ICS-CERT
Industrial Control Systems
Cyber Emergency Response Team

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Joint Security Awareness Report

JSAR-12-151-01A—(UPDATE) sKyWIper/Flame Information-Stealing Malware

UPDATE A

June 5, 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.”

--------- Begin Update A Part 1 of 1 --------

The sKyWIper malware uses a new cryptographic collision attack in combination with the terminal server licensing service certificates to sign code as if it came from Microsoft. However, code-signing without performing a collision is also possible. This is an avenue for compromise that may be used by additional attackers on systems not originally the focus of the sKyWIper malware. In all cases, Windows Update can only be spoofed with an unauthorized certificate combined with a man-in-the-middle attack. This issue affects all supported releases of Microsoft Windows.

On June 3, 2012, Microsoft published Security Advisory 2718704[b] Unauthorized Digital Certificates Could Allow Spoofing. Microsoft recommends that users apply this update immediately using update management software or by checking for updates using the Microsoft Update service. For more information, see the Suggested Actions section of the Microsoft Security Advisory.

ICS-CERT and US-CERT recommend that industrial control systems owners and operators review the Microsoft Advisory and work with equipment vendors to install this update. Control

[a] sKyWIper: A complex malware for targeted attacks, http://www.crysys.hu/skywiper/skywiper.pdf, Web site last accessed June 05, 2012.

[b] Microsoft Security Advisory, http://technet.microsoft.com/en-us/security/advisory/2718704, Website last accessed June 05, 2012.

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

systems asset owners are reminded to perform proper impact analysis and risk assessment prior to taking defensive measures.

--------- End Update A Part 1 of 1 --------

Because of the size and complexity of this 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 exist 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. 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.

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.[c]
- 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.

[c] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, web site last accessed June 05, 2012.

ICS-CERT recommends that organizations review the ICS-CERT Technical Information Paper ICS-TIP-12-146-01 Cyber Intrusion Mitigation Strategies[d] 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.[e]

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 AND US-CERT 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:

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

[d] 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 June 05, 2012.

[e] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 05, 2012.