



Homeland
Security



United States
Secret Service

ADVISORY

Backoff Malware: Infection Assessment

22 August 2014

Summary

The Department of Homeland Security (DHS) encourages organizations, regardless of size, to proactively check for possible Point of Sale (PoS) malware infections. One particular family of malware, which was detected in October 2013 and was not recognized by antivirus software solutions until August 2014, has likely infected many victims who are unaware that they have been compromised.

The National Cybersecurity and Communications Integration Center (NCCIC), United States Secret Service (Secret Service), and third-party partners issued an [advisory](#) on July 31, 2014 regarding PoS malware dubbed "Backoff" which was discovered exploiting businesses' administrator accounts remotely and exfiltrating consumer payment data. Over the past year, the Secret Service has responded to network intrusions at numerous businesses throughout the United States that have been impacted by the "Backoff" malware. Seven PoS system providers/vendors have confirmed that they have had multiple clients affected. Reporting continues on additional compromised locations, involving private sector entities of all sizes, and the Secret Service currently estimates that over 1,000 U.S. businesses are affected.

DHS strongly recommends actively contacting your IT team, antivirus vendor, managed service provider, and/or point of sale system vendor to assess whether your assets may be vulnerable and/or compromised. The Secret Service is active in contacting impacted businesses, as they are identified, and continues to work with and support those businesses that have been impacted by this PoS malware. Companies that believe they have been the victim of this malware should contact their local Secret Service field office and may contact the NCCIC for additional information.

Points of Contact

For all inquiries pertaining to this product, please contact the NCCIC Duty Officer at NCCIC@hq.dhs.gov or (888) 282-0870. To report an incident, contact US-CERT at soc@us-cert.gov or visit: <http://www.us-cert.gov>.

To report suspected cybercrimes, to include network intrusions or use of malware, contact your local U.S. Secret Service Field Office, Electronic Crimes Task Force (ECTF), or the Secret Service toll free number at (877) 242-3375. Victims of cybercrimes may have evidence important to ongoing investigations or to the eventual prosecution of cyber criminals.

DISCLAIMER: This advisory is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any the information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is marked TLP: WHITE. Recipients may share TLP: WHITE information with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information about TLP, see <http://www.us-cert.gov/tlp>.