HC3: Sector Alert

May 28, 2021 TLP: White Report: 202105281600

New Phishing Campaign Launched by SOLARWINDS Attackers

Executive Summary

On May 28, 2020, Microsoft published details of a widespread campaign from a group they labeled NOBELIUM. NOBELIUM, attributed to the SolarWinds supply chain attack, targeted over 150 organizations with approximately 3,000 emails from a compromised email marketing service utilized by the US Agency for International Development (USAID). The masquerading USAID emails if interacted with, could infect a target system with malware and grant persistent access. HC3 recommends applying suggested Microsoft mitigations to reduce the impact of threat.

Report

The Microsoft Threat Intelligence Center (MSTIC) began monitoring a spear phishing campaign in January 2021 from a group they call NOBELIUM. NOBELIUM has been attributed to the SolarWinds attack. Microsoft observed cyberattacks by Nobelium targeting government agencies, think tanks, consultants, and non-governmental organizations. On May 25, 2021, Microsoft observed and tracked NOBELIUM changing techniques from early stages of the campaign. NOBELIUM compromised USAIDs email marketing platform, Constant Contact. The social engineering emails were labeled USAID Special Alert with references to election fraud. NOBELIUM was able to masquerade approximately 3,000 targeted emails with an attached HTML file. When this malicious attachment is opened, an embedded JavaScript deposits an ISO image file on the system. If the user opened that file, the ISO file would be mounted similar to an external/network drive. A shortcut file (LNK) would then execute an accompanying DLL, which would execute a Cobalt Strike Beacon. A malicious ISO file is then delivered to the system. The successful placement of these payloads enables NOBELIUM to laterally move throughout the compromised system and exfiltrate data.

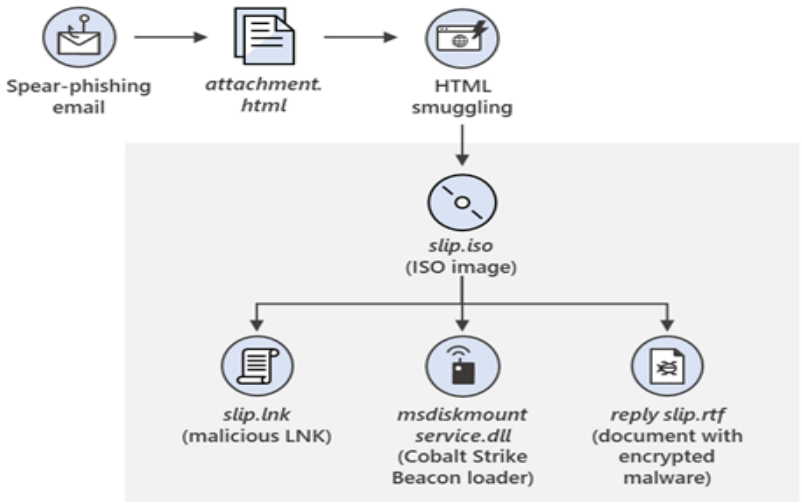

Image source: Microsoft.com

HC3: Sector Alert

May 28, 2021 TLP: White Report: 202105281600

Analysis

NOBELIUM Threat Actors carefully researched their victims and used legitimate services to get end users to click malicious links. Microsoft reported that due to the volume of emails distributed, automated email threat detection systems blocked most of the malicious emails and marked them as spam. However, some emails may have successfully delivered.

Patches, Mitigations, and Workarounds

HC3 highly recommends organizations to investigate and monitor communications matching characteristics described by MSTIC to ensure protection against possible exploits. Microsoft mitigation actions and Indicators of Compromise (IOCS) of active campaign can be found via Microsoft Blog. Due to newly information published from NOBELIUM active campaign, CISA has also updated Exploitation of Pulse Connect Secure Vulnerabilities Alert AA21-110A with recent revealed TTPs, IOCs, and updated guidance.

References

New sophisticated email-based attack from NOBELIUM
https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

Another Nobelium Cyberattack
https://blogs.microsoft.com/on-the-issues/2021/05/27/nobelium-cyberattack-nativezone-solarwinds/

Microsoft Announces New Campaign from NOBELIUM
https://us-cert.cisa.gov/ncas/current-activity/2021/05/27/microsoft-announces-new-campaign-nobelium

Suspected APT29 Operation Launches Election Fraud Themed Phishing Campaigns
https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

Microsoft warns of current Nobelium phishing campaign impersonating USAID
https://www.zdnet.com/article/microsoft-warns-of-current-nobelium-phishing-campaign-impersonating-usaid/

Alert (AA21-110A) Exploitation of Pulse Connect Secure Vulnerabilities
https://us-cert.cisa.gov/ncas/alerts/aa21-110a

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback