undeniably contributes to public safety. However, this formidable power doesn't come without a price—our privacy.

In the interconnected, digital world we inhabit, the line between surveillance for safety and invasion of privacy has blurred. Edward Snowden's 2013 revelations peeled back the curtain on the extensive data harvesting activities of the alliance, throwing a spotlight on the precarious balance between security and individual privacy rights.

In this landscape, our digital footprints—emails, phone calls, online shopping and social media activity—could be open books, potentially read without our knowledge or consent. This stark reality fuels ongoing debates about privacy, state power and the fine line between surveillance and civil liberties.

This is where a commonly heard phrase enters the debate: "If you're doing nothing wrong, you have nothing to hide." This argument is often used to justify surveillance practices, suggesting that those leading law-abiding lives shouldn't be concerned about privacy invasions.

However, this standpoint is simplistic and overlooks a key facet of privacy—it isn't solely about hiding wrongdoing. Privacy is also about the right to control personal information, the freedom to express opinions without fear of reprisal and maintaining spaces where we can be free from outside observation.

While the Five Eyes alliance certainly plays a crucial role in global security, it's equally important to remember that privacy forms a cornerstone of democratic societies. As such, the alliance's activities highlight the need for a delicate balance between security and individual rights—a balance that remains a significant topic of ongoing debates.

UNDERSTANDING PLAY RANSOMWARE: TACTICS, TECHNIQUES, AND PROTECTIVE MEASURES

Tools and Persistence Techniques

- Remote Access Tools: Plink, AnyDesk.
- Credential Theft: Mimikatz.
- Data Exfiltration: WinRAR compresses and exports data in chunks.

Lateral Movement

- Tools:
  - Cobalt Strike SMB Beacon.
  - SystemBC RAT, Empire framework.
- Living-Off-the-Land (LOLBins): Uses legitimate binaries like WinSCP for stealth.
- Scripts: Batch scripts and GPOs deploy ransomware across networks.

Double Extortion

- Method: Encrypts data and threatens to publish sensitive information unless the ransom is paid.

Connections to Other Ransomware Groups

- Shared Tactics and Tools: Similarities with Hive, Nokoyawa, and Quantum ransomware suggest potential links.
- Indicators: Use of AdFind, Cobalt Strike, and common file paths.

PLAYRANSOMWARE LINK

DECRYPTING LOCKBIT 3.0: UNPACKING A SOPHISTICATED RANSOMWARE THREAT

Introduction

Ransomware attacks, such as LockBit 3.0, have redefined cyber extortion. With advanced encryption methods and innovative attack models, LockBit 3.0 demands a robust cybersecurity approach to counter its threats effectively.

Evolution of LockBit

1. LockBit Original (2019): Rapid encryption via SMB & PowerShell, used “ABCD” extension.
2. LockBit 2.0 (2021): Enhanced speed, bypassed Microsoft Defender, added StealBit for data targeting.
3. LockBit 3.0 (2022): Bug bounty program introduced, refined encryption.
4. LockBit Green: Influenced by Conti ransomware, compatible with Windows.

Key Features

- RaaS Model: Personalized attack options for hackers.
- Exploitation: Targets weak passwords and accounts without MFA.
- Bug Bounty Program: Encourages discovering vulnerabilities.

Attack Anatomy

1. Initial Access: Phishing, RDP brute force, exploiting software flaws.
2. Lateral Movement: Privilege escalation, security disabling, high-value data targeting.
3. Ransomware Deployment: Encrypts files and issues ransom demands.

Notable Incidents

- Accenture (2021): 6 GB data stolen, $50M ransom demanded.
- Nameless Organization (2020): Exploited weak credentials, spread via PowerShell scripts.

DECRYPTING LOCKBIT 3.0: UNPACKING A SOPHISTICATED RANSOMWARE THREAT

Impacts
Financial loss (ransom demands in millions).
Operational downtime.
Reputation damage and stakeholder trust erosion.
Expensive recovery processes.

Challenges in Negotiation
No Guarantees: Attackers may not honor agreements.
Regulatory Risks: Payment may violate laws.
Ethical Issues: Funds criminal operations.

LOCKBIT LINK

APT28 HACKER GROUP: OVERVIEW OF LATEST PHISHING CAMPAIGNS

Aliases: Fancy Bear, Sofacy, Iron Twilight
Attribution: Russia-linked Advanced Persistent Threat (APT) group
Key Highlights

- Targeted Regions: Europe, Americas, Asia (Nov 2023–Feb 2024)
- Themes: Finance, critical infrastructure, healthcare, defense, cybersecurity.

Tactics, Techniques, and Procedures (TTPs)

1. Microsoft Vulnerabilities
    - CVE-2023-23397: Exploits to steal NTLMv2 hashes for privilege escalation.
2. URI Protocol Abuse
    - search-ms: used to download malware from attacker-controlled WebDAV servers.
3. Compromised Infrastructure
    - Botnets hosted on compromised Ubiquiti routers.
4. Malware Arsenal
    - MASEPIE: Steals browser data and files.
    - OCEANMAP: Advanced backdoor for persistence.
    - STEELHOOK: Modular implant for command execution.
5. Thematic Lures
    - Decoys exploiting high-profile events (e.g., Israel-Hamas conflict).

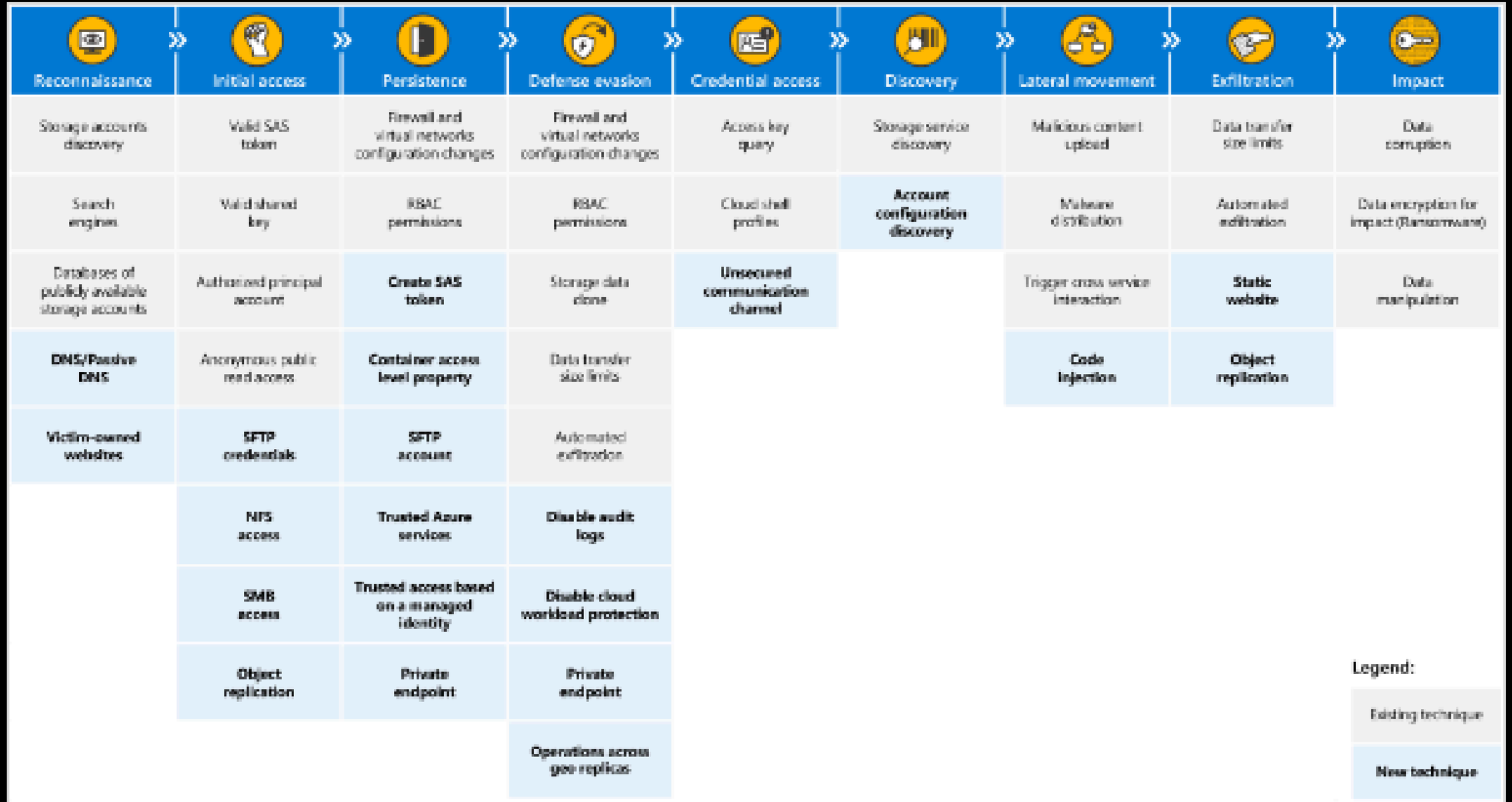
APT28 HACKER GROUP: OVERVIEW OF LATEST PHISHING CAMPAIGNS

Mitigation and Key Observations
Impact
Governments/NGOs: Data breaches, operational disruptions.
Private Sector: Economic instability, weakened critical services.
Infrastructure: Highlighting systemic global weaknesses.
Key Incidents
Ukrainian and Polish Targets: High-stakes geopolitical phishing campaigns.
Israel-Hamas Conflict Decoys: Used custom malware (HeadLace).

