Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

NCCIC/ICS-CERT INCIDENT ALERT

IR-ALERT-H-16-043-01AP CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE

UPDATE A

March 7, 2016

ALERT

SUMMARY

This alert update is a follow-up to the original NCCIC/ICS-CERT Alert titled IR-ALERT-H-16-043-01P Ukrainian Power Outage Event that was published February 12, 2016, on the US-CERT secure Portal library.

--------- Begin Update A Part 1 of 2 --------

On December 23, 2015, Ukrainian power companies (Oblenergos) experienced an unprecedented cyber-attack causing power outages, which impacted over 225,000 customers in Ukraine. These attacks were conducted by remote cyber-attackers who, leveraging legitimate credentials obtained via unknown means, remotely operated breakers to disconnect power. 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. There have been public reports that indicate BlackEnergy (BE) malware was responsible for the attack. However, National Cybersecurity and Communications Integration Center (NCCIC)/Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) does not have sufficient supporting evidence to confirm the role of BE but continues to conduct further analysis. If BE played a role, it was most likely in the reconnaissance and preparatory phases, not during the actual attack. Many malware implants could have conducted this activity.

This incident highlights the urgent need for critical infrastructure owners and operators across all sectors to implement enhanced cyber measures that reduce risks from the following types of adversary techniques:

- Theft of legitimate user credentials to enable access masquerading as approved users,
- Leveraging legitimate remote access pathways (VPNs),
- The remote operation of human-machine interface (HMI) via company installed remote access software (such as RDP, TeamViewer or rlogin)
- The use of destructive malware such as KillDisk to disable industrial control systems (ICSs) and corporate network systems
- Firmware overwrites that disable/destroy field equipment
- Unauthorized scheduled disconnects of uninterruptable power supplies (UPS) to devices to deny their availability
- The delivery of malware via spear-phishing emails and the use of malicious Microsoft Office attachments
- Use of Telephone Denial of Service (TDoS) to disrupt operations and restoration.

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 and detection mechanisms contained within this report.

DETAILS

An interagency team composed of representatives from the NCCIC/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.

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. 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 Ukraine experienced on December 23, 2015, were caused by remote cyber-attacks 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 team assesses that the attacks against the Oblenergos demonstrated some Tactics, Techniques, and Procedures (TTPs) that, while previously known, have not been previously observed in an actual cyber-attack. The cyber-attacks were reportedly synchronized and coordinated, probably following extensive reconnaissance of the victim networks.

After gaining a foothold in the victim networks, attackers acquired legitimate credentials and leveraged valid remote access pathways to conduct their attack. The physical impact events of the cyber-attacks launched within 30 minutes of each other, impacting multiple central and regional facilities. Over 50 regional substations experienced malicious remote operation of their breakers conducted by multiple external humans. This was done using either existing remote administration tools at the operating system level or remote ICS client software via virtual private network (VPN) connections.

All three impacted 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 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 interrupted power to some data centers through scheduled power outages on server UPS via the remote management interface. The team assesses that these actions were done in an attempt to interfere with expected restoration efforts.

Initial intrusion appears to have been through malware, which was delivered via spear-phishing emails with malicious Microsoft Office attachments. While it has not been confirmed with technical artifacts, it is probable that the two events are related. While the cyber-attack has been widely attributed to BE in the open press, any remote access trojan could have been used in these attacks, and none of BE's unique capabilities were leveraged. At this time, no definitive link can be drawn between the outage and the presence of the BE malware, however analysis is ongoing.

TACTICS, TECHNIQUES, AND PROCEDURES (TTP)

According to reports and reviewed artifacts, the primary access pathway was the use of legitimate remote access pathways such as VPN to access local systems. The ICSs were accessed with the use of compromised legitimate credentials or accounts that the adversaries created in company networks. The exact nature of the credential harvesting remains unknown. It is likely that the credentials were obtained well ahead of the December 23, 2015, event.

Most breakers were tripped when remote human operators accessed the dispatcher workstations and remotely took control of the terminals using legitimately installed remote access tools. The functionality of these tools were similar to Remote Desktop Protocol (RDP) and RAdmin. Local operators were locked out of their own workstations, disabling keyboard and mouse control. However, they could observe attacker actions on their screens.

Some of the breakers were tripped when remote human attackers remotely commanded them to open via a properly configured Distribution Management System (DMS) client application sending commands directly to the DMS server via the VPN.

In multiple cases, the attackers changed passwords for key systems. This resulted in legitimate users being unable to access the systems during the recovery process.

Near the conclusion of the attack, the attackers corrupted the firmware of some of the serial-to-Ethernet converters employed for substation communications and some network routers. The firmware overwrite was neither recoverable in the field or by the manufacturer necessitating the replacement of the device. Impacted devices were the Moxa UC 7408-LX-Plus and the IRZ-RUH2 3G. However, there are many devices susceptible to these types of malicious firmware corruptions. The exact mechanism of this firmware corruption is unknown; however, both devices allow authorized users to remotely update the firmware. It is possible that the attackers gained these credentials, as they gained other legitimate credentials in the system, and used them to push invalid firmware to the devices.

All three companies indicated that attackers wiped targeted systems by executing the KillDisk malware at the conclusion of the attack. The KillDisk malware erased selected files on target systems and corrupted the master boot record, rendering systems inoperable. KillDisk was not executed against every system in the environment; however, management, HR, finance, and ICS operations staff and servers were targeted. There have been unconfirmed reports that the BE malware was used to download and launch the KillDisk malware.

It was further reported that in at least one instance, a Remote Terminal Unit (RTU) product with an embedded Windows HMI card (ABB RTU 560 CMU-02 - PLC Daughter Card) was overwritten with KillDisk.

In multiple cases, one of the first actions taken by the attacker was to schedule an unauthorized power outage on supporting UPS devices. In one instance, an internal telephone communications server was targeted effectively cutting off all internal communications with regional offices and distribution substations. At a different company, 30 minutes prior to the first unauthorized breaker operation, the actor used the local UPS to schedule a power shutdown of the main

datacenter to occur several hours later. In addition to standard consequences of power loss, a reboot caused the full impact of the KillDisk efforts to take effect.

In one case, a TDoS was reported during the time of the attacks against a company call center. This TDoS impacted customer outage reporting as well as internal company coordination in response to the incident.

Multiple rounds of spear phishing starting as early as March 2015 and as recently as January 20, 2016, with MS Office attachments and generally popular topics were observed. These spear-phishing emails dropped a variety of malware artifacts but primarily dropped BE variants. The role and connection between this spear phishing and the outage is unclear. If connected, it may have been a vector for initial recognizance and information gathering. There are also reports of the installation of backdoors such as GCat, DropBear, and Kryptik.

ICS-CERT assesses that these destructive actions (firmware overwrites, KillDisk, etc.) were done in an attempt to interfere with expected restoration efforts.

MITIGATION

It is the assessment of ICS-CERT that critical infrastructure ICS networks, across multiple sectors, are vulnerable to similar attacks. Asset owners should take proactive steps to prevent similar attacks from impacting their own systems. There are a number of mitigations suggested to address these risks, as follow:

- Contingency planning for active participation of ICS against the safe operation of the process,
- Limiting remote access,
- Network and credential monitoring,
- Multifactor authentication,
- Firmware driver signing,
- Network architecture documentation and planning,
- Application Whitelisting,
- Backdoor detection and alerting, and
- Contingency planning for TDoS.

Organizations should develop and exercise contingency plans that allow for the safe operation and/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. While the Ukrainian companies did not have such a plan prepared, their experience with manual operation of their distribution systems allowed them to quickly recover. As US infrastructure is generally more reliant on automation, a comprehensive plan is needed to ensure safe operation or shutdown of processes under this condition.

