Dharma (CrySiS) Ransomware: Technical Analysis, Context and Mitigation

By Acronis

Published: 2025-12-05 · Archived: 2026-04-06 00:48:58 UTC

- Ransomware as a service: Dharma (CrySiS) has been active since 2016 and is distributed through a ransomware as a service model. The 2021 variant appends a .biden extension to encrypted files.
- Initial infection through remote services: According to the MITRE CAPEC database, adversaries commonly use stolen credentials to log in to remote services such as Remote Desktop Protocol (RDP). Dharma is typically deployed manually through RDP using weak or leaked credentials. Restricting or disabling RDP, limiting remote login accounts, and enabling multi factor authentication reduce exposure.
- Installation and persistence: Dharma executes as a 32 bit process on all Windows platforms, disables Wow64 file system redirection, copies itself to the %System% directory and Startup folders, and adds Run keys for persistence. It also creates mutexes to ensure a single active instance.
- Service and process termination: Dharma stops database, backup, and productivity services to remove file locks before encryption. This behavior aligns with ransomware families observed by MITRE, such as LockBit 3.0, which terminate security and database services before encrypting files.
- File encryption: Dharma encrypts files in multiple threads using AES 256 in CBC mode. NIST defines AES as a U.S. Government approved symmetric block cipher used to protect electronic data. Each file key is encrypted with a 1024 bit RSA public key embedded in the malware.
- Mitigation and detection: Acronis products detect and block Dharma ransomware. Organizations should harden RDP, enforce multi factor authentication, maintain offline backups, and isolate infected systems during incidents. OverviewOverview

Overview

Dharma, also known as CrySiS, is a long running ransomware family first observed in 2016. It operates as ransomware as a service, where developers lease the malware to affiliates who deploy it. A variant discovered in March 2021 appends the ".biden" extension to encrypted files. This article provides a technical analysis of Dharma, outlines its infection vector, describes its encryption workflow, and offers guidance for mitigation.

Attack vector

Many Dharma intrusions begin when threat actors gain access to a Windows system through Remote Desktop Protocol (RDP). The Common Attack Pattern Enumeration and Classification (CAPEC) project reports that adversaries use stolen credentials to log in to remote services, including RDP, Telnet, and SSH (capec.mitre.org).

Once connected, attackers manually deploy ransomware. Recommended security practices include:

- Disable unnecessary remote services: CAPEC guidance recommends disabling RDP and similar services when not required, blocking remote service traffic at the firewall, and removing the local Administrators group from RDP access (capec.mitre.org).
- Restrict accounts and enforce multi factor authentication: Only essential accounts should have remote login privileges. CAPEC also recommends limiting remote user permissions and using remote desktop gateways and multi factor authentication (capec.mitre.org; attack.mitre.org).
- Use strong, unique credentials and monitor for leaks.

Deobfuscation and runtime linking

When executed, Dharma uses the RC4 stream cipher to decrypt embedded strings that contain Windows API function names. It resolves these function addresses at runtime. RC4 is a symmetric stream cipher that is deprecated for secure communications but remains common in malware for basic obfuscation. Dharma uses the same RC4 routine to decrypt additional operational strings during execution.

Installation and persistence

To operate as a 32 bit process on both 32 bit and 64 bit Windows systems, Dharma calls the Wow64DisableWow64FsRedirection() function to disable file system redirection. It then copies itself to the %System% directory using the original filename and creates autorun registry entries under HKLM and HKCU:

```
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]
<filename>.exe = %System%\<filename>.exe

[HKCU\Software\Microsoft\Windows\CurrentVersion\Run]
<filename>.exe = %System%\<filename>.exe
```

The malware also copies itself into both Start Menu Startup folders. It creates two global mutexes, Global\syncronize_FQBL57A and Global\syncronize_FQBL57U, to ensure that only one instance runs. If the Windows version is older than Windows Vista, or if the mutexes already exist, Dharma exits.

Payload: service termination and process manipulation

Before encrypting files, Dharma attempts to stop services and terminate processes that may restrict file access. It stops database services such as Firebird and MSSQL, terminates processes including postgres.exe, mysqld.exe, sqlservr.exe, and Outlook, and deletes shadow copies using:

```
vssadmin delete shadows /all /quiet
```

It also sets the console code page to Windows 1251 for compatibility.

Terminating critical processes and services is a common ransomware technique. MITRE reports that LockBit 3.0 terminates security, backup, and database services to avoid interference during encryption (attack.mitre.org).

File encryption

Dharma encrypts files in multiple threads. It uses AES 256 in CBC mode for file encryption. NIST describes AES as a U.S. Government approved symmetric block cipher suitable for encrypting and decrypting electronic data (csrc.nist.gov).

For each file:

- A unique 256 bit AES key and 128 bit initialization vector are generated using pseudo random values and RC4.
- The AES key is encrypted using a 1024 bit RSA public key embedded in the malware.
- The key and IV are appended to the encrypted file.

Dharma excludes key system files (e.g., boot.ini, .exe) and encrypts a broad range of file types including documents, media, databases, archives, and source code.

Encrypted files follow this naming pattern:

```
<original_file>.id-<drive_serial_number>.[<attacker_email>].biden
```

For example:

```
desktop.ini.id-4AFE57F0.[biden@cock.li].biden
```

Ransom note

After encryption, Dharma drops ransom notes (Info.hta and MANUAL.txt) into Startup folders and the root of the system drive. These notes instruct victims to contact the attacker by email to purchase a decryption key. They warn victims that data loss may occur if they attempt self recovery.

Detection by Acronis and recommended response

Acronis Cyber Protect and Acronis Cyber Protect Cloud detect and block Dharma ransomware. Recommended response steps include:

- Isolate the affected system to prevent further spread.
- Do not pay the ransom, as payment supports criminal activity and does not guarantee recovery.
- Notify law enforcement and follow regulatory requirements.
- Restore from offline or immutable backups to ensure data integrity.
- Investigate the intrusion to identify root cause issues such as exposed RDP services or weak credentials.

Prevention and hardening

- Secure remote services: Disable RDP if it is not required. CAPEC recommends blocking RDP, Telnet, and SSH at the firewall, limiting remote login permissions, removing the local Administrators group from RDP access, and enabling multi factor authentication (capec.mitre.org; attack.mitre.org).
- Patch systems regularly: Apply operating system and software patches promptly.
- Implement least privilege access: Restrict administrative rights, limit service accounts, and monitor for anomalous logins.
- Deploy endpoint protection: Use solutions such as Acronis Cyber Protect to detect ransomware behaviors and prevent unauthorized encryption.
- Maintain offline backups: Regularly back up critical data to storage that is immutable or otherwise inaccessible to malware.
