Recorded Future®
Sandbox

Malware Analysis Report

2026-02-03 14:32

Sample ID	260203-rrxkkset7b
Target	notepad-classico.exe
SHA256	d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2
Tags	discovery

score

3/10

Table of Contents

Part 1. Analysis Overview

score

3/10

SHA256
d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2

Threat Level: Likely benign

The file notepad-classico.exe was found to be: Likely benign.

Malicious Activity Summary

discovery

> **Unsigned PE**

> **System Location Discovery: System Language Discovery**

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043	
Resource Development TA0042	
Initial Access TA0001	
Execution TA0002	
Persistence TA0003	
Privilege Escalation TA0004	
Defense Evasion TA0005	
Credential Access TA0006	
Discovery **TA0007**	System Location Discovery T1614
	System Language … T1614.001
Lateral Movement TA0008	
Collection TA0009	
Command and Control TA0011	
Exfiltration TA0010	
Impact TA0040	

Part 3. Analysis: static1

3. 1. Detonation Overview

Target	Reported
notepad-classico.exe	2026-02-03 14:26

3. 2. Signatures

Unsigned PE

Description	Indicator	Process	Target
N/A	N/A	N/A	N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Target	SHA256	Filesize
notepad-classico.exe	d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2	282KB

Submitted	Reported	Platform	Max time kernel	Max time network
2026-02-03 14:26	2026-02-03 14:31	win10v2004-20260130-en	149s	145s

4. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"
```

4. 3. Signatures

> **System Location Discovery: System Language Discovery**
>
> discovery
>
> | Description | Indicator | Process | Target |
> |---|---|---|---|
> | Key opened | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language | C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe | N/A |

4. 4. Processes

C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe

```
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"
```

4. 5. Network

Country	Destination	Domain	Proto
N/A	192.168.50.100:9001		tcp
US	8.8.8.8:53	c.pki.goog	udp
GB	142.251.29.94:80	c.pki.goog	tcp

4. 6. Files

memory/4820-0-0x0000000001000000-0x000000000104ADB0-memory.dmp

memory/4820-2-0x0000000000EA0000-0x0000000000ED1000-memory.dmp

memory/4820-5-0x0000000001000000-0x000000000104ADB0-memory.dmp

Part 5. Analysis: behavioral2

5. 1. Detonation Overview

Target	SHA256	Filesize
notepad-classico.exe	d2e6c9f9273663f3218bcd7cbfb3b6f599fbce7a4ba986f9bbff77e3603988f2	282KB

Submitted	Reported	Platform	Max time kernel	Max time network
2026-02-03 14:26	2026-02-03 14:31	win11-20260130-en	149s	142s

5. 2. Command Line

```
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"
```

5. 3. Signatures

> **System Location Discovery: System Language Discovery**
>
> discovery
>
> | Description | Indicator | Process | Target |
> |---|---|---|---|
> | Key opened | \REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\NLS\Language | C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe | N/A |

5. 4. Processes

C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe

```
"C:\Users\Admin\AppData\Local\Temp\notepad-classico.exe"
```

5. 5. Network

Country	Destination	Domain	Proto
N/A	192.168.50.100:9001		tcp

5. 6. Files

memory/4896-0-0x0000000001000000-0x000000000104ADB0-memory.dmp

memory/4896-1-0x0000000002460000-0x0000000002491000-memory.dmp

memory/4896-5-0x0000000001000000-0x000000000104ADB0-memory.dmp