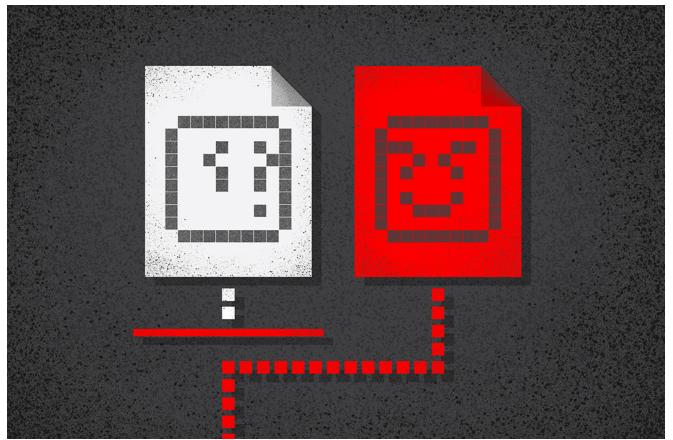
Herpaderping: Security Risk or Unintended Behavior?

trowdstrike.com/blog/herpaderping-security-risk-or-unintended-behavior/

Johnny Shaw

January 21, 2021



The answer to that question often depends on who you ask.

By definition, **process herpaderping** is a hacking technique in which digital adversaries modify on-disk content after the image has been mapped in order to obscure the process. This obscurity can confuse security products or the operating system itself, sometimes allowing malicious code to be executed. For more information on process herpaderping, please read my earlier explainer post <u>here</u>.

At a Glance: How Process Herpaderping Occurs

- 1. Write target binary to disk, keeping the handle open. This is what will execute in memory.
- 2. Map the file as an image section (<u>NtCreateSection</u>, <u>SEC_IMAGE</u>).
- 3. Create the process object using the section handle (NtCreateProcessEx).
- 4. Using the same target file handle, obscure the file on disk.
- 5. Create the initial thread in the process (NtCreateThreadEx). At this point the process creation callback in the kernel will fire. The contents on disk do not match what was mapped. Inspection of the file at this point will result in incorrect attribution.

6. Close the handle. <u>IRP_MJ_CLEANUP</u> will occur here. Since we've hidden the contents of what is executing, inspection at this point will result in incorrect attribution.

From an OS's perspective, herpaderp attacks are often categorized as unintentional activity. But from a developer's point of view, it's a clear security threat—and a potent one at that.

To illustrate this principle, let's take a look at a recent example. Over the summer, it may have appeared that Google distributed a signed copy of Mimikatz. Sounds strange? It should because Google did not distribute a signed copy of Mimikatz. Rather, if you saw this, you were witnessing a case of process herpaderping, an exploit technique that obscures the intentions of a process by modifying the content on disk after the image has been mapped.



My team disclosed this process herpaderping attack to the Microsoft Security Response Center (MSRC) in mid-July. A case was opened a few days later. MSRC concluded their investigation near the end of August and determined the findings of the MSRC investigation were valid but did not require immediate servicing.

And with that, the case was closed—without a real resolution or timeline for future review, despite our reiterated belief to MSRC that this bug is severe.

Review the details here.

What Does Herpaderping Mean for Developers?

The consensus from the cybersecurity community and researchers sees the situation quite differently. The POC shows this is exploitable and as a "defense evasion" or "masquerading" technique.

When an attack of this nature is miscategorized by an OS as unintentional activity it has major cybersecurity implications for any and all developers, not just security vendors. For example, where a Microsoft OS categorizes this attack as unintentional, Microsoft Defender Antivirus scans completed on the image backing the process may not prevent execution by a known malicious binary. Once the file is copied to the desktop, Microsoft Defender will likely realize there is a problem, but by then, the damage is done.

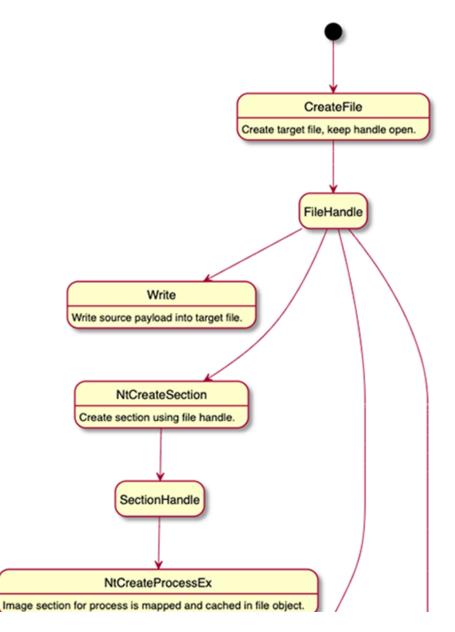
Many antivirus vendors are thought to be vulnerable to this type of attack, which means that many organizations are at risk of experiencing a herpaderping attack.

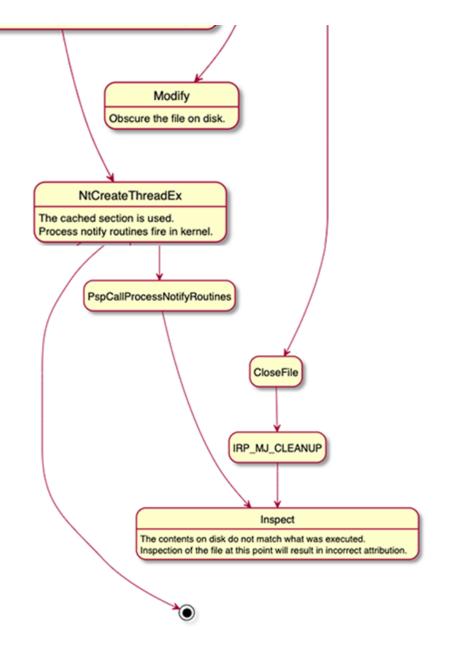
Herpaderping: How It's Done

When the OS characterizes herpaderping as unintentional activity, it fails to address such exploits, and thus the burden of the solution falls on developers, both cybersecurity vendors and general app developers. But in order to defend against such attacks, we must first understand how they work.

Generally, a security product takes action on process creation by registering a callback in the OS kernel (<u>PsSetCreateProcessNotifyRoutineEx</u>). At this point, a security product may inspect the file that was used to map the executable and determine if this process should be allowed to execute. However, the kernel callback is invoked when the initial thread is inserted, not when the process object is created.

Because of this disconnect, an actor can create and map a process, modify the content of the file, then create the initial thread. A product that does inspection at the creation callback would then see the modified content.





Click image to enlarge

In addition, some products use an on-write scanning approach that consists of monitoring for file writes. A familiar optimization is recording the file as written and deferring the actual inspection until <u>IRP_MJ_CLEANUP</u> occurs (e.g. the file handle is closed). Thus, an actor using a write -> map -> modify -> execute -> close workflow will subvert on-write scanning that solely relies on inspection at <u>IRP_MJ_CLEANUP</u>.

To abuse this convention, adversaries first write a binary to a target file on disk. Then, they map an image of the target file and provide it to the OS to use for process creation. The OS then maps the original binary. Using the existing file handle, and before creating the initial thread, the adversary then modifies the target file content to obscure or fake the file backing the image. Later, the initial thread is created in order to begin execution of the original binary. Finally, the target file handle can be closed.

Let's look at an example of herpaderping in action.

As you can see in the demo linked above, Cmd.exe is used as the execution target. The first run overwrites the bytes on disk with a pattern. The second run overwrites .exe with ProcessHacker.exe.

The herpaderping tool then fixes the binary to look as close to ProcessHacker.exe as possible, even retaining the original signature. Note the multiple executions of the same binary and how the process looks to the user compared to what is in the file on disk.

Looking at this flow from Process Monitor, we observe the source file being written and the OS mapping the image at the section creation. Using the same handle, the exploit overwrites the source binary with whatever it likes before creating the initial thread. By the time the process creation notification fires in the kernel the file backing the image is not what was mapped:

