


Detecting Advanced Process Tampering Tactics with Sysmon v13

 blog.netwrix.com/2023/07/06/sysmon-13-process-tampering-detection

Joe Dibley

Sysmon is a component of Microsoft's Sysinternals Suite, a comprehensive set of tools for monitoring, managing and troubleshooting Windows operating systems. Version 13 of Sysmon introduced monitoring for two advanced malware tactics: process hollowing and herpaderping. This article explains what these tactics are, why they are so dangerous and how you can now detect them using Sysmon.

What Are Process Hollowing and Herpaderping?

Sysmon version 13 introduced monitoring for two advanced malware tactics:

- **Process hollowing**—Used to replace code in a Windows process with malicious code, so the malicious code runs under the guise of a legitimate Windows process. This tactic has been around for years.
- **Process herpaderping**—Used to modify the contents of a process on disk after the image has been mapped, so that the on-disk file appears to be the trusted process while malicious code runs in memory. This is a relatively new technique.

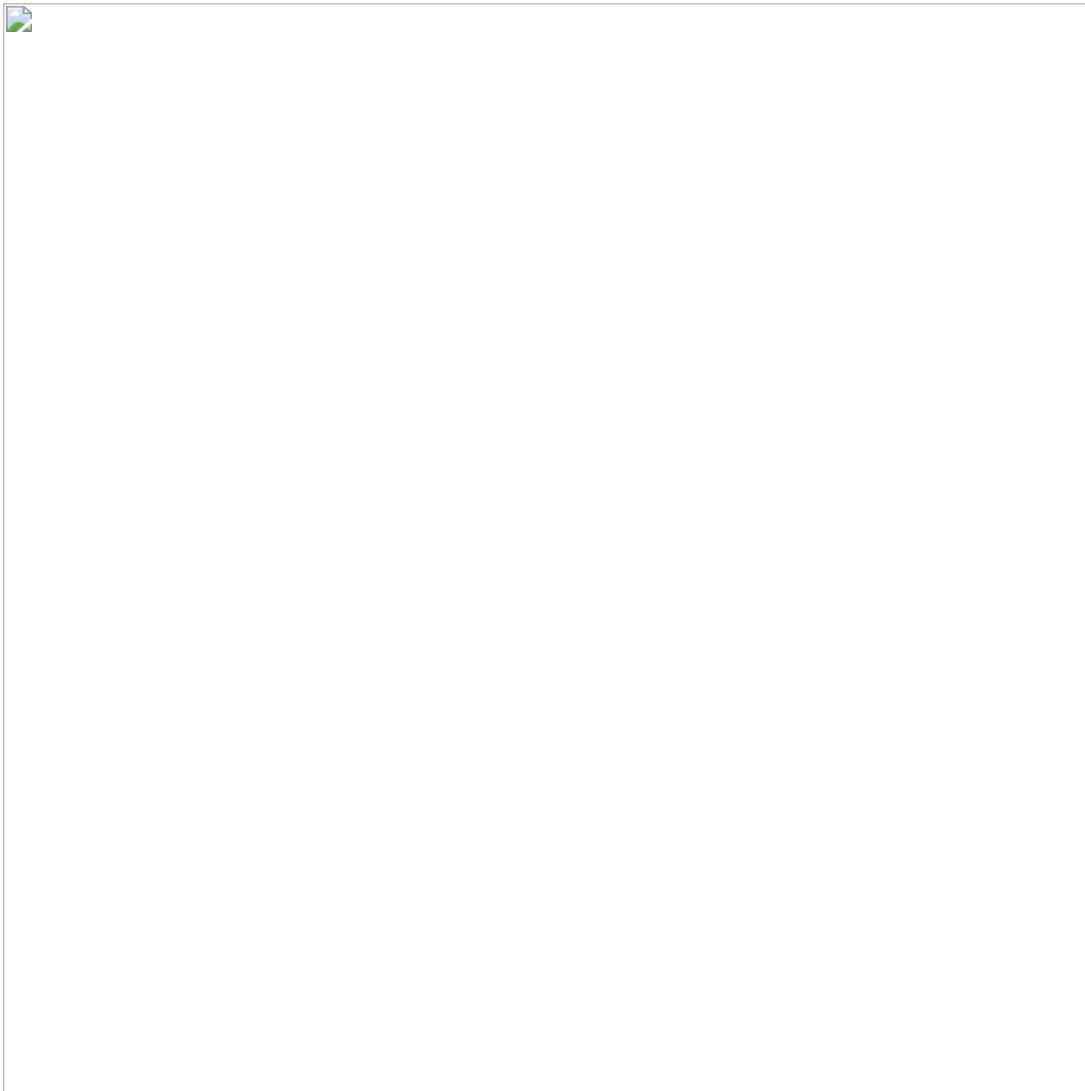
Both of these tactics can cause serious damage. For example, suppose process herpaderping was employed to execute Mimikatz under a web browser's legitimate process (e.g., Google Chrome). It appears to the OS that Google Chrome (rather than Mimikatz) is running — and the process would even have a valid Google signature! Thus, an attacker running Mimikatz could remain completely undetected unless you have security software that's specifically monitoring for process herpaderping.

