Bad Rabbit, Software S0606 | MITRE ATT&CK®

Archived: 2026-04-02 11:49:53 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

Bad Rabbit has attempted to bypass UAC and gain elevated administrative privileges.[1]

Enterprise T1110 .003 Brute Force: Password Spraying

Bad Rabbit's `infpub.dat` file uses NTLM login credentials to brute force Windows machines.[1]

Enterprise T1486 Data Encrypted for Impact

Bad Rabbit has encrypted files and disks using AES-128-CBC and RSA-2048.[1]

Enterprise T1189 Drive-by Compromise

Bad Rabbit spread through watering holes on popular sites by injecting JavaScript into the HTML body or a `.js` file.[2][1]

Enterprise T1210 Exploitation of Remote Services

Bad Rabbit used the EternalRomance SMB exploit to spread through victim networks.[1]

Enterprise T1495 Firmware Corruption

Bad Rabbit has used an executable that installs a modified bootloader to prevent normal boot-up.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Bad Rabbit has masqueraded as a Flash Player installer through the executable file `install_flash_player.exe`. [2][1]

Enterprise T1106 Native API

Bad Rabbit has used various Windows API calls.[2]

Enterprise T1135 Network Share Discovery

Bad Rabbit enumerates open SMB shares on internal victim networks.[2]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Bad Rabbit has used Mimikatz to harvest credentials from the victim's machine.[2]

Enterprise T1057 Process Discovery

Bad Rabbit can enumerate all running processes to compare hashes.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Bad Rabbit's `infpub.dat` file creates a scheduled task to launch a malicious executable.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Bad Rabbit has used rundll32 to launch a malicious DLL as `C:Windowsinfpub.dat`.[1]

Enterprise T1569 .002 System Services: Service Execution

Bad Rabbit drops a file named `infpub.dat` into the Windows directory and is executed through SCManager and `rundll.exe`.

Enterprise T1204 .002 User Execution: Malicious File

Bad Rabbit has been executed through user installation of an executable disguised as a flash installer.[2][1]

ICS T0817 Drive-by Compromise

Bad Rabbit ransomware spreads through drive-by attacks where insecure websites are compromised. While the target is visiting a legitimate website, a malware dropper is being downloaded from the threat actors infrastructure. [4]

ICS T0866 Exploitation of Remote Services

Bad Rabbit initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks. [5]

ICS T0867 Lateral Tool Transfer

Bad Rabbit can move laterally through industrial networks by means of the SMB service. [5]

ICS T0828 Loss of Productivity and Revenue

Several transportation organizations in Ukraine have suffered from being infected by Bad Rabbit, resulting in some computers becoming encrypted, according to media reports. [2]

ICS T0863 User Execution

Bad Rabbit is disguised as an Adobe Flash installer. When the file is opened it starts locking the infected computer. [4]
