INTELLIGENCE BRIEF

COSMICENERGY – Not an Immediate Threat

JIMMY WYLIE | TECHNICAL LEAD MALWARE ANALYST

CONTRIBUTORS: REID WIGHTMAN, CAROLYN AHLERS, SAM HANSON, KATE VAJDA, CASEY BROOKS

DRAGOS, INC

JUNE 2023

Overview

On May 25, 2023, Mandiant released details about a new industrial control systems (ICS) malware dubbed COSMICENERGY.[1] This malware, designed to target IEC 104 devices, exploits existing Microsoft SQL (MS SQL) servers that are connected to remote terminal units (RTUs). Dragos Threat Intelligence independently analyzed the malware and, counter to media headlines claiming power disruption or grid crippling abilities, concluded that COSMICENERGY is not an immediate threat to operational technology. In this brief, we provide an analysis of the COSMICENERGY malware and how it compares to other more concerning threats like CRASHOVERIDE and Industroyer2.

Key Findings

- COSMICENERGY is not an immediate threat to operational technology (OT).
- The overall codebase of COSMICENERGY lacks maturity, contains errors, and is far from being a full-fledged attack capability like Industroyer2 or CRASHOVERRIDE.
- There is no evidence that COSMICENERGY is being deployed in the wild.
- Operators should reach out to vendors to see if software packages include MS SQL.
- Operators should ensure they have network monitoring in place, watch for xp_cmdshell alerts, and out of an abundance of caution, audit their MS SQL Servers.
- Analysis indicates that the tool is likely part of a training exercise or for use in detection development.

[1] COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises — Mandiant

COSMICENERGY: PIEHOP and LIGHTWORK

Dragos analyzed COSMICENERGY, which is composed of two malware samples, PIEHOP and LIGHTWORK.

PIEHOP is a PyInstaller binary. PyInstaller bundles a Python application and all its dependencies into a single package. The user can run the packaged app without installing a Python interpreter or any modules. Upon execution, like any PyInstaller binary, PIEHOP unpacks all the required files and dependencies for the main Python program's execution, which in this case includes the LIGHTWORK binary. After completing the unpacking process, it executes the main Python script, **r3_iec104_control.py,** via the Python interpreter dynamic-link library (DLL). PIEHOP's primary function is to enable **xp_cmdshell** on a remote MS SQL server specified via the command line and then to use **xp_cmdshell** to upload and execute the LIGHTWORK binary. After LIGHTWORK executes, PIEHOP can check the results to verify whether the execution was successful, delete LIGHTWORK from the server, and then delete itself. PIEHOP's MS SQL capabilities show some resemblance to a script on GitHub,[2] and they may have been based on that.

PIEHOP

EXE Name:	r3_iec104_control.exe
MD5:	cd8f394652db3 d0376ba24a990403d20
SHA-1:	bc07686b422aa0dd01c87ccf557863ee62f6a435
SHA-256:	358f0f8c23acea82c5f75d6a2de37b6bea7785ed0e32c41109c217c48bf16010

LIGHTWORK

EXE Name:	OT_T855_IEC104_GR.exe
MD5:	7b6678a1c0000344f4faf975c0cfc43d
SHA-1:	6eceb78acd1066294d72fe86ed57bf43bc6de6eb
SHA-256:	740e0d2fba550308344b2fb0e5ecfebdd09329bdcfaa909d3357ad4fe5552532

