APT33

attack.mitre.org/groups/G0064/

APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors. [1] [2]

ID: G0064

ⓘ

Associated Groups: HOLMIUM, Elfin

Contributors: Dragos Threat Intelligence

Version: 1.4

Created: 18 April 2018

Last Modified: 23 May 2022

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
HOLMIUM	[3]
Elfin	[4]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT33 has used HTTP for command and control.[4]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT33 has used WinRAR to compress data prior to exfil.[4]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT33 has deployed a tool known as DarkComet to the Startup folder of a victim, and used Registry run keys to gain persistence.[4][3]
Enterprise	T1110	.003	Brute Force: Password Spraying	APT33 has used password spraying to gain access to target systems.[5][3]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	APT33 has utilized PowerShell to download files from the C2 server and run various scripts.[4][3]

Domain	ID	Name	Use	
		.005	Command and Scripting Interpreter: Visual Basic	APT33 has used VBScript to initiate the delivery of payloads.[3]
Enterprise	T1555	Credentials from Password Stores	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]	
		.003	Credentials from Web Browsers	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	APT33 has used base64 to encode command and control traffic.[5]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	APT33 has used AES for encryption of command and control traffic.[5]
Enterprise	T1546	.003	Event Triggered Execution: Windows Management Instrumentation Event Subscription	APT33 has attempted to use WMI event subscriptions to establish persistence on compromised hosts.[3]

Domain	ID	Name	Use	
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	APT33 has used FTP to exfiltrate files (separately from the C2 channel).[4]
Enterprise	T1203	Exploitation for Client Execution	APT33 has attempted to exploit a known vulnerability in WinRAR (CVE-2018-20250), and attempted to gain remote code execution via a security bypass vulnerability (CVE-2017-11774).[4][5]	
Enterprise	T1068	Exploitation for Privilege Escalation	APT33 has used a publicly available exploit for CVE-2017-0213 to escalate privileges on a local system.[5]	
Enterprise	T1105	Ingress Tool Transfer	APT33 has downloaded additional files and programs from its C2 server.[4][3]	
Enterprise	T1040	Network Sniffing	APT33 has used SniffPass to collect credentials by sniffing network traffic.[4]	
Enterprise	T1571	Non-Standard Port	APT33 has used HTTP over TCP ports 808 and 880 for command and control.[4]	
Enterprise	T1027	Obfuscated Files or Information	APT33 has used base64 to encode payloads.[5]	
Enterprise	T1588	.002	Obtain Capabilities: Tool	APT33 has obtained and leveraged publicly-available tools for early intrusion activities.[5][4]

Domain	ID	Name	Use	
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, and ProcDump to dump credentials.[4][5]
		.004	OS Credential Dumping: LSA Secrets	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]
		.005	OS Credential Dumping: Cached Domain Credentials	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	APT33 has sent spearphishing e-mails with archive attachments.[3]
		.002	Phishing: Spearphishing Link	APT33 has sent spearphishing emails containing links to .hta files.[1][4]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day.[4]

Domain	ID	Name	Use	
Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][5]
		.006	Unsecured Credentials: Group Policy Preferences	APT33 has used a variety of publicly available tools like Gpppassword to gather credentials.[4][5]
Enterprise	T1204	.001	User Execution: Malicious Link	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails.[1][4]
		.002	User Execution: Malicious File	APT33 has used malicious e-mail attachments to lure victims into executing malware.[3]
Enterprise	T1078	Valid Accounts	APT33 has used valid accounts for initial access and privilege escalation.[2][5]	

Domain	ID	Name	Use	
		.004	Cloud Accounts	APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints.[3]
ICS	T0852	Screen Capture	APT33 utilize backdoors capable of capturing screenshots once installed on a system. [6] [7]	
ICS	T0853	Scripting	APT33 utilized PowerShell scripts to establish command and control and install files for execution. [8] [9]	
ICS	T0865	Spearphishing Attachment	APT33 sent spear phishing emails containing links to HTML application files, which were embedded with malicious code.[6] APT33 has conducted targeted spear phishing campaigns against U.S. government agencies and private sector companies. [10]	

Software

ID	Name	References	Techniques
S0129	AutoIt backdoor	[4]	Abuse Elevation Control Mechanism: Bypass User Account Control, Command and Scripting Interpreter: PowerShell, Data Encoding: Standard Encoding, File and Directory Discovery
S0363	Empire	[5][4]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Create Process with Token, Access Token Manipulation: SID-History Injection, Access Token

