# Comparison of Attack Chains: APT1 vs. APT29 Using MITRE ATT&CK Navigator By Pranith Jain

#### Overview

This report examines the attack chains of two prominent Advanced Persistent Threat (APT) groups, APT1 and APT29, using the MITRE ATT&CK framework as a basis for comparison. APT1, attributed to a Chinese state-sponsored actor, is known for its widespread cyber-espionage activities across various industries. In contrast, APT29, linked to Russian intelligence, is renowned for its sophisticated and stealthy operations, particularly targeting governmental and diplomatic sectors.

By leveraging the MITRE ATT&CK Navigator, this report provides a detailed comparison of the tactics, techniques, and procedures (TTPs) utilized by these groups. The analysis highlights commonalities in their methodologies while underscoring the unique approaches each group employs to achieve their objectives. This comparison not only enhances our understanding of these specific threat actors but also offers insights into improving cybersecurity defenses against similar threats.

#### 1. Introduction

Advanced Persistent Threats (APTs) are sophisticated, long-term cyber-espionage campaigns carried out by well-funded and highly skilled threat actors. Two of the most notable APT groups are APT1 and APT29. APT1, attributed to a Chinese state-sponsored group, is known for its extensive cyber espionage operations targeting a broad range of industries. On the other hand, APT29, believed to be associated with Russian intelligence, is recognized for its stealthy operations and focus on government and diplomatic entities.

#### 2. Methodology

The comparison was conducted using the MITRE ATT&CK Navigator, a tool that allows users to create and visualize layers of TTPs used by various threat groups. The following steps were taken:

- 1. Laver Creation: Created separate layers for APT1 and APT29, enabling a side-by-side comparison.
- **2. Data Collection:** Loaded the TTPs associated with APT1 and APT29 from the MITRE ATT&CK database into the Navigator.
- **3. Analysis**: Compared the layers to identify common and unique TTPs across different stages of the attack lifecycle.
- 4. **Documentation:** Captured insights and visual evidence from the Navigator to include in this report.

#### 3. Analysis

#### 3.1 Initial Access

- APT1: Frequently uses phishing attacks with malicious attachments or links to gain initial access. They also exploit vulnerabilities in web-facing applications.
- APT29: Also relies heavily on spear-phishing but is known for using more sophisticated social engineering techniques. Additionally, APT29 exploits supply chain compromises as part of their initial access.

Comparison: Both APT1 and APT29 use phishing as a primary method for initial access, though APT29 tends to employ more advanced techniques and also targets supply chains.

#### 3.2 Execution

- APT1: Commonly uses malware to execute code after gaining initial access, with tactics such as scheduled tasks and command-line interface (CLI) tools.
- APT29: Leverages various execution techniques, including the use of legitimate credentials to blend in with normal network traffic. They are also known for using customized malware.

Comparison: While both groups use malware and legitimate tools, APT29's approach is more nuanced, often attempting to remain under the radar by mimicking legitimate activities.

#### 3.3 Persistence

- APT1: Maintains persistence through the use of web shells, creating new user accounts, and utilizing backdoors.
- APT29: Uses stealthier methods such as maintaining legitimate remote access tools and embedding backdoors within legitimate software updates.

Comparison: APT1 often relies on creating artifacts that are easier to detect, whereas APT29 prioritizes stealth and evasion, making them harder to detect over long periods.

#### 3.4 Privilege Escalation

- APT1: Exploits known vulnerabilities in operating systems and software to escalate privileges.
- APT29: Similar in approach but often utilizes zero-day vulnerabilities to gain higher privileges without detection.

Comparison: APT29 has a more advanced arsenal for privilege escalation, often using sophisticated zero-day exploits.

#### 3.5 Defense Evasion

- APT1: Uses techniques such as file obfuscation and disabling security tools.
- APT29: Employs advanced evasion techniques, including process hollowing, fileless malware, and exploitation of trust relationships to avoid detection.

Comparison: APT29's defense evasion techniques are significantly more advanced and are designed to avoid detection for extended periods.

