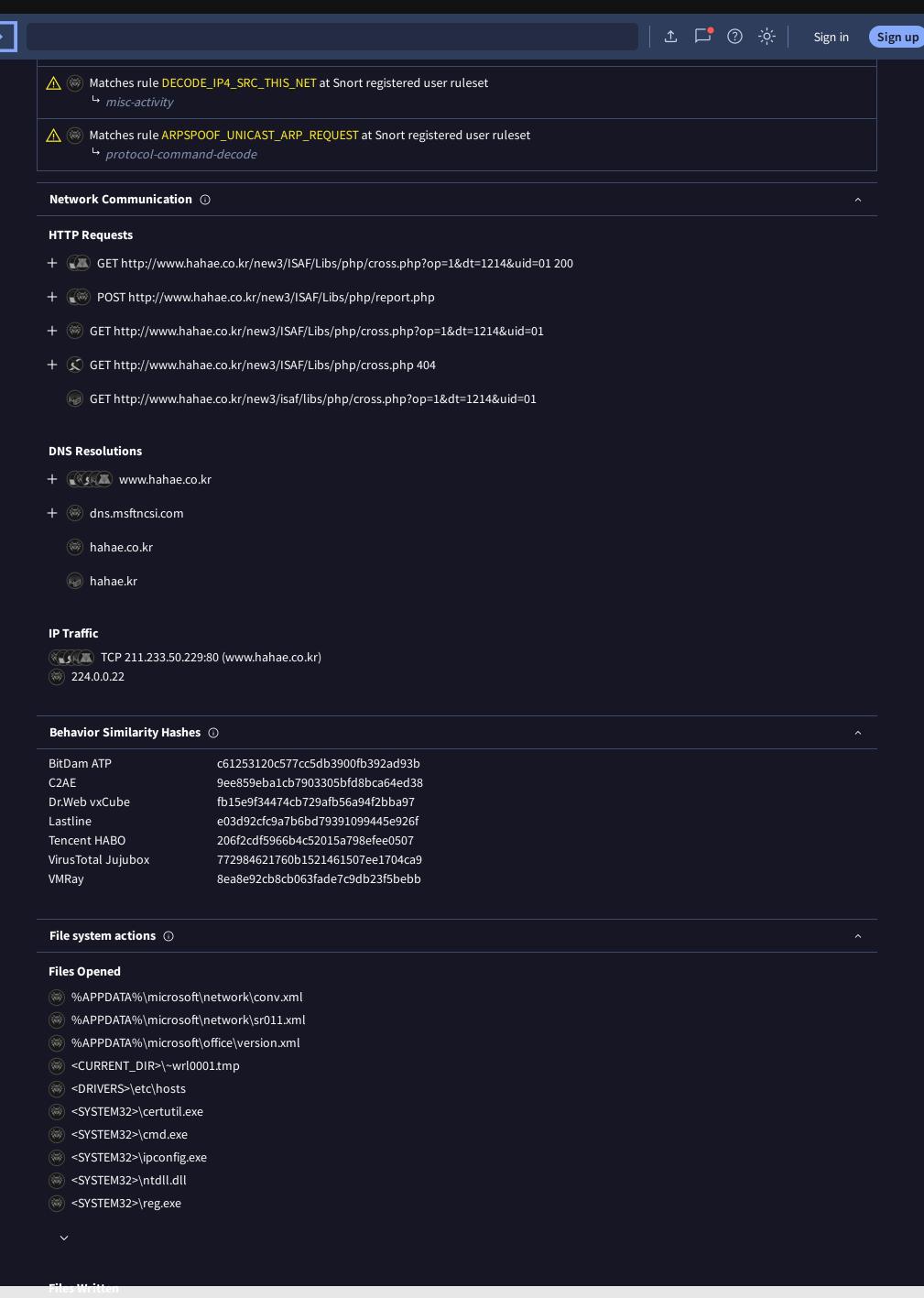


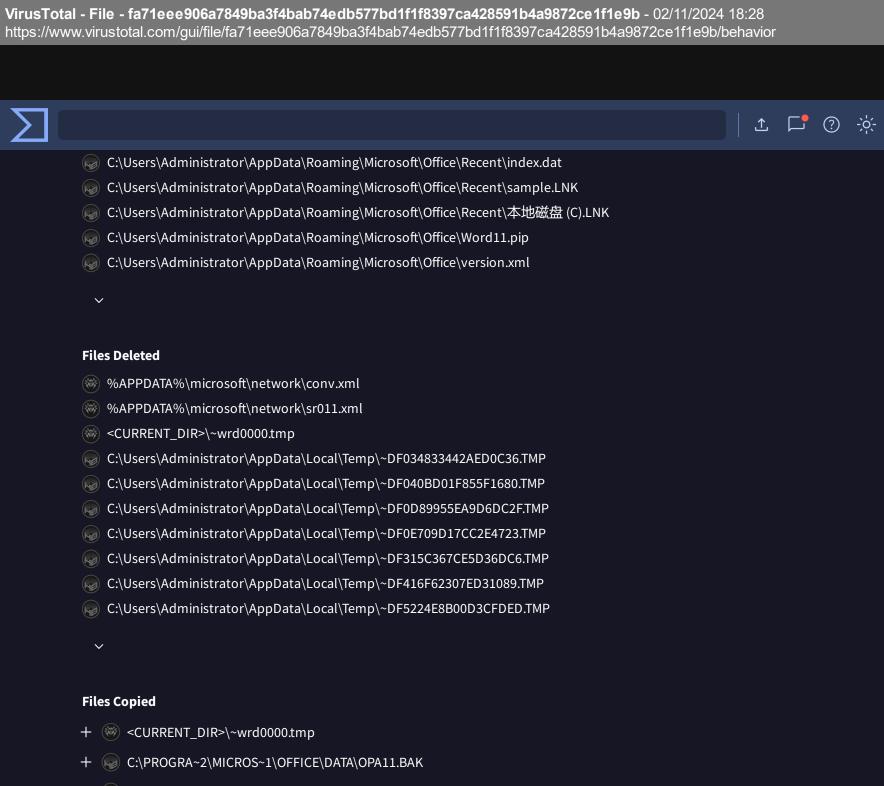
more about cookies in our <u>Privacy Notice</u>.

Matches rule PSNG\_UDP\_PORTSWEEP\_FILTERED at Snort registered user ruleset



cooking and related took

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>. work sr011 xml



- + C:\sample.doc

## **Files With Modified Attributes**

- <</pre><</pre></pr
- <</pre></pre
- C:\Users\Mason\AppData\Roaming\Microsoft\Office\Recent\index.dat
- C:\Users\Mason\Documents\~WRD0000.tmp
- C:\Users\Mason\Documents\~WRD0002.tmp
- C:\Users\Mason\Documents\~WRL0001.tmp
- C:\Users\Mason\Documents\~WRL0003.tmp

## Files Dropped

- + %APPDATA%\microsoft\network\conv.xml
- + %APPDATA%\microsoft\network\sr011.xml
- + <CURRENT\_DIR>\~wrd0000.tmp
- + <PATH\_SAMPLE>.doc
- + <SYSTEM32>\tasks\ahnlabupdate
- + data.txt
- + 9fe3031c7df47e30c8eb99dfe80ffdece11c9421fb2ca5566ddf82759a2f0989
- + C:\Users\FD1HVy\AppData\Roaming\Microsoft\Office\version.xml

