2017 年 10 月 13 日，星期五

一周威胁综述（10 月 6 日至 10 月 13 日）

本文概括介绍 Talos 在 10 月 6 日至 10 月 13 日观察到的最常见威胁。与之前的威胁综述一样，本文不进行深入分析，而是重点从以下方面总结我们观察到的威胁：关键行为特征、感染指标，以及我们的客户是如何自动得到保护、免受这些威胁的。

在此提醒，本文中介绍的关于以下威胁的信息并不十分详尽，但所述内容截至发稿日期为止为最新。对以下威胁的检测和防护会根据进一步的威胁或漏洞分析进行更新。如需获取最新信息，请参阅 Firepower 管理中心、Snort.org 或 ClamAV.net。

本周观察到的最常见的威胁主要如下：

- **Doc.Trojan.Emotet-6344335-2**
  木马
  这些恶意 Office 文档包含嵌入式 OLE 对象、经过混淆处理的宏代码，并可利用 Powershell 下载负载。值得指出的是，我们还发现这些样本删除了 Emotet 银行木马。

- **Doc.Dropper.Agent-6346631-0**
  Office 宏下载程序
  这是一种经过混淆处理的 Office 宏下载程序，它会尝试下载恶意负载可执行文件。

- **Doc.Macro.DollarShell-6346616-0**
  Office 宏下载程序
  这是一种经过混淆处理的 Office 宏下载程序，它会尝试下载恶意负载可执行文件。它使用 VBA.Shell$ 开始执行 shell 以及宏自动打开函数

- **Doc.Macro.Obfuscation-6344051-0**
  Office 宏
  这些 Office 文档样本利用各种混淆技术来逃避检测。此集群侧重于向宏中添加未经使用的花指令以阻止快速分析。

- **Doc.Macro.VBSDownloader-6346528-1**
  Office 宏下载程序
  具有使用 base64 编码的宏的 Word 文档在最近几天十分猖獗。最近的一些样本试图分割“powershell”一词并在其中插入字符来逃避检测。

- **Win.Downloader.Trickbot-6344490-1**
  下载程序
  Trickbot 是一种银行木马，目标在于获取选定金融机构的敏感信息。最近的这些下载程序作为安全文档通过垃圾邮件进行传播，发件人伪装成多个不同的银行。

- **Win.Trojan.RevengeRat-6344273-0**
  木马
  此远程访问工具 (RAT) 可让操作人员在受感染的系统上执行任何操作，例如对用户实施间谍行动、泄露数据或运行其他恶意软件。

- **Win.Trojan.Tofsee-6345150-0**
  木马
  此恶意软件为其他捆绑恶意软件提供切入点。我们已经注意到这些样本与 Zeus 僵尸网络相连，表现出勒索软件的行为并发送垃圾邮件。捆绑内容以多层加密作掩护。

- **Win.Trojan.Vilsel-4621**
  木马
  Vilsel 使用 Visual Basic 编写而成，是一种形式老但攻击力强的恶意软件。它可以在受害者的计算机上将自身复制到多个位置，进而将随机字节串联到每个副本的结尾。它还可以通过将自身复制到受害计算机的 Startup 文件夹来获取持久存在。

威胁

Doc.Trojan.Emotet-6344335-2

感染指标

注册表项

- **<HKU>\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**ProxyServer
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKU>\.DEFAULT\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**ProxyOverride

互斥体

- \BaseNamedObjects\Global\I9B0091C
- Global\I98B68E3C
- Global\M98B68E3C
- \BaseNamedObjects\M3AD7726C
- MC1D37BE7

IP 地址

- 不适用

域名

- dmsdjing[.]com
- giantsinthesky[.]com
- ihugny[.]com
- haylophoto[.]com
- joshzak[.]com

创建的文件和/或目录

- \Users\Administrator\Documents\20170925\PowerShell_transcript.PC.FsvUAdg8.20170925212636.txt
- \Users\Administrator\Documents\20171010\PowerShell_transcript.PC.ywSjiQPH.20171010164255.txt

文件散列值

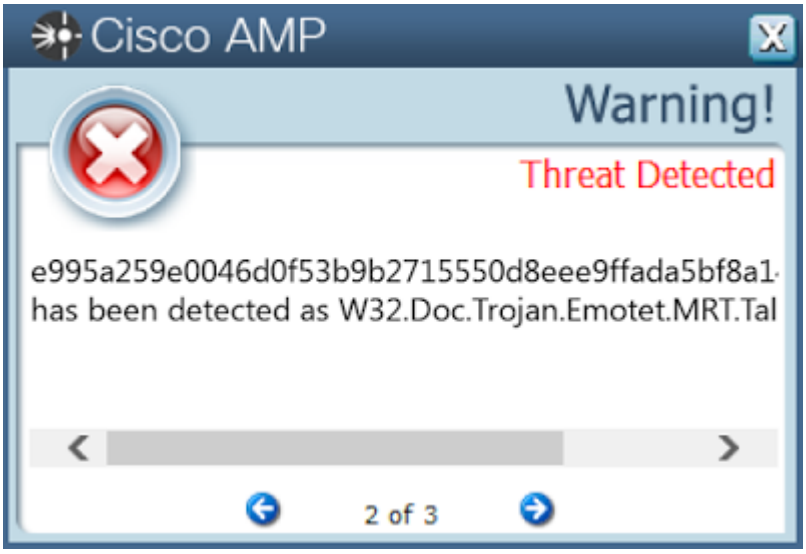
- e995a259e0046d0f53b9b2715550d8eee9ffada5bf8a14faaaf6a77a7ce2fbcf
- 56aa0e876398efcb1ba2e8465e8bd91109e700147eff81acac5ad2514e2f011a
- a54134f7e0303f27781cdb6152e87ac0be5a6e736e242f9f5bcaca0e79dfca89
- 5b060682f0a97793797856af8c37265825d2c6769d9e69bc14833a98672e004a
- a38563a27a75eab4ddc5d76a99a1e8589775add35fce1e20d0b2bc6b64bf2cfb
- f7972ab6d27883f9c1a0fb6b0e54466eb6305eaa1bfb6c09da82e1539bbe7fc4
- d91e08ac9c92e97acc03c87aeb20383150f17a26946e74eb450f48ddf612d5dc
- 4a5d8769935f5126bca4ccfd5f0c658fb6e7d41a34475d9b7712d51b3884e2f3
- 4beabf7a352c6dc30a2273392f4daa5793e43412c3eba3724e2ed9e5631c41c2
- 0c34b872ba2266c2028e27c9fc9bed8fe9c6f04221695e19c5194200a9638d6e
- 24b041585da64a03245c460805f68dbac94b63d19aba6f1bbf7f7d6fa3a26033
- ee69976d53e2f0ee0d502f416ac54cb795059005f82989e095bdc7e5e299acbe
- 73ca04dd07cefa6bc4fc68714e0f2ec98f251833ff48eb8276f8cea09526fa89
- 3204f0c0ea5cafad98a2884d6c44a6eb7d4de82978962bbe2dbe332919b1185f
- 4ce5366c7eef1fff1260d5d7a0aec72c1246621838bf8df07f4a6ab3e5369d96
- ef38926f1932b370abe835b38c51b806d4282e420ee06b312d9a2a25c446cf44
- e77ff24ea71560ffcb9b6e63e9920787d858865ba09f5d63a7e44cb86a569a6e
- b160f7e0036a12a9b7b499249950aaeec569484ff0d50122c4d32d72c75aaf49

