2017 年 11 月 17 日，星期五

一周威胁综述（11 月 10 日至 11 月 17 日）

本文概括介绍 Talos 在 11 月 10 日至 11 月 17 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.Macro.Downloader-6360616-1**
  下载程序
  这一波恶意的 Office 文档使用经过混淆处理的宏来启动 PowerShell。然后，PowerShell 进程会下载并执行恶意负载可执行文件或 VBS 脚本。

- **Doc.Macro.Emotet-6374344-0**
  Office 宏
  Emotet 的初始攻击媒介是一个具有经过混淆处理的宏代码的 Office 文档。混淆处理技术包括花指令、随机生成的变量名称、函数重新分配、重定向，以及如果不以正确顺序执行则会覆盖数据的附加代码等。

- **Win.Ransomware.Kovter-6376319-1**
  勒索软件
  Kovter 是一个恶意软件系列，自 2013 年以来便一直存在。目前该系列的勒索软件活动猖獗。

- **Win.Trojan.BitCoinMiner-6374577-0**
  挖矿程序
  要执行此 64 位加密数字货币挖矿程序，受感染的计算机上需要具备一个支持 CUDA 的 GPU。CUDA（计算统一设备架构）是 NVIDIA 开发的一个并行计算平台。

- **Win.Trojan.CosmicDuke-6376318-0**
  木马
  此系列木马已众所周知，它与臭名昭著的 MiniDuke APT 直接相关。由于检测环境中缺少某些 DLL，因此动态分析失败。如果执行此程序，它会收集存储在受害者磁盘上的所有凭证，并与远程服务器通信。

- **Win.Trojan.MSILTrojan-6376261-0**
  木马

此 MSIL 木马会通过进行屏幕截图和放置键盘钩子来监视用户的活动。之后，它将通过合法邮件服务（例如 smtp.live.com）发送邮件，从而利用它们泄露信息或传播恶意软件。此外，它还会使用 checkmyip.dyndns.org 服务检查受感染计算机的外部 IP。请注意，此报告中包含的网络感染指标 (IOC) 属于合法服务。

威胁

Doc.Macro.Downloader-6360616-1

感染指标

注册表项
- 不适用

互斥体
- 不适用

IP 地址
- 不适用

域名
- procuratorkn[.]top
- touchlifefoundation[.]biz
- www[.]bobnew[.]com[.]br

创建的文件和/或目录
- C:\Users\ADMINI~1\AppData\Local\Temp.exe
- C:\Users\ADMINI~1\AppData\Local\Temp\S5c.vbs

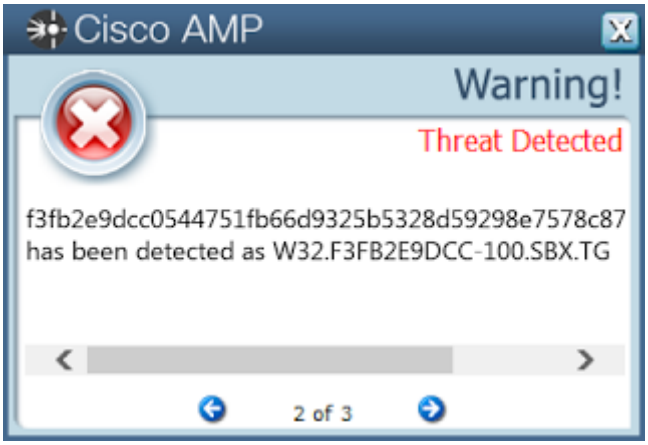
文件散列值
- 0b8bcc0c7281c9ad5e2c03b08c881b48015d064906deeccbe7bf944f4ef6d532
- 1e2833b296489c39f605de502f5c9527270f1a55ce5d0d8ed4453b299ea5840f
- 4d9f3de7aeca86a1ba1a653e04994eb69d31c6afc5802691ee9178bf8d593ed5
- 7372b2b16620b1a35fa83f4bd31af1f78fbb3fe7d3235b06c064c4d617461f69
- 7684aa4355b4992a8e168956e54424f03acca1cab32d0c62a4c87e6b5522d991
- 7c056f1a930943cd3afcba96555185cb598210f96c1b098b321a6e7d087599a8
- bac652b6a5cb65db95afdd9628c389f34c0e5609ed60d96f5598e43ebb151b73
- dd8bd175e95c9bdc963f6b7a188f9a0e4184411097123e2bb76111c9550b12dd
- e849be0adc49da7cc9b82c7a6ab45a0d082302dddd33c7c04824d14f968ba2cd
- ecdeeda6b71b88d0367bfb63291afe5ab5e34a5a43244791604c28d43323f59a
- f1231de08447a85356afedfdad5262e7ebba32bc68d23e73e5385164caf2182b
- f3fb2e9dcc0544751fb66d9325b5328d59298e7578c877924bc26944cbadb078

