about ————————————————————————————————————					domain ————————————————————————————————————					platforms Linux, macOS, Windows, PRE, Containers, Network, Office 365,				
Capa con la y técnicas c	as tácticas que usa el ran:	somware Pys	a.							SaaS, Google Workspace, IaaS, Azure AD				
Reconnaissance	Resource Development	Initial Access	Execution	n Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Contro	ol Exfiltration	Impact	
T1595: Active Scanning T1592: Gather	T1583: Acquire Infrastructure T1586:	T1189: Drive-by-Compromise T1199: Evelop	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T154E Abuse Elevation Control Mechanism T154E.002: Bypess	T1548: Abuse Elevation Control Mechanism	T1557: Adversary in the Middle	T1007: Account Discovery T1010: Application	T1210: Exploitation of Remote Services	T1557: Adversary-in-the-Middle	T1071: Application Layer Protocol	T1020: Automated Exfitration T1030: Data	T1531: Account Access Removal	
Victim Host Information T1589: Gather Victim	Compromise Accounts T1584: Compromise	T1190: Exploit Public-Facing Application T1133: External Remote Services	AppleScript T1059.007:	T1197: BUTS Jobs T1547: Boot or Logon	User Account Control T1548.004: Elevated	User Account Control T1548.004: Elevated	T1100: Brute Force T1555: Credentials from Password Sto	Window Discovery T1217: Browser	T1534: Internal Spearphishing T1570: Lateral Tool Transfer	Archive Collected Data T1123: Audio Capture	T1071.004: DNS	Transfer Size Limits T1048: Earlitration Over Alternative Protocol	T1455: Data Destruction T1456: Data	
Identity Information T1590: Gather Victim Network Information	Infrastructure T1587: Develop Capabilities	T1200: Hardware Additions	JavaScript T1059.008: Network Device CLI	Autostart Execution T1037: Boot or Logon Initialization Scripts	Execution with Prompt T1548.001: Setuid and Setgld	Execution with Prompt T1548.001: Setuid and Setgid	from W	Bookmank Discovery T1580: Cloud Infrastructure Discovery	T1553: Remote Service Session Hijacking	T1119: Automated Collection	Transfer Protocols T1071.003: Mail Protocols	T1041: Exfitration Over C2 Channel	T1565: Data Manipulation	
T1591: Gather Victim Org Information T1598: Phishing	T1585: Establish Accounts T1588:	T1556: Phishing T1091: Replication	T1059.001; PowerShell T1059.006; Python	T1176: Browner Extensions T1554: Compromise	T154E.003: Sudo and Sudo Caching T1134: Access	T1548.003: Sudo and Sudo Caching T1134: Access	T1555.001: Keychain T1555.005:	T1538: Cloud Service Dashboard T1526:	T1021: Remote Services T1021.003: Distributed	T1185: Browser Session Hijacking	T1071.001: Web Protocols T1092: Communication	T1011: Exfitration C Other Network Med T1052: Exfitration	T1491: Defacement T1561: Disk Wipe	
T1598: Phishing for Information T1597: Search Closed Sources	T1588: Obtain Capabilities T1600: Stage Capabilities	T1091: Replication Through Removable Media T1195: Supply Chain Compromise	T1059.006: Python T1059.004: Unix Shell	T1554: Compromise Client Software Briary T1136: Create Account	Token Manipulation T1547: Boot or Logen Autostart Execution	Token Manipulation T1197: BITS Jobs	Password Managers T1555.002: Securityd Memory	T1526: Cloud Service Discovery T1619: Cloud Storage Object Discovery	Component Object Model T1021.001: Remote	T1115: Clipboard Deta T1530: Data from	T1092: Communication Through Removable Media T1132: Data Encoding	Over Physical Media T1567: Edifitration Over Web Service	T1551: Disk Wipe T1499: Endpoint Denial of Service	