What's more, the payload does not have to be Mimikatz — bad actors could use this tactic to execute anything they like in your network: TrickBot, Emotet, Ryuk, Mirai, etc. Accordingly, Sysmon now being able to detect these tactics is invaluable.

How Does Sysmon 13 Record Process Hollowing and Process Herpaderping?

Sysmon 13 can detect both process hollowing and process herpaderping attacks. They are logged to the Windows Event Viewer as Event ID 25, Process Tampering:





Images courtesy of [Mark Russinovich's public Twitter account](#) (author of [Sysmon](#) via [Sysinternals](#))

Configuring Sysmon 13 to Detect Process Hollowing and Process Herpaderping

Take the following steps to install Sysmon and configure monitoring for process hollowing and process herpaderping:

1. [Download Sysmon](#), unzip the file, and run Sysmon.exe in an elevated command prompt:

```
>> Sysmon.exe -i -accepteula
```

```
System Monitor v13.01 - System activity monitor
```

```
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
```

```
Sysinternals - www.sysinternals.com
```

```
Sysmon installed.
```

```
SysmonDrv installed.
```

```
Starting SysmonDrv.
```

```
SysmonDrv started.
```

```
Starting Sysmon..
```

```
Sysmon started.
```

The default installation doesn't include monitoring and logging for process tampering (Event ID 25), so we need to update our Sysmon configuration. Here's a very basic Sysmon configuration XML that includes an event filter for process tampering; save it as **Sysmon.XML**.

```
<Sysmon schemaversion="4.50">
```

```
  <EventFiltering>
```

```
    <ProcessTampering onmatch="exclude">
```

```
  </ProcessTampering>
```

```
</EventFiltering>
```

```
</Sysmon>
```

Navigate to the directory containing the file in an elevated command prompt and load the configuration with the following command:

```
>> sysmon.exe -c Sysmon.xml
```

```
System Monitor v13.01 - System activity monitor
```

```
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
```

```
Sysinternals - www.sysinternals.com
```

```
Loading configuration file with schema version 4.50
```

```
Configuration file validated.
```

```
Configuration updated.
```

Example of Sysmon 13 Detecting Process Herpaderping

Now let's test our configuration.

Executing a Process Herpaderping Attack

First, we'll use the process herpaderping technique found [here](#) to execute Mimikatz under the guise of Google Chrome's process (chrome.exe).

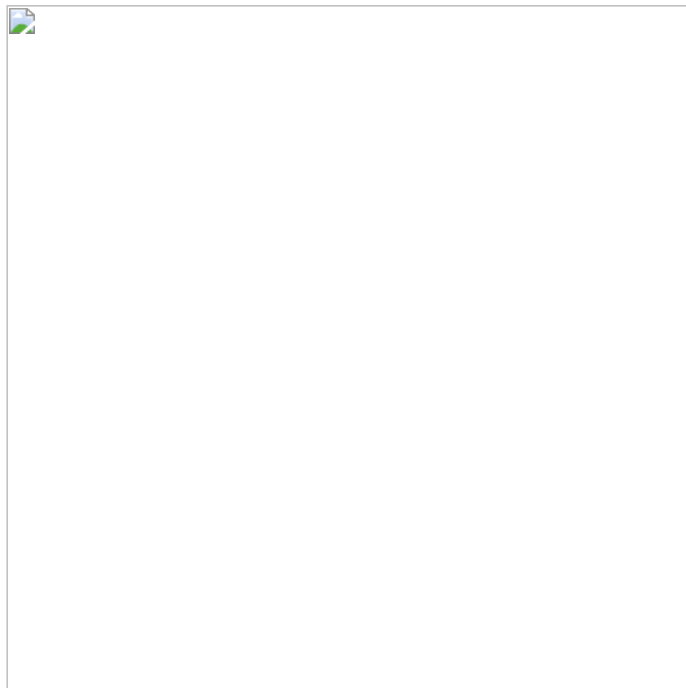
Important: Keep in mind that attempting process herpaderping can render target processes inoperable. Please proceed with caution, and always test security and malware techniques in secure sandbox environments.

