ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Joint Security Awareness Report

JSAR-12-222-01—Gauss Information-Stealing Malware

August 9, 2012

OVERVIEW

On August 9, 2012, Kaspersky Lab released a report[a] on a new information-stealing malware they have named "Gauss." According to the report, Gauss is designed to collect information and send the data to its command-and-control servers.

Kaspersky has detected Gauss predominantly on systems in Lebanon, the Palestinian Territories, and Israel. Gauss has also been detected on a limited number of networks in the U.S.; however, the impact to these systems is currently unknown. Based on initial reporting and analysis of Gauss, no evidence exists that Gauss targets industrial control systems (ICS) or U.S. government agencies.

According to Kaspersky, information is collected by Gauss using various modules and has the following functionality:

- injecting its own modules into different browsers in order to intercept user sessions and steal passwords, cookies, and browser history,
- collecting information about the computer's network connections,
- collecting information about processes and folders,
- collecting information about BIOS and CMOS RAM,
- collecting information about local, network and removable drives,
- infecting removable media drives with an information-stealing module in order to steal information from other computers,
- installing the custom "Palida Narrow" font (purpose unknown),
- ensuring the entire toolkit's loading and operation, and
- interacting with the command and control server, sending the information collected to it, and downloading additional modules.

a. http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution

Kaspersky's analysis indicates that Gauss has a number of similarities to Duqu, Flame, and Stuxnet. The USB device information-stealing module exploits a known ".LNK" vulnerability (CVE-2010-2568[b]), the same vulnerability exploited by Stuxnet. According to the report, the USB module also includes an encrypted payload that has unknown functionality. Both ICS-CERT and US-CERT are evaluating the malware to understand the full functionality and will report updates as needed.

MITIGATION

At this time, no specific mitigations are available; however, several indicators associated with Gauss have been published in Kaspersky's report. Organizations should consider taking defensive measures using the available indicators where practical.

In addition to leveraging the available indicators for defensive purposes, ICS-CERT and US-CERT encourage organizations to:

- Exercise caution when using removable media, including USB drives, in order to prevent the spread of Gauss.[c]
- Apply Windows Updates to patch CVE-2010-2568.[d]
- Update antivirus definitions for detection of the Gauss malware.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[e]
- Locate 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[f] for high-level strategies that can

---

b. CVE ID- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568, Web site last accessed Aug 9, 2012.

c. Using Caution with USB Drives, http://www.us-cert.gov/cas/tips/ST08-001.html, Web site last accessed August 9, 2012.

d. Microsoft Security Advisory (2286198), http://technet.microsoft.com/en-us/security/advisory/2286198, Web site last accessed August 9, 2012.

e. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, Web site last accessed August 9, 2012.

f. ICS-CERT TIP—Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01.pdf, Web site last accessed August 9, 2012.

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.[g]

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.

ICS-CERT or US-CERT CONTACT INFORMATION

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

E-mail: 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:

E-mail: 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

g. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed August 9, 2012.