TLP:AMBER

MSS-EDR REPORT

GLESEC

May 15, 2023

TLP AMBER
MSS-EDR REPORT

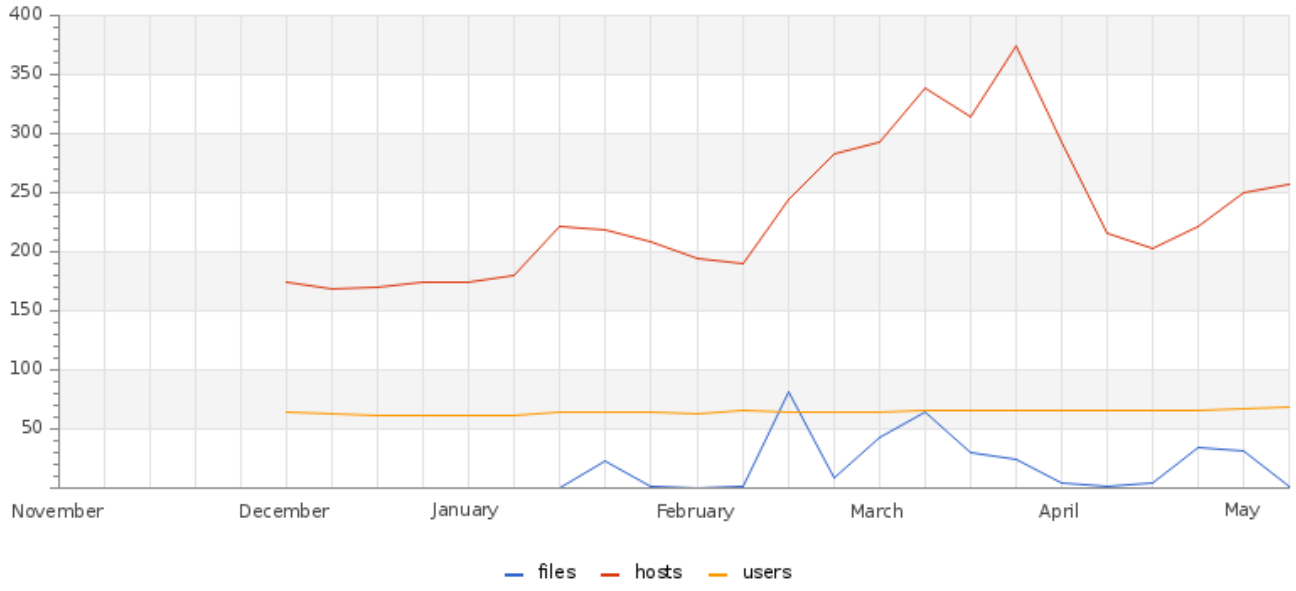
About this report

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

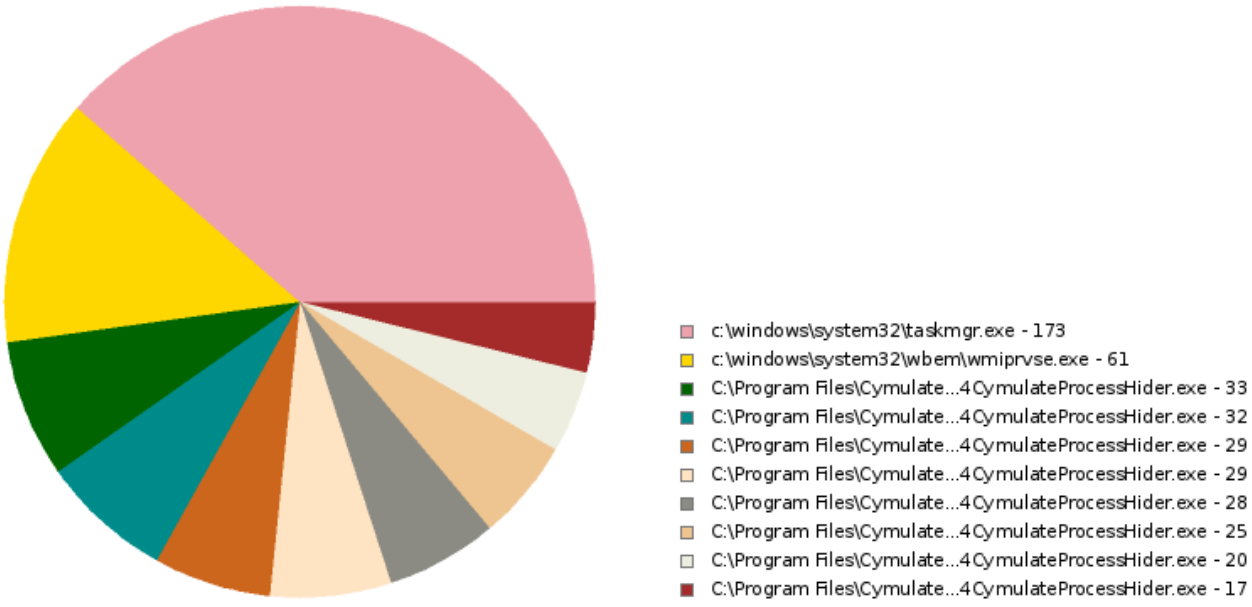


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

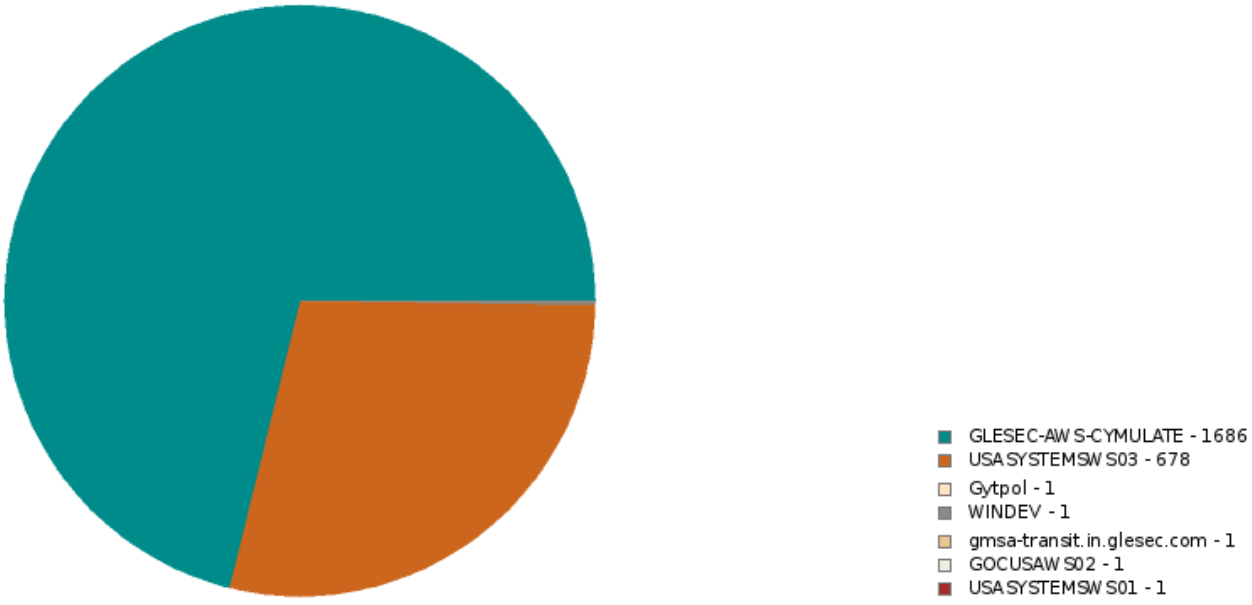
MSS-EDR REPORT

GLESEC 05/15/2023

Events by File Path - User Defined