防护

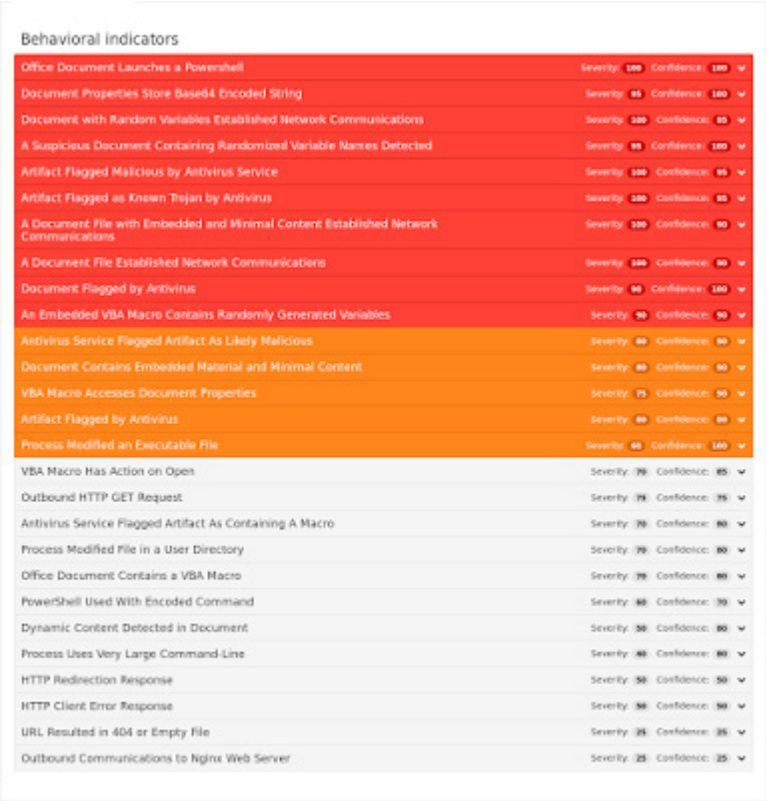
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Umbrella

Doc.Dropper.Agent-6346631-0

感染指标

注册表项

- 不适用

互斥体

- Local\ZonesLockedCacheCounterMutex
- Local\WinSpl64To32Mutex_e39d_0_3000
- Local\MSCTF.Asm.MutexDefault1
- Local\ZonesCacheCounterMutex
- Global\552FFA80-3393-423d-8671-7BA046BB5906

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- \Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C5F7053F-0132-4AED-9DD3-3BD5F82E6BF2}.tmp
- \TEMP\~$f56d32aea142f2f1bd162f709949a06025a400defd6a8fa564be8fdd02d81d.doc
- \Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4312D399-C51E-4E15-8491-42FD34DED614}.tmp
- \Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRD0000.doc
- \TEMP\6ff56d32aea142f2f1bd162f709949a06025a400defd6a8fa564be8fdd02d81d.doc
- %AppData%\Microsoft\Office\Recent\6ff56d32aea142f2f1bd162f709949a06025a400defd6a8fa564be8fdd02d81d.LNK
- %TEMP%\CVR700.tmp.cvr

文件散列值

- 6ff56d32aea142f2f1bd162f709949a06025a400defd6a8fa564be8fdd02d81d
- 71f2070d889c5d68b49bf31c45681cef343fbcf591b5f78e33471bc561541555
- 9246db170b7877dd00c0ea6154e28c33d0fc4c474efa934012657baf4f2b305a
- 2534cdf72fdb3f4e7580f2afc0eab07abb547aea1e3ac8dd36d34303d4370d73
- 64ffe80a9df394598ce7f1129242510c3fdeadadd374721e954910a5f0cd88ad
- 96894cb20067c2dad1d342f918b3c8aa4bb3941571c237ba1d830f584d9a116b
- bad6335692e4deeea9050fe22a88dda2723b053bf165c076d67262d9d40064c2
- d8cc4e04f80fa3073d7522f28d0c4a94ba7c2867e27b37175b02e11103ceb1d1
- 4ccf25007d397304643830d11f5f39bd9bdd73469b71caf4696cc4f466c98183

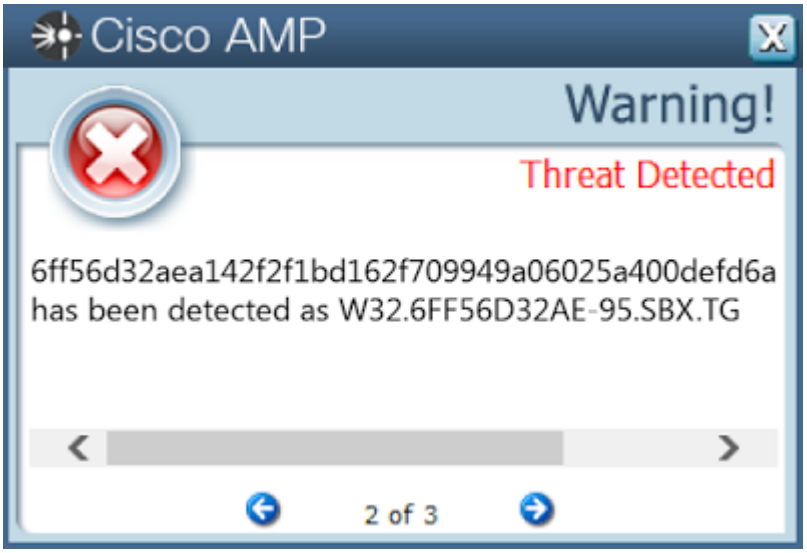
- 3cb3476f8998fdd58ba76d636cf18040ca3503c9e713da2ef1a65e15e39c9b69
- ab88aa6377b9721c3091183632db23b817d99a3f3c5aafc4d5d549ef59d55040
- e0a31ea6e31090ac6826033b96ea3bbe27b925b228e4f94c232beb5dfc289577
- b47f65ff1975b3eb15e0b41872221d655d99e13f952d32b334168b8c3a684ea5

防护

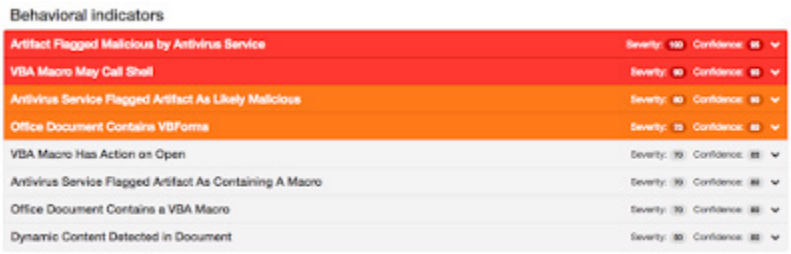
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

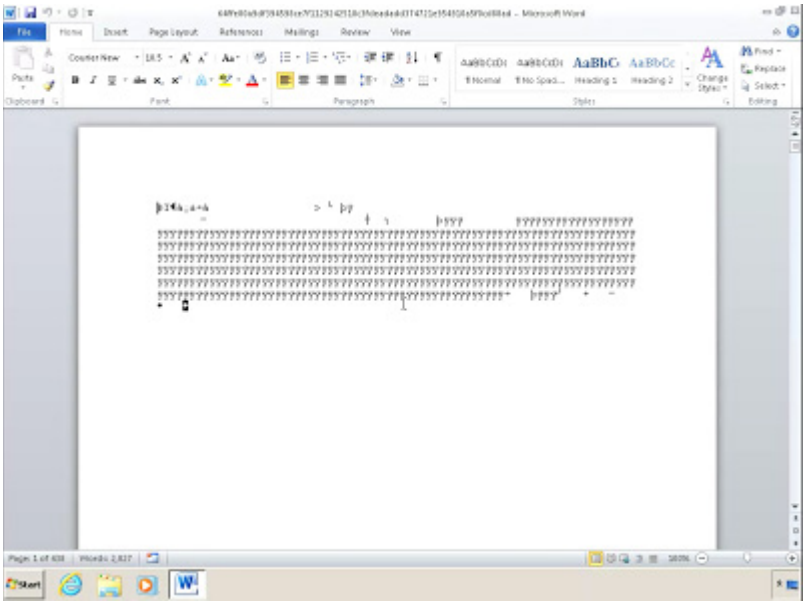
AMP



ThreatGrid



屏幕截图



Doc.Macro.DollarShell-6346616-0

感染指标

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 185[.]35[.]228[.]6
- 52[.]179[.]17[.]38
- 192[.]168[.]1[.]219
- 167[.]114[.]121[.]80

域名

- halalsecurities[.]com

创建的文件和/或目录

- %WinDir%\SysWOW64\specsystem.exe

文件散列值

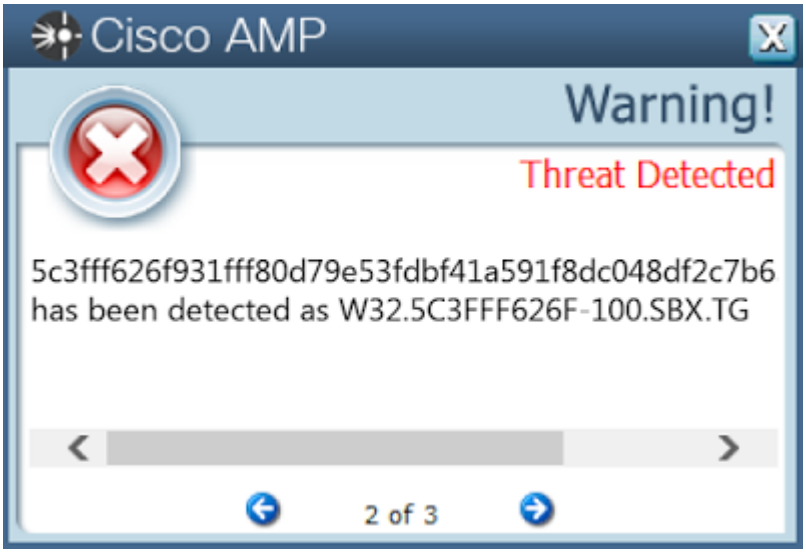
- 5c3fff626f931fff80d79e53fdbf41a591f8dc048df2c7b636aa2d7a388d8e63
- 26582ff0d7d9578d564bedc4f3add7d0d2326be6959039b7dc2372458390e810
- 2c34d5de4bfbca74b4a782a221c44311fba086f876af6020f16c36b8759dcd24
- bb1a67049f2f65ce40d68a111becaf0f772754c024013b8d8a869d59472af9eb
- 25948723a1ed54e5d7994639b0002f5074ff60b0bbd61a78c1e59dd80ebb4c54

