McAfee Labs Threat Advisory

Ransomware-BitPaymer

December 4, 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://www.mcafee.com/enterprise/en-us/sns/preferences/sns-form.html

Summary

On execution, Ransomware-BitPaymer encrypts files present on a 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, Ransomware-BitPaymer is suspected to be distributed via targeted attacks. Attackers might 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-BitPaymer	7AC671E1ED2E6156149CADA08AF394E9	9412	17/10/2019

The Threat Intelligence Library contains the date when the above signatures were most recently updated. See the previously mentioned Threat Library for the most up-to-date coverage information.

Infection and Propagation Vectors

The infection vector of Ransomware-BitPaymer is currently unknown. Most ransomware campaigns typically spread via Exploit Kits and malspam campaigns instrumented through various botnets. However, BitPaymer is suspected to be distributed using highly targeted attacks such as brute forcing of RDP connections on unprotected systems in an organization's network. After the attackers gain access to an organization's network, BitPaymer might be deployed on 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 can be achieved at several 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.

See following KB articles to configure Access Protection Rules in VirusScan Enterprise:

- KB81095- How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Additional User Recommendations

- **Do NOT open Microsoft Office document file attachments unless specifically requested by the sender**. View the email header or send a separate email to validate the sender before you open attachments.
- **Disable macros in Microsoft Office applications**. Macros can run in Office applications only if the macro settings are set to "Enable all macros" or if the user manually enables a macro. By default, the macros settings are set to disabled. The recommended setting is to select the option "Disable all macros with notification" under "Macro Settings."
- **Back up your business data to the organization's shared folders**. Data that resides on user devices can be permanently lost in case of ransomware infection.
- **Report suspicious emails to the organization's Security Operations Center**. Remind your employees how and where to submit suspicious email safely.

Endpoint Security
Mitigation methods for assorted malware are available in the following product guide:
https://docs.mcafee.com/bundle/endpoint-security-10.6.0-threat-prevention-product-guide-windows

Specific mitigation steps, if needed, are described later in this advisory.

ePolicy Orchestrator (ePO)
- To block the access to USB drives through ePO DLP policy, see KB86007.

Endpoint Security (ENS) 10.x
- To create an ENS Threat Prevention user-defined Access Protection Rule for a file or folder registry, see KB86577.

VirusScan Enterprise (VSE)
- To use Access Protection policies in VSE to protect against viruses that can disable regedit, see KB53346.
- To use Access Protection policies in VSE to protect against viruses that can disable Task Manager, see KB53355.
- To use Access Protection policies in VSE to prevent malware from changing folder options, see KB53356.

Host Intrusion Prevention (Host IPS)
- To blacklist applications that use a Host IPS custom signature, see KB71329.
- To create an Application Blocking Rules policy to prevent the binary from running, see KB71794.
- To create an Application Blocking Rules policy that prevents a specific executable from hooking any other executable, see KB71794.

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

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

Characteristics and Symptoms

The Ransomware-BitPaymer encrypts several files, but mainly files that have the following extensions:
- .bmp
- .jpg
- .jpeg
- .png
- .gif
- .doc
- .docx
- .xls
- .xlsx
- .ppt
- .pptx
- .pdf
- .mp3

Files that are encrypted will have the following extension:
- .locked

Ransomware-BitPaymer does not encrypt files in folders whose name contains any of the following strings:

- $RECYCLEBIN
- $RecycleBin
- AppData
- ApplicationData
- Boot
- SystemVolumeInformation
- Windows
- temp
- thumb
- tmp
- winnt

Ransomware-BitPaymer does not encrypt any files with the following extensions:

- .lnk
- .lock

Ransomware-BitPaymer uses the RSA and AES encryption algorithms. Upon execution, it creates a malicious file in the %UserProfile%\AppData\Roaming folder and starts the following process using the command line:

- Process Name: "36oR0l6IMWUm44gJG7z1x02U"

It then hides the console window:

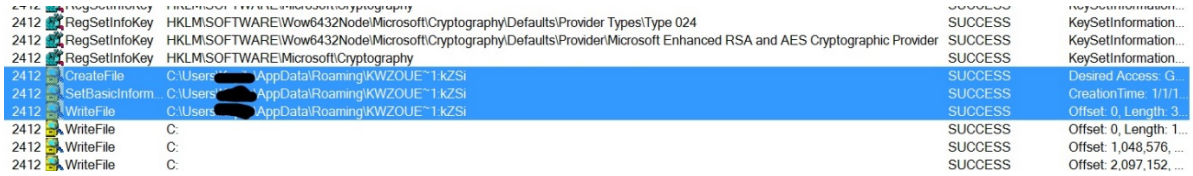


Figure - 1. Malicious copy under %UserProfile%\AppData\Roaming

This malware then searches for a random service that is running and replaces this legitimate service application with a malicious one.

In the example below, the malware randomly selects the RpcLocator Service and changes its name to Locator.exe. The file of the newly created service resides in the %Sysdir% folder:

Figure - 2. Service overwriting

The malware modifies the configuration of the newly created service name in the registry. It modifies the ImagePath value so that it is executed via the command line as 36oR0l6IMWUm44gJG7z1x02U.

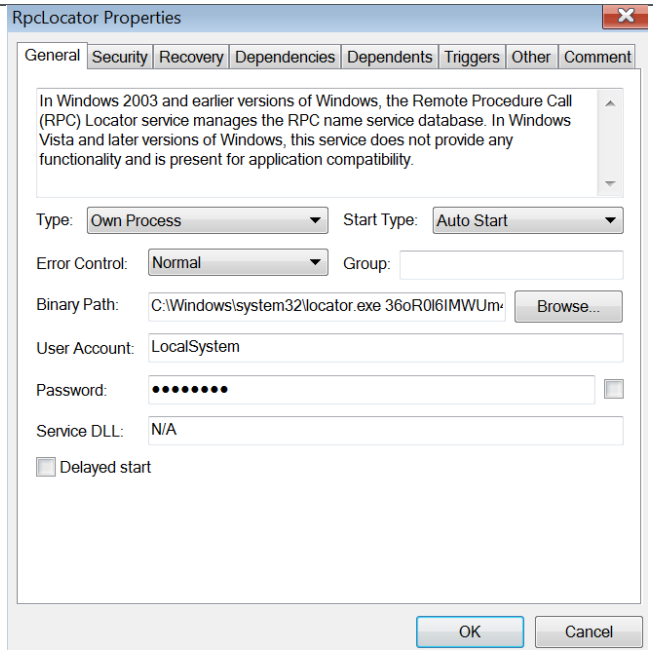


Figure - 3. Modified service property

The “Recovery” properties of the newly created Service are changed so that if it fails, it will be restarted automatically.

After the malware has made its configuration changes, it will delete itself:

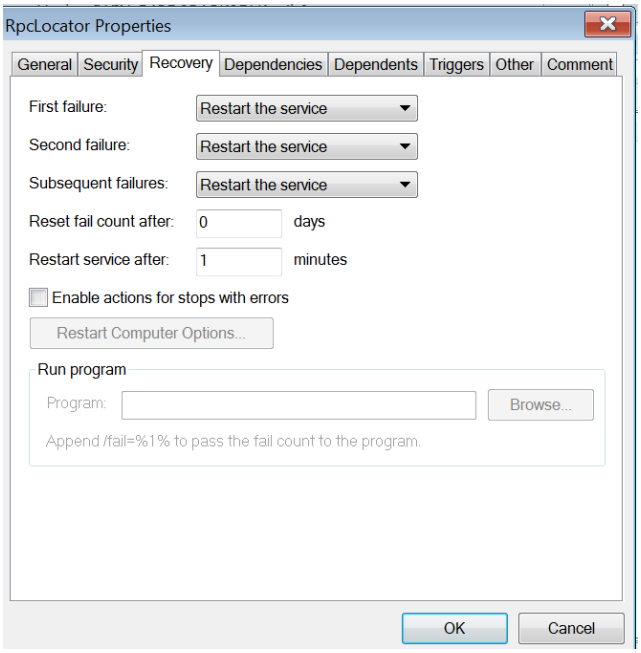
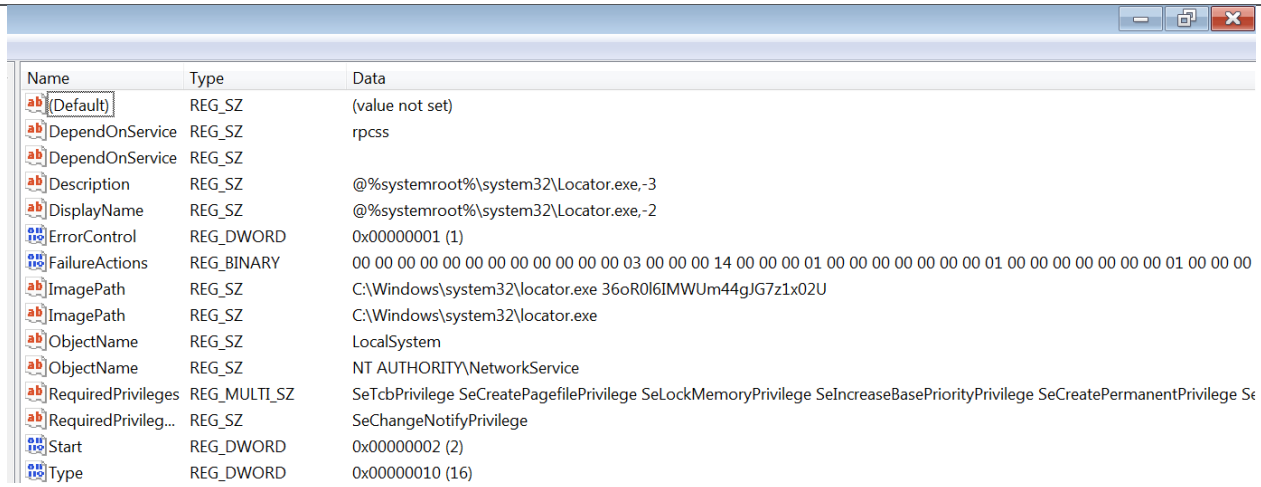