Registry actions ①

## **Registry Keys Opened**

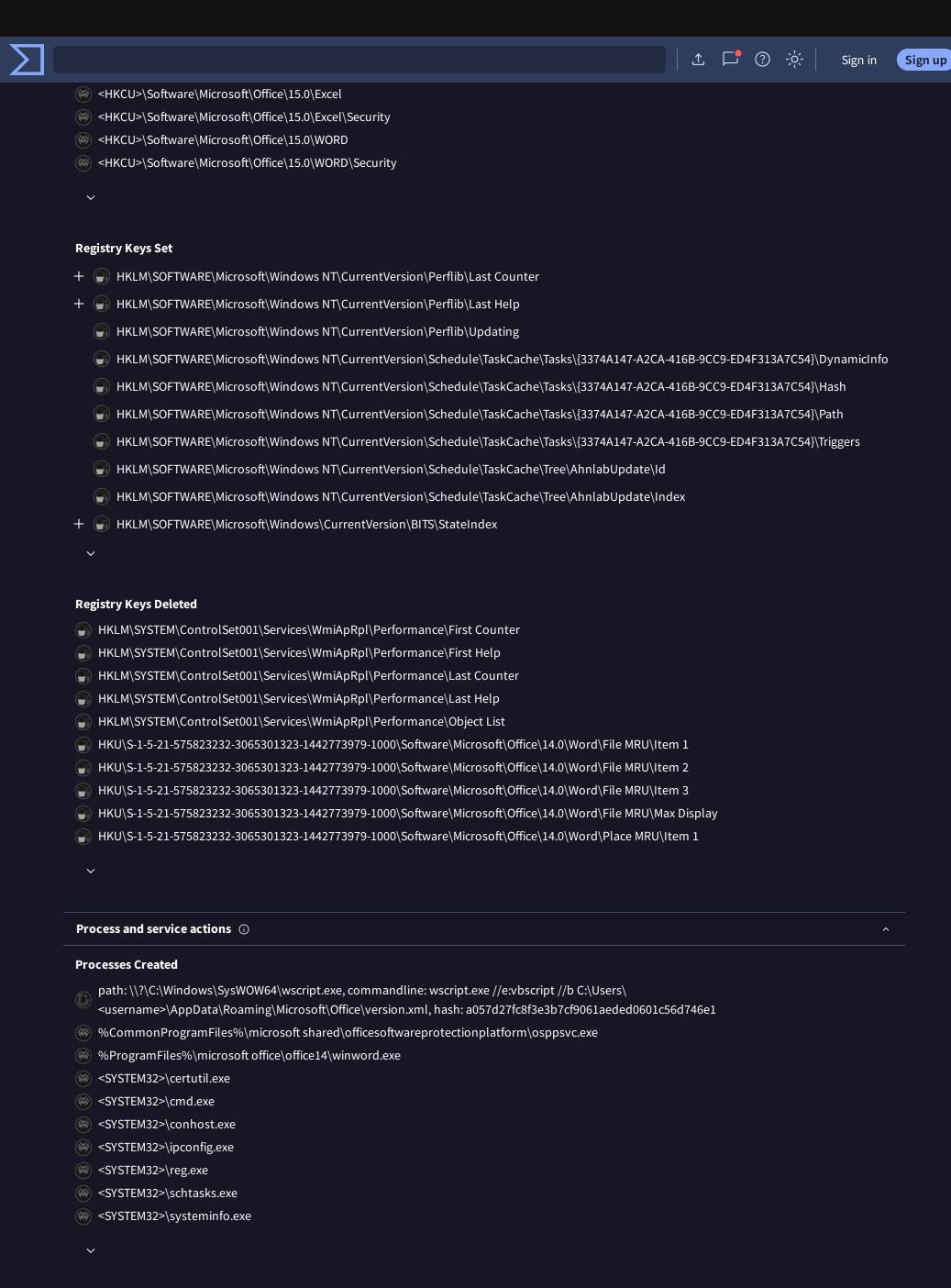
<HKCU>\Software

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>.