防护

产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

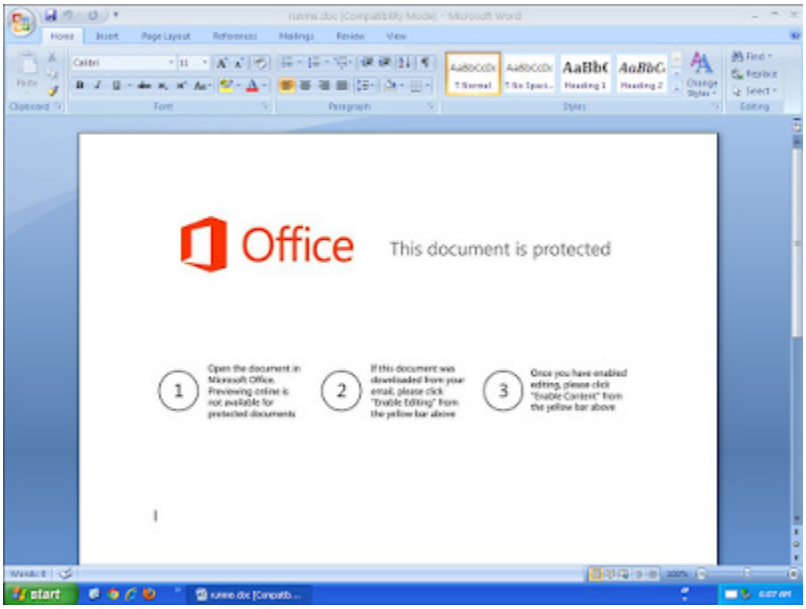
AMP



ThreatGrid

Umbrella

屏幕截图



Doc.Macro.Obfuscation-6344051-0

感染指标

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 52[.]179[.]17[.]38

域名

- 不适用

创建的文件和/或目录

- 不适用

文件散列值

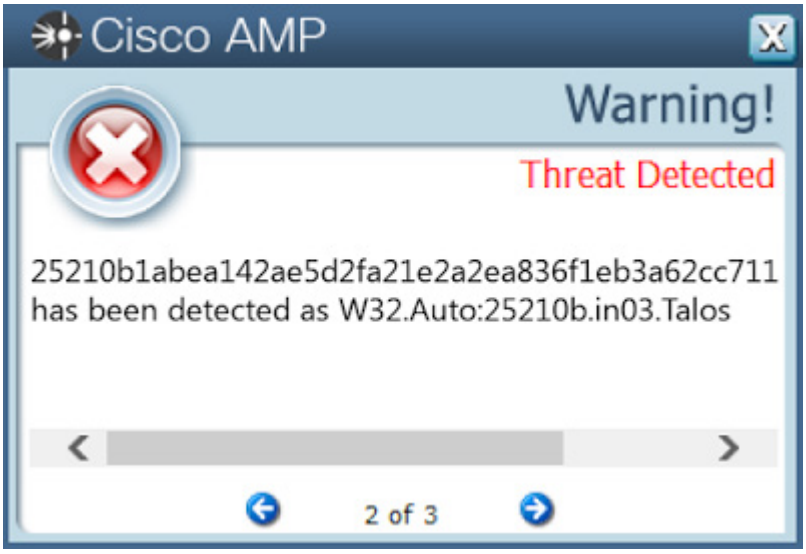
- 25210b1abea142ae5d2fa21e2a2ea836f1eb3a62cc7118f2188bf63904c9523a
- 1da8eda0545dbe5a53d41fb1b9ed71c7129cf14b2395acffd601056b7d6765fd
- 1e85b7f0d09e6a43cd83a66c287c1d34125ab9ee8e2f81d86a6c46ef44e37c20
- a7b7a582248f4ed47c8816c9436e7a49f2c02a83d18014509d0215e217f19e9e
- 6f7b63d2f5be6d7ada5c8146e076af21acd4273d538d46c1dddf6bed222a6d4d
- 4abacdd4177a4446dedc00992c7d33538fd0046ba99971c2dcbdff49d51a7664
- 81bcde515e51332cd4b92996655fb28448c2b3a83b6a63443ee680ad63acdce1
- c1a87f71d9f51cbbc82c03b58b75bdd6feb7d1be1d9d292c4a6a107b78a64efc
- 9e316bc8edd80e260d8ef24accfd2f1c1561665171d0721f4a36585e9b1cbe99
- 7ba4b97d8ef2eb865b6d6e76c77446657eb39269b5d276e77f458fa3fd639e2c
- 0b2799af3a38a865c37fe534c3f2f67d085757b09f5e489025037a1ed90f9b98
- fd5c9b1ea6c9c76f3282634f8d7b02e0dba6e9813ae0143c7073ecdd925ee2f8
- e0d0d55c04eb477c6becda415eed279895c56e4468df63ae302be7d389c95741
- 85fe7541480ab4165d31d0d83a020068a3de0f673e50b3aefa4be22f51f47704
- 7cdeb17d6bfa95e937868b7761be87ded361ec49cf6be88286a1c2cb22f3976a
- ee787d5959e57fe1787b36a3bfa3fd4d90e4a0b1705f96f4a90a06d0bdd75cab
- 984730d87bc7df01d890f8719f83712c7eaf7af05de5cb9a49d3132dc6251751
- a60e1a67b0080b342a5586a53497f2ea2ac51c55cf5b2b721593ddfc1248c838
- 0ff727f106fecde4e4292f0e35092376786cf8a9097da064623ffa912db7e9bf
- b2c8a5be4249b5eb4b4a28cffaa3ef247589e0eb5ce0b7a914f8c1704b7f6cb4
- 6adbd32b36470178e4cbc4bf7c757e4338457cac8c53fc5f8a86b3bcfec2fa6d
- b49adc35b4a6add49bc0accfc9ce9b6d2f8c093af0c2ee6dd05750aba2c75503
- 9de97b64e55209d946f21d8e1be015932f0df9df1acc0c282b8aaf6885b5d254
- 485ac8f15a1ed8005940365da1dd1031244eb9b18b86cc97a001483d23983e01

防护

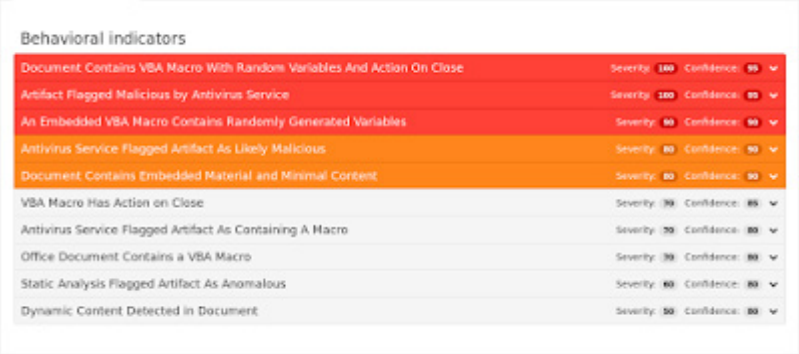
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Doc.Macro.VBSDownloader-6346528-1

感染指标

注册表项

- **<HKLM>\SYSTEM\CONTROLSET001\CONTROL\NETWORK\{4D36E972-E325-11CE-BFC1-08002BE10318}\{9EB90D23-C5F9-4104-85A8-47DD7F6C4070}\CONNECTION**
  - **值：**PnpInstanceID
- **<HKLM>\SYSTEM\CONTROLSET001\ENUM\SW\{EEAB7790-C514-11D1-B42B-00805FC1270E}\ASYNCMAC**
  - **值：**CustomPropertyHwIdKey
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**AutoDetect
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**IntranetName
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**IntranetName

- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
    - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
    - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\OFFICE\14.0\WORD\RESILIENCY\DOCUMENTRECOVERY\52125234**
    - **值：**52125234
- **<HKCU>\Printers\DevModePerUser**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap**

互斥体

- Local\WinSpl64To32Mutex_44fd9_0_3000
- RasPbFile
- Local\MSCTF.Asm.MutexDefault1
- Global\552FFA80-3393-423d-8671-7BA046BB5906

IP 地址

- 74[.]220[.]215[.]115
- 66[.]147[.]244[.]177
- 80[.]93[.]29[.]189
- 74[.]220[.]207[.]77
- 202[.]191[.]62[.]28
- 74[.]220[.]215[.]235

域名

- damanidigital[.]com
- markjgriffin[.]ie
- ardentfilms[.]com
- matteostocchino[.]com
- on-int[.]com

创建的文件和/或目录

- \Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{91051D81-AD46-4035-86B1-0308A15C9AA9}.tmp
- %TEMP%\CVR4C79.tmp.cvr
- \TEMP\~$5cb14fade7c435e10d673170dd975ee9b3f1c15fd932dc5c9d2663b4a7af10.doc
- \Users\Administrator\Documents\20171013\PowerShell_transcript.PC._mX5ReZQ.20171013054549.txt
- %AppData%\Microsoft\Office\Recent\195cb14fade7c435e10d673170dd975ee9b3f1c15fd932dc5c9d2663b4a7af10.LNK