APT28 LINK

DIRECTION >COLLECTION > ANALYSIS > DISSEMINATION

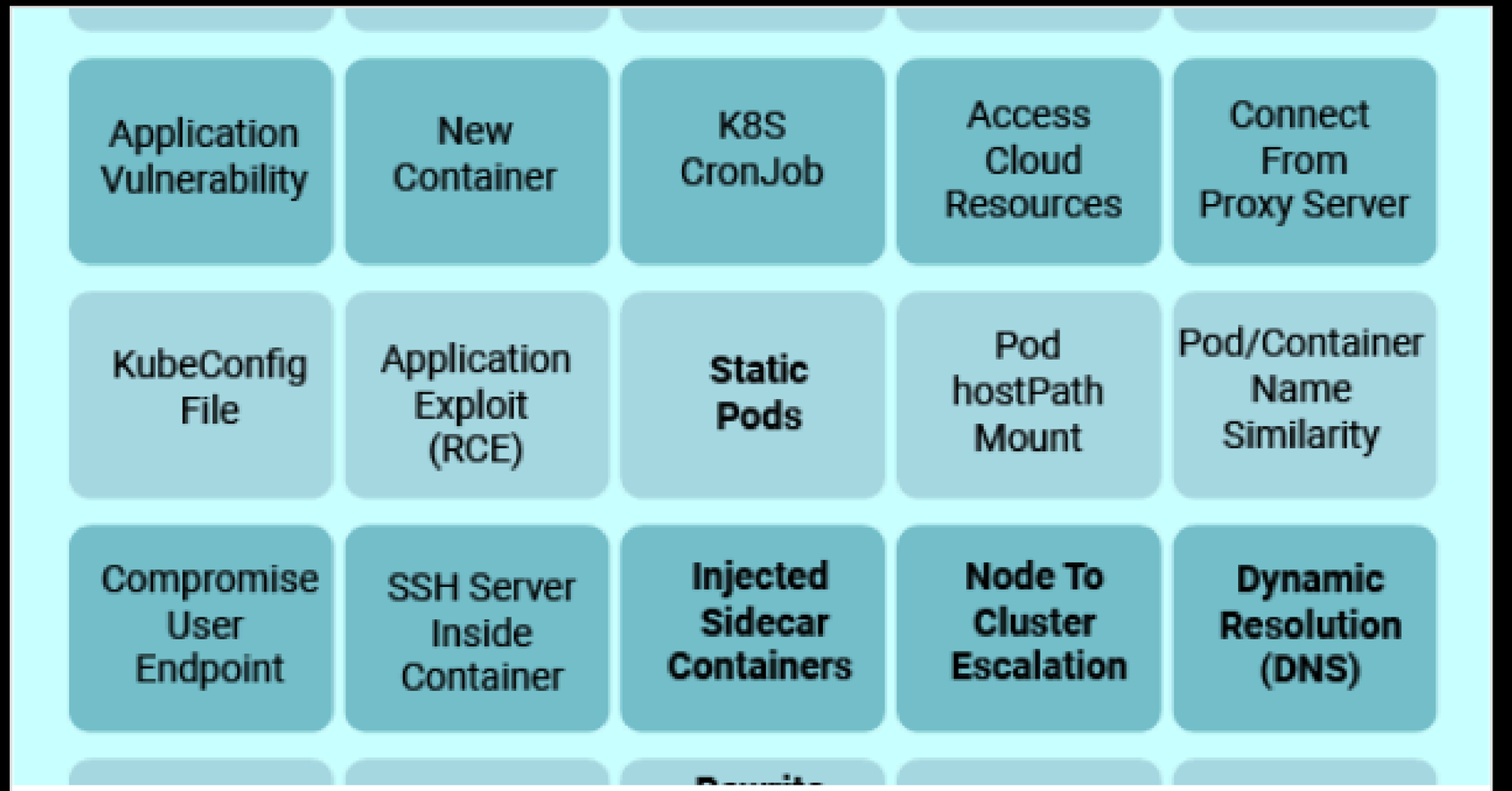
DATA PROTECTION ACT 1998
COMPUTER MISUSE ACT 1990
POLICE AND JUSTICE ACT 2006
BRIBERY ACT 2010
REGULATION OF INVESTIGATORY POWERS ACT 2000
PROCEEDS OF CRIME ACT 2002
OFFICIAL SECRETS ACT 1989
TELECOMMUNICATIONS 2000
HUMAN RIGHTS ACT 1998



Cloud storage security: What's new in the threat matrix

orchestration security, with focus on Kubernetes.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed Dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	



Microsoft's Kubernetes Threat Matrix: Here's What's Missing

With a fuller picture of the Kubernetes threat matrix, security teams can begin to implement mitigation strategies to protect their cluster from threats.

