Technical Report

The NetApp Solution for Ransomware

Product Security Team, NetApp
May 2019 | TR-4572

Abstract

This guide covers what ransomware is; how it has evolved; and how to identify, thwart, and remediate this threat using the NetApp® ONTAP® solution. The guidance and solutions provided in this guide are designed to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

n NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1   What Is Ransomware?

The evolution of today's threat landscape continues to present organizations with unique challenges for protecting their most valuable data and information. Current threats and vulnerabilities continue to increase in sophistication. In 2017, ransomware saw a 32% increase in the number of ransomware families (Figure 1). In addition, despite the lower number of breaches from 2016 to 2017, the number of affected records increased by 49%, as seen and documented by the FBI in the TrendLabs 2017 Security Roundup (Table 1). This increase highlights the improved effectiveness of ransomware breaches. Ransomware is a threat to everyone in an organization, from the chief information officer to the business continuity leadership.

Ransomware is malware that prevents or limits the use of systems or resources until a ransom is paid. Although ransomware can attack businesses and other institutions, attacks can occur on a personal level as well. Such attacks can be placed into two categories:

- **Encrypted ransomware.** Encrypted ransomware uses algorithms to encrypt files and resource access. The malware then demands a ransom in exchange for the keys or decryption method. This is the most common ransomware that organizations encounter today.

- **Locker ransomware.** Locker ransomware is more prevalent in individual or personal environments. This method locks access to the host or operating system. Although this method is most common in the personal realm, it can also affect organizations and business environments. In addition, because it occurs at the lower scale of individual hosts or operating systems, the ransoms demanded are usually less as well (one hundred to a couple of hundred dollars, for example). In a typical scenario, a parent might receive a message indicating that access to their computer and pictures stored on it has been locked and a ransom must be paid to unlock it.

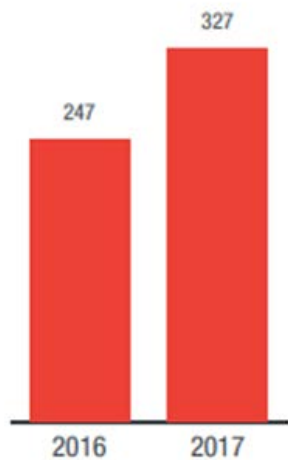**Figure 1) Increase in ransomware families in 2017.**

Table 1) Number of affected records 2016–2017.

Year	Data Breaches Disclosed	Affected Records
2016	813	3,310,435,941
2017	553	4,923,053,245

Notably, the nature of the threat vectors is always changing and growing more widespread. Ransomware typically uses the following vectors:

- Email

- URL downloads
- Exploit kits
- Direct ransomware files
- USB dongles and flash drives

In addition to vectors, the methodologies used to convince users to pay the ransom is also changing. A few examples are as follows:

- **Jigsaw.** Threatens to delete files every hour until the ransom is paid.
- **Surprise.** Increases the ransom amount if the entity fails to pay the ransom prior to the deadline.

Another key evolution of this threat is malware exploit behavior. Common exploits include CRYPSAM, which targets unpatched servers. Exploits also target network segments, database-related files, tax returns, and even files related to web hosting.

How does an organization deal with this threat? A successful solution includes a layered defense that encompasses corporate policies, procedures, and resources coupled with capable partners. A successful solution typically includes the following components:

- Next-generation platforms, including firewalls, intrusion detection systems, an intrusion prevention system (IPS), web filtering, and antimalware solutions (network and endpoint)
- Malware-based protection signatures
- Access control solutions that perform functions such as authentication, authorization, accounting for visibility, and role-based access control
- Web applications, such as Microsoft SharePoint, in which a user must authenticate with a browser

These kinds of architecture solutions are often overlooked with regard to ransomware because administrators often focus instead on recovery and remediation. However, these layered constructs should remain proactive visibility solutions that provide an initial defense to thwart miscreants from accessing the environment.

In response, NetApp recommends using network-based and endpoint-based solutions to establish a security posture. NetApp also recommends using a partner organization for help establishing the architecture. The remainder of this report focuses on the following recommendations and solutions for ransomware specific to NetApp:

- **Visibility and detection.** Visibility is critical for defending against and subsequently remediating a ransomware attack.
- **Remediation.** Creating backups with NetApp Snapshot™ copies protects critical data from deliberate destruction.

2   NetApp Solutions for Ransomware

2.1   Visibility and Detection

Visibility is critical for security. If malware is moving through your file system architecture and encrypting files, the rate of data change increases. In addition, storage efficiencies such as deduplication and compression decrease. Indeed, a rate-of-change increase is a key indicator of malware activity. The NetApp solution provides monitoring tools that can help identify ransomware by comparing the change-of-data signature with other antivirus software to show a pattern.

