<https://www.securityweek.com/group-behind-solarwinds-hack-bypassed-mfa-access-emails-us-think-tank>

Group Behind SolarWinds Hack Bypassed MFA to Access Emails at US Think Tank

December 15, 2020

Using indicators of compromise (IoCs) made available by FireEye, threat intelligence and incident response firm Volexity determined that the threat group behind the SolarWinds hack targeted a U.S. think tank earlier this year, and it used a clever method to bypass multi-factor authentication (MFA) and access emails.

IT management and monitoring solutions provider SolarWinds has confirmed that a sophisticated threat group compromised the software build system for its Orion monitoring platform, allowing it to deliver trojanized updates to the company’s customers between March and June 2020.

The campaign apparently targeted several U.S. government organizations — including the DHS, the Treasury Department and the Commerce Department — as well as many other organizations in North America, Europe, Asia and the Middle East. FireEye was apparently also targeted by the same group, which managed to steal some Red Team tools from the cybersecurity firm.

SolarWinds said in a SEC filing that 18,000 of its 300,000 customers may have used the compromised products. One of those customers, according to Volexity, was a U.S.-based think tank that failed to detect the attackers’ presence and, once it did detect them, failed to keep them out.

Volexity said the group, which it tracks as Dark Halo (FireEye tracks it as UNC2452), remained undetected for several years. When they breached the think tank’s systems for a second time, the hackers leveraged a vulnerability in the organization’s Microsoft Exchange Control Panel and used a novel technique to bypass MFA from Cisco-owned Duo Security and access emails.

When the attackers struck the third time, in June and July 2020, they exploited the SolarWinds Orion product.

“At the time of the investigation, Volexity deduced that the likely infection was the result of the SolarWinds box on the target network; however, it was not fully understood exactly how the breach occurred (i.e., whether there was some unknown exploit in play, or other means of access), therefore Volexity was not in a position to report the circumstances surrounding the breach to SolarWinds,” Volexity said.

However, the most interesting part of Volexity’s report describes how Dark Halo bypassed MFA during the second breach it observed at the think tank. The method involved bypassing the Duo MFA to access an email account through the victim’s Outlook Web App (OWA) service.

“Logs from the Exchange server showed that the attacker provided username and password authentication like normal but were not challenged for a second factor through Duo. The logs from the Duo authentication server further showed that no attempts had been made to log into the account in question. Volexity was able to confirm that session hijacking was not involved and, through a memory dump of the OWA server, could also confirm that the attacker had presented cookie tied to a Duo MFA session named duo-sid,” Volexity explained.

“Volexity’s investigation into this incident determined the attacker had accessed the Duo integration secret key (akey) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account,” it added.

Volexity has clarified that the method did not involve exploitation of a vulnerability in the Duo product. The attack was possible due to the victim’s failure to change all secrets associated with key integrations after the breach was discovered.

SolarWinds also reported observing an attack targeting its Office 365 email systems, but it has yet to determine if it was related to the Orion hack. In a blog post on the attacks, Microsoft also described interesting methods used by the hackers to access emails.

While some reports say Russia is behind the SolarWinds hack, specifically the group tracked as APT29 and Cozy Bear, Volexity said it had found no links during its investigation to a known threat actor. Russia has denied the allegations.

| ID | Name | Description | Date |
| --- | --- | --- | --- |
| T1195.002 | Supply Chain Compromise – Compromise Software Supply Chain | IT management and monitoring solutions provider SolarWinds has confirmed that a sophisticated threat group compromised the software build system for its Orion monitoring platform, allowing it to deliver trojanized updates to the company’s customers between March and June 2020. | March/June 2020 – could narrow down |
| TA0010 | Exfiltration | FireEye was apparently also targeted by the same group, which managed to steal some Red Team tools from the cybersecurity firm. | ?? |
| T1078.004 | Valid Accounts – Cloud Accounts | “Logs from the Exchange server showed that the attacker provided username and password authentication like normal but were not challenged for a second factor through Duo. The logs from the Duo authentication server further showed that no attempts had been made to log into the account in question. Volexity was able to confirm that session hijacking was not involved and, through a memory dump of the OWA server, could also confirm that the attacker had presented cookie tied to a Duo MFA session named duo-sid,” Volexity explained.  “Volexity’s investigation into this incident determined the attacker had accessed the Duo integration secret key (akey) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account,” it added. | ?? |
| T1539 | Steal Web Session Cookie – Note: this is as close as Mitre have, should be ‘forge cookie’. | “Logs from the Exchange server showed that the attacker provided username and password authentication like normal but were not challenged for a second factor through Duo. The logs from the Duo authentication server further showed that no attempts had been made to log into the account in question. Volexity was able to confirm that session hijacking was not involved and, through a memory dump of the OWA server, could also confirm that the attacker had presented cookie tied to a Duo MFA session named duo-sid,” Volexity explained.  “Volexity’s investigation into this incident determined the attacker had accessed the Duo integration secret key (akey) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account,” it added. |  |
| T1083 | File and Directory Discovery – to find the akey | “Logs from the Exchange server showed that the attacker provided username and password authentication like normal but were not challenged for a second factor through Duo. The logs from the Duo authentication server further showed that no attempts had been made to log into the account in question. Volexity was able to confirm that session hijacking was not involved and, through a memory dump of the OWA server, could also confirm that the attacker had presented cookie tied to a Duo MFA session named duo-sid,” Volexity explained.  “Volexity’s investigation into this incident determined the attacker had accessed the Duo integration secret key (akey) from the OWA server. This key then allowed the attacker to derive a pre-computed value to be set in the duo-sid cookie. After successful password authentication, the server evaluated the duo-sid cookie and determined it to be valid. This allowed the attacker with knowledge of a user account and password to then completely bypass the MFA set on the account,” it added. |  |