

# Diamond model

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

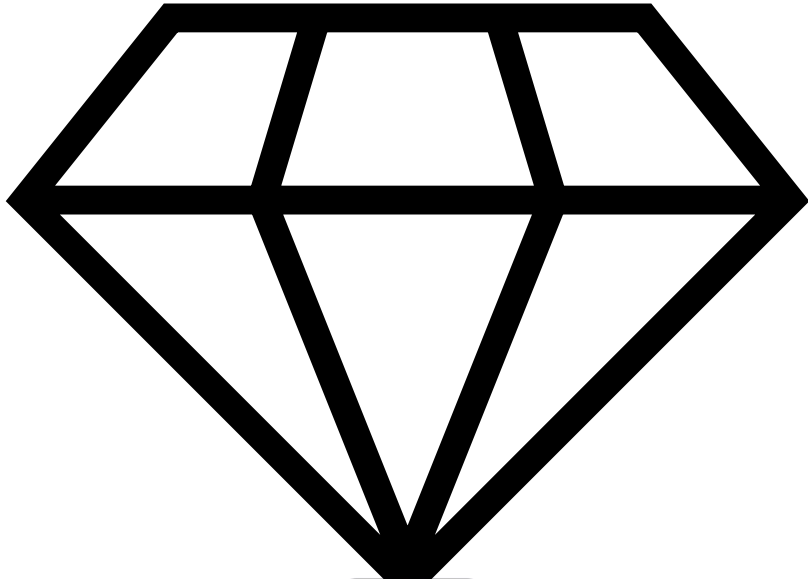
gpoaccess [.]com  
webb-institute[.]com  
symantke[.]com  
206[.]189[.]208[.]156  
75[.]145[.]243[.]85  
47[.]207[.]9[.]89  
98[.]160[.]48[.]170  
173[.]220[.]106[.]166  
73[.]128[.]178[.]221  
50[.]243[.]177[.]161  
50[.]213[.]208[.]89  
64[.]24[.]179[.]210  
75[.]145[.]224[.]109  
50[.]215[.]39[.]49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

IOCs:

[Volexity](#)

[Mandiant](#)

UTA0178  
UTA0188



- 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 Shell
- 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 Shell
- 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](#)

# 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>

TIDALCYBER

Draft

Ivanti VPN Zero-Da...

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
External Remote Services	Command and Scripting Interpreter (1)	External Remote Services	Valid Accounts	Impair Defenses (1)	Input Capture (1)	System Location Discovery	Remote Services (3)	Archive Collected Data (1)	Ingress Tool Transfer
Valid Accounts	Unix Shell	Server Software Component (1)		Disable or Modify Tools	Web Portal Capture		Remote Desktop Protocol	Archive via Utility	
		Web Shell		Indicator Removal (3)	OS Credential Dumping (2)		SMB/Windows Admin Shares	Input Capture (1)	
		Valid Accounts		Clear Linux or Mac System Logs	LSASS Memory		SSH	Web Portal Capture	
				Clear Persistence	NTDS				
				File Deletion					
				Valid Accounts					