防护

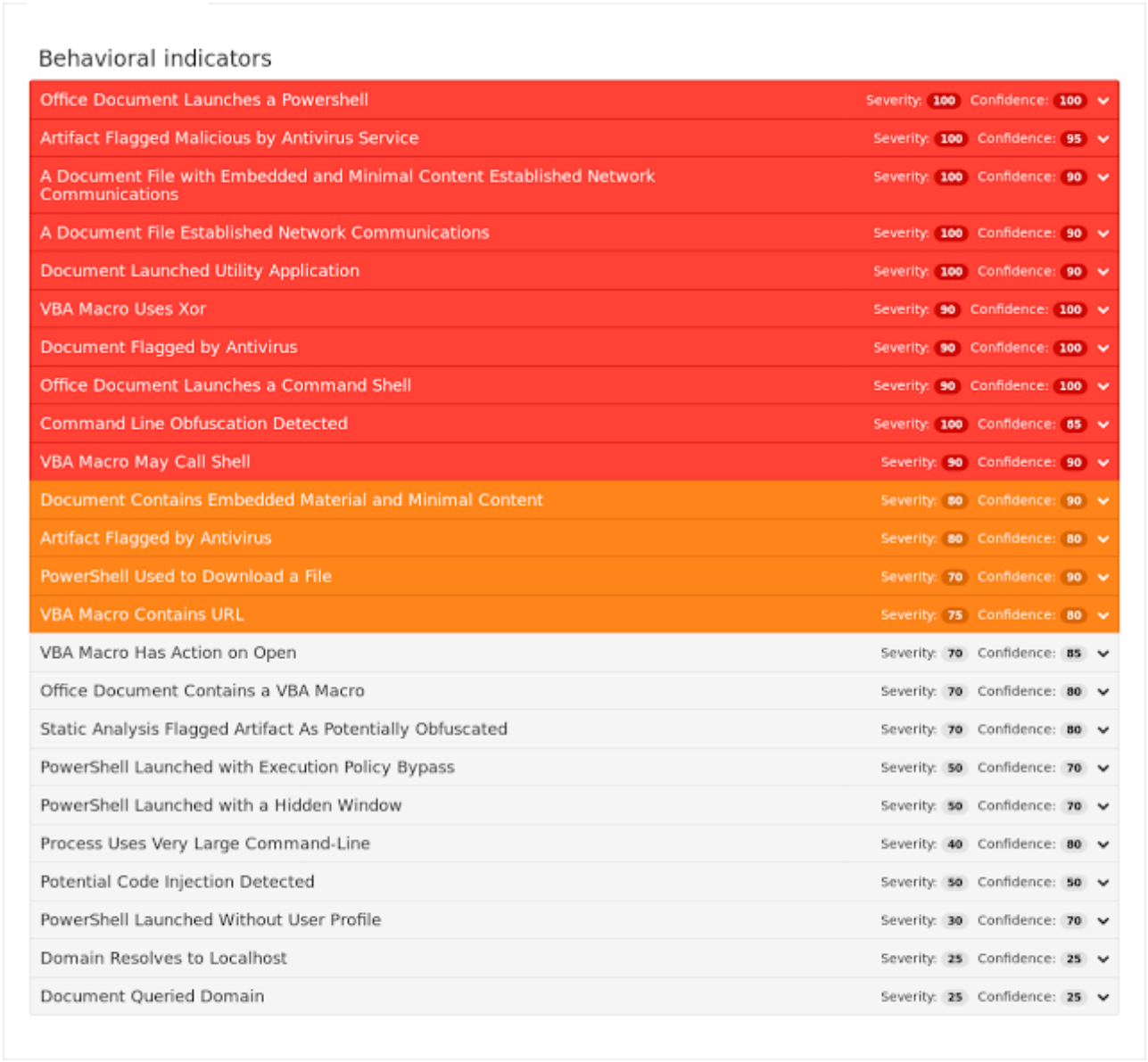
产品	保护
AMP	✔
CWS	不适用
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	不适用