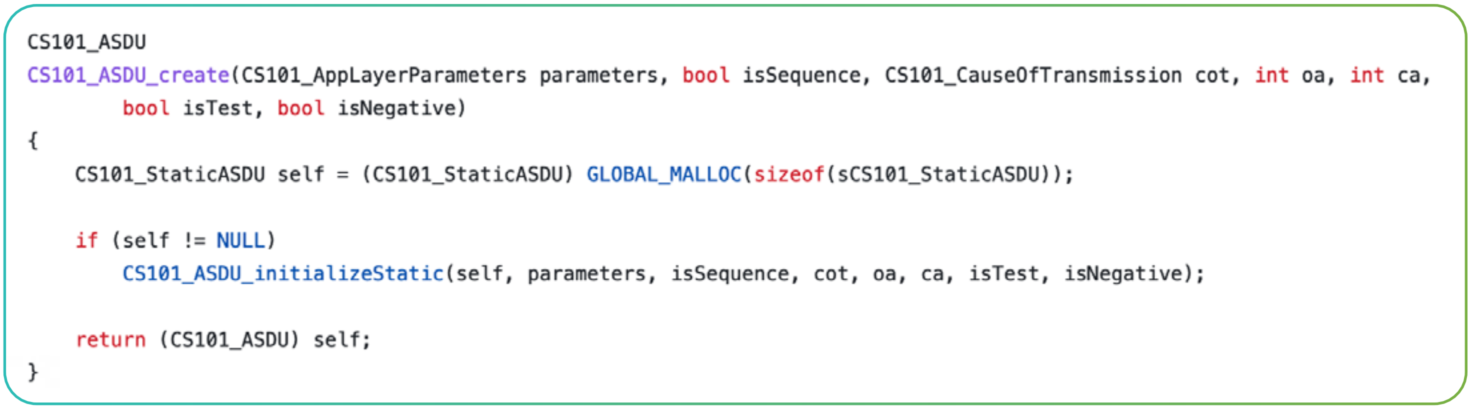
LIGHTWORK is a native Windows executable with IEC104 capabilities. It takes an IP address via the command line and another argument dictating whether to send ON or OFF messages to IEC104 devices. It initiates an IEC104 connection with the IP address and sends an IEC104 Single Command with either ON or OFF, depending on the command line argument, to a list of hard-coded Information Object Addresses (IOAs). The messages here lack configuration. It can only send Single Commands, and those messages have to be all ONs or all OFFs. It's not configured per IOA. Further, the Common Address of ASDU (COA) or Application Service Data Unit (ASDU) address, is hard-coded to 1 for all messages. We know that's a lot of IEC104 jargon, so the short summary is that LIGHTWORK is hard-coded to affect a specific IEC104 network configuration.

LIGHTWORK is not CRASHOVERRIDE/Industroyer2

LIGHTWORK is not a variant of the CRASHOVERRIDE/Industroyer2 family of malware or any other ICS malware discovered to date. LIGHTWORK was compiled with symbol information which means Dragos recovered all function and argument names in the binary and produced an easy-to-read decompilation. The majority of the code is from a known 60870 open-source library, lib60870-C,[3] maintained by MZ Automation GmbH, not a custom IEC104 library like the one in CRASHOVERRIDE and Industroyer2.

