RCA for continuous restarts of Sophos AV engine on some of the Email Security Appliances

Cisco would like to share details about Sophos AV engine restart issue, recently affecting customers using the X90 series of Email Security Appliances:

Incident Description

On January 2nd 2017, at 11:30am ET, Cisco support received complaints from multiple customers about Email work queue build up on their appliances. Investigation revealed that the Sophos AV engine on those appliances was continuously restarting

Customer Impact

- Delay in Email delivery
- Emails were not scanned by Sophos AV Engine
- Only X90 series of Appliances were impacted by this issue

Chronology of Event/Timelines in Eastern Time (ET)

01/02/2017 – 11:30am	Cisco support received calls from customers about Email Work queue build up
01/02/2017 – 01:30pm	**+ 2:00 hours**– Main issue identified and a manual mitigation workaround provided
01/02/2017 – 10:00pm	**+ 10:30 hours** – Root cause identified and corrective steps defined
01/05/2017 – 11:10pm	**+ 3 days & 11:40 hours** – Patch update pushed to alleviate the manual workaround

Findings and Root cause

There were multiple issues which resulted in the Sophos Engine restarts on X90 series appliances

1. There was a failure in the Cisco Security signature update server. Due to which, no Sophos updates were published starting from 12/31/2016

2. On 01/02/2017, as there were no Sophos updates, a Sophos configuration file was deleted on X90 series appliances due to an existing bug (CSCvc39693).
3. On 01/02/2017, the Cisco Security signature update server was restarted and new updates from Sophos were published. On x90 series appliances, since the Sophos Configuration file was already deleted, it resulted in a continuous restarts of Sophos AV engine

Corrective Actions

Security signature update server failure:

The Security signature update server has been moved to new distribution system to avoid process failures and lack of signature updates. This change was carried out on 01/04/2017, 01:00pm ET

Additional Signature update validation in staging environment before publishing to customers:

Cisco has been validating signature updates for some of the security engines in a staging environment before publishing it to customers. This has been now extended to include Sophos AV engine. This will not only detect malfunctioning signature updates, but also identifies missing signature updates at a very early stage. This change was carried out on 01/04/2017, 02:00pm ET

Planned additional actions to prevent reoccurrence of such issues

Avoid deletion of Sophos Configuration file:

A change will be made on the ESA, to prevent deletion of Sophos Configuration file when there are no updates. This change is tracking for customer release during the week of 23rd Jan 2017