检测结果屏幕截图

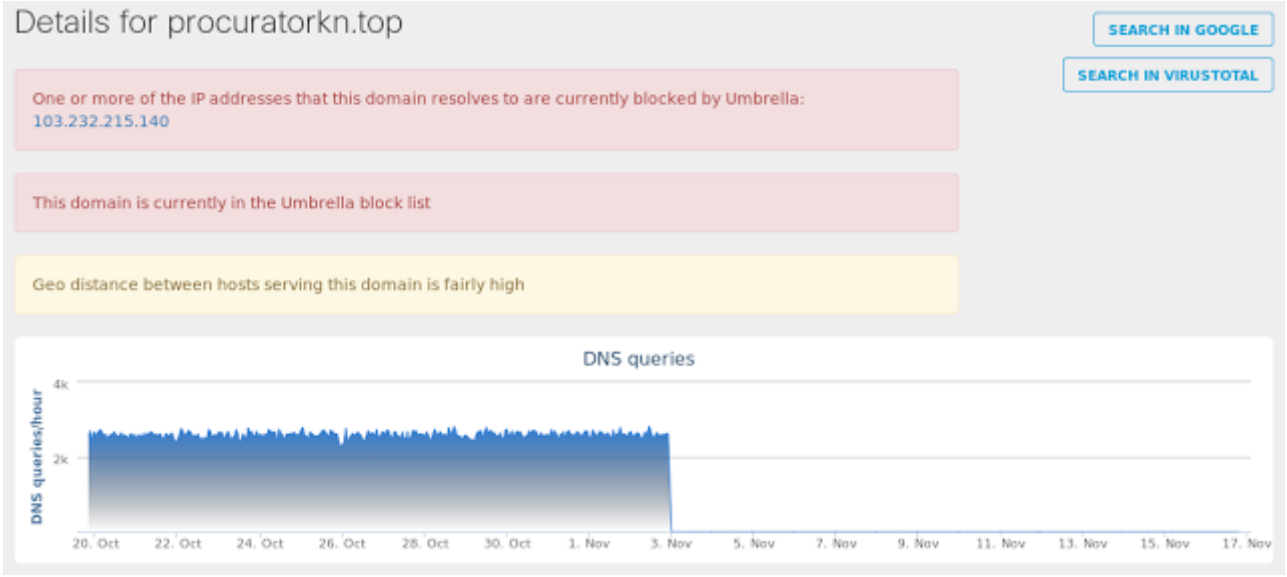
AMP



ThreatGrid


Behavioral indicators
Office Document Launches a Powershell Severity: 100 Confidence: 100
Artifact Flagged Malicious by Antivirus Service Severity: 100 Confidence: 95
A Document File with Embedded and Minimal Content Established Network Communications Severity: 100 Confidence: 90
A Document File Established Network Communications Severity: 100 Confidence: 90
Document Launched Utility Application Severity: 100 Confidence: 90
VBA Macro Uses Xor Severity: 90 Confidence: 100
Document Flagged by Antivirus Severity: 90 Confidence: 100
Office Document Launches a Command Shell Severity: 90 Confidence: 100
Command Line Obfuscation Detected Severity: 100 Confidence: 85
VBA Macro May Call Shell Severity: 90 Confidence: 90
Document Contains Embedded Material and Minimal Content Severity: 80 Confidence: 90
Artifact Flagged by Antivirus Severity: 80 Confidence: 80
PowerShell Used to Download a File Severity: 70 Confidence: 90
VBA Macro Contains URL Severity: 75 Confidence: 80
VBA Macro Has Action on Open Severity: 70 Confidence: 85
Office Document Contains a VBA Macro Severity: 70 Confidence: 80
Static Analysis Flagged Artifact As Potentially Obfuscated Severity: 70 Confidence: 80
PowerShell Launched with Execution Policy Bypass Severity: 50 Confidence: 70
PowerShell Launched with a Hidden Window Severity: 50 Confidence: 70
Process Uses Very Large Command-Line Severity: 40 Confidence: 80
Potential Code Injection Detected Severity: 50 Confidence: 50
PowerShell Launched Without User Profile Severity: 30 Confidence: 70
Domain Resolves to Localhost Severity: 25 Confidence: 25
Document Queried Domain Severity: 25 Confidence: 25

Umbrella



Doc.Macro.Emotet-6374344-0

感染指标

注册表项

- 不适用

互斥体

- MC8D2645C
- MF349C666
- Global\I98B68E3C
- Global\M98B68E3C
- M167D3CCB

IP 地址

- 77[.]220[.]64[.]49
- 45[.]73[.]17[.]164
- 103[.]247[.]96[.]21
- 195[.]16[.]207[.]211
- 148[.]251[.]33[.]195
- 213[.]192[.]1[.]170

- 95[.]163[.]86[.]154
- 5[.]63[.]14[.]41
- 78[.]47[.]56[.]164

域名

- liansamaneh[.]ir
- conceptttb[.]in

创建的文件和/或目录

- \Users\Administrator\Documents\20171117\PowerShell_transcript.PC.w9wNiwMK.20171117113000.txt