- \TEMP\195cb14fade7c435e10d673170dd975ee9b3f1c15fd932dc5c9d2663b4a7af10.doc

文件散列值

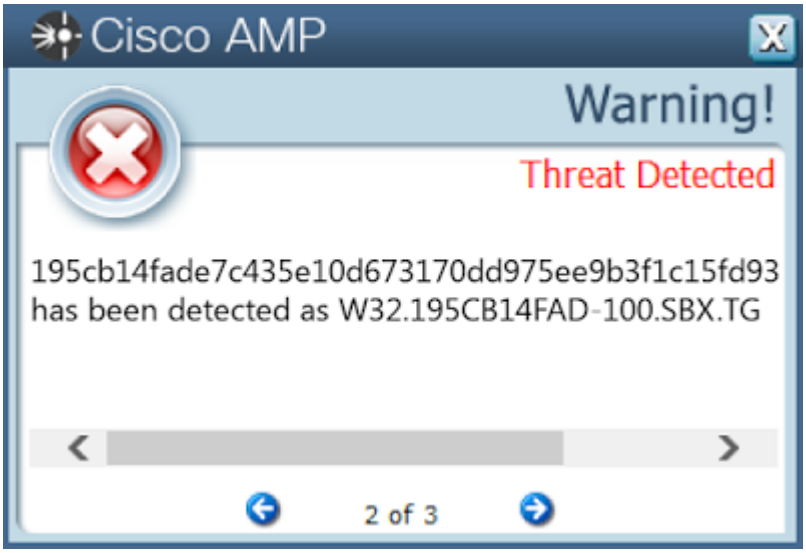
- 195cb14fade7c435e10d673170dd975ee9b3f1c15fd932dc5c9d2663b4a7af10
- 2374d35b524259f14a3cd41eca49417c69fafdab226a4d00788c014b3c2c922c
- 25948723a1ed54e5d7994639b0002f5074ff60b0bbd61a78c1e59dd80ebb4c54
- 26582ff0d7d9578d564bedc4f3add7d0d2326be6959039b7dc2372458390e810
- 2747932c56b816aae80ace812975e868b3227ab651903c1dc01e987231cccc96
- 2c34d5de4bfbca74b4a782a221c44311fba086f876af6020f16c36b8759dcd24
- 4b9703f52464b8025e0146ae4792400f7c077194b0007b3d2ae31eb80642c517
- 4bc6d7e5960831476f33ac3d9f632ebae9c2a22aa975d20fffb0830b94bf3143
- 57794867310c0c673a34eccea666780b09287f8ca42e4c5aadd21abec43d8168
- 5c3fff626f931fff80d79e53fdbf41a591f8dc048df2c7b636aa2d7a388d8e63
- 9949dccece62023379790e8b563d8a93bae156be13e7698f851a3804b72fa1c3
- a6026baa4f4062b2bbf66dc3a3707f965e34271cdd3f00cae45f771e4b4b9013
- bb1a67049f2f65ce40d68a111becaf0f772754c024013b8d8a869d59472af9eb
- ca38154915f53ec6c2793e94639e2ce9701de8236e41064cba35fe7e6387af70
- db1ba6f50f367209db4733b94e8d22c8703665bf5b90716bfc754b3639d4c76a
- e95c8bf136de1cd79bfd3811072e7d02441aa5e8f57ab60e2b1478a4d4ca5678

防护

产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

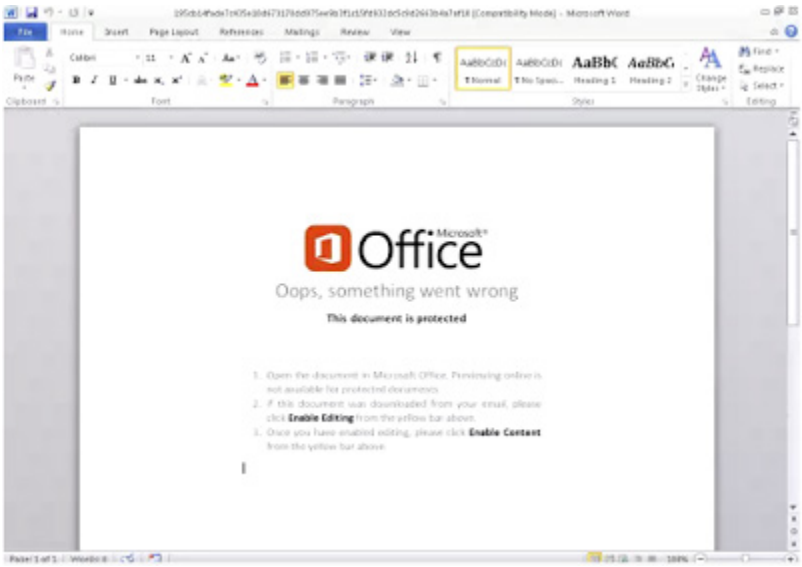
AMP



ThreatGrid

Umbrella

屏幕截图



Win.Downloader.Trickbot-6344490-1

感染指标

注册表项

- **<HKU>\Software\Microsoft\Windows\ShellNoRoam\MUICache**

互斥体

- rdyboost_Perf_Library_Lock_PID_99c
- WBEMPROVIDERSTATICMUTEX
- 316D1C7871E00
- \BaseNamedObjects\647C097C25F0128
- \BaseNamedObjects\E572F578D5E00

IP 地址

- 174[.]129[.]241[.]106
- 194[.]87[.]103[.]184
- 52[.]179[.]17[.]38
- 87[.]106[.]222[.]158
- 185[.]158[.]152[.]225
- 162[.]255[.]93[.]51
- 184[.]73[.]220[.]206
- 23[.]23[.]170[.]235

域名

- diga-consult[.]de
- hill-familie[.]de
- deversdesign[.]com
- essenza[.]co[.]id

创建的文件和/或目录

- \Users\Administrator\Documents\20171004\PowerShell_transcript.PC.9v8wz+M+.20171004215407.txt
- \Users\Administrator\Documents\20171004\PowerShell_transcript.PC.44+uZp3a.20171004215409.txt
- %AppData%\winapp\Yqtgdelssjn.exE
- %TEMP%\Gce8.bat
- %WinDir%\Tasks\services update.job
- %AppData%\winapp\Xqtfcdkssin.exE
- %System32%\config\TxR\{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
- %TEMP%\Ovvgpiua-_2.exE
- %AppData%\winapp\Pvvhpjua-_3.exE

文件散列值

- 0d92b1656112ed73fe98fd6c714d7959dd8ecc85759b87a6b01747a2ab0f8335
- 3ac1c23c28d19111e254649153b2cf0c03782f7523ce2062200a5ecd1c24f210
- 5351019f9879a285561e72acae1024e8a86a822f33b7bbb95c795a6bc465ff53
- 6acd175a2971b370ae7413bad180f8f745a4b391b0fa4f3e70ef660f5e3bee75
- ae860de508c56045b39679b72b570028f820d9523f7e5d6ddb326c9a757c5c77
- e6bd4d23467ee8df96837140695de5689cc7f7b73cffd9a9d40e33444766496a
- 08a5a27b430bdc6d157ebdbf5dd0e7c648d7fc0e9e3e52baf54f5b770f72e919

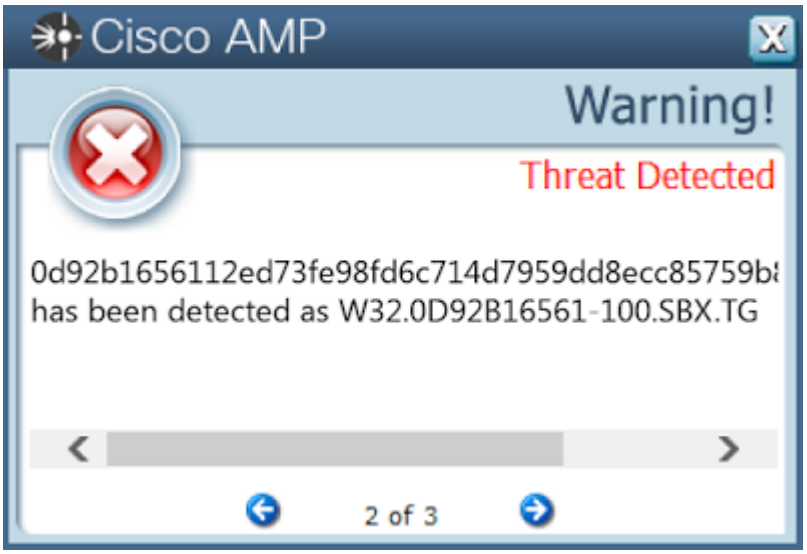
- 3a4ea7d6ce3bf31398f34e831249aaccc3a6c123eae239bca37ab1dd57749c19
- 8c937c4364f8c5c003f35771dd7983def26a073a9ad5dda9fca302f762dd4c83
- 793c3af7a30ca9cbb1a9f33b1986b8628af45ec1c2a04c1dd98a5cfa376f55be
- dcfcc1a702447925e8826cf1b15a79db9ceee264c46e0447f62856c52be76c9a
- 37e7afe3da64064dacbc53b5cac88972662a181aa864e094b4a45ce88318d7f3
- 721c1d648a245bc350d1ace7537db518162f725f2dab14bd4a149d8165144962
- b4492030182ee0e7c3257f417fe98d4e52d301230e31491a4563cb41fa6b3343
- 5619eeb7b8702693f78b452a0ca3df99a23b858d2b4d181bcd5588878411284e
- f45334629dc79665d85cd4748e97b876de4330094759dc4c227da19ffbbd2a34
- 27bc34902437285c3f4fe0a0e3446314baecb7ee002fcd1060b91543c27b9369
- 38748c33121e51307108ca9711c4a5109223d86565f8902268e902f83a202fbd
- a3355d8e3e5f21b84072993032341bf1edee8dd6b28a9aece5cc6ffe0e123621
- 28df3fd75d3c3748b26931a449229f585f4e4543aa25a0caf37367444bb7a7c2
- 99714908dc8d8316bcad7089c8d100755cd25f77c52bce91af0ed3a9a44db1bf

防护

产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

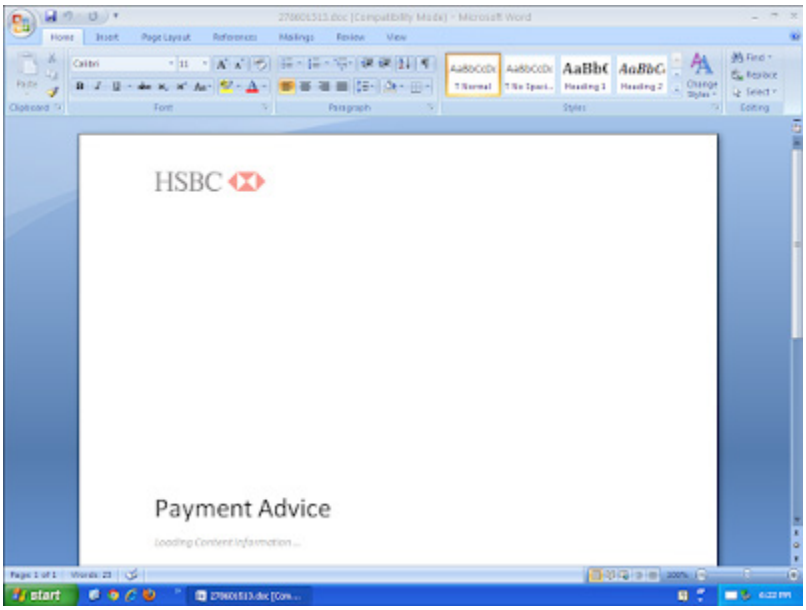
AMP



ThreatGrid

Umbrella

屏幕截图



Win.Trojan.RevengeRat-6344273-0

感染指标

注册表项

- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**

    - **值：**WindowsServices
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
    - **值：**internat.exe
- **<HKU>\Software\Microsoft\Windows\ShellNoRoam\MUICache**
- **<HKU>\Software\Microsoft\Windows\CurrentVersion\Run**

互斥体

- RV_MUTEX-yHuiGGjjtnxDp
- \BaseNamedObjects\RV_MUTEX-yHuiGGjjtnxDp

IP 地址

- 86[.]120[.]105[.]76

域名

- darkcometratttt[.]ddns[.]net

创建的文件和/或目录

- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\WindowsServices.exe
- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Startup\WindowsServices.exe

文件散列值

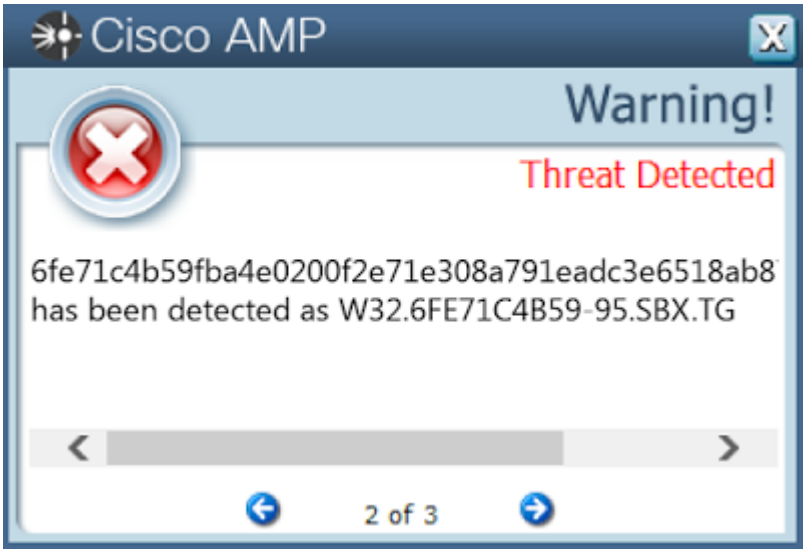
- 6fe71c4b59fba4e0200f2e71e308a791eadc3e6518ab87acb66db4c79df66985
- 7d0474c514e78deac6f690006546bf92c029836c60d547504ceebdd21bf6130c
- bd3bcfecf479bd347540d6305001b068583696aa81279739ee8b32eb34f2a0df
- e422cc0f5bb2d56d1def4063ac21cb8e18f97dfc48287e8b47ba07863704a8af
- e60613e2453d6568cb04ad8e09ac64b6652318079be2444156293f092cc9ff52
- b110def3771963078f3ce54d13d23a6f751ea6dc41e5177e242208791a0a8342
- fdb99a0527be797fc7d7b7f48088c21d034bce6a5c848ede43714d86d3266661
- 0d576038349acf0892cbb0124b9558bb4b80c070875017c320dd12bdc0c21f9a
- d06ffdfe71bd471b8ba5c2c9fd1191e661c6a9d2332243bc4f93f3838cbff75b

防护

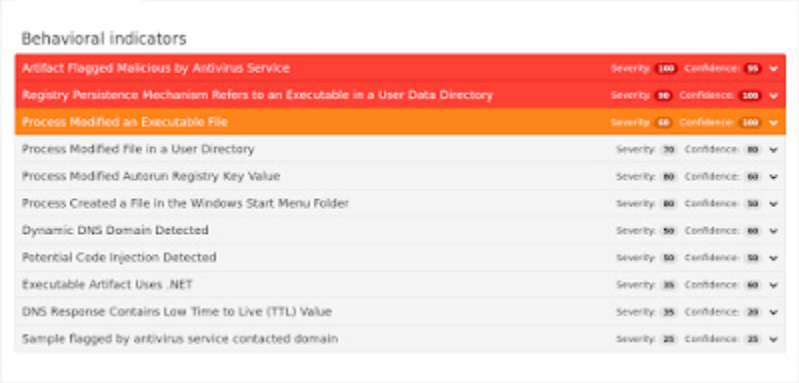
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Umbrella