#### 3.6 Command and Control (C2)

- APT1: Uses compromised infrastructure for C2, often relying on HTTP/S, DNS, and custom protocols.
- APT29: Operates through encrypted channels and often uses multi-layered C2 infrastructures to obscure communications.

Comparison: APT29's C2 operations are more sophisticated, using encryption and multi-layered approaches to protect their command and control mechanisms from being intercepted.

#### 3.7 Exfiltration

- APT1: Typically exfiltrates data via compressed archives sent over HTTP/S or FTP.
- APT29: Employs more covert methods, including embedding exfiltrated data in legitimate network traffic or using encrypted communications.

Comparison: APT29's methods of exfiltration are more covert and harder to detect compared to APT1's more straightforward approach.

#### 4. Conclusion

The comparison between APT1 and APT29 reveals both commonalities and differences in their attack chains. While both groups employ similar tactics, such as phishing for initial access and using malware for execution, APT29 demonstrates a higher level of sophistication and stealth across the entire attack lifecycle. Their techniques for defense evasion, persistence, and C2 are particularly advanced, indicating a significant investment in avoiding detection and maintaining long-term access to compromised environments.

For organizations, understanding these differences is crucial for developing effective threat detection and response strategies. By focusing on the advanced techniques used by groups like APT29, security teams can better prepare for and mitigate the risks posed by these and similar threat actors.

#### 5. Visual Representation

## APT1:

APT1				filters				score gradient 1 100			
				ptatjesmact	Vindows, Lii	nux, macOS					
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Contraind And	Exfiltration	Impact
11 items	34 items	.bash profile and .bashro	32 items	69 items	21 items	23 items	18 items AppleScript	13 items Audio Capture	22 items	9 items Automated Exfiltration	16 items
Drive-by Compromise Exploit Public-Facing	AppleScript CMSTP	.bash_profile and .bashro Accessibility Features	Access Token Manipulation Accessibility Features	Access Token Manipulation Binary Padding	Account Manipulation Bash History	Application Window Discovery	Application Deployment	Audio Capture	Commonly Used Port Communication Through	Automated Exhitration	Account Access Removal  Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	RITS John	Brute Force	Browser Bookmark	Component Object Model and Distributed COM Exploitation of Remote	Clipboard Data	Occasional Design	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account	Credential Dumning	Domain Trust Discovery	Exploitation of Remote	Data from Information Repositories	Custom Command and Custom Cryptographic Custom Cryptographic Protogol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	Applnit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items  Dynamic Data Exchange	Application Shimming Authentication Package	Bypass User Account DLL Search Order Historia	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Data from Removable Media	Data Encoding Data Obfuscation	Exfiltration Over Command and Control Channel Exfiltration Over Other	Disk Structure Wipe Endpoint Denial of Service
Spearphishing Link Spearphishing via Service	Execution through API	RITS John	Dylib Hilacking	Code Signing Compile After Delivery	Credentials in Registry Exploitation for Credential	Network Sniffing	Pass the Ticket	Media Data Staged	Domain Fronting	Exfiltration Over Other Network Medium Exfiltration Over Physical Medium	Firmware Cornintion
Supply Chain Compromise	Execution through Module	Bootkit	Elevated Execution with	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	December Entennione	Emond	Component Firmware Component Object Model	Hooking	Peripheral Device	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File	Exploitation for Privilege extra Window Memory		Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil Launchetl	Component Firmware Component Object Model		Connection Proxy Control Panel Items	Input Prompt	Process Discovery	Removable Mediar Shared Webroot	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Local Job Scheduling	Create Account	File System Permissions Weakhess Hooking	DCShadow	Kerberoasting Keychain	Query Registry Remote System Discovery	SSH Hijacking	Video Capture	Multiband Communication Multilayer Encryption	1	Service Stop Stored Data Manipulation
	LSASS Driver	DLL Search Order	Image File Execution	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning	Security Software	Taint Shared Content	1	Port Knocking	1	System Shutdown/Reboot
	Mshta	Dyllo Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software	1	Remote Access Tools	]	Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hilacking	Password Filter DLL	System Information Discovery	Windows Admin Shares Windows Remote	4	Remote File Copy Standard Application Layer Protocol	-	
	Regsvcs/Regasm Regsvr32	External Remote Services File System Permissions Weakless	Parent PID Spoofing Path Interception	DLL Side-Loading Execution Guardraits	Private Keys Securityd Memory	Challouration Discovery System Network	Management Management	1	Standard Cryptographic		
	Rundli32	Weakhess Hidden Files and Birectories	Plist Modification	Exploitation for Defense	Steal Web Session Cookie	System Owner/User			Standard Non-Application		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory	Two-Factor Authentication	System Service Discovery			Uncommonly Used Port	1	
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Collines Injection Kernel Modules and	Process Injection	File Deletion		Virtualization/Sandbox	_				
	Signed Binary Proxy Execution Signed Script Proxy Execution	Extensions Launch Agent	Scheduled Task Service Registry Permissions Weakness	File System Logical Offsets Gatekeeper Bypass							
	Source	Launch Daemon	Permissions Weakness Setuid and Setgid	Group Policy Modification							
	Space after Filename	Launchetl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users							
	Trap Trusted Developer Utilities	Local Job Scheduling Login Item	Sudo Caching	Hidden Window							
	User Execution	Login item Login Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Management	LSASS Driver	Web Shell	Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service Office Application Startup		Indirect Command Execution Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchoti							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		PowerShell Profile Rc.common		Modify Registry Mshta							
		Re-opened Applications		Network Share Connection							
		Redundant Access	1	NTES File Attributes	1						
		Registry Run Keys / Startus Forder		Obfuscated Files or information							
		Scheduled Task		Parent PID Spoofing Plist Modification							
		Screensaver Security Support Provider		Plist Modification Port Knocking							
		Security Support Provider Server Software		Process Doppelgänging							
		Service Registry Permissions Weakness	1	Process Hollowing							
		Setuid and Setgid		Process Injection							
		Shortcut Modification		Redundant Access							
		SIP and Trust Provider Hisacking Startup Items		Regsvcs/Regasm Regsvr32							
		System Firmware		Regsvr32							
		Systemd Service		Rundli32	1						
		Time Providers		Scripting							
		Trap		Signed Binary Proxy Execution Signed Script Proxy							
		Valid Accounts Web Shell		Signed Script Proxy Execution SIP and Trust Provider							
		Kondowe Weekelener		Rijacking Software Packing							
		Winlogon Helper DLL		Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities Valid Accounts							
				Virtualization/Sandbox							
				Web Service	1						
				XSL Script Processing	I						