文件散列值

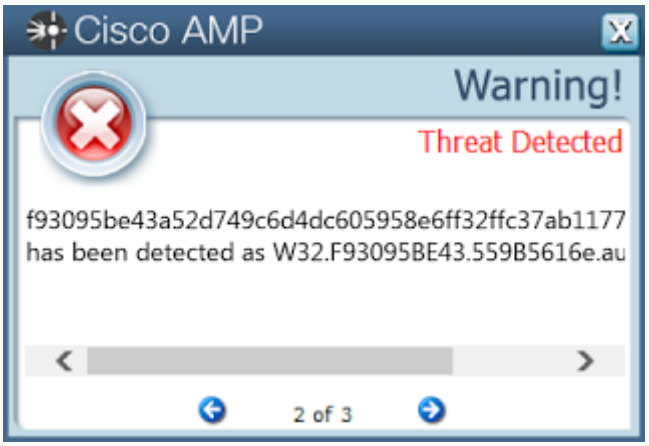
- f93095be43a52d749c6d4dc605958e6ff32ffc37ab117734c61deebbee0fdc28
- 6d0d7e3180a65517917e9d46f13a0ab6d54bc194edc950130aff9f3bec564d95
- 201e15ced36c0840b80fc6bb314b404868988155920a19098fb815e4b391f352
- a2bf120258c17c7153f7b05cc8cb8d74bd10645b472a18bc75dca1f04ae5cff1
- 6e999d2626bb074d7f5df5b97cdd8b21faa050233b608d4d8395ab941569cd50
- 81425c15025f0fe9f4314c0130b00fd974f4522eb622f030f613e7940111f8bf
- 04745cf34ca1dbfee1b638d41675e1ccf6ed65059f839ed8734f34f14b989ee6
- 7cca822e0fdfeca033762213bf16a3f04d7cac8c345f84a0d740324d97f671c0
- 9ce688608f54dcedd2497715359c9b19b0c5fc7e5ce441c55f897082b9f1ccae
- f5142c005f1ebd6c1769b77d58e3614cd9d7bfa28cfcbd64660ef73e392ecd09
- 3b5df8063fa79a19c231b8d019e150a1821d6ecbf27855ba4aef4bfb3c0f0d77