Events by Host Name - User Defined

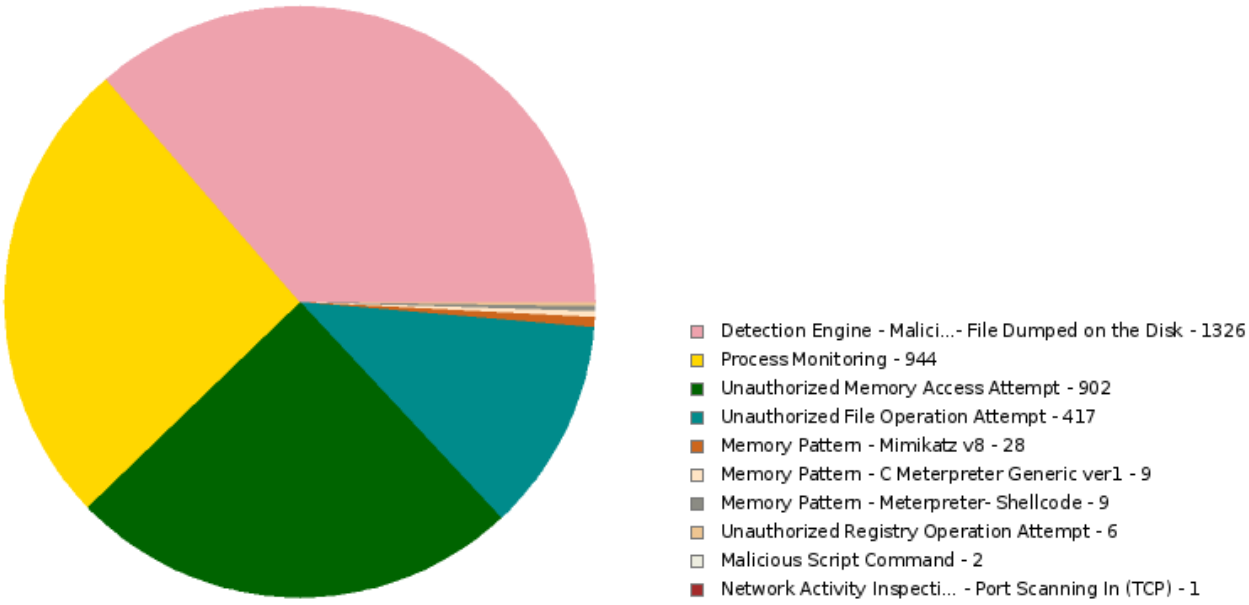


LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

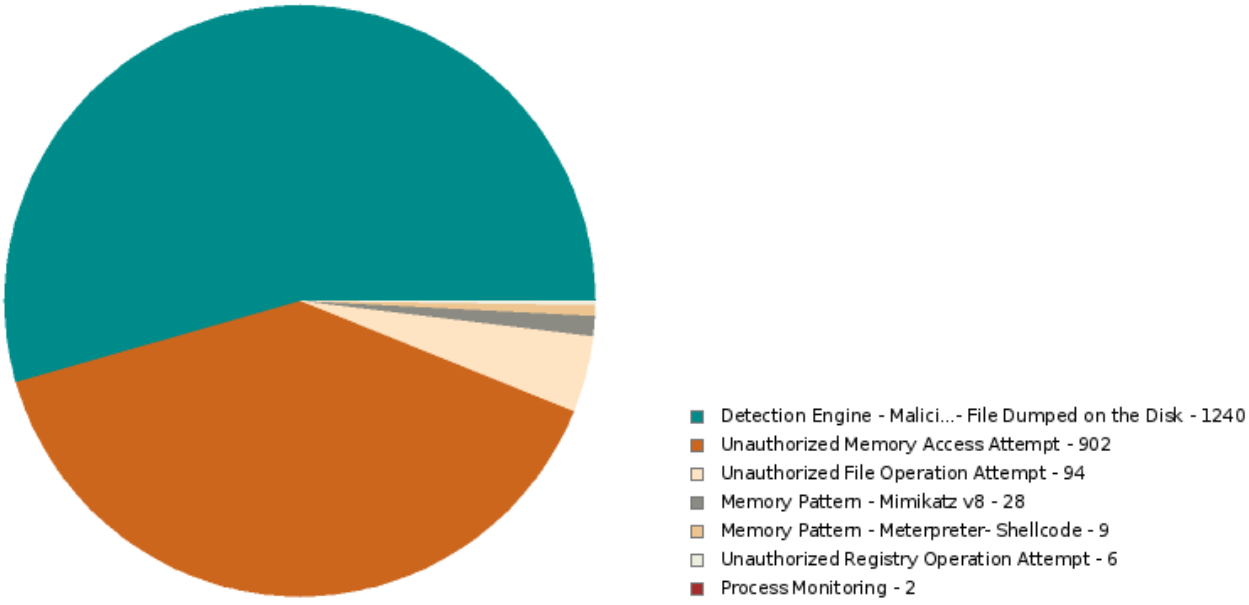
MSS-EDR REPORT

GLESEC 05/15/2023

Events by Event Name - User Defined



High Severity Events by Event Name - User Defined



LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-EDR REPORT

GLESEC 05/15/2023

Brute Force Detection by Ratio - User Defined

Host \ User Name	Ratio (Bad : Good)	Probability
veeam_server\administrator	1160 : 97	11.96
dc-01\administrator	12 : 47	0.26
dc-01\luis.montenegro	1 : 8	0.13
glesec-aws-cons\administrator	4 : 80	0.05
dc-01\jose.taipe	1 : 29	0.03
glesec-aws-cymulate\cymulate	1 : 126	0.01
dc-01\simon.weizman	1 : 720	0.00
dc-02\atala.issa	1 : 710	0.00

