

## Lazarus luring employees with trojanized coding challenges: The case of a Spanish aerospace company

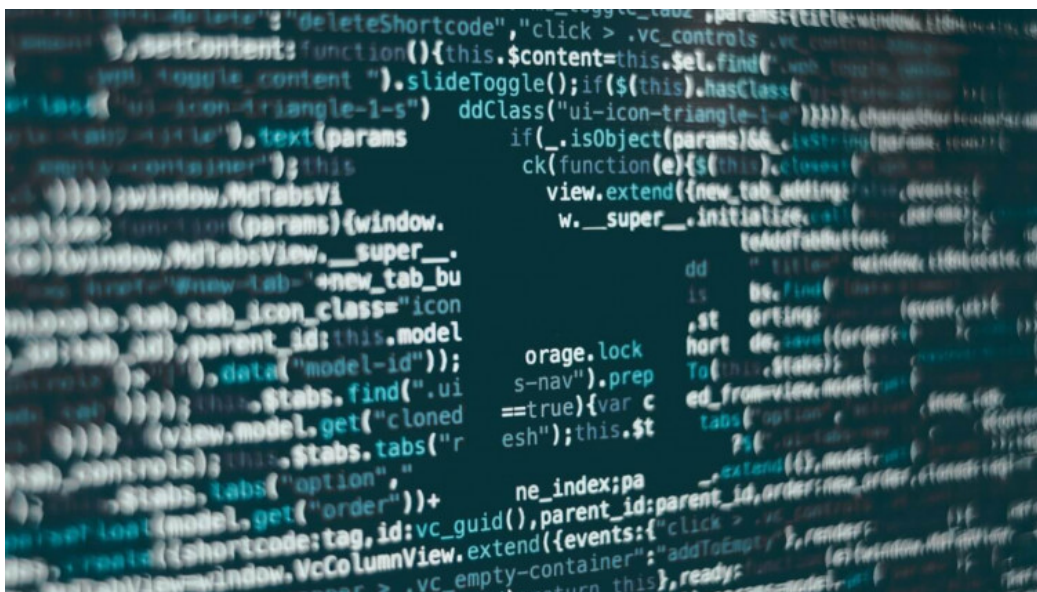
ESET Research

While analyzing a Lazarus attack luring employees of an aerospace company, ESET researchers discovered a publicly undocumented backdoor



Peter Kálnai

29 Sep 2023 • , 29 min. read



ESET researchers have uncovered a Lazarus attack against an aerospace company in Spain, where the group deployed several tools, most notably a publicly undocumented backdoor we named LightlessCan. Lazarus operators obtained initial access to the company's network last year after a successful spearphishing campaign, masquerading as a recruiter for Meta – the company behind Facebook, Instagram, and WhatsApp.

The fake recruiter contacted the victim via LinkedIn Messaging, a feature within the LinkedIn professional social networking platform, and sent two coding challenges required as part of a hiring process, which the victim downloaded and executed on a company device. The first challenge is a very basic project that displays the text "Hello, World!", the second one prints a Fibonacci sequence – a series of numbers in which each number is the sum of the two preceding ones. ESET Research was able to reconstruct the initial access steps and analyze the toolset used by Lazarus thanks to cooperation with the affected aerospace company.

In this blogpost, we describe the method of infiltration and the tools deployed during this Lazarus attack. We will also present some of our findings about this attack at the [Virus Bulletin conference](#) on October 4, 2023.

### Key points of the blogpost:

- *Employees of the targeted company were contacted by a fake recruiter via LinkedIn and tricked into opening a malicious executable presenting itself as a coding challenge or quiz.*
- *We identified four different execution chains, delivering three types of payloads via DLL side-loading .*
- *The most notable payload is the LightlessCan backdoor, implementing techniques to hinder detection by real-time security monitoring software and analysis by cybersecurity professionals; this presents a major shift in comparison with its predecessor BlindingCan, a flagship HTTP(S) Lazarus RAT.*
- *We attribute this activity with a high level of confidence to Lazarus, particularly to its campaigns related to Operation DreamJob.*
- *The final goal of the attack was cyberespionage.*

Lazarus delivered various payloads to the victims' systems; the most notable is a publicly undocumented and sophisticated remote access trojan (RAT) that we named LightlessCan, which represents a significant advancement

compared to its predecessor, BlindingCan. LightlessCan mimics the functionalities of a wide range of native Windows commands, enabling discreet execution within the RAT itself instead of noisy console executions. This strategic shift enhances stealthiness, making detecting and analyzing the attacker's activities more challenging.

Another mechanism used to minimize exposure is the employment of execution guardrails; Lazarus made sure the payload can only be decrypted on the intended victim's machine. Execution guardrails are a set of protective protocols and mechanisms implemented to safeguard the integrity and confidentiality of the payload during its deployment and execution, effectively preventing unauthorized decryption on unintended machines, such as those of security researchers. We describe the implementation of this mechanism in the [Execution chain 3: LightlessCan \(complex version\)](#) section.

## Attribution to the Lazarus group

The Lazarus group (also known as HIDDEN COBRA) is a cyberespionage group [linked to North Korea](#) that has been active since at least 2009. It is responsible for high-profile incidents such as both the [Sony Pictures Entertainment hack](#) and tens-of-millions-of-dollar [cyberheists in 2016](#), the [WannaCryptor](#) (aka WannaCry) outbreak in 2017, the 3CX and X\_TRADER [supply-chain attacks](#), and a long history of [disruptive attacks against South Korean](#) public and critical infrastructure since at least 2011. The diversity, number, and eccentricity in implementation of Lazarus campaigns define this group, as well as that it performs all three pillars of cybercriminal activities: cyberespionage, cybersabotage, and pursuit of financial gain.

Aerospace companies are not an unusual target for North Korea-aligned advanced persistent threat (APT) groups. The country has conducted [multiple nuclear tests](#) and launched intercontinental ballistic missiles, which violate United Nations (UN) Security Council [resolutions](#). The UN monitors North Korea's nuclear activities to prevent further development and proliferation of nuclear weapons or weapons of mass destruction, and publishes [biannual reports](#) tracking such activities. According to these reports, North Korea-aligned APT groups attack aerospace companies in attempts to access sensitive technology and aerospace know-how, as intercontinental ballistic missiles spend their midcourse phase in the space outside of Earth's atmosphere. These reports also claim that money gained from cyberattacks accounts for a portion of North Korea's missile development costs.

We attribute the attack in Spain to the Lazarus group, specifically to Operation DreamJob, with a high level of confidence. The name for Operation DreamJob was coined in a [blogpost](#) by ClearSky from August 2020, describing a Lazarus campaign targeting defense and aerospace companies, with the objective of cyberespionage. Since then, we have loosely used the term to denote various Lazarus operations leveraging job-offering lures but not deploying tools clearly similar to those involved in its other activities, such as [Operation In\(ter\)ception](#). For example, the campaign involving tools signed with 2 TOY GUYS certificates (see [ESET Threat Report T1 2021, page 11](#)), and the case of [Amazon-themed lures](#) in the Netherlands and Belgium published in September 2022.

Our attribution is based on the following factors, which show a relationship mostly with the previously mentioned Amazon-themed campaign:

### 1. Malware (the intrusion set):

- Initial access was obtained by making contact via LinkedIn and then convincing the target to execute malware, disguised as a test, in order to succeed in a hiring process. This is a known Lazarus tactic, used at least since Operation DreamJob.
- We observed new variants of payloads that were previously identified in the Dutch case from last year, such as intermediate loaders and the BlindingCan backdoor [linked with Lazarus](#).
- Multiple types of strong encryption were leveraged in the tools of this Lazarus campaign – AES-128 and RC6 with a 256-bit key – that were also used in the Amazon-themed campaign.

### 2. Infrastructure:

- For the first-level C&C servers (listed in the Network section at the end of this blogpost), the attackers do not set up their own servers, but compromise existing ones, usually those having poor security and that host sites with neglected maintenance. This is a [typical](#), yet weak-confidence behavior, of Lazarus.