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	✔

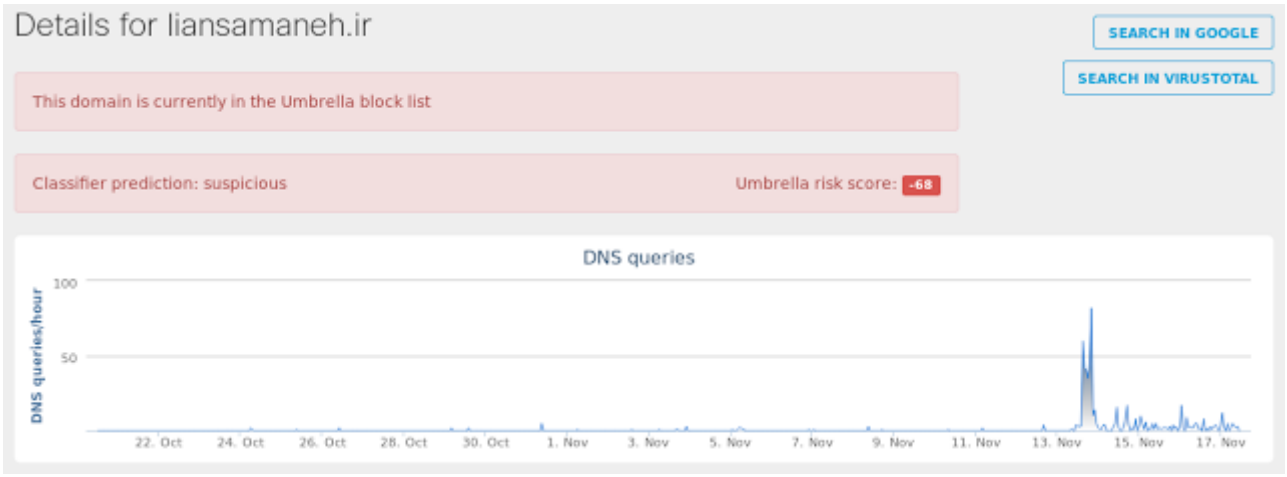
检测结果屏幕截图

AMP



ThreatGrid

Umbrella



Win.Ransomware.Kovter-6376319-1

感染指标

注册表项

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

互斥体

- Global\M98B68E3C
- MC8D2645C
- MA008EE15
- Global\I98B68E3C
- M772FF100

IP 地址

- 77[.]220[.]64[.]57
- 185[.]94[.]252[.]102

- 213[.]192[.]1[.]170
- 78[.]47[.]56[.]190

域名

- 不适用

创建的文件和/或目录

- 不适用

文件散列值

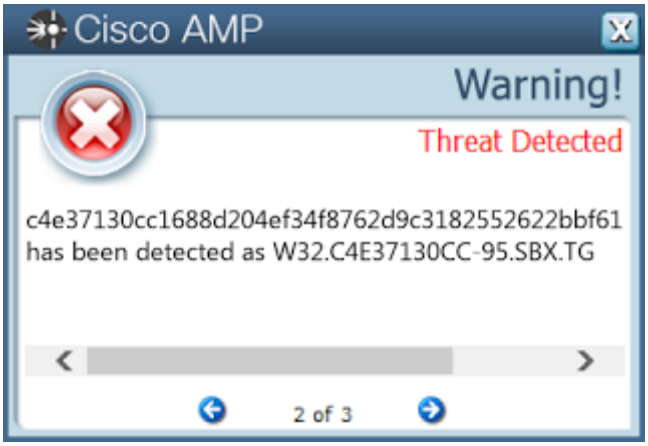
- c4e37130cc1688d204ef34f8762d9c3182552622bbf61b127b22c0b733a3b700
- da973bebb2c14bcd3f493ffc1cc2cd6225f3b49fe77c1189de35f2dcfa72bbf8
- fa0577e117929e21a3881b615a0a3cb087f5bbda6628b7612f036d0753c1b24b
- 36d5cee0fd6862ae64e0074e12ca1599be7953d7cdfa93ca3993c5f83c9cf1b2
- b0d41c21e5d8396f711e1224f190b3281bb04d3f797ceb9c77558a5f567e3fe4
- 6e445be806032f4a73d17d73cb00639f632b23f2731ac0c2267a4bb34237fd32
- cc714cbf5aac23f09bcc9eea1b8577d2e1673d9fe1433f5658eecc818a2f8469
- be11330dfb54a48734679f458381d69059c037bd45deb69f70148f9c2e36fc0d
- e0467fca9d07a69a53cb436d7962499bc25be34295dacf5a5d19ae9596ad2d98
- 468fdeeba11609d222b9554616dcb8b1ab10f565dcb6291bc5360dda3a97ab08

防护

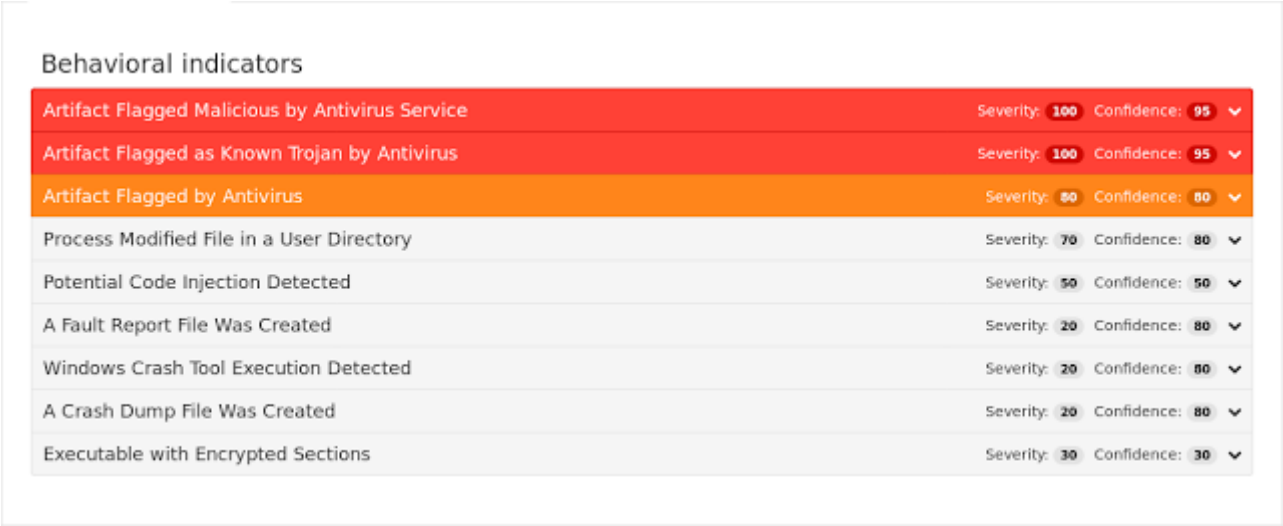
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Win.Trojan.BitCoinMiner-6374577-0

感染指标

注册表项

- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{36B75FF8-A007-46F0-8EEE-76A6D3513381}**
  - **值：**Path

- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\COMPATIBILITYADAPTER\SIGNATURES**
  - **值：**winupdate.job.fp
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\COMPATIBILITYADAPTER\SIGNATURES**
  - **值：**TB_DEADLINE_START.job
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{6C1DC24A-11D8-4DD7-A934-6C033C5CB501}**
  - **值：**DynamicInfo
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{36B75FF8-A007-46F0-8EEE-76A6D3513381}**
  - **值：**DynamicInfo
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\TB_DEADLINE_START**
  - **值：**Index
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\WINUPDATE**
  - **值：**Index
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{36B75FF8-A007-46F0-8EEE-76A6D3513381}**
  - **值：**Hash
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\COMPATIBILITYADAPTER\SIGNATURES**
  - **值：**TB_DEADLINE_START.job.fp
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{6C1DC24A-11D8-4DD7-A934-6C033C5CB501}**
  - **值：**Path
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\TB_DEADLINE_START**
  - **值：**Id
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\COMPATIBILITYADAPTER\SIGNATURES**
  - **值：**winupdate.job
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{6C1DC24A-11D8-4DD7-A934-6C033C5CB501}**
  - **值：**Triggers

- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\WINUPDATE**
  - **值：**Id
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{6C1DC24A-11D8-4DD7-A934-6C033C5CB501}**
  - **值：**Hash
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{36B75FF8-A007-46F0-8EEE-76A6D3513381}**
  - **值：**Triggers

互斥体

- Local\MSCTF.Asm.MutexDefault1

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- %System32%\winupdate.xml
- %System32%\Tasks\winupdate
- \TEMP\fdfe3ab063fd7dad96a6492cc1b7f43c169e270868a3541a89e177b8dacaf16b.exe
- %System32%\cudart32_80.dll
- %System32%\wsus.exe
- %System32%\cudart64_80.dll
- %System32%\config\TxR\{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
- %System32%\Tasks\TB_DEADLINE_START
- %System32%\TB_DEADLINE_START.XML

文件散列值

- fdfe3ab063fd7dad96a6492cc1b7f43c169e270868a3541a89e177b8dacaf16b
- 3df78335904328db44168cfda613d0aff3761b6d767824476c6d34b582bf7a73
- 82bbc279515e29a63b38752d3532e6f9e5e36ffb6b4f1dd783c370eb68667b76
- 019538248027b51c92cef1cc2e8cff4577c30508e0aa06a65adfdcc125c6846c
- 0487114a1df2852b2f3ba69aaa49930055e04c81ffc1e68dad6b47bec7ba2faa
- 0e92444bdc28dbd0e645cedb0c7f1d81708e2073b7c7567956b7bc665cb6b648
- 1814256a36032c226ddd8263395ecbe6fad92b4b11e62120ee4d35354cb670fe
- 1a736b816b476800c1adb87169100192e503a1737ebedef5b1f14d695a100011
- 293548f39cdaeac4d59fb55efbce7ac214349aa5ae46df0f905a0ab5cc1ae5ee
- 29b4419555c41019e98c3a0e5ffa69733b9a1d71d48f0b9879a21581ab548c1e