Organizations should isolate ICS networks from any untrusted networks, especially the Internet. All unused protocol ports should be locked down and all unused services turned off. Only allow real-time connectivity to external networks if a defined business requirement or control function exists. 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. By establishing separate credentials for each network, as well as preventing data flow between the business network and the control system network, attackers are prevented from leveraging information gained from a successful compromise of the enterprise against the control system. Separating these networks results in attackers being prevented from pivoting through the generally weaker and more chaotic business network. By using different authentication systems on each network, attackers cannot reuse compromised credentials found on enterprise systems on control system networks. Additional information about implementing this high-level architecture can be found in the ICS-CERT document "Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies" (https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf).

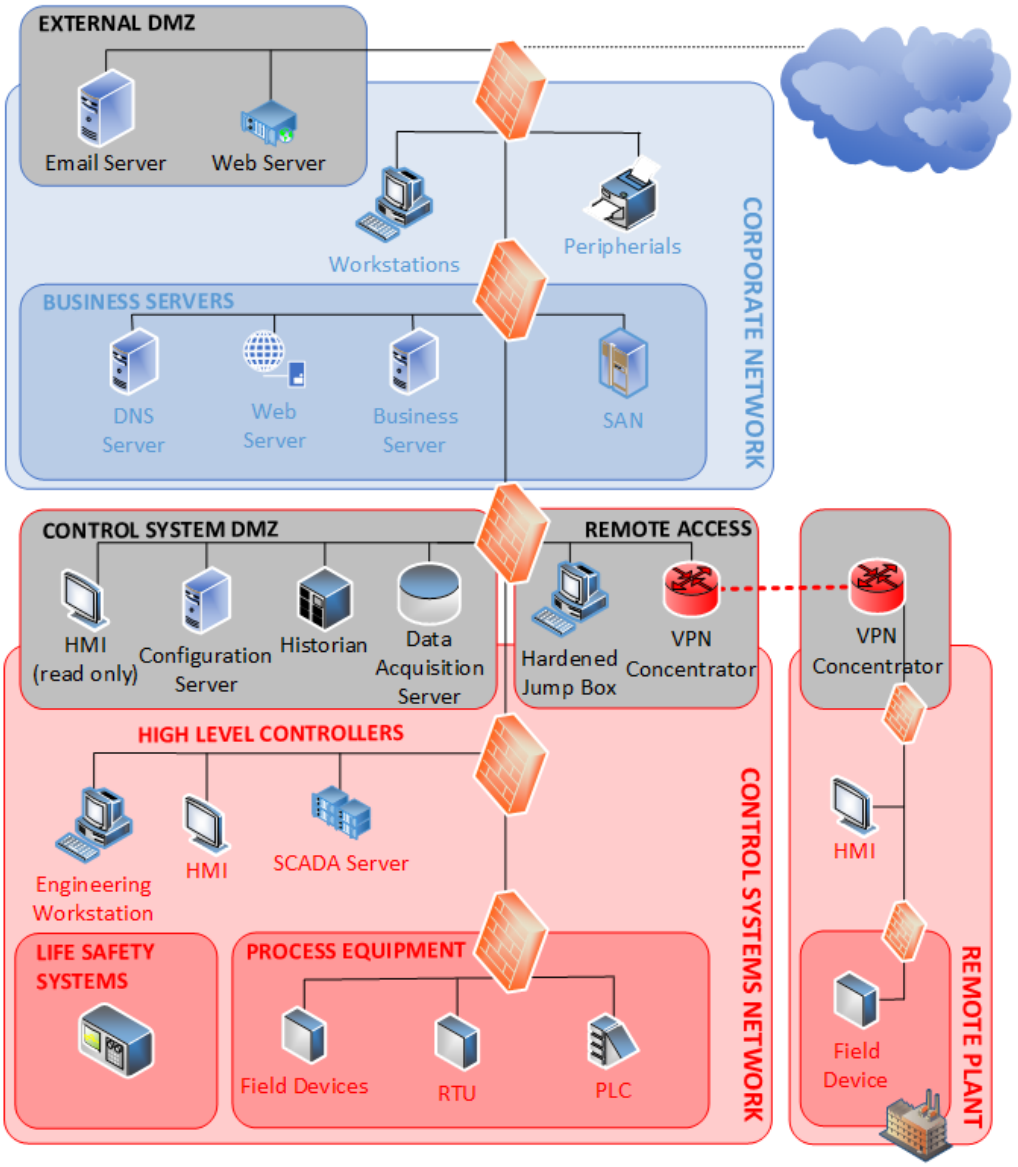

Figure 1: Ideal ICS Network Configuration

Organizations should limit remote access functionality wherever possible. Modems are especially insecure. Users should implement "monitoring only" access that is enforced by data diodes, and not rely on "read only" access enforced by software configurations or permissions.

Remote persistent vendor connections should not be allowed into the control system 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.

Credential monitoring should be used to identify compromised credentials being used by unauthorized attackers. Had credential monitoring been in place during the attack, it is plausible that the attackers' behavior would have been detected while in the reconnaissance phase. As an example, in one case the attackers' first action was creating new unauthorized domain accounts and granting them certain privileges. Had this been monitored, it would have alerted system administrators weeks prior to the attack. By identifying unusual events in network traffic and/or credential usage, there is a significantly increased probability that network defenders will identify initial intrusions attacks during the reconnaissance phase, prior to any damage occurring.

When looking at network perimeter components, the modern IT architecture will have technologies to provide for robust remote access. These technologies often include firewalls, externally facing interfaces, 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 exploit. Interconnected networks are particularly attractive to a malicious actor, because a single point of compromise may provide extended access due to the pre-existing trust established among interconnected resources.[a]