### **APT29:**

Herboten Additions Composed HTML File Segregation (1997) Segregation (	APT29		•		filters	•			score gradient			
11 January   12					ptatfesmact	Windows, Lir	nux, macOS		100			
Control   Cont								Lateral Movement				
Sign Park   Company   Co								Apple Script				
Transport Company of the Company of	Exploit Public-Facing Application				Binary Padding		Application Window	Application Deployment	Automated Collection			
Transport Company of the Company of	External Remote Services						Browser Bookmark	Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	
Part	Hardware Additions	Compiled HTML File				Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services		Custom Command and Control Protocol	Data Transfer Size Limits	
Companying as   Companying a		and Distributed COM	Applnit DLLs	Application Shimming		Browsers Trom VVeb		Internal Spearphishing	Data from Local System	Protocol Protocol		
Company of the Comp				Confrol DI Search Order		Overdontials in Decision			Data from Removable			
Supplement   Sup						Exploitation for Credential					Network Medium Exfiltration Over Physical	
Transch indicative   Springer Former   Company   Former   Company   Company		Execution through Module					Password Policy Discovery				Scheduled Transfer	
Description   Compound From Prince   Compou		Exploitation for Client	Browser Extensions	Emond	Component Firmware		Perinheral Device					
Description   Compound From Prince   Compou	Valid Accounts	Graphical User Interface	Change Default File	Exploitation for Privilege	Component Object Model	Input Capture	Permission Groups		Man in the Browser	Multi-hop Proxy		Resource Hijacking
Lood als Cardady Cortin According House Control Control House Control Ho			Component Firmware		Connection Proxy		Process Discovery					
LOSS Developed (Loss of the Control of Control Control of Control Control of Control Control of Control Contro			Hisacking						Video Capture		4	
March   Chief Mayoring   Cannot Distance   Chief Sept Month   Chief			Ureate Account DLL Search Order	Image File Execution	Deobfuscate/Decode Files	LUMNR/NBT-NS Poisoning	Remote System Discovery Security Software		-		1	
Parent Plant   Crood   New Service   This plant   Crood   Parent P									4		+	
Region Region Comman Remote Reviews Property Projection Command Region (Command Region Command Region Re					DLL Search Order		System Information		+		1	Manipulation
Register 22   Billion Personal Personal Personal Procession Countries   Register 22   Billion Personal			External Remote Services		DLL Side-Loading		System Network	Windows Remote	1	Standard Application Layer	1	
Scheduling Task   Secondary		Regsvr32	File System Permissions	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery	management.	-	Standard Cryptographic	1	
Service Secolar Policy Expension Process injection Process injecti		Rundl32		Plist Modification		Steal Web Session Cookie				Standard Non-Application		
Personal Security of Programme Communication (Programme Communication Co						Two-Factor Authentication Interception						
Segretal prices in Process  George Lannot Demons and England England  Tour Lannot Agent Membra Schools and Agent Schools			Hypervisor				System Time Discovery	4		Web Service	]	
Security County		Service Execution Signed Binary Proxy	Options Injection  Kernel Modules and				Evasion	_				
Source of Launch Charmon Signow after Financian Launchind Lau		Signed Script Proxy	Extensions Launch Agent	Service Registry		-						
Spora after Filewares Tribig party Orbital Trip  Well Common Comm		Source		Setuid and Setoid		1						
Trape Developer Utilises  Trained Developer Utilises  Will See See See See See See See See See S		Space after Filename	Launchetl		Hidden Files and Directories							
Tradeo Developer Utilities User Execution Logon Service User Execution Modern (Logon Revenue) Modern (Logon Revenu												
User Securior   User Story   Valet Accounts   Figure 1   Experience   Valet Story												
