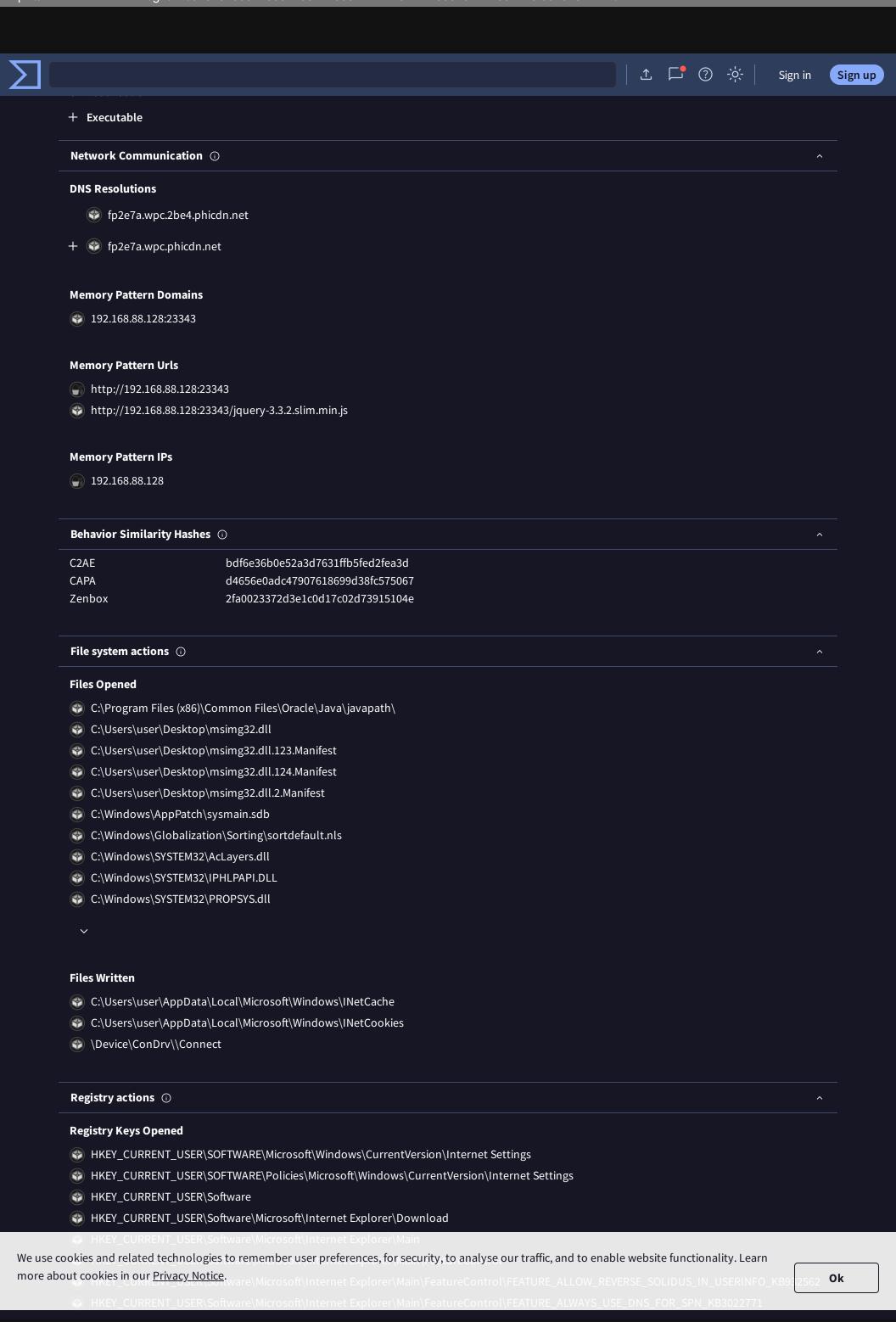


We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our <u>Privacy Notice</u>.

