BlackEnergy 3 – Exfiltration of Data in ICS Networks

Malware Report

Version: 1.0

May, 2015

This paper is the result of a research lead by the security researcher David Atch. The authors expect to make revisions to this document after its release due to new findings that might arise.

Executive Summary

As ICS-CERT published its ICS-ALERT-14-281-01B alert, it triggered the question of the attackers' goal when compromising ICS networks. In order to acquire better understanding of their intentions, we analyzed a series of samples related to the BlackEnergy family of malwares. The most interesting sample that produced the findings in this report was BlackEnergy 3, which is probably a private modification of the publicly available BlackEnergy DDOS Bot. After analyzing the malware, we found clues that the attackers might be leveraging the initial infection in order to perform data exfiltration from the inner parts of these networks. The module that led us to this conclusion has the ability of serving RPC functions to remote clients in the same network, which means it is able to send commands to the deeper ends of the same network.

When harnessing these capabilities inside ICS environments, which might be considered isolated, exfiltration of valuable data can take place, allowing attackers to gain insights regarding network structure and operational processes. This data is considered highly valuable when targeting such networks, and it is a necessary step before starting a large scale operation.

Introduction

On October 29, 2014, the Department of Homeland Security and its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an alert titled ICS-ALERT-14-281-01A Ongoing Sophisticated Malware Campaign Compromising ICS. The alert detailed a *"campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware"*. The analysis done by ICS-CERT indicates that this campaign has been ongoing since at least 2011.

The main attack vector observed was infection of Human-Machine-Interface (HMI) machines in ICS networks. These machines provide a user interface for interacting and controlling industrial networks. According to the alert issued by ICS-CERT, various vendors were targeted, including GE CIMPLICITY, Advantech/Broadwin WebAccess, and Siemens WinCC.

It is stated in the alert that ICS-CERT was not able to verify whether the attackers gained deeper control into the ICS network. This has led us to investigate this campaign, in an effort to focus on the attackers' true intention.

In our research we managed to find indicators that the attackers aim to perform data exfiltration from these networks. After studying a series of samples we managed to focus on BlackEnergy 3 (the third generation of the BlackEnergy family of malwares), which incorporates a mechanism that seems to be designed for this purpose.

Background

Even though it is believed various HMI vendors were affected, we will provide a short background focused on GE CIMPLICITY, since it includes the most detailed description of the probable attack vector.

According to the ICS-CERT, the initial infection was of GE CIMPLICITY with direct connection to the internet, by exploiting vulnerability CVE-2014-0751. This vulnerability is assumed to have been exploited since at least January 2012. This initial infection ultimately allowed the attackers to install a BlackEnergy malware on windows machines running GE CIMPLICITY web server. Analysis performed by the ICS-CERT suggests that automated tools were used to discover and compromise these vulnerable systems.

The vulnerability itself (CVE-2014-0751) allowed for the attackers to execute a malicious .cim file (CIMPLICITY screen file) on the HMI machine. The file is hosted on an attacker-controlled server. When the .cim file executes, it downloads the BlackEnergy installer and performs the installation.

This also means that the attack is targeted, and that companies that have been running the GE CIMPLICITY with direct connection to the internet since 2012, might have been infected with BlackEnergy.

Exfiltration of Data

The previous sections described the steps performed by the attackers in order to install and execute arbitrary code on HMI machines in ICS networks. In this section we will describe the general architecture of the mechanism we have found, which can allow the attackers to leverage the infection, in order to perform data exfiltration from these networks.

Data exfiltration from these networks has high value as these are considered isolated networks performing sensitive operations related to industrial processes. However, in various cases, these networks are not completely isolated, as the separation from the outside world is accomplished by using a Firewall, which denies connections to the internet. This configuration is illustrated in figure 1 below.

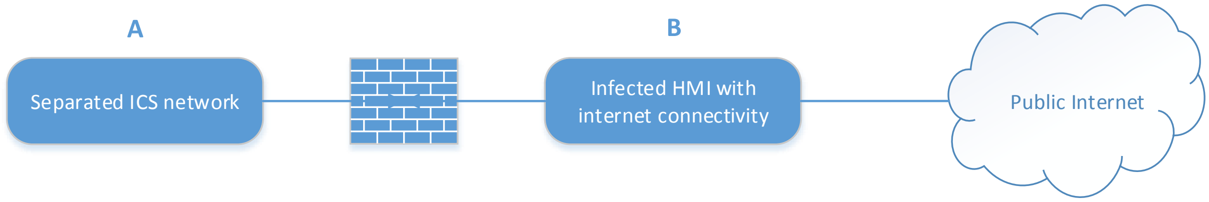

Figure 1: an ICS network separated by a Firewall

While these Firewalls are best configured when denying internet communications, they are usually configured to allow the SMB protocol , as this protocol is common and is required for the routinely operation of the network components.

