LOLBin to INC Ransomware | Huntress

Archived: 2026-04-05 17:04:55 UTC

This blog post was originally published on May 1, 2024.

Background

Huntress analysts have previously observed INC ransomware being deployed, and recently observed this specific ransomware variant being deployed in a customer environment. The ransomware variant was identified, in part, through the threat actor's efforts to verify that their deployment was effective, as illustrated through the following command line:

```
"C:\windows\system32\NOTEPAD.EXE"
```

```
C:\Users\user\Documents\+<REDACTED>\INC-README.txt
```

Digging deeper into the incident, Huntress analysts were able to identify a specific pattern of activity associated with the threat actor, particularly during what appears to be the intermediate stages of their attack, and prior to ransomware deployment. Upon identifying this pattern, Huntress analysts began hunting across the entire infrastructure to identify other endpoints where this same pattern of activity was observed, and in doing so, notifying customers in an effort to head off the ransomware deployment. Even though the initial means of access and the follow-on activities varied slightly between the identified endpoints, this one pattern remained consistent and served to quickly surface impacted endpoints.

Attack Pattern

Looking across multiple endpoints, Huntress analysts observed a common, overarching pattern; that is, at the point where their activities could be explicitly identified, the threat actor appeared to have significant prior knowledge of the infrastructure in which they were operating.

The initial endpoint that was investigated in detail revealed the activity illustrated in Figure 1, associated with the user account known to be compromised within the customer's infrastructure.

