Keys to the (SaaS) kingdom

By Jennifer Ring

Published: 2025-05-29 · Archived: 2026-04-05 13:39:27 UTC

Published by Digital Forensics and Incident Response (DFIR) and Cyber Intelligence on 29 May 2025

Primary author: Tony Mau, DFIR

In May 2025, the CyberCX Digital Forensics and Incident Response (**DFIR**) team was engaged to investigate an incident in which the threat actor performed a domain registration hijacking attack through social engineering to verify themselves as legitimate domain owners to the domain registrar to take control of an organisation's domain.

During the investigation, the CyberCX DFIR and CyberCX Intelligence teams became aware of a campaign consisting of multiple incidents associated with the same threat actor utilising domain registration hijacking to target financial technology, technology and professional service sectors.

Using this access, the threat actor was able to modify domain name system (**DNS**) records, including mail exchanger (**MX**) records, to redirect inbound emails to an attacker-controlled mail server. The threat actor was able to leverage legitimate functionality to verify the compromised domains on various SaaS platforms and attempted to abuse password reset functionality to reset credentials to privileged accounts through redirected emails.

This article focuses on some of the tactics, techniques and procedures (**TTPs**) that we've observed as part of this campaign:

Domain registration hijacking

CyberCX understands that the threat actor undertook a social engineering attack, leveraging fraudulent identity documents, including passports, to impersonate and verify themselves as the legitimate domain owners to the domain registrar.

Using this access, the threat actor modified DNS records, including nameserver (**NS**) records and mail exchanger (**MX**) records, to threat actor controlled IP addresses. As a result, inbound emails to the domain were redirected to the attacker's mail server. Notably in at least one instance, these emails were not redirected back to the legitimate mail servers.

By leveraging their control over the domain, the threat actor was able to perform the following attack chain to target software-as-a-service platforms associated with the domain:

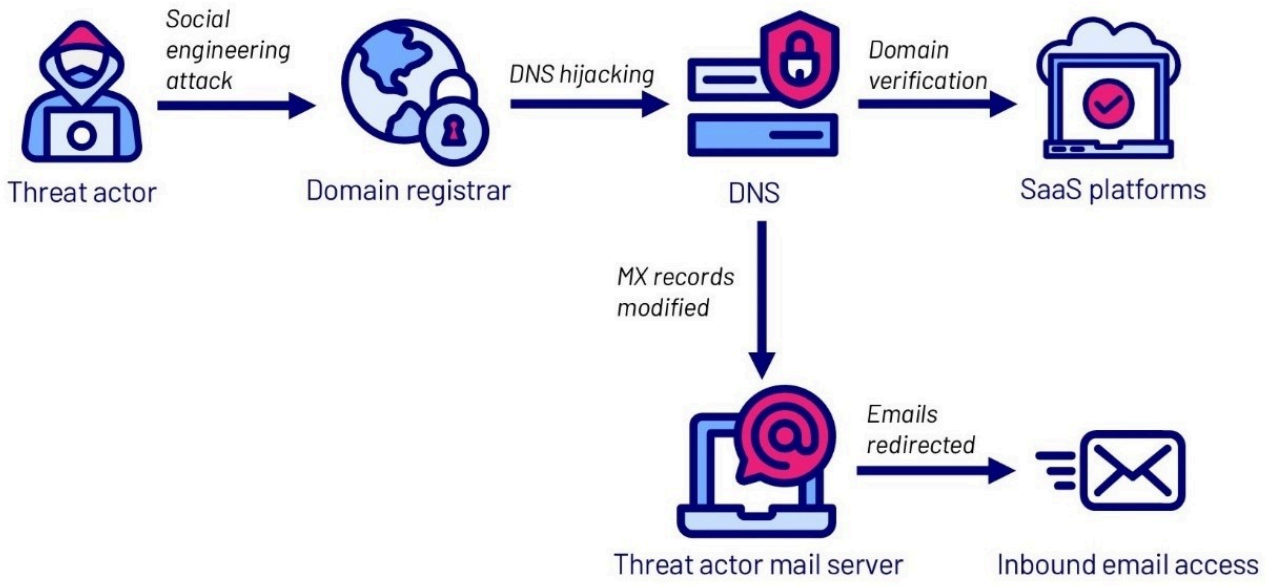

Figure 1 – Threat actor attack chain

SaaS platform domain verification

In at least one instance, the threat actor performed a novel technique to add an external cloud account with the highest level of administrator permissions to the legitimate SaaS platform's administration portal.

The threat actor was able to verify the domain on an external Atlassian organization, likely by **adding TXT records to the compromised DNS**, which enabled them to discover and centrally manage all Atlassian products associated with the domain by leveraging Atlassian Guard's **Automatic Product Discovery** feature. This feature is intended to allow Atlassian organization owners to discover and take control of shadow IT infrastructure created by users in their domain.

In February 2024, as part of **updated Automatic Product Discovery functionality**, Atlassian introduced the ability for Organization Admins in the verified domain to join unmanaged Atlassian instances associated with the domain. These users are added with the Organization Admin role.

