datto

Table of Contents



# Dharma Threat Brief

CrySiS

Dharma is a ransomware sold by its developers under a Ransomware-as-a-Service (RaaS) model since 2016.

Based on the contents of the RaaS offering, it appears Dharma is intended for use by inexperienced cybercriminals. Operators package and provide affiliates with resources, commonly used by malicious actors and red teams, to perform ransomware attacks.

## Motives

Both the developers and affiliates of Dharma are financially motivated. Affiliates are known to target small and medium-sized enterprises, with a high-volume of attacks, but low ransom demands. This kind of operation is in stark contrast to other RaaS groups who run low-frequency but high-value attacks known as Big Game Hunting.

## Tactics, Techniques, and Procedures (TTPs)

The Dharma ransomware service appears to be offered to inexperienced cybercriminals as a package of pre-built tools and scripts is included in the service for use throughout the ransomware attack.

Reporting from Coveware reveals, a majority of Dharma ransomware attacks gain initial access to victim networks via remote desktop protocol (RDP). RDP credentials are sold on dark web markets, making it easy for affiliates to pick a target and begin a ransomware attack without having to perform any reconnaissance or resource development themselves.

Once initial access has been established, affiliates have been observed utilizing publicly available hacking tools to harvest credentials. Then move laterally around the network and escalate privileges to perform a ransomware attack to full effect. These tools have been observed packaged into a PowerShell script that allows affiliates to perform all necessary commands and operations from a single PowerShell console window, simplifying the process for inexperienced affiliates.

## Mitre ATT&CK

The following maps Dharma's TTPs to MITRE ATT&CK:

### Initial Access

- **External Remote Services (T1133) -** Dharma affiliates have gained initial access to victim networks via RDP.
- **Valid Accounts (T1078) -** Dharma affiliates have used valid account credentials to gain access to victim networks.

### Execution

- **Command and Scripting Interpreter: Windows Command Shell (T1059.003) -** Dharma starts cmd.exe to execute commands.
- **Command and Scripting Interpreter: Powershell (T1059.001) -** Dharma affiliates have used PowerShell to execute commands.
- **Windows Management Instrumentation (T1047) -** Dharma affiliates have been observed executing WMI commands.

### Persistence

- **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) -** Dharma adds itself to the Registry Autorun and Startup folder to maintain persistence.

### Privilege Escalation

- **Scheduled Task/Job: Scheduled Task (T1053.005) -** Dharma affiliates have tried to escalate privileges by running schtasks with the /RL HIGHEST flag.

### Defense Evasion

- **Impair Defenses: Disable or Modify Tools (T1562.001) -** Dharma affiliates have been observed disabling Windows Defender during attacks.
- **Modify Registry (T1112) -** Dharma affiliates have modified the registry in order to attempt to bypass UAC.
- **Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) -** Dharma affiliates have been observed disabling UAC.

### Discovery

- **Network Service Scanning (T1046) -** Dharma affiliates have used Advanced IP Scanner to scan victim networks.
- **Process Discovery (T1057) -** Dharma affiliates have used Process Hacker for process discovery.
- **Remote System Discovery (T1018) -** Dharma affiliates have used PowerShell scripts to retrieve a list of computers from Active Directory.
- **Network Share Discovery (T1135) -** Dharma affiliates have used PowerShell scripts to discover network shares.

### Impact

- **Inhibit System Recovery (T1490) -** Dharma can delete shadow copies to prevent easy restoration post-encryption.
- **Data Encrypted for Impact (T1486) -** Dharma can encrypt files and demands a ransom to decrypt the files.

## Mitigations/Defenses

Implementing a strong foundation of security controls is recommended to defend your network against Dharma ransomware attacks. In particular, ensuring that RDP access is properly secured and not publicly accessible is one of the best ways to prevent your network from being a target of Dharma affiliates.

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

**The following table maps Dharma's MITRE ATT&CK techniques to CIS v8 Safeguards:**

| MITRE ATT&CK | CIS Safeguards |
|---|---|
| External Remote Services (T1133) | **IG1**<br>2.3: Address Unauthorized Software<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure<br>4.4: Implement and Manage a Firewall on Servers<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.3: Require MFA for Externally-Exposed Applications<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>7.1: Establish and Maintain a Vulnerability Management Process<br>7.2: Establish and Maintain a Remediation Process<br>7.3: Perform Automated Operating System Patch Management<br>7.4: Perform Automated Application Patch Management<br>11.3: Protect Recovery Data<br>11.4: Establish and Maintain an Isolated Instance of Recovery Data |