368	KB
200	ND

IP ProcessHepadepring exe 5948 B, F IP Proces	IRP_M_CREATE FASTD_OUERY_INFORMATION FASTDO QUERY_INFORMATION FASTDO QUERY_INFORMATION IRP_M_WIRE FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_WRITE FASTDO_READ FASTDO_WRITE FASTDO_READ FASTDO_WRITE FASTDO_READ FASTDO_WRITE FASTDO_READ	C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe	SUCCESS SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO N Desired Access: Generic Read/Write, Disposition: Overwritef, Options: Synchr Type: CueryStandardIrformationFile, Allocations: ze: 28, 264, EndOfFile: 200, Type: CueryStandardIrformationFile, AllocationSize: 20, E34, EndOfFile: 200, Offset: 0, Length: 32, 768, Priority: Normal Offset: 0, Length: 32, 768, Priority: Normal Offset: 32, 768, Length: 32, 768 Offset: 32, 768, Length: 32, 768 Offset: 59, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 193, 400, Length: 32, 768 Offset: 113, 400, Length: 32, 768
ProcessHemaderping exe 544 B/R Pro	IRP_M_CREATE FASTD_OUERY_INFORMATION FASTDO QUERY_INFORMATION FASTDO QUERY_INFORMATION IRP_M_WIRE FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_READ FASTDO_WRITE FASTDO_READ FASTDO_WRITE FASTDO_READ FASTDO_WRITE FASTDO_READ FASTDO_WRITE FASTDO_READ	C:\Usen'yay\Desktop Vol exe C:\Wrndows\System32\cmd.exe C:\Wrndows\System32\cmd.exe C:\Usen'yay\Desktop Vol exe C:\Usen'yay\Desktop Vol exe	SUCCESS SUCESS	Desired Access: Generic Read/Write, Disposition: Overwritef, Options: Synchr Type: QueryStandardInformationFile, AllocationSize: 282.624, EndOfFile: 280.0 Type: QueryStandardInformationFile, AllocationSize: 0. EndOfFile: 280.0 Offset: 0. Length: 32,768, Priority: Normal Offset: 0. Length: 32,768, Priority: Normal Offset: 32,768, Length: 32,768 Offset: 536, Length: 32,768 Offset: 536, Length: 32,768 Offset: 536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 136,840, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 5948 8,7 ProcessHepadeping.exe 5448 8,7 ProcessHepadeping.exe 5448 8,7 ProcessHepadeping.exe 5448 8,7 Pro	FASTID GUERY INFORMATION FASTID GUERY INFORMATION IRP_MJ_READ IRP_MJ_READ FASTID READ FASTID QWRITE FASTID QWRITE FASTI	C:\Undows\System32\cmd exe C:\Users\yvy\Desktop\0el.exe	SUCCESS SUCCESS	Type: Ouery/StandardInformationFile, AllocationSize: 228, 624, End/OFFile: 280.0 Type: Ouery/StandardInformationFile, AllocationSize: 282, 624, End/OFFile: 280.0 Offset: 0, Length: 32,768, Priority: Normal Offset: 0, Length: 32,768, Priority: Normal Offset: 32,768, Length: 32,768 Offset: 32,768, Length: 32,768 Offset: 53,2768, Length: 32,768 Offset: 58,306, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 132,768, Length: 32,768 Offset: 134,040, Length: 32,768 Offset: 156,360, Length: 32,768 Offset: 156,360, Length: 32,768 Offset: 156,080, Length: 32,768
ProcessHemaderping.ex 5845 8/1 ProcessHemaderping.ex 5846 8/1 ProcessHemaderping.ex 5846 8/1 ProcessHemaderping.ex 5848 8/1 Pro	FASTID CUERY INFORMATION IRP MJ. PEAD IRP MJ. PEAD FASTID, VIRITE FASTID, VIRITE IRP, MJ. WIRTE IRP, MJ. WIRTE FASTID, VIRITE FASTID,	C:\Users \u00fcork) Desktop Vole exe C:\Windows \System32\cmd exe C:\Windows \System32\cmd exe C:\Users \u00fcork) Desktop Vole exe	SUCCESS SUCESS SUCESS SUCESS SU	Type: CoursyStandardInformationFile: AllocationSize: 0. EndOfFile: 0. NumberOl Offset: 0. Length: 32,768. Priority: Normal Source file to Offset: 32,768. Length: 32,768 Source file Course file Offset: 32,768. Length: 32,768 Offset: 32,768. Priority: Normal Offset: 32,768. Priority: Normal Offset: 53,56. Length: 32,768 Offset: 32,768. Length: 32,768 Offset: 53,561. Length: 32,768 Offset: 98,304. Length: 32,768 Offset: 98,304. Length: 32,768 Offset: 98,304. Length: 32,768 Offset: 131,072. Length: 32,768 Offset: 153,840. Length: 32,768 Offset: 153,840. Length: 32,768 Offset: 153,840. Length: 32,768 Offset: 153,840. Length: 32,768 Offset: 153,840. Length: 32,768
ProcessHepadeping.exe 544 SIR ProcessHepadeping.exe </td <td>IRP_MJ_NEAD IRP_MJ_VRITE FASTID_VRITE IRP_MJ_VRITE FASTID_VRITE IRP_MJ_VRITE IRP_MJ_FLUSS_BUFFERS FASTD_CACUURE_FOR_CC_FLUSH</td> <td>C:\Usen'yay\Desktop Vol.exe C:\Usen'yay\Desktop Vol.exe</td> <td>SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS</td> <td>Offset: 0, Length: 32,768, Priority: Normal Source file to Offset: 0, Length: 32,768, Priority: Normal Source file to Offset: 32,768, Length: 32,768 Source file to Offset: 52,768, Length: 32,768 Source file to Offset: 55,556, Length: 32,768 Source file to Offset: 59,304, Length: 32,768 Source file to Offset: 98,304, Length: 32,768 Source file to Offset: 131,072, Length: 32,768 Source file to Offset: 131,072, Length: 32,768 Source file to Offset: 163,840, Length: 32,768 Source file to Offset: 163,840, Length: 32,768 Source file to Offset: 196,608, Length: 32,768 Source file to Offset: 196,608, Length: 32,768 Source file to Offset: 196,608, Length: 32,768 Source file to</td>	IRP_MJ_NEAD IRP_MJ_VRITE FASTID_VRITE IRP_MJ_VRITE FASTID_VRITE IRP_MJ_VRITE IRP_MJ_FLUSS_BUFFERS FASTD_CACUURE_FOR_CC_FLUSH	C:\Usen'yay\Desktop Vol.exe C:\Usen'yay\Desktop Vol.exe	SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 0, Length: 32,768, Priority: Normal Source file to Offset: 0, Length: 32,768, Priority: Normal Source file to Offset: 32,768, Length: 32,768 Source file to Offset: 52,768, Length: 32,768 Source file to Offset: 55,556, Length: 32,768 Source file to Offset: 59,304, Length: 32,768 Source file to Offset: 98,304, Length: 32,768 Source file to Offset: 131,072, Length: 32,768 Source file to Offset: 131,072, Length: 32,768 Source file to Offset: 163,840, Length: 32,768 Source file to Offset: 163,840, Length: 32,768 Source file to Offset: 196,608, Length: 32,768 Source file to Offset: 196,608, Length: 32,768 Source file to Offset: 196,608, Length: 32,768 Source file to
ProcessHemaderping.exe 5848 IAF	IRP_M_VINITE FASTIO_READ FASTIO_VINITE IRP_ML_VINITE IRP_ML_VINITE FASTIO_VI	C:Windows System 32:cmd exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe C:Windows System 32:cmd exe C:Windows System 32:cmd exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe C:Windows System 32:cmd exe C:Windows System 32:cmd exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe	SUCCESS FAST IO DISALLOWED SUCCESS	Offset: 32,768, Length: 32,768 Offset: 32,768, Length: 32,768 Offset: 32,768, Length: 32,768 Offset: 32,768, Length: 32,768 Offset: 55,536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 151,072, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 196,508, Length: 32,768 Offset: 196,508, Length: 32,768