[2] mssql_shell.py

[3] lib60870-C - GitHub

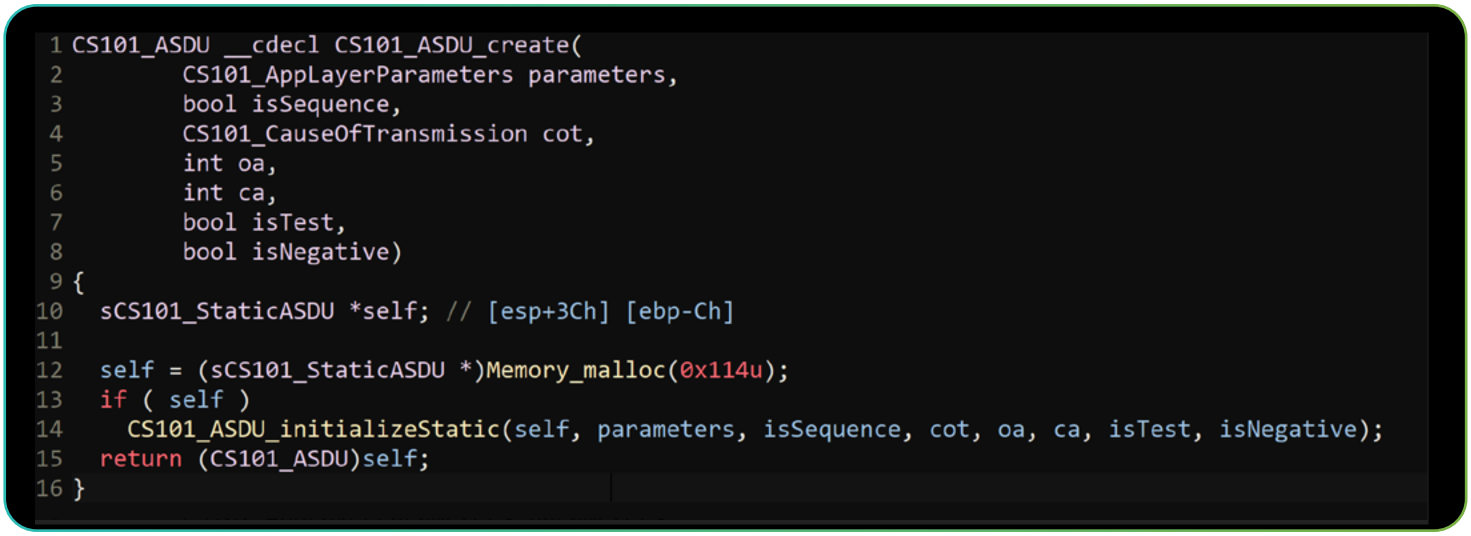


```
CS101_ASDU
CS101_ASDU_create(CS101_AppLayerParameters parameters, bool isSequence, CS101_CauseOfTransmission cot, int oa, int ca,
        bool isTest, bool isNegative)
{
    CS101_StaticASDU self = (CS101_StaticASDU) GLOBAL_MALLOC(sizeof(sCS101_StaticASDU));

    if (self != NULL)
        CS101_ASDU_initializeStatic(self, parameters, isSequence, cot, oa, ca, isTest, isNegative);

    return (CS101_ASDU) self;
}
```

Figure 1: CS101_ASDU_create function from lib60870-C source



```
CS101_ASDU __cdecl CS101_ASDU_create(
        CS101_AppLayerParameters parameters,
        bool isSequence,
        CS101_CauseOfTransmission cot,
        int oa,
        int ca,
        bool isTest,
        bool isNegative)
{
  sCS101_StaticASDU *self; // [esp+3Ch] [ebp-Ch]

  self = (sCS101_StaticASDU *)Memory_malloc(0x114u);
  if ( self )
    CS101_ASDU_initializeStatic(self, parameters, isSequence, cot, oa, ca, isTest, isNegative);
  return (CS101_ASDU)self;
}
```

Figure 2: Decompiled version of CS101_ASDU_create in LIGHTWORK

Dragos compared the code inside of LIGHTWORK to a reference 60870 DLL provided by a related project, **nim_lib60870,**[4] that wraps lib60870-C, and found that 98 percent of the functions in LIGHTWORK are the same (or very similar) to those found in the reference DLL. Of the remaining 2 percent that didn't match, only 1 of those functions, *main*, is of any importance. That function amounts to about 68 lines of decompiled code, which isn't much. A similar comparison of LIGHTWORK to Industroyer2 yielded no significant overlap.