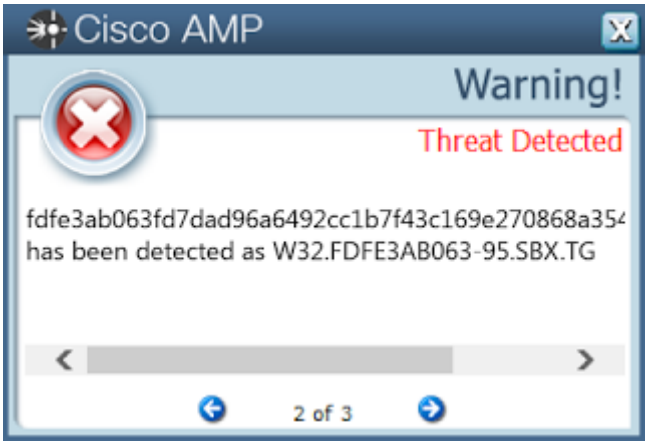
- 314fa254bd1da034501300e8766d000aa0ab306bbd19f42e243f9d2370473712
- 3bcd92e4b5d1961e6b85f140d83698c37f0eba71993e41fc62c80a32e1a091c2
- 3daa009acb66af54564e8dd02da9f2ec1fbebb8c86382c461600cca5ca63ce20
- 459a5346ac350d03b7e5fd5b9882afee243f2d1f838ead99ab06a2cde783c522
- 5927953796300be0c5778fc9e9d6bb52a8640f33cae1c684d5225eed327d547d
- 63544397a0cfbf53588ad8792a870e6b7ff2fa0cf16dc6a3796a3ea4805776d6
- 714069902c8b82e636cda415148847f5867a32706eaf4a3a04fcb0efac7cc03a
- 7a6d865285069c90fcf5b8b3671b6daa7c9e6a9e39a37d4854ab630c6f094178
- 7b4fbaabf1374e4f6c817f0ed5a359f65eabbda7cbd970cb427d57a8a44773d6
- 7f783789ba87d344bf6450be97b0466c9b73e8cd1d320c08df8cb3636f09fbff
- 84dd02debbf2b0c5ed7eebf813305543265e34ec98635139787bf8b882e7c7b4
- 9d6b9fa1861b72f348a4fa8b209eb7f40f4a497bcf98204ba5fd389f7fa82b93
- 9dd467e34763c06e251c25d5c679e291030564a0b95b6a23a35bbe5a86889c01
- a23bdb4e3973bc0a4e746038df90e5834efbd521a59df4d488f226a956144da5
- a3d46a4fb9c6fa286c5dec80dd70a43c9ad70770b5d1540dea13e16b15d2ad26
- aecfcd163d2665720b7b63288b6964dcab57960c2c3cd77e7674445c282c3188
- bc9a756357e8a0d29931d1d9ec1747bb73855cdac99021abe99b444e5332a749
- cc9e68134aab06089ec5b7404d5b54c572b56b04e61053d068cc8b4e67625cce
- e9a76ace7562d53aaa889caf517b827427162f8512c01ced0657cb08df4121f2
- ed78e63401ee4290fb334cb0b159b1e94d86de345706f4fc30a4c1df0bd606f7
- f26e6efc015b0dc9982b88fa02e3f2b2601173aaa300feb558104ef453c94941
- ee4a6876f192c6a43f1475fbe16e4c4315282e2bc9165ba4dcdf45f07275ec0d
- cc075ad3073992532759ac2a31b3c57e25bd3a24f1d5a35958d25afa703d7b26
- 02ec6e8adf56df5bb0cda19ddd04327658c36d493c6cbe6fba42ab0f25034c88
- f5b88f4034f9c1e0c2f246b8dc21f7fd875638aba63c133f925b8a03b7078657
- 3ca1fc58bbe212f901523f9ba8800a8bcc47cd054f0648a571abda66c2cbc9c7
- 2888cc28bac5a432b2a819e08420e8f7e59f28d56ce8168c5865e6c3cd875776
- de7d4019549e2f018789c902afe9552bd9127328dc439bbe59d8b79a8565569c
- 70de06f4911513162eb141787027f2cbe463e4382905e80724ad52ca6bae17bb

防护

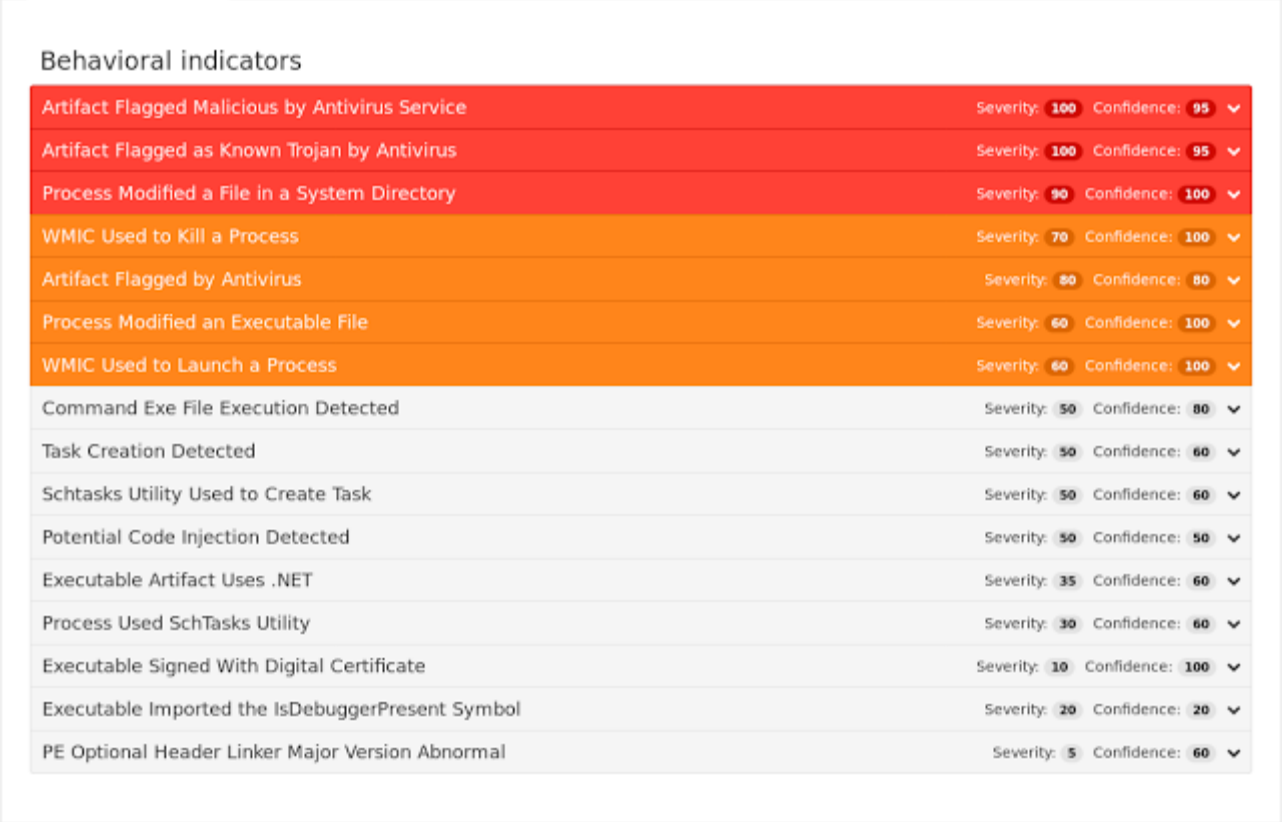
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Win.Trojan.CosmicDuke-6376318-0