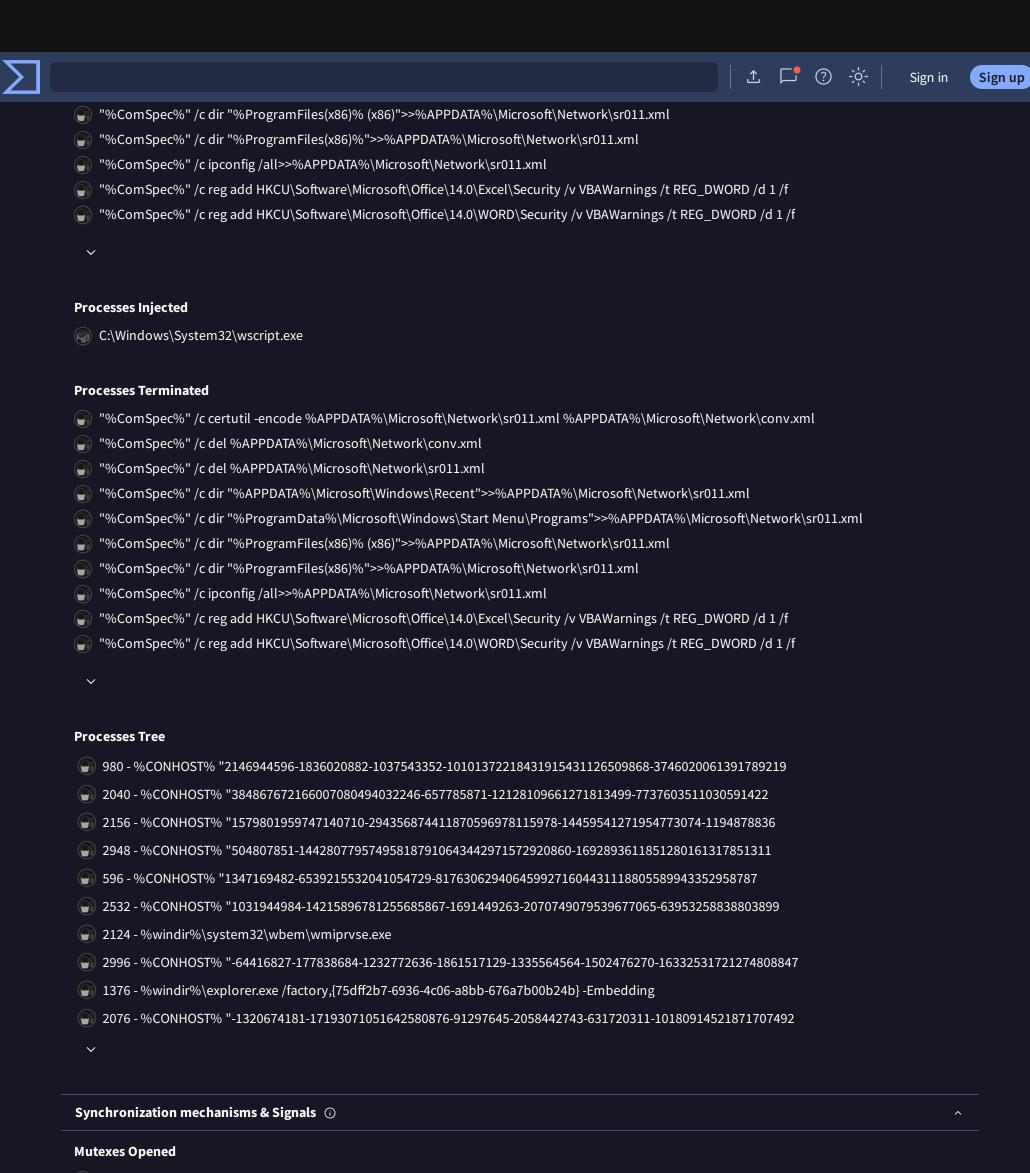
Ok

Sign in

Sign up



Shell Commands



\(\sigma\) \Sessions\1\BaseNamedObjects\Global\BFE\_Notify\_Event\_{\lab6c556-6a09-4d0a-bd5a-d316ef552c3f}