### 3. *Cui bono*:

- Pilfering the know-how of an aerospace company is aligned with long-term goals manifested by Lazarus.

## Initial access

The group targeted multiple company employees via LinkedIn Messaging. Masquerading as a [Meta](#) recruiter, the attacker used a job offer lure to attract the target's attention and trust; a screenshot of this conversation, which we obtained during our cooperation with the Spanish aerospace company, is depicted in Figure 1.

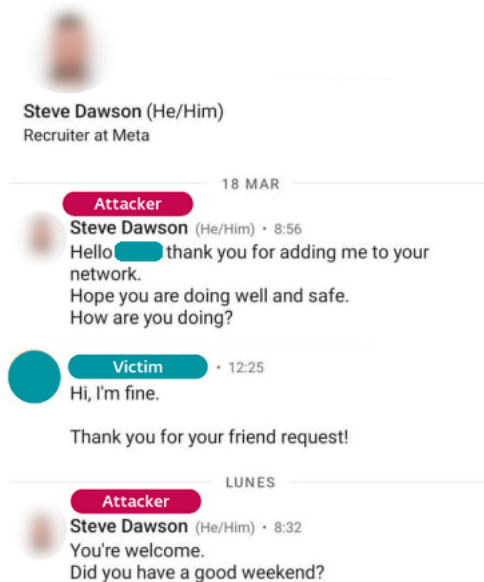


Figure 1. The initial contact by the attacker impersonating a recruiter from Meta

At the beginning of Lazarus attacks, the unaware targets are usually convinced to recklessly self-compromise their systems. For this purpose, the attackers employ different strategies; for example, the target is lured to execute an attacker-provided (and trojanized) PDF viewer to see the full content of a job offer. Alternately, the target is encouraged to connect with a trojanized SSL/VPN client, being provided with an IP address and login details. Both scenarios are described in a [Microsoft blogpost](#) published in September 2022. The narrative in this case was the scammer's request to prove the victim's proficiency in the C++ programming language.

Two malicious executables, Quiz1.exe and Quiz2.exe, were provided for that purpose and delivered via the Quiz1.iso and Quiz2.iso images hosted on a third-party cloud storage platform. Both executables are very simple command line applications asking for input.

The first one is a Hello World project, which is a very basic program, often consisting of just a single line of code, that displays the text "Hello, World!" when executed. The second prints a Fibonacci sequence up to the largest element smaller than the number entered as input. A Fibonacci sequence is a series of numbers in which each number is the sum of the two preceding ones, typically starting with 0 and 1; however, in this malicious challenge, the sequence starts with 1 and 2. Figure 2 displays example output from the Fibonacci sequence challenge. After the output is printed, both executables trigger the malicious action of installing additional payloads from the ISO images onto the target's system. The task for a targeted developer is to understand the logic of the program and rewrite it in the C++ programming language.

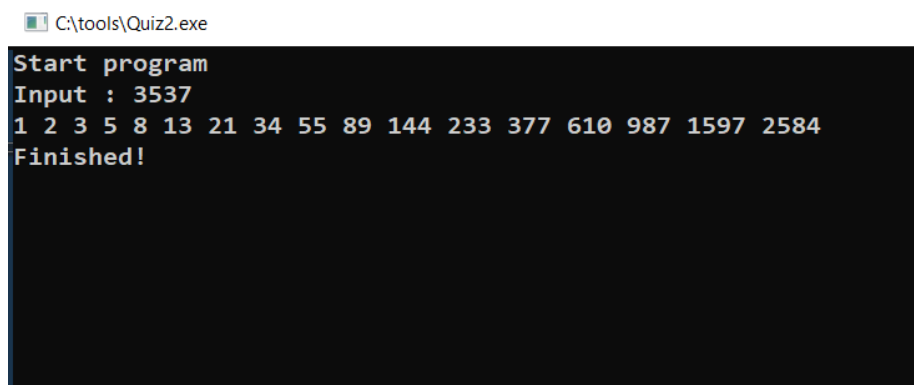


Figure 2. The output of the decoy program Quiz2.exe

The chain of events that led to the initial compromise is sketched in Figure 3. The first payload delivered to the target's system is an HTTP(S) downloader that we have named NickelLoader. The tool allows the attackers to deploy any desired program into the memory of the victim's computer.

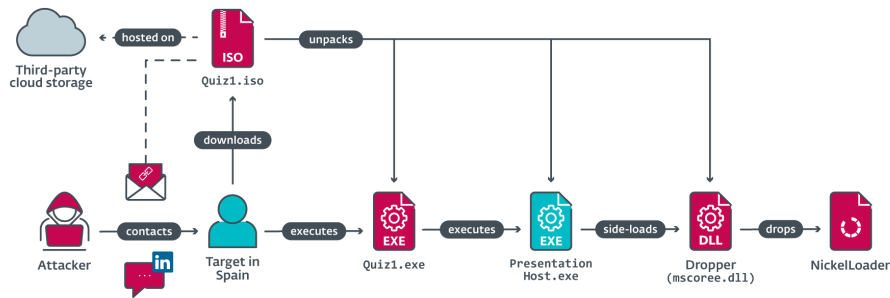


Figure 3. The chain of events completing the initial access

## Post-compromise toolset

Once NickelLoader is running on the target’s system, the attackers use it to deliver two types of RATs. One of these RATs is already known to be part of the Lazarus toolkit, specifically a variant of the BlindingCan backdoor with limited functionality but identical command processing logic. To distinguish it, we put the prefix mini- in front of the variant’s name. Additionally, the attackers introduced a RAT not previously undocumented publicly, which we have named LightlessCan.

The RATs are deployed as the final step of chains of stages with varying levels of complexity and are preceded by helper executables, like droppers and loaders. We denote an executable as a dropper if it contains an embedded payload, even if it’s not dropped onto the file system but instead loaded directly into memory and executed. Malware that doesn’t have an encrypted embedded data array, but that loads a payload from the file system, we denote as a loader.

Besides the initial quiz-related lures, Table 1 summarizes the executable files (EXEs) and dynamic link libraries (DLLs) delivered to the victim’s system. All the malware samples in the third column are trojanized open-source applications (see the fourth column for the underlying project), with a legitimate executable side-loading a malicious DLL. For example, the malicious mscoree.dll is a trojanized version of the legitimate NppyPluginDll; the DLL contains an embedded NickelLoader and is loaded by a legitimate PresentationHost.exe, both located in the C:\ProgramShared directory.

Table 1. Summary of binaries involved in the attack

Location directory	Legitimate parent process	Malicious side-loaded DLL	Trojanized project (payload)
C:\ProgramShared\	PresentationHost.exe	mscoree.dll	NppyPluginDll (NickelLoader)
C:\ProgramData\Adobe\	colorcpl.exe	colorui.dll	LibreSSL 2.6.5 (miniBlindingCan)
C:\ProgramData\Oracle\Java\	fixmapi.exe	mapistub.dll	Lua plugin for Notepad++ 1.4.0.0 (LightlessCan)
C:\ProgramData\Adobe\ARM\	tabcal.exe	HID.dll	MZC8051 for Notepad++ 3.2 (LightlessCan)

## LightlessCan – new backdoor

The most interesting payload used in this campaign is LightlessCan, a successor of the group’s flagship HTTP(S) Lazarus RAT named BlindingCan. LightlessCan is a new complex RAT that has support for up to 68 distinct commands, indexed in a custom function table, but in the current version, 1.0, only 43 of those commands are implemented with some functionality. The remaining commands are present but have a formal implementation in the form of placeholders, lacking actual functionality. The project behind the RAT is definitely based on the BlindingCan source code, as the order of the shared commands is preserved significantly, even though there may be differences in their indexing.