As ransomware spreads, it can affect more data, again indicated by an increased rate of change. Therefore, it is important to remain engaged with Snapshot copies, because monitoring Snapshot copies can provide an indicator of the infection point or any file changes. Maintaining awareness of the state of Snapshot copies can also help with the remediation phase. It can be difficult to go through individual

Snapshot copies to identify the point of infection, so you can opt to use an uninfected Snapshot copy for remediation. Because remediation is simpler when using an uninfected Snapshot copy, you should consider recovery time objectives (RTOs) and recovery point objectives (RPOs).

In addition to using partnerships and visibility tools to identify file modification dates, sweeping modifications, deletes, and so on, in-house or homegrown scripts can be used to perform such functions. The following example script uses Cygwin:

```
$ find . -exec stat -c "%n: %y" {} \;
.: 2016-10-20 11:10:41.630101100 +0200
./.rhel7 setup.txt.swp: 2016-10-20 11:06:38.029430400 +0200
./ava comparison.txt: 2016-08-23 10:41:09.616588100 +0200
./ava setup.txt: 2016-04-28 12:06:03.397551000 +0200
./ava.txt: 2016-09-05 18:15:24.272040700 +0200
./aws.setup.txt: 2016-07-10 20:09:23.603027000 +0200
./bare-metal-recovery.txt: 2016-07-20 11:19:53.291283000 +0200
./fli commands: 2016-06-17 17:35:59.978080600 +0200
./fli.setup.txt: 2016-06-16 12:21:29.403969100 +0200
./Lab.txt: 2016-04-17 13:11:16.864710300 +0200
./prepop commands.txt: 2016-08-01 11:05:50.021615300 +0200
./rac-setup.txt: 2016-06-03 09:08:52.290334900 +0200
./rhel7 setup.txt: 2016-10-20 02:45:18.480132000 +0200
./rhel7.1-4.setup.txt: 2016-05-30 14:13:14.945411500 +0200
```

This script locates and prints all files by using the file name and modification date and runs a diff to compare the ransomed files with the Snapshot copies. You can see which files have changed with an Excel spreadsheet.

Partners and third parties provide solutions and augmentations to the NetApp portfolio that help identify attack indicators. You must understand these solutions and the specific details and functions they provide so that you can understand the solution's impact on your environment.

Some solutions provide monitoring software that tracks user behaviors and interactions with data, including how and when they access files. This software uses proactive monitoring tools and dashboards that notify administrators and operators of potential rogue activities, such as when a user accesses known bad sites or when they encrypt files. In addition, some solutions provide preventive and actionable measures by leveraging the NetApp FPolicy™ function to perform filtering and access controls for file systems.

Other solutions apply intelligence details to data ownership, usage, and access details. This information depicts what data exists, who has access to it, who is using it, and how they are using it. The resulting information provides key visibility and insights that can indicate rogue or malicious activities. These types of solutions typically provide monitoring and visibility capabilities. Therefore, you must use other solutions to filter or actively thwart an attack.

2.2 Remediation

Performing backups is the industry best practice for ransomware remediation. You have two options after an organization has encountered ransomware: either pay the ransom or restore from backup. Having a backup solution in place is key for adopting the restoration option. NetApp recommends that organizations identify all data sources at risk for ransomware exposure (for example, file shares). Managers can then create or adjust RPOs with data recovery procedures to make sure that these sources are backed up regularly.

Most ransomware infects an end-user laptop or workstation and then spreads to shared drives and mappings (including cloud mappings). Indeed, as ransomware continues to evolve, it can also infect unmounted shares. In a typical environment, file and data synchronization, replication, and backup solutions are not affected by ransomware because an agent that does not execute malware or accept mappings (no mount points) handles these functions. Therefore, ransomware cannot travel to or execute in these subsystems, and restoring from backup remains the industry best practice. The NetApp solution

provides file blocking of certain file types created on the storage by using native file blocking or with the NetApp FPolicy solution.

NetApp FPolicy Solution

The NetApp FPolicy solution provides a file blocking methodology that allows organizations to filter or block traffic based on file extensions and file metadata. Common ransomware includes, but is not limited to, the following file types:

.micro	.encrypted	.locked	.crypto	.crypt	.crinf	.r5a
.XRNT	.XTBL	.R16M01D05	.pzdc	.good	.LOL!	.OMG!
.RDM	.RRK	.encryptedRSA	.crjoker	.EnCiPhErEd	.LeChiffre	._crypt
.locky	.SUPERCRYPT	.CTBL	.CTB2			

Creating an FPolicy policy to block or filter such file extensions or metadata helps to proactively thwart ransomware attacks. For more information concerning FPolicy, see the FPolicy page on the NetApp Support portal.