The mechanism we have found seems to allow for data exfiltration from the separated ICS network (component A in figure 1) in this common configuration. This is accomplished by sending data from an infected host with no internet connectivity (found on the separated ICS network), to an infected host that *has* internet connectivity (component B in figure 1. In relation to the previous section, this is the HMI machine running GE CIMPLICITY). This is performed by RPC communication of named pipes over SMB.

In the following section we will detail the RPC capabilities we have found in BlackEnergy 3, which seems to have been designed specifically for this purpose.

RPC Communications Module

We have used these samples for our analysis:

BlackEnergy 3 Core -
73ebb173b948a04bd68c1ce8f5c1d27f54c161c3d255e990fade64d80ba87705

BlackEnergy 3 si plugin -

16d68b740b5d9aa60929e39fd616d31be2c8528d0f1e58db4cbb16976f7cd725

By reverse engineering the Core module, we have found that its RPC server interface exposes 4 functions, detailed in table 1 below. As mentioned in publicly known information, the si module and probably the whole plugin system of BlackEnergy 3 use the same RPC interface to communicate. However, the plugins do not make use of "function_2" and "function_3", and these functions seem to be designed for usage by a remote plugin, as they contain information regarding the name of the originating host. In addition, 2 of the functions share common functionality, which indicates that one is intended to be used locally and the other remotely.

function_0	Get Command
function_1	Send String to Server
function_2	Send Command Result
function_3	Send File

Table 1: exposed RPC functions

The usage of RPC communications in order to circumvent Firewalls is also known as a technique used by attackers.

When taking all of these issues into consideration, it heavily indicates that other remote plugins are likely to make use of "function_2" and "function_3". This means that the aim of the authors of the malware in designing this interface, was to implement, or to set the ground for remote plugins in order to perform data exfiltration specifically in isolated networks.

The following section details the technical scope of the 4 functions mentioned in Table 1. The protocol uses ncacn_np RPC communications over named pipes. The pipe name is \\Pipe\\{AA0EED25-4167-4CBB-BDA8-9A0F5FF93EA8} and it exposes the 4 functions.

RPC Exposed Functions

This section details the technical scope of the functions in Table 1.

function_0(name, unused, out buffer, size, empty)

Pull out stored command.

The malware will store the last command after each successful connection to the server, the command must be a string separated by a [space] character, and it will be stored in an internal memory array.

The RPC function iterates over this array to extract a specific command, which will be stored in the buffer.

This function is used also by the si plugin.

function_1(size, string)

Send string to the server.

This RPC function will send the provided string using the default C&C mechanism (including all the encryption logic).

This function is used also by the si plugin.

function_2(command, computer, result, size)

Send command results to the server.

This RPC function will send the specified command and its result to the server. The data that is delivered to the server is stored in the following structure:

Command Result Structure

Field Value	**Size**	**Description**
0x4	4 bytes	Type
MODR	4 bytes	Response Type

Field Value	Size	Description
0x1010000	4 bytes	Version
	4 bytes	Overall Structure Size
COMP	4 bytes	Computer Name Field Header
0x14	4 bytes	Field Size
	20 bytes	**Computer Name**
CMDS	4 bytes	Field Header
	4 bytes	Field Size
		Command
RESS	4 bytes	Field Header
	4 bytes	Field Size

The structure contains a COMP field which is probably the remote computer name. If this function would have been used only for local modules this field would have been useless.

Also this function is not used by the si module.

One thing we have noticed during the analysis of this function, that it writes the contents of the structure into c:\1\[COMP].out, this is probably due to forgotten testing routine.

function_3(name, date, computer, size, offset, size, data)

Send a file to the server.

This RPC function takes a file name and its content and sends them to the server. The data that is delivered to the server is stored in the following structure:

File Upload Structure

Field Value	Size	Description
0x3	4 bytes	Type
FILE	4 bytes	Response Type
0x1010000	4 bytes	Version
	4 bytes	Overall Structure Size
COMP	4 bytes	Field Header

Field Value	**Size**	**Description**
0x14	4 bytes	Field Size
	20 bytes	**Computer Name**
NAME	4 bytes	Field Header
	4 bytes	Field Size
		File Name
DATE	4 bytes	Field Header
	4 bytes	Field Size
		Date
DATA	4 bytes	Field Header
	4 bytes	Field Size
		File Contents

The structure contains a COMP field which is probably the remote computer name. If this function would have been used only for local modules this field would have been useless.

Summary

In this research we set out to gain better understanding of the attackers' intentions in the campaign described in ICS-ALERT-14-281-01B. The alert detailed a "campaign that has compromised numerous industrial control systems (ICSs) environments using a variant of the BlackEnergy malware".

In order to accomplish this we have analyzed a series of samples related to the BlackEnergy family of malwares. The result of the analysis is a discovery of two RPC functions that are not being used by the si plugin and looks like they are meant for file and results delivery from remote machines. Our research has led us to the conclusion that there may be other undiscovered plugins, which would be responsible for the reconnaissance and data exfiltration from the deeper parts of the organizational network.

Finally, we would like to address the malware research community and the ICS industry with a warning that there might be more undiscovered BlackEnergy components in internal networks.