About  Pysa  Capa con las tácticas y técnicas que usa el ransomware Pysa.					domain ————————————————————————————————————				Lin	platforms  Linux, macOS, Windows,  PRE, Containers, Network, Office 365,				
					SaaS, Google Workspace, IaaS, Azure AD									
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
T1595: Active Scanning T1592: Gather	T1583: Acquire Infrastructure T1586:	T1189: Drive-by-Compromise	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism T1548.002: Bypass	T154E: Abuse Elevation Control Mechanism	T1557: Adversary-in-the-Middle	T1087: Account Discovery T1010: Application	T1210: Exploitation of Remote Services	T1557: Adversary-in-the-Middle	T1071: Application Layer Protocol	T1020: Automated Exfétration T1030: Data	T1531: Account Access Removal	
Victim Host Information T1589: Gather Victim	Compromise Accounts T1584: Compromise	T1190: Exploit Public-Facing Application T1133: Expernal	AppleScript T1059.007:	T1197: BITS Jobs T1547: Boot or Logan	User Account Control T1548.004: Elevated	User Account Control T1548.004: Elevated	T1110: Brute Force T1555: Credentials from Password Stores	T1010: Application Window Discovery T1217: Browser Bookmark Discovery	Internal Spearphishing T1570: Leteral Tool Transfer	T1560: Archive Collected Data T1123: Audio Capture	T1071.004: DNS T1071.002: File	Transfer Size Limits T1048: Exfitration Over Alternative Protocol	T1485: Data Destruction	
Identity Information T1590: Gather Victim Network Information	Infrastructure T1587: Develop Capabilities	T1202: Hardware Additions	JavaScript T1059.008: Network Device CLI	Autostert Execution T1037: Boot or Logon Initialization Scripts	Execution with Prompt T1548.001: Setuid and Setgid	Execution with Prompt T1548.001: Setuid and Setgid	T1555.003 from Web	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: Phinhing	T1585: Establish Accounts	T1506: Phishing	T1059.001; PowerShell	T1176: Browner Extensions T1554: Compromise	T1548,000: Sudo and Sudo Caching	T1548.003: Sudo and Sudo Caching T1134: Access	T1555.001: Keychain T1555.005:	T1538: Cloud Service Dashboard	T1021: Remote Services T1021.003: Distributed	T1185: Browser Session Hijacking	T1071.001: Web Protocols	T1011: Eafftration Over Other Network Medium	T1491: Defacement	
T1598: Phishing for Information T1597:	T1580: Obtain Capabilities T1600: Stage Capabilities	T1091: Replication Through Removable Media T1195:	T1059.00k: Python T1059.00k: Unix Shell	T1554: Compromise Client Software Binary T1136: Create Account	Token Manipulation T1547: Boot or Logon	Token Manipulation T1197: BITS Jobs	Password Managers T1595.002:	T1526: Cloud Service Discovery T1619: Cloud Storage	Component Object Model T1021.001: Remote	T1115: Clipboard Data T1530: Data from	T1092: Communication Through Removable Media T1132: Data Encoding	T1052: Exhiftration Over Physical Medium T1567: Exhiftration Over Web Service	T1561: Disk Wipe T1499: Endpoint Denial of Service	
Search Closed Sources T1596: Search Open Technical Databases T1590: Search	Stage Capabilities	Supply Chain Compromise T1199: Trusted Relationship	T1059,005: Visual Basic	T1543: Create or Modify System Process	Autostart Execution T1037: Boot or Logon Initialization Scripts	T1612: Build Image on Host	Securityd Memory T1535.004: Windows Credential Manager	Object Discovery T1612: Container and Resource Discovery	Desktop Protocol T1021.002: SMB/Windows Admin Shares	Cloud Storage Object T1602: 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	T1541001: Launch Agent T1541004:	T1543: Create or Modify System Process T1543,001:	T1622: Debugger Evasion T1140: Deobfuscate/Decode	T1212: Exploitation for Credential Access	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 T1498: Network	
Victim-Owned Websites	_		Administration Command T1610: Deploy Container	Launch Daemon T1541202: Systemd Service	Modify System Process T1543.001: Launch Agent T1543.006	Files or Information T1610: Deploy Container	Forced Authentication T1608:	Domain Trust Discovery T1003: File and Directory Discovery	T1021.005: VNC	Data from Local System T1039: Data from	Encrypted Channel T1008: Fallback Channels	$\dashv$	Denial of Service 11496: Resource Hjacking	
			T1203: Exploitation for Client Execution	T1541003: Windows Service	Launch Daemon T1543,002: Systemd Service	T1006: Direct Volume Access	Forge Web Credentials T1056: Input Capture		Remote Management T1091: Replication Through Remouble Media	Network Shared Drive T1025: Data from Removable Media	T1105: Ingress Tool Transfer		T1489: Service Stop	
			T1559: Inter-Process Communication	T1546: Event Triggered Execution T1133: External	T1543.003: Windows Service	T1484: Domain Policy Modification	T1556: Modify Authentication Process T1111: Multi-Factor	T1046: Network Service Discovery	T1072: Software Deployment Tools	T1074: Data Staged	T1104: Multi-Stage Channels T1095: Non-Application		T1529: System Shutdown/Rebook	
