
# Ransomware:
# Could Have-Would Have-Should Have

## Is Ransomware Back?

Following a notable decline in 2022, Kivu has observed signs of increased activity in Q1 2023. Most of these events result from threat actors targeting older, known vulnerabilities that could have been addressed.

Ransomware incidents lead to stressful times for an organization of any size. Realizing your business has been impacted by a successful ransomware attack can paralyze decision-makers causing long-term pain in the future. Below are some things for your organization to keep in mind.

## Unrecoverable and Destructive Actions

When identifying successful execution of ransomware in your environment, shutting down servers and systems is a common knee-jerk reaction. Often this can cause two significant issues:

1. Destruction of volatile forensic evidence, which may be required for any regulatory notification, insurance reports, and forensic investigation.

2. For any large files, such as a database that have been partially encrypted, shutting down the system may corrupt that database, potentially rendering it unrecoverable.

## Not all Backups are Made Equal

Organizations often assume, *"We have good data backups."* But have you checked? Threat actors often encrypt or delete backup data prior to the main ransomware event. That leaves victims with no ability to restore impacted data.

More importantly, backups created for disaster recovery are not the same as ransomware incident recovery backups. Catastrophic events like floods, earthquakes, or blackouts do not seek out and destroy data backups - but threat actors definitely do. Your adversaries know that if an organization can recover from backups, there goes any chance of them receiving a ransom payment.

If your backups are part of your domain/network, any threat actor with administrative domain credentials usually will encrypt backups as part of their standard tactics. If you have a third-party backup solution administered from your corporate network, threat actors will look for credentials to that backup by targeting IT Administrators. In multiple cases, Kivu found threat actors had deleted backups when credentials cached in browsers or sessions were still established to the third-party backup solution.

## Building Cyber Resilience

How can you prepare for the threat? Organizations can immediately take steps to avoid mistakes that make them an easy target:

1. Implement 24x7 endpoint detection and response technology, using the necessary resources to deploy and configure the software correctly that will protect all Internet-facing devices.

2. Create viable backups that will escape being encrypted and destroyed:

- If you have on-site backups, ensure they are access-controlled and only accessible from within your environment, and monitor and limit who has access to the data.
- Alongside on-site backups, implement offline backups and off-site backups.
- Use the 3-2-1 principle for your backup strategy. Backup data should be kept separate from your domain, network, and production service providers. Ensure these backups are immutable, are not administered from your operational network, and are only accessed by a limited number of personnel, and provide alerts if the data is accessed and/or deleted.
- Ensure the technology you are using to back up your "company crown jewels" and other business-critical data is fit for purpose, regularly tested, and accessible at any point in time.

3. During the incident, even as recovery is underway, preserve forensic evidence from being wiped to aid in the identification of the root cause of the incident.

4. Do not underestimate the preparedness needed for a time of crisis. Practice a fit-for-purpose, tried and tested cybersecurity incident response plan that organizes how you respond and accounts for what resources you will need. Develop the organization's cyber incident response support team by using the expertise of third-party vendors, including but not limited to outside legal counsel, crisis communications advisors, IR containment and recovery expertise, expert threat actor negotiators, forensics investigators, and IT vendors. This plan should be developed in coordination with legal counsel so that the organization can best assert any applicable claim of privilege in later litigation.

When considering the last step of incident response plans, the road to maturity is simple:

- If you do not have a cyber incident response plan - ***build it.***
- If you do have a cyber incident response plan - ***test it.***
- If you lack experts on retainer to provide the support - ***find them.***

## Closing

Companies struggling to understand how to create or test an incident response plan can engage with experts to review their current state of maturity. By doing so, organizations will practice thorough simulated exercises, understand the decisions they face during a cyber incident, invest in the right resources, and build their support network. Ultimately, you may save your business millions of dollars.

Most importantly, do not wait – act now.

*Kivu is a leading global cybersecurity firm dedicated to offering best-in-class cybersecurity services. Since 2009, Kivu has been providing a full suite of services covering the entire incident lifecycle, specializing in the forensic response to cyberattacks and ransomware incidents.*

Contact us to learn more at
info@kivuconsulting.com

# We Fight Cybercrime.

## *We Protect Humanity.*

If you are experiencing a suspected active data incident, contact us at
**incidentresponse@kivuconsulting.com** or call
**+1 855.548.8767 (United States)** or **+44 203.997.8334 (Europe).**

KIVU