MITRE ATT&CK for Industrial Control Systems in IriusRisk

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

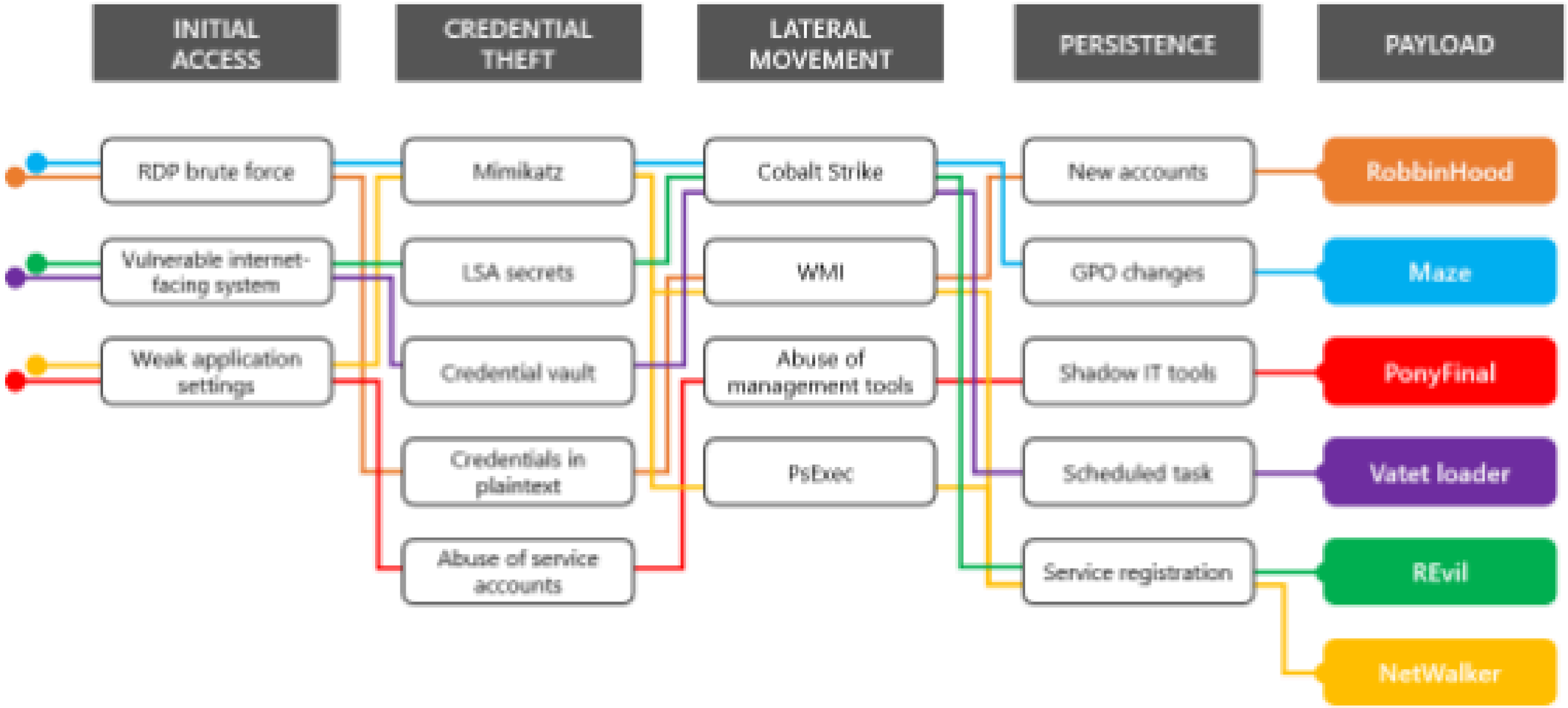
Analytics

Cyber Analytics Repository

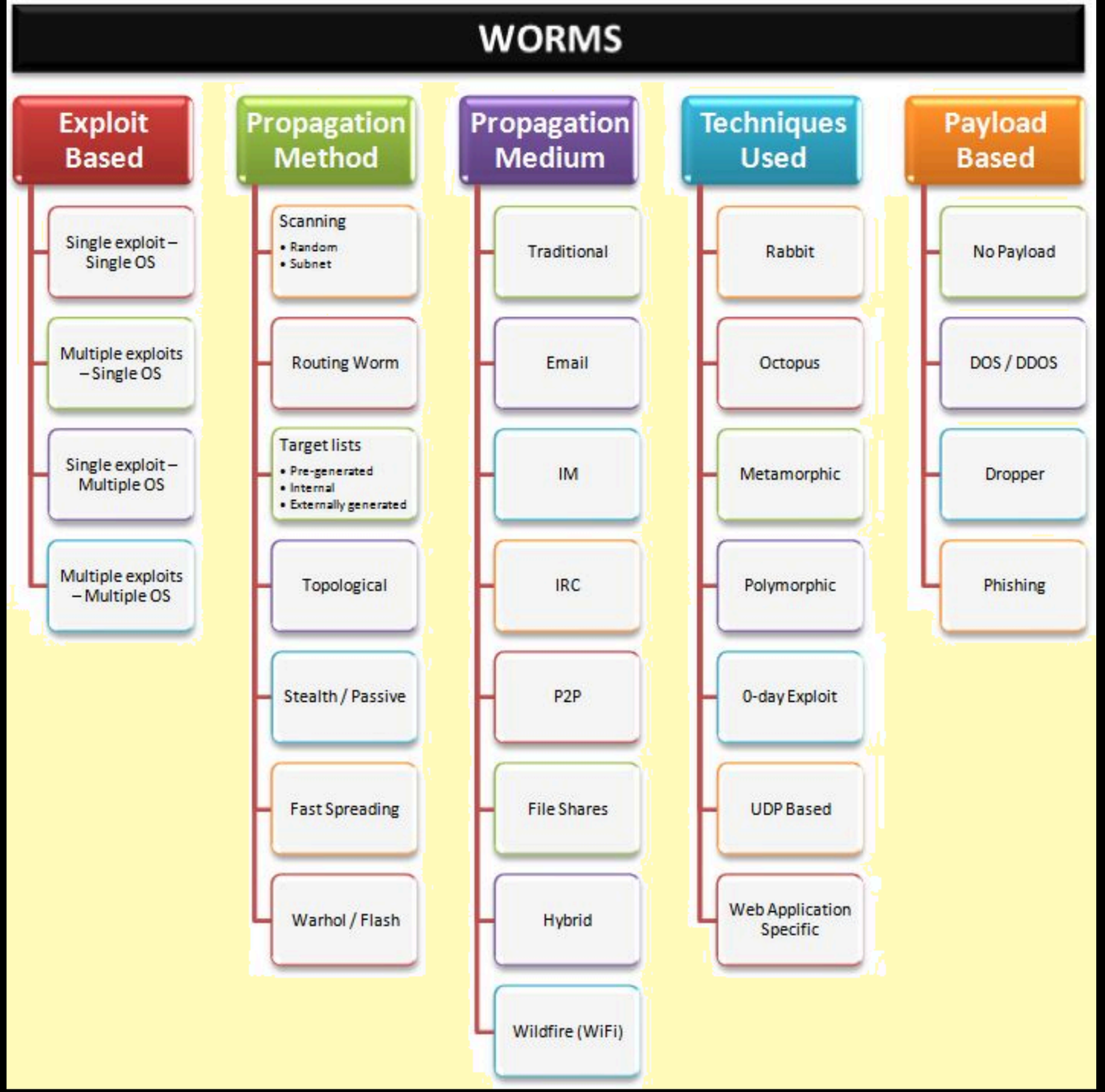
MITRE Cyber Analytics Repository /

Process flow diagram depicting ransomware incidents occurrence

Mentioned slide depicts the incident workflow diagram of a ransomware event. It starts with the threat actor's entry and ends with the threat actor demanding ransom.



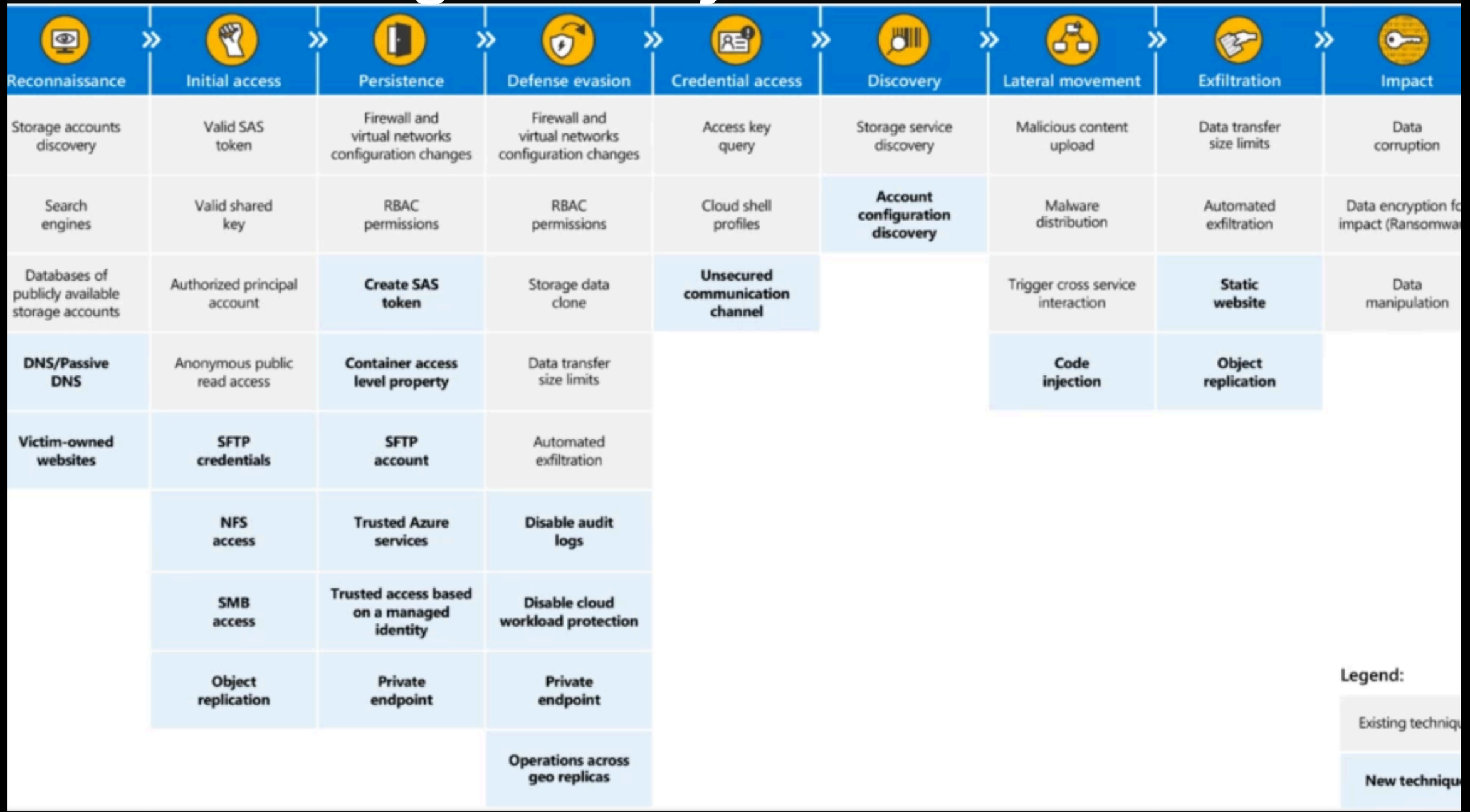
Ransomware groups continue to target healthcare, critical services; here's how to reduce risk


WORMS
Exploit Based
Single exploit – Single OS
Multiple exploits – Single OS
Single exploit – Multiple OS
Multiple exploits – Multiple OS
Propagation Method
Scanning
• Random
• Subnet
Routing Worm
Target lists
• Pre-generated
• Internal
• Externally generated
Topological
Stealth / Passive
Fast Spreading
Warhol / Flash
Propagation Medium
Traditional
Email
IM
IRC
P2P
File Shares
Hybrid
Wildfire (WiFi)
Techniques Used
Rabbit
Octopus
Metamorphic
Polymorphic
0-day Exploit
UDP Based
Web Application Specific
Payload Based
No Payload
DOS / DDOS
Dropper
Phishing

DevSecOps

Initial access	Execution	Persistence	Privilege escalation	Credential access	Lateral movement	Defense evasion	Impact	Exfiltration
SCM authentication	Poisoned pipeline execution (3)	Change code/pipeline configuration in repository (3)	Secrets stored in private repositories	User credentials	Compromise build artifacts	Service logs manipulation	DDoS using pipeline compute resources	Clone for private repositories
CI/CD service authentication	Dependencies tampering (3)	Inject in artifacts	Commit from pipeline to protected branches	Service credentials	Registry injection	Compilation manipulation (2)	Crypto mining over pipeline compute resources	Access to pipelines logs
Configured webhooks	DevOps resources compromise	Modify images in registry	Certificates and identities from metadata services		Spread from pipeline into deployment resources	Reconfigure branch protections	Local DoS to CI/CD pipelines	Exfiltrate data from production resources
Organization's public repositories	Control of common registry	Create service credentials					Resource deletion	
Endpoint compromise								