First, we'll download ProcessHerpaderping.exe from the link above. Then using an elevated command prompt from the directory containing that file, we'll run the following command:

```
>> ProcessHerpaderping.exe mimikatz.exe "\\Program Files\\Google\\Chrome\\Application\\chrome.exe"
```

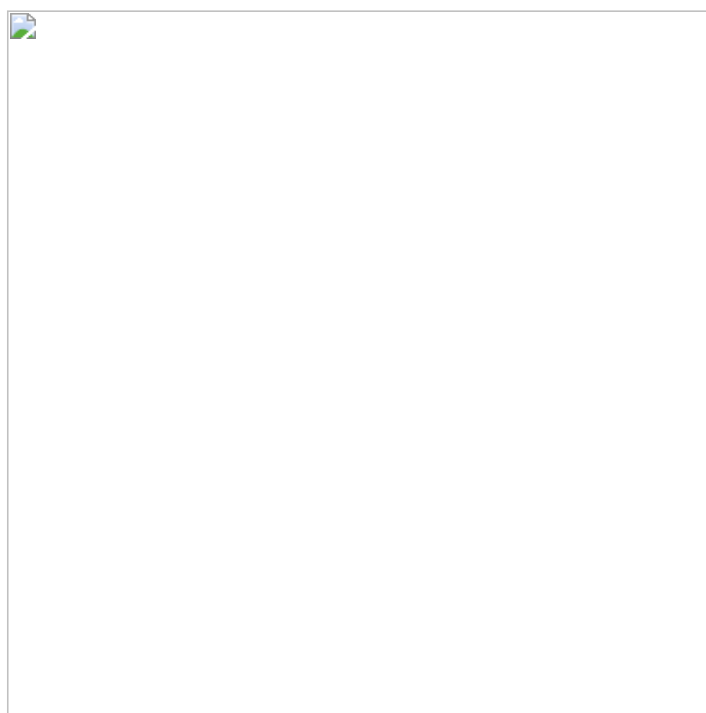


We've successfully executed mimikatz.exe from within chrome.exe (a widely trusted process) and checking the chrome.exe process shows a valid Google signature:



Sysmon 13 Detecting the Process Herpaderping Attack

However, thanks to our Sysmon 13 configuration, we immediately detected this malicious activity:



This is extremely valuable information that can be sent to admins and your security information and event management (SIEM) tool via Windows Event Forwarding (WEF).

Uninstalling Sysmon

If you installed Sysmon only for testing purposes, you can uninstall it using the following command:

```
>> Sysmon.exe -u

System Monitor v13.01 - System activity monitor

Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier

Sysinternals - www.sysinternals.com

Stopping Sysmon.

Sysmon stopped.

Sysmon removed.

Stopping SysmonDrv.

SysmonDrv stopped.

SysmonDrv removed.

Removing service files.
```

How Netwrix Can Help

Netwrix StealthINTERCEPT is a powerful cybersecurity solution that can help you protect your organization from advanced malware tactics. It can effectively identify authentication-based and file system attacks, abuse of privileged accounts, critical changes made to the IT environment, activity indicative of intruder reconnaissance, and much more. Its sophisticated capabilities enable it to detect specific threats, such as attempts to inject malicious code into the LSASS process Windows SSP injection attacks, and DCSync attacks. By proactively identifying and preventing these threats, this software provides a comprehensive defense against even the most advanced cyberattacks, ensuring that your organization's sensitive data and systems remain secure.

Joe Dibley

Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.

