E-BOOK

Why you can’t prevent ransomware

NetApp

Contents

Given the number of high-profile ransomware attacks in recent years and the grave consequences of an attack, you might think prevention methods would have stamped out ransomware entirely.

Consider the once ubiquitous threat of exploit kits, such as the infamous Angler, a massive headache for any security team at the time. These exploit kits have all but faded from memory thanks to relentless efforts to eliminate them.

But ransomware — typically sent through email attachments, malicious URLs, insecure Remote Desktop Protocols, or malicious advertising ("malvertising") — is still everywhere, and total prevention is effectively impossible.

Let's count down the reasons why.

5

It pays

Attackers are more motivated than ever because successful attacks offer huge payoffs. The average ransom paid by organizations in the United States, Canada, and Europe increased from $115,123 in 2019 to $312,493 in 2020 — a 171% year-over-year increase. The average payoff for the first fiscal quarter of 2021 came in at $850,000. With numbers like these, it's easy to see why ransomware continues to be a favorite criminal endeavor. In fact, since 2019, ransomware-related incidents have increased by 65%. The attack frequency will continue to grow; instead of an assault every 11 seconds, it's estimated that one will occur every two seconds by 2031.

Meanwhile, although law enforcement agencies advise against it, organizations keep paying the ransom. It's natural for companies to want to protect their data, and since the negative business impact of an attack often eclipses the ransom itself, paying up often seems the most cost-effective option.

4

It’s cheap

From the point of view of a cybercriminal, the costs of running a ransomware campaign are low. Today, an attacker can buy a prefab ransomware kit that contains everything needed to deploy and monetize an attack, including encryption services, the payload dropper, and obfuscation tools. A typical ransomware-as-a-service (RaaS) subscription starts at a little over $100 per month. More complex and powerful variants can cost thousands, but the payoff potential increases accordingly. Support plans are also included to ensure that attackers can extract the maximum value from the service.

3

It’s effective

Ransomware is a profitable business. Forget the stereotype of hoodie-wearing malefactors in dark rooms; this is a sophisticated enterprise comparable to any corporate partner program. One of the latest examples of RaaS is DarkSide, which was first identified at the beginning of August 2020 and moved to a RaaS distribution model by November. Based on incidents reported, the typical demand is between $200,000 and $2 million for keys to unlock your data.
Not only are DarkSide ransomware operators getting large paydays, but they’re also positioning themselves as “Robin Hoods”: taking money from large, profitable corporations and even making charitable donations from the proceeds. Reports indicate that at least 90 organizations have been victimized by DarkSide to date.
In total, more than 2TB of stolen data is currently being hosted on DarkSide sites, further demonstrating another incentive to pay up.

2

It delivers a rapid ROI

Another reason ransomware is so attractive is that once it infiltrates an organization — it moves fast. It scans the network to locate files, then encrypts the content and demands a ransom. Unfortunately, once the encryption process is underway, there's little that can undo it. And in an alarming new development, attackers are now able to steal data before encrypting it. In May 2021, Colonial Pipeline, supplier of 45% of the fuel for the U.S. East Coast, was hit with a ransomware attack. The attack was carried out by DarkSide or an affiliate. Besides locking Colonial Pipeline's computer systems, DarkSide stole more than 100GB of corporate data. In other words, the company was doubly extorted. The attackers not only demanded money to unlock the affected computers but also payment for the captured data — while threatening to publicly leak the stolen data if the victims didn't pay.

1

People are unreliable

So far, we've covered why ransomware is so pervasive without mentioning how to stop it. Although it's true that many attacks could be prevented by better patching hygiene, there's a big reason that total prevention is impossible: people. Of course, you trust that your employees will never intentionally harm your organization. But ransomware infections still happen because employees are not hyperalert at all times to the dangers of malicious links or email phishing attempts.

Your organization doubtless has some form of mandatory security-awareness training. Education certainly doesn't hurt, but even your most security-aware employees can have a momentary lapse in judgment. And in the absence of highly restrictive security policies that would get in the way of people doing their jobs, one single mistake is all it takes. Detection is needed within seconds, not minutes, hours, or longer.

Zero Trust ransomware protection

If you can’t prevent ransomware, what can you do to protect against it?

Your employees need access to data like ransomware does, so your employees become the attack vector. Policies and roles that restrict access to data can help, but too many of them can inhibit productivity.

The answer is early detection, user behavior analysis, and automated action when suspicious patterns occur. Within seconds.

The NetApp® BlueXP™ protection service offers just this type of detection with the Cloud Secure feature of NetApp Cloud Insights. With Cloud Secure, you can monitor activity, detect anomalies, and automate responses.

Monitor user activity

To accurately identify breaches, every user activity across on-premises and hybrid cloud environments is captured and analyzed. The data is collected using a lightweight, stateless data collector agent installed on a VM in your environment. This data also includes user data from Active Directory and LDAP servers and user file activity from NetApp ONTAP® storage, either in your data centers or the cloud.

Cloud Secure detects anomalies in user behavior by building a model for each user. From that model, it finds sketchy activity changes and analyzes those patterns to determine whether the threat is ransomware or a malicious user. This behavioral model also reduces false positive noise.

Detect anomalies and identify potential attacks

Today's ransomware and malware are sophisticated, using random extensions and file names, which makes detection by signature-based (blocked list) solutions ineffective. Cloud Secure uses advanced machine learning algorithms to uncover unusual data activity and detect a potential attack. This approach provides dynamic and accurate detection and reduces false detection noise.

