Thrip

attack.mitre.org/groups/G0076

Thrip is an espionage group that has targeted satellite communications, telecoms, and defense contractor companies in the U.S. and Southeast Asia. The group uses custom malware as well as "living off the land" techniques. [1]

ID: G0076

Version: 1.2

Created: 17 October 2018

Last Modified: 12 October 2021

Version Permalink
Live Version

Enterprise Layer

download view

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Thrip leveraged PowerShell to run commands to download payloads, traverse the compromised networks, and carry out reconnaissance.[1]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Thrip has used WinSCP to exfiltrate data from a targeted organization over FTP.[1]

Domain	ID	Name	Use	
Enterprise	T1588	.002	Obtain Capabilities: Tool	Thrip has obtained and used tools such as Mimikatz and PsExec.[1]
Enterprise	T1219	Remote Access Software	Thrip used a cloud-based remote access software called LogMeIn for their attacks.[1]	

Software

ID	Name	References	Techniques
S0261	Catchamas	[1]	Application Window Discovery, Clipboard Data, Create or Modify System Process: Windows Service, Data Staged: Local Data Staging, Input Capture: Keylogging, Masquerading: Masquerade Task or Service, Modify Registry, Screen Capture, System Network Configuration Discovery
S0002	Mimikatz	[1]	Access Token Manipulation: SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution: Security Support Provider, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores, Credentials from Password Stores: Credentials from Web Browsers, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Security Account Manager, OS Credential Dumping: DCSync, OS Credential Dumping: LSA Secrets, Rogue Domain Controller, Steal or Forge Kerberos Tickets: Golden Ticket, Steal or Forge Kerberos Tickets: Silver Ticket, Unsecured Credentials: Private Keys, Use Alternate Authentication Material: Pass the Ticket, Use Alternate Authentication Material: Pass the Hash

ID	Name	References	Techniques
S0029	PsExec	Thrip used PsExec to move laterally between computers on the victim's network.[1]	Create Account: Domain Account, Create or Modify System Process: Windows Service, Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, System Services: Service Execution

References

1. Security Response Attack Investigation Team. (2018, June 19). Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies. Retrieved July 10, 2018.