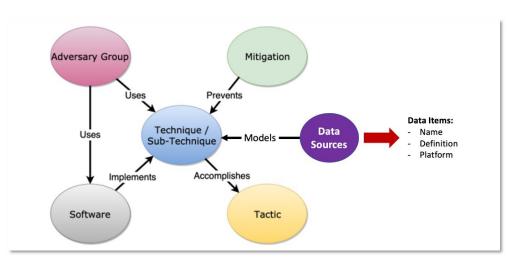
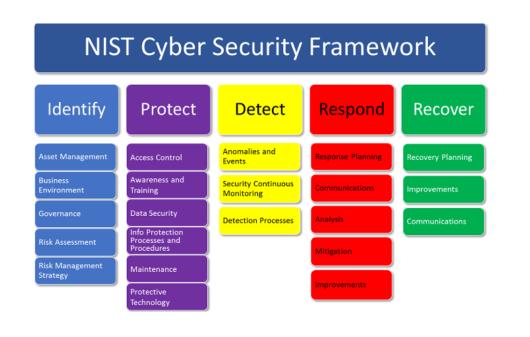
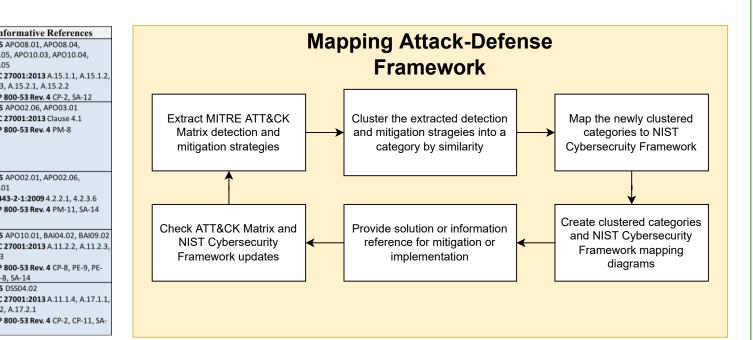
Definition and Diagram



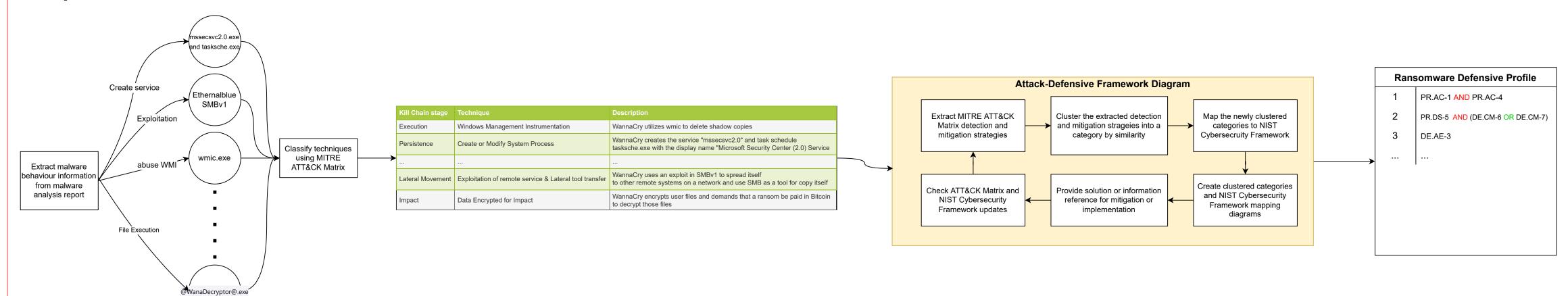
Tactic category	The adversary is trying to	Techniques	
Initial access	to get into your network	11	
Execution	to run malicious code	34	
Persistence	maintain their foothold	62	
Privilege escalation	gain higher-level permissions	32	
Defense evasion	avoid being detected	69	
Credential access	steal account names and passwords	21	
Discovery	figure out your environment	23	
Lateral movement	move through your environment	18	
Collection	gather data of interest to their goal	13	
Command and control	communicate with compromised systems to control them	22	
Exfiltration	steal data	9	
Impact	manipulate, interrupt, or destroy your systems and data	16	
ALL TACTIC EXPLOITS			



