16 October 2025

INTEL471

EMERGING THREATS

Crimson Collective

Crimson Collective is an emerging cyber threat group that has recently focused on cloud environments, particularly targeting AWS instances, cloud-based GitLab deployments, and other critical enterprise cloud infrastructure. Their observed activity indicates that the group has evolved from opportunistic attacks into highly targeted campaigns leveraging stolen credentials, misconfigured cloud resources, and supply chain access to infiltrate enterprise networks. Over the past few months, the collective has been linked to data exfiltration incidents impacting organizations in North America, Europe, and Asia, including high-value technology and software development sectors. High profile victims such as Nintendo have been allegedly targeted for example. The group's operations allow attackers to gain unauthorized access to sensitive source code repositories, cloud storage, and internal documentation, enabling both financial extortion and strategic theft of intellectual property. These campaigns have led to significant operational disruption, reputational damage, and potential compliance violations for affected organizations.

THREAT SUMMARY

Crimson Collective is an emerging cyber threat group that has recently focused on cloud environments, particularly targeting AWS instances, cloud-based GitLab deployments, and other critical enterprise cloud infrastructure. Their observed activity indicates that the group has evolved from opportunistic attacks into highly targeted campaigns leveraging stolen credentials, misconfigured cloud resources, and supply chain access to infiltrate enterprise networks. Over the past few months, the collective has been linked to data exfiltration incidents impacting organizations in North America, Europe, and Asia, including high-value technology and software development sectors. High profile victims such as Nintendo have been allegedly targeted for example. The group's operations allow attackers to gain unauthorized access to sensitive source code repositories, cloud storage, and internal documentation, enabling both financial extortion and strategic theft of intellectual property. These campaigns have led to significant operational disruption, reputational damage, and potential compliance violations for affected organizations.

Their evolution demonstrates an increasing sophistication in cloud-focused attacks, combining traditional credential compromise with automated scripts to enumerate exposed resources and deploy malware or backdoors in high-value environments. Crimson Collective's campaigns are designed to maximize the reach of a single compromised account, often leveraging the trust inherent in cloud platforms to bypass traditional perimeter defenses. By exploiting cloud-native orchestration and repository tools, the group can escalate privileges, pivot across services, and maintain persistent access while exfiltrating sensitive data over extended periods. The combined effect of these operations significantly magnifies the risk to organizations that rely heavily on cloud infrastructure for critical operations.

TITAN References:

- Info Report: Crimson Collective hacking group members claim to compromise US-based Red Hat software provider – https://titan.intel471.com/report/inforep/2c5f562c5d8a13ec2eaa13f790615a96
- Spot Report: 10 Oct 2025 – https://titan.intel471.com/report/spotrep/d7a18c567937b702ae61635f5221da0a
- Spot Report: 13 Oct 2025 – https://titan.intel471.com/report/spotrep/0fc33fc4f48a7bc41173a4513ee3cdfd

SYNOPSIS

Crimson Collective typically gains initial access through compromised credentials, exposed VPNs, or cloud misconfigurations that allow the attacker to authenticate to enterprise cloud platforms without triggering standard alerting mechanisms. Once inside, the group enumerates cloud resources using native platform APIs and automated scripts, identifying repositories, storage buckets, and infrastructure components that store sensitive data or secrets. In GitLab environments, they have also been observed leveraging administrative and developer credentials to clone repositories, inject malicious CI/CD workflows, and maintain backdoor access through pipeline configurations. On AWS, the attackers scan for IAM roles, exposed keys, and misconfigured S3 buckets to extract sensitive files and credentials.

After initial access and enumeration is achieved, Crimson Collective deploys post-compromise tooling to maintain persistence and facilitate lateral movement within the cloud tenant. This includes uploading custom scripts or agents to automate data exfiltration, monitoring account activity, and potentially escalating privileges by exploiting excessive IAM permissions or misconfigured security policies. The group also stages stolen data for exfiltration to attacker-controlled servers, allowing them to conduct both financial extortion and intellectual property theft. Their technical operations emphasize stealth, leveraging cloud-native functions and automation to minimize detection while maximizing the breadth of compromised assets. The combination of credential abuse, repository compromise, and cloud service manipulation highlights the advanced operational capabilities of Crimson Collective, making them a critical threat to organizations with cloud-dependent infrastructures.

CRIMSON COLLECTIVE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('84ee0d6e-42d2-4279-8099-f79bd369287b'),touched:!t)

RELATED HUNT PACKAGES

AWS RELATIONAL DATABASE SERVICE (RDS) DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/d152f447-91e1-456e-a0ef-87c3321fbee7

AWS NETWORK LEVEL INFORMATION DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/e41df558-8ce7-4952-8887-9a8e9e1e50e6

AWS ELASTIC COMPUTE CLOUD (EC2) DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/5ea5cb26-1c98-4121-aa62-8296cb2fc8a3

AWS GENERAL DISCOVERY ACTIVITY

https://hunter.cyborgsecurity.io/research/hunt-package/e58d5a8d-1b7a-42f7-97b4-e750ea97027c

AWS MESSAGING DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/da782f3c-2c50-47ae-9c8c-be8b878e4711

AWS SIMPLE STORAGE SERVICE (S3) DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/85ca18f7-8354-4f64-9b6a-db85d70097b9

AWS APPLICATION DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/143db723-f0e3-490f-8f21-a496a3782c7e

AWS MONITORING AND ALERT DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/1a63ed72-b9bc-4339-a7bd-89a961ebac97

AWS ELASTIC BLOCK STORE (EBS) DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/c1df38bc-0933-40f1-8c6e-5a18ed3fcc18

AWS IDENTITY AND ACCESS MANAGEMENT (IAM) DISCOVERY

https://hunter.cyborgsecurity.io/research/hunt-package/fcdafb78-7ac3-4b83-bbb4-cd182408e6eb

MITRE CONTEXT

- MITRE Tactic Names:
    - Discovery
- MITRE Technique Names:
    - Cloud Infrastructure Discovery
    - Cloud Storage Object Discovery
    - Cloud Service Discovery
    - Cloud Account
- MITRE Technique IDs:
    - T1526
    - T1087.004
    - T1619
    - T1580

REFERENCES

1. https://www.rapid7.com/blog/post/tr-crimson-collective-a-new-threat-group-observed-operating-in-the-cloud/
2. https://www.bleepingcomputer.com/news/security/crimson-collective-hackers-target-aws-cloud-instances-for-data-theft/
3. https://www.bleepingcomputer.com/news/security/red-hat-confirms-security-incident-after-hackers-breach-gitlab-instance/