Wedge   Section   Wedge   Section					Image File Execution	-						
Windle Eventry Genome   Logogato Removal on Hord   Logogato Removal on Ho		Windows Management	Logon Scripts		Online Injection	+						
Most Nervor Processing   Noth helper DLL   New Servor		Vindows Remote		TVEO SHEII	Indicator Removal from	1						
Office Applications Statute Part Interior Statute Part Modification Control of the Control of th				1								
Office Applications Statute Part Interior Statute Part Modification Control of the Control of th			New Service	1	Indirect Command							
Part Monitorian Port Monitoria												
Port Noncaing Pout Shall Profile												
Port Monitors  Power Monitors				-		-						
Powerford Profile  Rocement Applications  Rocement Rocement  Rocement Rocement  Society Support Provider  Proves Rocement  Proves Rocement  Proves Rocement  Proves Rocement  Proves Rocement  Proves Rocement				+	Masouerading	+						
Recommend Applications Redundant Access Redundant Redu				1		1						
Redunded Accounts    Part   Part   Part   Part   Part			Rc.common	1	Mshta	1						
Begangs Fees Com- Checkeder Task Growmaner Growmaner Growmaner Growmaner First Modification Fort Rockeding First Modification First Modific				]	Network Share Connection Removal	]						
Serveduled Tax  Screening Support Product  Decoration Support Product  Decoration Support Product  Decoration Support Product  Decoration Support Product  Statuta and Stagis  Decoration Support Statuta  Decoration Statuta  Dec			Redundant Access									
Scrownsaer Scrout's (speptif Provider Port Knocking Port Knocking Port Knocking Port Knocking Process Doppelighting Process Doppelighting Process Doppelighting Process Doppelighting Process Doppelighting Process Popting Stock Modification Plant of Process Popting Stock Modification Plant of Process Popting Stock Modification Plant of Process Popting 37 control Modification Poptin			Startius Forder	-		-						
Gecurity Gapport Provider    Provider				1		+						
Server Software  Bernoas Dospolatora  Bernoas Dospolatora  Bernoas Bernoas  Service Selection  Bernoas  Bernoas			Security Support Provider	1		1						
Biffords Collegia Managests Ground Modellandon Bifford Modellandon			Server Software	1		1						
Betutal and Settings  Chocate Modification File gray Trust Privated File gray Trust Private File g			Service Registry Permissions Weakness	1		1						
Beginsch Pergater   Shatep times   Beginsch Pergater			Setuid and Setgid	]								
Startup forms Syptem Firmware System Genrice Flooritie Trane Flooritie Trane Valid Accounts Web Dreit Web Dreit Web Dreit Web Dreit Web Dreit Flooritie Flor				1		1						
Spylant Firmane   Spylant Firmane   Time Providers			Air and Trust Provider	4	Regsvcs/Regasm	4						
System Service Trans Providers Trans Providers Valid Accounts Vivide Trans System State System Syste				-		-						
Trans Providers Trage Vale Accounts Vale Acc				+		1						
Trap  Vasid Accounts  Vivid Accounts  Vivid David  Vivid				1		1						
Valid Accounts   Spring Spring Privay				1	Signed Binary Proxy	1						
Schware Packing				1	Signed Script Proxy	1						
Software Packing  Writingon Helger DLL  Space after Financian  Template Injection  Timuster  Trusted Developer Utilities  Valid Accounts  Yeth Accounts  Yeth Service  Verile Service  Verile Service  Verile Service				1	SIP and Trust Provider							
Template Injection Timatorion Timatorion Tinuted Developer Utilities Valla Accounts Yesta Accounts Yesta Service Verse Service Verse Service				4	Software Packing							
Timesterry Trusted Developer Utilities Valat Accounts Yringuezion Sannbox Vives Service Vives Service			Vnnrogon Helper DLL	J		+						
Trusted Developer Utilities Valid Accounts Yurn, adjactation/Sarotidos Web Sevice Web Sevice						1						
Valid Accounts Yiff has action Sendox Uses Service Verb Service						1						
Web Service					Valid Accounts	1						
XSL Script Processing						1						
					XSL Script Processing	1						

