Dharma Ransomware Intrusions Exhibit Consistent Techniques

By Eric Loui - Karl Scheuerman - Aaron Pickett - Brendon Feeley

Archived: 2026-04-05 15:41:23 UTC

Since at least 2018, criminal actors have been conducting big game hunting (BGH) campaigns, deploying ransomware on a targeted scale against large corporations or governments in pursuit of lucrative payouts. These BGH campaigns have netted millions of dollars (USD) for major criminal actors like WIZARD SPIDER and INDRIK SPIDER. However, BGH is not exclusive to sophisticated adversaries deploying advanced malware. One example is a series of BGH intrusions where criminal actors used common tactics to deploy Dharma ransomware. Throughout 2019 and into 2020, the CrowdStrikes Falcon OverWatch™ and Intelligence teams have identified ongoing attempts by criminal actors to install Dharma ransomware across a diverse range of organizations worldwide. Dharma has been in operation since 2016 under a ransomware-as-a-service (RaaS) model, where developers license or sell ransomware to other criminals who then carry out an attack using the malware. Dharma affiliates do not appear to discriminate among industries. Victims have been identified in the following sectors:

- Academic
- Automotive
- Energy
- Extractive
- Financial Services
- Government
- Healthcare
- Hospitality
- Legal
- Logistics
- Manufacturing
- Media
- Retail
- Technology
- Telecommunications
- Transportation

These intrusions have exhibited consistent techniques that include gaining initial access over Remote Desktop Protocol (RDP) brute forcing or password spraying, using publicly available utilities to attempt to identify and uninstall security software, harvesting credentials, and mapping network shares.

Background: Dharma Status and Code Similarity Across Variants

CrowdStrike identified that the original author of Dharma released the source code in 2016 before ceasing activity. Since this threat actor’s departure, Dharma has been marketed and sold by multiple, apparently independent

actors, two of which were active in 2019 — and at least one remains active as of January 2020. Separately, while the Phobos ransomware is likely to have been inspired by Dharma, the codebase of Phobos appears separate from Dharma. Although Dharma is not centrally controlled — in contrast to major RaaS families, such as REvil, which is operated by PINCHY SPIDER — the code has not been forked or meaningfully altered across distribution channels. CrowdStrike® Intelligence analyzed Dharma variants from multiple sources, including BGH incidents tracked by the OverWatch team as well as separately identified Dharma samples. (For example, several samples were observed being dropped by Smoke Bot, a loader that is developed by an adversary tracked as SMOKY SPIDER by CrowdStrike Intelligence.) Code comparison of these Dharma samples rendered a 100% match of the functions in all analyzed samples. The sample files compared are 99% similar in their entirety. This analysis revealed that, across all samples, the only differences were the encryption keys, ransom note content, contact email, appended file extension, and ransom note file name, which are commonly customizable in RaaS operations. Due to the overlapping nature of these variants, it is not currently possible to distinguish Dharma used in BGH campaigns from other Dharma operations, so there is a lack of visibility into the operational clusters and operating actors.

Initial Access

Based on CrowdStrike's observations, Dharma affiliates running BGH operations gain access to victims primarily through RDP. These actors use brute forcing or password spraying to compromise accounts. Dharma affiliates have also been observed authenticating using valid credentials, which were likely obtained by the threat actor directly or purchased on underground forums. It is likely that brute forcing or password spraying are performed by automated tools, such as NLBrute, which is discussed in more detail below. Administrator accounts have specifically been targeted in multiple Dharma incidents, likely because they provide a higher-privilege level of access, which increases the actor's chances of a successful Dharma intrusion — particularly the infection of many hosts in one deployment. Outside of RDP, Dharma affiliates have likely exploited internet-facing software vulnerabilities, primarily in SQL servers. Following successful initial access, the Falcon OverWatch team has identified execution of the "Mouse Lock" utility, likely to prevent legitimate users from authenticating and interrupting an interactive session. If initial access was not gained over RDP, Dharma actors have been observed enabling remote desktop from the command line with the following command, probably to enable persistent access: `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t reg_dword /d 0 /f.`