The most significant update is mimicked functionality of many native Windows commands like ping, ipconfig, systeminfo, sc, net, etc. The hardcoded string “The operation completed successfully.”, the standard system message for the ERROR\_SUCCESS result, brought us to that idea. Table 2 contains a list of those commands that are implemented in LightlessCan. In previously reported Lazarus attacks, as documented in blogposts by Positive Technologies in April 2021 and HvS Consulting in December 2020, these native commands are often executed in many instances after the attackers have gotten a foothold in the target’s system. However, in this case, these commands are executed discreetly within the RAT itself, rather than being executed visibly in the system console. This approach offers a significant advantage in terms of stealthiness, both in evading real-time monitoring solutions like EDRs, and postmortem digital forensic tools. The internal version number (1.0) indicates that this represents a new development effort by the attackers.

As the core utilities of Windows are proprietary and not open-source, the developers of LightlessCan faced a choice: either to reverse engineer the closed-source system binaries or to get inspired by the code available via the [Wine](#) project, where many [programs](#) are rewritten in order to mimic their execution on other platforms like Linux, macOS, or ChromeOS. We are inclined to believe the developers chose the first option, as the corresponding Wine programs they mimicked in LightlessCan were implemented a little bit differently or not at all (e.g., netsh).

Interestingly, in one of the cases we analyzed, the LightlessCan payload is stored in an encrypted file on the compromised machine, which can only be decrypted using an environment-dependent key. More details about this can be found in the [Execution chain 3: LightlessCan \(complex version\)](#) section. This is to ensure that the payload can only be decrypted on the computer of the intended victim and not, for example, on a device of a security researcher.

Table 2. The list of LightlessCan commands mimicking those for Windows prompt

Index	Description
33	Mimic the ipconfig command from the Windows command prompt; see Figure 4.
34	Mimic the net command from the Windows prompt; see Figure 5.
35	Mimic the netshadvfirewall firewall command from the Windows prompt; see Figure 4.
36	Mimic the netstat command from the Windows prompt.
37	Mimic the ping -6 command from the Windows prompt.
38	Mimic the reg command from the Windows prompt; see Figure 7.
39	Mimic the sc command from the Windows prompt; see Figure 8.
40	Mimic the ping command from the Windows prompt.
41	Mimic the tasklist command from the Windows prompt.
42	Mimic the wmic process call create command from the Windows prompt; see Figure 9.
43	Mimic the nslookup command from the Windows Server prompt.
44	Mimic the schtasks command from the Windows prompt; see Figure 10.
45	Mimic the systeminfo command from the Windows prompt.
46	Mimic the arp command from the Windows prompt.
47	Mimic the mkdir command from the Windows prompt.

```
.rdata:0000001800605F1          align 20h
.rdata:000000180060600      aHostName_0:          ; DATA XREF: Command_ipconfig+1A2f0
.rdata:000000180060600          text "UTF-16LE",      Host Name . . . . . : %s ,0Dh,0Ah,0
.rdata:000000180060658          align 20h
.rdata:000000180060660      aPrimaryDnsSuffix:   ; DATA XREF: Command_ipconfig+20A7f0
.rdata:000000180060660          text "UTF-16LE",      Primary Dns Suffix . . . . . : %s ,0Dh,0Ah,0
.rdata:0000001800606B8          align 20h
.rdata:0000001800606C0      aNodeType:           ; DATA XREF: Command_ipconfig+25D7f0
.rdata:0000001800606C0          text "UTF-16LE",      Node Type . . . . . : %s ,0Dh,0Ah,0
.rdata:000000180060718          align 20h
.rdata:000000180060720      aIpRoutingEnabled:   ; DATA XREF: Command_ipconfig+2977f0
.rdata:000000180060720          text "UTF-16LE",      IP Routing Enabled. . . . . : %s ,0Ah,0
.rdata:000000180060776          align 20h
.rdata:000000180060780      aWinsProxyEnabled:   ; DATA XREF: Command_ipconfig+2CE7f0
.rdata:000000180060780          text "UTF-16LE",      WINS Proxy Enabled. . . . . : %s ,0Ah,0
.rdata:0000001800607D6          align 20h
.rdata:0000001800607E0      aDnsSuffixSearch:    ; DATA XREF: Command_ipconfig+3777f0
.rdata:0000001800607E0          text "UTF-16LE",      DNS Suffix Search List. . . . . : %s ,0Dh,0Ah,0
.rdata:000000180060838 ; const char a_GetAdaptersInfo[]
.rdata:000000180060838      a_GetAdaptersInfo db '=ICrk\gUAK8vS/t',0
```

Figure 4. Hardcoded strings revealing the subset of the ipconfig functionality

```
.rdata:00000018005E400      net_params          wide_char_260 <'unknown'>
.rdata:00000018005E400          ; DATA XREF: Command_net:loc_180004995f0
.rdata:00000018005E400          ; sub_180004B20:loc_180004BE0 to ...
.rdata:00000018005E608          wide_char_260 <'use'>
.rdata:00000018005E810          wide_char_260 <'user'>
.rdata:00000018005EA18          wide_char_260 <'share'>
.rdata:00000018005EC20          wide_char_260 <'view'>
.rdata:00000018005EE28          wide_char_260 <'group'>
.rdata:00000018005F030          wide_char_260 <'localgroup'>
.rdata:00000018005F238          wide_char_260 <'delete'>
.rdata:00000018005F440          wide_char_260 <'del'>
.rdata:00000018005F648          wide_char_260 <'user'>
.rdata:00000018005F850          wide_char_260 <'u'>
.rdata:00000018005FA58          wide_char_260 <'add'>
.rdata:00000018005FC60          wide_char_260 <'domain'>
```

Figure 5. Hardcoded strings revealing the subset of the net functionality

```
.rdata:00000018005CBA0      netsh_params        wide_char_260 <'unknown'>
.rdata:00000018005CBA0          ; DATA XREF: Command_netsh+56f0
.rdata:00000018005CBA0          ; Command_netsh:loc_18000ACC0 to ...
.rdata:00000018005CDA8          wide_char_260 <'add'>
.rdata:00000018005CFB0          wide_char_260 <'show'>
.rdata:00000018005D1B8          wide_char_260 <'delete'>
.rdata:00000018005D3C0          wide_char_260 <'name='>
.rdata:00000018005D5C8          wide_char_260 <'dir='>
.rdata:00000018005D7D0          wide_char_260 <'action='>
.rdata:00000018005D9D8          wide_char_260 <'protocol='>
.rdata:00000018005DBE0          wide_char_260 <'localport='>
.rdata:00000018005DDE8          wide_char_260 <'remoteport='>
.rdata:00000018005DFF0          wide_char_260 <'description'>
.rdata:00000018005E1F8          wide_char_260 <'program='>
```

Figure 6. Hardcoded strings revealing the netsh firewall functionality

```

.rdata:000000018005AD20 reg_params wide_char_260 <'unknown'>
.rdata:000000018005AD20 ; DATA XREF: Command_reg+531o
.rdata:000000018005AD20 ; sub_18000EC10:loc_18000ED101o
.rdata:000000018005AF28 wide_char_260 <'query'>
.rdata:000000018005B130 wide_char_260 <'add'>
.rdata:000000018005B338 wide_char_260 <'delete'>
.rdata:000000018005B540 wide_char_260 <'save'>
.rdata:000000018005B748 wide_char_260 <'/'v'>
.rdata:000000018005B950 wide_char_260 <'/'ve'>
.rdata:000000018005BB58 wide_char_260 <'/'s'>
.rdata:000000018005BD60 wide_char_260 <'/'se'>
.rdata:000000018005BF68 wide_char_260 <'/'f'>
.rdata:000000018005C170 wide_char_260 <'/'k'>
.rdata:000000018005C378 wide_char_260 <'/'d'>
.rdata:000000018005C580 wide_char_260 <'/'t'>
.rdata:000000018005C788 wide_char_260 <'/'va'>
.rdata:000000018005C990 wide_char_260 <'/'y'>

