INTERRUPT AND ALERT ON RANSOMWARE ATTACKS

WITH NORTHERN

NORTHERN

INTERRUPT AND ALERT

Northern's software solution (NSS) offers the ability to prevent files that have extensions associated with ransomware from being saved and to alert security teams when attempts to save these types of files are made.

Through integration with proprietary APIs ("FPolicy" on NetApp systems, "CEPA" on EMC systems, "File Filtering" on HDS HNAS), Northern delivers the ability to monitor file system activity as it is taking place and to deny file operations if they do not comply with standards determined by the organization.

The majority of ransomware attacks result in files becoming encrypted and saved with a new file extension. This is true for most of the common ransomware families (CrySiS, Dharma, Locky, TeslaCrypt, CryPy, etc.).

By creating policies to deny attempts to write or rename files with known ransomware encryption extensions, Northern is able to interrupt ransomware attacks. Additionally, and perhaps most importantly, attempts to perform denied operations are logged and alerts can be triggered; informing the organization's security team that an attack has commenced and enabling them to respond immediately.

REGULAR REPORTING

In addition to the ability to continuously monitor for ransomware attacks, Northern's file system content reporting capabilities can be used to periodically scan for files that reveal a ransomware infection.

By regularly reviewing file systems for files created by ransomware, such as files containing instructions for how to decrypt or recover data, the organization is able to isolate and decontaminate infected systems.

VALUE

Northern is not suggesting that this approach is a replacement for ant-virus solutions or other anti-malware best practices. However, as an addition to existing protections Northern is able to offer a valuable final layer of defense.

The primary value of configuring NSS to report on ransomware infections, and monitor for, interrupt, and alert on, ransomware attacks lies in the alerting capability.

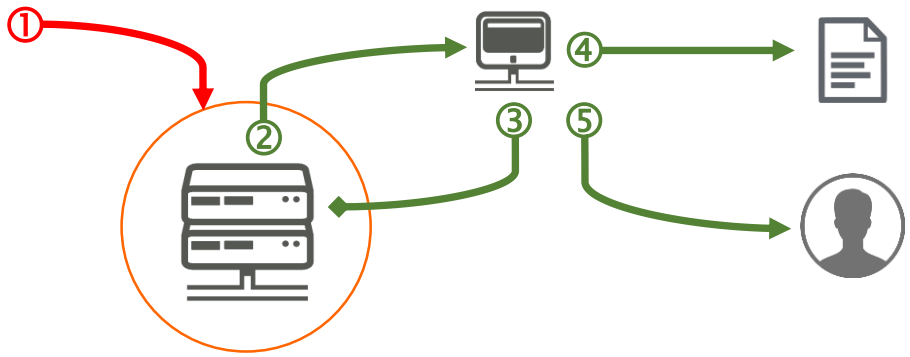
By notifying the organization's security team of an ongoing attack, within minutes of its commencement, the organization is able to significantly limit the cost and complexity of data recovery operations.

NORTHERN

RUNTIME OPERATIONS

The image below provides an overview of key operations that take place when NSS is configured to prevent the saving of file types associated with ransomware.

Figure 1: Runtime operations in NSS File Block:



1. A request is made to write/rename a file.
2. The request is sent to NSS for comparison against configured policies (FPolicy, CEPA, HNAS).
3. The intended file extension is found to be in violation of the configured policy and a denied response is returned to the target storage device – the operation is not performed.
4. The deny action is logged in NSS' internal logs (txt file format).
5. A report is sent via email to a target address or group. The report is sent every five minutes (default setting that can be changed) if an attempted violation occurred. The report includes path, user, intended file name, and timestamp information.

SYSTEM REQUIREMENTS

- A complete installation of NSS on one or more (virtualized) application servers.
  - Windows Server 2012 R2 (preferred, older systems supported)
  - CPU: 6 core Xeon 5500 or equivalent
  - RAM: 6 GB or higher
  - HDD: 20 GB available
- A compatible target storage device
  - Dell EMC Unity or VNX (DART 7.0.12 or later, VEPA/CEPA installed)
  - HDS HNAS (12.3 or later)
  - NetApp 7-Mode (Data ONTAP 8 or later)
  - NetApp Clustered Data ONTAP (Data ONTAP 8.3 or later)

NORTHERN