ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

# Joint Security Awareness Report

# JSAR-12-151-01—sKyWIper/Flame Information-Stealing Malware

May 30, 2012

## OVERVIEW

On May 28, 2012, the Laboratory of Cryptography and Systems Security (CrySyS) located at the Budapest University of Technology and Economics, Department of Telecommunications, released a report[a] on a new sophisticated information-stealing malware they have identified as sKyWIper. Various other sources also refer to this malware as “Flame” and “Flamer.”

Due to the size and complexity of the malware, comparisons have been drawn to Stuxnet and Duqu malware. However, initial analysis by the CrySyS team indicates that sKyWIper has few similarities when compared to Duqu and Stuxnet. At this time, insufficient data exists to conclude that sKyWIper is related to Duqu or Stuxnet, or produced by the same author.

According to the report, sKyWIper uses a modular structure incorporating multiple propagation and attack techniques. The malware is reported to be complex and sophisticated using multiple compression and encryption techniques, multiple file formats, and special code injection techniques. This malware is a comprehensive toolkit that creates a backdoor on the infected machine, contains worm-like features allowing it to spread throughout the network, and has the ability to proliferate through removable media or malicious links and email attachments. sKyWIper has the ability to sniff network traffic, take screenshots, record audio via an installed microphone, record keystrokes, and conduct other monitoring activities.

Based on initial reporting and analysis of this malware, no evidence exists that sKyWIper specifically targets industrial control systems (ICS). Both ICS-CERT and US-CERT are evaluating the malware and will report updates as needed.

Currently, neither ICS-CERT nor US-CERT have received any reports of affected entities and are not aware of any sKyWIper malware infections in the United States.

[a] sKyWIper:A complex malware for targeted attacks, http://www.crysys.hu/skywiper/skywiper.pdf, Web site last accessed May 30, 2012.

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

## MITIGATION

The full extent of the threat posed by sKyWIper is currently being evaluated. At this time, no specific mitigations are available; however, organizations should consider taking defensive measures against this threat. Specifically, ICS-CERT and US-CERT encourage organizations to:

- Update antivirus definitions for detection of the sKyWIper/Flame malware.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[b]
- 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[c] 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.[d]

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

[b] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, web site last accessed May 28, 2012.

[c] 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 May 28, 2012.

[d] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, web site last accessed May 28, 2012.

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