Win.Trojan.Tofsee-6345150-0

感染指标

注册表项

- **<A>\{461C21F0-877D-11E7-AB94-00501E3AE7B5}\DEFAULTOBJECTSTORE\OBJECTTABLE\A9C**
  - **值：**AeFileID
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**Start

- **<A>\{461C21F0-877D-11E7-AB94-00501E3AE7B5}\DEFAULTOBJECTSTORE\OBJECTTABLE\A9D**
  - **值：**AeProgramID
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**Description
- **<A>\{461C21F0-877D-11E7-AB94-00501E3AE7B5}\DEFAULTOBJECTSTORE\OBJECTTABLE\A9D\INDEXES\FILEIDINDEX-{3F37BA64-EF5C-11E4-BB8D-806E6F6E6963}**
  - **值：**10000000095A9
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**ObjectName
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**ErrorControl
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**DisplayName
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS DEFENDER\EXCLUSIONS\PATHS**
  - **值：**C:\Windows\SysWOW64\qpyyzgqi
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**WOW64
- **<A>\{461C21F0-877D-11E7-AB94-00501E3AE7B5}\DEFAULTOBJECTSTORE\OBJECTTABLE\A9C**
  - **值：**_FileId_
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\QPYYZGQI**
  - **值：**ImagePath
- **<A>\{461C21F0-877D-11E7-AB94-00501E3AE7B5}\DEFAULTOBJECTSTORE\OBJECTTABLE\A9D\Indexes**

互斥体

- 不适用

IP 地址

- 185[.]12[.]95[.]147
- 207[.]46[.]8[.]167
- 64[.]12[.]88[.]132
- 200[.]138[.]219[.]72
- 199[.]212[.]0[.]46
- 185[.]7[.]123[.]158
- 65[.]55[.]92[.]184
- 23[.]103[.]156[.]42
- 66[.]196[.]118[.]37
- 185[.]195[.]27[.]81

- 65[.]55[.]92[.]152
- 74[.]125[.]133[.]27
- 98[.]138[.]112[.]38
- 23[.]103[.]156[.]74
- 64[.]12[.]91[.]196
- 98[.]136[.]216[.]26
- 103[.]248[.]137[.]133
- 64[.]12[.]88[.]164
- 65[.]55[.]33[.]135
- 89[.]233[.]43[.]71
- 110[.]77[.]183[.]122
- 172[.]217[.]13[.]67
- 65[.]55[.]33[.]119
- 152[.]163[.]0[.]67
- 195[.]154[.]242[.]211
- 192[.]0[.]47[.]59
- 191[.]239[.]213[.]197
- 5[.]133[.]235[.]100
- 65[.]55[.]37[.]120
- 104[.]44[.]194[.]231
- 65[.]55[.]37[.]72
- 65[.]54[.]188[.]94
- 209[.]244[.]0[.]3
- 66[.]196[.]118[.]240

域名

- mailin-01[.]mx[.]aol[.]com
- mailin-04[.]mx[.]aol[.]com
- mailin-02[.]mx[.]aol[.]com
- mx4[.]hotmail[.]com
- mta5[.]am0[.]yahoodns[.]net
- mta6[.]am0[.]yahoodns[.]net
- www[.]google[.]co[.]uk
- mx3[.]hotmail[.]com
- whois[.]arin[.]net
- mx1[.]hotmail[.]com
- comcast[.]net
- mx2[.]hotmail[.]com
- 250[.]5[.]55[.]69[.]in-addr[.]arpa
- alt4[.]gmail-smtp-in[.]l[.]google[.]com
- mta7[.]am0[.]yahoodns[.]net

- 250[.]5[.]55[.]69[.]zen[.]spamhaus[.]org
- mx1[.]comcast[.]net
- mx1[.]charter[.]net
- 250[.]5[.]55[.]69[.]bl[.]spamcop[.]net
- alt3[.]gmail-smtp-in[.]l[.]google[.]com
- www[.]google[.]com
- microsoft-com[.]mail[.]protection[.]outlook[.]com
- microsoft[.]com
- 250[.]5[.]55[.]69[.]sbl-xbl[.]spamhaus[.]org
- mailin-03[.]mx[.]aol[.]com
- charter[.]net
- whois[.]iana[.]org
- 250[.]5[.]55[.]69[.]dnsbl[.]sorbs[.]net
- gaby-gorny[.]de
- gaby-gerstner[.]com

创建的文件和/或目录

- %WinDir%\SysWOW64\config\systemprofile\Local Settings:init
- %WinDir%\AppCompat\Programs\RecentFileCache.bcf
- %System32%\bbscpfka\pdqccygi.exe (copy)
- %WinDir%\Temp\rohwayag.exe
- %WinDir%\SysWOW64\config\systemprofile\Local Settings
- %WinDir%\SysWOW64\qpyyzgqi\eoopfgxb.exe

文件散列值

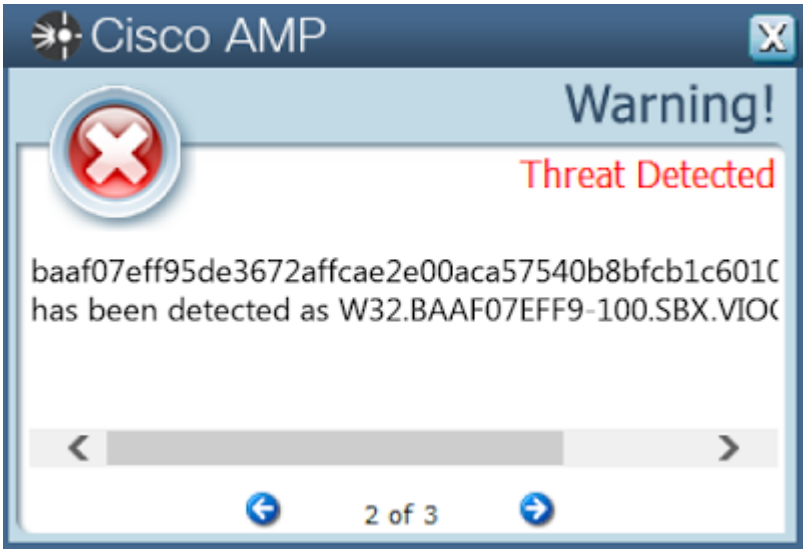
- baaf07eff95de3672affcae2e00aca57540b8bfcb1c6010ee359213d8700bd0e
- 6cbb53ee5485e756bd8680944961b6c27d59c1a610c5f93c1788a2dafd1f5706
- 0f4d468818d80d3048879c26546dc5b413956ca2a5ec5261fa54a00d03e0b393
- d02cd223f8284826a4dd1d51ecb61cc39e2588c534c0e6b848f6fbfd772fc02a
- b637127d56d4b02c131bfdeaa8a42d95210bdd33285ef5788249ba8f631a0abf
- 9f33ee45c11c52f6c6a38bb004457046f5743d51bde77282b2dc1847e9c6cbe9
- 94cab1cdda2cdf19e077add232b00de9b141f981f6def5c7309521613f6423cb
- fa1645ec20a84fd16d9d5eb2960b1caafb168f4456c7a14c8b8e5219bd15b29c
- b29d5908edaa7a98e7b7aca5614e0dbbcbaa5e15e93540f037451db52905ebdf
- 5ecce618b7b65cac1a5930608aa939241f4312a54a3efbfaf8c3bb5e27056b91

