Digital Security
Progress. Protected.

Tech Spotlight

Ransomware Rollback

Chasing Shadows

Unmasking Ransomware Rollback's Shiny Promise

Backups play a vital role in ransomware readiness, and nowadays, many security products include backup functionalities within their endpoint security solutions. Ransomware rollback capabilities are being promoted as a convenient 'undo' option in the event of a ransomware attack. With just a few clicks, victims can seemingly bid farewell to the arduous hours spent on post-attack cleanup and data restoration, effortlessly reverting to a previous, ransomware-free snapshot of their affected environment. But does it truly live up to the silver bullet status that security vendors claim?

What is Ransomware Rollback and How Does it Work?

Ransomware rollback technology involves the regular creation of snapshots, referred to as shadow copies, of the endpoint's disk space. These snapshots can be generated at scheduled intervals or through intelligent monitoring of changes within the system. In the event of a ransomware breach in the endpoint environment, administrators have the option to revert to a previous snapshot using the Volume Shadow Copy Service (VSS), which is native to the Windows environment, or through a proprietary file restoration tool.

Essentially, the production file system undergoes a 'rollback' to an earlier, unencrypted version, erasing all changes made in the interim, including any file encryption modifications imposed by the ransomware attack.

After an attack, business leaders are eager to revert to normal operations with minimal disruption to operational continuity. The advantages of ransomware rollback features in endpoint security are evident: they offer a swift and straightforward method to restore the production environment to a functional state. However, while switching to a security provider that offers rollback features may be enticing, there are several considerations to take into account:

REFERENCES Veeam | MITRE | BlackFrog | NIST

1. Shadow Copies Are the First Source of Attack

In the event of a breach, the hacker's primary objective often involves compromising data backups, which encompasses the deletion of all shadow copies. As outlined in the MITRE ATT&CK framework, several native utilities are leveraged to delete or disable system recovery features, with one of the most prevalent being 'vssadmin.' Despite the allure of ransomware rollback, it is crucial to recognize that its functionality is likely to be rendered inoperable during an ongoing cyberattack.

2. No Solution for Data Exfiltration

The days of straightforward 'pay-to-decrypt' attacks, which simply locked victims out of their data, are mostly behind us. Contemporary attacks have evolved to include data copying and exfiltration, with the intent of using sensitive information as leverage with the threat of publicizing in retaliation for unpaid ransoms. Ransomware rollback features do not address this growing attack trend which is now present in 89% of ransomware incidents.

Securing Against Ransomware

Offense is the Best Defense

In securing against modern attack vectors, it's important not to lose sight of the real goal: keeping malware off the system in the first place. The best defense against ransomware is offense and building a multi-layered security approach with best-of-breed scanning, detection, and response is the winning strategy.

3. Rolling Back Too Soon Can Hinder Recovery

While business leaders may be eager to get operational as quickly as possible after the attack, rolling back too soon may hinder recovery efforts. The NIST Incident Response Guidance for ransomware recovery states that containing the entire attack is the most important goal to ensure that no trace of malware including backdoors, spyware, potentially unwanted applications (PUA), or silent fileless attacks are left behind. Rollback features may offer a false sense of security that can hinder recovery efforts.

Evaluating ransomware solutions? Here's what to look for:

Strong Perimeter Defenses
that focus on keeping malware out with early detection and intelligent scanning

Fast, Automated Threat Response
with incident reporting and quarantining to stop the spread of infection and assist in forensic research

Comprehensive Reporting
To show where vulnerabilities may lie in the network and which types of attacks are most common

User-Friendly Full Disk Encryption
that will secure data against exfiltration attempts while not interfering with everyday activities

Multi-Factor Authentication
To control access to sensitive data

Complete Coverage
that secures all surfaces including endpoints, cloud applications, email, and more.

For more information on ESET Protect solutions including ESET PROTECT Complete, visit: www.eset.com/us/business

LEARN MORE