Kivu

Microsoft 365 Investigations at Kivu

A new and improved 24-hour service for victims of Business Email Compromise.

Attackers are always trying to gain unauthorized access to business email accounts to commit either identity, employee payroll, or financial fraud. This poses a risk not only to the affected business, but also to their clients and partners, in fact anyone with whom employees have communicated via email.

Business Email Compromise (BEC) affects organizations across all sectors and industries. In fact, instances of BEC have increased as more organizations adopt cloud-based email systems such as Microsoft 365.

Kivu's Improved Microsoft 365 Investigations Service

Kivu's new Microsoft 365 incident service provides a comprehensive BEC incident analysis that identifies the extent of the BEC compromise, data accessed, malicious rules which may have been initiated and, in most cases, emails synced by the attacker across all email accounts.

Kivu's analysis can be completed within 24 hours of receiving Microsoft 365 credentials from the client.

Most Microsoft 365 analysis takes 3 to 5 days due to the number of accounts typically affected and the forensic analysis required to provide insight. **Kivu has developed a process that combines automation with analyst insight to cut this time down to 24 hours.**

Kivu

Service Overview

Kivu's Microsoft 365 investigation will:

- Complete due diligence Microsoft 365 account analysis on all user accounts (up to 2,000)
- Run a detailed analysis on up to five compromised accounts
- Identify compromised accounts
- Provide a detailed report of the findings

Service Delivery

The **Microsoft 365 Investigation** service is available for a fixed cost of $6,000 ($7,500 CAD | £5,000 GBP).

PHASE ONE

Microsoft Office 365 – Due Diligence Analysis

Search for Indicators of Compromise on up to 2,000 User Accounts

PHASE TWO

Detailed Analysis of up to five Microsoft 365 User Accounts

- Review account configuration.
- Identify/preserve the phishing email that caused the account compromise.
- Identify unauthorized user activity in common applications and directories.
- Identify unauthorized mailbox rules/forwarding of email messages.
- Conduct a Message Trace when necessary.
- Export/Preserve PST file of compromised mailbox.

PHASE THREE

Reporting

Searchable Multi-tab Timeline

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

Business Email Compromise can have serious repercussions for any business. Speak to our incident response experts today to find out how Kivu can help mitigate a BEC incident.

info@kivuconsulting.com