Cloud Storage Security



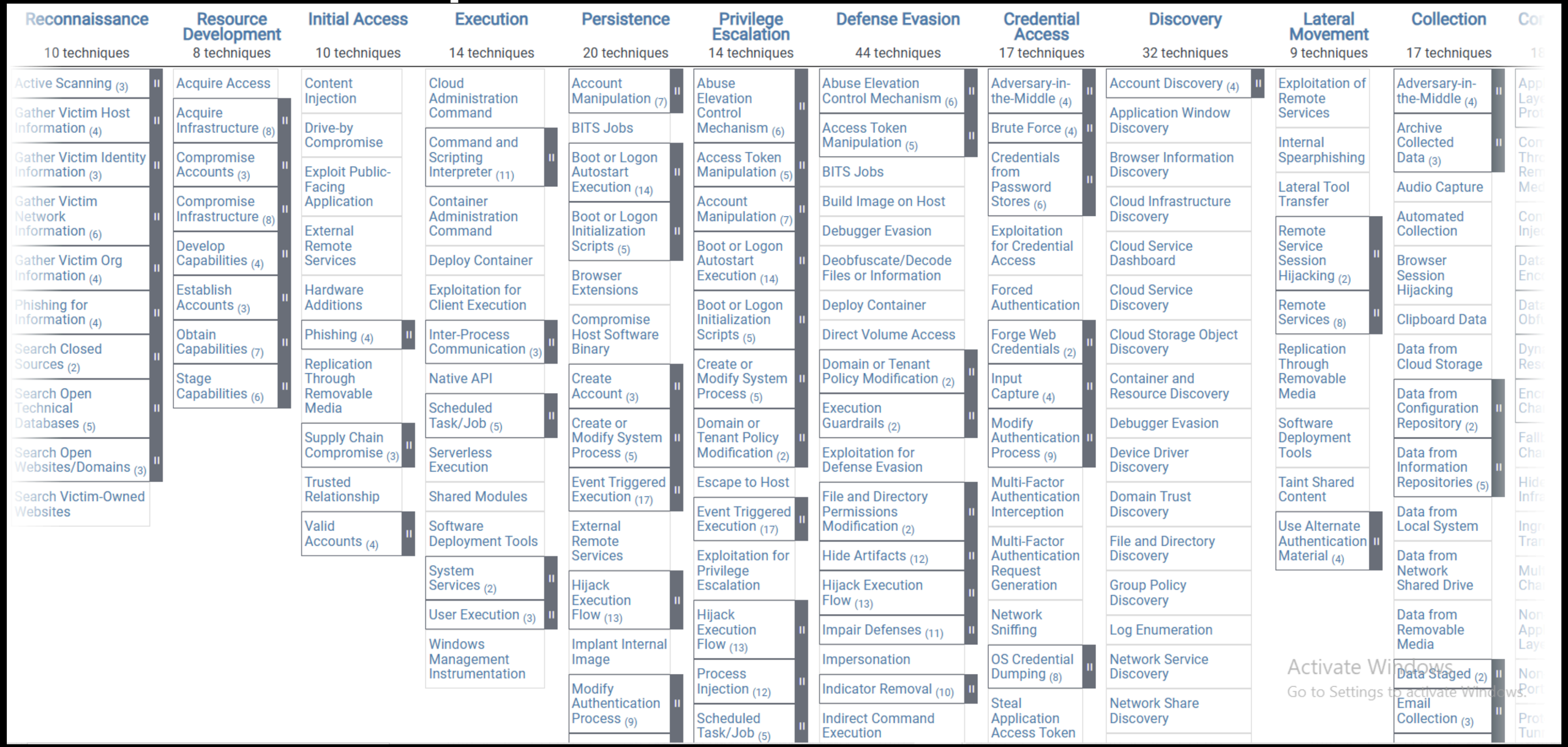
Reconnaissance	Initial access	Persistence	Defense evasion	Credential access	Discovery	Lateral movement	Exfiltration	Impact
Storage accounts discovery	Valid SAS token	Firewall and virtual networks configuration changes	Firewall and virtual networks configuration changes	Access key query	Storage service discovery	Malicious content upload	Data transfer size limits	Data corruption
Search engines	Valid shared key	RBAC permissions	RBAC permissions	Cloud shell profiles	**Account configuration discovery**	Malware distribution	Automated exfiltration	Data encryption fo impact (Ransomwa
Databases of publicly available storage accounts	Authorized principal account	**Create SAS token**	Storage data clone	**Unsecured communication channel**		Trigger cross service interaction	**Static website**	Data manipulation
DNS/Passive DNS	Anonymous public read access	**Container access level property**	Data transfer size limits			**Code injection**	**Object replication**	
Victim-owned websites	**SFTP credentials**	**SFTP account**	Automated exfiltration					
	NFS access	**Trusted Azure services**	**Disable audit logs**					
	SMB access	**Trusted access based on a managed identity**	**Disable cloud workload protection**					
	Object replication	**Private endpoint**	**Private endpoint**					
			Operations across geo replicas					

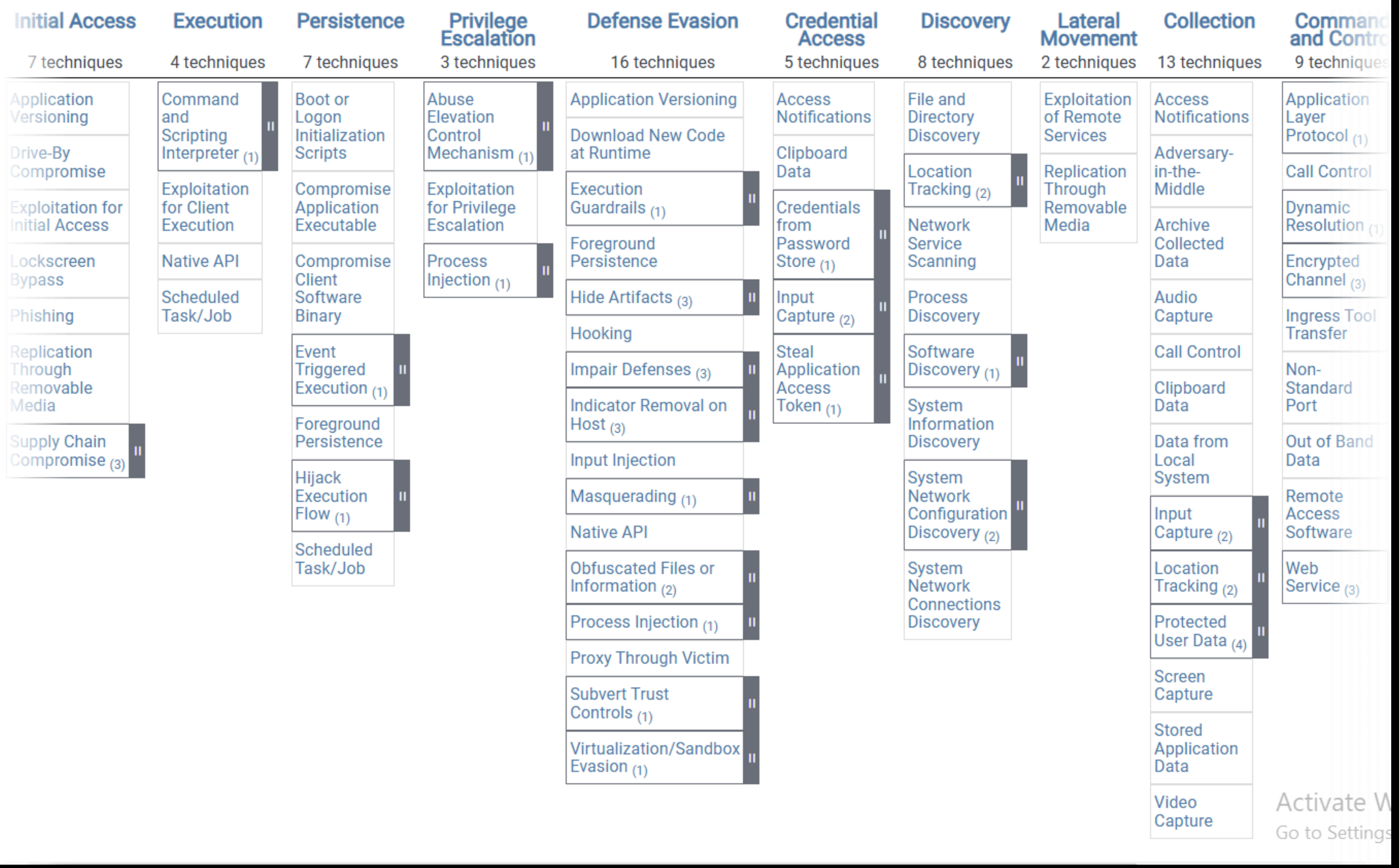
Legend:

Existing techniq

New techniqu

Enterprise Mitre





Kubernet

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed Dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

