Ukraine Cyber Attack:
Implications for US Stakeholders

Unclassified Threat Briefing Campaign

OVERVIEW and PURPOSE

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been actively working with the government of Ukraine and other U.S. Federal Government entities to understand the December 23, 2015 attacks against Ukrainian power infrastructure. These events represent one of the first known physical impacts to critical infrastructure which resulted from cyber-attack. The attacks leveraged commonly available tools and tactics against the control systems which could be used against infrastructure in every sector.

To increase awareness of the threat and provide additional context for the events in late 2015, ICS-CERT and the FBI will conduct unclassified in-person briefings as well as online webinars for asset owners and supporting personnel. The briefing sessions will provide details about the events surrounding the attack, techniques used by the threat actors, and strategies for mitigating risks and improving an organization's cyber defensive posture. In the interim, technical details and mitigation strategies about this attack have been released in various products produced by ICS-CERT and are immediately available for network defense. Links to these products are included below.

SESSION CONTENT

The briefings will include analysis of the attack timeline and threat vector, identifying critical tactics, techniques, and procedures (TTPs) as well as mitigation strategies. The focus of the briefing will be on applying the lessons learned from the Ukraine attack to U.S. Critical Infrastructure. The strategies presented are appropriate for all sectors, and should not be limited to energy-related organizations. The briefings will highlight:

- Context and detailed information about the cyber-attacks against Ukrainian infrastructure that resulted in physical impact for three Ukrainian companies and additional attacks against three other companies that did not have physical impact.
- The role and impact of BlackEnergy malware in the attacks, as understood by the U.S. Government.
- Discussion about the TTPs used as part of the attack.
- Detailed mitigations strategies for detecting, preventing and/or responding to a similar attack against U.S. Critical Infrastructure.

REGISTRATION

If you would like to attend an in-person session or webinar, please register online at the link below. Attendance is limited and approval will be based on association to critical infrastructure. As guidance, only asset owners, supporting organizations, ICS vendors, and government personnel will be allowed to attend. Additional details regarding the location of the briefing will be emailed with the confirmation of your registration.

- Registration available at: https://secure.inl.gov/ics-cert-briefing/?campaignName=Ukraine Cyber Attack.
- Please retain a copy of your registration confirmation to ensure entry to in-person briefings.
- Online webinars will be conducted using the HSIN network. Please confirm that you can successfully connect to the technology prior to the event. Details will be provided in the approval email.
- All future communications will come from ics-cert.events@dhs.gov or csoc@inl.gov. Please ensure these emails are included on your safe senders list.

WEBINARS

Online webinars will be held on the following dates and times:

DATE	Time
March 31, 2016	2:00 pm - 3:00 pm EDT
April 5, 2016	11:00 am - 12:00 pm EDT
April 14, 2016	3:00 pm - 4:00 pm EDT
April 28, 2016	11:00 am - 12:00 pm EDT

IN-PERSON BRIEFINGS

Dates and cities have been listed below for the unclassified briefings. The content of the briefing is very similar to that of the webinar. Some of the sessions will also offer a hands-on simulation of the attack using actual ICS equipment.

Date	Local Time	City	Presentation Format
April 12, 2016	10:00 am - 12:00 pm EDT	Washington, DC	Briefing and Simulation
April 14, 2016	9:00 am - 10:00 am CDT	Kansas City, MO	Briefing Only
April 18, 2016	10:00 am - 11:00 am EDT	New York, NY	Briefing Only
April 19, 2016	10:30 am - 11:30 am CDT	Houston, TX	Briefing Only
April 22, 2106	10:00 am - 12:00 pm EDT	Atlanta, GA	Briefing and Simulation
April 25, 2016	10:00 am - 11:00 am CDT	Chicago, IL	Briefing Only
April 27, 2016	10:00 am - 11:00 am MDT	Denver, CO	Briefing Only
April 29, 2016	10:30 am - 11:30 am PDT	Los Angeles, CA	Briefing Only

Please see the website for registration deadlines for each event. All attendees of the webinar or in-person briefings must register prior to the event.

IMMEDIATE ACTIONABLE INFORMATION

The technical details of these two campaigns have been released in various products produced by ICS-CERT and are immediately available for network defense. These alerts contain indicators such as IPs, Domains, Hashes, YARA rules, and detailed malware information that can be used for immediate network defense and detection.

US-CERT Portal Alerts (limited access)

Alert (IR-ALERT-H-16-043-01P) Ukrainian Power Outage Event
Alert (ICS-ALERT-16-013-01P) BlackEnergy 3 Malware
Alert (ICS-ALERT-14-281-01DP) Ongoing Sophisticated Malware Campaign Compromising ICS

ICS-CERT Website Alert

Alert (IR-ALERT-H-16-056-01) Cyber Attack Against Ukrainian Critical Infrastructure

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

ICS-CERT Operations Center
Toll Free: 1-877-776-7585
International: 1-208-526-0900
Email: ics-cert@hq.dhs.gov