ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

SUMMARY

On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. In addition, there have also been reports of malware found in Ukrainian companies in a variety of critical infrastructure sectors. Public reports indicate that the BlackEnergy (BE) malware was discovered on the companies' computer networks, however it is important to note that the role of BE in this event remains unknown pending further technical analysis.

An interagency team comprised of representatives from the National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), U.S. Computer Emergency Readiness Team (US-CERT), Department of Energy, Federal Bureau of Investigation, and the North American Electric Reliability Corporation traveled to Ukraine to collaborate and gain more insight. The Ukrainian government worked closely and openly with the U.S. team and shared information to help prevent future cyber-attacks.

This report provides an account of the events that took place based on interviews with company personnel. This report is being shared for situational awareness and network defense purposes. ICS-CERT strongly encourages organizations across all sectors to review and employ the mitigation strategies listed below.

Additional information on this incident including technical indicators can be found in the TLP GREEN alert (IR-ALERT-H-16-043-01P and subsequent updates) that was released to the US-CERT secure portal. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

DETAILS

The following account of events is based on the interagency team's interviews with operations and information technology staff and leadership at six Ukrainian organizations with first-hand experience of the event. Following these discussions and interviews, the team assesses that the outages experienced on December 23, 2015, were caused by external cyber-attackers. The team was not able to independently review technical evidence of the cyber-attack; however, a significant number of independent reports from the team's interviews as well as documentary findings corroborate the events as outlined below.

Through interviews with impacted entities, the team learned that power outages were caused by remote cyber intrusions at three regional electric power distribution companies (Oblenergos) impacting approximately 225,000 customers. While power has been restored, all the impacted Oblenergos continue to run under constrained operations. In addition, three other organizations, some from other critical infrastructure sectors, were also intruded upon but did not experience operational impacts

The cyber-attack was reportedly synchronized and coordinated, probably following extensive reconnaissance of the victim networks. According to company personnel, the cyber-attacks at each company occurred within 30 minutes of each other and impacted multiple central and regional facilities. During the cyber-attacks, malicious remote operation of the breakers was conducted by multiple external humans using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. The companies believe that the actors acquired legitimate credentials prior to the cyber-attack to facilitate remote access.

All three companies indicated that the actors wiped some systems by executing the KillDisk malware at the conclusion of the cyber-attack. The KillDisk malware erases selected files on target systems and corrupts the master boot record, rendering systems inoperable. It was further reported that in at least one instance, Windows-based human-machine interfaces (HMIs) embedded in remote terminal units were also overwritten with KillDisk. The actors also rendered Serial-to-Ethernet devices at substations inoperable by corrupting their firmware. In addition, the actors reportedly scheduled disconnects for server Uninterruptable Power Supplies (UPS) via the UPS remote management interface. The team assesses that these actions were done in an attempt to interfere with expected restoration efforts.

Each company also reported that they had been infected with BlackEnergy malware however we do not know whether the malware played a role in the cyber-attacks. The malware was reportedly delivered via spear phishing emails with malicious Microsoft Office attachments. It is suspected that BlackEnergy may have been used as an initial access vector to acquire legitimate credentials; however, this information is still being evaluated. It is important to underscore that any remote access Trojan could have been used and none of BlackEnergy's specific capabilities were reportedly leveraged.

MITIGATION

The first, most important step in cybersecurity is implementation of information resources management best practices. Key examples include: procurement and licensing of trusted hardware and software systems; knowing who and what is on your network through hardware and software asset management automation; on time patching of systems; and strategic technology refresh.

Organizations should develop and exercise contingency plans that allow for the safe operation or shutdown of operational processes in the event that their ICS is breached. These plans should include the assumption that the ICS is actively working counter to the safe operation of the process.

ICS-CERT recommends that asset owners take defensive measures by leveraging best practices to minimize the risk from similar malicious cyber activity.

Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by malicious actors. The static nature of some systems, such as database servers and HMI computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.[a]
Organizations should isolate ICS networks from any untrusted networks, especially the Internet. All unused ports should be locked down and all unused services turned off. If a defined business requirement or control function exists, only allow real-time connectivity to external networks. If one-way communication can accomplish a task, use optical separation ("data diode"). If bidirectional communication is necessary, then use a single open port over a restricted network path.[a]
Organizations should also limit Remote Access functionality wherever possible. Modems are especially insecure. Users should implement "monitoring only" access that is enforced by data diodes, and do not rely on "read only" access enforced by software configurations or permissions. Remote persistent vendor connections should not be allowed into the control network. Remote access should be operator controlled, time limited, and procedurally similar to "lock out, tag out." The same remote access paths for vendor and employee connections can be used; however, double standards should not be allowed. Strong multi-factor authentication should be used if possible, avoiding schemes where both tokens are similar types and can be easily stolen (e.g., password and soft certificate).[a]

As in common networking environments, control system domains can be subject to a myriad of vulnerabilities that can provide malicious actors with a "backdoor" to gain unauthorized access. Often, backdoors are simple shortcomings in the architecture perimeter, or embedded capabilities that are forgotten, unnoticed, or simply disregarded. Malicious actors often do not require physical access to a domain to gain access to it and will usually leverage any discovered access functionality. Modern networks, especially those in the control systems arena, often have inherent capabilities that are deployed without sufficient security analysis and can provide access to malicious actors once they are discovered. These backdoors can be accidentally created in various places on the network, but it is the network perimeter that is of greatest concern.

When looking at network perimeter components, the modern IT architecture will have technologies to provide for robust remote access. These technologies often include firewalls, public facing services, and wireless access. Each technology will allow enhanced communications in and amongst affiliated networks and will often be a subsystem of a much larger and more complex information infrastructure. However, each of these components can (and often do) have associated security vulnerabilities that an adversary will try to detect and leverage. Interconnected networks are particularly attractive to a malicious actor, because a single point of compromise may provide extended access because of pre-existing trust established among interconnected resources.[b]

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

ICS-CERT also provides a recommended practices section for control systems on the ICS-CERT web site (http://ics-cert.us-cert.gov). Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies and Seven Steps to Effectively Defend Industrial Control Systems.

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

For more information on securely working with dangerous malware, please see US-CERT Security Tip ST13-003 Handling Destructive Malware at https://www.us-cert.gov/ncas/tips/ST13-003 .

DETECTION

While the role of BlackEnergy in this incident is still being evaluated, the malware was reported to be present on several systems. Detection of the BlackEnergy malware should be conducted using the latest published YARA signature. This can be found at: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01E. Additional information about using YARA signatures can be found in the May/June 2015 ICS-CERT Monitor available at: https://ics-cert.us-cert.gov/monitors/ICS-MM201506.

Additional information on this incident including technical indicators can be found in the TLP GREEN alert (IR-ALERT-H-16-043-01P and subsequent updates) that was released to the US-CERT secure portal. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov(link sends e-mail).

- a.NCCIC/ICS-CERT, Seven Steps to Effectively Defend Industrial Control Systems, https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-C..., web site last accessed February 25, 2016.
- b.NCCIC/ICS-CERT, Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/D... , web site last accessed February 25, 2016.