Src: Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email | MSRC Blog | Microsoft Security Response Center

Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email

MSRC / By MSRC / July 11, 2023 / 3 min read

UPDATE: Microsoft has released threat analysis on Storm-0558 activity here. Microsoft additionally released additional defense-in-depth security fixes to help customers improve token validation in their custom applications.

Microsoft has mitigated an attack by a China-based threat actor Microsoft tracks as Storm-0558 which targeted customer emails. Storm-0558 primarily targets government agencies in Western Europe and focuses on espionage, data theft, and credential access. Based on customer reported information on June 16, 2023, 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 accounts affecting approximately 25 organizations in the public cloud including government agencies as well as 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.

Our telemetry indicates that we have successfully blocked Storm-0558 from accessing customer email using forged authentication tokens. No customer action is required. As with any observed nation-state actor activity, Microsoft has contacted all targeted or compromised organizations directly via their tenant admins and provided them with important information to help them investigate and respond. We continue to work closely with these organizations. If you have not been contacted, our investigations indicate that you have not been impacted.

Microsoft is partnering with DHS CISA and others to protect affected customers and address the issue. We continue to investigate and monitor the Storm-0558 activity.

Commented [1]: Why customer reported? What happened to the billions spent in ML/AI?
What was the initial customer report? How did it get escalated and flagged to MSRC?

Commented [2]: This statement confirms that none of the ML/AI and anomaly detection algos across OWA/AzureAD picked this up.
If Nick Carr has to trawl through logs for a year to make sense of this, then ML didn't do its job.

Commented [3]: Note: *KEY1*
What does acquiring MSA consumer signing key mean here? (I understand what signing keys are in JWT/context)
How many consumer signing keys are there? Is there 1-signing key per tenant, or is the MSFT signing key unique for all tenants, or the answer is something in between.

Need contention-ration (Signing keys <-> Tenant e.g. 100:1)

Commented [4]: Blocked what? (IP, Email, Killed the other tenant,)
Blocked HOW ? (Depends on answer to previous question)

Commented [5]: Assuming this is via TAN?
What happens if the registered GlobalAdmins are dummy service accounts / break-glass accounts?
How will MSFT notify the tenant admin if the Tenant Admin is not a named account?

Details

Microsoft investigations determined that Storm-0558 gained access to customer email accounts using Outlook Web Access in Exchange Online (OWA) and Outlook.com by forging authentication tokens to access user email.

The actor used an acquired MSA key to forge tokens to access OWA and Outlook.com. MSA (consumer) keys and Azure AD (enterprise) keys are issued and managed from separate systems and should only be valid for their respective systems. The actor exploited a token validation issue to impersonate Azure AD users and gain access to enterprise mail. We have no indications that Azure AD keys or any other MSA keys were used by this actor. OWA and Outlook.com are the only services where we have observed the actor using tokens forged with the acquired MSA key.

Microsoft has mitigated the acquired MSA key and our telemetry indicates the actor activities have been blocked. We took the following proactive steps as our investigation proceeded:

- Microsoft blocked the usage of tokens signed with the acquired MSA key in OWA preventing further threat actor enterprise mail activity.
- Microsoft completed the replacement of the key to prevent the threat actor from using it to forge tokens.
- Microsoft blocked usage of tokens issued with the key for all impacted consumer customers.

We have continuously improved the security of the MSA key management systems since the acquired MSA key was issued, as part of defense in depth, to ensure the safety and security of consumer keys.

As part of our ongoing efforts to improve security of token validation for customers, we released defense-in-depth changes to the Microsoft.IdentityModel and Microsoft.Identity.Web libraries. As the acquired signing key has already been invalidated by Microsoft, there is no immediate risk to customers. Customers are encouraged to pick up this update as part of their next security maintenance window.

We will update this guidance with new details and recommendations as appropriate.

Revision History

Commented [6]: *KEY-1*

Commented [7]: *KEY-2*

Commented [8]: *Separate for every tenant?* (Tenant1 key is separate from Tenant2 key)

OR *Separate for other MSFT key-issuing systems?*(Meaning, there is a boundary between MSA/AAD keys and Dynamics key)

Commented [9]: *Buried the lede here*
Exploited what?
How did impersonation work? Is this OAUTH2 impersonation?
Where is the CVE for this potentially glaring auth-bug?

Commented [10]: *Correction*
These are the only systems you *know-off*.
If the actor stole the key and didn't use it, you have no-record of that.

Commented [11]: This is just a standard stolen API key replacement procedure.
- Block usage of current key.
- Reissue new key.
- Expire all tokens issue with the current API key.

Aside: Not sure if *CAE* was used to disable this, because this is how CAE is being sold publicly.

Commented [12]: This is strange. Nobody said anything about the key-issuing infrastructure. Did MSFT just admit that the key-management systems were *also* attacked?

Was the key-issuing infrastructure attacked? Why did it need to be strengthened?
Does MSFT have accurate logs of every usage of every key issued by the key-issuing infrastructure?
What's other retention policy of those logs?

- 2023-07-11 – Initial release
- 2023-07-13 – Added links to additional threat intelligence defenders can use as well as links for updated validation libraries for customers.