Ok



	.	土		?	-;•;-	Sign in	Sign up
~							
Registry Keys Set							
+ HKU\S-1-5-21-575823232-3065301323-1442773979- 1000\Software\Microsoft\SystemCertificates\Root\Certificates\0174E68C97DDF1E0EEEA415EA336A163 HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\			-D\Blo	b			
+ Settings\Connections\SavedLegacySettings							
$+ \hspace{0.1in} \textbf{HKU} \\ \textbf{S-1-5-21-575823232-3065301323-1442773979-1000} \\ \textbf{Software} \\ \textbf{Microsoft} \\ \textbf{Windows} \\ \textbf{CurrentVersion} \\ \textbf{Version} \\ $	∖Inter	net	Settin	gs\Pro	oxyEna	able	
+	\Inter	net	Settin	gs\Pro	oxySer	ver	
+ 🕝 HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\Windows Error F	Repoi	rting	ζ∖Debι	ug\Stc	reLoca	ation	
Process and service actions ①							^
Shell Commands							
SANDBOX_DLL_LOADER_AMD64% %SAMPLEPATH% %WORKDIR% 483							
rundll32.exe %SAMPLEPATH%,DllGetClassObject							
rundll32.exe %SAMPLEPATH%,DllMain							
Processes Terminated							
%windir%\System32\svchost.exe -k WerSvcGroup							
%windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}							
⊚ %windir%\system32\WerFault.exe -u -p 2616 -s 92							
⊚ %windir%\system32\WerFault.exe -u -p 2700 -s 640							
rundll32.exe %SAMPLEPATH%,DllGetClassObject							
rundll32.exe %SAMPLEPATH%,DllMain							
rundll32.exe %SAMPLEPATH%,StartW							
wmiadap.exe /F /T /R							
Processes Tree							
② 2616 - %SANDBOX_DLL_LOADER_AMD64% %SAMPLEPATH% %WORKDIR% 483							
→ 2692 - rundll32.exe %SAMPLEPATH%,DllMain							
→ 2700 - rundll32.exe %SAMPLEPATH%,StartW							
→ 2684 - rundll32.exe %SAMPLEPATH%,DllGetClassObject							
2208 - %windir%\System32\svchost.exe -k WerSvcGroup							
→ 2732 - %windir%\system32\WerFault.exe -u -p 2616 -s 92							
→ 2868 - %windir%\system32\WerFault.exe -u -p 2700 -s 640							
816 - wmiadap.exe /F /T /R							
2808 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}							
2008 - %windir%\system32\wbem\wmiprvse.exe							
> 2000 /owindii /o/jystemsz/wbem/wmprvsc.exe							
Synchronization mechanisms & Signals ①							^
Mutexes Created							
\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex							
Highlighted actions ①							^

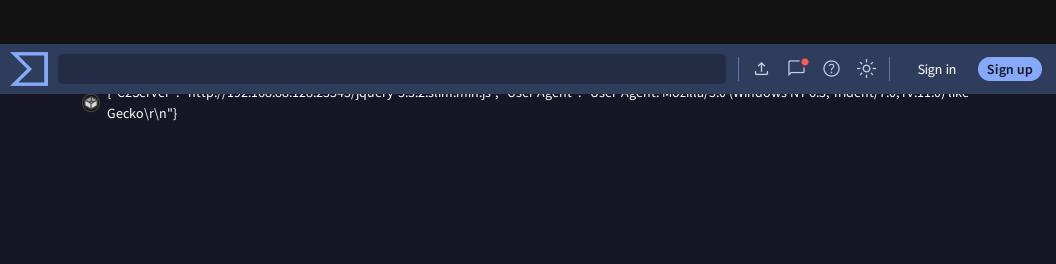
Page 3 of 4

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn

more about cookies in our $\underline{\text{Privacy Notice}}.$

Ok

VirusTotal - File - 94816439312563db982cd038cf77cbc5ef4c7003e3edee86e2b0f99e675ed4ed - 02/11/2024 19:08 https://www.virustotal.com/gui/file/94816439312563db982cd038cf77cbc5ef4c7003e3edee86e2b0f99e675ed4ed/behavior



Our product	Community	Tools	Premium Services	Documentation
Contact Us	Join Community	API Scripts	Get a demo	Searching
Get Support	Vote and Comment	YARA	Intelligence	Reports
How It Works	Contributors	Desktop Apps	Hunting	API v3 v2
ToS Privacy Notice	Top Users	Browser Extensions	Graph	Use Cases
Blog Releases	Community Buzz	Mohile Ann	API v3 l v2	

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our <u>Privacy Notice</u>.

Ok