Only one of the six companies was following ICS-CERT's recommended practices for monitoring industrial control systems networks. (The outlying company was not one of the three which experienced physical impacts.) Because of the more constrained nature of control system networks, and due to the limited number of protocols being used, ICSs networks are generally easier to monitor and detect anomalous network traffic. It is recommended that administrators develop a trusted profile of their network traffic and then use this as a baseline to identify unexpected events. Of special attention to ICS networks, traffic from IP addresses other than expected devices and unusual behaviors such as events occurring during unusual times can be of especially significant value.

Requiring signed drivers and validating these signatures provides a significant layer of protection from malicious drivers as well as firmware overwrites as was seen in Ukraine. This technology prevents tampered drivers from being loaded on devices, and alerts to malicious activity on a

a. NCCIC/ICS-CERT, Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf , Web site last accessed March 7, 2016.

network. While implementing these measures requires participation by both the equipment vendor and the asset owner, users should leverage this technology where available and consider appropriate procurement requirements when acquiring new equipment.

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.[b] Alerts should be established when applications commonly used in cyber-attacks are attempted to be loaded on any system. Pertaining to this incident and assuming that the spear-phishing emails were the recon component of the attack, had AWL been in place when the BE, DropBear GCat, or other malware attempted to execute; it would have been stopped by the AWL solution. Even if these were not detected, the KillDisk malware was executed as a separate binary and, therefore, would have been prevented from running by AWL limiting the damage.

Strong multi-factor authentication should be used whenever possible, ensuring tokens are different categories (something you know, something you have, something you are, etc.) and cannot be easily stolen together (e.g., password and soft certificate). Evidence was found in Ukraine that demonstrated the weakness of single-factor authentication. While not a complete solution on its own, implementing multi-factor authentication, especially on externally facing connections, presents significant obstacles for attackers. In addition, access logs should be carefully monitored and appropriately alerted. Intrusion detection systems should be trained to recognize anomalies to normal behavior, and notify upon unusual events, such as local accounts being used to access systems from remote IP addresses.

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 will leverage any discovered access functionality to gain remote access to a domain. Modern networks, especially those in the control systems arena, often have inherent capabilities that are deployed without sufficient security analysis and can provide malicious actors access through undocumented channels. These backdoors can be accidentally created in various places on the network, but the network perimeter is of greatest concern. Regular architecture reviews, passive and active penetration testing, and network traffic monitoring can all help to identify these backdoors.

b. NCCIC/ICS-CERT, Seven Steps to Effectively Defend Industrial Control Systems, https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems, web site last accessed March 7, 2016.