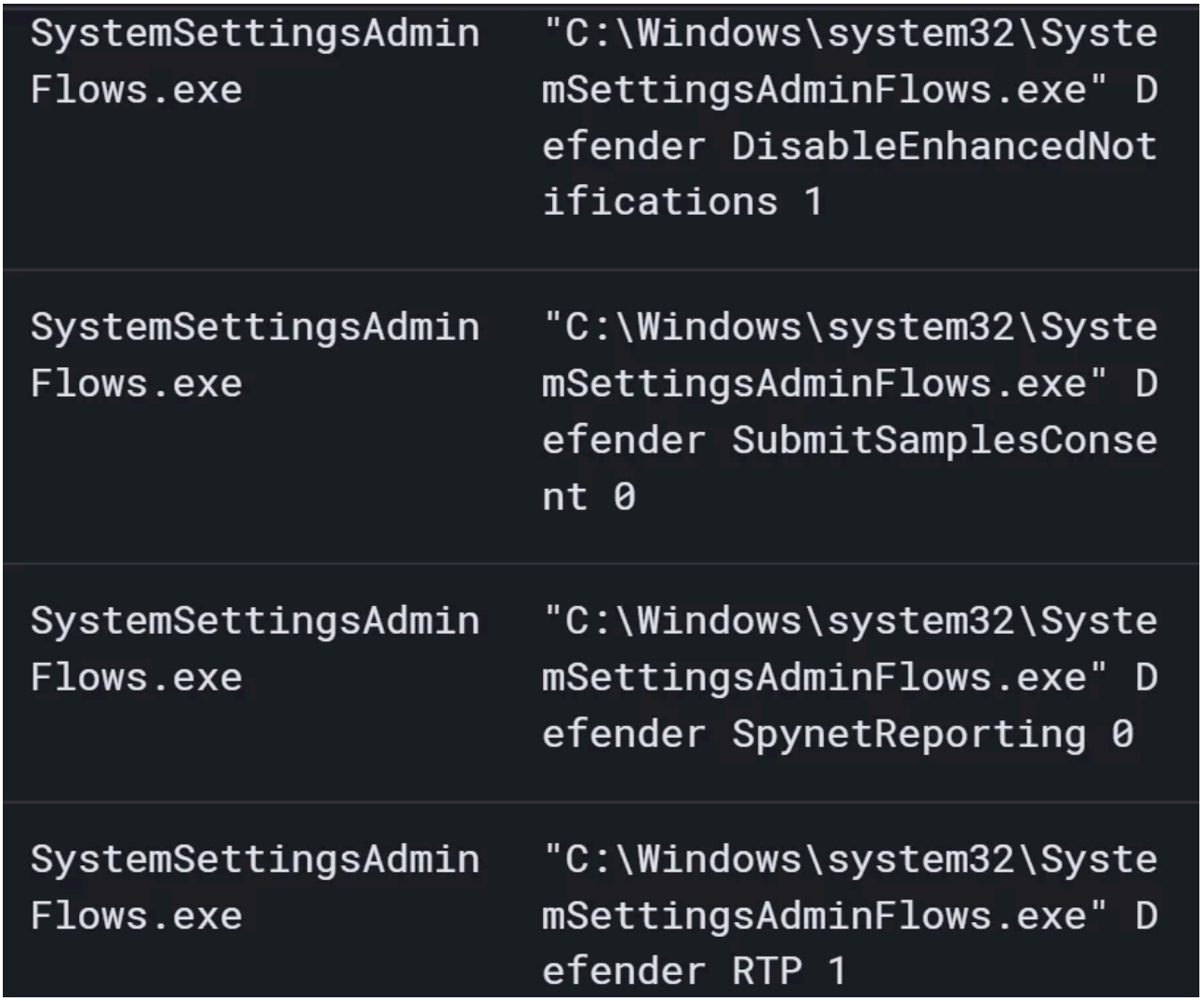

Figure 1: Pattern of LOLBin Activity

The commands illustrated in Figure 1 were pulled directly from the Huntress platform, and are listed with the most recent command at the top of the image. The threat actor used `SystemSettingsAdminFlows.exe`, a native Windows utility, to essentially disable Windows Defender. As illustrated in Figure 2, these modifications are manifest in the *Microsoft-Windows-Windows Defender/Operational* Event Log as event ID 5007 records, indicating that the change took place.

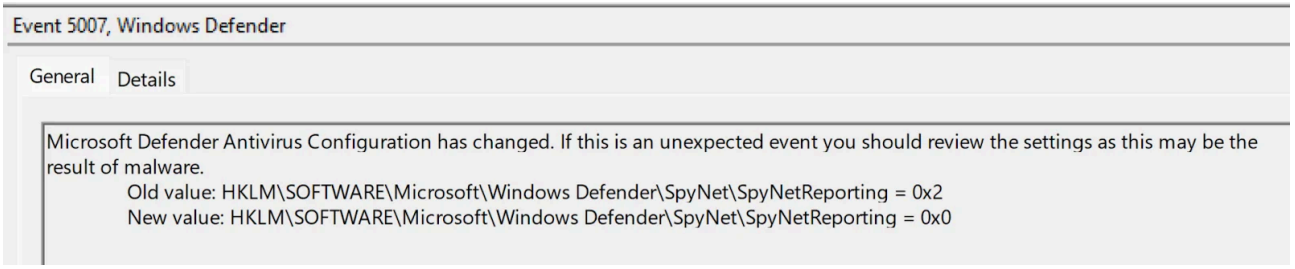

Figure 2: Windows Defender Event ID 5007 Record

It's important to note that the threat actor ran these commands on endpoints where Windows Defender was actively in use, indicating prior knowledge of the environment. In several instances, the threat actor brought along

the necessary tools to attempt to disable other installed security applications. However, in each instance, those applications were clearly installed and running on the endpoint. For example, on one endpoint where CylancePROTECT was installed, the following command line was observed:

```
C:\Windows\temp\av.exe -p CylanceSvc.exe
```

Twenty-three seconds later, a Service Control Manager record was created in the *System* Event Log with event ID 7031, indicating that the CylancePROTECT service had been abnormally terminated. Windows Defender did detect the file `av.exe` as `Trojan:Script/Wacatac.H!ml`, and quarantined the file, but not before it was able to terminate the CylancePROTECT service. The file was deleted from quarantine before Huntress had a chance to retrieve a copy of the file. However, this activity has only been noted on endpoints where CylancePROTECT is running. Huntress has previously observed the use of a file by the same name to disable Sophos Anti-Virus applications.

Also seen within the same timeframe was the usage of an executable named `kaz.exe` that executed from the same folder. Unfortunately, we were unable to recover this executable and it is not apparent what its functionality in this attack was at this time. One interesting thing about this executable, however, was that the original file name was `Treasury Secretary Steven Mnuchin`, as taken from the PE header at run time. This field is illustrated in Figure 3. This executable was run within 4 minutes of `av.exe`, and after Windows Defender had been disabled.

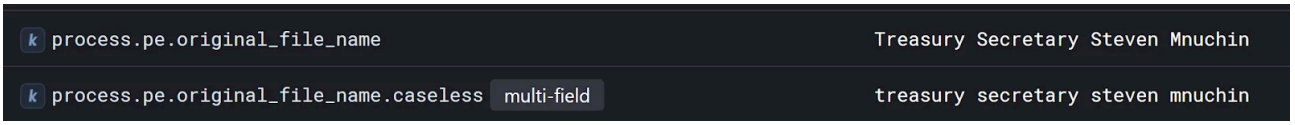

*Figure 3: **kaz.exe** Original File Name field*

The common activity illustrated in Figure 1 is consistent across all impacted endpoints so far, and has allowed Huntress to notify customers for whom ransomware has yet to be deployed. Hunting for activity on specific endpoints associated with the accounts found to be used by the threat actor, it's clear that as the threat actor is approaching the point of heightened activity and likely getting ready to deploy file encryption software, their actions become more directed and efficient, as illustrated in Figures 4 and 5. Figure 3 illustrates the threat actor's window of activity on an endpoint on April 27, 2024.