ProcessHeipadeping exe 544 F/F Pro	FASTID_VIRITE FASTID_VIRITE IRP_MJ_WRITE FASTID_VIRITE FASTID_VIRITE FASTID_READ FASTID_READ FASTID_READ FASTID_READ FASTID_VIRITE	C:Windows System 32:cmd exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe C:Windows System 32:cmd exe C:Windows System 32:cmd exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe C:Windows System 32:cmd exe C:Windows System 32:cmd exe C:Usen 3yo/Desktop Vol.exe C:Usen 3yo/Desktop Vol.exe	FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 32,768, Length: 32,768 Offset: 32,768, Length: 32,768 Offset: 55,356, Length: 32,768 Offset: 55,356, Length: 32,768 Offset: 55,356, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 13,1072, Length: 32,768 Offset: 13,1072, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 196,508, Length: 32,768 Offset: 196,508, Length: 32,768
ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe </td <td>FASTID_VRITE IFASTID_READ FASTID_READ FASTID_VRITE FAS</td> <td>C:\Usen' joy/Desktop Vol.exe C:\Usen' joy/Desktop Vol.exe</td> <td>FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS</td> <td>Offset: 32,768, Length: 32,768 Offset: 53,2768, Length: 32,768, Priority: Normal Offset: 55,356, Length: 32,768 Offset: 56,536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 38,304, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 133,400, Length: 32,768 Offset: 153,840, Length: 32,768 Offset: 196,608, Length: 32,768</td>	FASTID_VRITE IFASTID_READ FASTID_READ FASTID_VRITE FAS	C:\Usen' joy/Desktop Vol.exe C:\Usen' joy/Desktop Vol.exe	FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 32,768, Length: 32,768 Offset: 53,2768, Length: 32,768, Priority: Normal Offset: 55,356, Length: 32,768 Offset: 56,536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 38,304, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 133,400, Length: 32,768 Offset: 153,840, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 5948 SIA Pro	FASTIO_IEAD FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_DEAD FASTIO_UWRITE FASTIO_DEAD FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_VWRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_COURE_FOR_CC_FLUSH	C:\Usen'yay.Desktop Vol exe C:\Windows\System32\cmd exe C:\Windows\System32\cmd exe C:\Usen'yay.Desktop Vol exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 32,768, Length: 32,768, Priority: Nomal Offset: 65,536, Length: 32,768 Offset: 65,536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768, Priority: Nomal Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 136,800, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHeinadering exe 544 F/F Pro	FASTIO_IEAD FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_DEAD FASTIO_UWRITE FASTIO_DEAD FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_VWRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_COURE_FOR_CC_FLUSH	C: Windows System 32 cmd exe C: Users yay. Desktop Vol exe C: Windows System 32 cmd exe C: Windows System 32 cmd exe C: Windows System 32 cmd exe C: Users yay. Desktop Vol exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 55,536, Length: 32,768 Offset: 65,536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 153,840, Length: 32,768 Offset: 153,840, Length: 32,768 Offset: 163,840, Length: 32,768
ProcessHempadeping.exe 544 F/F Pro	FASTIO_VINITE FASTIO_VINITE FASTIO_VINITE IRP_ML_VINITE FASTIO	C:\Users'yay\Desktop Vol exe C:\Windows\System32\cmd.exe C:\Users'yay\Desktop Vol exe C:\Users'yay\Desktop Vol exe C:\Users'yay\Desktop Vol exe C:\Windows\System32\cmd.exe C:\Windows\System32\cmd.exe C:\Users'yay\Desktop Vol exe C:\Users'yay\Desktop Vol exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 55,536, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 98,304, Length: 32,768 Offset: 13,1072, Length: 32,768 Offset: 13,1072, Length: 32,768 Offset: 153,840, Length: 32,768 Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe </td <td>FASTIO_READ FASTIO_WRITE FASTIO_WRITE FASTIO_READ FASTIO_READ FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_READ FASTIO_</td> <td>C:\Windows\System32\cmd exe C:\Usens iyo/Deaktop Vol.exe C:\Usens iyo/Deaktop Vol.exe</td> <td>SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS</td> <td>Offset: 88, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 163, 340, Length: 32, 768 Offset: 163, 840, Length: 32, 768 Offset: 163, 840, Length: 32, 768 Offset: 163, 608, Length: 32, 768</td>	FASTIO_READ FASTIO_WRITE FASTIO_WRITE FASTIO_READ FASTIO_READ FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_READ FASTIO_	C:\Windows\System32\cmd exe C:\Usens iyo/Deaktop Vol.exe C:\Usens iyo/Deaktop Vol.exe	SUCCESS FAST IO DISALLOWED SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Offset: 88, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 98, 304, Length: 32, 768 Offset: 163, 340, Length: 32, 768 Offset: 163, 840, Length: 32, 768 Offset: 163, 840, Length: 32, 768 Offset: 163, 608, Length: 32, 768
ProcessHemaderping exe 544 F/R Pro	FASTIO_VRITE IFASTIO_READ FASTIO_VRITE FASTIO_VRITE FASTIO_VRITE FASTIO_VRITE FASTIO_VRITE FASTIO_VRITE FASTIO_VRITE IRP_ML_VRITE FASTIO_VRITE FASTIO_VRITE IRP_ML_FLUSH_BUFFERS FASTIO_VRITE_FOR_CC_FLUSH	C:\Usen:\yoy.Desktop Vol.exe C:\Usen:\yoy.Desktop Vol.exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 98.304, Length: 32,768 Offset: 98.304, Length: 32,768, Priority: Nomal Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 196,508, Length: 32,768 Offset: 196,508, Length: 32,768
