New Kid on the Cloud: Crimson Collective's Rapid Rise

C-Suite level threat review by applicable business area addressing active threats.

This month, attention turns to Crimson Collective, a new hacking group making itself known worldwide. Their operations highlight the use of legitimate cloud credentials to access, copy, and exfiltrate sensitive data without triggering endpoint defenses. Understanding the group's tactics is critical for organizations aiming to stay ahead of evolving cloud-based threats.

Crimson Collective:

Crimson Collective emerged in September 2025 and has already claimed high-profile attacks against a Red Hat Consulting GitLab instance and the AWS Cloud Environment. There are also alleged claims involving Nintendo and Colombia's state lottery. The group is suspected of collaborating with other major actors, such as the Trinity of Chaos (Scattered Lapsus$ Hunters), bringing them up the ranking from the "new kid on the block" to a high-profile player in the threat landscape.

Crimson Collective

Threat Level: Medium

Attack:

Crimson Collective's playbook focuses on using leaked long-term cloud credentials (often discovered with tools like TruffleHog) to sign in as legitimate users (MITRE T1078.004). The group ignores low-privilege accounts, concentrating only on those that provide the access needed for their operations. Once inside, they create new accounts and attach AWS polices such as 'AdministratorAccess', which allows them to establish persistence and elevate privileges (MITRE T1136.003). As part of their discovery process, the group maps the environment and locates where valuable data is stored (MITRE 1087). Once valuable data is found, their data collection focuses on managed databases and cloud object stores. In AWS, these typically include the Relational Database Service (RDS), Elastic Block Store (EBS), and Simple Storage Service (S3), which are used in different ways to store data, system snapshots, and large file repositories. Crimson Collective takes database and disk snapshots, exports stored objects for offline access, and monetizes it through extortion (MITRE T1530, T1567).

Remediation:

- Regularly rotate and disable long-term AWS access keys.
- Implement alerts for new user creation and privilege escalation.
- Enforce the principle of least privilege across all cloud accounts.

Looking Ahead:

Our next newsletter edition will feature more than just monthly threat briefings. Each edition will now feature recent cyber trends, threat intelligence insights, and updates from our consulting team in action. Also, since not all news in cybersecurity is bad, we'll highlight positive developments that are moving the field forward!

.

Crimson Collective:

- **Crimson Collective Tactics on the AWS Cloud Environment:** https://www.rapid7.com/blog/post/tr-crimson-collective-a-new-threat-group-observed-operating-in-the-cloud/
- **Crimson Collective attack on RedHat:** https://www.bleepingcomputer.com/news/security/red-hat-confirms-security-incident-after-hackers-breach-gitlab-instance/

How K logix Can Help

Technology Advisory

- Email Security
- Endpoint Detection and Response (EDR)
- Identity and Access Management (IAM)
- Managed Security Service Provider (MSSP)
- Security Information and Event Management (SIEM)
- Cloud Security Posture Management (CSPM)
- SaaS Security Posture Management (SaaS)

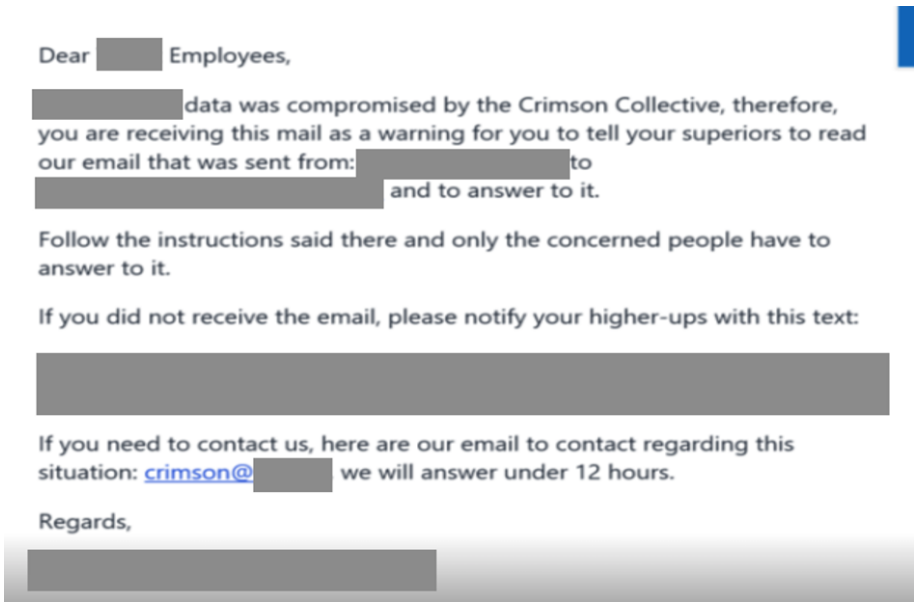
Program Advisory

- Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
- Cloud Security Maturity
- Identity and Access Management Program Maturity

Threat Intelligence

- Notification to customers of threats
- On-demand briefings
- Threat exposure workshops
- User awareness training seminars
- Monthly and quarterly threat intelligence reports

Crimson Collective Note:



Dear [redacted] Employees,

[redacted] data was compromised by the Crimson Collective, therefore, you are receiving this mail as a warning for you to tell your superiors to read our email that was sent from: [redacted] to [redacted] and to answer to it.

Follow the instructions said there and only the concerned people have to answer to it.

If you did not receive the email, please notify your higher-ups with this text:

[redacted]

If you need to contact us, here are our email to contact regarding this situation: crimson@[redacted] we will answer under 12 hours.

Regards,

[redacted]