Defense Evasion

Across observed Dharma cases, the operators used a consistent set of tools to identify and terminate security software, such as endpoint protection products or security information and event management (SIEM) alert forwarders. The presence of more than one of these tools may be an indicator of malicious activity and can be used to detect BGH Dharma attacks. Dharma affiliates have primarily used two publicly available utilities for this purpose — PCHunter and ProcessHacker. These powerful utilities allow actors to not only view and terminate processes, but also to directly interface with the Windows kernel itself. In most cases, these tools are actually saved and run with their default names, as `PCHunter32.exe, PCHunter64.exe` or `Processhacker.exe.` In at least one instance, PCHunter was downloaded by an adversary using a web browser and saved into the user's Downloads directory before being executed. Dharma affiliates have tried a variety of other free utilities for

terminating security software. These include: PowerTool x64, GMER, Total Uninstall Portable and Defender Control. The first two include kernel manipulation functionality similar to the capabilities of PCHunter and ProcessHacker. Total Uninstall is designed for uninstalling software, while Defender Control specifically seeks to disable Windows Defender. CrowdStrike has also identified Dharma affiliates attempting to use PowerShell and WMIC for similar purposes. One observed example of a WMIC command is: `wmic product where name="" call uninstall /nointeractive.` In addition to the above techniques, Dharma affiliates have attempted to modify pertinent registry keys to disable security protections. In one instance, the actors ran the following command line interface (CLI) instruction to disable user account control (UAC): `REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f` Other instances of registry tampering have focused on disabling Windows Defender functions.

Credential Access and Lateral Movement

Dharma affiliates tracked by CrowdStrike use typical methods to obtain credentials and propagate laterally within a network.Most Dharma cases include Mimikatz, and multiple cases included the use of NirSoft CredentialsFileView, which allows for the recovery of passwords stored in encrypted credential files. Any obtained credentials are likely used to attempt privilege escalation — if actors don't already have administrator access — as well as lateral movement. Dharma affiliates typically use a distinctive utility to map network shares, which can subsequently be encrypted by the ransomware. Additionally, the tool NLBrute has been identified in multiple Dharma incidents. This RDP brute-forcing tool has been available on underground forums since at least 2016 and is likely used to gain access to additional systems within a network. In multiple cases, CrowdStrike identified the presence of the free Advanced IP Scanner utility, which can be used to map a local area network (LAN) and enable control of systems via RDP.

Ransomware Execution

Prior to executing the ransomware, Dharma affiliates use scripts to disable and delete volume shadow copies or host file backups in order to prevent easy recovery. The actors have also used scripts to wipe system logs. To ensure Dharma has the maximum impact, affiliates have used IObit Unlocker to release locked files on shared drives so that these files may be encrypted. Similarly, Dharma actors commonly use scripts to terminate running services (e.g., by using `net stop`) to release files used by these services, therefore allowing them to be encrypted. CrowdStrike OverWatch has detected attempts to specifically stop database services, likely because database storage files are of high value. Dharma is then typically written to disk as an executable file (EXE) and subsequently executed. In an unsuccessful Dharma installation attempt identified on September 1, 2019, the ransomware was contained in a 7-zip, self-extracting executable. This file format is an EXE that can unpack an embedded `.7z` archive without the use of 7-zip software.

Outlook and Implications

These Dharma campaigns resemble other recent BGH campaigns. Attempts to disable security products running on victim hosts continued to be an observed tactic, technique and procedure (TTP) for BGH actors during 2019 and into 2020. One of the first instances of this TTP occurred during a February 2019 PINCHY SPIDER affiliate

campaign. ProcessHacker has also been used in DOPPEL SPIDER BGH campaigns to terminate security software. It is likely Dharma campaigns will continue for the foreseeable future.

Recommendations

Security solutions such as the CrowdStrike Falcon®® endpoint protection platform come with many preventive features to protect against threats like Dharma. These features — which include machine learning (ML), behavioral preventions and executable quarantining — are highly effective at stopping ransomware and other common techniques criminal organizations employ.

MITRE ATT&CK Tactic and Technique Mapping

The following table maps Dharma BGH affiliates' intrusion methods to the MITRE ATT&CK® framework.

