TALES FROM THE SOC

RANSOMWARE · HIGH PRIORITY

# Rapid Detection and Containment of a Qilin Ransomware Attack

## Incident Overview

**Threat Type**: Qilin ransomware — a sophisticated, hands-on-keyboard attack that encrypted 45 systems across a retail organization while simultaneously destroying backup infrastructure.

**Time to Containment**: 7 minutes from detection to device isolation and C2 severance.

**Attack Characteristics**: The attacker gained initial access through exposed backup servers with weak credentials and operated undetected for nearly three weeks. During that dwell period, they dumped Domain Controller credentials, compromised service and machine accounts, and methodically targeted backup infrastructure. On July 2, 2026, they executed mass ransomware deployment in three coordinated waves, using a compromised backup service account to write Qilin payloads over SMB to 45 devices simultaneously. When domain accounts were disabled, the attacker re-entered through a locally planted backdoor account — evidence of deliberate pre-planned persistence.

## Detection & Escalation

**Detection**: Microsoft Defender for Endpoint alerts fired across multiple hosts. Critical Start SOC analysts correlated signals across 58 systems, confirmed active hands-on-keyboard attacker behavior, and identified three distinct staging IPs simultaneously deploying ransomware in coordinated waves.

**SOC Escalation**: High priority. With an active attacker still conducting lateral movement, destroying Veeam backup repositories, and encrypting systems in real time, analysts immediately initiated device isolation and C2 severance across all identified hosts — working the customer call tree concurrently with containment actions.

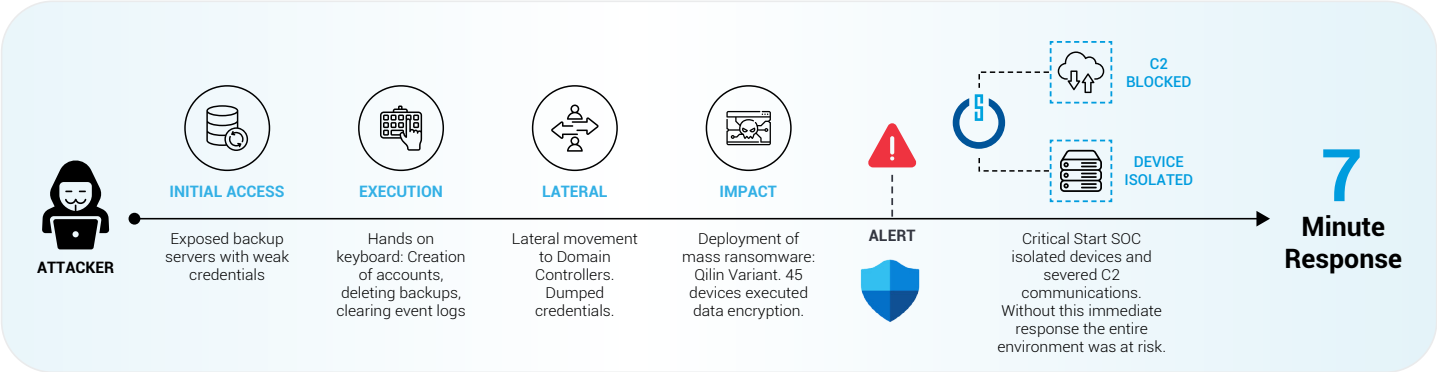
## Depth of Investigation

The Critical Start SOC reconstructed a three-week attack timeline to map every compromise point and deliver precise remediation guidance. Analysts traced the dwell period back to June 17, 2026, when a Veeam service account was first abused — the earliest indicator of compromise. Over the following days, the attacker used multiple compromised accounts to enumerate the environment, probe Active Directory Federation Services, and conduct daily scripted reconnaissance from attacker-controlled infrastructure.

Beginning June 30, the attacker pivoted to backup destruction — deleting Veeam repositories and positioning a compromised backup service account as the primary encryption weapon. The SOC identified three distinct attacker staging IPs and traced all three encryption waves to this single account, which held broad administrative rights across the environment. A locally planted backdoor account enabled re-entry after domain account disables, demonstrating that the attacker had planned for this contingency.

Analysts documented 13 compromised accounts requiring immediate disable and audit, six attacker staging IPs, and 58 affected hosts across three tiers: encrypted (45), hands-on-keyboard (2), and recon-touched (11). This tiered host register gave the customer's incident response team the precision to act decisively without a full environment rebuild.

## Attack Sequence




## Outcome

The Critical Start SOC isolated affected hosts and severed attacker command-and-control communications within 7 minutes — stopping the active encryption campaign and preventing complete backup destruction. Without immediate containment, the entire environment and all recovery capability were at risk of permanent loss. The SOC's detailed attack timeline, tiered host register, and account inventory gave the customer's incident response team the clarity to act decisively and recover with confidence.