TDoS attacks occur when perpetrators deliver a flood of telephone calls to an organization's telephone system disrupting normal operations. Ukraine experienced a TDoS as part of the recent cyber-attacks, disrupting their ability to interface with their customers as well as communicate internally. While TDoS attacks are difficult to mitigate, organizations should be prepared on how they would respond to such an event. Upstream telephony service providers may be able to provide technical controls which lessen the impacts. Consideration should be given on how appropriate logging and voice recordings will be captured for forensic review.

Accurate and detailed network documentation is critical to the mitigations above. Organizations must understand the network architecture of their ICS networks, including internal communications, ingress and egress points, and interdependencies. This documentation should be validated through regular administrative and technical assessments.

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

ICS-CERT 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 BE in this incident is still being evaluated, the malware was reported to be present on several systems. Detection of BE 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.

--------- End Update A Part 1 of 2 ----------

Indicator	Type
mail.baggins.biz	Domain
mx01.24.7h.com	Domain
SRV-EXMB01.kpb.ua	Domain
Received: from SRV-EXMB01.kbp.ua (10.1.1.63) by SRV-EXMB01.kbp.ua (10.1.1.63) with Microsoft SMTP Server (TLS) id 15.0.712.22 via MailboxTransport; Wed, 4 Mar 2015 18:59:59 +0000 Received: from SRV-EXCA02.kbp.ua (10.1.1.75) by srv-exmb01.kbp.ua (10.1.1.63) with Microsoft SMTP Server (TLS) id 15.0.712.22; Wed, 4 Mar 2015 18:59:57 +0000 Received: from [subdomain].[domain].[tld] (X.X.X.X) by SRV-EXCA02.kbp.ua (10.1.1.76) with Microsoft SMTP Server id 15.0.712.22 via Frontend Transport; Wed, 4 Mar 2015 18:59:57 +0000 X-IronPort-Anti-Spam-Filtered: true X-IronPort-Anti-Spam-Result: A0CeBACIVfdU/0P4lQXOEgECAgE X-IPAS-Result: A0CeBACIVfdU/0P4lQXOEgECAgE X-IronPort-AV: E=Sophos;i="5.09,689,1418083200"; d="pps'32,48?mf'32,48?exe'32,48,96?scan'32,48,96,32,96,48,208,245,217";a="574775" Received: from mail.baggins.biz ([xxx.xxx.xxx.xxx]) by [subdomain].[domain].[tld] with SMTP; 04 Mar 2015 18:59:53 +0000	Email Header Information
146.0.74.7	IP Address
148.251.82.21	IP Address

Indicator	Type
176.53.127.194	IP Address
188.40.8.72	IP Address
31.210.111.154	IP Address
41.77.136.250	IP Address
62.210.188.110	IP Address
78.108.190.20	IP Address
C:\Users\{user}\AppData\Local_FONTCACHE.DAT	Malicious File location
c:\Users\{user}\AppData\Local\FONTCACHE.DAT	Malicious File location
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\flashplayer.exe	Malicious File location
C:\Users\{user}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\flashplayerapp.exe	Malicious File location
C:\Windows\System32\drivers\acpipmi.sys	Malicious File location
c:\windows\system32\drivers\adpu320.sys	Malicious File location
c:\windows\system32\drivers\adpu320.sys (BlackEnergy)	Malicious File location
C:\WINDOWS\Temp\Dropbear	Malicious File location
148.25182.21/Microsoft/Update/KS4567890.php	Malicious URL
188.40.8.72/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php	Malicious URL
xxx.xxx.xxx.xxx/Microsoft/Update/KS1945777.php	Malicious URL
hxxp://xxx.xxx.xxx.xxx/fHKfvEhleQ/maincraft/derstatus.php	Malicious URL