Figure - 4. Recovery service property changed by Ransomware-BitPaymer

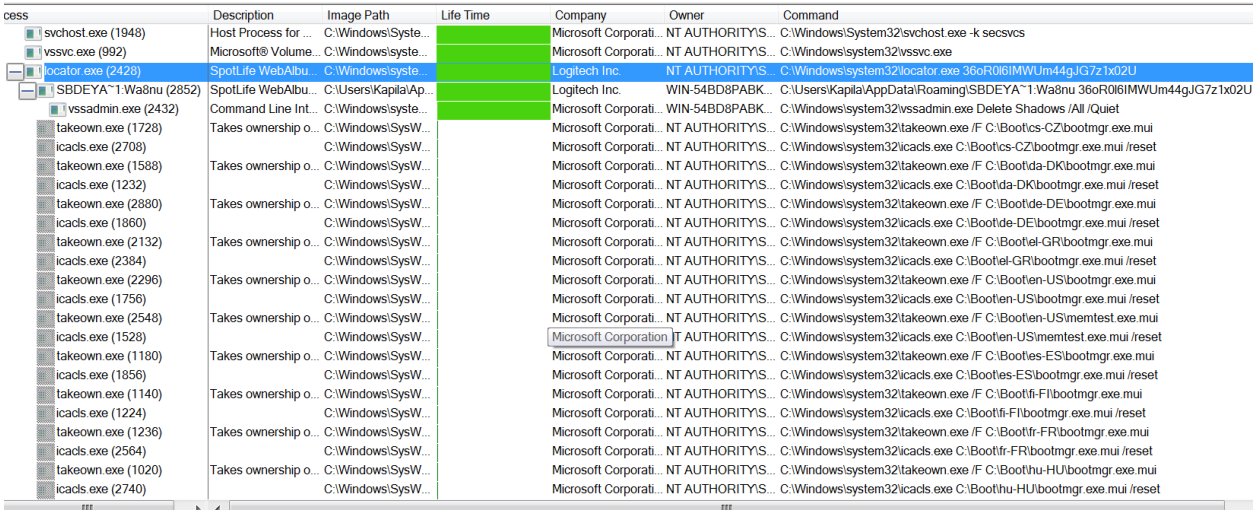


Name	Type	Data
(Default)	REG_SZ	(value not set)
DependOnService	REG_SZ	rpcss
DependOnService	REG_SZ	
Description	REG_SZ	@%systemroot%\system32\Locator.exe,-3
DisplayName	REG_SZ	@%systemroot%\system32\Locator.exe,-2
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 14 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 01 00 00 00
ImagePath	REG_SZ	C:\Windows\system32\locator.exe 36oR0l6IMWUm44gJG7z1x02U
ImagePath	REG_SZ	C:\Windows\system32\locator.exe
ObjectName	REG_SZ	LocalSystem
ObjectName	REG_SZ	NT AUTHORITY\NetworkService
RequiredPrivileges	REG_MULTI_SZ	SeTcbPrivilege SeCreatePagefilePrivilege SeLockMemoryPrivilege SeIncreaseBasePriorityPrivilege SeCreatePermanentPrivilege Se
RequiredPrivileg...	REG_SZ	SeChangeNotifyPrivilege
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

Figure - 5. Malicious service registry key value.

After the new service is started, the malware uses VSSADMIN.EXE to delete all Shadow Volume Copies.

It uses the built-in Windows tools such as takeown and icacls, to take ownership of files and make modifications to them.



cess	Description	Image Path	Life Time	Company	Owner	Command
svchost.exe (1948)	Host Process for ...	C:\Windows\Syste...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\System32\svchost.exe -k secsvcs
vssvc.exe (992)	Microsoft® Volume...	C:\Windows\syste...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\vssvc.exe
locator.exe (2428)	SpotLife WebAlbu...	C:\Windows\syste...		Logitech Inc.	NT AUTHORITY\S...	C:\Windows\system32\locator.exe 36oR0l6IMWUm44gJG7z1x02U
SBDEYA~1:Wa8nu (2852)	SpotLife WebAlbu...	C:\Users\Kapila\Ap...		Logitech Inc.	WIN-54BD8PABK...	C:\Users\Kapila\AppData\Roaming\SBDEYA~1:Wa8nu 36oR0l6IMWUm44gJG7z1x02U
vssadmin.exe (2432)	Command Line Int...	C:\Windows\syste...		Microsoft Corporati...	WIN-54BD8PABK...	C:\Windows\system32\vssadmin.exe Delete Shadows /All /Quiet
takeown.exe (1728)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\cs-CZ\bootmgr.exe.mui
icacls.exe (2708)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\cs-CZ\bootmgr.exe.mui /reset
takeown.exe (1588)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\da-DK\bootmgr.exe.mui
icacls.exe (1232)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\da-DK\bootmgr.exe.mui /reset
takeown.exe (2880)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\de-DE\bootmgr.exe.mui
icacls.exe (1860)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\de-DE\bootmgr.exe.mui /reset
takeown.exe (2132)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\el-GR\bootmgr.exe.mui
icacls.exe (2384)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\el-GR\bootmgr.exe.mui /reset
takeown.exe (2296)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\en-US\bootmgr.exe.mui
icacls.exe (1756)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\en-US\bootmgr.exe.mui /reset
takeown.exe (2548)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\en-US\memtest.exe.mui
icacls.exe (1528)		C:\Windows\SysW...		Microsoft Corporation	IT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\en-US\memtest.exe.mui /reset
takeown.exe (1180)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\es-ES\bootmgr.exe.mui
icacls.exe (1856)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\es-ES\bootmgr.exe.mui /reset
takeown.exe (1140)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\fi-FI\bootmgr.exe.mui
icacls.exe (1224)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\fi-FI\bootmgr.exe.mui /reset
takeown.exe (1236)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\fr-FR\bootmgr.exe.mui
icacls.exe (2564)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\fr-FR\bootmgr.exe.mui /reset
takeown.exe (1020)	Takes ownership o...	C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\takeown.exe /F C:\Boot\hu-HU\bootmgr.exe.mui
icacls.exe (2740)		C:\Windows\SysW...		Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\system32\icacls.exe C:\Boot\hu-HU\bootmgr.exe.mui /reset

