# When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777

unit42.paloaltonetworks.com/vatet-pyxie-defray777/3
Ryan Tracey, Drew Schmitt

November 7, 2020

By <u>Ryan Tracey</u> and <u>Drew Schmitt</u> November 6, 2020 at 6:15 PM Category: <u>Malware</u>, <u>Ransomware</u>, <u>Unit 42</u>

Tags: <u>Defray777</u>, <u>PyXie</u>, <u>Vatet</u>



This post is also available in: 日本語 (Japanese)

# Last, but Not Least: Defray777

Defray777 is an elusive family of ransomware also known as <u>Ransom X</u> and <u>RansomExx</u>. Although it has recently been covered in the news as a new family, it has been in use since at least 2018 and is responsible for a number of high-profile ransomware incidents -- as detailed in the articles we linked to.

Defray777 runs entirely in memory, which is why there have been so few publicly discussed samples to date. In several recent incidents, Defray777 was loaded into memory and executed by Cobalt Strike, which was delivered by the Vatet loader.

During our research, we discovered multiple decryptors for this ransomware family, going back as early as 2018. Reviewing decryptors from 2018 until present shows that there has been consistency in the ransomware's encryption and decryption methodology, as well as the use of <u>Themida</u> for packing their decryptors. Table 10 shows a list of Defray777 decryptors discovered in <u>AutoFocus</u>, with a list of organizations that suffered ransomware attacks. This shows that Defray777 has been consistently active since 2018.

Date	Victim
12/7/2018	Education Organization
2/4/2019	Healthcare Organization
3/1/2019	Technology Organization
3/15/2019	Education Organization
8/8/2019	Healthcare Organization
8/25/2019	Education Organization
8/28/2019	Transportation and Logistics Organization
9/3/2019	Legal Organization

9/6/2019	Education Organization
9/26/2019	Healthcare Organization
10/30/2019	Government Organization
11/1/2019	Healthcare Organization
2/4/2020	Technology Organization
2/10/2020	Government Organization
3/16/2020	Food Organization
10/17/2020	Finance Organization

Table 10. Defray777 ransomware attacks listed by date and victim.



Defray777 decryptor.

We have examined several recent Defray777 samples, including one sample that was obtained directly from memory during a recent incident. Our in-depth analysis resulted in the findings outlined below.

## **Decrypted Strings**

The string decryption process is the same as we saw with PyXie. The following strings were decrypted from a recent Defray777 sample:

Already active [%s] +%u (%u) files done [%s] [%u KB/s] Started (PID: %u; Workers: %u; AES-%s) [%s] Complete (+%u (%u) files done) [%s] Work time: %d:%02d:%02d Unable to get computer name CryptoGuard kernel32.dll ConvertStringSecurityDescriptorToSecurityDescriptorW advapi32.dll IsWow64Process SystemDrive **KiUserExceptionDispatcher** 

Table 11. Defray777 encrypted strings.

### Prioritizing Defray777 on the Impacted System

While deep diving on a recovered Defray777 sample, we found that Defray777 exhibits the following notable characteristics regarding the prioritization of threads and processes:

- During execution, the ransomware uses SetProcessPriorityBoost to prioritize the threads of the Defray777 process.
- Defray777 additionally focuses on creating and prioritizing threads for encryption by calling SetThreadAffinityMask and SetThreadPriorityBoost.
- · Defray777 uses multithreading to improve ransomware performance.



Figure 22. Prioritization of

#### Defray777 threads during execution.

#### Killing "Undesirable" Processes

As part of the execution workflow, Defray777 creates threads that will be responsible for the killing of processes that the threat actors deem to be "undesirable." The execution continues by getting a listing of processes using CreateToolhelp32Snapshot before iterating through all active processes (with the exception of itself) and killing all "undesirable" processes. Defray777 specifically targets process that can be opened with the desired access of SYNCHRONIZE | PROCESS\_QUERY\_INFORMATION | PROCESS\_VM\_WRITE | PROCESS\_VM\_READ | PROCESS\_VM\_OPERATION | PROCESS\_CREATE\_THREAD.

Defray777 excludes all processes that contain the system file path in their full image path. Additionally, the ransomware will exclude the following processes from being killed during execution:

powershell.exe	rundll32.exe
wefault.exe	explorer.exe
vmnat.exe	

#### Table 12. Excluded processes.

#### **Stopping System Services**

During execution, Defray777 stops the following services from running:

Acronis VSS Provider	MSExchangeADTopology	MSSQLSERVER	SQLAgent\$PRACT1
AcronisAgent	MSExchangeAntispamUpdate	MSSQLServerADHelper	SQLAgent\$PROD
AcronixAgent	MSExchangeEdgeSync	MSSQLServerADHelper100	SQLAgent\$PROFXE

Antivirus     MSExchangeFBA     MySQL57     SQLAgentSSIARE       ARSM     MSExchangeFDS     MySQL80     SQLAgentSSOPHO       AVP     MSExchangeBIS     NetMempActivator     SQLAgentSSOPHO       AVP     MSExchangeMalboxAssistants     ngirx     SQLAgentSSOLEXF       BackupExecAgentAccelerator     MSExchangeMalboxReplication     ntritscan     SQLAgentSTSSE       BackupExecAgentBrowser     MSExchangeMalboxReplication     ntritscan     SQLAgentSTSFEAM       BackupExecDeviceMediaService     MSExchangeMittoReplication     ntritscan     SQLAgentSTSFEAM       BackupExecDeviceMediaService     MSExchangeProtectedServiceHost     PDVFSService     SQLAgentSVEEAM       BackupExecVSProvder     MSExchangeRPC     ReportServerSQL2008     SQLagentSVEEAM       DCAgent     MSExchangeServiceHost     ReportServerSSCL_BGC     SQLSefORService       DCAgent     MSExchangeServiceHost     ReportServerSTEM_SGC     SQLSefORSerVERAGEN       ehttp://www.ds     MSExchangeTrageTragent     sacsvr     SQLSefORENERTSE       EPSocutItyServica     MSExchangeTrageTragent     sacsvr     SQLWitter       EPSocutItyServica     MSExchangeTrag				
ARSM     MSExchangeFDS     MySOL80     SOLAgentSSOPHO       AVP     MSExchangeIS     NetMsmaActivator     SOLAgentSSOL_20       BackupExecAgentAccelerator     MSExchangeMaliboxAssistants     ngirx     SOLAgentSSOLEXF       BackupExecAgentAccelerator     MSExchangeMaliboxReplication     nitracan     SOLAgentSSYSTER       BackupExecDeviceMediaService     MSExchangeMMIX     Oracle/ServiceActe     SOLAgentSYEEA       BackupExecDeviceMediaService     MSExchangeMIXT     Oracle/ServiceActe     SOLAgentSYEEA       BackupExecNPCService     MSExchangeProtected/ServiceActe     SOLAgentSYEEA     SOLAgentSYEEA       BackupExecNPCService     MSExchangeRot     ReportServer/SSOL_2008     SOLasife Filter Service       Dockyc     MSExchangeRot     ReportServer/SSOL_2008     SOLasife Filter Service       Dockyc     MSExchangeServiceHost     ReportServer/STSAL     SOLSIsfe Filter Service       Dockyc     MSExchangeRot     ReportServer/STSAL     SOLSIsfe Filter Service       Dockyc     MSExchangeRot     ReportServer/STSAL     SOLSIsfe/ERCER       BackupExecVPC     MSExchangeRot     ReportServer/STSAL     SOLSIsfe/ERCER       Bore	AcrSch2Svc	MSExchangeES	MSSQLServerOLAPService	SQLAgent\$SBSMO
AVP     MSExchangelS     NetMsmqActivator     Sol LagentSQL_2D       BackupExecAgentAccelerator     MSExchangeMailboxReplication     ntrscan     SOLAgentSQLEXF       BackupExecDeviceMediaService     MSExchangeMailboxReplication     ntrscan     SOLAgentSYSTED       BackupExecDeviceMediaService     MSExchangeMGT     OracleClentCache80     SOLAgentSYSTED       BackupExecDeviceMediaService     MSExchangeMGT     OracleXETTNSUstencr     SOLAgentSYEEAM       BackupExecRVService     MSExchangeRPT     OracleXETTNSUstencr     SOLAgentSYEEAM       BackupExecRVService     MSExchangeRpt     POVFSService     SOLAgentSYEEAM       BackupExecRVSsProvider     MSExchangeSa     ReportServerSQL_2008     SOLasfe Fiter Service       DXsvc     MSExchangeSarch     ReportServerSTSC     SOLSERVERAGE       BackupExectifyService     MSExchangeSarch     ReportServerSTSC     SOLSERVERAGE       ekm     MSExchangeSarch     ReportServerSTSC     SOLSERVERAGE       eltps/sr     MSExchangeTransport     sacsvr     SOLViter       EPSocutifyService     MSExchangeTransport     sacsvr     SoLWiter       EPIdedeService     MSExchangeTrans		MSExchangeFBA	MySQL57	SQLAgent\$SHAREF
BackupExecAgentAccelerator     MSExchangeMallboxAssistants     nginx     SQLAgentSQLEX       BackupExecAgentBrowser     MSExchangeMallboxReplication     ntrtscan     SQLAgentSYSTEK       BackupExecAgentBrowser     MSExchangeMallboxReplication     OracleServiceXE     SQLAgentSYER       BackupExecAbengine     MSExchangeMQIT     OracleServiceXE     SQLAgentSYEEAM       BackupExecAbenginementService     MSExchangeProtectedServiceHost     PDVFSService     SQLAgentSYEEAM       BackupExecAbenginementService     MSExchangeRepl     POP3svc     SQLagentSYEEAM       BackupExecVSSProvider     MSExchangeRepl     POP3svc     SQLasfe Backup Sec       DbXsvc     MSExchangeServiceHost     ReportServerSSQL_2008     SQLasfe Filer Servi       DCAgent     MSExchangeServiceHost     ReportServerSYSTEM_BGC     SQLSafe DixServerSQL       ekm     MSExchangeSRS     ReportServerSYSTEM_BGC     SQLVitfor       EPSecurityService     MSExchangeTrinotiting     RESvc     SQLVitfor       EPSecurityService     MSExchangeTransport     Sacs     SuLVitfor       EPSpacurityService     MSExchangeTransport     Sacs     SuLVitfor       EPSpacurityServ	ARSM	MSExchangeFDS	MySQL80	SQLAgent\$SOPHO
BackupExecAgentBrowser     MSExchangeMailborReplication     ntrscan     SQLAgentSYSTEL       BackupExecDeviceMediaService     MSExchangeMGMT     OracleServiceXE     SQLAgentSYFEAM       BackupExecLobEngine     MSExchangeMGMT     OracleServiceXE     SQLAgentSYFEAM       BackupExecLobEngine     MSExchangeMTA     OracleXETNSLIteIoner     SQLAgentSYFEAM       BackupExecRPCService     MSExchangeRpl     PDVFSService     SQLAgentSYFEAM       BackupExecRPCService     MSExchangeRpl     PDVSSv     SQLagentSYFEAM       BackupExecRPCService     MSExchangeRpl     PDVSsv     SQLsafe BackupE       DbxSvc     MSExchangeSA     ReportServerSQL_2008     SQLsafe BackupE       DbxSvc     MSExchangeSartin     ReportServerSYSTEM_BGC     SQLSerVERAGEN       ekm     MSExchangeSartineS     ReportServerSYSTEM_BGC     SQLSERVERAGEN       ekm     MSExchangeTransport     sacsvr     SQLVTERVERAGEN       PEPsecurityService     MSExchangeTransportLogSearch     SamSs     SatpSvc       EraserSvc11710     msftesqtPROD     SAVAdminService     swi_envice       FA_Scheduler     MSOLAPSYSTEM_BGC     SDRSVC <td< td=""><td>AVP</td><td>MSExchangelS</td><td>NetMsmqActivator</td><td>SQLAgent\$SQL_20</td></td<>	AVP	MSExchangelS	NetMsmqActivator	SQLAgent\$SQL_20
BackupExecDeviceMediaService     MSExchangeMGMT     OracleCientCache80     SQLAgentSTPS       BackupExecJobEngine     MSExchangeMGMT     OracleServiceXE     SQLAgentSTPSAM       BackupExecMaragementService     MSExchangeMTA     OracleXETNSListener     SQLAgentSYEEAM       BackupExecMPCService     MSExchangeProtectdServiceHost     PDVFSservice     SQLAgentSYEEAM       BackupExecVSProvider     MSExchangeProt     ReportServer     SQLAgentSYEEAM       BackupExecVSProvider     MSExchangeSA     ReportServerSQL_2008     SQLsafe Filter Servi       DbXvv     MSExchangeSA     ReportServerSSQL_2008     SQLSERVERAGEN       DbXvv     MSExchangeServiceHost     ReportServerSTPS     SQLSERVERAGEN       ekrn     MSExchangeTrotting     RESvc     SQLTELEMETRY       Erlsersfvc11710     msfexchangeTransport     saccvr     SQLSERVERAGEN       Ersersfvc11710     msfesql\$PROD     SAVAdminService     swLgenter       FA_Scheduler     MSOLAP\$TPS     SepMstor     swLgenter       KAVFS     MSOLAP\$TPSAMA     SMInolitor     swLgenter       ISAdamin     MSOLAP\$TRSQL_2008     SAVService     swLgitter <td>BackupExecAgentAccelerator</td> <td>MSExchangeMailboxAssistants</td> <td>nginx</td> <td>SQLAgent\$SQLEXF</td>	BackupExecAgentAccelerator	MSExchangeMailboxAssistants	nginx	SQLAgent\$SQLEXF
BackupExecJobEngine     MSExchangeMGMT     OracleServiceXE     SQLAgentSTPSAM       BackupExecManagementService     MSExchangePTotectedServiceHost     PDVFSService     SQLAgentSVEEAM       BackupExecVSSProvider     MSExchangeRpI     PDPSSvc     SQLagentSVEEAM       BackupExecVSSProvider     MSExchangeRpI     PDPSSvc     SQLaste Backup Exe       bedg     MSExchangeRPC     ReportServer     SQLaste Backup Exe       DbxSvc     MSExchangeSearch     ReportServerSSVSTEM_BGC     SQLSERVERAGEN       ekm     MSExchangeServiceHost     ReportServerSTPS     SQLSERVERAGEN       ekm     MSExchangeServiceHost     ReportServerSTPS     SQLSERVERAGEN       ekm     MSExchangeStrangeTransport     sacsvr     SQLWriter       EPDecurityService     MSExchangeTransport     sacsvr     SQLWriter       EPUpdateService     MSExchangeTransport     sacsvr     SQLWriter       ESAASTV     MSOLAPSSQL_2008     SAVService     swi_filter       ESAASTV     MSOLAPSSYSTEM_BGC     SDRSVC     swi_gervice       FA_Scheduler     MSOLAPSTSAMA     ShMonitor     swi_gervice       FA_Sched	BackupExecAgentBrowser	MSExchangeMailboxReplication	ntrtscan	SQLAgent\$SYSTEN
BackupExecManagementService     MSExchangeMTA     OracleXETNSListener     SQLAgent\$VEEAM       BackupExecRPCService     MSExchangeProtectedServiceHost     PDVFSService     SQLAgent\$VEEAM       BackupExecVSSProvider     MSExchangeRpl     POP3Svc     SQLagent\$VEEAM       BackupExecVSSProvider     MSExchangeRPC     ReportServer\$SQL_2008     SQLaste Backup Se       DbXsvc     MSExchangeSearch     ReportServer\$SQL_2008     SQLSterVERAGEN       DCAgent     MSExchangeServiceHost     ReportServer\$SYSTEM_BGC     SQLSterVERAGEN       ekm     MSExchangeServiceHost     ReportServer\$TPSAMA     SQLTELEMETRY       Enterprise Client Service     MSExchangeTransport     sacsvr     SQLWriter       EPSecurityService     MSExchangeTransport     sacsvr     SQLWriter       EPUpdateService     MSExchangeTransportLogSearch     SamSs     SstpSvc       EraserSvc11710     mstegt\$PROD     SAVAdminService     swi_gende       BASdMernel     MSOLAP\$STPS     SpeMastrService     swi_gende       FA_Scheduler     MSOLAP\$STPS     SpeMastrService     swi_gende       IISAdmin     MSOLAP\$STPSAMA     ShMonitor	BackupExecDeviceMediaService	MSExchangeMailSubmission	OracleClientCache80	SQLAgent\$TPS
BackupExecRPCService     MSExchangeProtectedServiceHost     PDVFSService     SQL4gent\$VEEAM       BackupExecVSSProvider     MSExchangeRp1     POP3Svc     SQL4are       bedbg     MSExchangeRp2     ReportServer     SQL5are       bedbg     MSExchangeSA     ReportServerSQL_2008     SQL5are       DXSvc     MSExchangeSarch     ReportServerSYSTEM_BGC     SQL5areEnterServer       DCAgent     MSExchangeServiceHost     ReportServerSTPS     SQL5areEnterTY       ekm     MSExchangeSRS     ReportServerSTPSAMA     SQLTELEMETRY       Enterprise Client Service     MSExchangeTransport     sacsvr     SQLWriter       EPSecurityService     MSExchangeTransport     sacsvr     SQLWriter       EsgShKernel     MSOLAPSSQL_2008     SAVService     swi_filter       ESHASRV     MSOLAPSTPS     SepMasterService     swi_update       IISAdmin     MSOLAPSTPSAMA     ShMonitor     swi_update_64       IMAP4Svc     MSSQL\$PRACTICEMGT     SmrSPsvc     TrucKeyScheduler       MAXFSGT     MSSQL\$PRACTICEMGT     SmrSPsvc     TrucKeyScheduler       MAXFSGT     MSSQL\$PRACTICEM	BackupExecJobEngine	MSExchangeMGMT	OracleServiceXE	SQLAgent\$TPSAM/
BackupExecVSSProvider     MSExchangeRepl     POP3Svc     SQLBrowser       bedbg     MSExchangeRPC     ReportServer     SQLsafe Backup Se       DbxSvc     MSExchangeSA     ReportServer/SSQL_2008     SQLsafe Filter Servi       DCAgent     MSExchangeSearch     ReportServer/SSYSTEM_BGC     SQLSafeOLRService       EhttpSrv     MSExchangeServiceHost     ReportServer/STPS     SQLSERVERAGEN       ekm     MSExchangeStrise     ReportServer/STPS     SQLVERVERAGEN       ekm     MSExchangeThrottling     RESvc     SQLWriter       EPSecurityService     MSExchangeTransport     sacsvr     SQLWriter       EPUdateService     MSExchangeTransportLogSearch     SamSs     SstpSvc       EraserSvc11710     msfteagl\$PROD     SAVAdminService     swi_service       ESHASRV     MSOLAPSTPS     SepMasterService     swi_update       IISAdmin     MSOLAPSTPSAMA     ShMonitor     swi_update       IISAdmin     MSOLAPSTPSAMA     ShMonitor     swi_update       IISAdmin     MSOLAPSTPSAMA     ShMonitor     swi_update       IISAdmin     MSSQL\$EVDEXC     Smch	BackupExecManagementService	MSExchangeMTA	OracleXETNSListener	SQLAgent\$VEEAM
beddgMSExchangeRPCReportServerSQLsafe Backup SeDbxSvcMSExchangeSAReportServer\$SQL_2008SQLsafe Filter ServiDCAgentMSExchangeSearchReportServer\$SYSTEM_BGCSQLSafeOLRServicEhttpSrvMSExchangeServiceHostReportServer\$TPSSQLSERVERAGENekmMSExchangeSRSReportServer\$TPSAMASQLTELEMETRYEnterprise Client ServiceMSExchangeTrrottlingRESvcSQLTELEMETRYSEEPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportSamSsSstpSvcEraserSvc11710msftesql\$PRODSAVAdminServicesvcGenericHostEsgShKernelMSOLAP\$SQL_2008SAVServiceswi_liiterESHASRVMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSOLSBKUPEXECSmcinstSymantec System RKAVFSMSSOLSPRACTICEMGTSMCTrucKeyKAVFSGTMSSOLSPROFXENGAGEMENTSophos AgentTrucKeyServiceHelpmaxevMSSOLSPROFXENGAGEMENTSophos AgentTrucKeyServiceHelpmaxevMSSOLSPROFXENGAGEMENTSophos AgentTrucKeyServiceCreckMBEndpointAgentMSSOLSSOHASSophos Device Control ServiceVeeamBackupSvcMcAfeeErganeworkMSSOLSSOHASCSophos NGS AgentVeeamBackupSvcMcAfeeFrameworkMSSOLSSOLEXPRESSSophos NGS AgentVeeamBackupSvcMcAfeeFrameworkMSSOLSSOLEXPRESSSophos NGS Agent<	BackupExecRPCService	MSExchangeProtectedServiceHost	PDVFSService	SQLAgent\$VEEAM
DbxSvcMSExchangeSAReportServer\$SQL_2008SQLsafe Filter ServiDCAgentMSExchangeSearchReportServer\$SYSTEM_BGCSQLSafeOLRServicEhttpSvvMSExchangeServiceHostReportServer\$TPSSQLSERVERAGENekmMSExchangeSRSReportServer\$TPSAMASQLTELEMETRYEnterprise Client ServiceMSExchangeThrottlingRESvcSQLWriterEPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportLogSearchSamSsSstpSvcEraserSvc11710msftesql\$PRODSAVAdminServicesvcGenericHostEgShKernelMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$SYSTEM_BGCSDRSVCswi_updateIISAdminMSOLAP\$TPSSepMasterServiceswi_updateIKAVFSMSSQLSBKUPEXECSmcIstSymantec System RKAVFSMSSQLSPRACTICEBGCSNACTrueKeykavfslpMSSQLSPRACTICEBGCSNACTrueKeyServiceHeltmacroxMSSQLSPROFXENGAGEMENTSophos AgentTrueKeyServiceHeltmacroxMSSQLSPROFXENGAGEMENTSophos Actoulpdate ServiceVeeamBackupSvcMBAMServiceMSSQLSSPACTICEMGTSophos Clean ServiceVeeamBackupSvcMBEndpointAgentMSSQLSSPACTICEMGESophos Natoulpdate ServiceVeeamBackupSvcMACfeeErianeworkMSSQLSSQLZ008Sophos Natoulpdate ServiceVeeamBackupSvcMACfeeFrameworkMSSQLSSPACTICEMGESophos Natoulpdate ServiceVeeamBackupSvcMACfeeFrameworkMcAfeeFramewor	BackupExecVSSProvider	MSExchangeRepl	POP3Svc	SQLBrowser
DCAgentMSExchangeSearchReportServer\$SYSTEM_BGCSQLSafeOLRServicEhttpSrvMSExchangeServiceHostReportServer\$TPSSQLSERVERAGENekmMSExchangeSRSReportServer\$TPSAMASQLTELEMETRYEnterprise Client ServiceMSExchangeThrottlingRESvcSQLWriterEPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportSamSsSstpSvcEraserSvc11710msftesql\$PRODSAVAdminServiceswcGenericHostEgShKernelMSOLAP\$SQL_2008SAVServiceswil_filterESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswil_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswil_updateIISAdminMSOLAP\$TPSAMAShMonitorswil_update_64IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEMGTSophos AgentTrueKeySchedulermaxocMSSQL\$PROFXENGAGEMENTSophos AutoUpdate ServiceVeeamBackup Cat ServiceMBAMServiceMSSQL\$SDHOSSophos AutoUpdate ServiceVeeamBackup Cat ServiceMBEndpointAgentMSSQL\$SQL_2008Sophos Pevice Control ServiceVeeamBackup Cat ServiceMEEndpointAgentMSSQL\$SQL_2008Sophos Pevice Control ServiceVeeamBackup Cat ServiceMEEndpointAgentMSSQL\$SQL_2008Sophos MALOUpdate ServiceVeeamBackup Svc <t< td=""><td>bedbg</td><td>MSExchangeRPC</td><td>ReportServer</td><td>SQLsafe Backup Se</td></t<>	bedbg	MSExchangeRPC	ReportServer	SQLsafe Backup Se
EhttpSrvMSExchangeServiceHostReportServer\$TPSSQLSERVERAGENekmMSExchangeSRSReportServer\$TPSAMASQLTELEMETRYEnterprise Client ServiceMSExchangeTrinsportsacsvrSQLWriterEPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportLogSearchSamSsSstpSvcEraserSvc11710msftesql\$PRODSAVAdminServicesvcGenericHostEggShKernelMSOLAP\$SQL_2008SAVServiceswi_serviceFA_SchedulerMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcisetSymantec System RKAVFSMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTTICEMGTSMPSvctmlistenkavfsslpMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SDHOSSophos Clean ServiceVeeamBackupCxteMEEndpointAgentMSSQL\$SDHOSSophos Price Control ServiceVeeamBackupCxteMcAfeeErameworkMSSQL\$SYETEM_BGCSophos MCS AgentVeeamCadagsvcMcAfeeFrameworkMSSQL\$YFEM_BGCSophos MCS AgentVeeamCadagsvcMcAfeeFrameworkMSSQL\$YFEM_BGCSophos MCS AgentVeeamCadagsvcMcAfeeFrameworkMSSQL\$YFEM_BGCSophos MCS AgentVeeamCadagsvc </td <td>DbxSvc</td> <td>MSExchangeSA</td> <td>ReportServer\$SQL_2008</td> <td>SQLsafe Filter Servi</td>	DbxSvc	MSExchangeSA	ReportServer\$SQL_2008	SQLsafe Filter Servi
ekmMSExchangeSRSReportServer\$TPSAMASQLTELEMETRYEnterprise Client ServiceMSExchangeTransportsacsvrSQLTELEMETRYSEEPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportLogSearchSamSsSstpSvcEraserSvc1710msftesql\$PRODSAVAdminServicesvcGenericHostEggShKernelMSOLAP\$SQL_2008SAVServiceswi_filterESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$ERVDE2SmcServiceTmCCSFKAVFSMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEBGCSNACTrueKeyklaagentMSSQL\$PROPXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SHAREPOINTSophos AgentTrueKeyServiceHelpMBAMServiceMSSQL\$SOPHOSSophos AlutoUpdate ServiceVeeamBackup CatzMBEndpointAgentMSSQL\$SOPHOSSophos Clean ServiceVeeamBackup CatzMAfeeErjanesworkMSSQL\$SYSTEM_BGCSophos MicS AgentVeeamBackup SvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MicS AgentVeeamCloudSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MicS AgentVeeamCloudSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MicS AgentVeeamCloudSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MicS AgentVeeamDeploy	DCAgent	MSExchangeSearch	ReportServer\$SYSTEM_BGC	SQLSafeOLRServic
Enterprise Client ServiceMSExchangeThrottlingRESvcSQLTELEMETRYSEEPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportLogSearchSamSsSstpSvcEraserSvc11710msttesql\$PRODSAVAdminServicesvcGenericHostEsgShKernelMSOLAP\$SQL_2008SAVServiceswi_filterEShASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRODSntpServiceTrueKeykinagentMSSQL\$PRODSntpServiceUl0DetectMBAMServiceMSSQL\$SEMONITORINGSophos AutoUpdate ServiceVeeam Backup Cat ServiceMBEndpointAgentMSSQL\$SOPHOSSophos File Scanner ServiceVeeamBackup Svc McAfeeFrameworkMSSQL\$STSTEM_BGCSophos MCS AgentVeeamBackupSvc McAfeeFrameworkVeeamCatalogSvcMcAfeeFrameworkMSSQL\$STEM_BGCSophos MCS AgentVeeamBackupSvcMcAfeeFrameworkMSSQL\$STEM_BGCSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMSSQL\$STEM_BGCSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMSSQL\$STEM_BGCSophos MCS AgentVeeamDeployment	EhttpSrv	MSExchangeServiceHost	ReportServer\$TPS	SQLSERVERAGEN
EPSecurityServiceMSExchangeTransportsacsvrSQLWriterEPUpdateServiceMSExchangeTransportLogSearchSamSsSstpSvcEraserSvc11710msftesql\$PRODSAVAdminServicesvcGenericHostEsgShKernelMSOLAP\$SQL_2008SAVServiceswi_filterESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_update_64IISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcServiceTmCCSFKAVFSMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEMGTSMCSTrueKeykinagentMSSQL\$PROFSophos AgentTrueKeySchedulermasvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SARACTIOINGSophos Device Control ServiceVeeam Backup CatzMBEndpointAgentMSSQL\$SOPHOSSophos Device Control ServiceVeeamBackup CatzMAfeeErgineServiceMSSQL\$SOL\$SAL\$PROFXENGAGEMENTSophos Device Control ServiceVeeamBackup CatzMBEndpointAgentMSSQL\$SOPHOSSophos Sophos File Scanner ServiceVeeamBackup SvcMcAfeeErgineServiceMSSQL\$SOL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS ClientVeeamDeployment	ekrn	MSExchangeSRS	ReportServer\$TPSAMA	SQLTELEMETRY
EPUpdateServiceMSExchangeTransportLogSearchSamSsSstpSvcEraserSvc11710msftesql\$PRODSAVAdminServicesvcGenericHostEsgShKernelMSOLAP\$SQL_2008SAVServiceswi_filterESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSSepMasterServiceswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEBGCSNACTrueKeyknagentMSSQL\$PROPSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeamBackupSvcMEEndpointAgentMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBackupSvcMcAfeeErrameworkMcAfeeFrameworkMSSQL\$SYTEM_BGCSophos Metalth ServiceVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYTEM_BGCSophos MCS ClientVeeamDeployment	Enterprise Client Service	MSExchangeThrottling	RESvc	SQLTELEMETRY\$E
EraserSvc11710msftesql\$PRODSAVAdminServicesvcGenericHostEsgShKernelMSOLAP\$SQL_2008SAVServiceswi_filterESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSSepMasterServiceswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEBGCSNACTrueKeyklaagentMSSQL\$PRODSntpServiceTrueKeySchedulermaxvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpMBAMServiceMSSQL\$SPROFYENGAGEMENTSophos Clean ServiceVeeam BackupSvcMBEndpointAgentMSSQL\$SOPHOSSophos File Scanner ServiceVeeamBackupSvcMcAfeeErameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS ClientVeeamDeployment	EPSecurityService	MSExchangeTransport	sacsvr	SQLWriter
EsgShKernelMSOLAP\$SQL_2008SAVServiceswi_filterESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$BKUPEXECSmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrucKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AutoUpdate ServiceUl0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup CateMBEndpointAgentMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBackupSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCatalogSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeployment	EPUpdateService	MSExchangeTransportLogSearch	SamSs	SstpSvc
ESHASRVMSOLAP\$SYSTEM_BGCSDRSVCswi_serviceFA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermaxvcMSSQL\$PROFXENGAGEMENTSophos AutoUpdate ServiceUIODetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cate ServiceMBEndpointAgentMSSQL\$SQLEXPRESSSophos File Scanner ServiceVeeamBackupSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$YSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$YSTEM_BGCSophos MCS ClientVeeamCloudSvc	EraserSvc11710	msftesql\$PROD	SAVAdminService	svcGenericHost
FA_SchedulerMSOLAP\$TPSSepMasterServiceswi_updateIISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SBSMONITORINGSophos Clean ServiceUl0DetectMBAMServiceMSSQL\$SOPHOSSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBackupSvcMcAfeeErameworkMSSQL\$SQL\$SQLEXPRESSSophos MCS AgentVeeamClaudSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamClaudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeployments	EsgShKernel	MSOLAP\$SQL_2008	SAVService	swi_filter
IISAdminMSOLAP\$TPSAMAShMonitorswi_update_64IIAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SALPPOSSophos Device Control ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBackupSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS ClientVeeamDeployments	ESHASRV	MSOLAP\$SYSTEM_BGC	SDRSVC	swi_service
IMAP4SvcMSSQL\$BKUPEXECSmcinstSymantec System RKAVFSMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUl0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SQL\$Q08Sophos File Scanner ServiceVeeamBackupSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeployments	FA_Scheduler	MSOLAP\$TPS	SepMasterService	swi_update
KAVFSMSSQL\$ECWDB2SmcServiceTmCCSFKAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelrmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBrokerSvcMcAfeeErameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCatalogSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	IISAdmin	MSOLAP\$TPSAMA	ShMonitor	swi_update_64
KAVFSGTMSSQL\$PRACTICEMGTSMTPSvctmlistenkavfsslpMSSQL\$PRACTTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelrmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SQL2008Sophos File Scanner ServiceVeeamBackupSvcMcAfeeErameworkMSSQL\$SQL2008Sophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	IMAP4Svc	MSSQL\$BKUPEXEC	Smcinst	Symantec System R
kavfsslpMSSQL\$PRACTTICEBGCSNACTrueKeyklnagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SOPHOSSophos Device Control ServiceVeeamBackupSvcMcAfeeErameworkMSSQL\$SQL£XPRESSSophos Health ServiceVeeamCatalogSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS ClientVeeamDeploymentS	KAVFS	MSSQL\$ECWDB2	SmcService	TmCCSF
kInagentMSSQL\$PRODSntpServiceTrueKeySchedulermacmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelrmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SOPHOSSophos Pevice Control ServiceVeeamBackupSvcMcAfeeEngineServiceMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBrokerSvcMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	KAVFSGT	MSSQL\$PRACTICEMGT	SMTPSvc	tmlisten
macmnsvcMSSQL\$PROFXENGAGEMENTSophos AgentTrueKeyServiceHelpmasvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SOPHOSSophos Device Control ServiceVeeamBackupSvcMcAfeeEngineServiceMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBrokerSvcMcAfeeFrameworkMSSQL\$SQLEXPRESSSophos MCS AgentVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	kavfsslp	MSSQL\$PRACTTICEBGC	SNAC	TrueKey
masvcMSSQL\$SBSMONITORINGSophos AutoUpdate ServiceUI0DetectMBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SOPHOSSophos Device Control ServiceVeeamBackupSvcMcAfeeEngineServiceMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBrokerSvcMcAfeeFrameworkMSSQL\$SQLEXPRESSSophos Health ServiceVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	kinagent	MSSQL\$PROD	SntpService	TrueKeyScheduler
MBAMServiceMSSQL\$SHAREPOINTSophos Clean ServiceVeeam Backup Cata ServiceMBEndpointAgentMSSQL\$SOPHOSSophos Device Control ServiceVeeamBackupSvcMcAfeeEngineServiceMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBrokerSvcMcAfeeFrameworkMSSQL\$SQLEXPRESSSophos Health ServiceVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	macmnsvc	MSSQL\$PROFXENGAGEMENT	Sophos Agent	TrueKeyServiceHelr
ServiceMBEndpointAgentMSSQL\$SOPHOSSophos Device Control ServiceVeeamBackupSvcMcAfeeEngineServiceMSSQL\$SQL_2008Sophos File Scanner ServiceVeeamBrokerSvcMcAfeeFrameworkMSSQL\$SQLEXPRESSSophos Health ServiceVeeamCatalogSvcMcAfeeFrameworkMcAfeeFrameworkMSSQL\$SYSTEM_BGCSophos MCS AgentVeeamCloudSvcMcShieldMSSQL\$TPSSophos MCS ClientVeeamDeploymentS	masvc	MSSQL\$SBSMONITORING	Sophos AutoUpdate Service	UI0Detect
McAfeeEngineService   MSSQL\$SQL_2008   Sophos File Scanner Service   VeeamBrokerSvc     McAfeeFramework   MSSQL\$SQLEXPRESS   Sophos Health Service   VeeamCatalogSvc     McAfeeFrameworkMcAfeeFramework   MSSQL\$SYSTEM_BGC   Sophos MCS Agent   VeeamCloudSvc     McShield   MSSQL\$TPS   Sophos MCS Client   VeeamDeploymentS	MBAMService	MSSQL\$SHAREPOINT	Sophos Clean Service	
McAfeeFramework   MSSQL\$SQLEXPRESS   Sophos Health Service   VeeamCatalogSvc     McAfeeFrameworkMcAfeeFramework   MSSQL\$SYSTEM_BGC   Sophos MCS Agent   VeeamCloudSvc     McShield   MSSQL\$TPS   Sophos MCS Client   VeeamDeploymentS	MBEndpointAgent	MSSQL\$SOPHOS	Sophos Device Control Service	VeeamBackupSvc
McAfeeFrameworkMcAfeeFramework   MSSQL\$SYSTEM_BGC   Sophos MCS Agent   VeeamCloudSvc     McShield   MSSQL\$TPS   Sophos MCS Client   VeeamDeploymentS	McAfeeEngineService	MSSQL\$SQL_2008	Sophos File Scanner Service	VeeamBrokerSvc
McShield MSSQL\$TPS Sophos MCS Client VeeamDeploymentS	McAfeeFramework	MSSQL\$SQLEXPRESS	Sophos Health Service	VeeamCatalogSvc
	McAfeeFrameworkMcAfeeFramework	MSSQL\$SYSTEM_BGC	Sophos MCS Agent	VeeamCloudSvc
McTaskManagar MSSOL ©TDSAMA Sanhas Magagas Bautar VacamDanlauSua	McShield	MSSQL\$TPS	Sophos MCS Client	VeeamDeploymentS
INICIASKINIANAYCI INICOQLATICANIA OUPIUS INIESSAGE KUULEI VEEAMDEPIUSSVC	McTaskManager	MSSQL\$TPSAMA	Sophos Message Router	VeeamDeploySvc
mfefire MSSQL\$VEEAMSQL2008R2 Sophos Safestore Service VeeamEnterpriseMa	mfefire	MSSQL\$VEEAMSQL2008R2	Sophos Safestore Service	VeeamEnterpriseMa

mfemms	MSSQL\$VEEAMSQL2012	Sophos System Protection Service	VeeamHvIntegration
mfevtp	MSSQLFDLauncher	Sophos Web Control Service	VeeamMountSvc
MMS	MSSQLFDLauncher\$PROFXENGAGEMENT	sophossps	VeeamNFSSvc
MongoDB	MSSQLFDLauncher\$SBSMONITORING	SQL Backups	VeeamRESTSvc
mozyprobackup	MSSQLFDLauncher\$SHAREPOINT	SQLAgent\$BKUPEXEC	VeeamTransportSvc
MsDtsServer	MSSQLFDLauncher\$SQL_2008	SQLAgent\$CITRIX_METAFRAME	W3Svc
MsDtsServer100	MSSQLFDLauncher\$SYSTEM_BGC	SQLAgent\$CXDB	wbengine
MsDtsServer110	MSSQLFDLauncher\$TPS	SQLAgent\$ECWDB2	WRSVC
MSExchangeAB	MSSQLFDLauncher\$TPSAMA	SQLAgent\$PRACTTICEBGC	Zoolz 2 Service

## Table 13. Services stopped by Defray777.

## File Encryption

Based on a recent Defray777 sample recovered from memory, the ransomware will get a listing of all logical drives on the system using a call to GetLogicalDriveStringsW before iterating through each drive to encrypt files using the following process:

 To begin, Defray777 checks for whether the processor feature PF\_XMMI64\_INSTRUCTIONS\_AVAILABLE is present on the impacted system.

If enabled, Defray777 knows that SSE2 is supported and more complex mathematical operations are possible.

- Defray777 will also determine if the processor is capable of using AES-NI for improved encryption performance.
- As encryption begins, a ransom note will be created in each directory where files will be encrypted.
  - The name of the ransom note will vary. However, from our research, the ransom notes most commonly contain a combination of exclamation points, the string "README," and a reference to the victim name.
  - o Example: !!!\_IMPACTED\_Client\_README\_!!!.txt
- The file contents will be encrypted using an on-the-fly generated AES key that gets encrypted with RSA-4096 and stored in the file footer in a 512-byte block.
- The encrypted file will be renamed by appending an extension that consists of a unique victim identifier and a randomized eight-digit hexadecimal number.

Example: .v1ct1m-1bc461ac

## Hello <Redacted> (NASDAQ: <Redacted>) !!!

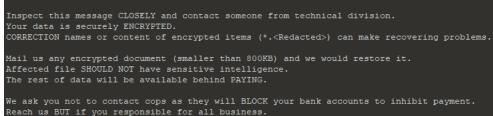


Figure 23. Recent example of a

## <Redacted>@protonmail.com Defray777 ransom note.

Specifically, the encryption mechanism consists of the following steps:

- Dynamically generate a 32-byte AES key.
- Encrypt the file with AES-256 in ECB mode using 16-byte blocks.
- Encrypt the AES key with RSA-4096 and append the 0x200 byte cipher text to the end of the encrypted file.

## **Encryption Exclusions**

During the encryption process, Defray777 aims to encrypt as many files as possible without impacting the system's core functionality. To accomplish this, Defray777 uses a set of excluded folders, files and file extensions that will not be encrypted during execution.

Excluded Folders:

\windows\system32\	\windows\syswow64\	\windows\system\
\windows\winsxs\	\appdata\roaming\	\appdata\local\
\appdata\locallow\	\all users\microsoft\	\inetpub\logs\

:\boot\	:\perflogs\	:\programdata\
:\drivers\	:\wsus\	:\efstmpwp\
:\\$recycle.bin\	:\EFSTMPWP\	crypt_detect
cryptolocker	ransomware	

Table 14. Folders excluded from encryption by Defray777.

Excluded files:

iconcache.db	thumbs.db	ransomware	ransom
debug.txt	boot.ini	desktop.ini	autorun.inf
ntuser.dat	ntldr	ntdetect.com	bootfont.bin
h + + h - h			

bootsect.bak

Table 15. Files excluded from encryption by Defray777.

It is also important to note that Defray777 adds the name of the ransom note into the excluded files list.

Excluded extensions:

.ani	.cab	.cpl	.cur	.diagcab
.diagpkg	.dll	.drv	.hlp	.icl
.icns	.ico	.iso	.ics	.lnk
.idx	.mod	.mpa	.msc	.msp
.msstyles	.msu	.nomedia	.0CX	.prf
.rtp	.scr	.shs	.spl	.sys
.theme	.themepack	.exe	.bat	.cmd

Table 16. Extensions excluded from encryption by Defray777.

# Searching for Unmapped File Shares

During execution, Defray777 uses WNetOpenEnumW and WNetEnumResourceW to search for file shares that may contain files that could be encrypted. This tactic has been seen amongst other ransomware variants in the wild to encrypt files that are accessible via unmapped file shares.



#### Anti-Forensic Measures

After all files are encrypted on the system, Defray777, like many other ransomware variants, implements common anti-forensics measures to remove as much evidence of the intrusion as possible and make it extremely difficult for the system to be recovered without a backup. Although these commands are common amongst other ransomware variants, Defray777 runs commands post-encryption, which means that when security tools alert or take action against Defray777, the files have already been encrypted.

Commands executed by Defray777:

cipher.exe /w:[DRIVE] fsutil.exe usn deletejournal /D [DRIVE] wbadmin.exe delete catalog -quiet bcdedit.exe /set {default} recoveryenabled no bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures schtasks.exe /Change /TN "\Microsoft\Windows\SystemRestore\SR" /disable wevtutil.exe cl Application wevtutil.exe cl System wevtutil.exe cl Setup wevtutil.exe cl Security wevtutil.exe sl Security /e:false

Table 17. Anti-forensic commands executed by Defray777.

Registry keys modified:

\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableConfig \Software\Microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR

\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableSR

\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore\DisableConfig

Table 18. Registry Keys Modified by Defray777.

#### Defray777's Port to Linux

During the course of our research, we found that Defray777 ransomware has been ported over to Linux. Before Defray777, ransomware that impacted both Windows and Linux operating systems was limited to being written in Java or scripting languages such as Python. These ransomware variants would be considered cross-functional since they were written in a single language that must be installed and supported by both operating systems. Defray777's port to Linux ensures that the ransomware has standalone executables for each platform with no external dependencies.

A ZIP archive was uploaded to a public malware repository on Oct. 17, 2020 that contained a Windows executable that was identified as a Defray777 decryptor. Additionally included in this ZIP archive was an ELF binary named decryptor64. Analysis of this binary determined it to be another Defray777 decryptor that had been ported to Linux.

Armed with the idea that there may be Linux versions of Defray777 in the wild, we began hunting in AutoFocus and quickly uncovered an ELF version of the ransomware encryptor.

Reviewing this sample further indicated that it was uploaded in August 2020. As of early October 2020, there appear to be zero detections by antivirus (AV) in VirusTotal for the Linux version of Defray777.

A deeper review of the Linux and Windows variants of Defray777 determined that the encryption and decryption processes used were nearly identical. In fact, by generating our own RSA key pair and modifying the binaries, we were able to confirm that the encryptors and decryptors for both operating systems were interchangeable.

Unlike the Windows versions, the developers didn't seem to put any effort into protecting the Linux samples. To our surprise, the binaries we analyzed still had their symbols intact, which made reversing them quite a bit easier.

Function name	Segment	Start
🗲 main	.text	000000000003454
🗲 GeneratePreData	.text	0000000000034E4
🗲 CryptOneBlock	.text	00000000003785
🗲 fsize	.text	0000000000037F1
🗲 CryptOneFile	.text	00000000000382F
🗲 GetMinimumBlockLength	.text	000000000003AFC
🗲 GetMaximumBlockLength	.text	000000000003B59
🗲 GetLogicByDataSize	.text	000000000003BB6
🗲 GetBlocksCountByDataSize	.text	00000000003C37
F ProcessFileHandleWithLogic	.text	000000000003C6B
🗲 encrypt_worker	.text	00000000003E2A
🗲 path_append	.text	00000000003F5E
🗲 add_task_to_worker	.text	000000000003FCF
🗲 wait_all_workers	.text	000000000004052
🗲 list_dir	.text	0000000000040B9
🗲 init_workers	.text	000000000004217
🗲 EnumFiles	.text	00000000004348
🗲 ReadMeStoreForDir	.text	0000000000043C6
F ReadMeRemoveForDir	.text	000000000004512

Figure 25. Named functions listing from ELF version of

Defray777.

One of the biggest differences between the Windows and Linux variants is the logic that determines which files to encrypt. The Windows version will recurse the file system and encrypt anything that isn't explicitly excluded. In contrast, the Linux variant will only encrypt directories specified in a command line argument.

Continue reading: Linking Vatet, PyXie and Defray777

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.