```

Figure 7. Hardcoded strings revealing the (partial) reg functionality

```

.rdata:00000001800592B0 sc_params wide_char_260 <'unknown'>
.rdata:00000001800592B0 ; DATA XREF: Command_sc:loc_180010BA01o
.rdata:00000001800592B0 ; sub_180010D00:loc_180010D921o
.rdata:0000000180059488 wide_char_260 <'create'>
.rdata:00000001800596C0 wide_char_260 <'delete'>
.rdata:00000001800598C8 wide_char_260 <'stop'>
.rdata:0000000180059AD0 wide_char_260 <'query'>
.rdata:0000000180059CD8 wide_char_260 <'start'>
.rdata:0000000180059EE0 wide_char_260 <'binpath='>
.rdata:000000018005A0E8 wide_char_260 <'type='>
.rdata:000000018005A2F0 wide_char_260 <'start='>
.rdata:000000018005A4F8 wide_char_260 <'error='>
.rdata:000000018005A700 wide_char_260 <'displayname='>
.rdata:000000018005A908 wide_char_260 <'obj='>
.rdata:000000018005AB10 wide_char_260 <'password='>

```

Figure 8. Hardcoded strings revealing the (partial) sc functionality

```

.rdata:00000001800520F0 wmic_params wide_char_260 <'unknown'>
.rdata:00000001800520F0 ; DATA XREF: Command_wmic+4E1o
.rdata:00000001800522F8 wide_char_260 <'process'>
.rdata:0000000180052500 wide_char_260 <'call'>
.rdata:0000000180052708 wide_char_260 <'create'>
.rdata:0000000180052910 wide_char_260 <'/'node'>
.rdata:0000000180052B18 wide_char_260 <'/'user'>
.rdata:0000000180052D20 wide_char_260 <'/'password'>
.rdata:0000000180052F28 wide_char_260 <'/'wql'>

```

Figure 9. Hardcoded strings revealing the wmic process call create functionality

```

.rdata:0000000180053130 schtasks_params wide_char_260 <'unknown'>
.rdata:0000000180053130 ; DATA XREF: Command_schtasks+461o
.rdata:0000000180053130 ; Command_schtasks:loc_1800122A01o
.rdata:0000000180053338 wide_char_260 <'/'create'>
.rdata:0000000180053540 wide_char_260 <'/'delete'>
.rdata:0000000180053748 wide_char_260 <'/'query'>
.rdata:0000000180053950 wide_char_260 <'/'change'>
.rdata:0000000180053B58 wide_char_260 <'/'run'>
.rdata:0000000180053D60 wide_char_260 <'/'end'>
.rdata:0000000180053F68 wide_char_260 <'/'s'>
.rdata:0000000180054170 wide_char_260 <'/'u'>
.rdata:0000000180054378 wide_char_260 <'/'p'>
.rdata:0000000180054580 wide_char_260 <'/'ru'>
.rdata:0000000180054788 wide_char_260 <'/'rp'>
.rdata:0000000180054990 wide_char_260 <'/'sc'>
.rdata:0000000180054B98 wide_char_260 <'/'mo'>
.rdata:0000000180054DA0 wide_char_260 <'/'d'>
.rdata:0000000180054FA8 wide_char_260 <'/'m'>
.rdata:00000001800551B0 wide_char_260 <'/'i'>
.rdata:00000001800553B8 wide_char_260 <'/'tn'>
.rdata:00000001800555C0 wide_char_260 <'/'tr'>
.rdata:00000001800557C8 wide_char_260 <'/'args'>

```

Figure 10. Hardcoded strings revealing the (partial) schtasks functionality

Furthermore, an examination of the RAT's internal configuration suggests that, in comparison to BlindingCan, Lazarus increased the code sophistication in LightlessCan.

## Technical analysis

In this section, we provide technical details about the compromise chain that delivers the NickelLoader downloader, and the three execution chains Lazarus used to deliver its payloads on the compromised system.

### Compromise chain: NickelLoader

NickelLoader is an HTTP(S) downloader executed on the compromised system via DLL side-loading, which is later used to deliver other Lazarus payloads.

The process of delivering NickelLoader unfolds in a series of stages, commencing with the execution of PresentationHost.exe, which is triggered automatically after the target manually executes the initial quiz challenges; the Quiz1 case is depicted in Figure 3. A malicious dynamically linked library, mscoree.dll, is then side-loaded by the legitimate PresentationHost.exe – both located in C:\ProgramShared\. This DLL is a trojanized NppPluginDll.dll, from the inactive [General Python Plugins DLL for Notepad++](#) project from 2011. It serves as a dropper and has

various exports: all the exports copied from the original NppyPluginDll.dll plus all the exports from the legitimate mscoree.dll. One of these legitimate exports, CorExitProcess, contains the malicious code responsible for the decryption and execution of the next malware stage.

To successfully decrypt an encrypted data array embedded in the dropper, three 16-character-long keywords are required by the dropper. These keywords are as follows:

1. the name of the parent process (PresentationHost),
2. the internal parameter hardcoded in the binary (9zCnQP6o78753qg8), and
3. the external parameter passed on the command line (-embeddingObject), which is inherited from the parent process of PresentationHost.exe, being provided by Quiz1.exe or Quiz2.exe.

The keywords are XOR-ed byte by byte and the output forms the AES-128 decryption key.

The payload is an HTTP(S) downloader that recognizes four commands, all five letters long, shown in Table 3. Because of those five letter commands, we chose to name this payload “NickelLoader”, drawing inspiration from the colloquial term for the US five-cent coin – a nickel. The most important commands are avdrq and gabnc. When these commands are issued, each of them loads data received from the C&C server as a DLL. For this purpose, the attackers probably used [MemoryModule](#), a library that can be used to load a DLL completely from memory.

Table 3. The list of magic keywords recognized in received buffers

Keyword	Description
abcde	Requests another immediate command without the usual long sleep delay that separates the execution of the commands.
avdrq	Loads a DLL contained in the received buffer and executes its hardcoded export info.
gabnc	Loads a DLL contained in the received buffer.
dcrqv	Terminates itself.

### Execution chain 1: miniBlindingCan

One of the payloads downloaded and executed by NickelLoader is miniBlindingCan, a simplified version of the group’s flagship BlindingCan RAT. It was reported for the first time by [Mandiant](#) in September 2022, under the name AIRDRY.V2.

To load miniBlindingCan, a 64-bit malicious dynamically linked library colorui.dll is side-loaded by a legitimate colorcpl.exe executed from C:\ProgramData\Adobe\ and serves as a dropper. The DLL is obfuscated using VMProtect and contains thousands of exports from which LaunchColorCpl is the most important, as it handles the execution of the next stage. There’s an encrypted data array in the DLL’s dumped body, together with multiple debug symbols revealing the root directory and the project from which it was built:

W:\Develop\Tool\ShellCodeLoader\App\libressl-2.6.5\

As the name ShellCodeLoader suggests, the main purpose of this initial stage is to decrypt and load the data array from its body, which contains shellcode. At the beginning of its execution, ShellCodeLoader employs anti-debugging techniques by inspecting the BeingDebugged value within the Process Environment Block (PEB) structure to determine if it’s being scrutinized or analyzed by debugging tools, and utilizes anti-sandbox techniques to avoid detection within sandboxed environments designed for security analysis. The malware also explicitly checks whether its parent process is colorcpl.exe; if not, it exits immediately.

The decrypted data array is not a complete DLL, but forms an intermediate blob with two parts: shellcode followed by another encrypted data array, which represents the last step of the chain. The shellcode seems to be produced by an instance of the open-source project [ShellcodeRDI](#) – in particular, the ShellcodeRDI.c code. It was probably produced by executing the Python script ConvertToShellcode.py from this project on a payload DLL acting as a source for [reflective DLL injection](#).