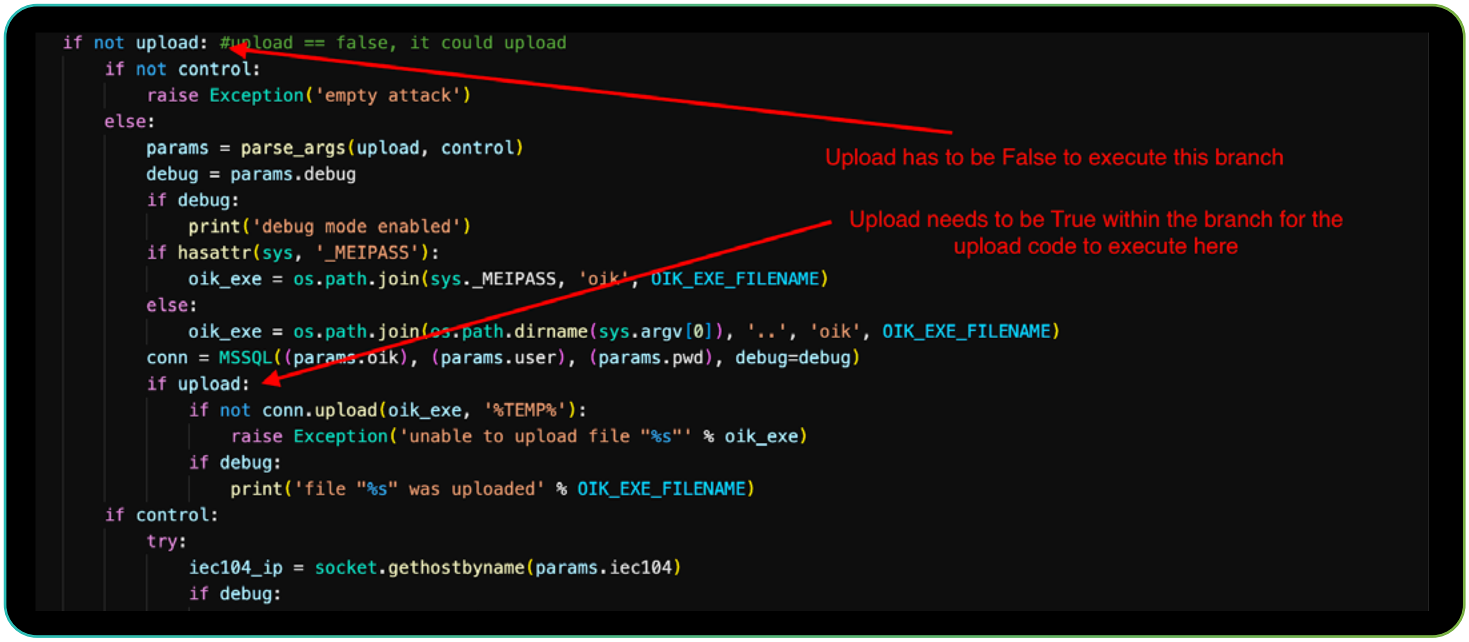
COSMICENERGY Is Not an Immediate Threat to OT

After analyzing COSMICENERGY, Dragos concluded that it is not an immediate risk to OT environments. The primary purpose of COSMICENERGY appears to have been for training scenarios rather than for deployment in real-world environments. There is currently no evidence to suggest that an adversary is actively deploying COSMICENERGY. This conclusion is further supported by the fact that LIGHTWORK's COA and IOAs are hard-coded to target a specific range of equipment. For reference, both CRASHOVERRIDE and Industroyer2 had configuration formats that allowed both of these IEC104 fields to change, among other parameters.

[4] **nim_lib60870** - GitHub

Further, LIGHTWORK's original file name is **OT_T855_IEC104_GR.exe** which appears to be a reference to MITRE ATT&CK for ICS, a catalog of malware tactics and techniques frequently used by defenders. Specifically, it references technique Code T0855[5] or Unauthorized Command Message, which is exactly the technique implemented by the LIGHTWORK tool. If you look at the examples, you'll see references to both CRASHOVERRIDE/Industroyer and Industroyer2's use of IEC104. This reference to MITRE ATT&CK is also an indication that this sample may be for training, education, or perhaps detection development and testing.