## Comparison APT1 and APT29:

Agricultural Description (Courted Forum Imm.) Agricultural Descripti		score gradient 1 3						filters			APT29	APT1+
1 Bears						nux, macOS	Windows, Lii	ptatfesmact				
Access for foreigness  Approximate  Approxim	Impact		Control And			Discovery		Defense Evasion	Privilege Escalation			
Column   C	16 items Account Access Remov					23 items						
Accord Management (Control Prince   P	Data Destruction	Data Compressed	Communication Through	Automated Collection	Application Deployment	Application Window						xploit Public-Facing
Appelland List State of Common Hard Internal Appelland State of Common Hard Internal A	Data Encrypted for Imp	Data Encrypted	Connection Proxy	Clipboard Data	Component Object Model	Browser Bookmark	Brute Force					xternal Remote Services
Secretary Law Control Franch Brown (Application Dates)  Application Description (Application Franchisto)  Control Franchisto Franchisto (Control Spring)  Control Franchisto Franchisto (Control Franchisto)  Control Franchisto (Control Franchisto)  Control Franchisto Franchisto (Control Franchi		Data Transfer Size Limits	Custom Command and Control Protocol	Data from Information Repositories		Domain Trust Discovery	Credential Dumping	Bypass User Account		AppCert DLLs		
Searching of Emilian Contracts Probaga Part (Contract Probaga) Part (Contract	nand Disk Content Wipe Disk Structure Wipe			Data from Local System  Data from Network Shared					Application Shimming Bypass User Account			
Emotion Brough API   Bit St. dots   Dyth Higheing   Composed Parties	Endpoint Denial of Serv	Extiltration Over Other	Data Obfuscation		Pass the Hash	Network Share Discovery	Crarlentials in Registry		BLL Search Order			
All Accounts Control User Institute Security (Control User Institu	Cal Firmware Corruption	Exfiltration Over Physical Medium	Domain Fronting	Data Staged	Pass the Ticket			Compile After Delivery	Dulih Mincking		Execution through API	
An Account of Accounts of Acco	Inhibit System Recover			Email Collection	Remote Desktop Protocol	Password Policy Discovery					Execution through Module	
Haushold Composed Filmers Lauched Englower Glogical Model Composed	Network Denial of Servi Resource Hijacking					Discovery  Permission Groups		Component Firmware Component Object Model		Browser Extensions Change Default File	Execution	
Learning Committed Systems (September Specific S	Runtime Data Manipula				Replication Through	Process Discovery			Extra Window Memory	Component Firmware		ind Accounts
Local Ass Scheduling Contact Account (Fig. 1) (Scheduling Contact Cont	Service Stop					Query Registry	Kerberoasting			Component Object Model		
Abota	Stored Data Manipulat					Remote System Discovery	Keychain		Hooking	Create Account		
ReproceRingsom Regron-Regional Regron-Re	System Shutdown/Reb Transmitted Data Manipulation			1			LLMNR/NBT-NS Poisoning and Relay					
Regrest Plans Services From Remote Services Plans Services From Remote Services Plans Services From Remote Service	Manipulation		Remote Access Tools	-		Software Discovery System Information		Disabling Security Tools  DLL Search Order				
Registriz   Discontinues and Peter Montrolland   Peter Montrolland		1	Standard Application Layer	1		System Network						
Rounting Generation From Honology From Honol			Standard Cryptographic	•	манадетеп	System Network Connections Discovery	Securityd Memory	Execution Guardrails	Path Interception	File System Permissions		
Service Execution Service Management Management Management Part Interded Service Part Interded Service Service Management Management Part Interded Service Part Interded Service Service Management S			Standard Non-Application Layer Protocol			System Owner/User Discovery	Steal Web Session Cookie	Exploitation for Defense	Plist Modification	Hidden Files and Directories	Rundli32	
Service Execution  Service Service Service  Service Service Service  Service Service Service  Service Service Service  Service						System Service Discovery	Two-Factor Authentication Interception					
Spring Register From J.  Spring Register From		l .	Web Service							Hypervisor		
Source Launch Damon Status and Seguing Company Physiological Company (Control Seguing Company Control Seguing					J	Evasion			Schoduled Task	Cettons Injection Kernel Modules and		
Source   Laurich Damon   Stellar and Stelged   Orcup Priory Modification   Space after Filamany Schower   Laurich Damon   Stellar and Stellar   Stellar and Stellar and Stellar   Stellar and Stel								Gatekeeper Bypass			Signed Script Proxy	
Trop only Software I. C. (LOAD DYTH Addition) Travel County as Starting South Software Interest Intere								Group Policy Modification	Setuid and Setgid	Launch Daemon	Source	