The final payload is extracted and decrypted using XOR with a long key, which is a string built by concatenating the name of the parent process (colorcpl.exe), the filename of the dropper (colorui.dll), and the external command line parameter – in this case resulting in COLORCPL.EXECOLORUI.DLL669498484488D3F22712CC5BACA6B7A7. This process is akin to what we observed with BlindingCan backdoor in the Dutch case we previously described in [this WeLiveSecurity blogpost](#). The decryption reveals an executable with download-and-execute functionality, whose internal logic of sending and parsing commands is strongly reminiscent of BlindingCan, a flagship HTTP(S) Lazarus RAT. Unlike the case in the Netherlands, it is not VMProtect-ed and it supports only a small subset of commands available previously: compare Table 4 in this blogpost and Table 3 in the [blogpost on the Dutch case](#) from September 2022. Because the features of this RAT are notably scaled down compared to those in BlindingCan, and yet they seem to share the same server-side infrastructure, we have chosen to distinguish it by appending the prefix “mini-“ to its name, highlighting its reduced functionality compared to its fully-featured RAT counterpart.

Table 4. Commands of miniBlindingCan

Command ID	Description
8201	Send system information like computer name, Windows version, and code page.

Command ID	Description
8232	Update the current communication interval with a value provided by the C&C server.
8233	Discontinue the command execution.
8241	Send the current configuration of size 9,392 bytes to the C&C server.
8242	Update the configuration of size 9,392 bytes, stored encrypted on the file system.
8247	Wait for the next command.
8248	Update the current communication interval with a value stored in the configuration.
8274	Download and decrypt a file from the C&C server.
8279	Execute shellcode passed as a parameter.

Figure 11 shows the decrypted state of a 9,392-byte-long configuration embedded in the RAT. It contains five URLs, in this case compromised websites, each limited by a maximum size of 260 wide characters.

```

00000000: 00 00 05 00-00 00 68 00-74 00 74 00-70 00 73 00  https
00000010: 3A 00 2F 00-2F 00 74 00-75 00 72 00-6E 00 73 00  : // turns
00000020: 63 00 6F 00-72 00 2E 00-63 00 6F 00-6D 00 2F 00  cor.com /
00000030: 77 00 70 00-2D 00 69 00-6E 00 63 00-6C 00 75 00  wp-inclu
00000040: 64 00 65 00-73 00 2F 00-63 00 6F 00-6E 00 74 00  des / cont
00000050: 61 00 63 00-74 00 73 00-2E 00 70 00-68 00 70 00  acts.php

00000820: 00 00 00 00-00 00 68 00-74 00 74 00-70 00 73 00  https
00000830: 3A 00 2F 00-2F 00 77 00-77 00 77 00-2E 00 65 00  : // www.e
00000840: 6C 00 69 00-74 00 65 00-34 00 70 00-72 00 69 00  lite4pri
00000850: 6E 00 74 00-2E 00 63 00-6F 00 6D 00-2F 00 73 00  nt.com / s
00000860: 75 00 70 00-70 00 6F 00-72 00 74 00-2F 00 73 00  upport / s
00000870: 75 00 70 00-70 00 6F 00-72 00 74 00-2E 00 61 00  upport.a
00000880: 73 00 70 00-00 00 00 00-00 00 00 00-00 00 00 00  sp

000018A0: 63 00 3A 00-5C 00 77 00-69 00 6E 00-64 00 6F 00  c : \ windo
000018B0: 77 00 73 00-5C 00 73 00-79 00 73 00-74 00 65 00  ws \ syste
000018C0: 6D 00 33 00-32 00 5C 00-63 00 6D 00-64 00 2E 00  m 3 2 \ cmd .
000018D0: 65 00 78 00-65 00 00 00-00 00 00 00-00 00 00 00  exe

00001AA0: 00 00 00 00-00 00 00 00-25 00 74 00-65 00 6D 00  % tem
00001AB0: 70 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  p

00002490: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
000024A0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00

```

Figure 11. A configuration of the miniBlindingCan backdoor. The highlighted value is the count of URLs, but only the first and the last of the five URLs are shown here. The purpose of the last two wide strings is not known

## Execution chain 2: LightlessCan (simple version)

Another payload we have seen executed by NickelLoader is LightlessCan, a new Lazarus backdoor. We have observed two different chains loading this backdoor.

In the simple version of the chain, the dropper of this payload is the malicious dynamically linked library mapistub.dll that is side-loaded by the legitimate fixmapi.exe executed from C:\ProgramData\Oracle\Java\. The DLL is a trojanized Lua plugin, version 1.4, with all the exports copied from the legitimate Windows mapi32.dll. The export FixMAPI contains malicious code responsible for decrypting and loading the next stage; all the other exports contain benign code sourced from a publicly available [MineSweeper sample project](#). This mapistub.dll dropper has persistence established via a scheduled task. Unfortunately, we lack additional details about this task, except that its parent process appears as %WINDOWS%\system32\svchost.exe -k netsvcs -p -s Schedule.

To successfully decrypt the embedded data array, the dropper needs three keywords to be provided correctly:

1. the name of the parent process (fixmapi.exe),
2. the internal parameter hardcoded in the binary (IP7pdINfE9uMz63n), and
3. the external parameter passed in the command line (AudioEndpointBuilder).

The keywords are XOR-ed byte by byte and the output forms a 128-bit AES key to be used for decryption. Note that the length of the keywords are not all exactly 16 bytes, but the decryption process will still work if the oversized string is truncated to a 16-byte length (for instance, AudioEndpointBuilder to AudioEndpointBui), and the undersized string, fixmapi.exe, is treated as fixmapi.exe\x00\x00\x00\x00, because the string was initialized as 260 instances of the NUL character.

## Execution chain 3: LightlessCan (complex version)

The most complex chain we observed on the compromised system also delivers LightlessCan, with various components involved in the complete chain of installation stages: a legitimate application, an initial dropper, a complete dropper (which contains the configuration), an intermediate dropper, a configuration file, a file with system information (for the decryption of encrypted payloads on the file system), an intermediate loader and the final step, the LightlessCan RAT. The connections and relationships among these files are illustrated in Figure 12.



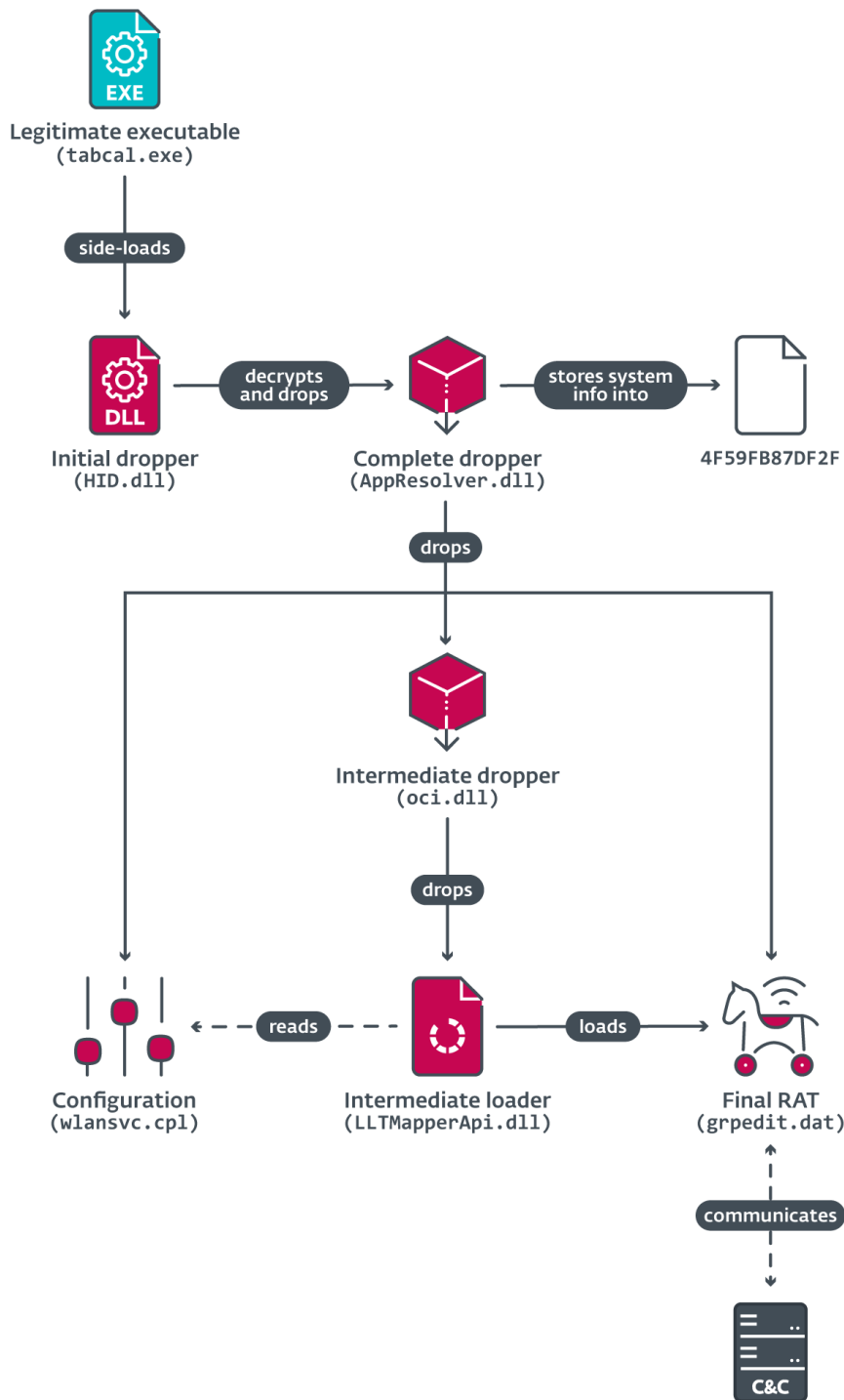


Figure 12. A complex chain of stages delivering the fourth payload

The initial dropper of the fourth chain is a malicious dynamically linked library HID.dll that is side-loaded by a legitimate executable, tabcal.exe, executed from C:\ProgramData\Adobe\ARM\l. The DLL is a trojanized version of MZC8051.dll, a legitimate file from the 8051 C compiler plugin project for Notepad++. It contains all the exports from the original project, but also the necessary exports from the legitimate Hid User Library by Microsoft, so that the side-loading by tabcal.exe will be successful. The export HidD\_GetHidGuid contains the malicious code responsible for dropping the next stage and, as in the case of the dropper of the previous chain (Execution chain 2), all the other exports contain the benign MineSweeper code.

As in the previous cases, three long keywords must be provided to decrypt the embedded payload:

1. the name of the parent process (tabcal.exe),
2. the internal parameter hardcoded in the binary (9zCnQP6o78753qg8), and
3. the external parameter (LocalServiceNetworkRestricted) – this time not expressed as a command line parameter, but instead as the content of a file located at %WINDOVS%\system32\thumbs.db.

Again, the keywords are XOR-ed byte by byte and the output forms a 128-bit AES key to be used for the decryption. As in the previous case, the lengths of the keywords are not all exactly 16 bytes, but the decryption will still work if the

oversized string is truncated (for instance, to LocalServiceNetw) and the undersized string is extended with nulls (for instance, to tabcal.exe\x00\x00\x00\x00\x00\x00).

The executable produced by the above recipe is the complete dropper from Figure 12 and has the InternalName resource AppResolver.dll (found in the VERSIONINFO resource). It contains two encrypted data arrays: a small one of 126 bytes, and a large one of 1,807,464 bytes (which contains three subparts). First, it decrypts the small array using the RC6 algorithm with the hardcoded 256-bit key DA 48 A3 14 8D BF E2 D2 EF 91 12 11 FF 75 59 A3 E1 6E A0 64 B8 78 89 77 A0 37 91 58 5A FF FF 07. The output represents paths to which the first two subparts of the large blob are dropped (i.e., LightlessCan and the intermediate dropper), and yields the strings C:\windows\system32\oci.dll and C:\windows\system32\grpedit.dat.

Next, it continues with decrypting the second data array – the large blob – using the same encryption key as before. The result is a decrypted blob containing three subparts: a DLL corresponding to grpedit.dat (LightlessCan), a DLL corresponding to oci.dll (the intermediate dropper), and a 14,948 byte encrypted file dropped to %WINDOWS%\System32\wlsnvc.cpl (configuration); as depicted in Figure 13.

```

00000000: 01 00 00 00-01 00 00 00-01 00 00 00-00 00 00 00  @ @ @
00000010: 1E 00 00 00-05 00 00 00-00 00 00 00-00 00 00 00  ^ +
00000020: 00 00 00 00-05 00 00 00-BE 2C 00 00-4D 00 53 00  + =, M S
00000030: 44 00 54 00-43 00 00 00-00 00 00 00-00 00 00 00  D T C
000000A0: 00 00 00 00-00 00 00 00-00 00 00 00-0F 00 63 00  o c
000000B0: 69 00 2E 00-64 00 6C 00-6C 00 00 00-00 00 00 00  i . d l l
00000120: 00 00 00 00-00 00 00 00-00 00 00 00-43 00 3A 00  C :
00000130: 5C 00 77 00-69 00 6E 00-64 00 6F 00-77 00 73 00  \ w i n d o w s
00000140: 5C 00 73 00-79 00 73 00-74 00 65 00-6D 00 33 00  \ s y s t e m 3
00000150: 32 00 5C 00-6F 00 63 00-69 00 2E 00-64 00 6C 00  2 \ o c i . d l
00000160: 6C 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  l
00000930: 43 00 3A 00-5C 00 77 00-69 00 6E 00-64 00 6F 00  C : \ w i n d o
00000940: 77 00 73 00-5C 00 73 00-79 00 73 00-74 00 65 00  w s \ s y s t e
00000950: 6D 00 33 00-32 00 5C 00-67 00 72 00-70 00 65 00  m 3 2 \ g r p e
00000960: 64 00 69 00-74 00 2E 00-64 00 61 00-74 00 00 00  d i t . d a t
00001130: 00 00 00 00-68 00 74 00-74 00 70 00-73 00 3A 00  h t t p s :
00001140: 2F 00 2F 00-6B 00 61 00-70 00 61 00-74 00 61 00  / / k a p a t a
00001150: 2D 00 61 00-72 00 6B 00-65 00 6F 00-6C 00 6F 00  - a r k e o l o
00001160: 67 00 69 00-2E 00 6B 00-65 00 6D 00-64 00 69 00  g i . k e m d i
00001170: 6B 00 62 00-75 00 64 00-2E 00 67 00-6F 00 2E 00  k b u d . g o .
00001180: 69 00 64 00-2F 00 70 00-61 00 67 00-65 00 73 00  i d / p a g e s
00001190: 2F 00 70 00-61 00 79 00-6D 00 65 00-6E 00 74 00  / p a y m e n t
000011A0: 2F 00 70 00-61 00 79 00-6D 00 65 00-6E 00 74 00  / p a y m e n t
000011B0: 2E 00 70 00-68 00 70 00-00 00 00 00-00 00 00 00  . p h p
000011C0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00003A30: 00 00 00 00-00 00 31 00-2E 00 30 00-00 00 00 00  1 . 0
00003A40: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00003A50: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00003A60: 00 00 00 00- - - -

```

Figure 13. The decrypted configuration stored in wlsnvc.cpl

Moreover, the complete dropper also stores several characteristics identifying the compromised system in the file %WINDOWS%\System32\4F59FB87DF2F, whose name is hardcoded in the binary. These characteristics are primarily retrieved from the Computer\HKLML\HARDWARE\DESCRIPTION\System\BIOS registry path. Here are the specific values of these characteristics, along with a PowerShell command provided in brackets that can be used to display the corresponding value on any Windows machine:

- SystemBIOSDate (Get-ItemProperty "HKLM:\HARDWARE\Description\System\BIOS" -Name BIOSReleaseDate | Select-Object -Property BIOSReleaseDate)
- SystemBIOSVersion (Get-CimInstance -ClassName Win32\_Bios | Select-Object -Property Version)
- SystemManufacturer (Get-CimInstance -ClassName Win32\_ComputerSystem | Select-Object -Property Manufacturer)
- SystemProductName (Get-CimInstance -ClassName Win32\_ComputerSystemProduct | Select-Object -Property Name)
- Identifier in Computer\HKEY\_LOCAL\_MACHINE\HARDWARE\DESCRIPTION\System\MultifunctionAdapter\0\DiskController\0\DiskPeripheral\0

The concatenation of the values is required for decryption of the encrypted grpedit.dat from the file system. On a test machine running an image of Windows 10 on VMWare, the output can be:

```
11/12/20INTEL - 6040000VMware, Inc.VMware Virtual Platform656ba047-20b25a2a-A
```

The oci.dll file is another dropping layer – the intermediate dropper that drops the intermediate loader, which is a payload similar to the one described in the previously mentioned Dutch case. Again, the attackers used an open-source project, the Flashing Tip plugin for Notepad++, which is no longer available online. Unlike the previous cases, only two long keywords must be provided in order to decrypt the embedded payload successfully using AES-128:

1. the name of the parent process (msdtc.exe), and
2. the internal parameter hardcoded in the binary (fb5XPNCr8v83Y85P).