nction	Category	ID		Subcategory	Informative References
,	Asset Management	ID.AM		ID.BE-1: The organization's role in the	COBIT 5 APO08.01, APO08.04,
	Business Environment	ID.BE	lh I	supply chain is identified and	APO08.05, APO10.03, APO10.04,
	Governance	ID.GV	[\	communicated	APO10.05
	Risk Assessment	ID.RA] \]		ISO/IEC 27001:2013 A.15.1.1, A.1
	Risk Management Strategy	ID.RM			A.15.1.3, A.15.2.1, A.15.2.2
	Supply Chain Risk	ID.SC)		NIST SP 800-53 Rev. 4 CP-2, SA-12
	Management	10.30		ID.BE-2: The organization's place in	COBIT 5 APO02.06, APO03.01
	Identity Management and	PR.AC]		ISO/IEC 27001:2013 Clause 4.1
otect	Access Control	PR.AC		sector is identified and communicated	
	Awareness and Training	PR.AT		sector is identified and communicated	NIST SP 800-53 Rev. 4 PM-8
	Data Security	PR.DS]		
	Information Protection	PR.IP] [
	Processes & Procedures	FK.IF			
	Maintenance	PR.MA		ID.BE-3: Priorities for organizational	COBIT 5 APO02.01, APO02.06,
	Protective Technology	PR.PT		mission, objectives, and activities are	APO03.01
	Anomalies and Events	DE.AE		Land Carlotte	ISA 62443-2-1:2009 4.2.2.1, 4.2.3
etect	Security Continuous	DE.CM			NIST SP 800-53 Rev. 4 PM-11, SA-
tect	Monitoring	DE.CIVI			14131 3F 800-33 Rev. 4 FW-11, 3A-
	Detection Processes	DE.DP			
	Response Planning	RS.RP		ID.BE-4: Dependencies and critical	COBIT 5 APO10.01, BAI04.02, BAI
	Communications	RS.CO		functions for delivery of critical	ISO/IEC 27001:2013 A.11.2.2, A.1
pond	Analysis	RS.AN		services are established	A.12.1.3
	Mitigation	RS.MI			NIST SP 800-53 Rev. 4 CP-8, PE-9,
	Improvements	RS.IM			11, PM-8, SA-14
cover	Recovery Planning	RC.RP		ID.BE-5: Resilience requirements to	COBIT 5 DSS04.02
	Improvements	RC.IM]	support delivery of critical services are	ISO/IEC 27001:2013 A.11.1.4, A.1
	Communications	RC.CO]		A.17.1.2, A.17.2.1
					NIST SP 800-53 Rev. 4 CP-2, CP-11
			(14



Sample in detail



Extract MITRE ATT&CK Matrix detection and mitigation strategies

Create or Modify

System Process

Exploitation of

Remote Services

- Code Signing

- Command

Process

 Exploit protection Mitigation - Network Segmentation

Network Traffic

- Service

Detection - Windows Registry

Detection - Application Log

- Driver

- Behavior Prevention on Endpoint

Application Isoliation and Sandboxing - Disable or remove feature or program

- Privileged account management Threat Intelligence program

- Limit Software Installation - Operating System Configuration

- Restrict File and Dictionary

- User account management

Cluster the extracted detection and mitigation strategies into a category by similarity

Category	Sub-Category		Category	Sub-Category	NIST Cybersecurity Framework
Audit	- Audit	→	Audit	- Audit	(PR.DS-6 AND PR.DS-8)AND PR.PT-1 AND DE.CM-8 AND PR.AC-1
Prevention & Protection	- Behavior Prevention on Endpoint - Exploit Protection		Prevention & Protection	- Behavior Prevention on Endpoint - Exploit Protection	ID.SC-1 AND ((PR.DS-1 AND PR.DS-2) OR PR.DS-4) AND PR.PT-2 AND DE.AE-2 AND (DE.CM-4 OR DE.CM-5) AND DE.CM-7
Validation or checksum	- Code signing		Validation or checksum	- Code signing	PR.DS-6
Limitation	- Limit software installation - Disable or remove feature or program		Limitation	- Limit software installation - Disable or remove feature or program	PR.PT-3
Configuration	- Operating System Configuration		Configuration	- Operating System Configuration	PR.PT-3 AND PR.IP-3
Privilege & permission	- Restrict File and dictionary permissions		Privilege & permission	- Restrict File and dictionary permissions	PR.AC-4
Account management	- User account management - Privileged account management		Account management	- User account management - Privileged account management	PR-AC-4 AND PR.AC-7
Intelligence capability	- Threat Intelligence program		Intelligence capability	- Threat Intelligence program	ID.RA-2
Logging	- Command - Driver - File - Process - Service - Windows Registry - Application Log - Network Traffic		Logging	- Command - Driver - File - Process - Service - Windows Registry - Application Log - Network Traffic	DE.AE-3 AND DE.CM-7

AND/OR Logic in NIST Cybersecurity Framework Provide solution or information reference for mitigation or implementation

All inputs through the 'AND' gate

needs to be fully or largely

implemented

At least one of inputs through the

'OR' gate need to be fully or largely

implemented

Example: (PR.DS-1 AND PR.DS-2) OR PR.DS-4

PR.DS-1

PR.DS-2

PR.DS-4

If user choose any subcategory of NIST CSF, they should go to check detail at NIST CSF Core.

For example, User choose PR.DS-3 to implementation. User go to check at NIST CSF Core and choose one standard for implementation.

ı	1	· CIS CSC I
		· COBIT 5 BAI09.03
J	PR.DS-3: Assets are formally managed	· ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1
	throughout removal, transfers, and disposition	· ISA 62443-3-3:2013 SR 4.2
		· ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7
		· NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
ı	•	