T1596: Search Open Technical Databases T1593: Search		T1 199: Trusted Relationship	T1059.005: Visual Basic	T1543: Create or Modify System Process T1543,001:	T1037: Boot or Logon Initialization Scripts	T1612: Build Image on Host	T1555.004: Windows Credential Manager	T1613: Container and Resource Discovery	Desktop Protocol T1021.002: SMB/Win Admin Shares	Cloud Storage Object T1600: Data from Configuration Repository	T1001: Data Obfuscation	T1029: Scheduled Transfer	T1495: Firmware Corruption	
T1593: Search Open Websites/Domains T1594: Search	-	T1078: Valid Accounts	T1059.003: Windows Command Shell T1609: Container	T1541.001: Launth Agent T1541.004:	T1542: Create or Modify System Process T1543:001:	T1622: Debugger Evasion T1140: Debbfuscate/Decode	T1212: Exploitation for Credential Access T1187:	T1622: Debugger Evasion T1482:	T1021.004:55H	T1213: Data from Information Repositories T1005:	T1568: Dynamic Resolution T1573:	T1537: Transfer Data to Cloud Account	T1490: Inhibit System Recovery T1490: Network	
Wctim-Owned Websites	_		Administration Command T1610: Deploy Container	Launch Daemon T1543.002: Systemd Service	Launch Agent T1543.004: Launch Daemon	Files or Information	Forced Authentication T1606: Forge Web Credentials	Domain Trust Discovery T1083: File and Directory Discovery	T1021.005: Windows Remote Management	Data from Local System T1009: Data from Network Shared Drive	Encrypted Channel T1008: Fallback Channels	\dashv	Denial of Service T1406: Resource Hjacking	
			T1203: Exploitation for Client Execution	T1541003: Windows Service	T1543.002: Systemd Service	T1006: Direct Volume Access	T1056: Input Capture	T1615: Group Policy Discovery	T1091: Replication Through Removable Media	T1025: Data from Removable Media	T1105: Ingress Tool Transfer		T1489: Service Stop	
			T1559: Inter-Process Communication	T1546: Event Triggered Execution	T1543.003: Windows Service	T1484: Domain Policy Modification T1480:	T1556: Modify Authentication Process T1111: Multi-Factor	T1040: Network Service Discovery	T1072: Software Deployment Tools T1090:	T1074: Data Staged	T1104: Multi-Stage Channels T1095: Non-Application	_	T1529: System Shutdown/Reboot	
			T1106: Native API T1053: Scheduled Task/Job	Remote Services T1574: Hijack Execution Flox	T1-854: Domain Policy Modification T1631: Escape to Host	Execution Guardrails T1211: Exploitation for Defense Evasion	Authentication Interception T1621: Multi-Factor Authentication Request Generation	Network Share Discovery T1040: Network Sniffing	Taint Shared Content T1550: Use Alternate	T1114: Email Collection T1056: Input Capture	Layer Protocol T1571: Non-Standard Port	\dashv		
			T1053.002: At	T1525: Implant Internal Ima	T1546: Event Triggered Execution	T1222: File and Directory Permissions Modification	T1040: Network Sniffling	T1201: Password Policy Discovery	Authentication Material	T1113: Screen Capture	T1572: Protocol Tunneling			
			T1053.007: Container Orchestration Job T1053.003: Cron	T1556: Modify Authentication Process T1137: Office	T1068: Exploitation for Privilege Escalation T1574:	T1564: Hide Artifacts T1574:	T1003: OS Credential Dumping T1003.008: /etc/passwd	T1120: Periphenal Device Discovery T1069: Permission		T1125: Video Capture	T1090: Proxy	_		
			T1053.003: Cron T1053.005: Scheduled Task	Application Startup T1542: Pre-OS Boot	Hijack Execution Flow T1055: Process Injection	Hijack Execution Flow T1562: Impair Defenses	and /etc/shadow T1003.005: Cached Domain Credentials	Groups Discovery 11057: Propers Discovery			Remote Access Software T1205: Traffic Signaling	_		
			T1053.006: Systemd Timers	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1562.008: Disable Cloud Logs	T1003.006: DCSync	T1012: Query Reg			T1102: Web Service			