Both keywords are XOR-ed byte by byte (the parent process name is truncated, or padded with NULLs, as necessary to fill 16 bytes). The product of the decryption is the intermediate loader (LLTMapperAPI.dll). It uses the system information (same as the values stored in 4F59FB87DF2F) to decrypt the configuration file wiansvc.cpl and to locate, decrypt, and load the encrypted grpedit.dat, which is LightlessCan, the new full-featured RAT.

## Conclusion

We have described a new Lazarus attack that originated on LinkedIn where fake recruiters approached their potential victims, who were using corporate computers for personal purposes. Even though public awareness of these types of attacks should be high, the success rates of these campaigns have still not dropped to zero.

The most worrying aspect of the attack is the new type of payload, LightlessCan, a complex and possibly evolving tool that exhibits a high level of sophistication in its design and operation, representing a significant advancement in malicious capabilities compared to its predecessor, BlindingCan.

The attackers can now significantly limit the execution traces of their favorite Windows command line programs that are heavily used in their post-compromise activity. This maneuver has far-reaching implications, impacting the effectiveness of both real-time monitoring solutions and of post-mortem digital forensic tools.

For any inquiries about our research published on WeLiveSecurity, please contact us at [threatintel@eset.com](mailto:threatintel@eset.com).

ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

## IoCs

### Files

SHA-1	Filename	Detection
C273B244EA7DFF20B1D6B1C7FD97F343201984B3	%TEMP%\7zOC35416EE\Quiz1.exe	Win64/NukeSped.KT
38736CA46D7FC9B9E5C74D192EEC26F951E45752	%TEMP%\7zOCB3CC96D\Quiz2.exe	Win64/NukeSped.KT
C830B895FB934291507E490280164CC4234929F0	%ALLUSERSPROFILE%\Adobe\colorui.dll	Win64/NukeSped.KV
8CB37FA97E936F45FA8ECD7EB5CFB68545810A22	N/A	Win64/NukeSped.KU
0F33ECE7C32074520FBFA46314D7D5AB9265EC52	%ALLUSERSPROFILE%\Oracle\Java\mapistub.dll	Win64/NukeSped.KW
C7C6027ABDCED3093288AB75FAB907C598E0237D	N/A	Win64/NukeSped.KW
C136DD71F45EAEF3206BF5C03412195227D15F38	C:\ProgramShared\mscoree.dll	Win64/NukeSped.KT
E61672B23DBD03FE3B97EE469FA0895ED1F9185D	N/A	Win64/NukeSped.KT
E18B9743EC203AB49D3B57FED6DF5A99061F80E0	%ALLUSERSPROFILE%\Adobe\ARM\HID.dll	Win64/NukeSped.KX
10BD3E6BA6A48D3F2E056C4F974D90549AED1B96	N/A	Win64/NukeSped.KT
3007DDA05CA8C7DE85CD169F3773D43B1A009318	%WINDIR%\system32\grpedit.dat	Win64/NukeSped.KW
247C5F59CFFBAF099203F5BA3680F82A95C51E6E	%WINDIR%\system32\loci.dll	@Trojan.Win64/NukeSp
EBD3EF268C71A0ED11AE103AA745F1D8A63DDF13	N/A	Win64/NukeSped.KT

### Network

IP	Domain	Hosting provider	First seen	Details
46.105.57[.]169	bug.restoroad[.]com	OVH SAS	2021-10-10	A compromised legitimate site hosting the C&C server: <a href="http://bug.restoroad[.]com/admin/view_status.php">http://bug.restoroad[.]com/admin/view_status.php</a>
50.192.28[.]29	hurricanepub[.]com	Comcast Cable Communications, LLC	2020-01-06	A compromised legitimate site hosting the C&C server: <a href="https://hurricanepub[.]com/include/include.php">https://hurricanepub[.]com/include/include.php</a>
67.225.140[.]4	turnscor[.]com	Liquid Web, L.L.C	2020-01-03	A compromised legitimate WordPress-based site hosting the C&C server: <a href="https://turnscor[.]com/wp-includes/contacts.php">https://turnscor[.]com/wp-includes/contacts.php</a>
78.11.12[.]13	mantis.quick.net[.]pl	Netia SA	2021-03-22	A compromised legitimate site hosting the C&C server: <a href="http://mantis.quick.net[.]pl/library/secimage/index.php">http://mantis.quick.net[.]pl/library/secimage/index.php</a>
89.187.86[.]214	www.radiographers[.]org	Coreix Ltd	2020-10-23	A compromised legitimate site hosting the C&C server: <a href="https://www.radiographers[.]org/aboutus/aboutus.php">https://www.radiographers[.]org/aboutus/aboutus.php</a>
118.98.221[.]14	kapata- arkeologi.kemdikbud.go[.]id	Pustekkom	2020-01-02	A compromised legitimate site hosting the C&C server: <a href="https://kapata-&lt;br/&gt;arkeologi.kemdikbud.go[.]id/pages/payment/payment.pr">https://kapata- arkeologi.kemdikbud.go[.]id/pages/payment/payment.pr</a>
160.153.33[.]195	barsaji.com[.]mx	GoDaddy.com, LLC	2020-03-27	A compromised legitimate site hosting the C&C server: <a href="http://barsaji.com[.]mx/src/recaptcha/index.php">http://barsaji.com[.]mx/src/recaptcha/index.php</a>
175.207.13[.]231	www.keewoom.co[.]kr	Korea Telecom	2021-01-17	A compromised legitimate site hosting the C&C server: <a href="http://www.keewoom.co[.]kr/prod_img/201409/prod.php">http://www.keewoom.co[.]kr/prod_img/201409/prod.php</a>

IP	Domain	Hosting provider	First seen	Details
178.251.26[.]65	kerstpakketten.horesca-meppel[.]nl	InterRacks B.V.	2020-11-02	A compromised legitimate WordPress-based site hosting the C&C server: <a href="https://kerstpakketten.horesca-meppel[.]nl/wp-content/plugins/woocommerce/lib.php">https://kerstpakketten.horesca-meppel[.]nl/wp-content/plugins/woocommerce/lib.php</a>
185.51.65[.]233	kittimasszazs[.]hu	DoclerNet Operations, ORG-DHK1-RIPE	2020-02-22	A compromised legitimate site hosting the C&C server: <a href="https://kittimasszazs[.]hu/images/virag.php">https://kittimasszazs[.]hu/images/virag.php</a>
199.188.206[.]75	nrfm[.]lk	Namecheap, Inc.	2021-03-13	A compromised legitimate WordPress-based site hosting the C&C server: <a href="https://nrfm[.]lk/wp-includes/SimplePie/content.php">https://nrfm[.]lk/wp-includes/SimplePie/content.php</a>

## MITRE ATT&CK techniques

This table was built using [version 13](#) of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Reconnaissance	<a href="#">T1593.001</a>	Search Open Websites/Domains: Social Media	Lazarus attackers used LinkedIn to identify and contact specific employees of a company of interest.
	<a href="#">T1584.004</a>	Acquire Infrastructure: Server	Compromised servers were used by the Lazarus HTTP(S) backdoors and the downloader for C&C.
Resource Development	<a href="#">T1585.001</a>	Establish Accounts: Social Media Accounts	Lazarus attackers created a fake LinkedIn identity of a headhunter from Meta.
	<a href="#">T1585.003</a>	Establish Accounts: Cloud Accounts	Lazarus attackers had to create an account on a third-party cloud storage in order to deliver the initial ISO images.
	<a href="#">T1587.001</a>	Develop Capabilities: Malware	Custom tools from the attack are likely developed by the attackers. Some exhibit highly specific kernel development capacities seen earlier in Lazarus tools.
	<a href="#">T1608.001</a>	Stage Capabilities: Upload Malware	Lazarus attackers uploaded the initial ISO images to a cloud storage.
	Initial Access	<a href="#">T1566.002</a>	Phishing: Spearphishing Link
<a href="#">T1566.003</a>		Phishing: Spearphishing via Service	The target was contacted via LinkedIn Messaging.
Execution	<a href="#">T1106</a>	Native API	Windows APIs are essential for miniBlindingCan and LightlessCan to function and are resolved dynamically at runtime.
	<a href="#">T1053</a>	Scheduled Task/Job	Based on the parent process, a scheduled task was probably created to trigger the simple chain of the LightlessCan execution.
	<a href="#">T1129</a>	Shared Modules	NickelLoader can load and execute an arbitrary DLL within memory.
	<a href="#">T1204.002</a>	User Execution: Malicious File	Lazarus attackers relied on the execution of Quiz1.exe and Quiz2.exe from the ISO files.
	<a href="#">T1047</a>	Windows Management Instrumentation	One of the LightlessCan commands allows creation of a new process via WMI.
Persistence	<a href="#">T1053</a>	Scheduled Task/Job	Based on the parent process, a scheduled task was probably created to trigger the simple chain of the LightlessCan execution. Moreover, LightlessCan can mimic the schtasks command.
Defense Evasion	<a href="#">T1134.002</a>	Access Token Manipulation: Create Process with Token	LightlessCan can create a new process in the security context of the user represented by the specified token and collect the output.
	<a href="#">T1622</a>	Debugger Evasion	There's an anti-debug check in the dropper of miniBlindingCan.

Tactic	ID	Name	Description
	T1480	Execution Guardrails	There's a parent process check in the miniBlindingCan dropper. The concatenation of the values is required for decryption of the encrypted LightlessCan from the file system.
	T1140	Deobfuscate/Decode Files or Information	Many of these Lazarus tools and configurations are encrypted on the file system, e.g., LightlessCan in grpedit.dat and its configuration in wlansvc.cpl.
	T1574.002	Hijack Execution Flow: DLL Side-Loading	Many of the Lazarus droppers and loaders use a legitimate program for their loading.
	T1027.002	Obfuscated Files or Information: Software Packing	Lazarus obfuscated several executables by VMProtect in this attack, e.g., colorui.dll
	T1027.007	Obfuscated Files or Information: Dynamic API Resolution	Both LightlessCan and miniBlindingCan resolve Windows APIs dynamically.
	T1027.009	Obfuscated Files or Information: Embedded Payloads	The droppers of all malicious chains contain an embedded data array with an additional stage.
	T1562.003	Impair Defenses: Impair Command History Logging	New features of LightlessCan mimic the most useful Windows command line utilities, to avoid executing the original console utilities.
	T1562.004	Impair Defenses: Disable or Modify System Firewall	LightlessCan can mimic the netsh command and interact with firewall rules.
	T1070.004	Indicator Removal: File Deletion	LightlessCan has the ability to delete files securely.
	T1070.006	Indicator Removal: Timestomp	LightlessCan can alter the modification timestamps of files.
	T1202	Indirect Command Execution	LightlessCan bypasses command execution by implementing their functionality.
	T1055	Process Injection	LightlessCan and miniBlindingCan use various types of process injection.
	T1497.003	Virtualization/Sandbox Evasion: Time Based Evasion	The miniBlindingCan dropper has an intentional initial execution delay.
	T1620	Reflective Code Loading	Most of the droppers use reflective DLL injection.
Discovery	T1083	File and Directory Discovery	LightlessCan can locate a file by its name.
	T1135	Network Share Discovery	LightlessCan can mimic the net share command.
	T1057	Process Discovery	LightlessCan identifies processes by name.
	T1012	Query Registry	LightlessCan queries the registry for various system information it uses for encryption.
	T1018	Remote System Discovery	LightlessCan can mimic the net view command.
	T1016	System Network Configuration Discovery	LightlessCan can mimic the arp and ipconfig commands.
	T1049	System Network Connections Discovery	LightlessCan can mimic the netstat command.
	T1007	System Service Discovery	LightlessCan can mimic the sc query and tasklist commands.
Command and Control	T1071.001	Application Layer Protocol: Web Protocols	NickelLoader, LightlessCan, and miniBlindingCan use HTTP and HTTPS for C&C.
	T1573.001	Encrypted Channel: Symmetric Cryptography	LightlessCan and miniBlindingCan encrypt C&C traffic using the AES-128 algorithm.
	T1132.001	Data Encoding: Standard Encoding	LightlessCan and miniBlindingCan encode C&C traffic using base64.
Exfiltration	T1041	Exfiltration Over C2 Channel	LightlessCan can exfiltrate data to its C&C server.

## References

- [1] Microsoft Security Threat Intelligence, "[ZINC weaponizing open-source software](#)," 29 September 2022. [Online].
- [2] D. Breitenbacher and O. Kaspars, "[Operation In\(ter\)ception: Aerospace and military companies in the crosshairs of cyberspies](#)," June 2020. [Online].
- [3] HVS-Consulting AG, "[Greetings from Lazarus: Anatomy of a cyber-espionage campaign](#)," 15 December 2020. [Online].
- [4] Positive Technologies Expert Security Center, "[Lazarus Group Recruitment: Threat Hunters vs Head Hunters](#)," Positive Technologies, 27 April 2021. [Online].
- [5] P. Kálnai, "[Amazon-themed campaigns of Lazarus in the Netherlands](#)," 30 September 2022. [Online].
- [6] P. Kálnai, "Lazarus campaigns and backdoors in 2022-2023," in Virus Bulletin International Conference, London, 2023.
- [7] A. Martin, "[Sony Pictures hacking traced to Thai hotel as North Korea denies involvement](#)," WeLiveSecurity.com, 08 December 2014. [Online].
- [8] P. Kálnai and M.-É. M. Leveillé, "[Linux malware strengthens links between Lazarus and the 3CX supply chain attack](#)," ESET, 20 April 2023. [Online].
- [9] Defense Intelligence Agency, North Korea military power : a growing regional and global threat, Washington, D.C.: U.S. Government Publishing Office, 2021, p. 98.
- [10] UN Panel of Experts, "[UN Security Council Resolutions](#)," 1993-2023. [Online].
- [11] ESET Editor, "[WannaCryptor aka WannaCry: Key questions answered](#)," WeLiveSecurity.com, 15 May 2017. [Online].
- [12] Security Council Committee, "[Sanctions Committee \(DPRK\), Panel of Experts, Reports](#)," United Nations Security Council, 2010-2023. [Online].
- [13] ClearSky Research Team, "[Operation 'Dream Job' Widespread North Korean Espionage Campaign](#)," 13 August 2020. [Online].
- [14] ESET Research, "[Threat Report T1 2022](#)," ESET, June 2022. [Online].
- [15] D. Staples, "[An Improved Reflective DLL Injection Technique](#)," 30 January 2015. [Online].
- [16] J. MacLachlan, M. Potaczek, N. Isakovic, M. Williams and Y. Gupta, "[It's Time to PuTTY! DPRK Job Opportunity Phishing via WhatsApp](#)," Mandiant, 14 September 2022. [Online].
- [17] S. Tomonaga, "[Windows Commands Abused by Attackers](#)," JPCERT/CC, 26 January 2016. [Online].