| | |
|---|---|
| Valid Accounts (T1078) IG1 | **IG1**<br>3.1: Establish and Maintain a Data Management Process<br>3.3: Configure Data Access Control Lists<br>3.4: Enforce Data Retention<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.2: Establish and Maintain a Secure Configuration Process<br>for Network Infrastructure<br>4.4: Implement and Manage a Firewall on Servers<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.1: Establish and Maintain an Inventory of Accounts<br>5.2: Use Unique Passwords<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.3: Require MFA for Externally-Exposed Applications<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>7.1: Establish and Maintain a Vulnerability Management Process<br>7.2: Establish and Maintain a Remediation Process<br>7.3: Perform Automated Operating System Patch Management<br>7.4: Perform Automated Application Patch Management<br>8.1: Establish and Maintain an Audit Log Management Process<br>8.2: Collect Audit Logs<br>8.3: Ensure Adequate Audit Log Storage<br>9.2: Use DNS Filtering Services |
| Command and Scripting Interpreter: Windows Command Shell (T1059.003) | **IG1**<br>2.1: Establish and Maintain a Software Inventory<br>2.2: Ensure Authorized Software is Currently Supported<br>2.3: Address Unauthorized Software<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>10.1: Deploy and Maintain Anti-Malware Software<br>10.2: Configure Automatic Anti-Malware Signature Updates |

| | |
|---|---|
| Command and Scripting Interpreter: Powershell (T1059.001) | **IG1**<br>2.1: Establish and Maintain a Software Inventory<br>2.2: Ensure Authorized Software is Currently Supported<br>2.3: Address Unauthorized Software<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>10.1: Deploy and Maintain Anti-Malware Software<br>10.2: Configure Automatic Anti-Malware Signature Updates |
| Windows Management Instrumentation (T1047) | **IG1**<br>4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure<br>4.4: Implement and Manage a Firewall on Servers<br>4.6: Securely Manage Enterprise Assets and Software<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.2: Use Unique Passwords<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>9.2: Use DNS Filtering Services |
| Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) | **IG1**<br>2.3: Address Unauthorized Software<br>3.3: Configure Data Access Control Lists<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>10.1: Deploy and Maintain Anti-Malware Software<br>10.2: Configure Automatic Anti-Malware Signature Updates<br>14.3: Train Workforce Members on Authentication Best Practices<br>14.4: Train Workforce on Data Handling Best Practices |

| | |
|---|---|
| Scheduled Task/Job: Scheduled Task (T1053.005) | **IG1**<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.8: Define and Maintain Role-Based Access Control<br>8.3: Ensure Adequate Audit Log Storage<br>18.3: Remediate Penetration Test Findings<br>18.5: Perform Periodic Internal Penetration Tests |
| Impair Defenses: Disable or Modify Tools (T1562.001) | **IG1**<br>3.3: Configure Data Access Control Lists<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.2: Establish and Maintain a Secure Configuration Process or Network Infrastructure<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>8.1: Establish and Maintain an Audit Log Management Process<br>8.2: Collect Audit Logs<br>8.3: Ensure Adequate Audit Log Storage |
| Modify Registry (T1112) | **IG1**<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.2: Use Unique Passwords<br>5.3: Disable Dormant Accounts<br>6.3: Require MFA for Externally-Exposed Applications<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>11.4: Establish and Maintain an Isolated Instance of Recovery Data<br>14.1: Establish and Maintain a Security Awareness Program<br>14.3: Train Workforce Members on Authentication Best Practices |

| | |
|---|---|
| Abuse Elevation Control Mechanism: Bypass User Account Control (T1548.002) | **IG1**<br>3.3: Configure Data Access Control Lists<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>7.1: Establish and Maintain a Vulnerability Management Process<br>7.2: Establish and Maintain a Remediation Process<br>7.3:Perform Automated Operating System Patch Management |
| Credentials from Password Stores (T1555) | **IG1**<br>2.3: Address Unauthorized Software<br>3.1: Establish and Maintain a Data Management Process<br>3.2: Establish and Maintain a Data Inventory<br>3.3: Configure Data Access Control Lists<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure<br>4.4: Implement and Manage a Firewall on Servers<br>4.5: Implement and Manage a Firewall on End-User Devices<br>4.6: Securely Manage Enterprise Assets and Software<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.1: Establish and Maintain an Inventory of Accounts<br>5.2: Use Unique Passwords<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>7.1: Establish and Maintain a Vulnerability Management Process<br>7.2: Establish and Maintain a Remediation Process<br>7.3: Perform Automated Operating System Patch Management<br>11.3: Protect Recovery Data<br>14.2: Train Workforce Members to Recognize Social Engineering Attacks<br>14.3: Train Workforce Members on Authentication Best Practices<br>14.4: Train Workforce on Data Handling Best Practices<br>14.6: Train Workforce Members on Recognizing and Reporting Security Incidents |

