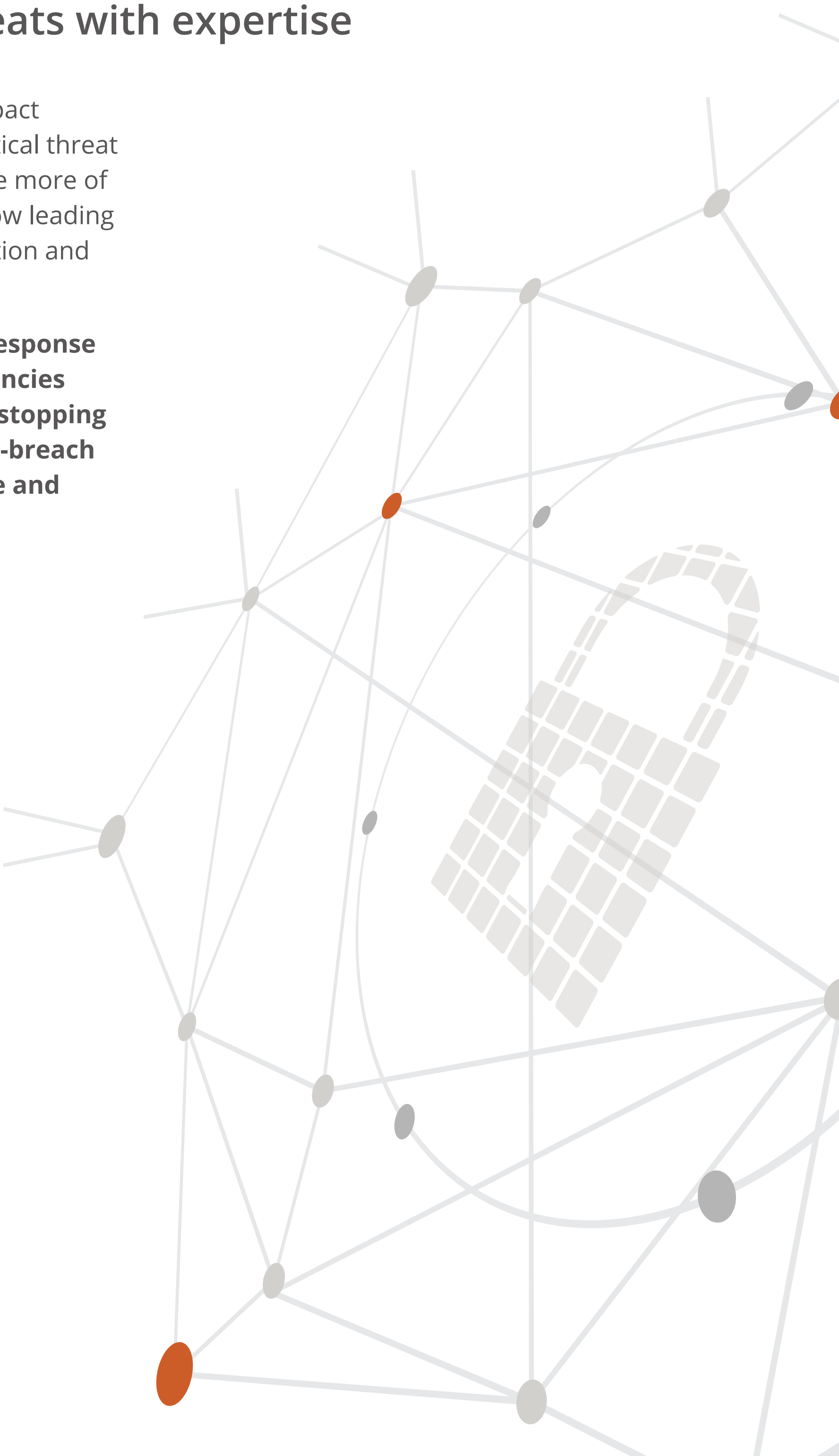
KIVU

Kivu’s Ransomware Incident Response

Countering ransomware threats with expertise

As attacks become more frequent and their impact increasingly severe, ransomware is posing a critical threat to organizations of all sizes and industries. Once more of a nuisance, these cyber extortion attacks are now leading to serious financial loss from business interruption and causing substantial reputational harm.

Kivu is a recognized expert in ransomware response and works closely with law enforcement agencies around the world to support their efforts in stopping cyber-crime. Our incident response and post-breach remediation services are tailored to mitigate and remediate ransomware attacks.



RANSOMWARE IN ACTION

STEP 1 • POINT OF ENTRY

Phishing emails and open remote desktop (RDP) ports are the most common attack vectors. Phishing emails can include attachments containing ransomware or other malware to facilitate later attacks. Threat actors can also use stolen credentials from the dark web or brute force access through unsecured RDP.

