SaaS Ransomware Observed in the Wild for Sharepoint in Microsoft 365 | Obsidian Security

By Emile Antone

Published: 2023-06-07 · Archived: 2026-04-05 17:19:43 UTC

Background

Obsidian's Threat Research team has observed a SaaS ransomware attack against a company's Sharepoint Online (Microsoft 365) without using a compromised endpoint. Our team and product were leveraged post-compromise to determine the finer details of the attack.

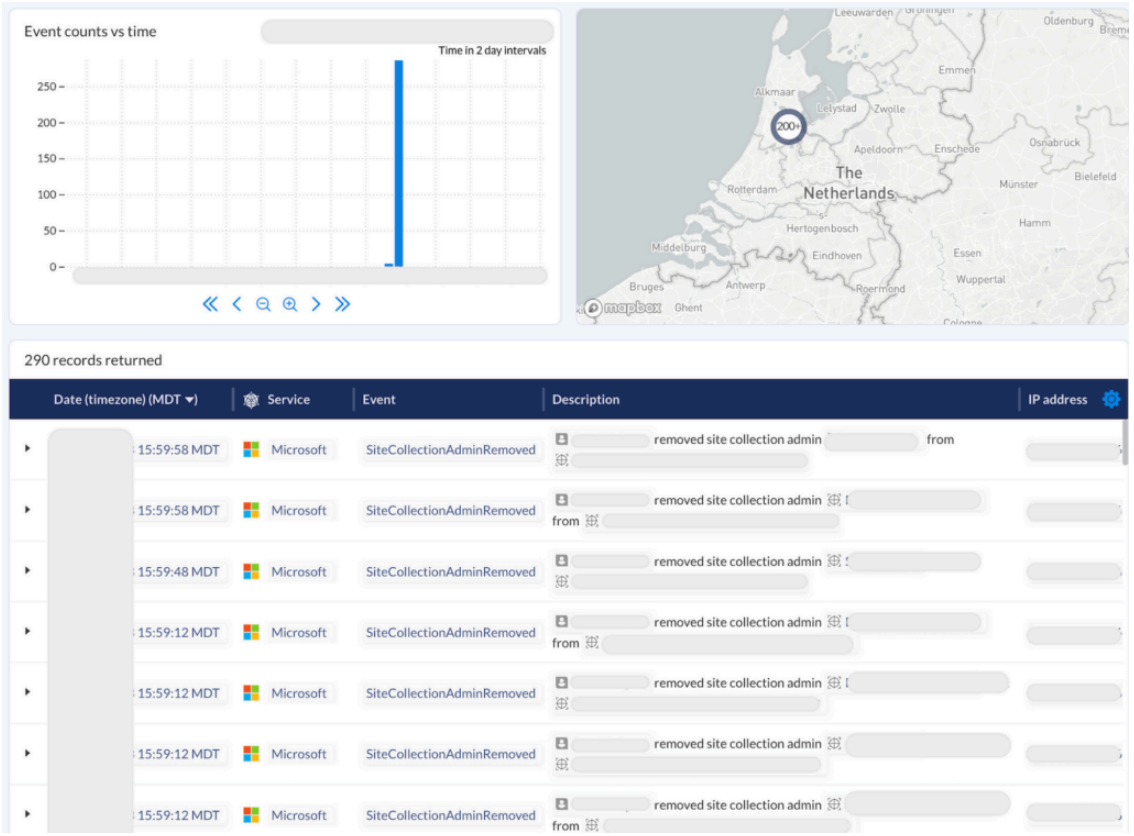
This approach is different from what has been observed in the wild, where some companies had their Sharepoint 365 instances ransomed when attackers encrypted files on a compromised user's machine or a mapped drive and then synchronized them to Sharepoint.

In this blog, we'll outline the details of the attack and provide detection methodologies and IOCs to assist the broader community. Some details have been redacted to protect the privacy of the impacted company.

