DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

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

(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:

- (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