5 Hidden Signs of Ransomware Attack

Swipe to discover what most teams miss

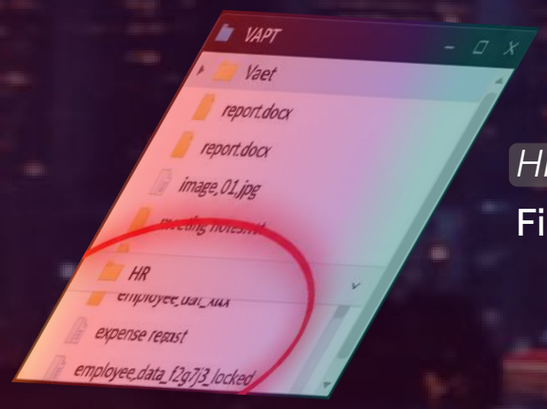
CREST. Accredited

certin Empanelled

sales@briskinfosec.com

Unusual File Renames in Unimportant Folders

Attackers test encryption on low-value folders first like `/temp`, `/downloads`, or shared drives. A few renamed files with random extensions quietly appear before mass encryption starts.



`HR_Shared/2024 Reports/Report1.xlsx.locked`

File modified 2 mins ago by “UnknownUser123”

CREST Accredited

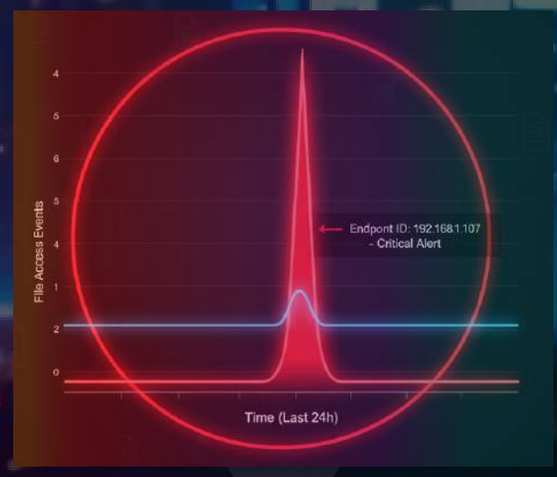
certin Empanelled

sales@briskinfosec.com

Unusual File Access Spikes from One Endpoint

Ransomware crawls the network rapidly, reading and writing thousands of files per minute. A single endpoint showing massive I/O activity = early-stage encryption in motion.

User: Mark-PC accessed 2,746 files in 4 minutes
no business reason logged.



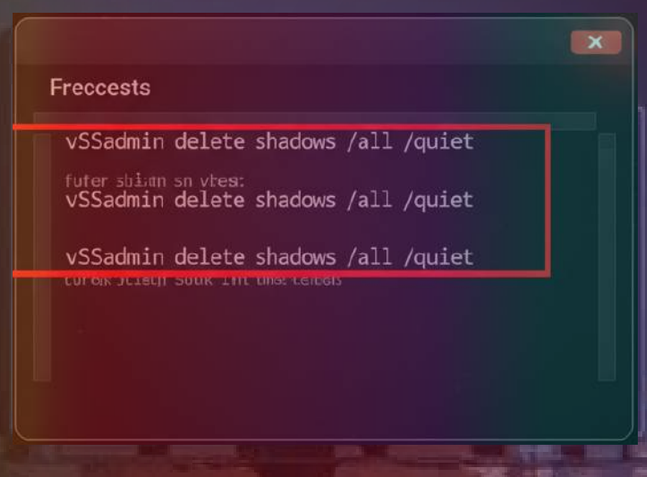
CREST Accredited
certin Empanelled

sales@briskinfosec.com

Disabled Shadow Copies or Backups Without Requests

Ransomware kills your lifelines first. They execute PowerShell commands like `vssadmin delete shadows /all /quiet` If your shadow copies disappear without IT approval, it's not maintenance. It's malice.

Backup schedule shows "Disabled" no change request from any admin.



CREST. Accredited

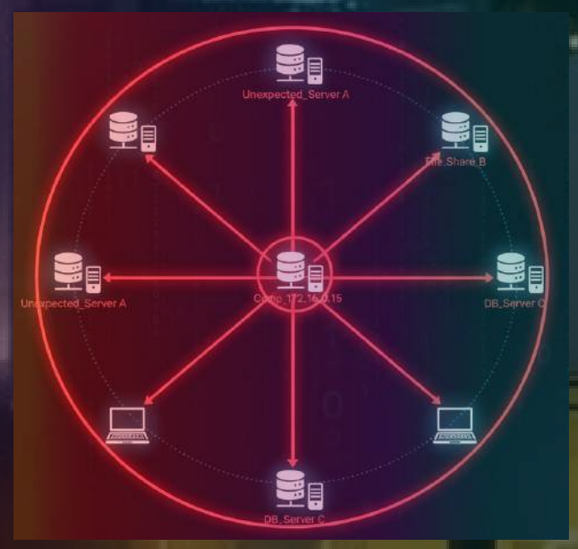
certin Empanelled

sales@briskinfosec.com

Suspicious Lateral Movement (SMB or PowerShell)

Attackers move laterally to reach domain controllers and servers before detonation. Look for strange authentication attempts between systems that never interacted before.

User: HR01 suddenly authenticates to *Finance-Server01* via SMB, first time ever.



CREST. Accredited

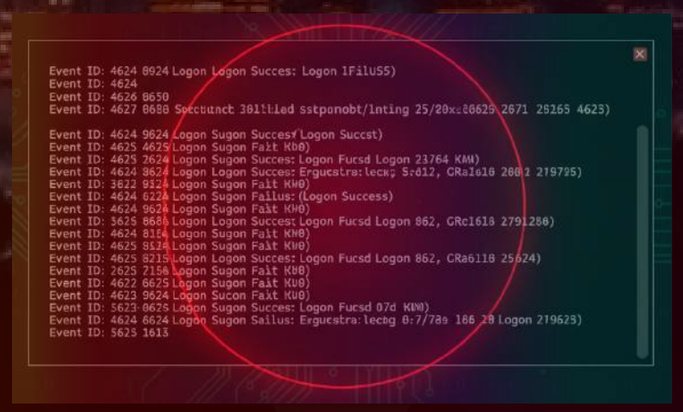
certin Empanelled

sales@briskinfosec.com

Surge in Login Events (4624/4625 IDs)

A flood of login attempts, successful (4624) and failed (4625), signals brute-force or credential-stuffing. It’s how attackers escalate before encrypting.

50 failed logins for the same admin account within 3 minutes from unknown IPs.



CREST. Accredited

certin Empanelled

sales@briskinfosec.com

By the time encryption starts, it’s too late to defend.

Train your team to detect behavior, not just alerts.

Ransomware Readiness Audit

Uncover your early warning gaps before attackers do

BOOK A MEETING

CREST Accredited

certin Empanelled

sales@briskinfosec.com