Vault 7 Leaks: CIA Tools with Potential Risks to Citizens, a Zombiegram

The Vault 7 leaks, released by WikiLeaks in 2017, exposed CIA hacking tools that, if misused, could compromise citizens' privacy and safety. Below is a comprehensive list of tools targeting consumer devices, including smart TVs and vehicles, with potential for abuse such as surveillance or remote control.

Tool/Project	Description	Targeted Devices	Risks if Abused
Weeping Angel	Activates TV microphones for covert recording while device appears off.	Smart TVs (e.g., Samsung)	Unauthorized home surveillance, capturing private conversations.
Vehicle Control	Infiltrates networked vehicle systems for remote control.	Connected cars, trucks	Remote hijacking, causing accidents or tracking locations.
Angelfire	Persistent malware framework for data exfiltration.	Windows PCs	Data theft, ransomware, or system control.
ExpressLane	Exfiltrates biometric data from shared systems.	Biometric databases	Identity theft or tracking via fingerprints, iris scans.
CouchPotato	Captures video streams or images remotely.	Webcams, security cams	Video surveillance for stalking or extortion.
Dumbo	Corrupts webcam recordings to hide surveillance.	Windows PCs with webcams	Undetected spying via cameras, violating privacy.
Imperial	Trojans for disk images and rootkits.	macOS, Linux	Persistent data theft or control of personal computers.
HighRise	SMS proxy to redirect messages.	Android (4.0–4.3)	Interception of texts, compromising authentication.
BothanSpy/Gyrfalcon	Steals SSH credentials.	Windows, Linux PCs	Unauthorized account access, financial fraud.
OutlawCountry	Redirects network traffic to CIA servers.	Linux systems	Man-in-the-middle attacks, intercepting internet data.
ELSA	Logs WiFi access points for location tracking.	Windows laptops	Real-time tracking, enabling stalking.
Brutal Kangaroo	Infects air-gapped systems via USB.	Windows PCs	Data leaks from secure devices, breaching privacy.
Cherry Blossom	Monitors, redirects router traffic.	Routers (e.g., D-Link)	Network-wide surveillance of household internet.
Pandemic	Replaces files in shared networks.	Windows file shares	Malware spread, infecting personal files.
Athena	Remote beacon for file delivery, execution.	Windows (XP–10)	Backdoor access, enabling espionage or data wipes.
AfterMidnight/Assassin	Dynamic malware for automated data collection.	Windows systems	Periodic data theft, eroding privacy.
Sonic Screwdriver	Bypasses firmware passwords via Thunderbolt.	iPhones, Macs	Access to encrypted personal data, photos, messages.
Marble Framework	Obfuscates malware to hide origins.	Any device	Undetected infections, prolonging privacy breaches.
Grasshopper	Custom malware evading antivirus.	Windows PCs	Silent hacking for surveillance or control.
HIVE	Malware suite for data transfer, commands.	Desktops, smartphones	Remote control, turning devices into spying tools.
Scribbles	Tracks document openings via beacons.	MS Office documents	Exposes citizens sharing sensitive info, risking retaliation.
Archimedes	Redirects LAN browser sessions.	LAN computers	Intercepts web traffic, eavesdropping on activities.

Released from March to September 2017, these tools target consumer devices, posing risks like unauthorized surveillance or vehicle manipulation. No new releases have occurred since. Visit zombiegram.org for more content like this.