TLP:CLEAR "Spacecolon" Toolkit Used to Target Multiple Industries with Scarab Ransomware, including Hospitality and Entertainment Organizations

TTPs

ESET researcher provided the following MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs):

Tactic	ID	Name	Description
Reconnaissance	*T1595.002*	Active Scanning: Vulnerability Scanning	CosmicBeetle looked for vulnerable servers as potential targets.
Resource Development	*T1583.001*	Acquire Infrastructure: Domains	CosmicBeetle used various hosting providers to register domains.
	T1587.001	Develop Capabilities: Malware	CosmicBeetle developed its own malware.
	T1587.003	Develop Capabilities: Digital Certificates	ScService and ScInstaller use a custom SSL certificate in TLS communications.
Initial Access	*T1190*	Exploit Public-Facing Application	CosmicBeetle exploited ZeroLogon, and probably other vulnerabilities, to compromise systems.
Execution	*T1059.003*	Command and Scripting Interpreter: Windows Command Shell	CosmicBeetle executed many commands using cmd.exe. Many of the additionally downloaded tools are BAT scripts.
	T1059.001	Command and Scripting Interpreter: PowerShell	ScHackTool uses PowerShell to perform various tasks.
	T1059.005	Command and Scripting Interpreter: Visual Basic	Many of the additionally downloaded tools are VBScripts.

	T1053.005	Scheduled Task/Job: Scheduled Task	ScService utilizes scheduled tasks to execute payloads.
Persistence	T1133	External Remote Services	CosmicBeetle attempted to brute force credentials that were then used to enter.
	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ScHackTool and the Scarab ransomware utilize the Run or RunOnce key for persistence.
	T1136.001	Create Account: Local Account	CosmicBeetle often created its own administrator account.
	T1543.003	Create or Modify System Process: Windows Service	ScService is implemented as a Windows service.
Defense Evasion	T1078.003	Valid Accounts: Local Accounts	CosmicBeetle may deploy a large variety of tools to crack or brute force credentials for local accounts.
	T1140	Deobfuscate/Decode Files or Information	Spacecolon components employ several kinds of data obfuscation.
	T1070.001	Indicator Removal: Clear Windows Event Logs	CosmicBeetle may deploy a large variety of tools to clear Windows Event Logs.
	T1036.005	Masquerading: Match Legitimate Name or Location	Scarab ransomware attempts to hide by naming its processes as legitimate Windows process names.
	T1218.005	System Binary Proxy Execution: Mshta	Scarab ransomware utilizes mshta.exe to perform various tasks.
Credential Access	T1110.001	Brute Force: Password Guessing	CosmicBeetle may deploy a large variety of tools designed to brute force passwords.

	T1110.003	Brute Force: Password Spraying	CosmicBeetle may deploy a large variety of tools designed to test a large number of passwords.
	T1003.001	OS Credential Dumping: LSASS Memory	CosmicBeetle may deploy tools capable of dumping lsass.exe.
Discovery	*T1082*	System Information Discovery	ScService queries system information to fingerprint the victim.
	T1016	System Network Configuration Discovery	ScService retrieves the local network configuration and MAC address.
	T1124	System Time Discovery	ScService retrieves the system time.
Collection	*T1560.002*	Archive Collected Data: Archive via Library	ScHackTool uses the standard ZIP library to archive files before extracting them to the C&C server.
	T1115	Clipboard Data	Scarab ransomware deploys a ClipBanker that monitors the clipboard for cryptocurrency wallets, and changes them.
Command and Control	*T1071.001*	Application Layer Protocol: Web Protocols	Spacecolon components communicate via HTTPS.
	T1132.001	Data Encoding: Standard Encoding	ScService uses AES encryption.
	T1095	Non-Application Layer Protocol	Older ScService builds communicate via a custom TCP/IP protocol.
	T1571	Non-Standard Port	New ScService builds run a local HTTP server on port 8347.
	T1090.002	Proxy: External Proxy	ScService may be instructed to use an external proxy.

Exfiltration	*T1041*	Exfiltration Over C2 Channel	ScHackTool exfiltrates data to the C&C server.
Impact	*T1485*	Data Destruction	CosmicBeetle may deploy a number of tools to destroy data on disks.
	T1486	Data Encrypted for Impact	CosmicBeetle may deploy Scarab ransomware to encrypt sensitive data.
	T1561	Disk Wipe	CosmicBeetle may deploy a number of tools to wipe disks.
	T1529	System Shutdown/Reboot	ScHackTool is capable of rebooting the system.