ProcessHepadeping.exe 5948 B/F Pro	IRP_ML_WRITE FASTID_READ FASTID_READ FASTID_WRITE FASTID_WRITE FASTID_WRITE FASTID_WRITE FASTID_WRITE FASTID_VRITE FASTID_VRITE FASTID_VRITE FASTID_VRITE FASTID_VRITE FASTID_CREAD FASTID_WRITE FASTID_CREAD FASTID_VRITE FASTID_CREAURE_FOR_CC_FLUSH	C:\Usen'yay\Desktop Vol exe C:\Wndrows\System32cmd exe C:\Usen'yay\Desktop Vol.exe C:\Usen'yay\Desktop Vol.exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 98,304, Length: 32,768, Priority: Normal Offset: 131,072, Length: 32,768 Offset: 131,072, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe 548 5.7 ProcessHepadeping.exe </td <td>FASTIO_IEAD FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_WRITE IRP_ML_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_COURE_FOR_CC_FLUSH</td> <td>C:\Windows\System32\cmd exe C:\Users\yoy\Desktop Vol.exe C:\Windows\System32\cmd exe C:\Users\yoy\Desktop Vol.exe C:\Windows\System32\cmd exe C:\Windows\System32\cmd exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe</td> <td>SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED</td> <td>Offset: 131.072, Length: 32.768 Offset: 153.840, Length: 32.768 Offset: 156.840, Length: 32.768 Offset: 196.608, Length: 32.768</td>	FASTIO_IEAD FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_READ FASTIO_WRITE FASTIO_WRITE IRP_ML_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_COURE_FOR_CC_FLUSH	C:\Windows\System32\cmd exe C:\Users\yoy\Desktop Vol.exe C:\Windows\System32\cmd exe C:\Users\yoy\Desktop Vol.exe C:\Windows\System32\cmd exe C:\Windows\System32\cmd exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe C:\Users\yoy\Desktop Vol.exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 131.072, Length: 32.768 Offset: 153.840, Length: 32.768 Offset: 156.840, Length: 32.768 Offset: 196.608, Length: 32.768
ProcessHepadeping.exe 544 5,7 ProcessHepadeping.exe 544 5,7 ProcessHepadeping.exe 548 5,4 ProcessHepadeping.exe </td <td>FASTIO_FEAD FASTIO_WRITE FASTIO_READ FASTIO_UWRITE FASTIO_UWRITE IRP_ML_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C: Windows System 32 cmd exe C: Users yoy Desktop Vol exe C: Windows System 32 cmd exe C: Wandows System 32 cmd exe C: Wandows System 32 cmd exe C: Users yoy Desktop Vol exe C: Users yoy Desktop Vol exe C: Windows System 32 cmd exe C: Users yoy Desktop Vol exe</td> <td>SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED</td> <td>Offset: 163,840, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768</td>	FASTIO_FEAD FASTIO_WRITE FASTIO_READ FASTIO_UWRITE FASTIO_UWRITE IRP_ML_WRITE FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C: Windows System 32 cmd exe C: Users yoy Desktop Vol exe C: Windows System 32 cmd exe C: Wandows System 32 cmd exe C: Wandows System 32 cmd exe C: Users yoy Desktop Vol exe C: Users yoy Desktop Vol exe C: Windows System 32 cmd exe C: Users yoy Desktop Vol exe	SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 163,840, Length: 32,768 Offset: 163,840, Length: 32,768 Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe 543 5.7 ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe </td <td>FASTID_VIRITE FASTID_EAD FASTID_EAD FASTID_WRITE IRP_ML_WRITE IRP_ML_WRITE FASTID_READ FASTID_READ FASTID_VIRITE IRP_ML_FLUSH_BUFFERS FASTID_ACQUIRE_FOR_CC_FLUSH</td> <td>C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe</td> <td>SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED</td> <td>Offset: 163,840, Length: 32,768 Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768</td>	FASTID_VIRITE FASTID_EAD FASTID_EAD FASTID_WRITE IRP_ML_WRITE IRP_ML_WRITE FASTID_READ FASTID_READ FASTID_VIRITE IRP_ML_FLUSH_BUFFERS FASTID_ACQUIRE_FOR_CC_FLUSH	C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe	SUCCESS SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 163,840, Length: 32,768 Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 544 F/F ProcessHepadeping.exe </td <td>FASTIO_FREAD FASTIO_UWRITE FASTIO_READ FASTIO_WRITE JRP_MJ_WRITE FASTIO_READ FASTIO_VRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C:Windows/System32/cmd.exe C:Users/yay/Desktop/loi exe C:Windows/System32/cmd.exe C:Users/yay/Desktop/loi exe C:Windows/System32/cmd.exe C:Users/yay/Desktop/loi exe</td> <td>SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED</td> <td>Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768</td>	FASTIO_FREAD FASTIO_UWRITE FASTIO_READ FASTIO_WRITE JRP_MJ_WRITE FASTIO_READ FASTIO_VRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C:Windows/System32/cmd.exe C:Users/yay/Desktop/loi exe C:Windows/System32/cmd.exe C:Users/yay/Desktop/loi exe C:Windows/System32/cmd.exe C:Users/yay/Desktop/loi exe	SUCCESS SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 196,608, Length: 32,768 Offset: 196,608, Length: 32,768
ProcessHenjaderping exe 584 517 ProcessHenjaderping exe 584 518 ProcessHenjaderping exe 584 517	FASTIO_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_WRITE FASTIO_READ FASTIO_WRITE IRP_ML_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Users\jxy\Desktop\ol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\ol.exe	SUCCESS SUCCESS FAST IO DISALLOWED	Offset: 196,608, Length: 32,768
ProcessHepadeping.exe 544 5.7 ProcessHepadeping.exe </td <td>FASTIO_IPEAD FASTIO_VINITE IRP_MJ_VINITE FASTIO_READ FASTIO_VINITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\ol.exe</td> <td>SUCCESS FAST IO DISALLOWED</td> <td></td>	FASTIO_IPEAD FASTIO_VINITE IRP_MJ_VINITE FASTIO_READ FASTIO_VINITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\ol.exe C:\Users\jxy\Desktop\ol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\ol.exe	SUCCESS FAST IO DISALLOWED	
ProcessHepadeping.exe 544 547 ProcessHepadeping.exe 548 547 ProcessHepadeping.exe </td <td>FASTIO_WRITE IRP_MJ_WRITE FASTIO_READ FASTIO_WRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\lol.exe</td> <td>FAST IO DISALLOWED</td> <td>011-11-220-220 1</td>	FASTIO_WRITE IRP_MJ_WRITE FASTIO_READ FASTIO_WRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\lol.exe	FAST IO DISALLOWED	011-11-220-220 1
ProcessHepadeping exe 544 SIA ProcessHepadeping exe 543 SIA ProcessHepadeping exe 544 SIA ProcessHepadeping exe </td <td>IRP_MJ_WRITE FASTIO_READ FASTIO_WRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C:\Users\jxy\Desktop\lol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\lol.exe</td> <td></td> <td>Offset: 229,376, Length: 32,768</td>	IRP_MJ_WRITE FASTIO_READ FASTIO_WRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Users\jxy\Desktop\lol.exe C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\lol.exe		Offset: 229,376, Length: 32,768