Aside from indications that the tool may not be malicious, several coding errors in PIEHOP prevent the malware from running properly as discovered or limit its potential flexibility. Control flow problems mean it is unable to upload LIGHTWORK properly to the server.



```
if not upload: #upload == false, it could upload
    if not control:
        raise Exception('empty attack')
    else:
        params = parse_args(upload, control)
        debug = params.debug
        if debug:
            print('debug mode enabled')
        if hasattr(sys, '_MEIPASS'):
            oik_exe = os.path.join(sys._MEIPASS, 'oik', OIK_EXE_FILENAME)
        else:
            oik_exe = os.path.join(os.path.dirname(sys.argv[0]), '..', 'oik', OIK_EXE_FILENAME)
        conn = MSSQL((params.oik), (params.user), (params.pwd), debug=debug)
        if upload:
            if not conn.upload(oik_exe, '%TEMP%'):
                raise Exception('unable to upload file "%s"' % oik_exe)
            if debug:
                print('file "%s" was uploaded' % OIK_EXE_FILENAME)
    if control:
        try:
            iec104_ip = socket.gethostbyname(params.iec104)
            if debug:
```

Upload has to be False to execute this branch

Upload needs to be True within the branch for the upload code to execute here

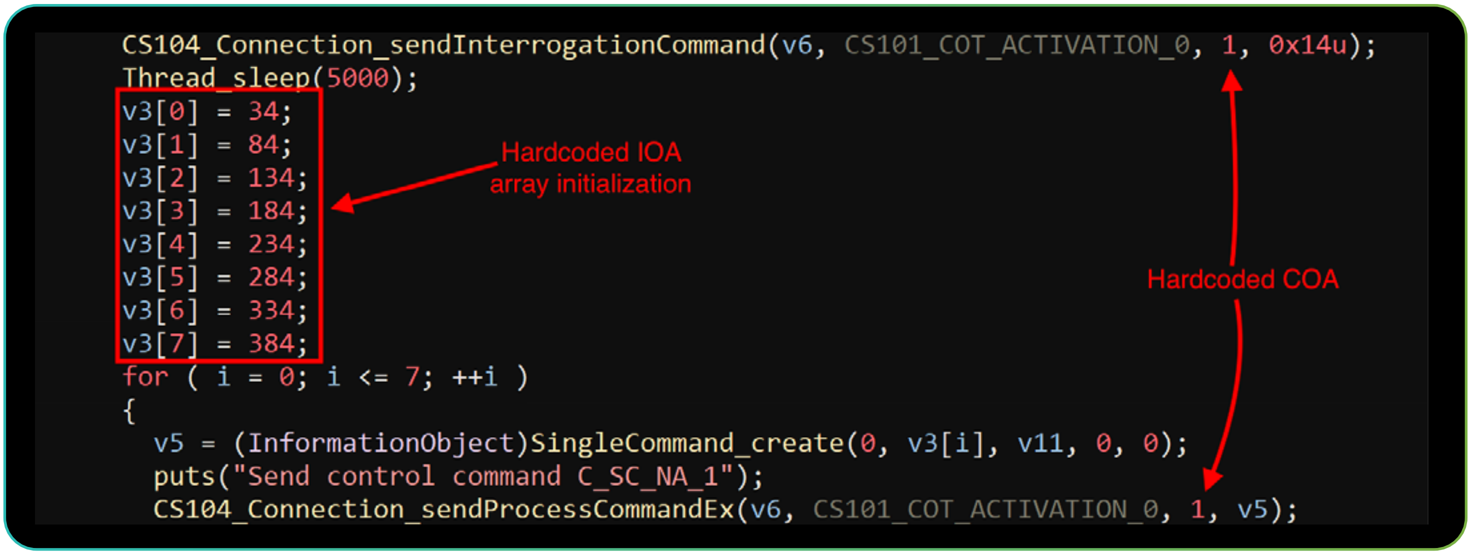
Figure 3. Upload code can't be reached

If that issue is fixed, it still requires multiple executions to both upload and execute LIGHTWORK. If code execution reaches the portion that should execute LIGHTWORK, the code will crash due to uninitialized variables being referenced.