Car Hacking Matrics

Manipulate Environment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Vehicle Function
Adversarial Machine Learning	Aftermarket, Customer, or Dealer Equipment	Command and Scripting Interpreter	Abuse UDS for Persistence	Abuse Elevation Control Mechanism	Bypass Code Integrity Protections	Exploit TEE Vulnerability	File and Directory Discovery	Abuse Standard Diagnostic Protocol for Lateral Movement	Capture SMS Message	Aftermarket, Customer, or Dealer Equipment	Aftermarket, Customer, or Dealer Equipment	Adversarial Machine Learning
Analog Sensor Attacks	Browser Compromise	Native API	Disable Software Update	Exploit Co-Located Computing Device for Privilege Escalation	Bypass Network Filtering	Capture SMS Message	Location Tracking	Bridge Vehicle Networks	Input Capture	Cellular Communication	Cellular Communication	Analog Sensor Attacks
Downgrade to Insecure Protocols	Exploit via Radio Interface	Abuse UDS to Temporarily Modify Execution	Modify OS Kernel, Boot Partition, or System Partition	Exploit OS Vulnerability	Bypass UDS Security Access	Input Capture	Network Service Scanning	Exploit ECU for Lateral Movement	Network Sniffing	Internet Communication	Internet Communication	Abuse UDS for Affecting Vehicle Function
Jamming or Denial of Service	Exploit via Removable Media		Modify Isolated Execution Environment	Exploit TEE Vulnerability	Bypass Mandatory Access Control	Input Prompt	Process Discovery	Remote Services	Location Tracking	Receive Only Communication	Short Range Wireless Communication	CAN Bus Denial of Service
Manipulate Communications	Malicious App			Hardware Fault Injection		Network Sniffing	Software Discovery	Reprogram ECU for Lateral Movement	Abuse UDS for Collection	Short Range Wireless Communication	Standard Cryptographic Protocol	Denial of Service on Vehicle Function
Relay Communications	Phishing			Process Injection		ECU Credential Dumping	System Information Discovery		Capture Camera or Audio	Standard Cryptographic Protocol	Removable Media	Local Function
Rogue Cellular Base Station	Physical Modification			Reprogram Co-Located Computing Device for		Unsecured Credentials	System Network Configuration		Data from Local System		Physical Access	Modify Bus Message

Drone Hacking

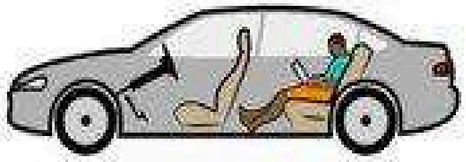
Reconnaissance	Protocol Tampering	Denial of Service	Injection	Exfiltration	Firmware Attacks
Wifi Analysis & Cracking	Telemetry Spoofing	Battery Drain Attack	MAVLink Command Injection	Flight Log Extraction	Firmware Decompile
Drone Discovery	Flight Mode Spoofing	Communication Link Flooding	Camera Gimbal Takeover	Parameter Extraction	Firmware Modding
Packet Sniffing	Drone State Spoofing	Denial-of-Takeoff	Waypoint Injection	Mission Extraction	
Protocol Fingerprinting	GPS Spoofing	Geo-Squeezing	Sensor Data Injection	FTP Eavesdropping	
GPS & Telemetry Analysis		Altitude Limiting	Flight Mode Injection	Camera Feed Eavesdropping	
Payload Detection		GPS Jamming			
		Wireless Deauthentication			

We are here!

Level 5

Full automation: the vehicle can perform all aspects of dynamic driving tasks under all conditions.

Level 4



High automation: the vehicle can handle all dynamic driving tasks in a specific environment without intervention.

Level 3

Conditional automation: the vehicle can handle all dynamic driving tasks in a specific environment but it may request human intervention.

Level 2

Partial automation: at least two functions of driving are handled autonomously.

Level 1

Driver assistance: one aspect of driving is controlled autonomously, e.g. automatic braking.

Level 0

No automation: classic driving in which the driver controls all aspects of dynamic driving task.

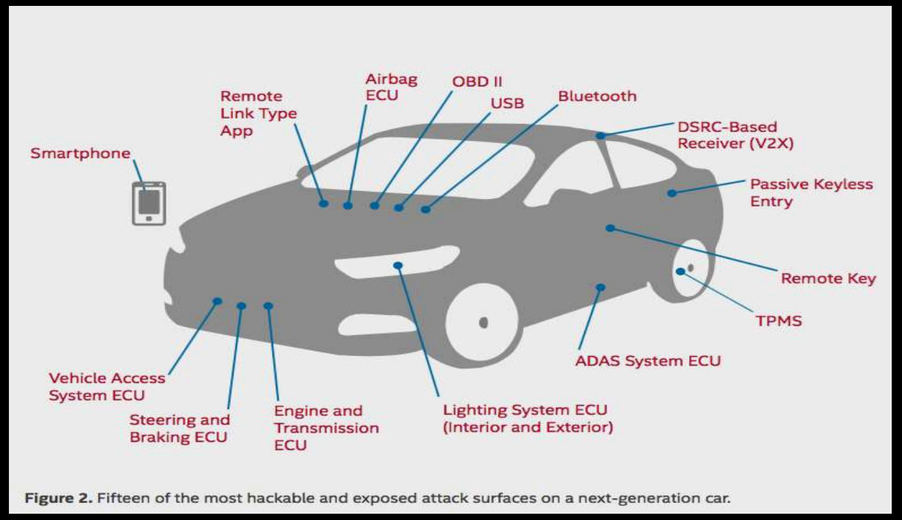
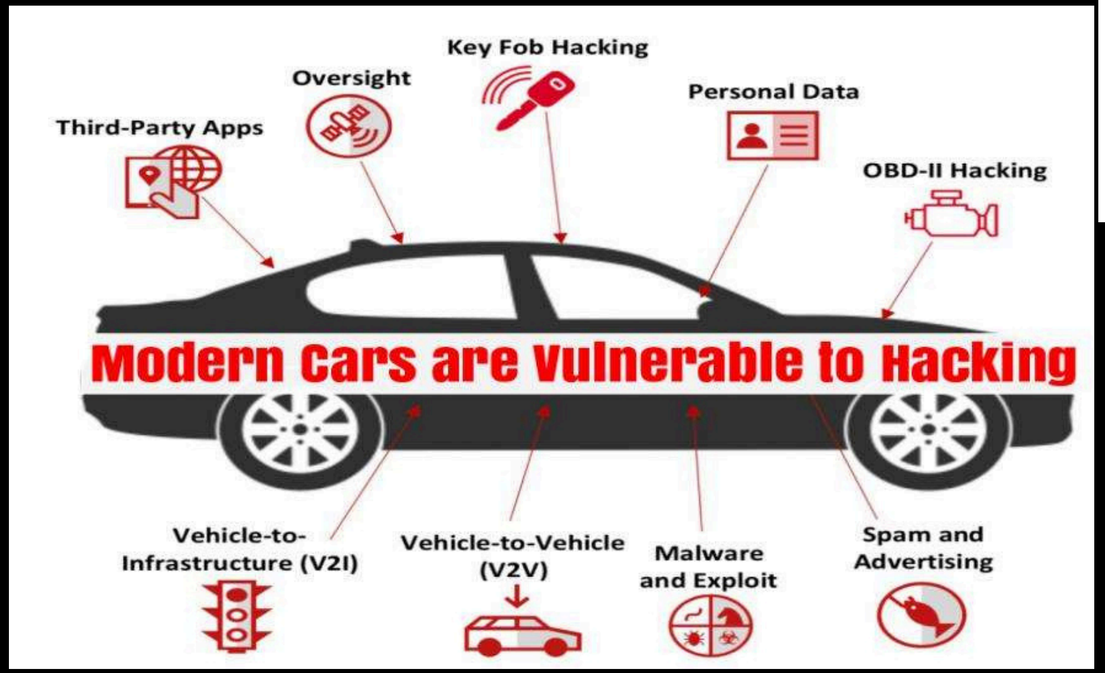
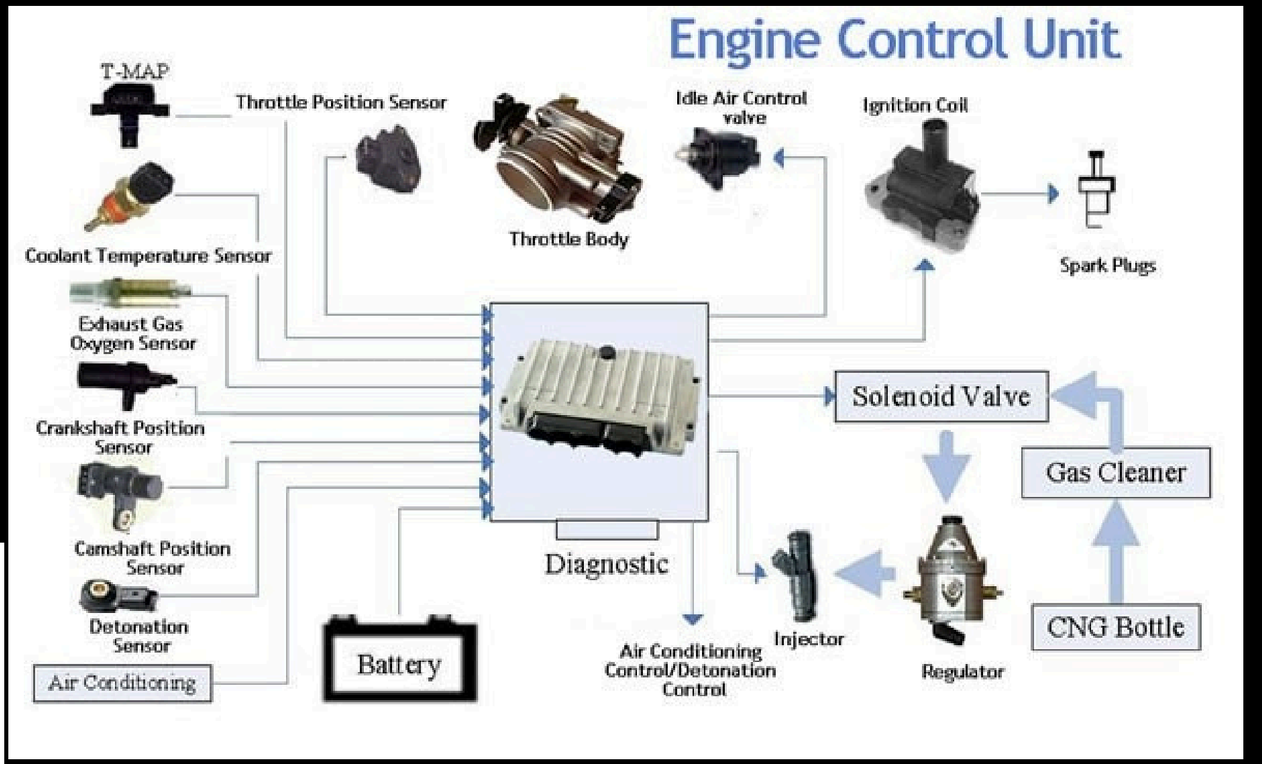


Figure 2. Fifteen of the most hackable and exposed attack surfaces on a next-generation car.