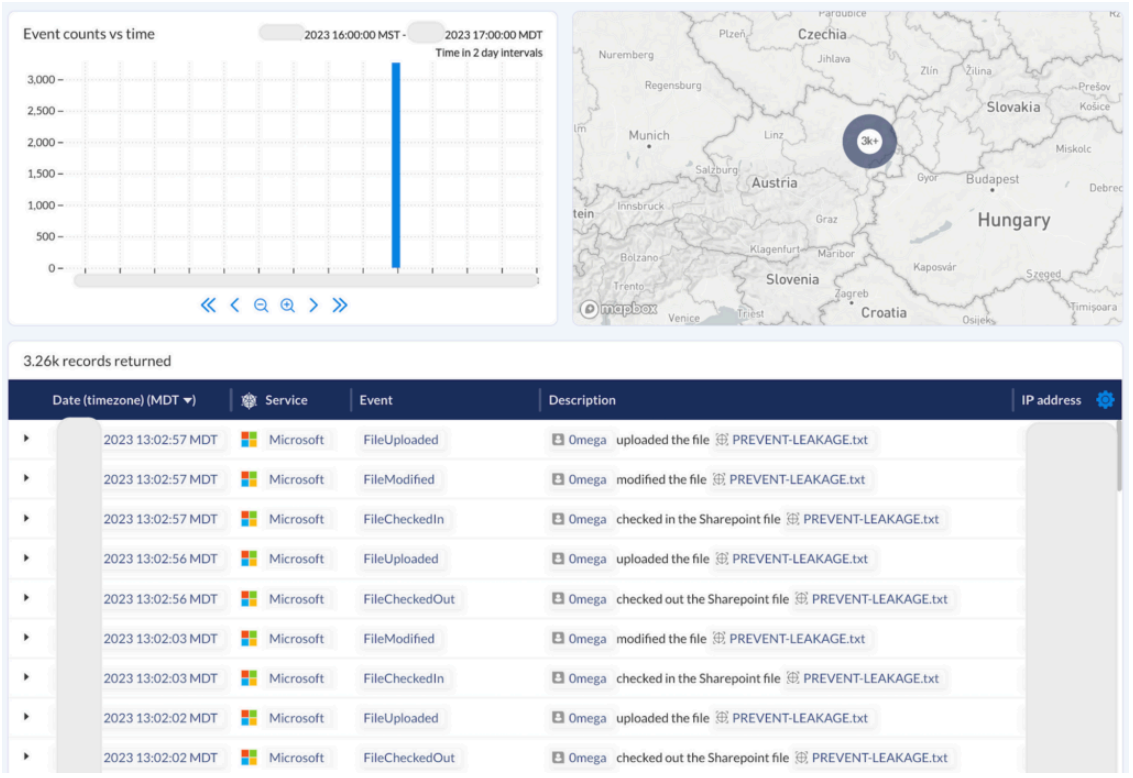
Attack Details

- A Microsoft Global admin service account's credentials were compromised.
- The compromised service account did not have MFA/2FA enabled and could be leveraged from the public internet.
- The service account was accessed from a VPS host provided by VDSinra.ru, with an ip-geolocation that was anomalous relative to legitimate, historical access patterns.
- The compromised service account made a new AD user called *0mega*.
    - UserPrincipalName: *0mega@<redacted>.com*

    - Department: *Contact us <https://0mega-connect>[.]biz/c/<redacted_guid>*
    - StreetAddress: *http://<redacted>[.]onion/c/<redacted_guid>*
- The compromised service account granted the *0mega* account elevated permissions, including *Global Administrator*, *SharePoint Administrator*, *Exchange Administrator*, & *Teams Administrator*.
- The compromised service account granted the *0mega* account *site collection administrator* capabilities to multiple Sharepoint sites and collections, while also removing existing administrators. Over 200 admin removal operations occurred within a 2-hour period.



- Hundreds of files are exfiltrated by the VPS endpoint by leveraging *sppull* (https://www.npmjs.com/package/sppull), a publicly available Node.js module that simplifies the downloading of files from SharePoint.
- Thousands of *PREVENT-LEAKAGE.txt* files are uploaded to Sharepoint, to draw attention to the data exfiltration. This activity is automated using *got* (https://github.com/sindresorhus/got), a publicly available Node.js library for simplifying HTTP requests



- The *0mega-connect[.]biz* and *<redacted>.onion* websites allow impacted companies to chat with the ransomware operators and negotiate the payment, to avoid having details about the breach or their files published online.
- Observables (accounts, infrastructure, etc.) suggest the known *0mega* operators performed this operation.

Detection Opportunities & IOCs

Note: The logs for these detection opportunities can be obtained from Office 365 APIs, assuming audit logging is enabled. Opportunities are labeled as either Generic*, meaning the detection could detect multiple adversaries, or* Specific*, indicating the detection is intended to catch this specific ransomware group. It should be noted that while the Specific detections are pretty accurate, modifications could be made by the ransomware group in the future in the same way that C2 infrastructure and malware file attributes can change.*

- Service accounts
  - Generic: Alert on logins with an ip-geolocation that is anomalous, e.g., the account is typically logged into from a particular country.
  - Generic: Alert on logins that suggest impossible travel, e.g., the account was logged into from two different countries or distant locations in a short timeframe.
  - Generic: If the service account is not intended for regular interactive logins or use, alert on any behaviors that are not defined in code.
- New AD users
  - Specific: alert on any new users with any of the following attributes
    - UserPrincipalName: *0mega@<your_company_domain>.com*
    - MailNickname: *0mega*
    - DisplayName: *0mega* or *Zero Mega*

        - Department: *Contact us <https://0mega-connect>[.]biz/c/<redacted_guid>*
        - StreetAddress: *http://<redacted>[.]onion/c/<redacted_guid>*
        - **Example log in the below image.**
    - Generic: Alert on new AD users that are granted multiple administrative privileges, like *Global Administrator*, *SharePoint Administrator*, *Exchange Administrator*, & *Teams Administrator*.

- New AD groups
    - Specific: alert on any new AD groups called *_0mega_prevent_leakage*.
- Sharepoint Files
    - Specific: alert on any new files named *PREVENT-LEAKAGE.txt* (e.g., logs that contain *“SourceFileName”:”PREVENT-LEAKAGE.txt”*).
    - Generic: alert on high volume file uploads or checkin operations with a *.txt* extension (e.g., logs that contain *“SourceFileExtension”:”txt”*). This alert may be too noisy for some organizations.

- User-Agent
    - Specific: alert on any Microsoft 365 activities from a user-agent of *sppull* or *got (<https://github.com/sindresorhus/got>)*.

Conclusion

Companies pour hundreds of thousands to millions of dollars into SaaS to enable their business, commonly entrusting regulated, confidential, and otherwise sensitive information to these applications. While meaningful progress has been made on endpoint, network, and cloud threat detection, SaaS threat detection remains an area that many companies are still only beginning to consider.

We have always encouraged organizations to both take steps to protect themselves against threats and continuously monitor for indications of malicious activity.

Proactive risk management can include hardening SaaS controls, roping in excessive privileges, and revoking unsanctioned or high risk integrations. Robust threat response involves the consolidation and analysis of associated SaaS audit/activity logs to uncover patterns consistent with a breach, an insider threat, or a compromised third-party integration. As a leading SaaS security posture management (SSPM) platform, Obsidian helps teams address each of these security considerations across their entire SaaS ecosystem.