ProcessHeinadering exe 544 517 ProcessHeinaderping exe 544 517 <	FASTIO_READ FASTIO_WRITE IRP_MJ_FLUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Windows\System32\cmd.exe C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 229,376, Length: 32,768
ProcessHepadeping.ex 544 5.7 ProcessHepadeping.ex 543 5.7 ProcessHepadeping.ex 544 5.7 ProcessHepadeping.ex 544 </td <td>.FASTIO_WRITE .IRP_MJ_FLUSH_BUFFERS .FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C:\Users\jxy\Desktop\lol.exe</td> <td></td> <td>Offset: 229,376, Length: 32,768, Priority: Normal</td>	.FASTIO_WRITE .IRP_MJ_FLUSH_BUFFERS .FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Users\jxy\Desktop\lol.exe		Offset: 229,376, Length: 32,768, Priority: Normal
ProcessHepadeping.ex 545 5.7 ProcessHepadeping.ex 548 5.7 ProcessHepadeping.ex 548 </td <td>.IRP_MJ_FLUSH_BUFFERS .FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td></td> <td>SUCCESS</td> <td>Offset: 262,144, Length: 17,920</td>	.IRP_MJ_FLUSH_BUFFERS .FASTIO_ACQUIRE_FOR_CC_FLUSH		SUCCESS	Offset: 262,144, Length: 17,920
ProcessHepadeping exe 544 5/4 ProcessHepadeping exe </td <td>FASTIO_ACQUIRE_FOR_CC_FLUSH</td> <td>C:\Lloom\inu\Declates\LeLew</td> <td>SUCCESS</td> <td>Offset: 262,144, Length: 17,920</td>	FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\Lloom\inu\Declates\LeLew	SUCCESS	Offset: 262,144, Length: 17,920
ProcessHemaderping exe 544 B/R Pro		C:\Users\jxy\Desktop\lol.exe	SUCCESS	
ProcessHemaderping exe 584 SIR Pro	IRP MJ WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	
ProcessHepadeping exe 544 5.7 ProcessHepadeping exe 548 5.1 ProcessHepadeping exe 548 5.7 ProcessHepadeping exe </td <td>and TurkTurk and P</td> <td>C:\Users\jxy\Desktop\lol.exe</td> <td>SUCCESS</td> <td>Offset: 0, Length: 282,624, I/O Flags: Non-cached, Paging I/O, Synchronous</td>	and TurkTurk and P	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 0, Length: 282,624, I/O Flags: Non-cached, Paging I/O, Synchronous
ProcessHepadeping exe 544 SIR ProcessHepadeping exe </td <td></td> <td>C:\\$LogFile</td> <td>SUCCESS</td> <td>Offset: 77,824, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchron</td>		C:\\$LogFile	SUCCESS	Offset: 77,824, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchron
ProcessHepadeping exe 544 SIA ProcessHepadeping exe </td <td></td> <td>C:\Users\jxy\Desktop\lol.exe</td> <td>SUCCESS</td> <td></td>		C:\Users\jxy\Desktop\lol.exe	SUCCESS	
ProcessHepadepring.exe 5948 B/R		C:\\$LogFile	SUCCESS	Offset: 24,576, Length: 8,192, I/O Flags: Non-cached, Paging I/O, Synchrono
ProcessHepadeping exe 5945 s.11 ProcessHepadeping exe 5948 s.74	IRP_MJ_SET_INFORMATION	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Type: SetEndOfFileInformationFile, EndOfFile: 280,064
IP nocessHepadepring exe 544 5/4 IP nocessHepadepring exe 548 5/4		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Type: SetAllocationInformationFile, AllocationSize: 280,064
IP occessHepadeping exe 5948 6.7 IP occessHepadeping exe 5948 6.7 IP occessHepadeping exe 5948 6.1 IP occessHepadeping exe 5948 6.7 IP occessHepadeping exe 5848 6.7 IP occessHepadeping exe 5848 6.7 IP occessHepadeping exe 5848 6.7		C:\Windows\System32\cmd.exe	SUCCESS	
IP occessHepadeping exe 5948 6,7 IP occessHepadeping exe 5948 6,1 IP occessHepadeping exe 5948 6,4	FASTIO_ACQUIRE_FOR_SECTION_SYNCHRONIZATION		FILE LOCKED WITH WRITERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTEIPAGE
IP occessHepadeping exe 544 SI R IP orcessHepadeping exe 543 SI R IP orcessHepadeping exe 543 SI R IP orcessHepadeping exe 543 SI R IP orcessHepadeping exe 544 SI R IP orcessHepadeping exe 544 SI R IP orcessHepadeping exe 544 SI R		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Type: QueryStandardInformationFile, AllocationSize: 282,624, EndOfFile: 280,0
IP occessHepadeping exe 5948 SIA IP opcessHepadeping exe 5948 SIA	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION		SUCCESS	
IP nocessHepadeping exe 544 SI R IP nocessHepadeping exe 548 SI R		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 1,024, Length: 190,976, I/O Flags: Non-cached, Paging I/O, Priority: N
IP occessHemaderping exe 5848 IAI IP nocessHemaderping exe 5848<		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 192,000, Length: 42,496, I/O Flags: Non-cached, Paging I/O, Priority:
IP ProcessHemaderping exe 544 B.IR IP ProcessHemaderping exe <td></td> <td>C:\Users\jxy\Desktop\lol.exe</td> <td>SUCCESS</td> <td>Offset: 234,496, Length: 512, I/O Flags: Non-cached, Paging I/O, Priority: Nor</td>		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 234,496, Length: 512, I/O Flags: Non-cached, Paging I/O, Priority: Nor
IP occessHepadeping exe 5948 B.I.R IP rocessHepadeping exe 5948 B.F.A IP rocessHepadeping exe	IRP_MJ_READ	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 235,008, Length: 9,216, I/O Flags: Non-cached, Paging I/O, Priority: N
IP ProcessHepadeping exe 5948 SIA IP ProcessHepadeping exe 5948<	.IRP_MJ_READ .IRP_MJ_READ	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 244,224, Length: 512, I/O Flags: Non-cached, Paging I/O, Priority: Nor
IP nocessHepadeping exe 544 6.7 IP nocessHepadeping exe 543 6.7 IP nocessHepadeping exe 544 6.7	IRP_MJ_READ	C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 244,736, Length: 34,304, I/O Flags: Non-cached, Paging I/O, Priority: Offset: 279,040, Length: 1,024, I/O Flags: Non-cached, Paging I/O, Priority: N
ProcessHemaderping.exe 544 517 ProcessHemaderping.exe 548 518 ProcessHemaderping.exe 548 518 ProcessHemaderping.exe 548 517 Pro			SUCCESS	SyncType: SyncTypeOther
ProcessHepadeping exe 544 B.IR Pro			SUCCESS	Sync Type. Sync TypeOther
ProcessHepadeping exe 5948 \$147 ProcessHepadeping exe 5948 \$174	IRP_MJ_QUERY_SECURITY	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Information: Label
IP rocessHepaderping exe 543 5,7	IRP_MJ_QUERY_INFORMATION	C:\Users\jxy\Desktop\ol.exe	SUCCESS	Type: QueryNameInformationFile, Name: \Users\jxy\Desktop\lol.exe
IP ProcessHemaderping.exe 5943 B, F IP rocessHemaderping.exe 5943 B, F IP rocessHemaderping.exe <td>FASTIO_QUERY_INFORMATION</td> <td>C:\Users\jxy\Desktop\lol.exe</td> <td>SUCCESS</td> <td>Type: QueryStandardInformationFile, AllocationSize: 282,624, EndOfFile: 280,</td>	FASTIO_QUERY_INFORMATION	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Type: QueryStandardInformationFile, AllocationSize: 282,624, EndOfFile: 280,
IP rocessHepadeping exe 548 5.7	FASTIO_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	C:\Users\ixy\Desktop\lol exe	FILE LOCKED WITH WRITERS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTEIPAGE
ProcessHepadepring.exe 584 547 ProcessHepadepring.exe 5848 547 ProcessHepadepring.exe 5848 547 ProcessHepadepring.exe 5848 547 ProcessHepadepring.exe 5848 547		C:\Users\jxy\Desktop\ol.exe	SUCCESS	Type: QueryStandardInformationFile, AllocationSize: 282,624, EndOfFile: 280,
IP rocessHemademing exe 543 1,67	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION		SUCCESS	,, , ,
E ProcessHemademing.exe 5443 b.7	FASTIO_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Sync Type: Sync TypeOther
IP occessHepademing.exe 594 B.F. ProcessHepademing.exe 594 B.F.	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\Users\jxy\Desktop\lol.exe	SUCCESS	
• ProcessHepadeping are 548 a, F1	FASTIO QUERY INFORMATION	C:\Users\ixy\Desktop\lol.exe	SUCCESS	Type: QueryStandardInformationFile, AllocationSize: 282,624, EndOfFile: 280,
IP ProcessHerpaderping exe 5848 B, IP IP ProcessHerpaderping exe 5848 B, F/	FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	FAST IO DISALLOWED	Offset: 0, Length: 32,768 Target file (lol.
ProcessHepademing.exe 5848 F/	IRP_MJ_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 0, Length: 32,768, Priority: Normal al ready cached to
ProcessHepademing.exe 5848 F/		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Uffset: 32,768, Length: 32,768
ProcessHepadeping.exe ProcessHepadeping.exe ProcessHepadeping.exe ProcessHepadeping.exe ProcessHepadeping.exe S848 ProcessHepadeping.exe S848 ProcessHepadeping.exe S848		C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 65,536, Length: 32,768 represent source
ProcessHerpaderping.exe 5848 5848 5848 ProcessHerpaderping.exe 5848 5848 5848 ProcessHerpaderping.exe 5848 5848	FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 98,304, Length: 32,768
ProcessHerpaderping.exe 5848 ProcessHerpaderping.exe 5848 F/	.FASTIO_WRITE .FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 131,072, Length: 32,768 0:000> dt ntoskri
ProcessHerpaderping.exe 5848 - FA	.FASTIO_WRITE .FASTIO_WRITE .FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 163,840, Length: 32,768
ProcessHerpaderping.exe 5848 F/ ProcessHerpaderping.exe 5848 F/ F/	,FASTIO_WRITE ,FASTIO_WRITE ,FASTIO_WRITE ,FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Uffset: 196,608, Length: 32,768
💶 ProcessHerpaderping.exe 5848 🔜 FA	FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 229,376, Length: 32,768 +0x008 Shared
	FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE	C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 262,144, Length: 17,920 +0x010 ImageS
ProcessHerpaderping.exe 5848	FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE		SUCCESS	
ProcessHerpaderping.exe 5848 S848 F/	FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE MSP_MJ_FLUSH_BUFFERS	C:\Users\jxy\Desktop\lol.exe	SUCCESS	
ProcessHerpaderping.exe 5848 Rev IR	FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE TASTID_ACQUIRE_FOR_CC_FLUSH	C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe	SUCCESS	Offset: 0, Length: 282,624, I/O Flags: Non-cached, Paging I/O, Synchronous
ProcessHerpaderping.exe 5848 S848	FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE IRP_MJ_FLUSH_BUFFERS FASTID_ACQUIRE_FOR_CC_FLUSH IRP_MJ_VRITE	C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe		Offset: 94,208, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchrone
	FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE FASTIO_WRITE IRP_MJ_FUSH_BUFFERS FASTIO_ACQUIRE_FOR_CC_FLUSH IRP_MJ_WRITE	C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe C:\Users\jxy\Desktop\lol.exe C:\\$LogFile	SUCCESS	
ProcessHerpaderping.exe 5848	FASTID_WRITE FASTID_WRITE FASTID_WRITE FASTID_WRITE FASTID_WRITE FASTID_WRITE IRP_MI_VRITE FASTID_ACQUIRE_FOR_CC_FLUSH IRP_MI_WRITE IRP_MI_WRITE IRP_MI_WRITE IRP_MI_WRITE	C:\Users\ixy\Desktop\ol.exe C:\Users\ixy\Desktop\ol.exe C:\Users\ixy\Desktop\ol.exe C:\SLogFile C:\Users\ixy\Desktop\ol.exe	SUCCESS	Offset: 28,672, Length: 4,096, I/O Flags: Non-cached, Paging I/O, Synchronom
ProcessHerpaderping.exe 5848 APPr 7100 7100 7100 7100 7100 7100 7100 7100	FASTIO_VMITE FASTIO_VMITE FASTIO_VMITE FASTIO_VMITE FASTIO_VMITE FASTIO_VMITE IRP_ML_FULSH_BUFFERS IRP_ML_VMITE IRP_ML_VMITE IRP_ML_VMITE IRP_ML_VMITE FASTIO_RELEASE_FOR_CC_FLUSH IRP_ML_VMITE	C:\Users\ixy\Desktop\ol.exe C:\Users\ixy\Desktop\ol.exe C:\Users\ixy\Desktop\ol.exe C:\SLogFile C:\Users\ixy\Desktop\ol.exe C:\Users\ixy\Desktop\ol.exe C:\SLogFile	SUCCESS SUCCESS	
 Iol.exe 7188 APr 7188 APr 7188 APr 	FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_ACOURTE_FOR_CC_FLUSH IRP_MJ_VWITE IRP_MJ_VWITE IRP_MJ_VWITE FASTID_RELEASE_FOR_CC_FLUSH IRP_MJ_VWITE Process Create	C:\Users\yxy\Desktop\ol.exe C:\Users\yxy\Desktop\ol.exe C:\Users\yxy\Desktop\ol.exe C:\SLogFile C:\SLogFile C:\SLogFile Users\yxy\Desktop\ol.exe	SUCCESS SUCCESS SUCCESS	PID: 7188, Command line: .Vol.exe
■-lol.exe /188 47 In ■-lol.exe 7188 47 Lo	FASTID_VMITE FASTID_VMITE FASTID_VMITE FASTID_VMITE FASTID_VMITE FASTID_VMITE FASTID_VMITE IMP_MJ_FUSH_BUFFERS IAP_MJ_VMITE IRP_MJ_VMITE IRP_MJ_VMITE FASTID_RELEASE_FOR_CC_FLUSH IRP_MJ_VMITE Process Create Process Screate Process Screate	C:\Users\yxy\Desktop\ol.exe C:\Users\yxy\Desktop\ol.exe C:\Users\yxy\Desktop\ol.exe C:\SLogFile C:\SLogFile C:\SLogFile Users\yxy\Desktop\ol.exe	SUCCESS SUCCESS SUCCESS SUCCESS	PID: 7188, Command line: .Vol.exe Parent PID: 5848, Command line: .Vol.exe, Current directory: C:\Users\jxy\De
 Iol.exe 7188 Array Lo Iol.exe 7188 Array Lo 7188 Array Lo 	FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_VWITE FASTID_ACOURTE_FOR_CC_FLUSH IRP_MJ_VWITE IRP_MJ_VWITE IRP_MJ_VWITE FASTID_RELEASE_FOR_CC_FLUSH IRP_MJ_VWITE Process Create	C:\Users\yxy\Desktop\ol.exe C:\Users\yxy\Desktop\ol.exe C:\Users\yxy\Desktop\ol.exe C:\SLogFile C:\SLogFile C:\SLogFile Users\yxy\Desktop\ol.exe	SUCCESS SUCCESS SUCCESS	