9 Terrifying Ways Hackers Can Control Your Car

- **Braking System Manipulation**: Hackers can remotely disable or abruptly engage the brakes, causing accidents or making the car uncontrollable.
- **Engine Shutdown:** Attackers can shut down the car's engine while it is in motion, posing a serious risk to the driver and passengers.
- **Steering Control:** Hackers can take control of the vehicle's steering system, particularly at lower speeds, potentially causing collisions.
- **Unlocking and Starting the Car**: Using key fob signal amplification or other exploits, hackers can unlock and start the car without having the physical key.
- **Disabling Safety Features**: Hackers can turn off critical safety systems such as airbags, ABS, and traction control, increasing the risk of injury during accidents.
- **Hijacking Infotainment System**: Attackers can control the infotainment system to distract the driver by changing settings, blasting loud sounds, or displaying fake alerts.
- **Tracking Vehicle Location**: By accessing GPS and telematics systems, hackers can track the car's real-time location and monitor the driver's movements.
- **Data Theft from Connected Devices**: Hackers can access personal information stored in the car's system, such as phone contacts, messages, and app data.
- **CAN Bus Injection Attacks**: Hackers can inject malicious messages into the car's CAN bus network to control multiple functions, such as windows, lights, and horn, or even disable the vehicle entirely.

Reminder: the TAXII 2.0 server will be retiring on December 18. Please switch to the TAXII 2.1 server to ensure uninterrupted service.

ATT&CK®

Get Started | Take a Tour

Contribute | Blog

FAQ | Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side | show sub-techniques | hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network	Compromise Infrastructure (8)			Boot or Logon		Build Image on Host		Cloud Infrastructure Discovery		Automated

Threat Intelligence Framework

1. NIST Cybersecurity Framework (CSF)
2. ISO/IEC 27001
3. COBIT (Control Objectives for Information and Related Technologies)
4. CIS Critical Security Controls
5. OWASP Application Security Verification Standard (ASVS)
6. FAIR (Factor Analysis of Information Risk)
7. CWE (Common Weakness Enumeration)
8. CIS Controls for Industrial Control Systems (ICS)
9. MITRE ATT&CK for Cloud
10. CMMC (Cybersecurity Maturity Model Certification)
11. IETF (Internet Engineering Task Force) Security Standards
12. CISA's Cyber Essentials
13. PCI DSS (Payment Card Industry Data Security Standard)
14. FISMA (Federal Information Security Management Act)
15. NIST SP 800-171
16. SANS Critical Security Controls
17. Zero Trust Security Model ThreatConnect, etc.)
18. Center for Internet Security (CIS) Controls for Effective Cyber Defense
19. Open Source Threat Intelligence Platforms (MISP, ThreatConnect, etc.)
20. Center for Internet Security (CIS) Controls for Effective Cyber Defense
21. OWASP Software Assurance Maturity Model (SAMM)
22. OSI Model (Open Systems Interconnection)
23. OWASP Amass
24. Atlas Mitre (AI Hacking)

1. Cyber Kill Chain
2. HITRUST CSF (Health Information Trust Alliance Common Security Framework)
3. SWIFT Customer Security Controls Framework
4. OVAL (Open Vulnerability and Assessment Language)
5. CAPEC (Common Attack Pattern Enumeration and Classification)
6. SANS Internet Storm Center
7. ATT&CK for Containers
8. Cyber Threat Intelligence Models (Diamond Model, MITRE ATT&CK, etc.)
9. NICE Cybersecurity Workforce Framework
10. EDR (Endpoint Detection and Response) Frameworks
11. National Cyber Range (NCR)
12. Cybersecurity Framework for IoT
13. MITRE Shield
14. ICS-CERT Recommended Practices
15. ICS-CERT Incident Response Plan (IRP) Framework
16. ICS-CERT Security Assurance Framework (SAF)
17. NIST SP 800-53
18. OWASP Mobile Security Testing Guide
19. CAASM (Continuous Adaptive Authentication and Security Monitoring)
20. NIST Cybersecurity Workforce Framework
21. OWASP Internet of Things Project
22. The Open Group Architecture Framework (TOGAF)
23. DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability)

Cybersecurity Risk Assessment Parameters

1. Threat Identification
2. Vulnerability Analysis
3. Asset Criticality
4. Likelihood of Exploitation
5. Impact Assessment
6. Attack Surface Analysis
7. Security Controls Effectiveness
8. Compliance & Regulatory Risks
9. Insider Threat Evaluation
10. Data Sensitivity & Classification
11. Third-Party & Supply Chain Risks
12. Network & Infrastructure Security
13. Endpoint Security Posture
14. Cloud Security Risks
15. Application Security (Web & Mobile)
16. Zero-Day Vulnerability Exposure
17. Incident Response Readiness
18. Access Control & Privilege Management
19. Phishing & Social Engineering Susceptibility
20. Ransomware & Malware Threats
21. DDoS & Availability Risks
22. Encryption & Data Protection
23. Security Awareness & Training Gaps
24. Security Patch & Update Management
25. Threat Intelligence & Emerging Risks

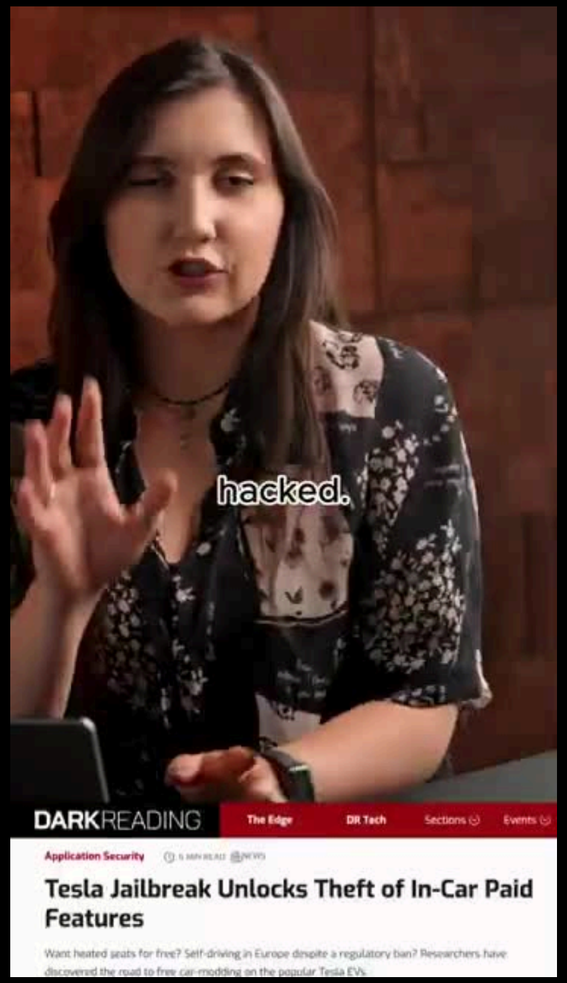
Risk Assessment Parameters in Cybersecurity & Threat Intelligence

- Asset Identification
- Threat Landscape Analysis
- Vulnerability Assessment
- Attack Surface Analysis
- Business Impact Analysis (BIA)
- Data Sensitivity & Classification
- Access Control & Privilege Management
- Third-Party & Supply Chain Risks
- Insider Threats
- Network Security Posture
- Endpoint Security Measures
- Cloud Security Risks
- Application Security Gaps
- Compliance & Regulatory Risks
- Incident Response & Recovery Readiness
- Threat Intelligence Feeds & Indicators of Compromise (IoCs)
- Security Awareness & Employee Training
- Phishing & Social Engineering Exposure
- Advanced Persistent Threat (APT) Detection
- Zero-Day Exploit Exposure
- Malware & Ransomware Readiness
- Security Patch & Update Management
- SIEM & Log Monitoring Effectiveness
- Red Team vs. Blue Team Findings
- Penetration Testing & Security Audits
- DDoS & Availability Risks
- Dark Web Monitoring for Leaked Credentials
- Cyber Insurance & Financial Impact
- Physical Security & Data Center Protection
- Threat Actor TTPs (Tactics, Techniques, and Procedures) Mapping