			T1105: Native API T1053:	Remote Services T1574: Hijack Execution Flow	T1484: Domain Policy Modification T1611: Escape to Host	T1480: Execution Guardrafis T1211: Exploitation for Defense Evasion	Authentication Interception T1621: Multi-Factor Authentication Request Generation	Network Share Discovery T1040: Network Sniffing	T1050: Taint Shared Content T1550: Use Alternate	T1114: Email Collection T1056: Input Capture	Layer Protocol T1571:	_		
			Scheduled Task/Job T1053.002: At	Hijack Execution Flow T1525: Implant Internal Image	T1546: Event Triggered Execution	for Defense Evasion  T1222: File and Directory  Permissions Modification	T1040: Network Sniffing	T1040: Network Sniffing T1201: Password Policy Discovery	Authentication Material	T1113: Screen Capture	Non-Standard Port T1572: Protocol Tunneling			
			T1053.007: Container Orchestration Job	T1556: Modify Authentication Process T1137: Office	T1058: Exploitation for Privilege Escalation T1574:	T1561: Hide Artifacts T1574:	T1003: OS Credential Dumping T1003.008: /etc/passwd	T1120: Periphenal Device Discovery T1002: Permission	`	T1125: Video Capture	T1090: Proxy T1219:			
			T1053.003: Cron T1053.005:	Application Startup T1542: Pre-OS Boot	Hijack Execution Flow T1055:	Hijack Execution Flow T1562: Impair Defenses	and /etc/shadow T1003.005: Cached	Groups Discovery T1057:			Remote Access Software T1205:	_		
			Scheduled Task T1053.006: Systemd Timers	T1053: Scheduled Task/Job	Process Injection T1053: Scheduled Task/Job	T1562.008: Disable Cloud Logs	Domain Credentials T1003.006: DCSync	Process Discovery T1012: Query Registry			Traffic Signaling 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:	71018: Remote System Discovery						
			Deployment Tools T1569: System Services	Orchestration Job T1053.003: Cron	Orchestration Job T1053.003: Cron	T1502 D04: Disable or Modify System Firewall T1502 D01: Disable or Modify Tools T1502 D02: Disable	LSASS Memory T1003.003: NTDS	T1518: Software Discovery T1082: System	-					
		[	T1569.001: Launchotl	T1053.005: Scheduled Task	T1053,005	T1562.002: Dinable Windows Event Loggin T1562.010:		Information Discovery T1614: System Location Discovery						
			T1565.000: Service Execution	T1053.008: Systemd Timers T1505: Server	Scheduled Task T1053.006: Systemd Timers T1078: Valid Accounts	T1562.010: Downgrade Attack T1562.003: Impair	T1003.002: Security Account Manager T1528: Steal	T1016: System Network Configuration Discovery T1040: System Network						
			T1204: User Esecution T1204:002: Mobiles of Fig.	Software Component 11205: Traffic Signaling	T107E Valid Accounts	Command History Logging 11562,006: Indicator Blocking	Application Access Token T1558: Steal or Forge Kerberos Tickets	Connections Discovery T1033: System						
			T1040 Milesona Transport	T1078: Valid Accounts		T1562.009: Safe Mode Boot	T1539: Steal Web Session Cookie	Owner/User Discovery  11007: System Service Discovery						
						T1070: Indicator Removal on Host  11070.003: Clear	T1552: Unsecured Credentials T1552.000:	T1124: System Time Discovery T1497: Virtualization/Sandbox						
						Command History T1070.002: Clear Linux or Mac System Logs	T1552,000: Bash History T1552,005: Cloud Impace Metadata APS	Evasion						
						T1070.001: Clear Windows Event Logs	T1552.007: Container API	□ `						
						T1070.004: File Deletion T1070.005: Network	T1532.001: Credentials In Files T1532.002: Credentials							
						Share Connection Removal T1070.006:	in Registry T1552.006: Group Policy Preferences							
						Timestomp T1202: Indirect Command Execution	T1552.094: Private Keys							
						T1036: Masquerading T1036.007: Double								
						File Extension T1036.001: Invalid	_							
						Code Signature T1036.004: Masquerade Task or Service T1036.005: Match								
						Legitimate Name or Location								
						T1035.001: Rename System Utilities T1035.002: Right-to-Left Override T1035.000: Space after Electron	<b>=</b>							
						Right-to-Left Override T1035.005: Space after Filename								
						T1556: Modify Authentication Process								
						T1578: Modify Cloud Compute Infrastructure								
						T1601: Modify System Image								
						T1599: Network Boundary Bridging T1027: Obfuscated	$\Box$							
						T1647:								
						Plat File Modification T1542: Pre-OS Boot								
						T1055: Process Injection								
						T1620: Reflective Code Loading T1207:	_							
						Roque Domain Controller T1014: Rootkit	$\dashv$							
						T1553: Subvert Trust Controls								
						T1218: System Binary Proxy Execution T1216: System								
						Script Presy Execution T1221:	$\dashv$							
						Template Injection T1205: Traffic Signaling								
						T1127: Trusted Developer Utilities Proxy Execution	_							
						T1535: Unused/Unsupported Cloud Regions T1550: Use Alternate	$\dashv$							
						Authentication Material T1078: Valid Accounts								
						T1497: Virtualization/Sandbox Evasion T1600:								
						Weaken Encryption T1220:	$\dashv$							
						XSL Script Processing								