Figure - 6.Ransomware-BitPaymer uses built-in Windows tools

The malware drops the following text file, which contains the ransom message shown below:

- readme2unlock.txt

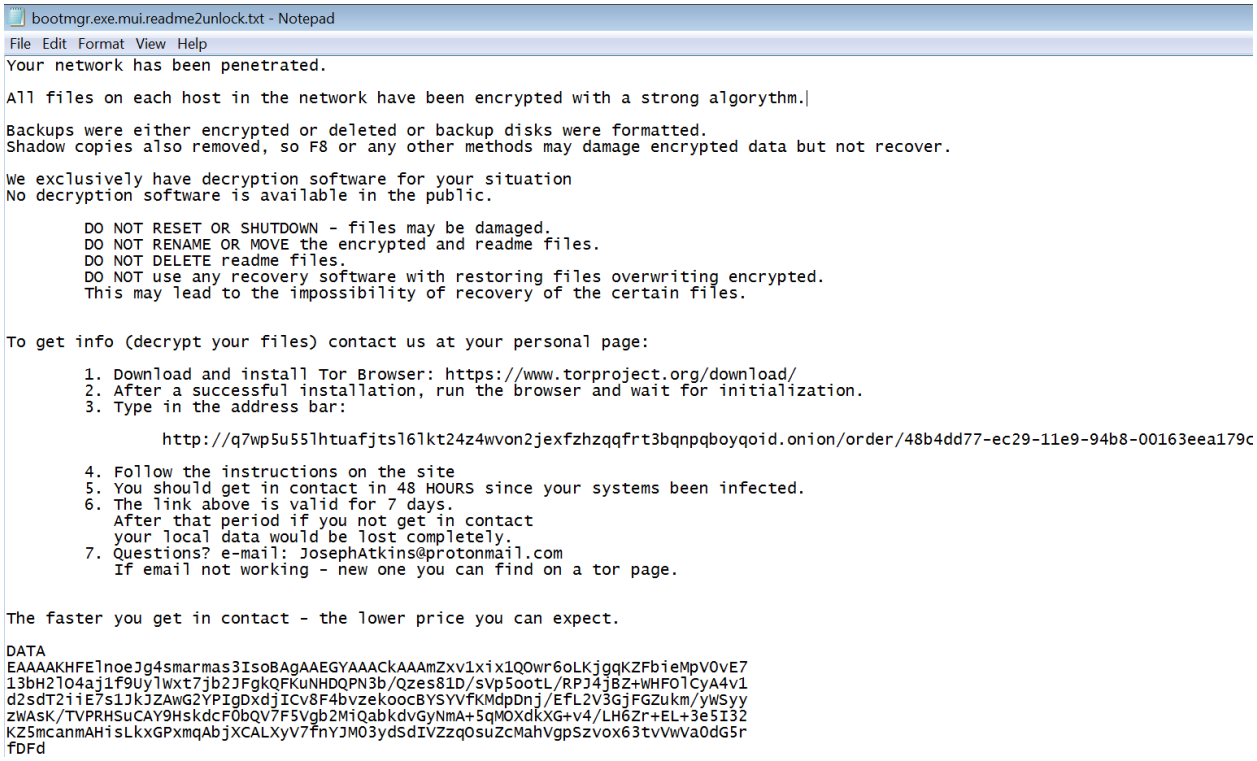


Figure - 7.Ransomware-BitPaymer encryption notification

After execution of the malware, the registry entry will be restored to its original settings, but the reference to the malicious file is still present.

Restart Mechanism

After the machine is encrypted, there were no signs of any restart mechanism for this malware on the system.

Remediation

- The minimum V2 DAT versions required for detection is: 9412.
- The minimum V3 DAT versions required for detection is: 3863.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers, and can prevent or reduce loss when a computer is compromised.
- Turn off file sharing if not needed. Use ACLs and password protection to limit access, if file sharing is required.

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.