CERT-MU Security Alert

CERT-MU

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations

Issue Date: 28 December 2020

Severity Rating: High

Description

Security researchers have discovered an Advanced Persistent Threat (*An advanced persistent threat is a stealthy threat actor which gains unauthorized access to a computer network and remains undetected for an extended period*) which targets and compromises critical infrastructure entities, government agencies and private sector organisations. The security threat has the ability to exploit software supply chains and also has shown significant knowledge of Windows networks.

The following details have been gathered about the APT:

1. The threat actor has been observed targeting compromised SolarWinds Orion products. SolarWinds Orion is an enterprise network management software suite that includes performance and application monitoring and network configuration management along with several different types of analyzing tools. SolarWinds Orion is used to monitor and manage on-premise and hosted infrastructures. To provide SolarWinds Orion with the necessary visibility into this diverse set of technologies, it is common for network administrators to configure SolarWinds Orion with pervasive privileges, making it a valuable target for adversary activity.

2. The threat makes extensive use of obfuscation to hide Command & Command communications. Virtual private servers (VPSs) are used with IP addresses in the home country of the victim for most communications to hide their activity among legitimate user traffic. The attackers also frequently rotate their "last mile" IP addresses to different endpoints to obscure their activity and avoid detection.

3. The threat adds authentication tokens and credentials to highly privileged Active Directory domain accounts as a persistence and escalation mechanism. In many

instances, the tokens enable access to both on-premise and hosted resources. Microsoft has released a query that can help detect this activity.

4. The threat collects information from victims' environments. This is done by compromising the Security Assertion Markup Language (SAML) signing certificate using their escalated Active Directory privileges. Once this is accomplished, the threat creates unauthorized but valid tokens and presents them to services that trust SAML tokens from the environment. These tokens can then be used to access resources in hosted environments, such as email, for data exfiltration via authorized application programming interfaces (APIs).

5. The threat uses a complex network of IP addresses to obscure its activity, which can result in a detection opportunity referred to as "impossible travel." Impossible travel occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses during the time period between the logins)

Workarounds

1. If the threat has compromised administrative level credentials in an environment or if organisations identify SAML abuse in the environment, simply mitigating individual issues, systems, servers, or specific user accounts will likely not lead to the threat removal from the network. In such cases, organisations should consider the entire identity trust store as compromised. In the event of a total identity compromise, a full reconstitution of identity and trust services is required to successfully remediate. In this reconstitution, it bears repeating that this threat actor is among the most capable, and in many cases, a full rebuild of the environment is the safest action.

2. For organisations using the SolarWinds Orion product, specific mitigation is required on the networks. Details of the implementing the workarounds is available on: https://us-cert.cisa.gov/ncas/alerts/aa20-352a

CERT-MU wishes to inform organisations to be cautious of this threat and apply workarounds if they suspect any compromise.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu