# Taming the Storm: Understanding and Mitigating the Consequences of CVE-2023-27350

research.loginsoft.com/threat-research/taming-the-storm-understanding-and-mitigating-the-consequences-of-cve-2023-27350/

May 23, 2023

May 23, 2023
By Saharsh Agrawal

The world of cybersecurity is constantly evolving, with new threats emerging every day. One of the latest threats to emerge is the use of CVE-2023-27350 by threat actors to gain initial access to victim machines and servers. This vulnerability is found in the popular print management software, Papercut. In this blog post, we will explore how the threat actors of Cl0p, Lockbit, and Truebot malware are exploiting this vulnerability, and Osquery detections to safeguard from the risks it poses to businesses and organizations.

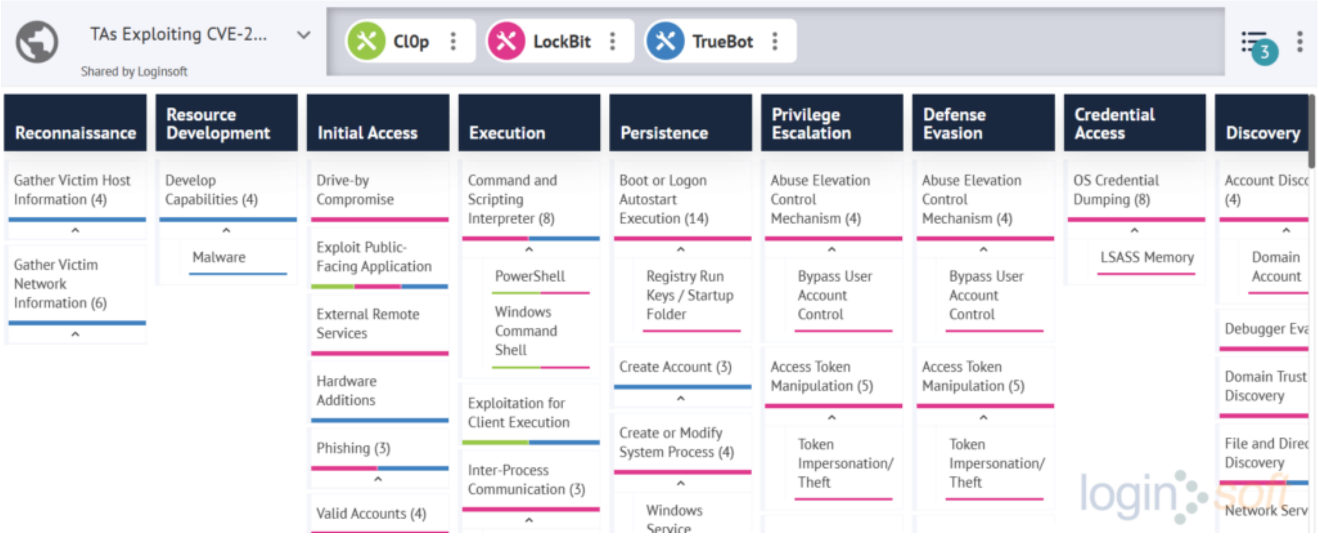
## What is CVE-2023-27350?

CVE-2023-27350 is a vulnerability found in Papercut, a popular printer management software used by businesses and organizations around the world. This vulnerability allows threat actors to gain unauthenticated remote access to victim's machines and servers by exploiting the vulnerability in the software. As Papercut runs with system administrator privileges, when the attacker exploits the vulnerability, they gain administrative privileges and has the ability to execute remote code on the hosted machine. Below you can find the vulnerable versions.

- 8.0.0 – 19.2.7
- 20.0.0 – 20.1.6
- 21.0.0 – 21.2.10
- 22.0.0 – 22.0.8

## How are TAs exploiting this vulnerability?

Numerous threat actors (TAs) have noticed this vulnerability and are exploiting it to gain initial access. Once they have gained a foothold on a system, they perform various Tactics, Techniques and Procedures (TTPs) to exploit the victims. The below image displays the TTPs for each malware deployed by these threat actors.



| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery |
|---|---|---|---|---|---|---|---|---|
| Gather Victim Host Information (4) | Develop Capabilities (4) | Drive-by Compromise | Command and Scripting Interpreter (8) | Boot or Logon Autostart Execution (14) | Abuse Elevation Control Mechanism (4) | Abuse Elevation Control Mechanism (4) | OS Credential Dumping (8) | Account Disc (4) |
| Gather Victim Network Information (6) | Malware | Exploit Public-Facing Application | PowerShell | Registry Run Keys / Startup Folder | Bypass User Account Control | Bypass User Account Control | LSASS Memory | Domain Account |
| | | External Remote Services | Windows Command Shell | Create Account (3) | Access Token Manipulation (5) | Access Token Manipulation (5) | | Debugger Eva |
| | | Hardware Additions | Exploitation for Client Execution | Create or Modify System Process (4) | Token Impersonation/ Theft | Token Impersonation/ Theft | | Domain Trust Discovery |
| | | Phishing (3) | Inter-Process Communication (3) | Windows Service | | | | File and Direc Discovery |
| | | Valid Accounts (4) | | | | | | Network Serv |

*Threat Actors (TAs) Exploiting CVE-2023-27350*

An important insight that can be gained from examining the TTPs of the malware is that the TAs are motivated by financial gain and achieve this by encrypting all user data by detonating ransomware. It's noteworthy that a significant number of schools use the Papercut software, which increases their vulnerability to attacks if they continue to use the vulnerable version.