While PIEHOLE fails to run without modification, LIGHTWORK (surprisingly) executes without crashing. However, the tool lacks development maturity and requires more work before it's a full-fledged IEC104 attack capability. Compared with CRASHOVERRIDE and Industroyer2, it appears that LIGHTWORK's developers know even less than their predecessors about how to use IEC104 or were simply testing to see if they could reach IEC104 equipment.

Further, LIGHTWORK lacks configurability, affecting its ability to target multiple substation addresses, different IOAs, and different types of equipment. In its current state, each execution of LIGHTWORK can only affect a specific range of equipment since both the IOAs and COA are hard-coded.

[5] **Unauthorized Command Message, T0855** – MITRE



```
CS104_Connection_sendInterrogationCommand(v6, CS101_COT_ACTIVATION_0, 1, 0x14u);
Thread_sleep(5000);
v3[0] = 34;
v3[1] = 84;
v3[2] = 134;
v3[3] = 184;
v3[4] = 234;
v3[5] = 284;
v3[6] = 334;
v3[7] = 384;
for ( i = 0; i <= 7; ++i )
{
  v5 = (InformationObject)SingleCommand_create(0, v3[i], v11, 0, 0);
  puts("Send control command C_SC_NA_1");
  CS104_Connection_sendProcessCommandEx(v6, CS101_COT_ACTIVATION_0, 1, v5);
```

Hardcoded IOA array initialization

Hardcoded COA

Figure 4. Hard-coded information in LIGHTWORK

In the simplest case, LIGHTWORK could target another set of equipment if the targeted IEC104 device shares the same COA and IOAs, and the targeted state for each of those IOAs are stored as Single Point information. In this case, simply specifying the IP address will suffice.

If the LIGHTWORK developers wanted to target a range of equipment with different IOAs, they would have to at least consider the following questions:

- Do the IOAs share the same COA? If not, then some logic changes would need to be made to support addressing IOAs with different COAs.
- Do the IOAs all use the same information type (Single Point, Double Point, etc), if not, logic changes need to be made to support setting different information types.
- Are all the devices reachable from the same RTU? Otherwise, logic needs to be changed to support multiple IP addresses and specifications of the corresponding IOAs.

The developers of **CRASHOVERRIDE** and Industroyer2[5] understood these questions and more, and the result was their custom configuration format. LIGHTWORK is very limited by comparison and requires much more development time for it to be a realistic and flexible attack capability.

[5] **Industroyer2: Industroyer reloaded** – welivesecurity by ESET

Recommendations

To safeguard against potential threats of this nature, Dragos recommends the following:

- Restrict access to engineering workstations (EWS) and OT servers running MS SQL. Increase monitoring efforts for new connections probing MS SQL servers or enabling **xp_cmdshell** on servers communicating with IEC104 devices.
- Restrict access to port TCP/1443 on the MS SQL host. Restrict access to port TCP/2404 on the RTUs and other IEC104 equipment.
- Asset owners are encouraged to:
  - Stay abreast of emerging threat behaviors.
  - Identify IEC104 devices within their network.
  - Ensure that access to these devices and any others that can communicate with RTUs is appropriately restricted.
- Any attack of this nature will require dwell time in order to understand the OT network and derive the appropriate COAs and IOAs. This is an opportunity to detect the adversary, so ensure that network monitoring is deployed. For guidance on setting up defensible network infrastructure, reference the **5 Critical Controls**.

Conclusion

In its current form, COSMICENERGY is not a direct threat to OT. Indications that it is a training tool with coding errors and a lack of development maturity lessen its potential risk. Its discovery hints at a trend, also witnessed in PIPEDREAM, towards developers leveraging known standard ICS protocols to achieve an effect and incorporating open-source projects like lib60870-C to implement their tools. Even though there's no evidence that COSMICENERGY is being deployed, its existence should prompt all organizations to reassess their firewall rules and configurations and ensure they have visibility into the ICS protocols traversing their network. This is the third discovery of IEC104 targeted tooling, so organizations should take notice and implement good security posture to raise the probability of detecting and mitigating potential future attacks.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.