STEP 2 • PRIVILEGE ESCALATION

Once on a network, threat actors need to gain access to an administrator level account. With admin credentials harvested from the affected system they can now freely execute any program, change settings and move through a network.

STEP 3 • RECONNAISSANCE & PREPARATION

Threat actors now start reconnaissance, either by using network scanners, collecting operating system information, monitoring processes or installing backdoors. They may also disable antivirus and other security programs.

STEP 4 • LATERAL MOVEMENT & ENCRYPTION

Next, threat actors need to distribute ransomware across other devices in the network. Some ransomware variants delete backups and volume shadow copies before starting encryption, others simply encrypt everything. Once encryption is completed, most threat actors leave the network.

STEP 5 • DISCOVERY AND RECOVERY

Most ransomware attacks are noticed within 24 hours. Victims will find their network, email and/or website inaccessible, and a ransom note. If backups are not available, obtaining a decryption tool is usually the first step toward data recovery. Paying a ransom is always the last resort, but sometimes it is the only option.

What Makes Ransomware So Dangerous?

- ⚠ It encrypts an organization’s systems and can interrupt business operations across an entire global network.
- ⚠ It can delete or encrypt back-ups, leaving victims with no alternatives to ransom payment.
- ⚠ It may include data exfiltration, resulting in the double-risk of business interruption and data theft.
- ⚠ Ransomware attack vectors are continuously evolving, requiring organizations to constantly adapt their defences and employee training.
- ⚠ It can mask a secondary attack. Often a ransomware attack serves to hide other malware installed in the victim’s network, which launches once the primary attack is mitigated.

Data Exfiltration

Threat actors are increasingly including data exfiltration in their ransomware exploits, further damaging victim organizations.

Our Process

1

Our analysts assess whether backups or other means of data recovery exist. We then determine whether the victim can safely refuse ransom payment, or whether payment provides a faster, more cost effective and complete restoration of data.

2

We investigate whether data was stolen and, if so, identify the extent of the exfiltration, working with the client to ensure they adhere to data breach notification requirements.

3

Kivu's trained responders will anonymously reach out to attackers and begin negotiations, in many cases reducing ransoms significantly from the initial demand.

4

In cases where the client decides to pay the cryptocurrency ransom, we will provide a Sanctions Report outlining Kivu's due diligence on the attacker and confirming our compliance with relevant legislation.

5

We will work with the client and attacker to ensure "proof-of-life" and confirm that any provided decryption tool functions as intended.

6

Our in-house post-breach remediation team can work with clients to recover data and restore their systems in the aftermath of the attack.

Our Expertise

Kivu staff bring criminal investigations experience from a variety of backgrounds, including the military, police and other law enforcement agencies.

Our analysts have first-hand experience of shifting ransomware trends and different threat actors as we closely follow their movements on the Dark Web.

Kivu's regulatory compliance and due diligence process is the industry gold standard – we take the greatest precautions to ensure our actions are tracked and lawful.

Kivu is registered with the U.S. Financial Crimes Enforcement Network (FinCEN) as a Money Service Business (MSB). This allows us to provide the highest degree of regulatory compliance if paying a ransom on a client's behalf.

As a U.S.-registered MSB, we file Suspicious Activities Reports (SAR) with US Treasury FinCEN without identifying clients by name.

Exclusive Threat Intel
Kivu conducts in-depth research into ransomware trends and cyber security threats, which we share with law enforcement and publish as Threat Intelligence reports for our clients and insurance partners.

Why Kivu?

From data protection and incident response to post-breach remediation and endpoint monitoring, Kivu is dedicated to offering best-in-class cyber security services to organizations worldwide.

We are proud to offer:

FAST RESPONSE

Practical logistics and quick action mean we schedule scoping calls within the first hour and can deploy on-site within 24 hours

TAILORED SERVICE

Kivu has the largest dedicated in-house Post Breach Remediation team in the industry

EXPERIENCED RESPONDERS

Kivu's highly certified analysts and project managers have handled over 700 ransomware cases, and have backgrounds in the military, police, tech multinationals and government bodies

We are:

TRULY LOCAL

Kivu has North American and European capacity, with offices and qualified responders on both sides of the Atlantic. We respond to events worldwide through our global partner network

DEDICATED INSURANCE PARTNERS

Kivu is a long-time partner to the insurance industry and found on most cyber vendor panels. We work closely with claims adjusters and breach coaches, which gives us a deep understanding of insurance pain points

About Kivu

Kivu is a leading global cyber security firm that offers a full suite of pre- and post-breach services, specializing in the forensic response to cyber-attacks and ransomware incidents. We deliver cutting edge cyber security solutions to organizations in need and are a trusted cyber incident partner to insurance carriers and law firms worldwide.

KIVUCONSULTING.COM

CONTACT US

Our purpose is to restore freedom of operation and to minimize business interruption, getting organizations back online quickly and securely, regardless of the nature of the incident. Contact us to learn more at **info@kivuconsulting.com**