Tactic	Technique	Description
Initial Access	Exploit Public-Facing Application (T1190), Valid Accounts (T1078)	Dharma operatives primarily access accounts using RDP brute force and password spraying attempts, which will result in authentication failure events. In multiple instances, Dharma affiliates gained an initial foothold following successful exploitation of a SQL server application.
Execution	Command Line Interface (T1059), Graphical User Interface (T1061), PowerShell (T1086), Scheduled Task (T1053), Scripting (T1064), Windows Management Instrumentation (T1047)	Dharma is deployed during interactive RDP sessions. During these sessions, the actors both pass instructions to the CLI and use the graphical user interfaces (GUIs) built into the aforementioned utilities. The CLI may be used to execute dropped scripts (such as with Wscript) or to run PowerShell and WMI commands. In at least one intrusion, actors used the schtasks utility to schedule an executable to run every 60 minutes.
Persistence	Valid Accounts (T1078)	Authentication credentials enable Dharma affiliates to maintain access to target systems without using malware.
Privilege Escalation	Valid Accounts (T1078), Scheduled Task (T1053)	In the bulk of Dharma intrusions, the operators specifically attempt to gain access to administrator accounts over RDP. Dharma actors may also attempt to use schtasks with the `/RL HIGHEST` flag to execute a file with the highest privilege level.
Defense Evasion	Bypass UAC (T1088), Disabling Security Tools (T1089), Modify	Dharma affiliates use a variety of free utilities to attempt to uninstall security products, as well as using PowerShell (e.g., `powershell.exe Set-MpPreference -`

	Registry (T1112), Valid Accounts (T1078)	`DisableRealtimeMonitoring $true`) or WMI for this purpose. Additionally, in some circumstances Dharma actors will modify registry keys to disable UAC, disable Windows Defender or enable RDP access. The use of administrative accounts allows actors to bypass access controls throughout all phases of the intrusion.
Credential Access	Brute Force (T1110), Credential Dumping (T1003), Credentials in Files (T1081)	Mimikatz allows actors to retrieve credentials from memory. Mimikatz and NirSoft CredentialsFileView each allow collection of credentials from various types of files, including Windows credential files specifically. Additionally, Dharma affiliates use brute force and password spraying over RDP to gain access to systems within a network.
Discovery	File and Directory Discovery (T1083), Network Share Discovery (T1135), Network Service Scanning (T1046), Process Discovery (T1057), Remote System Discovery (T1018), Security Software Discovery (T1063), System Network Configuration Discovery (T1016), System Network Connections Discovery (T1049)	Dharma affiliates routinely deploy tools to map the LAN that a compromised system is on — including network shares. These actors also likely identify security services in order to attempt to terminate these services. These actors have also used the free Everything indexer tool to enumerate the contents of a victim system.
Lateral Movement	Remote Desktop Protocol (T1076), Windows Admin Shares (T1077)	RDP provides the main lateral movement vector for Dharma affiliates, who both use previously collected legitimate credentials and attempt brute force or password spraying. Additionally, Dharma affiliates seek to map and authenticate to network shares in order to encrypt them.
Collection	N/A	There is no evidence Dharma actors seek to steal information from compromised systems.
Exfiltration	N/A	There is no evidence Dharma actors seek to steal information from compromised systems.
Command and Control	Remote File Copy (T1105), Standard Application Layer Protocol (T1071)	The actors typically download a variety of utilities to interfere with security software. As mentioned above, systems are controlled through manual RDP sessions rather than beaconing malware.

Impact	Data Encrypted for Impact (T1486), Inhibit System Recovery (T1490), Service Stop (T1489)	Prior to attempting to execute Dharma, threat actors will typically attempt to delete shadow copies or disable host file backups, and may attempt to stop services running on servers in order to be able to encrypt files accessed by those services.

Table 1. MITRE ATT&CK Mapping

Additional Resources

- *Download the CrowdStrike 2020 Global Threat Report.*
- *To learn more about how to incorporate intelligence on threat actors and their tactics techniques and procedures (TTPs) into your security strategy, please visit the CROWDSTRIKE FALCON® INTELLIGENCE™ Threat Intelligence page.*
- *Get a full-featured free trial of CrowdStrike Falcon® Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*