High Severity Events

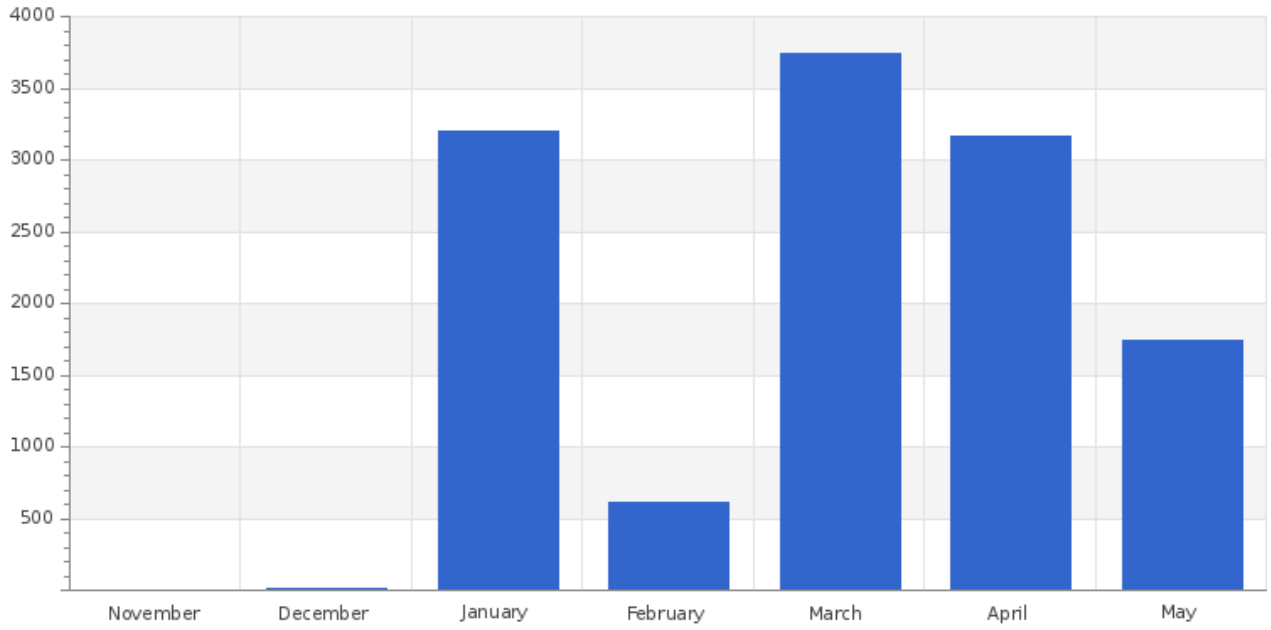
Host	File Path	Severity	count
GLESEC-AWS-CYMULATE	C:\Windows\Temp\026a788db9a824d4606321feb9abd4b0_APT_SCENARIO_DotNetInjectDll_64.dll	4	1
GLESEC-AWS-CYMULATE	C:\Windows\Temp\3m3v3wry\3m3v3wry.dll	4	1
GLESEC-AWS-CYMULATE	c:\program files\qualys\qualysagent\qualysagent.exe	4	2
GLESEC-AWS-CYMULATE	c:\windows\system32\rundll32.exe	4	1
GLESEC-AWS-CYMULATE	c:\windows\system32\schtasks.exe	4	2
GLESEC-AWS-CYMULATE	c:\windows\system32\services.exe	4	3
GLESEC-AWS-CYMULATE	c:\windows\system32\taskmgr.exe	4	173
GLESEC-AWS-CYMULATE	c:\windows\system32\wbem\wmiprvse.exe	4	61
GOCUSAWS02	c:\windows\system32\windowspowershell\v1.0\powershell.exe	4	1
USASYSTEMSWS01	c:\windows\system32\windowspowershell\v1.0\powershell.exe	4	1

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-EDR REPORT

GLESEC 05/15/2023

Events



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\CVE-2009-3867.jar	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2009-3869.jar	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2010-1297.swf	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2011-0611.swf	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2011-2110.swf	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2012-0507.jar	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2012-0779.swf	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2012-1535\Main.swf	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2013-0634\exploit.swf	5	1
C:\metasploit-framework\embedded\framework\data\exploits\CVE-2013-2171.bin	5	1

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

MSS-EDR REPORT

GLESEC 05/15/2023

High Severity Events by Host Name - User Defined

Host	Severity	Event Count
USASYSTEMSWS03	5	532
GLESEC-AWS-CYMULATE	5	28
GLESEC-AWS-CYMULATE	4	1575
USASYSTEMSWS03	4	143
WINDEV	4	1
GOCUSAWS02	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.**

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

MSS-EDR REPORT

HOW CAN WE HELP?

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

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500