Ransomware Attacks Are Getting More Sophisticated.

Can your organization confidently meet the threat?

OVERVIEW

Ransomware perpetrators are getting more sophisticated, increasingly targeting organizations with larger extortion demands and highly disruptive attacks that can bring IT and operational systems to a halt. Many organizations have discovered that they lack a resilient defense to maintain control when ransomware strikes.

As CSO.com observed, "Ransomware attacks have matured over the years, adopting more stealthy and sophisticated techniques, while at the same time fixing many of the implementation errors that earlier iterations had." Simply put, trends indicate these attacks are not going away.

"Ransomware actors are getting more skilled and their attacks are getting more complex, more creative, and certainly more targeted toward the enterprise," says Alex Restrepo, Solutions Marketing with Veritas.

Because private companies aren't always legally required to disclose ransomware incidents, the impact of attacks on these businesses is difficult to quantify in terms of cost and prevalence. It's also challenging to confirm how often victims decide to pay the ransom, although it's clear many do, as cybercriminals have continued investing in engineering advanced forms of ransomware.

LOSSES FROM RANSOMWARE ON THE RISE

In an alert issued last October, the FBI Internet Crime Complaint Center (IC3) warned, "Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information."

> "Ransomware actors are getting more skilled and their attacks are getting more complex, more creative, and certainly more targeted toward the enterprise."
>
> ***— Alex Restrepo, Solutions Marketing, Veritas***

Perhaps the most notorious case of ransomware so far was the 2017 NotPetya attack, in which transport giant Maersk had to suspend operations at 17 port terminals, causing huge waiting lines for cargo loading and a logistical nightmare that took months to sort out. It's been estimated the incident cost the company more than $10 billion.

In a report released last August looking at the evolution of ransomware, security firm Malwarebytes noted, "This once dangerous-but-recently-dormant threat has come back to life in a big way, switching from mass consumer campaigns to highly-targeted, artisanal attacks on businesses."

DEVELOPING A SOUND STRATEGY TO PROTECT, DETECT, AND RECOVER DATA

Many organizations have invested in frontline security solutions aimed at preventing ransomware assaults. But with constant changes and updates to system configurations and user access, it's virtually impossible to maintain an impenetrable barrier guaranteed to keep out 100% of assaults.

Criminals have shown they are persistent, constantly probing defenses to identify system weaknesses, and they've proven adept at finding and encrypting any data that can be accessed, including network-accessible backup files.

"Some organizations mistakenly believe ransomware is only going to attack their emails or documents and spreadsheets, and they assume they can just recover those from their backups," Restrepo says. "But ransomware attacks have become extremely good at routing out the interconnected nature of enterprise systems, so even if you have documents in more than one place, that's no guarantee they're safe."

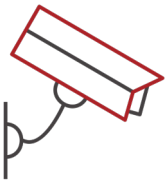
As the CSO.com article reported, "In some documented cases, organizations decided or were forced to pay the ransom because their backups were corrupted or the restoration process would have taken too long."

Although sound backup practices are an important part of recovering from a ransomware attack, they're only part of a comprehensive strategy that should be put into play to effectively defend an organization from falling victim.

When it comes to ransomware, there are many preventive steps organizations can take to contain the threat. Veritas advises adoption of a three-tiered strategy:

1 PROACTIVELY PROTECT DATA.

In addition to having a frontline security solution, implementing hardening measures is essential to protect data integrity. Steps such as maintaining multiple copies of data, including storing copies on air-gapped and immutable storage, provide assurance backups will function when needed.



2 MAINTAIN AWARENESS OF DATA AND INFRASTRUCTURE.

Detection and mitigation tools and processes can ensure appropriate action is taken in the event of a breach. This requires end-to-end visibility across the IT infrastructure, with monitoring and reporting tools to ensure data is accessed and managed only by trusted parties and changes in data access and baseline data activity are detected and reported.

3 GUARANTEE SWIFT, EFFECTIVE RECOVERY.

Ransomware infecting and corrupting one device can quickly spiral and endanger the entire data center, given today's hybrid multicloud infrastructures. An automated, orchestrated recovery process is required to regain control following an attack, ideally complemented by the ability to rehearse and test.

The Veritas Enterprise Data Services Platform provides a comprehensive set of technologies supporting IT system protection, the detection of anomalous system activity, and certain, strategic recovery in the face of an attack.

For more information on how to maintain control over the enterprise when ransomware strikes, go to www.veritas.com/ransomware.