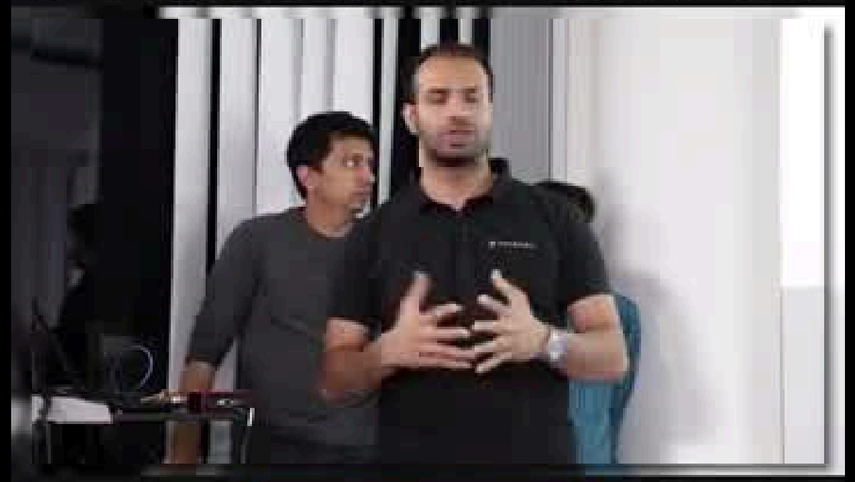
RESOURCES

- https://www.ransomware.live/
- https://www.ransom-db.com/ransomware-groups
- https://threatmap.checkpoint.com/
- https://id-ransomware.malwarehunterteam.com/
- https://ransomwhe.re/
- https://www.nomoreransom.org/
- https://www.halcyon.ai/attacks
- https://cybermap.kaspersky.com/special/ransomware
- https://www.watchguard.com/wgrd-security-hub/ransomware-tracker
- https://www.ctx.io/
- https://threatintelligenceplatform.com/
- https://leak-lookup.com/ https://leakbase.io/threads/venezuela-consorcio-credicard-c-a.31201/
- https://virusscan.jotti.org/#
- https://attack.mitre.org/
- https://atlas.mitre.org/
- https://atm.automotiveisac.com/

https://atlas.mitre.org/matrices/ATLAS
https://airc.nist.gov/airmf-resources/playbook/
https://learn.microsoft.com/en-us/security/ai-red-team/
https://owasp.org/www-project-top-10-for-large-language-model-applications/



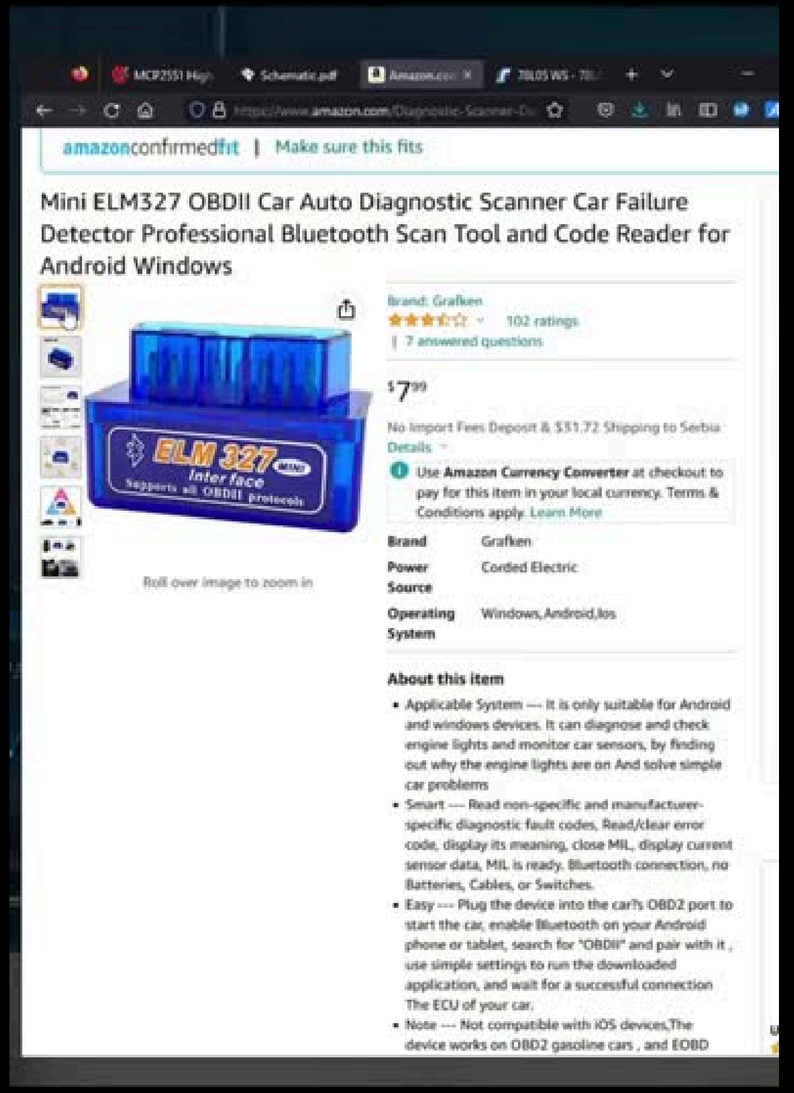
CAR HACKING POSSIBILITIES



THERE ARE TWO TYPES

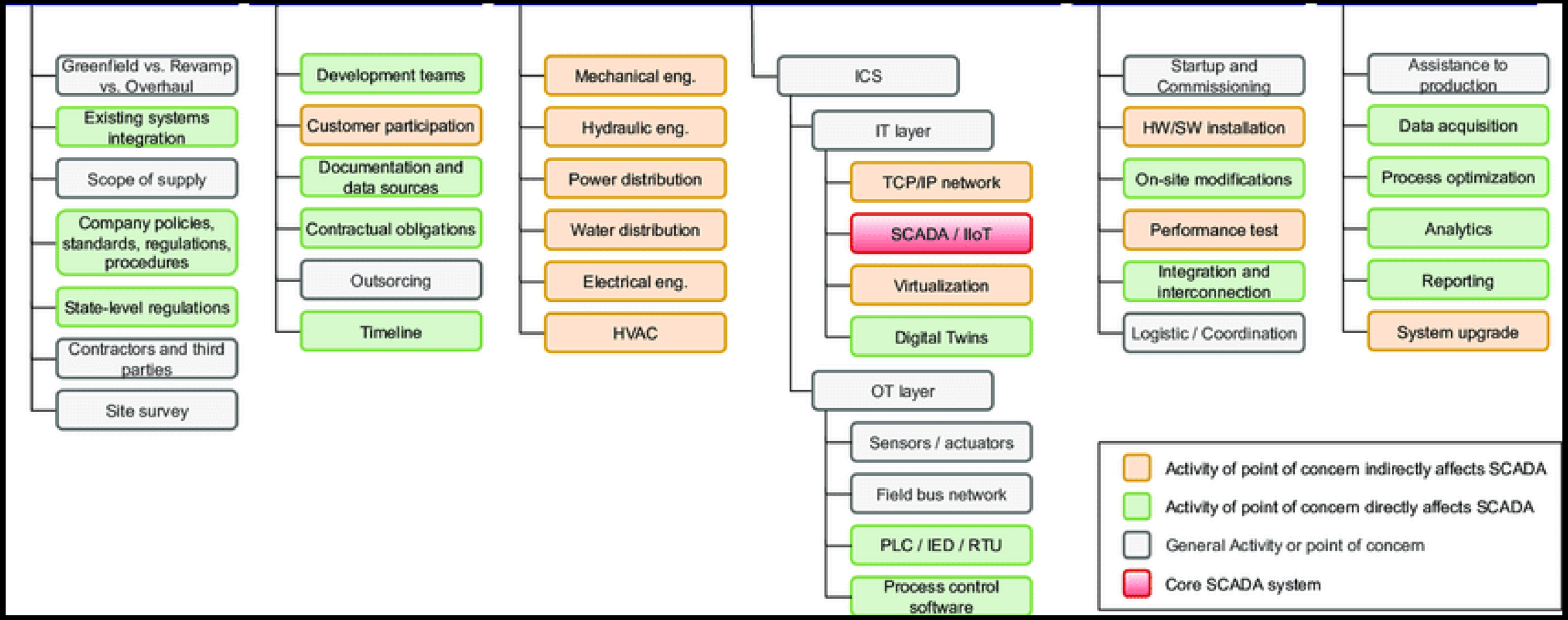

Hacking a vehicle other than your own
is illegal. Jamming is illegal in the UK
and might be illegal in your country too.