Click image to enlarge

The <u>SECTION_OBJECT_POINTERS</u> of the <u>FILE_OBJECT</u> play a key role here. The OS will cache the initial image mapping and re-use the already mapped section, even if there is active write access to the <u>FILE_OBJECT</u>. This also means that a user can open the original file with exclusive access. While this won't necessarily create an issue for the kernel callback, it does affect downstream logic in that it assumes that when the user opens the file with read access it will be broken. However, such logic does not apply, given that the file content has been overwritten. Further, the kernel callback is hopeless too, since reading directly from the file using that <u>FILE_OBJECT</u> will read the wrong data.

This also means if a user tries to execute that process again it will result in a sharing violation. From user mode, without access to that original target file handle, no one may conventionally execute the process.

Resolving This Issue: A Short-term Fix and Long-term Solution

Unfortunately, there is not a clear fix for herpaderping attacks. It seems reasonable that preventing an image section from being mapped/cached when there is write access to the file should close the hole. However, that may or may not be a practical solution.

There is a frustration among the development community about the incoherency between what is on disc and what it is going to execute, which is a common issue with all major operating systems. As such, that is something that should be considered when designing a security product.

While there isn't a clear mechanism to guarantee that coherency, there are ways that security vendors, as well as security engineers and analysts, can foresee this issue and minimize the risk.

One way to detect this type of exploit is to look for write access to the related file object when the process is created. The exploit seems achievable through a higher-level API call. That said, the API juggling involved usually requires a native-call, which allows the attacker to tightly control the process creation flow.

Another way to detect this type of exploit is checking for coherency between the file on disk and the mapped process. Viewing the image coherency between the file on disk and the mapped process may be seen in an addition I've made to Process Hacker, and also shows the spoofed display of "Google" as the "signer" due to the exploit.

1	Process	Hacker	[JSHAW	-DESKTOP	\Johnny]+	(Administrator)
---	---------	--------	--------	----------	-----------	-----------------

Hacker View Tools U	sers Hel	р					
🏶 🔄 🔗 💀							
Processes Services Netw	ork Disk						
Name		Image Coherency	PID	CPU	I/O total	Private b	Net
conho	st.exe	99.91%	7748			6.38 MB	
🗸 📧 ServiceHu	ıb.Host	100.00%	10716			55.36 MB	
conho	conhost.exe					6.37 MB	
🗸 📧 ServiceHu	✓ ■ ServiceHub.Thre					69.85 MB	
🔤 conho	st.exe	99.91%	9952			6.38 MB	
🗸 🔽 msvsmon.ex	✓ → msvsmon.exe			0.01	5.99 kB/s	132.9 MB	
👰 ProcessHa	acker.exe	99.91%	5344	0.26	27.86 kB/s	68.49 MB	
📮 msvsmon.ex	e	99.91%	9380			242.15 MB	
ScriptedSand	lbox64	99.91%	11176	0.42	58.38 kB/s	91.8 MB	
📧 vcpkgsrv.exe		99.88%	17948			79.25 MB	
🗸 🔀 WindowsTermin	✓ Σ WindowsTerminal.exe					52 MB	
🔤 OpenConsol	99.91%	17520			2.17 MB		
💙 🔀 powershell.e	99.91%	18536			76.67 MB		
🗸 🐻 ProcessHe	99.84%	9620			1.22 MB		
🗡 🏧 lol.exe		 14.31%	8640			2.01 MB	
SnippingTool.ex SnippingTool.ex vmmem SoogleCrashHandl SoogleCrashHandl Signached.exe Sattle.net.exe Battle.net.exe Sattle.net.exe	C:\Use Windo Micros Notes: Signer: Low In	99.91% rs\Johnny\source\re ws Command Proces oft Corporation Google LLC nage Coherency: 14.3 le host: conhost.exe 89.98%	ssor 10.0.1				
✓ III Agent.exe		82.34%	10448	0.01		58.06 MB	
conhost.exe		<	10440	0.01		50.00 1410	
	al memor	ry: 10.56 GB (16.51%)	Free mer	morv: 53	.4 GB (83.49%	6)	
		,					

Click image to enlarge

Here is a link to the enhancement proposal I've made to Process Hacker: https://github.com/processhacker/processhacker/issues/744

Process Tampering may also be seen through a recent addition to SysMon by Mark Russinovich, CTO of Microsoft Azure, reproduced below and in this tweet.

Information	11/1//2020 10:30:08 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	11/17/2020 10:30:08 AM	Sysmon	25	Process Tampering (rule: ProcessTampering)
(i) Information	11/17/2020 10:30:07 AM	Sysmon	1	Process Create (rule: ProcessCreate)
 Information 	11/17/2020 10:30:07 AM	Sysmon	1	Process Create (rule: ProcessCreate)
 Information 	11/17/2020 10:29:57 AM	Sysmon	25	Process Tampering (rule: ProcessTampering)

Event 25, Sysmon

General Details

Process Tampering: RuleName: -UtcTime: 2020-11-17 18:30:07.855 ProcessGuid: {bee51ebb-16af-5fb4-9f02-000000005000} ProcessId: 7128 Image: C:\Temp\HelloWorld1.exe Type: Image is locked for access

Click image to enlarge

evel	Date and Time	Source	Even	Task Category
Information	11/17/2020 10:30:35 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	11/17/2020 10:30:35 AM	Sysmon	25	Process Tampering (rule: ProcessTampering)
Information	11/17/2020 10:30:34 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	11/17/2020 10:30:34 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	11/17/2020 10:30:08 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	11/17/2020 10:30:08 AM	Sysmon	25	Process Tampering (rule: ProcessTampering)
Information	11/17/2020 10:30:07 AM	Sysmon	1	Process Create (rule: ProcessCreate)
Process Tamp RuleName: - UtcTime: 2020	ering:)-11-17 18:30:34.733 {bee51ebb-16ca-5fb4-a202-000	00005000}		
Descent	{bee51ebb-10ca-5tb4-a202-000	000005000}		

Click image to enlarge

As for a long-term solution, that would require working with the OS to agree on a joint approach. We're hopeful that as the technique gains broader awareness, the OS vendors will work with the cybersecurity community to adopt more stringent countermeasures directly in the OS.

What are your thoughts? How do you reduce the risk of herpaderping in the short-term? What steps do you think the OS community must take to address this issue more systematically? For additional context and insight, see what industry professionals are saying and join the conversation on Twitter. https://twitter.com/gentilkiwi/status/1321001331755286529?s=20

https://twitter.com/Mordor_Project/status/1320949216018112514?s=20

https://twitter.com/jxy__s/status/1320873966752329729?s=20

https://twitter.com/analyzev/status/1320914701514084352?s=20

https://twitter.com/markrussinovich/status/1328769178233237504?s=20

Does this work sound interesting to you? Visit CrowdStrike's Engineering and Technology page to learn more about our engineering team, our culture and current open positions: <u>https://www.crowdstrike.com/careers/engineering-technology-team/</u>