\(\sigma\) \Sessions\1\BaseNamedObjects\Global\TermSrvReadyEvent

@ Global\MTX\_MSO\_AdHoc1\_S-1-5-21-1547548985-192504236-2982455695-500

@ Global\MTX\_MSO\_Formal1\_S-1-5-21-1547548985-192504236-2982455695-500

Local\MSCTF.Asm.MutexDefault1

♠ Local\MU\_ACBPIDS08

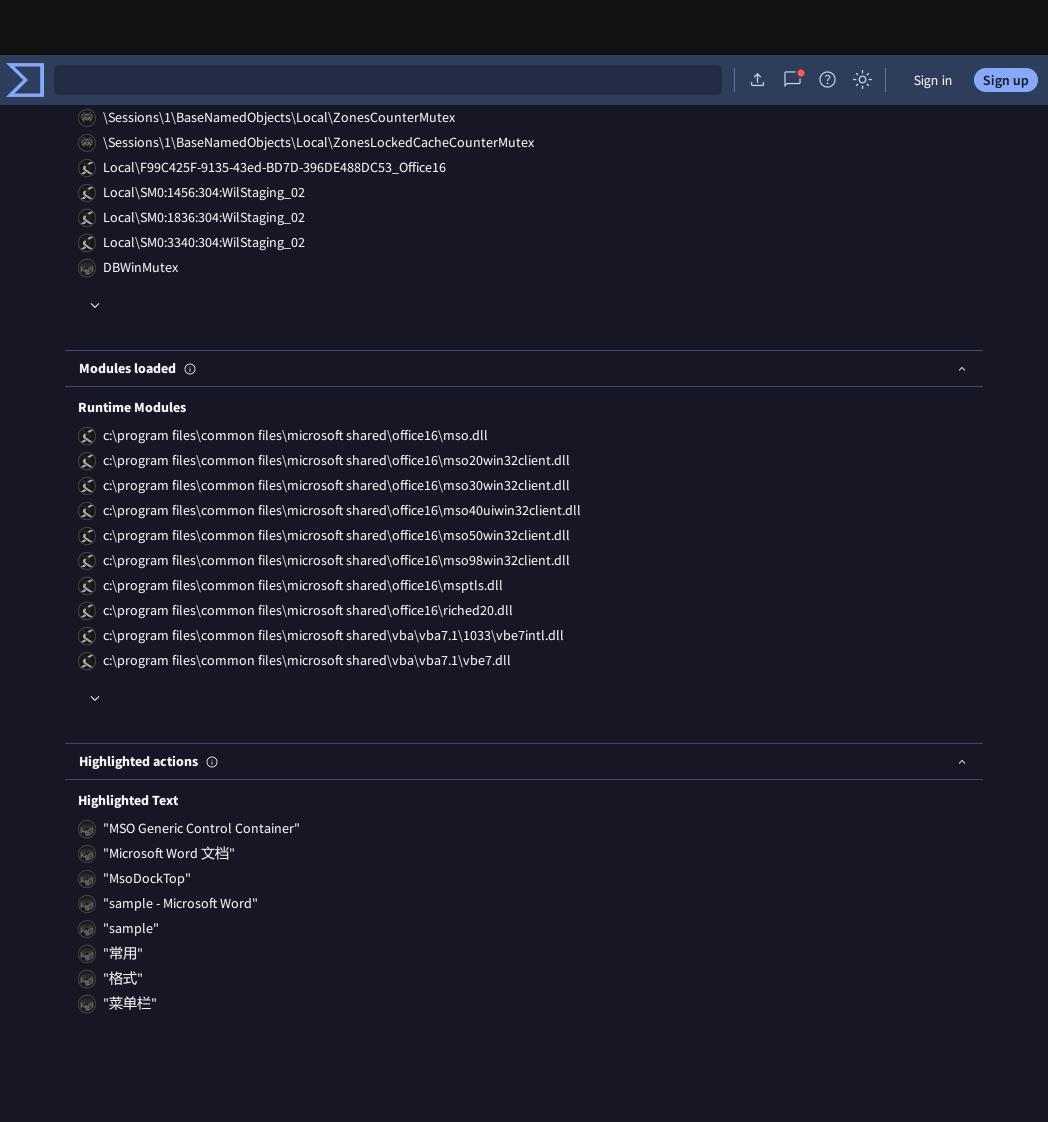
Local\Mso97SharedDg19211105606Mutex

Local\Mso97SharedDg19521105606Mutex

Local\Mso97SharedDg19531105606Mutex

Local\Mso97SharedDg20321105606Mutex

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>.



Our product	Community	10015	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	Mobile App	API v3   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>.