DNP3 Security Notice SN2017-001 CrashOverride/Industroyer Malware

1 Issue

DNP User Group members are advised of the recent publication of a DHS ICS-CERT alert (found here: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01 and a US-CERT alert (found here: https://www.us-cert.gov/ncas/alerts/TA17-163A) that discuss malware believed to have been used to attack the Ukrainian power industry in December 2016. The alerts cite reports published by security firms ESET and Dragos that describe the malware.

The analysis suggests that the malware includes a framework and a set of target-specific software modules that can attack the power grid by obstructing normal SCADA system communication and replacing it with malicious traffic intended to disrupt grid operations.

The samples of the malware found in the Ukrainian power grid include modules that attack the control system communication interfaces used in that system, including SCADA protocols that are functionally similar to IEEE 1815 (DNP3). No module that uses DNP3 has been identified in the malware to date, but its design supports the inclusion of additional modules, such as a specific module that could attack an insufficiently secured DNP3 system in a similar manner.

It is strongly recommended that User Group members take suitable steps to secure their systems. This DNP3 Security Notice provides information that may assist in this process.

2 Details

Dragos has applied the name CRASHOVERRIDE to this malware. ESET has used the name Industroyer. Both names refer to the same malware. The ICS-CERT and US-CERT alerts adopt the CrashOverride name. It is understood that Dragos selected this name in reference to artifacts within the malware and also to the character “Crash Override” from MGM’s 1995 movie “Hackers”.

A number of other bodies have issued commentary on the malware, including:

- Belden: http://www.belden.com/blog/industrialsecurity/crashoverride-first-malware-platform-designed-to-take-down-electric-grids.cfm
- Dragos: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
- ESET: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf
- SANS: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

Each document adds commentary that reflects each author’s specific areas of interest. Each document also provides some recommendations for identifying the malware and securing systems.

The Directors of the DNP Users Group recommend that Users Group members:

- make themselves aware of the content of these reports
- carefully review the recommendations contained in the reports to decide which may be relevant to their systems.

3 DNP Technical Committee Opinion

Members of the DNP Technical Committee who have reviewed the reports made the following observations:

The particular variant of the malware that was analyzed affects the operation of control system computers as part of a concerted effort to attack a power grid. The attack apparently consisted of several phases, leading up to the activation of the malware analyzed in these reports.

When the malware has infected a system running a SCADA master or HMI it kills the master communication interface and replaces it with a malicious master. It then performs a series of actions such as injecting control commands that use the grid operation protocols to disrupt the operation of the grid (e.g. by tripping circuit breakers). Other variants of the malware might implement other attack scenarios.

The malware samples that have been analyzed and reported do not appear to include mechanisms to attack DNP3; however, it appears that the malware supports the ability to have this functionality added. Because of this, the operation of other parts of the malware have been reviewed to identify if DNP3 could be attacked in a similar manner. The operation of the malware's IEC 60870-5-101 and -104 modules are particularly instructive as they provide functionality similar to DNP3. These modules operate by inhibiting the normal SCADA master communication functions and then activate a replacement master communication module managed by the malware, which executes a script of commands to issue normal protocol messages.

The malware analysis reports indicate that protocol messages are issued that trip the power system circuit breakers. Since the commands issued by the malware are normal SCADA protocol messages that originate from the system's master station, they are unlikely to be identified as malicious by automated security appliances that check and validate the source, destination and content of messages.

It should be noted that because the messages are routed through the control network in the usual manner, they are not inhibited by access point-to-access point or device-to-device security protections such as VPN routers or the use of TLS that is not an integral part of the master application.

What follows is conjecture, which would apply to a malware module that attacks DNP3, but is otherwise functionally equivalent to the IEC 60870 module described above:

> The malware inhibits the operation of the protocol master software and launches a replacement protocol handler. A system using DNP3 Secure Authentication (DNP3-SA) adds application-to-application authentication information to all control commands. Only a master configured with the correct security keys is able to successfully control an outstation that has DNP3-SA enabled. The malware's replacement protocol handler may not have access to these security keys, unless they have also been compromised. If the security keys used for DNP3-SA are not available to the malware, DNP3-SA provides a level of protection against attacks from malware of this kind, or makes compromise of the system significantly more difficult for the attacker. DNP3-SA can be applied to systems using serial and/or Ethernet communication.
>
> Similarly, systems using TLS as an integral part of the Master application adds authentication below the DNP3 application layer for all the communication. In such a case, only a master with the correct security credentials can successfully establish a TLS connection over TCP/IP with the outstation. The malware's replacement protocol handler may not have access to the security credentials, unless they have also been compromised. Therefore using TLS for DNP3 communication over TCP/IP also adds a level of protection against attacks from malware of this kind. Note that DNP3-SA may be used in conjunction with DNP3 over TLS. Multiple security layers (the practice of "defense-in-depth") can provide additional protection.

NOTE: IEC 60870-5-7 defines the same application layer security functions for the IEC 60870-5-101/-104 protocols that DNP3-SA provides for DNP3. IEC 60870-5-7 could therefore potentially protect those protocols from CrashOverride (in its current form).

The attack appears to have been performed in a manner that specifically targeted the system in question and suggests that the attacker undertook significant reconnaissance to determine the nature and configuration of that system. The reduction of likelihood of such an attack is likely to involve steps that:

- limit or prevent the attacker's access to the system and ability to install malicious software
- identify intrusion into the system and the presence of unauthorized software
- detect and limit unusual traffic on the system

4 Recommendation

In addition to other measures to isolate the control system and identify the presence of the malware (discussed in other reports linked above), the Directors of the DNP Users Group recommend the implementation of DNP3 Secure Authentication as a step to enhance the cybersecurity of DNP3 systems, as part of a defense-in-depth security strategy.

The Directors also recommend that steps be taken in the implementation of DNP3-SA to protect the keys used by DNP3-SA from access by unauthorized users and unauthorized applications (including malware).

NOTE: It is not the purpose of this Notice to specify all aspects of securing DNP3 systems. Nor does it describe the process for creating a defense-in-depth control system cybersecurity strategy. The factors that should be considered in creating and deploying a security policy depend on the particular requirements and characteristics of each individual system. No single security recommendation (even the implementation of DNP3-SA) or other guidance should be considered to be universally applicable and sufficient in all cases.

5 Last Updated

16-August-2017