			T1129: Shared Modules T1072: Software	T1053.002: At T1053.007: Container	T1053.002: At T1053.007: Container	T1562.007: Disable or Modify Cloud Firewall T1562.004: Disable or	T1003.004: LSA Secrets T1003.001:	T1018: Remote System D. T1518: Software Discovery						
			Deployment Tools T1569: System Services	Orchestration job T1051.003: Cron	Orchestration Job T1053.003: Cron	Modify System Firewall T1502.001: Disable or Modify Tools	T1003.003: NTDS	Software Discovery T1082: System Information Discovery						
			T1569,001: Launchoti T1569,002:	T1051.005: Scheduled Task	T1053.005: Scheduled Task T1053.006: Systemd Timers	T1562.002: Disable Windows Event Logging	T1003.007: Proc Plesystem	T1614: System Location Discovery						
			T1569.002: Service Execution	T1051.006: Systemd Timers T1505: Server	T1053.006: Systemd Timers T1076: Valid Accounts	T1562.010: Downgrade Attack T1562.003: Impair Command History Logging T1562.006:	Proc Flesystem T1003.002: Security Account Manager T1528: Steal	T1016: System Network Configuration Discovery T1049: System Network						
			T1204.002: Malicious File	Software Component T1205: Treffic Signaling		Indicator Blocking	Application Access Token T1558: Steal or Forge Kerberos Tickets	Connections Discovery 11033: System Owner/User Discovery						
			T1204.003: Malicious Image	T1078: Valid Accounts	`	T1562.009: Safe Mode Boot T1070: Indicator	T1539: Steal Web Session Cookie	T1007: System Service Discovery						
			T1204.001: Malkious Link T1047: Windows Management			Removal on Host T1070.003: Clear	Unsecured Credentials T1552,000: Bash History	System Time Discovery T1497: Virtualization/Sandbox	_					
			Instrumentation			Command History T1070.002: Clear Linux or Mac System Logs	Bash History T1552.005: Cloud Irrotance Metadata API	Evasion						
						T1070.001: Clear Windows Event Logs T1070.004:	T1552.007: Container API	`						
						File Deletion T1070.005: Network	T1552,001: Credentials In Files T1552,002: Credentials							
						Share Connection Ret	in Registry T1552.006: Group Policy Preferences							
						T1202: Indirect Command Execution	T1552.004: Private Keys							
						T1036: Masquerading T1036:007: Double	-							
						File Extension T1036.001: Invalid Code Signature								
						T1035.004: Masquerade Task or Service T1035.005: Metch								
						Legitimate Name or Location T1036.003: Rename System Utilities								
						System Utilities T1036.002: Right-to-Left Override T1036.006: Space								
						aner Hename								
						T1556: Modify Authentication Process T1578: Modify Cloud	-							
						Compute Infrastructure T1112: Modify Registry								
						T1601: Modify System Image								
						T1599: Network Boundary Bridging T1027: Obfuscated	_							
						Files or Information T1647: Plist File Modification								
						T1542: Pre-OS Book T1055:								
						Process Injection T1620:	_							
						Reflective Code Loading 11207: Roque Domain Controller								
						T1014: Rootkit								
						T1503: Subvert Trust Controls T1218: System								
						Binary Proxy Execution 11216: System Script Proxy Execution								
						T1221: Template Injection								
						T1205: Traffic Signaling T1127: Trusted Developer	-							
						Utilities Proxy Execution 11535: UnspecifUnsupported Cloud Regions	1							
						T1550: Use Alternate Authentication Material								
						T1078: Valid Accounts T1497: Virtualization/Sandbox	-							
						Evasion T1600: Weeken Encryption	1							
						T1220: XSL Script Processing								