



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

MSS-EDR REPORT

ACME FINANCIAL SERVICES

May 15, 2023



MSS-EDR REPORT

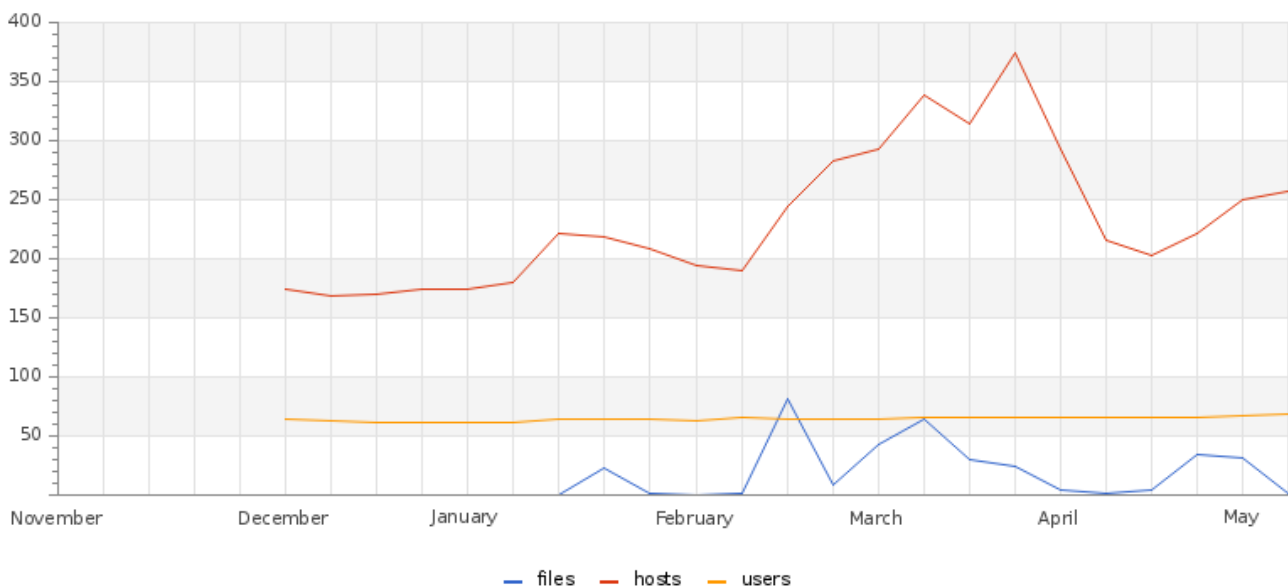
ACME FINANCIAL SERVICES 05/15/2023

TLP AMBER

MSS-EDR REPORT

About this report

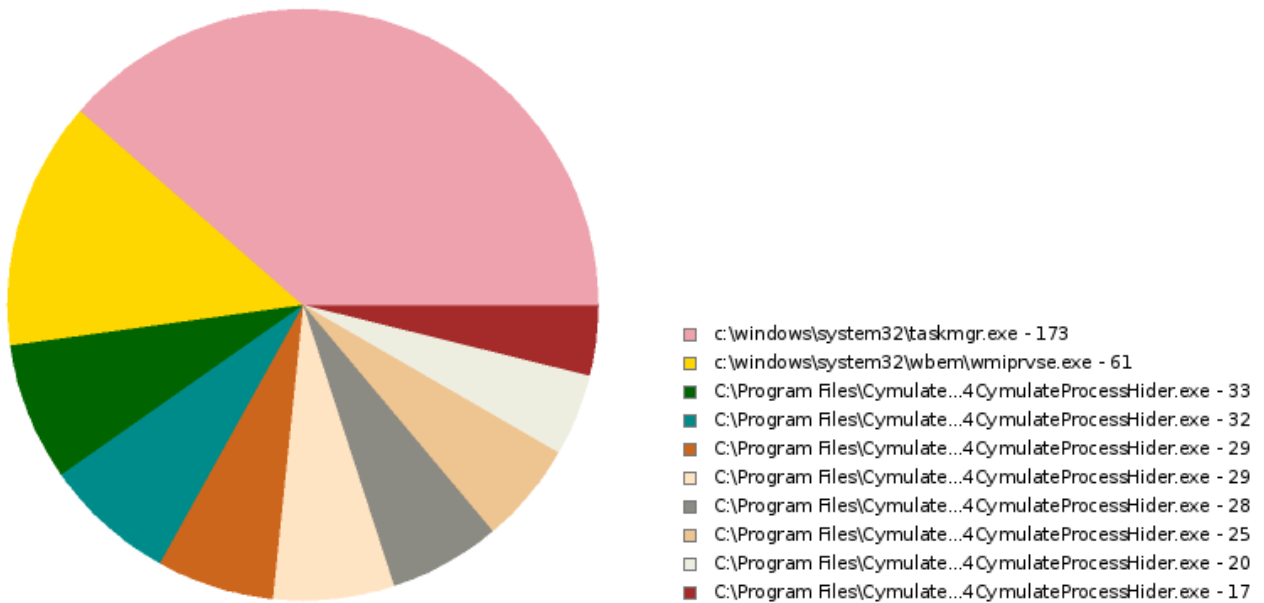
This is a SKYWATCH report that presents the most up-to-date information for the MSS-EDR as displayed in the service dashboard.