ID	Name	References	Techniques
			Manipulation, Account Discovery: Domain Account, Account Discovery: Local Account, Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Application Layer Protocol: Web Protocols, Archive Collected Data, Boot or Logon Autostart Execution: Shortcut Modification, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Boot or Logon Autostart Execution: Security Support Provider, Browser Bookmark Discovery, Clipboard Data, Command and Scripting Interpreter: Windows Command Shell, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter, Commonly Used Port, Create Account: Domain Account, Create Account: Local Account, Create or Modify System Process: Windows Service, Credentials from Password Stores: Credentials from Web Browsers, Domain Policy Modification: Group Policy Modification, Domain Trust Discovery, Email Collection: Local Email Collection, Encrypted Channel: Asymmetric Cryptography, Event Triggered Execution: Accessibility Features, Exfiltration Over C2 Channel, Exfiltration Over Web Service: Exfiltration to Code Repository, Exfiltration Over Web Service: Exfiltration to Cloud Storage, Exploitation for Privilege Escalation, Exploitation of Remote Services, File and Directory Discovery, Group Policy Discovery, Hijack Execution Flow: Path Interception by Unquoted Path, Hijack Execution Flow: Dylib Hijacking, Hijack Execution Flow: Path Interception by PATH Environment Variable, Hijack Execution Flow: DLL Search Order Hijacking, Hijack Execution Flow: Path Interception by Search Order Hijacking, Indicator Removal on Host: Timestomp, Ingress Tool Transfer, Input Capture: Keylogging, Input Capture: Credential API Hooking, Native API, Network Service Discovery, Network Share Discovery, Network Sniffing, Obfuscated Files or Information, OS Credential Dumping: LSASS Memory, Process Discovery, Process Injection, Remote Services: SSH, Remote Services: Distributed Component Object Model, Scheduled Task/Job: Scheduled Task, Screen Capture, Software Discovery: Security Software Discovery, Steal or Forge Kerberos Tickets: Kerberoasting, Steal or Forge Kerberos Tickets: Silver Ticket, Steal or Forge Kerberos Tickets: Golden Ticket, System Information Discovery, System Network

ID	Name	References	Techniques
			Configuration Discovery, System Network Connections Discovery, System Services: Service Execution, Trusted Developer Utilities Proxy Execution: MSBuild, Unsecured Credentials: Private Keys, Unsecured Credentials: Credentials In Files, Use Alternate Authentication Material: Pass the Hash, Video Capture, Web Service: Bidirectional Communication, Windows Management Instrumentation
S0095	ftp	[4]	Commonly Used Port, Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol, Ingress Tool Transfer, Lateral Tool Transfer
S0349	LaZagne	[4]	Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores: Keychain, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Cached Domain Credentials, OS Credential Dumping: Proc Filesystem, OS Credential Dumping: LSA Secrets, OS Credential Dumping: /etc/passwd and /etc/shadow, Unsecured Credentials: Credentials In Files
S0002	Mimikatz	[4]	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
S0336	NanoCore	[2]	Audio Capture, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Windows Command Shell, Encrypted Channel: Symmetric Cryptography, Impair Defenses: Disable or Modify System Firewall, Impair Defenses: Disable or Modify Tools, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Obfuscated Files or Information, System Network Configuration Discovery, Video Capture
S0039	Net	[4]	Account Discovery: Domain Account, Account Discovery: Local Account, Create Account: Local Account, Create Account: Domain Account, Indicator Removal on Host: Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery: Domain Groups, Permission Groups Discovery: Local Groups, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, System Time Discovery

ID	Name	References	Techniques
S0198	NETWIRE	[1][2]	Application Layer Protocol: Web Protocols, Application Window Discovery, Archive Collected Data, Archive Collected Data: Archive via Custom Method, Automated Collection, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Boot or Logon Autostart Execution: XDG Autostart Entries, Boot or Logon Autostart Execution: Login Items, Command and Scripting Interpreter: PowerShell, Command and Scripting Interpreter: Windows Command Shell, Command and Scripting Interpreter: Visual Basic, Command and Scripting Interpreter: Unix Shell, Create or Modify System Process: Launch Agent, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Data Staged: Local Data Staging, Encrypted Channel, Encrypted Channel: Symmetric Cryptography, File and Directory Discovery, Hide Artifacts: Hidden Files and Directories, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Invalid Code Signature, Masquerading: Match Legitimate Name or Location, Modify Registry, Native API, Non-Application Layer Protocol, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, Phishing: Spearphishing Link, Phishing: Spearphishing Attachment, Process Discovery, Process Injection: Process Hollowing, Process Injection, Proxy, Scheduled Task/Job: Scheduled Task, Scheduled Task/Job: Cron, Screen Capture, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, User Execution: Malicious File, User Execution: Malicious Link, Web Service

ID	Name	References	Techniques
S0378	PoshC2	[5][4]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Create Process with Token, Access Token Manipulation, Account Discovery: Local Account, Account Discovery: Domain Account, Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Utility, Automated Collection, Brute Force, Domain Trust Discovery, Event Triggered Execution: Windows Management Instrumentation Event Subscription, Exploitation for Privilege Escalation, Exploitation of Remote Services, File and Directory Discovery, Input Capture: Keylogging, Network Service Discovery, Network Sniffing, OS Credential Dumping: LSASS Memory, Password Policy Discovery, Permission Groups Discovery: Local Groups, Process Injection, Proxy, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Service Discovery, System Services: Service Execution, Unsecured Credentials: Credentials In Files, Use Alternate Authentication Material: Pass the Hash, Windows Management Instrumentation

