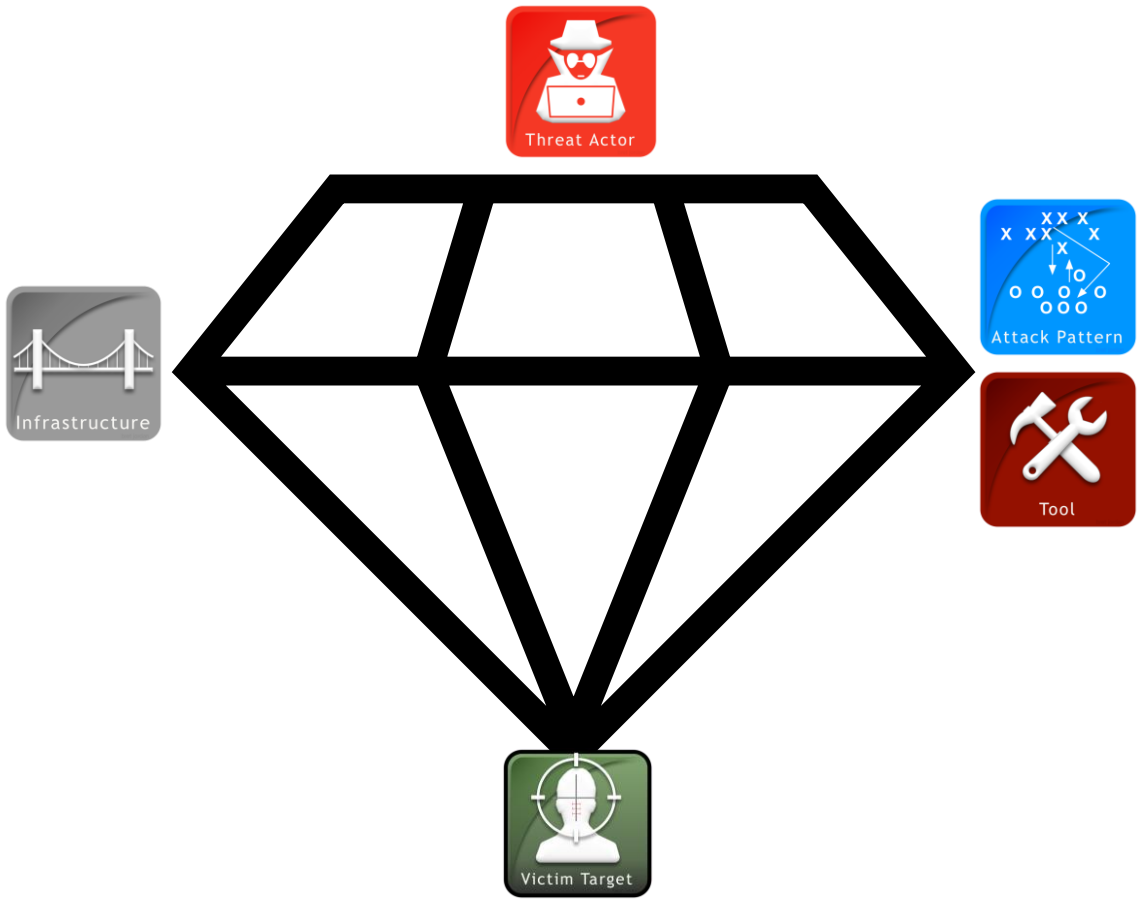
Diamond model

[Ivanti VPN Zero-Day Vulnerabilities: CVE-2024-21887 and CVE-2023-46805]

UTA0178
UTA0188
...

gpoaccess [.]com
webb-institute[.]com
symantke[.]com
206[.]189[.]208[.]156
75[.]145[.]243[.]85
47[.]207[.]9[.]89
98[.]160[.]48[.]170
173[.]220[.]106[.]166
73[.]128[.]178[.]221
50[.]243[.]177[.]161
50[.]213[.]208[.]89
64[.]24[.]179[.]210
75[.]145[.]224[.]109
50[.]215[.]39[.]49
71[.]127[.]149[.]194
173[.]53[.]43[.]7
IOCs:
Volexity
Mandiant



- Global government and military departments
- National telecommunications companies
- Defense contractors
- Technology
- Banking, Finance, and Accounting
- Worldwide consulting
- Aerospace, Aviation, and Engineering

Techniques

Stage 1:
T1133: External Remote Services
T1105: Ingress Tool Transfer
T1505.003: Web Shel
T1059.004: Unix Shell
T1614: System Location Discovery
T1056.003: Web Portal Capture
T1070.002: Clear Linux or Mac System Logs
T1070.009: Clear Persistence
T1070.004: File Deletion
T1562.001: Disable or Modify Tools

Stage 2:
T1078: Valid Accounts
T1021.001: Remote Desktop Protocol
T1021.002: SMB/Windows Admin Shares
T1021.004: SSH
T1505.003: Web Shel
T1003.001: LSASS Memory
T1003.003: NTDS
T1560.001: Archive via Utility

Tools:
T1588: Obtain Capabilities
PySoxy - SOCKS5 proxy: GitHub
Veeam-creds: GitHub
7-Zip

T1587: Develop Capabilities
GLASSTOKEN: Custom Webshell

Ref:
Volexity
Mandiant

@Nounou Mbeiri

Tidal Cyber Community Edition Mapped Techniques

Ivanti VPN Zero-Day Vulnerabilities: CVE-2024-21887 and CVE-2023-46805

https://app.tidalcyber.com/share/e6d1552d-ecbb-43f4-8c91-75718274390b