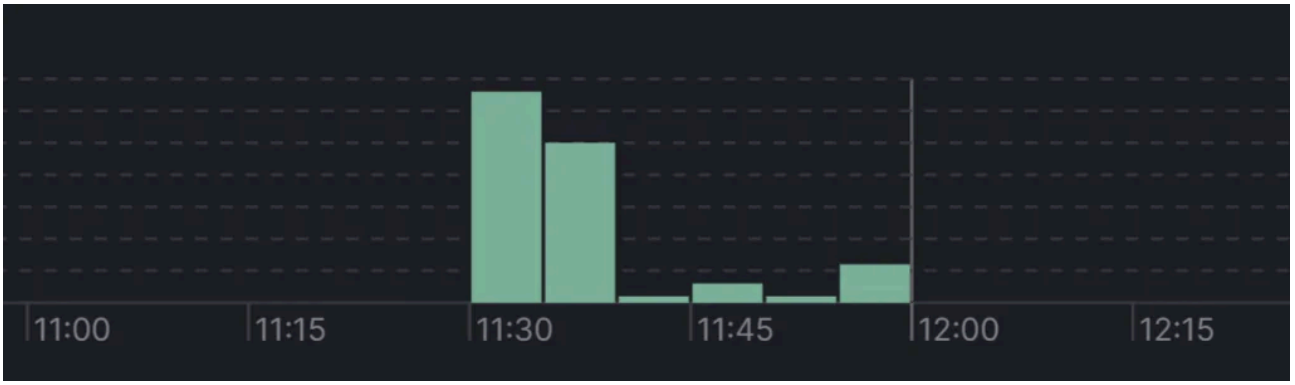

Figure 4: Threat actor activity, April 27, 2024 (UTC)

Figure 5 illustrates the timeframe of the threat actor's activities identified on a different, completely disparate endpoint on April 30, 2024.

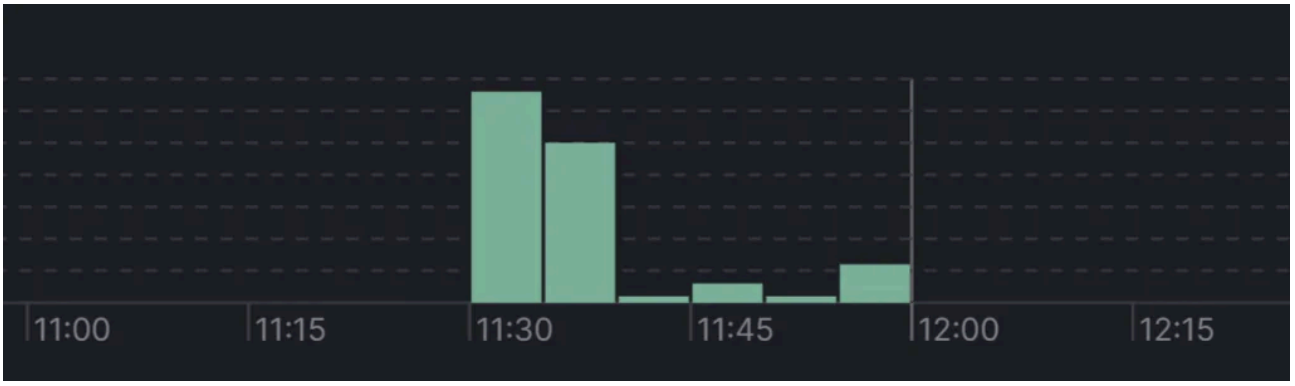

Figure 5: Threat actor activity, April 30, 2024 (UTC)

In both Figures 4 and 5, each showing threat actor activity on different endpoints and different days, it's abundantly clear that the threat actor has a prior understanding of the target infrastructure, and arrives with an efficient playbook.

Looking across the breadth of data available thus far, there are a number of other activities that appear to be isolated to particular endpoints. For example, one endpoint had already generated an alert for a rogue ScreenConnect installation, and a detailed investigation indicated that the infrastructure employed an entirely different RMM tool. After accessing the endpoint via the newly installed ScreenConnect instance, the threat actor changed the password on an existing account via `net.exe`. On another endpoint, the threat actor used a valid, previously compromised account to access the endpoint via the Remote Desktop Protocol (RDP). In other instances, the threat actor was observed viewing various files using `notepad.exe` and `wordpad.exe`.

