UNCLASSIFIED

DCSA-SIB-0042-21 Dissemination Date: 20 May 2021 Date of Information: 25 April 2021

Cyber Shared Indicator Bulletin (SIB)

(U) Passwordstate Compromised in Supply Chain Attack

actor logged back in and deleted the sign-in page and ZIP file. On 7 December 2020, there was a

successful authentication with a user account to a second Pulse Secure appliance web portal, from the same IP previously seen authenticating to the Pulse Secure with IVEADMIN. It appears email resources were accessed for this user. It also appears that sections of logs are missing from the appliances indicative of APT obfuscation efforts.

(CUI) The IP addresses used by the threat actors in this attack are as follows:

81.151.38.243
216.196.79.223
76.72.43.198
174.67.97.170
24.117.18.111
31.54.182.205
76.72.43.198
128.125.146.117
71.61.214.247
41.210.159.108
167.99.169.182

CUI

(CUI) On 16 April 2021, a CC identified one non-production Pulse Secure VPN device used to pilot new installations had 2 mismatch files. All other Pulse Secure devices, which are used to provide remote access to users, came back clean. That same day CC uploaded the 2 mismatch files to Pulse Secure for decryption and analysis. The Pulse Secure forensics team concluded that the files from the CCs pilot device contained malicious code. However, the Pulse Secure forensic team concluded that the code looked garbled and un-useable in its current form. Further forensic analysis is under way. The garbling of code in the above instance is likely indicative of APT obfuscation efforts after successful compromises.

(U) From at least March 2020 through February 2021, CISA determined a threat actor connected to a CC via the CCs Pulse Secure VPN appliance. The threat actor connected via the U.S.-based residential IP addresses listed below, which allowed them to masquerade as teleworking employees. (Note: these IP addresses belong to routers that are all similar models; based on this activity, CISA suspects that these routers were likely exploited by the threat actor.)

207.89.9.153

24.140.28.90
24.117.18.111
UNCLASSIFIED
(U) The threat actor authenticated to the VPN appliance through several user accounts, none of which had multi-factor authentication (MFA) enabled. Once authenticated to the VPN appliance, the threat actor initiated a VPN connection to the environment. The med

(U) WARNING: This product may contain information associated with United States Persons (USPER) as
defined by Executive Order (EO) 12333 and Department of Defense Manual (DODM) 5240.01. Such
information should be handled and protected in accordance with applicable Intelligence Oversight rules
by persons and organizations subject to those rules. The Defense Counterintelligence Security Agency
(DCSA) collects, retains, and disseminates USPER Information (USPI) in accordance with all applicable
laws, directives, and policies. Should you require minimized USPI, contact Eric Kutchins, Commercial 571-
305-6592, Eric.d.kutchins.civ@mail.mil.

(U) SUMMARY
(U) On April 24, 2021, Danish Cybersecurity Firm, CSIS Security Group, reported that widely used
password-management software, Passwordstate, was compromised by malicious cyber actors during an
in-place update from 20-22 April. Any Passwordstate customers that performed an in-place upgrade
during this time are believed to be affected and any passwords stored in Passwordstate were likely
harvested.

(U) TECHNICAL DETAILS
(U) Between the April 20, 2021, 8:33 p.m. coordinated universal time (UTC) and April 22, 2021, 00.30 a.m.
UTC, the update mechanism of Passwordstate was used to drop a malicious update via a zip file
“Passwordstate_upgrade.zip” containing a rogue dynamic link library (dll) “moserware.secretsplitter.dll.”
The rogue dll was injected/modified with a malicious code snippet. The command and control of the
rogue dll was using a Content Delivery Network (CDN) that was terminated on April 22, 2021, 7:00 a.m.
UTC. While the command and control (C2) servers for this attack are currently offline, harvested
information and credentials could be used at a later date if the C2 servers come back online.

(U) Indicators of Compromise:

-
-
-

asdfhaiughfia https://google.com/fg/3462576

fdsgtr url: hxxp://google[.]com/adgae347q2/5tj

(U) Malicious dll:
f23f9c2aaf94147b2c5d4b39b56514cd67102d3293bdef85101e2c05ee1c3bf9
Moserware.SecretSplitter.dll

(U) User-Agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36

(U) C2:
https://passwordstate-18ed2.kxcdn[.]com/upgrade_service_upgrade.zip

(U) DCSA recommends all Passwordstate users check the file size of moserware.secretsplitter.dll located in their c:\inetpub\passwordstate\bin\ directory. If the file size is 65kb, then compromise is likely. All Passwordstate users should immediately reset all passwords stored in Passwordstate, including Virtual Private Networks, firewalls, switches, local accounts, and servers. Additionally, all users should follow any

additional Passwordstate guidelines for remediation. All known or suspected compromises should be immediately reported to DCSA.

(U) ADDITIONAL INFORMATION
(U) Companies should follow established internal procedures if they suspect any malicious activity and promptly report the incident in accordance with existing policies, regulations, and agreements. The DCSA

cyber threat products are not intended to serve as definitive block lists. DCSA does not provide recommendations or advice regarding protections of information systems processing unclassified information. Product recipients must decide how to use the information contained in this document. Each company must weigh possible risks against operational requirements when determining any block list implementation.

(U) This product contains information derived from DCSA analysis or reports from multiple sources, including National Industrial Security Program participants and U.S. Government agencies. DCSA provides this product to cleared contractor security professionals to facilitate cyber threat awareness for their classified and unclassified networks and to aid in identifying and developing appropriate actions, priorities, and follow-on measures. DCSA receives, analyzes, and disseminates the information in this product in accordance with its assigned missions. The intrusion behavior descriptions and general methodologies cited in this bulletin may be used to monitor for and detect traffic of interest; however, no action should be taken against any of the IP addresses or hostnames. Users should note that information contained in this product does not, unless otherwise noted, contain finished intelligence.

(U) Reporting Notice & Feedback: DCSA CI CD prepared this product. Please contact DCSA CD with any technical questions related to these products at DCSA.CYBERCI@mail.mil. In the event that new or reportable cyber/counterintelligence information comes to light; please contact your local DCSA field office and agent.

(U) REFERENCES

(U) WARNING: This product may contain information associated with USPER as defined by EO 12333 and DODM 5240.01. Such information should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. DCSA collects, retains, and disseminates USPI in accordance with all applicable laws, directives, and policies. Should you require minimized USPI, contact Eric Kutchins, Commercial 571-305-6592, Eric.d.kutchins.civ@mail.mil.

(U) CSIS. “Supply chain attack on the password manager Clickstudios – PASSWORDSTATE.” 23 April 2021. https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/

(U) ZDNet. “Enterprises need to change passwords following ClickStudios, Passwordstate attack.” 24 April 2021. https://www.zdnet.com/article/enterprises-need-to-change-passwords-following-clickstudios-passwordstate-attack/

(U) DarkReading. “Password Manager Suffers 'Supply Chain' Attack.” 23 April 2021. https://beta.darkreading.com/attacks-breaches/password-manager-suffers-supply-chain-attack

↑