Average Threat - User Defined**87****Threat Score**

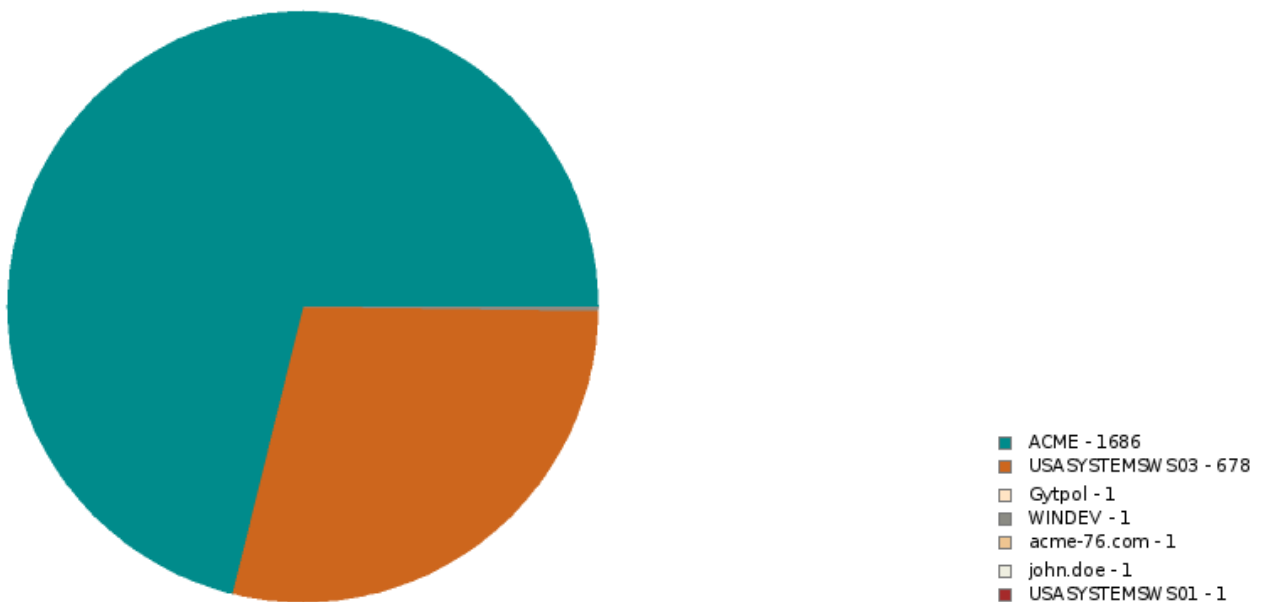
MSS-EDR REPORT

ACME FINANCIAL SERVICES 05/15/2023

Events by File Path - User Defined



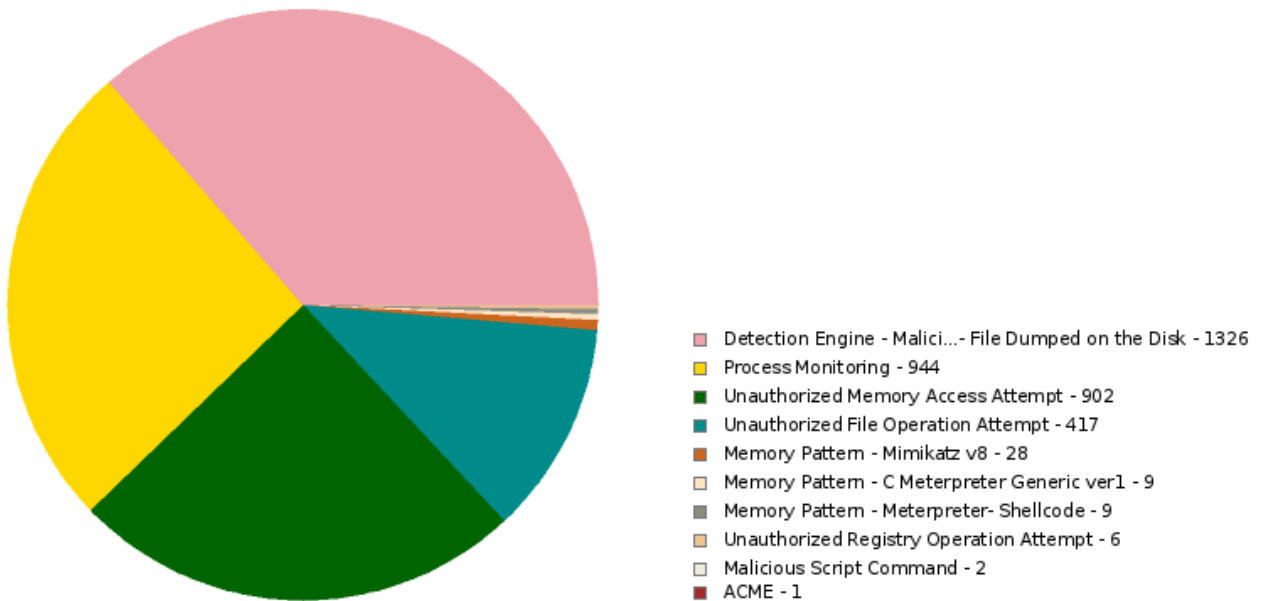
Events by Host Name - User Defined