NetApp Ransomware Assessment

NetApp assesses the risk of a ransomware attack according to the number of Snapshot copies on a volume. While the level of risk is ultimately dependent on a data's rate of change, volumes with no Snapshot copies are deemed as volumes with a "very high" risk, due to the potential impact of a ransomware attack. Volumes with no Snapshot copies lack a quick recovery option that results in more costly backup recovery methods if an attack occurs.

In addition to assessing risk at the volume level, NetApp also analyzes each controller in a NetApp installed system. Illustrating a system's level of risk at the controller level allows NetApp to provide a descriptive ransomware risk assessment that helps you make informed decisions regarding backups and the use of NetApp Snapshot technology. For more information about how to receive a NetApp ransomware risk assessment, contact a NetApp sales representative.

NetApp Snapshot Technology

The key solution for ransomware remediation is restoring from images that are known to be uninfected. The NetApp solution is very well positioned in this area, with the NetApp Snapshot technology implemented throughout the Data Fabric. Snapshot copies are point-in-time copies that protect data with no performance effect and minimal storage space consumption. Snapshot technology also provides the granularity to create images of a single file copy or a complete disaster recovery solution.

In addition, with Snapshot technology, you can perform these operations in an efficient manner while applications are running. Snapshot copies can be made in less than a second on average, regardless of volume size, data activity, or function. Moreover, Snapshot copies are read-only files stored in the NetApp solution. For more information about NetApp Snapshot technology, see the NetApp Snapshot Technology Datasheet.

Malware comes in many forms. Dormant malware can infect an environment weeks or months prior to activation. Therefore, NetApp recommends increasing the retention time so that malware can be identified and uninfected files can be restored.

NetApp SnapRestore Technology and Other NetApp Solutions

There is an active remediation component in the Snapshot solution called NetApp SnapRestore® data recovery technology. SnapRestore can recover a single file or multiterabyte data volumes. SnapRestore also enables the automation of data recovery. The SnapRestore data recovery process is nearly instantaneous and is independent of the storage capacity or the number of files restored. NetApp

Snapshot technology is the foundation for the NetApp SnapManager®, NetApp SnapMirror®, SnapRestore, and NetApp SnapVault® solutions, all of which provide different capabilities to the Snapshot technology portfolio. For more information about NetApp SnapRestore technology, see the NetApp SnapRestore page on the NetApp portal.

Note: You must make sure that older Snapshot copies are not recycled. In addition, restores cannot come from previously infected files.

To help administrators identify malicious or unexpected behavior, the NetApp solution provides the following key outputs. These outputs can be used to identify Snapshot details and potentially infected files so that only clean files are restored:

- **atime.** This output represents the time of the last read or write to a file, indicating the last time the file was accessed.
- **ctime.** This output represents the time of the last size or status change, indicating the last time the file's inode was modified.
- **mtime.** This output represents the time of the last write to a file, indicating the last time the file was modified.

Case Study: Kroll Ontrack

If during a malware remediation process, all of your preencryption Snapshot copies have been lost, you might require the assistance of a third party. Kroll Ontrack has provided services in this area that use the NetApp solution for remediation. Kroll Ontrack has published a blog post discussing how it was able to recover malware-encrypted data from a customer environment by using NetApp Snapshot copies.

2.3   Snapshot Immutability and the SnapLock Solution

Given the threat of ransomware and it's specific impact on infiltrating or infecting files, it is key to understand the immutability of NetApp Snapshot copies. In addition to being read only, the NetApp SnapLock solution can be leveraged to add snapshot copies on specified cadence and automatically discard the snapshot copies that have aged out. This ensures that snapshot copies cannot be changed, renamed, or deleted until they are aged out based on the administrators configured policy. This solution effectively adds an additional layer of immunity to threats such as ransomware. For more details see the solution brief "Using SnapLock to recover from ransomware and other malicious events" (login required).

3   Conclusion

It is very clear that ransomware, like so many other malware threats, continues to evolve. Just as defensive methods improve, so do the attack methods and vectors. Although no single solution can thwart all attacks, using a portfolio of solutions, including partnerships and third parties, provides a layered defense.

The NetApp solution provides various effective tools for visibility, detection, and remediation. Traditional layered defense solutions remain prevalent, as do third parties and partner solutions for visibility and detection. Effective remediation remains a crucial part of the response to any threat. The unique industry approach leveraging the immutable NetApp Snapshot technology and SnapLock solution is an industry differentiator and the industry best practice for ransomware remediation.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NetApp ONTAP Documentation Center
  http://docs.netapp.com/ontap-9/index.jsp
- NetApp ONTAP Resources page
  http://mysupport.netapp.com/ontap/resources
- NetApp Product Security
  https://security.netapp.com/resources/
- NetApp Snapshot Technology
  www.netapp.com/us/media/ds-2477.pdf
- All other NetApp Product Documentation
  https://docs.netapp.com

Refer to the [Interoperability Matrix Tool (IMT)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

n NetApp®