# Microsoft breach led to theft of 60,000 US State Dept emails

By Sergiu Gatlan

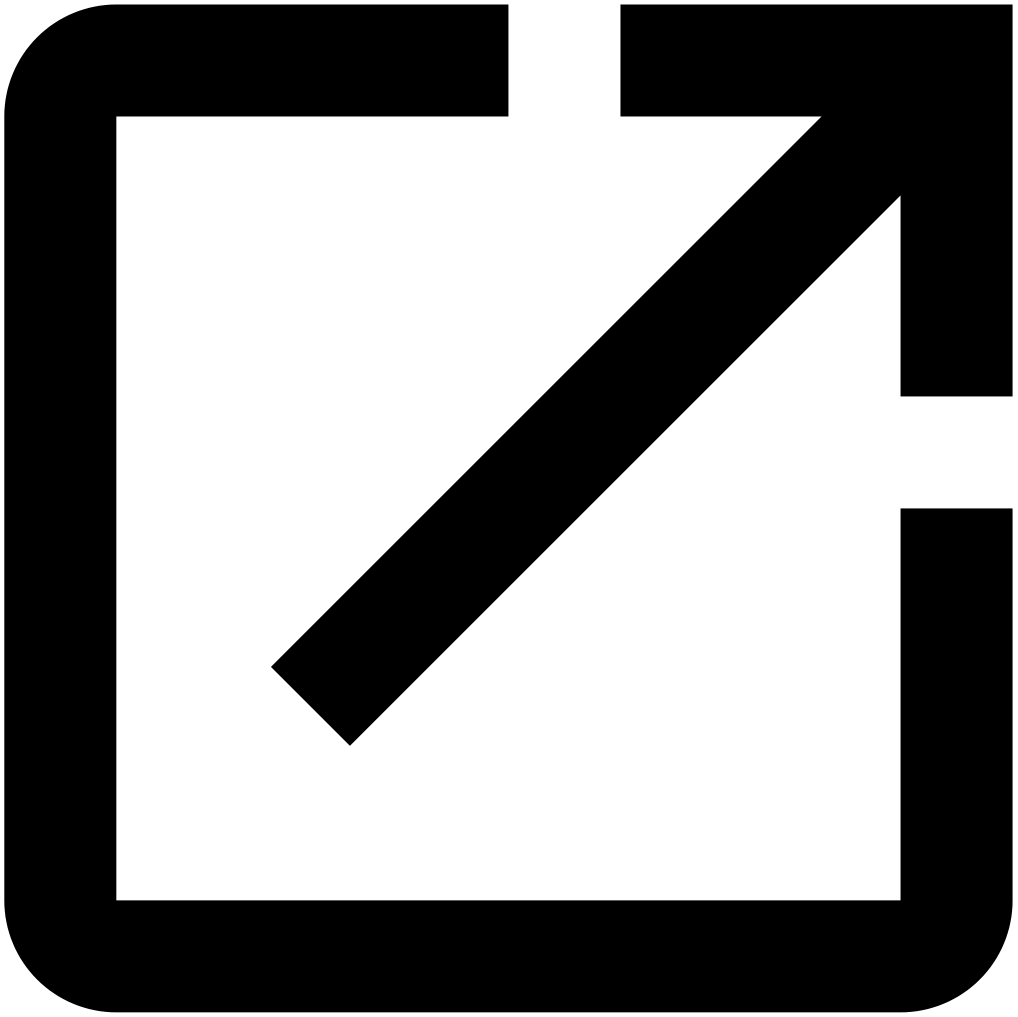
Published: 2023-09-28 · Archived: 2026-04-05 14:06:38 UTC

Chinese hackers stole tens of thousands of emails from U.S. State Department accounts after breaching Microsoft's cloud-based Exchange email platform in May.

During a recent Senate staff briefing, U.S. State Department officials disclosed that the attackers stole at least 60,000 emails from Outlook accounts belonging to State Department officials stationed in East Asia, the Pacific, and Europe, as Reuters first reported.

Additionally, the hackers managed to obtain a list containing all of the department's email accounts. The compromised State Department personnel primarily focused on Indo-Pacific diplomacy efforts.


DIE LINKE.
0:00



"We need to harden our defenses against these types of cyberattacks and intrusions in the future, and we need to take a hard look at the federal government's reliance on a single vendor as a potential weak point," Senator Eric Schmitt said in a statement.

The reports were also confirmed by State Department spokesperson Matthew Miller in a press briefing on Thursday.

"Yes, it was approximately 60,000 unclassified emails that were exfiltrated as a part of that breach. No, classified systems were not hacked. These only related to the unclassified system," Miller told reporters.

"We have not made an attribution at this point, but, as I said before, we have no reason to doubt the attribution that Microsoft has made publicly. Again this was a hack of Microsoft systems that the State Department uncovered and notified Microsoft about."

## Email breaches linked to Storm-0558 Chinese cyberspies

In July, Microsoft revealed that beginning on May 15, 2023, threat actors successfully breached Outlook accounts associated with approximately 25 organizations. The compromised organizations include the U.S. State and Commerce Departments and certain consumer accounts presumably linked to them.

Microsoft did not disclose specific details regarding the affected organizations, government agencies, or countries impacted by this email breach.

The company attributed the attacks to a cyber-espionage collective known as Storm-0558, suspected of being focused on obtaining sensitive information by infiltrating the email systems of their targets.

Earlier this month, Microsoft disclosed that the threat group first obtained a consumer signing key from a Windows crash dump, a breach facilitated after compromising the corporate account of a Microsoft engineer, which enabled access to the government email accounts.

The stolen Microsoft Account (MSA) key was employed to compromise Exchange Online and Azure Active Directory (AD) accounts by exploiting a previously patched zero-day validation vulnerability in the GetAccessTokenForResourceAPI. The flaw allowed the attackers to generate counterfeit signed access tokens, which allowed them to impersonate accounts within the targeted organizations.

In response to the security breach, Microsoft revoked the stolen signing key and, following investigations, found no additional instances of unauthorized access to customer accounts through the same method of access token forgery.

Under pressure from the Cybersecurity and Infrastructure Security Agency (CISA), Microsoft has also agreed to broaden access to cloud logging data at no cost, which would help network defenders identify potential breach attempts of a similar nature in the future.

Previously, such logging capabilities were exclusively accessible to customers with Purview Audit (Premium) logging licenses. Because of this, Microsoft faced criticism for impeding organizations from promptly detecting Storm-0558's attacks.



---

Source: https://www.bleepingcomputer.com/news/security/microsoft-breach-led-to-theft-of-60-000-us-state-dept-emails/