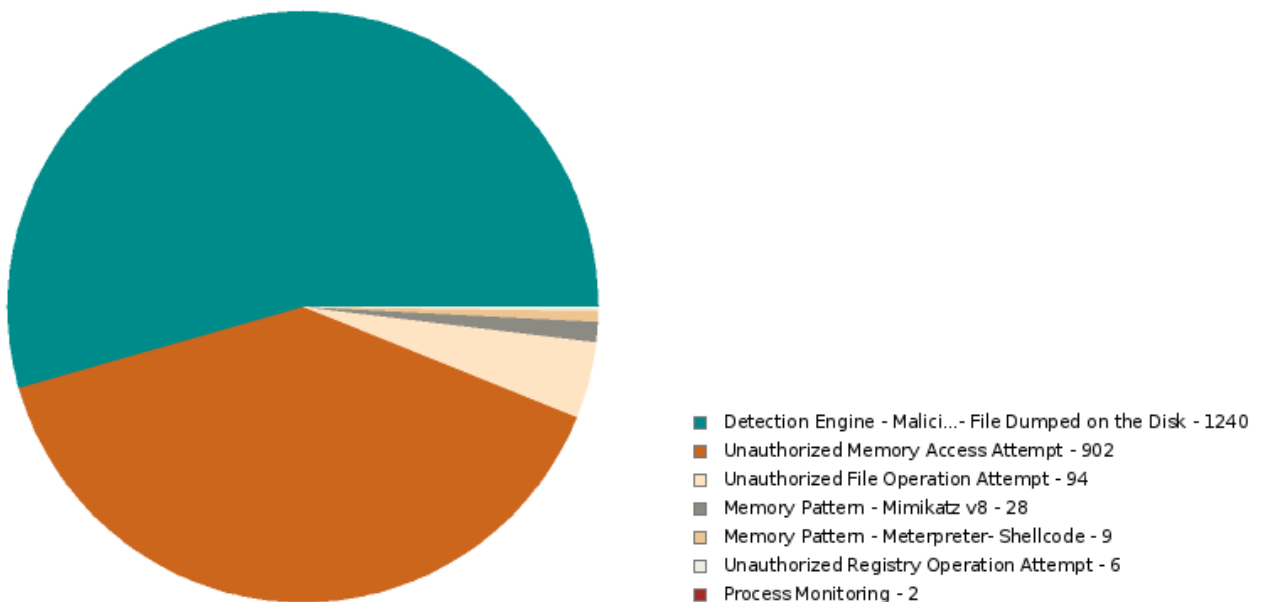
MSS-EDR REPORT

ACME FINANCIAL SERVICES 05/15/2023

Events by Event Name - User Defined



High Severity Events by Event Name - User Defined



MSS-EDR REPORT

ACME FINANCIAL SERVICES 05/15/2023

Brute Force Detection by Ratio - User Defined