Indicator	Type
hxxp://31.210.111.154/Microsoft/Update/KS081274.php	Malicious URL
hxxp://41.77.136.250/Microsoft/Update/KS081274.php	Malicious URL
hxxp://xxx.xxx.xxx.xxx /Microsoft/Update/KC074913.php	Malicious URL
hxxps://31.210.111.154/Microsoft/Update/KS081274.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /Microsoft/Update/KS1945777.php	Malicious URL
hxxps://146.0.74.7/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php	Malicious URL
hxxps://148.251.82.21/Microsoft/Update/KS4567890.php	Malicious URL
hxxps://188.40.8.72/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php	Malicious URL
hxxps://31.210.111.154/Microsoft/Update/KS081274.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /Microsoft/Update/KC074913.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /Microsoft/Update/KS1945777.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /fHKfvEhleQ/maincraft/derstatus.php	Malicious URL
DropBear.exe	Malware Variant Observed
Pnote_o.exe	Malware Variant Observed
Pservice_PPD.exe	Malware Variant Observed
Starter.exe	Malware Variant Observed
tsk.exe (PC)	Malware Variant Observed

Indicator	Type
tsk2.exe (server)	Malware Variant Observed
vba_macro.exe (SHA-1:4C424D5C8CFEDF8D2164B9F833F7C631F94C5A4C)	Malware Variant Observed
Win32/Kill Disk.NBD	Malware Variant Observed
Win32/Rootkit.BlackEnergy.BF trojan	Malware Variant Observed
Java/TrojanDropper.Agent.BB trojan	Malware Variant Observed

--------- **Begin Update A Part 2 of 2** --------

Indicator	Type
khelmn.exe	File Indicator
msupdate_6789.exe	File Indicator
F:/www/fengoffice/tmp/tmp9067/09kh.exe	File Indicator
95.141.37.205	IP Address
/tmp/11236tmp.php	Webshell
/tmp/17271tmp.php	Webshell
/tmp/17513tmp.php	Webshell
/tmp/17778tmp.php	Webshell
/tmp/18054tmp.php	Webshell
/tmp/19198shell.php	Webshell
/tmp/21682tmp.php	Webshell

Indicator	Type
/tmp/21982tmp.php	Webshell
/tmp/27770tmp.php	Webshell
/tmp/28274tmp.php	Webshell
/tmp/2887tmp.ph	Webshell
/tmp/2887tmp.php	Webshell
/tmp/28892tmp.php	Webshell
/tmp/301tmp.php	Webshell
/tmp/32195tmp.php	Webshell
/tmp/8445tmp.php	Webshell
/tmp/9388shell	Webshell
/tmp/9388shell3.php	Webshell
/tmp/9642tmp.php	Webshell
/tmp/shell.php	Webshell
/tmp/tmp27770.php	Webshell
/tmp/tmp28274.php	Webshell
/tmp/tmp8454.php	Webshell
/tmp/tmp9067/reDuh.php	Webshell
/tmp/tmp9067/tm1563.php	Webshell
/tmp/weevely.php	Webshell

Indicator	Type
/tmp/weevly.php	Webshell
6903A0CE131CF0E1B105EC844E846173	MD5 hash of malware
hxxps://31.210.111.154/Microsoft/Update/KS081274.php	Malicious Website
hxxps://88.198.25.92/fHKfvEhleQ/maincraft/derstatus.php	Malicious Website
hxxps://5.9.32.230/Microsoft/Update/KS1945777.php	Malicious Website
hxxps://41.77.136.250/Microsoft/Update/KS081274.php	Malicious Website
31.210.111.154	IP Address
88.198.25.92	IP Address
5.9.32.230	IP Address
41.77.136.250	IP Address
CSIDL_APPDATA\Adobe\settings.sol	File Indicator

--------- End Update A Part 2 of 2 ----------

ICS-CERT will provide additional analysis and technical indicators as they become available.

Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

ICS-CERT CONTACT

For any questions related to this report, 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

Please visit the ICS-CERT Web site for more information on industrial control systems security, or to report an incident.

DOCUMENT FAQ

What is an ICS-CERT Incident Alert? An ICS-CERT Incident Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.