APT33, HOLMIUM, Elfin, Peach Sandstorm, Group G0064

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.[6][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]

.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][6]

.003 Credentials from Web Browsers

APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][6]

Enterprise T1132 .001 Data Encoding: Standard Encoding

APT33 has used base64 to encode command and control traffic.[6]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

APT33 has used AES for encryption of command and control traffic.[6]

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]

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][3]

Enterprise T1068 Exploitation for Privilege Escalation

APT33 has used a publicly available exploit for CVE-2017-0213 to escalate privileges on a local system.[6]

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 .013 Obfuscated Files or Information: Encrypted/Encoded File

APT33 has used base64 to encode payloads.[6]

Enterprise T1588 .002 Obtain Capabilities: Tool

APT33 has obtained and leveraged publicly-available tools for early intrusion activities.[6][4]

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][6]

.004 OS Credential Dumping: LSA Secrets

APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][6]

.005 OS Credential Dumping: Cached Domain Credentials

APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][6]

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]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

APT33 has used a variety of publicly available tools like LaZagne to gather credentials.[4][6]

.006 Unsecured Credentials: Group Policy Preferences

APT33 has used a variety of publicly available tools like Gpppassword to gather credentials.[4][6]

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][6]

.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. [7][8]

ICS T0853 Scripting

APT33 utilized PowerShell scripts to establish command and control and install files for execution. [9] [10]

ICS T0865 Spearphishing Attachment

APT33 sent spear phishing emails containing links to HTML application files, which were embedded with malicious code. [7] APT33 has conducted targeted spear phishing campaigns against U.S. government agencies and private sector companies. [11]

Source: https://attack.mitre.org/groups/G0064/