Trape Local 20 Scheduling Sudo Checkery History Windows  Trusted Developer Utilizes (Logn Rem Sudo Cachery History CAPTROC)  Lase Execution Logn Graphs Valid Accounts Profession History Captro History												
Treated Developer United  User Execution  User Execution  Void Control Logon Screen  Void Control  Part Note Control  Part No												
Liver   Execution							•					
Vocations (Septiment)  Most Factoring Service  Note In Higher CLL  Note Control Service  Note In Higher CLL  Note Control Service  Note In Higher CLL  Note Control Service  Path Interception  Path Interception  Path Interception  Path Modification  Per Knooling  Per Knooling  Per Control Service  Per Control Service  Recomment							1	Image File Execution				
West Service  XSIs, Sorpt Processing  XSIs, Sorpt Processing  Ness Service  Ness Service  Ness Service  Ness Service  Ness Service  Part Modification  Part Modification  Part Modification  Port Modification  Port Modification  Port Modification  Port Modification  Port Modification  Port Modification  Ness Service  Ness Se							1	Indicator Blocking	Web Shell	LSASS Driver	Windows Management Instrumentation	
New Service  Chick Agelactors Statup Path Interception Path Montification Path Montification Path Condition Path Montification Path Montific								Indicator Removal from				
Office Application Starting Part Interruption Fall Interruption Fa								Indicator Removal on Host			XSL Script Processing	
Path Indicaction  Path Modification  Recomment  Recomm							1	Execution Install Post Conficate	-			
Pint Modification Peri frocidation Peri												
Port Menotores Powerfords Profile Re common Response Resp							1	Launchetl	1	Plist Modification		
PowerFolia Profile Re. common Re. common Re. period Applications Re. period Applications Responsed Applications Re								LC_MAIN Hijacking	]			
Re common  Re coperated Registrations  Reput Market  Reput												
Re-opened Applications Redundant Accesses Signify 7,900, Fore 1 Signify 7,900, Fore 2 Signify 7,900, Fore 3 Si							1		+			
Read-moder Access NTTS File Attributions Significant Access NTTS File Attributions Schoolsack Task December 1975 Schoolsack Task Person PCD Schooling Schoolsack State File Access Schoolsack Schoolsa							1		1			
Someration of the Control of Sporting  Someration of Sporting  Someration of Sporting  Someration of Sporting  Someration of Sporting  Sporting Sp							1	NTFS File Attributes	1	Redundant Access		
Somewater  Beacurify Support Provider P								Information		Stattup/Folder		
Security Support Proviser  Byone Support Support  Process Process Process  Process Process Process  British God Williamses  Setud and Segue  Brock Modification  Brock Modification  Regular Process  Regular Regular  Regular Regular  Regular Regular  Regula							1					
Section and Selgid							1		+	Screensaver		
Sentia and Selgids Process Injection  Shortcut Modification IDI egg 7 milet Provider Registraci Registraci Sturtup Items System Firmware System Firmware Registraci Registraci System Service Firm Providers Timp Providers Timp Valid Accounts Verdi Shell Web Shell IDI egg 7 milet Provider IDI egg 8 milet Privaty Valid Accounts Verdi Shell IDI egg 7 milet Privaty IDI egg 8 milet Privaty IDI egg 9 milet Privaty IDI							1		1	Server Software		
Section and Selgid Process Repection  Shortcat Modification Shortcat Modification Sill agg 7 mark Proceder Shortcat Repeated Register Shurtup Brens Shurtup Brens Shurtup Brens System Firmware Register System Firmware Fiscolit System Sarvice Time Providens Time Providens Timp Timp Varial Accounts Wed Sheel Sill agg 7 mark Provider Segregation State Provider Sill agg 7 mark Provider							1		1	Service Registry		
Start   Private							1	Process Injection	1	Setuid and Setgid		
Sturfup Barea   Fingspart2										Shortcut Modification		
System Firmware System Garvice True Providers True Providers Trap Spring Genry Provy Vaid Accounts Web Shell System Syste												
Systems Service Time Providers Signify Systems												
Trap Segreg Status Priory Vaild Accounts Segreg Status Priory Version Status Segreg Priory Wes Sheet William July Towndar Hill Imply July Priorder								Rundli32	1			
Viets Shell Blaggior								Scripting	1	Time Providers		
Viets Shell Blaggior								Signed Binary Proxy Execution	]	Trap		
							1	SIP and Trust Provider	1			
								Software Packing		Web Shell Kondows Management		
Bissupprogrammer Software reacong Viringon Helper D.L. Space after Flename									-	Winiogon Helper D.L.		
Vintogori resperatus.  Sopuse enter remaine  Template ligication							1		,	gon respectives		
Timestomp							1	Timestomp				
Trusted Developer Utilities							1					
Valid Accounts Yimaga attorio Sarefloox							1	Valid Accounts Virtualization/Sandbox				
Production of the Control of the Con							1	Evasion Web Service				
viveo Servicio XSL Script Processing							i					