Microsoft Internal Solorigate Investigation Update

msrc-blog.microsoft.com/2020/12/31/microsoft-internal-solorigate-investigation-update/

As we said in our recent blog, we believe the Solorigate incident is an opportunity to work together in important ways, to share information, strengthen defenses and respond to attacks. Like other SolarWinds customers, we have been actively looking for indicators of the Solorigate actor and want to share an update from our ongoing internal investigation.

Our investigation into our own environment has **found no evidence of access to production services or customer data. The investigation, which is ongoing, has also found no indications that our systems were used to attack others**.

As we previously reported, we detected malicious SolarWinds applications in our environment, which we isolated and removed. Having investigated further, we can now report that we have not found evidence of the common TTPs (tools, techniques and procedures) related to the abuse of forged SAML tokens against our corporate domains.

Our investigation has, however, revealed attempted activities beyond just the presence of malicious SolarWinds code in our environment. This activity has not put at risk the security of our services or any customer data, but we want to be transparent and share what we're learning as we combat what we believe is a very sophisticated nation-state actor.

We detected unusual activity with a small number of internal accounts and upon review, we discovered one account had been used to view source code in a number of source code repositories. The account did not have permissions to modify any code or engineering systems and our investigation further confirmed no changes were made. These accounts were investigated and remediated.

At Microsoft, we have an inner source approach – the use of open source software development best practices and an open source-like culture – to making source code viewable within Microsoft. This means we do not rely on the secrecy of source code for the security of products, and our threat models assume that attackers have knowledge of source code. So viewing source code isn't tied to elevation of risk.

As with many companies, we plan our security with an "assume breach" philosophy and layer in defense-in-depth protections and controls to stop attackers sooner when they do gain access. We have found evidence of attempted activities which were thwarted by our protections, so we want to re-iterate the value of industry best practices such as outlined here, and implementing Privileged Access Workstations (PAW) as part of a strategy to protect privileged accounts. We will provide additional updates if and when we discover new information to help inform and enable the community. As we learn more from our own internal investigation, and from helping customers, we will continue to improve our security products and share these learnings with the community. For the up-to-date information and guidance, please visit our resource center at https://aka.ms/solorigate.