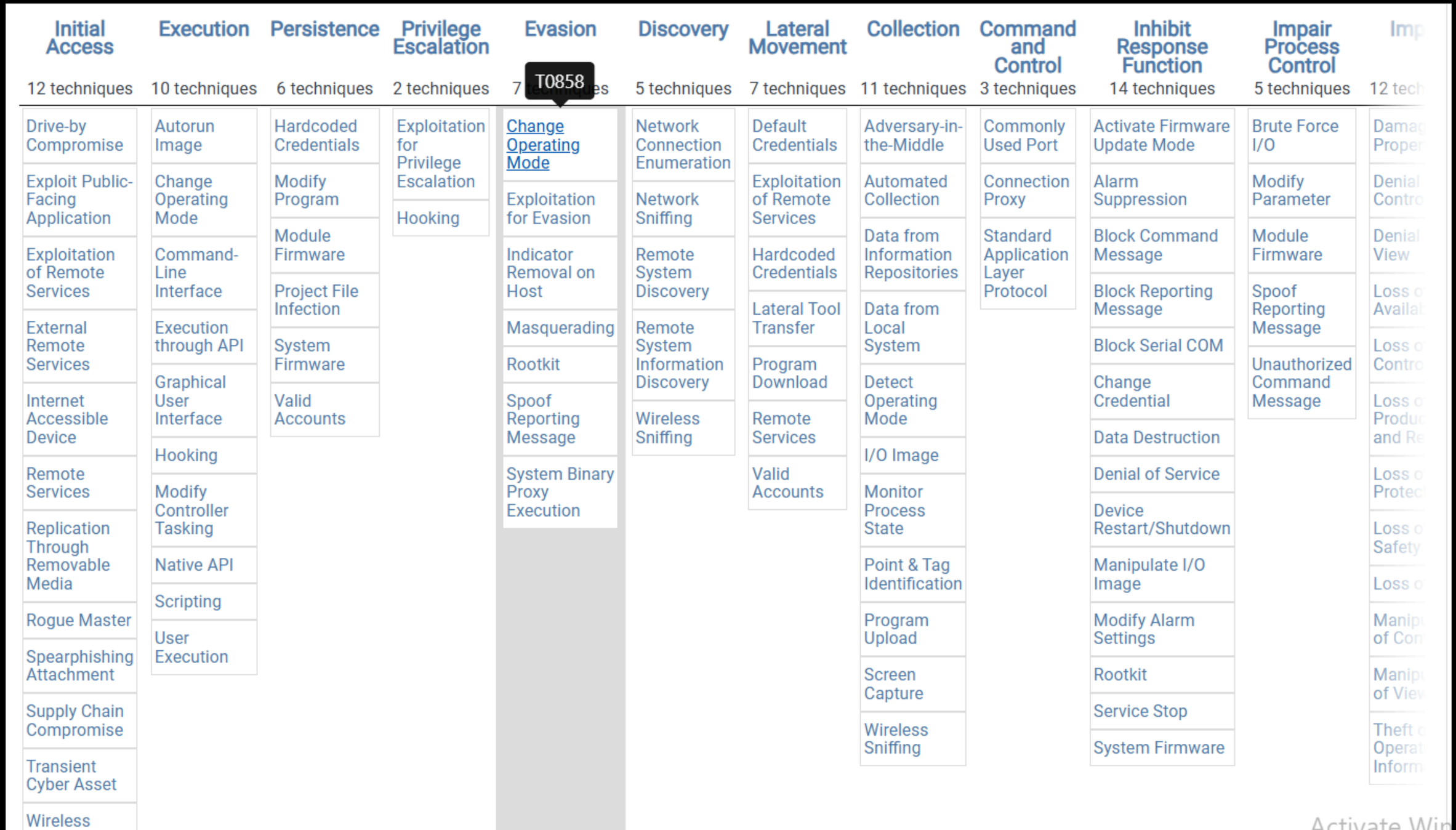

Applications
Sub-GHz
Sub-GHz Remote
FLIPPER
FLIPPER ZERO


amazonconfirmedfit | Make sure this fits
Mini ELM327 OBDII Car Auto Diagnostic Scanner Car Failure Detector Professional Bluetooth Scan Tool and Code Reader for Android Windows
Brand: Grafken
102 ratings
7 answered questions
$7.99
No Import Fees Deposit & $51.72 Shipping to Serbia
Details
Use Amazon Currency Converter at checkout to pay for this item in your local currency. Terms & Conditions apply. Learn More
Brand Grafken
Power Source Corded Electric
Operating System Windows,Android,Ios
ELM 327 MINI
Interface
Supports all OBDII protocols
Roll over image to zoom in
About this item
Applicable System --- It is only suitable for Android and windows devices. It can diagnose and check engine lights and monitor car sensors, by finding out why the engine lights are on And solve simple car problems
Smart --- Read non-specific and manufacturer-specific diagnostic fault codes, Read/clear error code, display its meaning, close MIL, display current sensor data, MIL is ready. Bluetooth connection, no Batteries, Cables, or Switches.
Easy --- Plug the device into the car's OBD2 port to start the car, enable Bluetooth on your Android phone or tablet, search for "OBDII" and pair with it , use simple settings to run the downloaded application, and wait for a successful connection The ECU of your car.
Note --- Not compatible with iOS devices,The device works on OBD2 gasoline cars , and EOBD

THANK YOU

Presentations are communication tools that can be used as lectures, speeches, reports, demonstrations and more.


Greenfield vs. Revamp vs. Overhaul
Existing systems integration
Scope of supply
Company policies, standards, regulations, procedures
State-level regulations
Contractors and third parties
Site survey
Development teams
Customer participation
Documentation and data sources
Contractual obligations
Outsorcing
Timeline
Mechanical eng.
Hydraulic eng.
Power distribution
Water distribution
Electrical eng.
HVAC
ICS
IT layer
TCP/IP network
SCADA / IIoT
Virtualization
Digital Twins
OT layer
Sensors / actuators
Field bus network
PLC / IED / RTU
Process control software
Startup and Commissioning
HW/SW installation
On-site modifications
Performance test
Integration and interconnection
Logistic / Coordination
Assistance to production
Data acquisition
Process optimization
Analytics
Reporting
System upgrade
Activity of point of concern indirectly affects SCADA
Activity of point of concern directly affects SCADA
General Activity or point of concern
Core SCADA system


Initial Access
12 techniques
Drive-by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue Master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless
Execution
10 techniques
Autorun Image
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution
Persistence
6 techniques
Hardcoded Credentials
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts
Privilege Escalation
2 techniques
Exploitation for Privilege Escalation
Hooking
Evasion
T0858
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message
System Binary Proxy Execution
Discovery
5 techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing
Lateral Movement
7 techniques
Default Credentials
Exploitation of Remote Services
Hardcoded Credentials
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts
Collection
11 techniques
Adversary-in-the-Middle
Automated Collection
Data from Information Repositories
Data from Local System
Detect Operating Mode
I/O Image
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing
Command and Control
3 techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol
Inhibit Response Function
14 techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Change Credential
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware
Impair Process Control
5 techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message
Imp
12 tech
Damag
Proper
Denial
Contro
Denial
View
Loss o
Availat
Loss o
Contro
Loss o
Produc
and Re
Loss o
Protect
Loss o
Safety
Loss o
Manipu
of Con
Manipu
of Vie
Theft o
Operat
Inform

Cyber Kill Chain vs. MITRE ATT&CK: An Insightful Comparison

Explore the differences between Cyber Kill Chain and MITRE ATT&CK frameworks. Gain insights into effective cyber defense strategies.

Hornetsecurity – Next-Gen Microsoft 365 Security / Apr 8, 2024

Kubernet threat matrix

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION
Using Cloud Credentials	Exec Into Container	Backdoor Container	Privileged Container	Clear Container Logs
Compromised Images In Registry	BASH/CMD Inside Container	Writable Host Path Mount	Cluster Admin Role Binding	Delete K8s Events
Application Vulnerability	New Container	K8S CronJob	Access Cloud Resources	Connect From Proxy Server
KubeConfig File	Application Exploit (RCE)	**Static Pods**	Pod hostPath Mount	Pod/Container Name Similarity
Compromise User Endpoint	SSH Server Inside Container	**Injected Sidecar Containers**	**Node To Cluster Escalation**	**Dynamic Resolution (DNS)**
K8S API Server Vulnerability	**Container Life Cycle Hooks**	**Rewrite Container Life Cycle Hooks**	**Control Plane To Cloud Escalation**	
			Compromise Admission Controller	
			Compromise K8S Operator	

Attack Scenarios

The list of attack scenarios below is organized by stages. Note that some attacks are only possible during certain flight states.

Reconnaissance	Protocol Tampering	Denial of Service	Injection	Exfiltration
Wifi Analysis & Cracking	Telemetry Spoofing	Battery Drain Attack	MAVLink Command Injection	Flight Log Extraction
Drone Discovery	Flight Mode Spoofing	Communication Link Flooding	Camera Gimbal Takeover	Parameter Extraction
Packet Sniffing	Drone State Spoofing	Denial-of-Takeoff	Waypoint Injection	Mission Extraction
Protocol Fingerprinting	GPS Spoofing	Geo-Squeezing	Sensor Data Injection	FTP Eavesdropping
GPS & Telemetry Analysis		Altitude Limiting	Flight Mode Injection	Camera Feed Eavesdropping
Payload Detection		GPS Jamming		
		Wireless Deauthentication		

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
API Enumeration	Compromised Tokens	Stolen API Keys	Command Injection via APIs	Hijacked Tokens	Role Misconfiguration Exploitation	Obfuscated API Calls	Token Harvesting	Endpoint Probing	API Pivoting	Bulk Data Collection	API-based Command Channel	Data Exfiltration via APIs	Denial of Service (DoS)
Documentation Scraping	Acquisition of Exploit Tools	Broken Authentication	API Abuse for Resource Exhaustion	OAuth Token Manipulation	OAuth Scope Abuse	IP Spoofing	Session Hijacking	Error Message Analysis	Exploiting Third-Party Integrations	Credential Collection	Covert C2 over HTTPS	Unencrypted Data Exfiltration	Data Manipulation
		Exposed Endpoints	Parameter Tampering			Disabling Audit Logs			Exploiting API Chains				Data Encryption (Ransomware)