Host \ User Name	Ratio (Bad : Good)	Probability
jdoe	1307 : 97	13.47
adoe	12 : 47	0.26
doe.john	1 : 8	0.13
ACME	4 : 80	0.05
odoe	1 : 29	0.03
ACME	1 : 126	0.01
john22	1 : 720	0.00
idoe	1 : 710	0.00

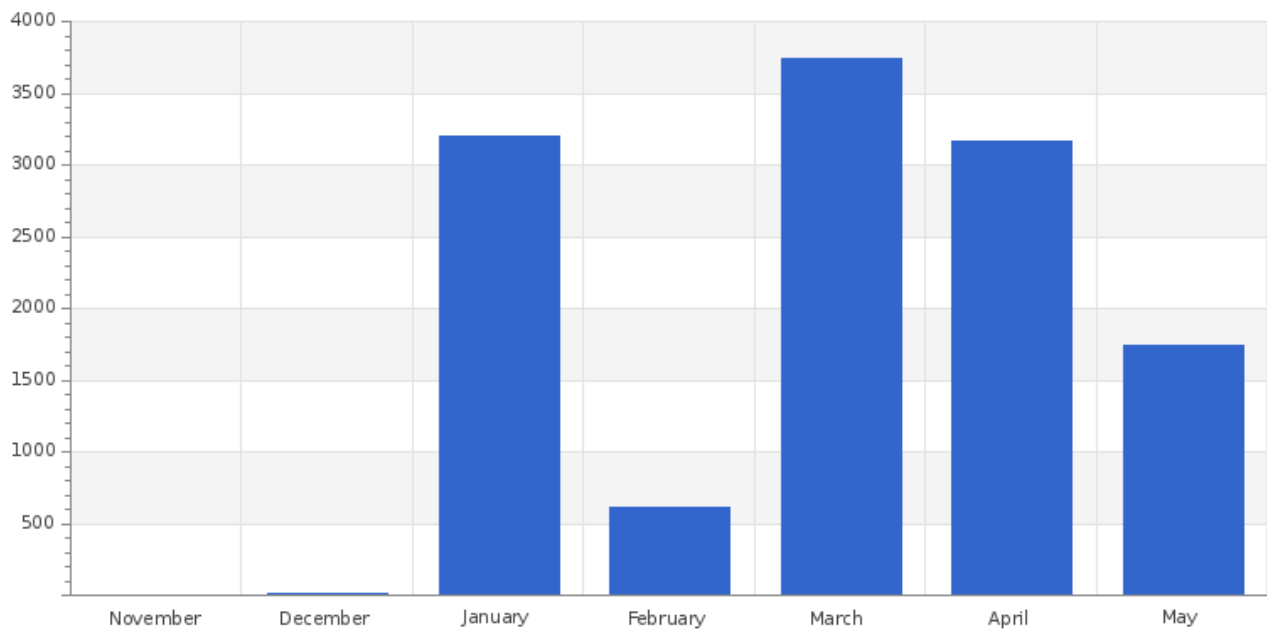
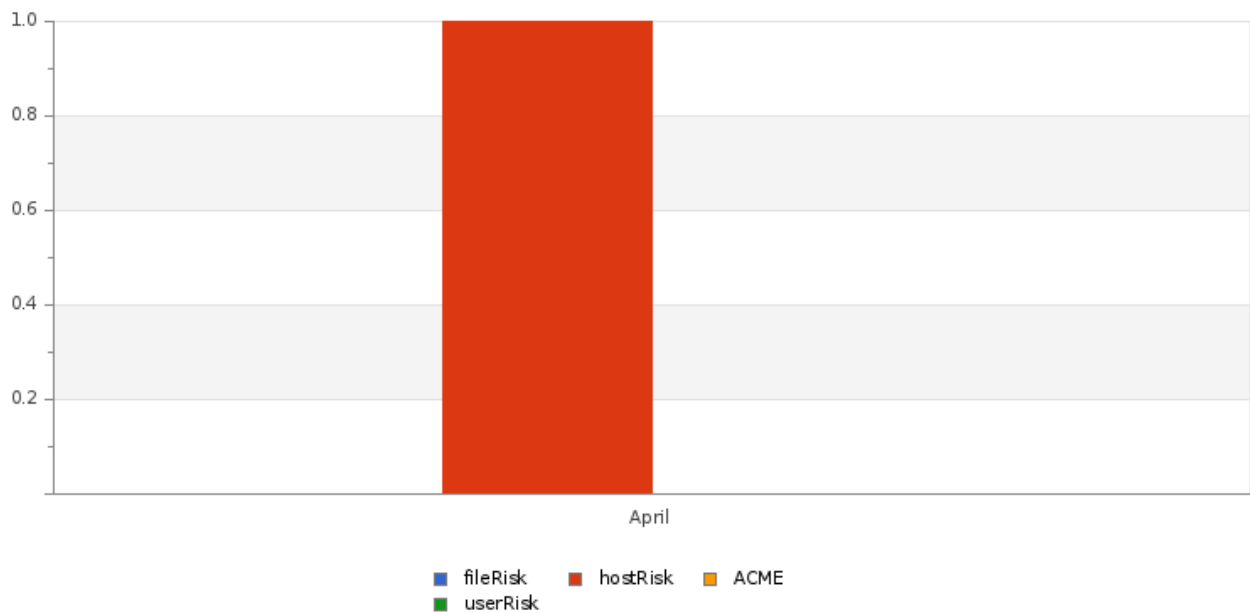
High Severity Events