| | |
|---|---|
| OS Credential Dumping (T1003) | **IG1**<br>3.3: Configure Data Access Control Lists<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.2: Use Unique Passwords<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>11.3: Protect Recovery Data<br>14.1: Establish and Maintain a Security Awareness Program<br>14.3: Train Workforce Members on Authentication Best Practices |
| Network Service Scanning (T1046) | **IG1**<br>4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure<br>4.4: Implement and Manage a Firewall on Servers<br>4.6: Securely Manage Enterprise Assets and Software<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.2: Use Unique Passwords<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>9.2: Use DNS Filtering Services |
| Process Discovery (T1057) | **IG1**<br>2.1: Establish and Maintain a Software Inventory<br>2.2: Ensure Authorized Software is Currently Supported<br>2.3: Address Unauthorized Software<br>3.3: Configure Data Access Control Lists<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>8.1: Establish and Maintain an Audit Log Management Process<br>8.2: Collect Audit Logs<br>8.3: Ensure Adequate Audit Log Storage<br>10.1: Deploy and Maintain Anti-Malware Software<br>10.2: Configure Automatic Anti-Malware Signature Updates<br>10.3: Disable Autorun and Autoplay for Removable Media<br>14.1: Establish and Maintain a Security Awareness Program<br>14.2: Train Workforce Members to Recognize Social Engineering Attacks<br>14.6: Train Workforce Members on Recognizing and Reporting Security Incidents |

| | |
|---|---|
| Remote System Discovery (T1018) | **IG1**<br>2.3: Address Unauthorized Software<br>4.1: Establish and Maintain a Secure Configuration Process |
| Network Share Discovery (T1135) | **IG1**<br>2.3: Address Unauthorized Software<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure<br>4.4: Implement and Manage a Firewall on Servers<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>6.3: Require MFA for Externally-Exposed Applications<br>6.4: Require MFA for Remote Network Access<br>6.5: Require MFA for Administrative Access<br>7.1: Establish and Maintain a Vulnerability Management Process<br>7.2: Establish and Maintain a Remediation Process<br>7.3: Perform Automated Operating System Patch Management<br>7.4: Perform Automated Application Patch Management<br>11.3: Protect Recovery Data<br>11.4: Establish and Maintain an Isolated Instance of Recovery Data |
| Inhibit System Recovery (T1490) | **IG1**<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>7.1: Establish and Maintain a Vulnerability Management Process<br>7.2: Establish and Maintain a Remediation Process<br>7.3: Perform Automated Operating System Patch Management<br>11.1: Establish and Maintain a Data Recovery Process<br>11.2: Perform Automated Backups<br>11.3: Protect Recovery Data<br>11.4: Establish and Maintain an Isolated Instance of Recovery Data |

| | |
|---|---|
| Data Encrypted for Impact (T1486) | **IG1**<br>4.1: Establish and Maintain a Secure Configuration Process<br>4.4: Implement and Manage a Firewall on Servers<br>4.7: Manage Default Accounts on Enterprise Assets and Software<br>5.3: Disable Dormant Accounts<br>5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts<br>6.1: Establish an Access Granting Process<br>6.2: Establish an Access Revoking Process<br>11.1: Establish and Maintain a Data Recovery Process<br>11.2: Perform Automated Backups<br>11.3: Protect Recovery Data<br>11.4: Establish and Maintain an Isolated Instance of Recovery Data |



## Detection Opportunities

Dharma affiliates use well-known tools and techniques in order to successfully deploy ransomware to victim networks, some of which can be detected

The following detection opportunities are mapped to MITRE ATT&CK v9 methods, CIS v8 Safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

### Detection Opportunity 1: Shadow Copy and System State Backup Deletion

**MITRE ATT&CK:** Scheduled Task (T1053.005)

**CIS Control(s):** 2.1, 2.2, 2.3, 3.3, 4.1, 4.7, 5.3, 5.4, 6.1, 6.2, 8.1, 8.2, 8.3, 10.1, 10.2, 10.3, 14.1, 14.2, 14.6

**Red Canary Atomic Red Team Test(s):** T1053.005 Atomic Test #2

In order to escalate privileges on victim machines, Dharma affiliates have been observed trying to create and run scheduled tasks with the /RL HIGHEST flag. This flag sets the 'run level' for the task, which defaults to LIMITED when not specified. By running the scheduled task at HIGHEST, the attacker is able to gain Administrator-level privileges to the victim device. To detect and defend against this method of privilege escalation within your own network, you can collect and alert on Windows command line logs where new scheduled tasks are being created with the /RL HIGHEST flag.

## References/Appendix/Resources

techcommunity.microsoft.com/t5/core-infrastructure-and-security/dharma-ransomware-recovery-and-preventative-measures/ba-p/1745297

news.sophos.com/en-us/2020/08/12/color-by-numbers-inside-a-dharma-ransomware-asa-service-attack/

blog.malwarebytes.com/threat-analysis/2019/05/threat-spotlight-crysis-aka-dharma-ransomware-causing-a-crisis-for-businesses/

app.any.run/tasks/1d5a3397-2f4d-44ec-8883-913829ef3b63/

crowdstrike.com/blog/targeted-dharma-ransomware-intrusions-exhibit-consistent-techniques/