about domain — - platforms ——— Conti Linux, macOS, Windows, PRE, Containers, Network, Office 365, Enterprise ATT&CK v11 Capa con las tácticas y SaaS, Google Workspace, IaaS, Azure AD técnicas que usa el ransomware Conti. Initial Access Execution Exfiltration Persistence Discovery Impact T1584: Compromise Infrastructure T1587: Develop Capabilities T1115: Clipboard Data
T1530: Data
from Cloud Storage Objec
T1600: Data from
Configuration Repository
T1213: Data from T1588: Obtain Capabilities T1499: Endpoint Denial of Service T1495: Firmware Corruption T1573: Encrypted Channel 1490: letwork Denial of Service T1205: Traffic Signaling T1562.002: Disable Windows Event Logging T1562.010: Downgrade Attack T1562.003: Impair Command History Logging cator Removal on Host
T1070,003:
Clear Command Histo
T1070,002: Clear Linux T1036.007:
Double File Extension
T1036.001: Invalid
Code Signature
T1036.004: Maxquerade
Task or Service
T1036.005: March
Legitimate Name or Locat