On another endpoint, the following command line was observed:

```
rclone copy E:\ <mount_point> --include-from include.txt
```

Huntress wasn't able to retrieve a copy of the `include.txt` file; however, the use of such a file indicates that the threat actor was clearly aware of the files they wanted to collect or exclude, further indicating likely prior knowledge of the environment.

Huntress also observed the use of `MEGAsync.exe` within one infrastructure. On the compromised endpoint, the threat actor installed 7Zip and MEGASync, then ran a total of 28 `7zG.exe` processes to archive data. Not long after the last `7zG.exe` process was run, both MEGASync and 7Zip were uninstalled from the endpoint. Huntress has previously observed the use of `MEGAsync.exe` during incidents where INC ransomware was later deployed.

Conclusion

The timing of the activity that came to the attention of Huntress analysts indicates that the threat actor had likely been active in or simply had detailed prior knowledge of the infrastructure before getting to the point where they were ready to deploy the INC ransomware. However, by leveraging the available details extracted from intensive investigations into the threat actor activity, Huntress was able to identify other customers who were likely being

subject to the same attack, from the same threat actor. Immediate notification of this activity, with the relevant details, allows customers to respond in an appropriate and timely manner, implementing their incident response plan, and obviating file encryption activity.

Thanks to Faith Stratton, Dray Agha, Jai Minton, Greg Linares, and Jamie Levy for their assistance in developing this content and blog post.

Indicators

`Av.exe` SHA-256 hash:

36eb4290aa11a950e60d12ab18a8e139d25464355ce761f98891e1ea94f39445

`kaz.exe` SHA-256 hash:

fc39cca5d71b1a9ed3c71cca6f1b86cfe03466624ad78cdb57580dba90847851

`ababcab28dcdb35c` - rogue ScreenConnect instance ID

MITRE ATT&CK Mapping

Initial Access - T1133, External Remote Services & T1078.002, Domain Accounts

Execution - T1059.003, Windows Command Shell (also observed use of GUI tools, browsers, etc.)

Persistence - T1078.003: Local Accounts, T1078.002: Domain Accounts, T1543.003: Windows Service

Privilege Escalation - Not Observed

Defense Evasion - T1562.001: Disable or Modify Tools

Credential Access - Not Observed

Discovery - Not Observed

Lateral Movement - Not Observed

Collection - T1560.001: Archive via Utility (rclone)

Command And Control - T1219: Remote Access Software, T1105: Ingress Tool Transfer

Exfiltration - T1537: Transfer Data to Cloud Account (use of MEGAsync.exe)

Impact - T1486: Data Encrypted For Impact

Detection Opportunities

We’ve provided a Sigma rule to detect the direct usage of SystemSettingsAdminFlows.exe to tamper with Windows Defender. While the binary is often used legitimately, this rule filters out instances with common parents

like SystemSettings.exe.

	title: Using SystemSettingsAdminFlows.exe To Tamper With Windows Defender
	id: ad44351e-89c4-4b1c-8cb0-676c55bf11ce
	status: experimental
	description: Detects the usage of SystemSettingsAdminFlows.exe to disable or tamper with Windows Defender
	references:
	- https://attack.mitre.org/techniques/T1562/001/
	author: Alden Schmidt, Matt Anderson
	date: 2024/04/30
	modified: 2024/04/30
	tags:
	- attack.defense_evasion
	- attack.t1562
	logsource:
	category: process_creation
	product: windows
	detection:
	selection_adminflows:
	- Image|endswith: '\SystemSettingsAdminFlows.exe'
	- OriginalFilename: 'SystemSettingsAdminFlows.exe'
	selection_cli:
	CommandLine|contains:
	- 'Defender DisableEnhancedNotifications 1'
	- 'Defender SubmitSamplesConsent 0'
	- 'Defender SpynetReporting 0'
	- 'Defender RTP 1'

	filter:
	- ParentImage|endswith: '\SystemSettings.exe'
	condition: all of selection_* and not filter
	falsepositives:
	- Legitimate use of SystemSettingsAdminFlows.exe as a child of SystemSettings.exe
	level: high

We recommend monitoring the following:

- Use of various RMM and Remote Control/Desktop tools, such as ScreenConnect, and limiting the use of unapproved applications.
- Use of any file sync or backup utilities, such as MEGAsync, that are not approved for use in your environment.