ID	Name	References	Techniques
S0194	PowerSploit	[5]	Access Token Manipulation, Account Discovery: Local Account, Audio Capture, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Boot or Logon Autostart Execution: Security Support Provider, Command and Scripting Interpreter: PowerShell, Create or Modify System Process: Windows Service, Credentials from Password Stores: Windows Credential Manager, Data from Local System, Domain Trust Discovery, Hijack Execution Flow: Path Interception by Search Order Hijacking, Hijack Execution Flow: Path Interception by PATH Environment Variable, Hijack Execution Flow: DLL Search Order Hijacking, Hijack Execution Flow: Path Interception by Unquoted Path, Input Capture: Keylogging, Obfuscated Files or Information: Indicator Removal from Tools, Obfuscated Files or Information, OS Credential Dumping: LSASS Memory, Path Interception, Process Discovery, Process Injection: Dynamic-link Library Injection, Query Registry, Reflective Code Loading, Scheduled Task/Job: Scheduled Task, Screen Capture, Steal or Forge Kerberos Tickets: Kerberoasting, Unsecured Credentials: Group Policy Preferences, Unsecured Credentials: Credentials in Registry, Windows Management Instrumentation
S0371	POWERTON	[5][3]	Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: PowerShell, Commonly Used Port, Encrypted Channel: Symmetric Cryptography, Event Triggered Execution: Windows Management Instrumentation Event Subscription, OS Credential Dumping: Security Account Manager

ID	Name	References	Techniques
S0192	Pupy	[5]	Abuse Elevation Control Mechanism: Bypass User Account Control, Access Token Manipulation: Token Impersonation/Theft, Account Discovery: Local Account, Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay, Application Layer Protocol: Web Protocols, Archive Collected Data: Archive via Utility, Audio Capture, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Python, Command and Scripting Interpreter: PowerShell, Create Account: Local Account, Create Account: Domain Account, Create or Modify System Process: Systemd Service, Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores, Email Collection: Local Email Collection, Encrypted Channel: Asymmetric Cryptography, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal on Host: Clear Windows Event Logs, Ingress Tool Transfer, Input Capture: Keylogging, Network Service Discovery, Network Share Discovery, OS Credential Dumping: LSASS Memory, OS Credential Dumping: LSA Secrets, OS Credential Dumping: Cached Domain Credentials, Process Discovery, Process Injection: Dynamic-link Library Injection, Remote Services: Remote Desktop Protocol, Screen Capture, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Services: Service Execution, Unsecured Credentials: Credentials In Files, Use Alternate Authentication Material: Pass the Ticket, Video Capture, Virtualization/Sandbox Evasion: System Checks
S0358	Ruler	[5][3]	Account Discovery: Email Account, Office Application Startup: Outlook Home Page, Office Application Startup: Outlook Rules, Office Application Startup: Outlook Forms

ID	Name	References	Techniques
S0380	StoneDrill	[1]	Command and Scripting Interpreter: Visual Basic, Data Destruction, Disk Wipe: Disk Structure Wipe, Disk Wipe: Disk Content Wipe, Indicator Removal on Host: File Deletion, Ingress Tool Transfer, Obfuscated Files or Information, Process Injection, Query Registry, Screen Capture, Software Discovery: Security Software Discovery, System Information Discovery, System Time Discovery, Virtualization/Sandbox Evasion, Windows Management Instrumentation
S0199	TURNEDUP	[1][2][4]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Ingress Tool Transfer, Process Injection: Asynchronous Procedure Call, Screen Capture, System Information Discovery

References

O'Leary, J., et al. (2017, September 20). Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware. Retrieved February 15, 2018. Davis, S. and Carr, N. (2017, September 21). APT33: New Insights into Iranian Cyber Espionage Group. Retrieved February 15, 2018. Microsoft Threat Protection Intelligence Team. (2020, June 18). Inside Microsoft Threat Protection: Mapping attack chains from cloud to endpoint. Retrieved June 22, 2020. Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.. Retrieved April 10, 2019. Ackerman, G., et al. (2018, December 21). OVERRULED: Containing a Potentially Destructive Adversary. Retrieved January 17, 2019. Jacqueline O'Leary et al. 2017, September 20 Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware Retrieved. 2019/12/02 Junnosuke Yagi 2017, March 07 Trojan.Stonedrill Retrieved. 2019/12/05 Symantec 2019, March 27 Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S. Retrieved. 2019/12/02 Dragos Symantec 2019, March 27 Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S. Retrieved. 2019/12/02 Magnallium Retrieved. 2019/10/27 Andy Greenburg 2019, June 20 Iranian Hackers Launch a New US-Targeted Campaign as Tensions Mount Retrieved. 2020/01/03