ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Joint Security Awareness Report

JSAR-12-241-01—Shamoon/DistTrack Malware

August 29, 2012

OVERVIEW

W32.DistTrack, also known as "Shamoon," is an information-stealing malware that also includes a destructive module. Shamoon renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data. Once overwritten, the data are not recoverable.

Based on initial reporting and analysis of the malware, no evidence exists that Shamoon specifically targets industrial control systems (ICSs) components or U.S. government agencies.

According to Symantec,[a] Shamoon has three primary functional components:

1. Dropper—the main component and source of the original infection. It installs a number of other modules.
2. Wiper—this module is responsible for the destructive functionality of the malware.
3. Reporter—this module is responsible for reporting infection information back to the attacker.

After the initial infection, Shamoon spreads via network shares to infect additional machines on the network. Symantec first detected Shamoon on August 16, 2012, and estimates only few infections exist worldwide (less than 50).[b]

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT and US-CERT for tracking and correlation against other incidents.

IMPACT

Because of the highly destructive functionality of the Shamoon "Wiper" module, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP) and disruption of critical systems. Actual impact to organizations vary, depending on the type and number of systems impacted.

a. http://www.symantec.com/connect/blogs/shamoon-attacks, Web site last accessed August 28, 2012.
b. http://www.symantec.com/security_response/writeup.jsp?docid=2012-081608-0202-99&om_rssid=sr-mixed30days, Web site last accessed August 28, 2012.

MITIGATION

ICS-CERT and US-CERT encourage organizations to:

- Update antivirus definitions for detection of the Shamoon (DistTrack) malware.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Exercise caution when using removable media, including USB drives.[c]
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[d]
- Place control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT and US-CERT remind organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

ICS-CERT recommends that organizations review the ICS-CERT Technical Information Paper ICS-TIP-12-146-01 Cyber Intrusion Mitigation Strategies[e] for high-level strategies that can improve overall visibility of a cyber intrusion and aid in recovery efforts should an incident occur.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[f]

c. Using Caution with USB Drives, http://www.us-cert.gov/cas/tips/ST08-001.html, Web site last accessed August 28, 2012.

d. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, Web site last accessed August 28, 2012.

e. ICS-CERT TIP – Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed August 28, 2012.

f. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 28, 2012.

CONTACT INFORMATION

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov
US-CERT Voice: 1-888-282-0870
ICS-CERT Watch Floor: 877-776-7585
Incident Reporting Form: https://forms.us-cert.gov/report/

DOCUMENT FAQ

What is a JSAR Advisory? A JSAR Advisory is a Joint Security Advisory intended to provide awareness or solicit feedback from critical infrastructure owners, integrators, peers and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

May I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. All comments or questions related to this document should be directed to either ICS-CERT or US-CERT at:
ICS-CERT: ics-cert@dhs.gov

US-CERT: soc@us-cert.gov