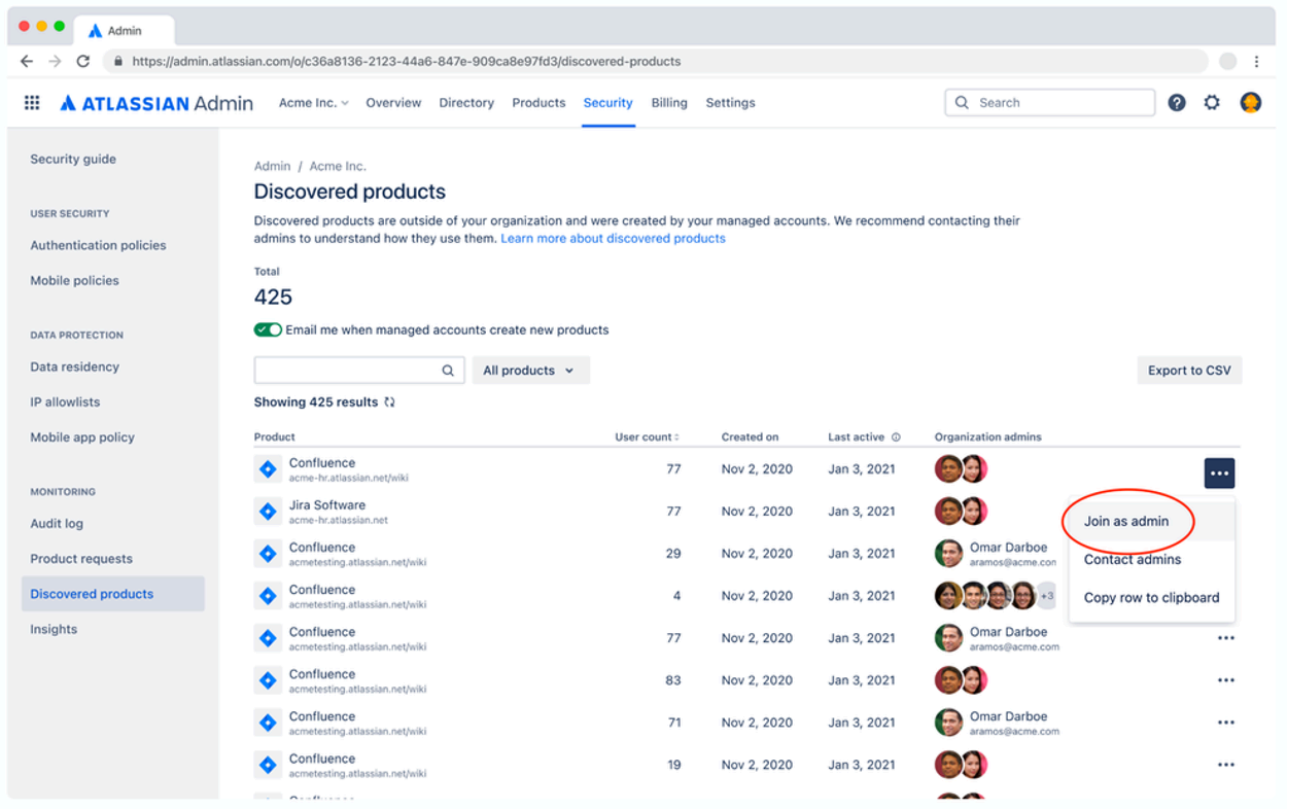

Figure 2 – Automatic Product Discovery "Join as admin" option, sourced from Atlassian documentation

The threat actor was able to abuse this functionality to add an external Gmail account from an external threat actor controlled Atlassian organization, after performing domain verification, to the legitimate Atlassian organization's Administration portal as an Organization Admin. Using this access, the threat actor would have been able to remove all other Organization Admins, effectively taking control of their Atlassian organization and all associated Atlassian products including Confluence and Jira.

Email redirection

The threat actor also leveraged the email redirection to target SaaS platforms that utilise "magic link" passwordless authentication. By forcing authentication to domain accounts on these SaaS platforms, the threat actor was able to generate and intercept magic link URLs. Notably, some SaaS platforms such as Slack allow users to join all workspaces associated with the domain that have the **"Allow invitations and approve invitations for any email address from these domains" option configured**. The threat actor was observed accessing unmonitored Slack workspaces using compromised accounts and using Slack Connect to direct message users outside of the organisation as part of further social engineering attacks.

Microsoft's self-service password reset portal was also abused for privileged account discovery using the automated emails generated using the "Contact your administrator" link to identify accounts with Helpdesk Administrator, Password Administrator, User Administrator or Global Administrator roles, as **configured by default in Microsoft Entra ID**.

Impact

CyberCX is not aware of any ransomware activity associated with this campaign, however, in multiple instances, the threat actor was able to successfully exfiltrate sensitive data and subsequently attempted to extort the compromised organisation.

Assessment

CyberCX Intelligence has observed limited public reporting relating to this technique.

CyberCX recommends organisations should work with their domain registrar to implement a domain registry lock, which will prevent any modifications to DNS server records, modification of contacts, transferring of domains or deletion of domain names without proper authentication. An out of band communication channel should further be established as part of this authentication procedure.

Additionally, organisations should audit their shadow IT infrastructure across all SaaS applications to ensure that they have sufficient visibility of all systems created by their domain users which have not been directly approved by the organisation.

MITRE ATT&CK mapping

Tactic	**Technique / Tool**	**Mitre ID**
Reconnaissance	Gather Victim Identity Information	T1589
Resource Development	Compromise Infrastructure: Domains	T1584.001
	Compromise Infrastructure: DNS Server	T1584.002
Initial Access	Valid Accounts: Cloud Accounts	T1078.004
Persistence	Valid Accounts: Cloud Accounts	T1078.004
Privilege Escalation	Account Manipulation: Additional Cloud Roles	T1098.003
Credential Access	Forced Authentication	T1187
Discovery	Account Discovery: Email Account	T1087.003
Lateral Movement	Remote Services: Cloud Services	T1021.007
Exfiltration	Email Collection: Remote Email Collection	T1114.002