## Detection

By utilizing the PoC shared by horizon3ai on GitHub, we successfully replicated CVE-2023-27350. This enabled us to develop detection mechanisms aimed at thwarting potential attackers who might attempt to exploit the CVE.

Below are specific osquery rules to help defend against the malicious behaviours exhibited by TAs exploiting CVE-2023-27350.

### PaperCut MF/NG CVE-2023-27350 Exploit

```
SELECT
      p1.name AS child_process_name,
      p1.pid AS child_process_id,
      p1.cmdline AS child_cmdline,
      p2.name AS parent_process_name,
      p2.pid AS parent_process_id,
      p2.cmdline AS parent_cmdline
    FROM processes p1, processes as p2
    ON p1.parent = p2.pid
    AND LOWER(parent_process_name) = 'pc-app.exe'
    AND LOWER(child_process_name) IN
('cmd.exe','powershell.exe','java.exe','certutil.exe','cscript.exe','wscript.exe','ft
p.exe','rundll32.exe','wmic.exe','curl.exe','regsvr32.exe');
```

### Abnormal LSASS Process Access and Injection

```
SELECT
      p1.name AS child_process,
      p1.pid AS child_process_id,
      p1.cmdline AS child_cmdline,
      p2.name AS parent_process,
      p2.pid AS parent_process_id,
      p2.cmdline AS parent_cmdline
    FROM processes p1, processes as p2
    ON p1.parent = p2.pid
    AND LOWER(child_process) = 'lsass.exe'
    AND
    (
      LOWER(parent_process) IN
('powershell.exe','taskmgr.exe','rundll32.exe','procdump.exe','procexp.exe')
      OR parent_process LIKE
REGEX_MATCH(parent_process,'nanodump(_ppl_dump|_ppl_medic|_ssp)?\.(x64|x86)\.exe',0)
    );
```

## Windows PowerShell Web Request

```
SELECT datetime,
           script_block_id,
           script_text,
           script_name,
           script_path
    FROM powershell_events
    WHERE
    (
      script_text LIKE '%Invoke-WebRequest%'
      OR script_text LIKE '%iwr%'
      OR script_text LIKE '%wget%'
      OR script_text LIKE '%curl%'
      OR script_text LIKE '%Net.WebClient%'
      OR script_text LIKE '%Start-BitsTransfer%'
    );
```

## Proxy execution of malicious payloads via wmic.exe

```
SELECT
      name,
      cmdline,
      path,
      pid,
      parent
    FROM processes
    WHERE LOWER(name) = 'wmic.exe'
    AND
    (
      cmdline LIKE '%call%'
      OR cmdline LIKE '%create%'
      OR cmdline LIKE '%process%'
    )
    AND
    (
      cmdline LIKE '%rundll32%'
      OR cmdline LIKE '%bitsadmin%'
      OR cmdline LIKE '%regsvr32%'
      OR cmdline LIKE '%cmd.exe /c%'
      OR cmdline LIKE '%cmd.exe /k%'
      OR cmdline LIKE '%cmd.exe /r%'
      OR cmdline LIKE '%cmd /c%'
      OR cmdline LIKE '%cmd /k%'
      OR cmdline LIKE '%cmd /r%'
      OR cmdline LIKE '%powershell%'
      OR cmdline LIKE '%pwsh%'
      OR cmdline LIKE '%certutil%'
      OR cmdline LIKE '%cscript%'
      OR cmdline LIKE '%wscript%'
      OR cmdline LIKE '%mshta%'
      OR cmdline LIKE '%Users\Public%'
      OR cmdline LIKE '%Windows\Temp%'
      OR cmdline LIKE '%AppData\Local%'
      OR cmdline LIKE '%\%temp\%%'
      OR cmdline LIKE '%\%tmp\%%'
      OR cmdline LIKE '%\%ProgramData\%%'
      OR cmdline LIKE '%\%appdata\%%'
      OR cmdline LIKE '%\%comspec\%%'
      OR cmdline LIKE '%*\%localappdata\%%'
    );
```

Below are several publicly accessible rules for detecting the above scenario.

## Threat Bites

| | | |
|---|---|---|
| **Threat Actor** | : | FIN11, TA505, DEV-0950, Evil Corp, PHOSPHORUS, Mint Sandstorm, MERCURY, Mango Sandstorm |
| **Malwares** | : | Cl0p, LockBit, TrueBot |

| | | |
|---|---|---|
| **Targeted Country** | : | United States, United Kingdom, Australia, France, Netherlands |
| **Targeted Industry** | : | Education |
| **First Seen** | : | 2023 |
| **Last Seen** | : | 2023 |
| **LOLBAS** | : | Wmic |
| **Telemetry** | : | Sysmon, Security, PowerShell |

## References

**Author**: Saharsh Agrawal
Security Researcher, Loginsoft