防护

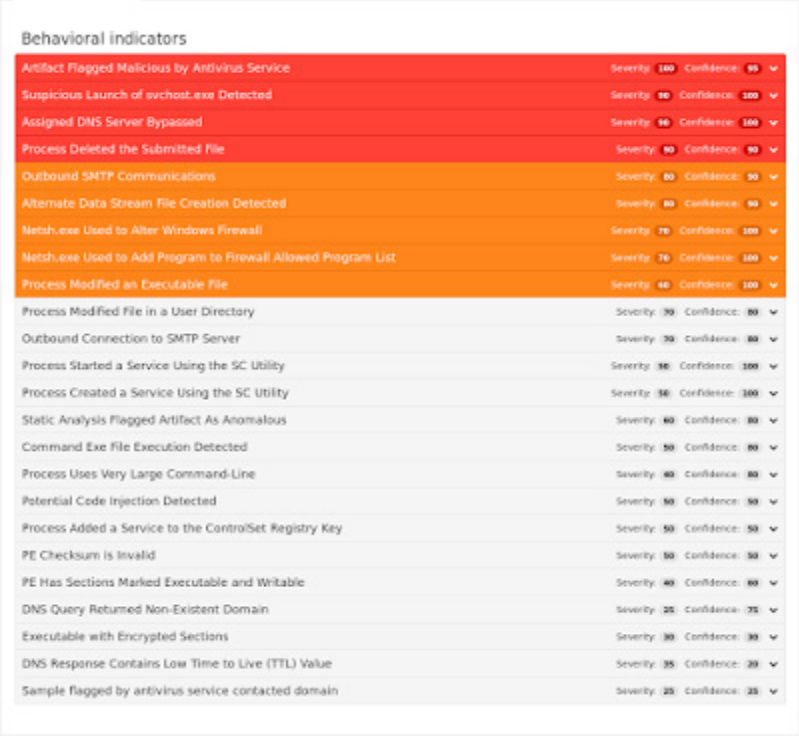
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

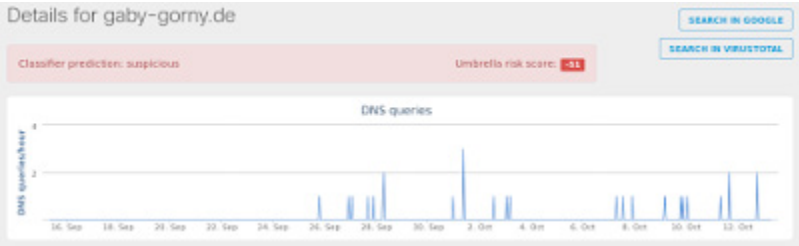
AMP



ThreatGrid



Umbrella



Win.Trojan.Vilsel-4621

感染指标

注册表项

- 不适用

互斥体

- \BaseNamedObjects\Pro3

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- %SystemDrive%\temp.zip (copy)
- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Google Chrome\backup.exe
- %SystemDrive%\c2d124b8466cec6b3e47c4\amd64\backup.exe
- %SystemDrive%\Documents and Settings\All Users\Documents\My Music\Sample Playlists\00A751EC\backup.exe
- %SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Microsoft Office\backup.exe
- %SystemDrive%\Documents and Settings\Administrator\My Documents\backup.exe
- %SystemDrive%\Documents and Settings\All Users\Favorites\backup.exe
- %SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Accessories\System Tools\update.exe
- %SystemDrive%\Documents and Settings\Administrator\Favorites\backup.exe
- %SystemDrive%\H1a02792
- %SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\backup.exe
- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Startup\data.exe
- %SystemDrive%\279862715.dat

文件散列值

- eff9dcc0bebee521ebc2cb48a4398c3fe55e878fe127fda6f2ac02208e135325
- c3ff4ab8815d9934a5a2bb5e02de372e20d70ef2ea519bf96bd3188187ab8a63
- c0a5e770e251be820ac40cf249d5e30eb74be677bc2be054ffd07ceae23cbc33
- 89782f35fef2dad9aadcad63b07fb6ed39077c9edfdccd0716facac53293f872
- 51b411f1c6b10e8ee9bea405e66fc2f1f8f84d29106f119b2423de59101bbbd8
- 4d0bbd53f71ad27a77602fa1b2c3e9a1f92976052ce575f73b4a78d5f9f9ef1a

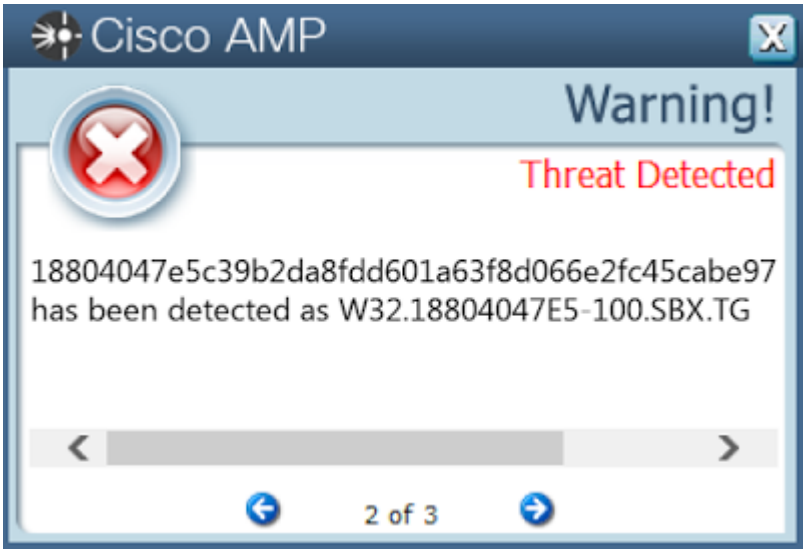
- 2cdaa2c24356b829da8b7aa4aac7e93f3727d9f7378f60e408fae2c2838237db
- 267d1e4423079ce2998b30ff031b854fd72f20754f693e958ed2aa537407b726
- 1b8ba3bde52f7c979d427a03d636c9658b010724b8b93fd98c31a888bcc3123c
- 18804047e5c39b2da8fdd601a63f8d066e2fc45cabe970859e09ffc7a9bd4823

防护

产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid

发布者：ALEXANDER CHIU；发布时间：3:01 PM

标签：CLAMAV、防护、SNORT、一周威胁综述、UMBRELLA

分享此文