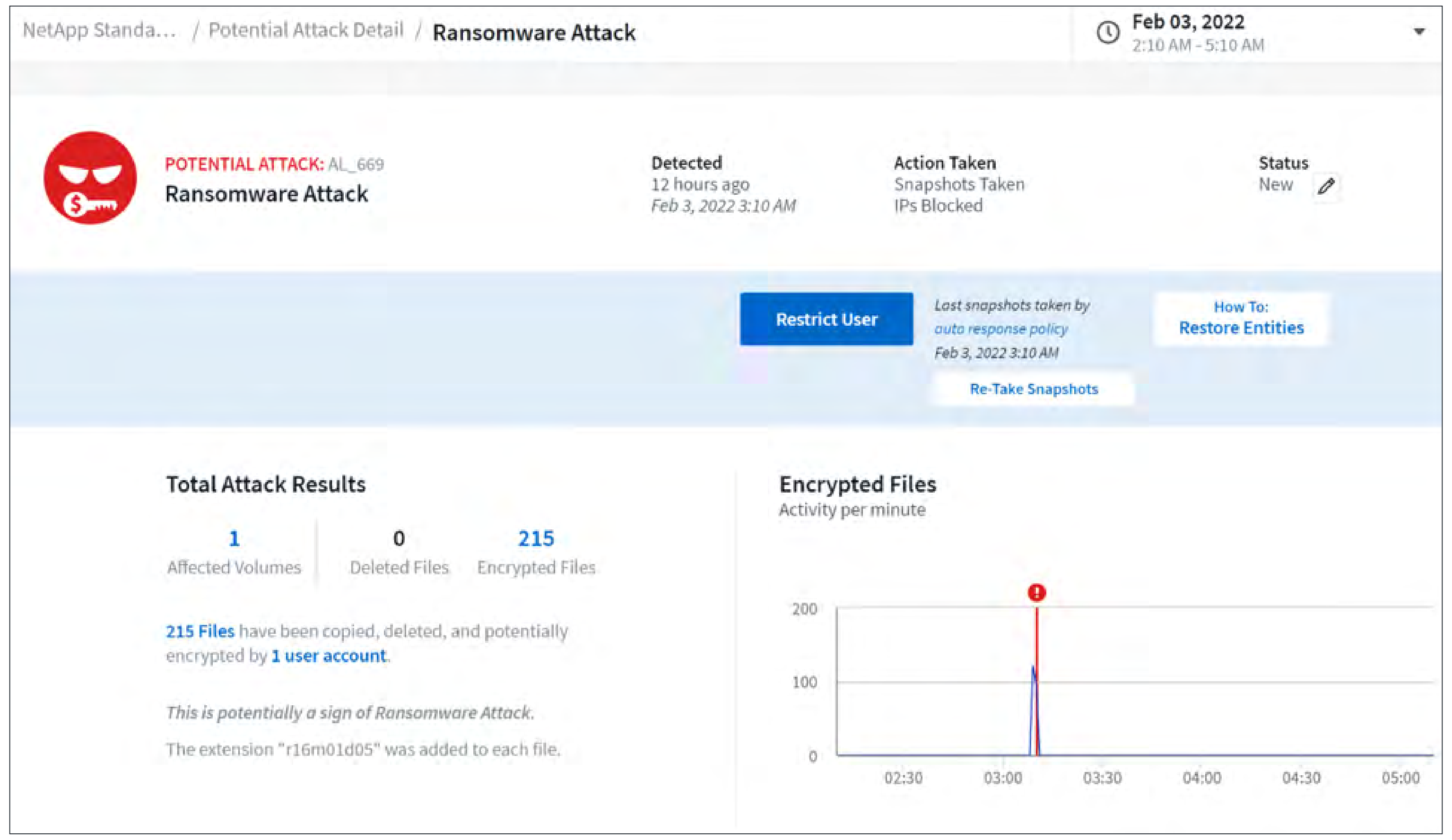
Automate response policies

Cloud Secure alerts you to a potential ransomware attack and provides multiple automatic response policies to protect your data. The service creates a NetApp Snapshot™ copy when it detects unusual behavior and protects your data so you can recover quickly. At the same time, it limits disruption from a false positive.

Cloud Secure restricts a user's ability to access data by either blocking or changing to read-only access:

- When abnormal (read/write) user behavior is detected
- When unusual file deletion behavior is detected

The software also provides detailed access auditing, so administrators can quickly identify compromised data and the source of the attack for quick remediation and recovery.


NetApp Standa... / Potential Attack Detail / Ransomware Attack
Feb 03, 2022
2:10 AM - 5:10 AM

POTENTIAL ATTACK: AL_669
Ransomware Attack

Detected
12 hours ago
Feb 3, 2022 3:10 AM

Action Taken
Snapshots Taken
IPs Blocked

Status
New

Last snapshots taken by auto response policy Feb 3, 2022 3:10 AM

Total Attack Results

1	0	215
Affected Volumes	Deleted Files	Encrypted Files

215 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of Ransomware Attack.

The extension "r16m01d05" was added to each file.

Figure 1) Cloud Secure dashboard showing ransomware attack.

About NetApp

If you're interested in Cloud Insights with Cloud Secure, sign up for a 30-day free trial.

→ **Learn more and start your free trial.**

aws marketplace

AWS Marketplace simplifies software provisioning by combining elastic consumption and contract models with flexible software build and delivery models. Visit NetApp in AWS Marketplace.

About NetApp
In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services, and applications to the right people — anytime, anywhere.

NetApp

+1 877 263 8277