Technical Report

The NetApp Solution for Ransomware

Product Security Team, NetApp
February 2017 | 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.

NetApp®

TABLE OF CONTENTS

LIST OF FIGURES

1 What Is Ransomware?

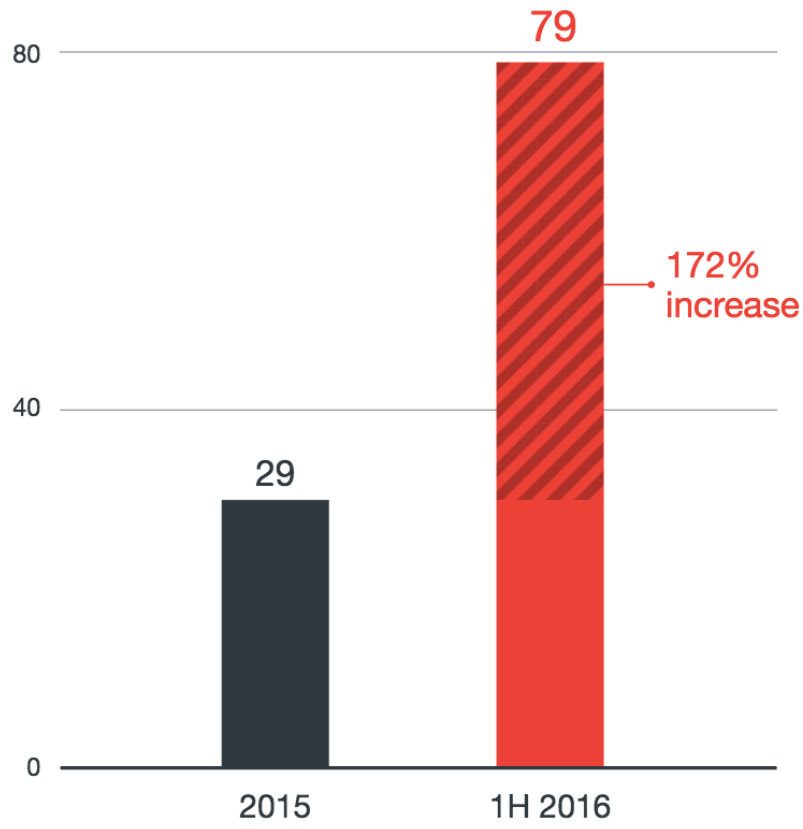
The evolution of today's threat landscape continues to present organizations with unique challenges for protecting their most valuable data and information. Current threats and vulnerabilities continue to increase in sophistication. In 2016, ransomware continued to dominate the threat landscape. In fact, the first half of 2016 saw a 172% increase in ransomware families over 2015 (see Figure 1). In addition, the first three months of 2016 saw enterprise organizations lose approximately $209 million to ransomware as reported by the FBI and documented in the TrendLabs 2016 Security Roundup. 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 organizations encounter today. Some recent examples are CryptoLocker and CryptoWall.
- **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, due to the fact that 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 paid to unlock it. A common example is Winlocker.

Figure 1 depicts the increase from 2015 to the first half of 2016 in the number of newly added ransomware families (source: Trend Micro TrendLabs 2016 1H Security Roundup).

Figure 1) Increase in ransomware attacks.



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

- E-mail
- 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 are also changing. Examples include the following:

- **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 the 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. In addition, NetApp recommends using a partner organization for help establishing the architecture. The remainder of this report focuses on the following recommendations and solutions for ransomware that are 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 Snapshot copies to identify the point of infection so that you can use preinfected Snapshot copies for remediation.

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. A few examples follow:

- Some solutions provide software that helps with monitoring that tracks user behaviors and interactions with data, including how and when they access files. Using this type of information, these solutions provide proactive monitoring tools and dashboards for alerting and intelligence. These tools notify administrator and operators of potential rogue activities, such as when a user accesses known bad sites or encrypts files. In addition, some solutions provide preventive and actionable measures with 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 an industry best practice for ransomware remediation. An organization has two options after it 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 recovery point objectives (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 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
- .crypt
- .R16M01D05
- .pzdc

- .good
- .LOL!
- .OMG!
- .RDM
- .RRK
- .encryptedRSA
- .crjoker
- .EnCiPhErEd
- .LeChiffre

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 site.

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 allow for point-in-time copies that protect data with no performance effect and minimal storage space consumption. A Snapshot copy is a point-in-time file-system image. Snapshot technology 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 or data activity or function. Moreover, Snapshot copies are read-only files stored within the NetApp solution. For more information about NetApp Snapshot technologies, 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 the 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, 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 SnapVault® solutions, which all 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 from or write to a file. This indicates the last time the file was accessed.
- **ctime.** This output represents the time of the last size or status change. This indicates the last time the file's inode was modified.

- **mtime.** This output represents the time of the last write to a file. This indicates the last time the file was modified.

Note: The Snapshot autodelete function is a volume-level option that allows administrators to define a policy that automatically deletes Snapshot copies based on a configurable threshold. The Snapshot autodelete function can evade or undermine the remediative action of Snapshot-copy use for ransomware depending on additional variables such as the autodelete policy configuration and volume use and capacity. In such cases, the Snapshot autodelete function and configuration could delete Snapshot copies too aggressively, effectively removing the data protection remediation that Snapshot copies provide.

Case Study: Kroll Ontrack

If, during the remediation process, all the preencryption Snapshot copies have been lost, customers 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.

3 Conclusion

It is very clear that ransomware, much like the 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 NetApp Snapshot technology provides the industry's best solution for ransomware remediation.

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.

Copyright Information

Trademark Information