Mitigation for China-based threat actor activity - Microsoft On the Issues

By Charlie Bell

Published: 2023-07-12 · Archived: 2026-04-05 18:46:50 UTC

Microsoft and others in the industry have called for transparency when it comes to cyber incidents so that we can learn and get better. As we've stated previously, we cannot ignore the exponential rise and frequency of sophisticated attacks. The growing challenges we face only reinforce our commitment to greater information sharing and industry partnership.

Today, we are publishing details of activity by a China-based actor Microsoft is tracking as Storm-0558 that gained access to email accounts affecting approximately 25 organizations including government agencies as well as related consumer accounts of individuals likely associated with these organizations. We have been working with the impacted customers and notifying them prior to going public with further details. At this stage – and in coordination with customers – we are sharing the details of the incident and threat actor to benefit the industry.

Cyberattacks continue to rise in sophistication and frequency

Motivated threat actors continue to focus on compromising IT systems. These well-resourced adversaries draw no distinction between trying to compromise business or personal accounts associated with targeted organizations, since it only takes one successfully compromised account login to gain persistent access, exfiltrate information and achieve espionage objectives. The threat actor Microsoft links to this incident is an adversary based in China that Microsoft calls Storm-0558. We assess this adversary is focused on espionage, such as gaining access to email systems for intelligence collection. This type of espionage-motivated adversary seeks to abuse credentials and gain access to data residing in sensitive systems.

Mitigation completed for all customers

On June 16, 2023, based on customer reported information, Microsoft began an investigation into anomalous mail activity. Over the next few weeks, our investigation revealed that beginning on May 15, 2023, Storm-0558 gained access to email data from approximately 25 organizations, and a small number of related consumer accounts of individuals likely associated with these organizations. They did this by using forged authentication tokens to access user email using an acquired Microsoft account (MSA) consumer signing key. **Microsoft has completed mitigation of this attack for all customers.**

We added substantial automated detections for known indicators of compromise associated with this attack to harden defenses and customer environments, and we have found no evidence of further access.

Coordinated response key to rapid mitigation

Microsoft's real-time investigation and collaboration with customers let us apply protections in the Microsoft Cloud to protect our customers from Storm-0558's intrusion attempts. We've mitigated the attack and have

contacted impacted customers. We've also been partnering with relevant government agencies like DHS CISA. We're thankful they and others are working with us to help protect affected customers and address the issue. We're grateful to our community for a swift, strong and coordinated response.

More details to support our customers and the defender community can be found here.

Accountability starts with us

The accountability starts right here at Microsoft. We remain steadfast in our commitment to keep our customers safe. We are continually self-evaluating, learning from incidents, and hardening our identity/access platforms to manage evolving risks around keys and tokens.

We need to continue to push the envelope on security so we're prepared for whatever might come our way. We will continue to work with our customers and community to share information and strengthen our collective defenses.