Host	File Path	Severity	count
ACME	C:\Windows\Temp\026a788db9a824d4606321feb9abd4b0_APT_SCENARIO_DotNetInjectDll_64.dll	4	1
ACME	C:\Windows\Temp\3m3v3wry\3m3v3wry.dll	4	1
ACME	c:\program files\qualys\qualysagent\qualysagent.exe	4	2
ACME	c:\windows\system32\rundll32.exe	4	1
ACME	c:\windows\system32\schtasks.exe	4	2
ACME	c:\windows\system32\services.exe	4	3
ACME	c:\windows\system32\taskmgr.exe	4	173
ACME	c:\windows\system32\wbem\wmiprvse.exe	4	61
john66	c:\windows\system32\windowspowershell\v1.0\powershell.exe	4	1
USASYSTEMSWS01	c:\windows\system32\windowspowershell\v1.0\powershell.exe	4	1



MSS-EDR REPORT

ACME FINANCIAL SERVICES 05/15/2023

Events**Close alerts ***

MSS-EDR REPORT

ACME FINANCIAL SERVICES 05/15/2023

Total Hosts - User Defined

37

High Severity Events by File Path - User Defined

File Path	Severity	Event Count
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2012-1535\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2013-0634\acme-96.com	5	1
C:\metasploit-framework\embedded\framework\data\exploits\acme-96.com	5	1

High Severity Events by Host Name - User Defined

Host	Severity	Event Count
USASYSTEMSWS03	5	532
ACME	5	29
ACME	4	1584
USASYSTEMSWS03	4	143
WINDEV	4	1
doe.john	4	1
USASYSTEMSWS01	4	1

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**





GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

MSS-EDR REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