感染指标

注册表项
- 不适用

互斥体
- Local\MSCTF.Asm.MutexDefault1

IP 地址
- 不适用

域名
- 不适用

创建的文件和/或目录
- %WinDir%\SoftwareDistribution\DataStore\Logs\tmp.edb
- \EVENTLOG

- %WinDir%\SoftwareDistribution\DataStore\DataStore.edb
- %WinDir%\WindowsUpdate.log

文件散列值

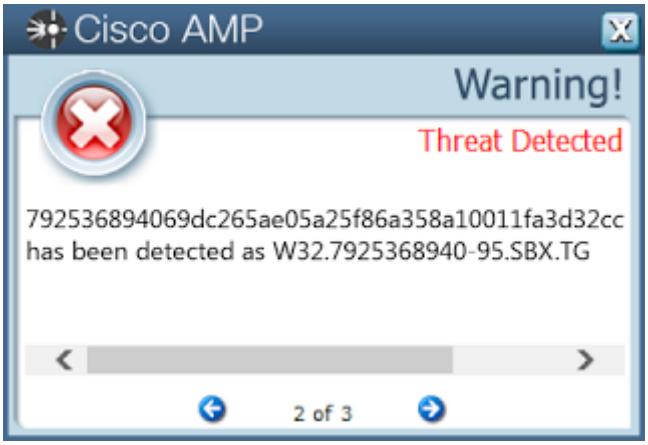
- 792536894069dc265ae05a25f86a358a10011fa3d32ccf972e5867f862997925
- 496220acf4b44f5564898533636dc3f19304d86ef7d223fbeedfb858e1570fd3
- 457bd4b9ad2c422f91fc5bcf74c52d392d32ace50f244d1beb624f42eebbaec8
- eababe6f24e25622d795bde97ccfc32c51c1d0ee346a3c345f26b8e191d54664
- 98e5bc8b136f2aafc7b46308f71ceeb675f057f3220a44e90e7498e226d746d3

防护

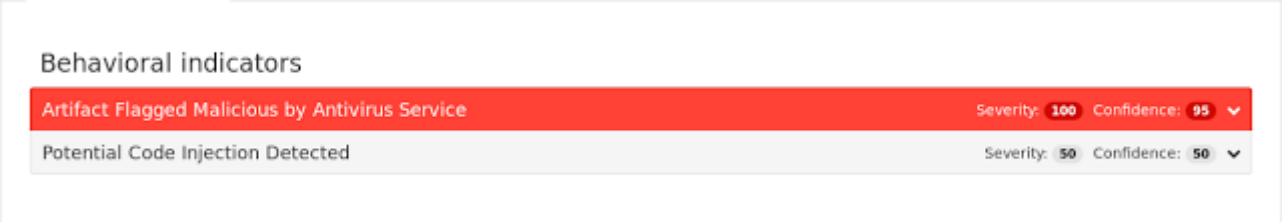
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Win.Trojan.MSILTrojan-6376261-0

感染指标

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 40[.]97[.]169[.]146
- 40[.]97[.]120[.]66
- 40[.]97[.]120[.]226
- 40[.]97[.]113[.]162
- 40[.]97[.]24[.]2
- 91[.]198[.]22[.]70
- 40[.]97[.]145[.]146
- 40[.]97[.]142[.]210
- 40[.]97[.]170[.]2
- 216[.]146[.]43[.]71
- 216[.]146[.]43[.]70
- 40[.]97[.]49[.]18
- 216[.]146[.]38[.]70
- 40[.]97[.]85[.]34

域名

- outlook-nameast2[.]office365[.]com
- checkip[.]dyndns[.]com

- smtp[.]live[.]com
- checkip[.]dyndns[.]org

创建的文件和/或目录

- %AppData%\ScreenShot\screen.jpeg

文件散列值

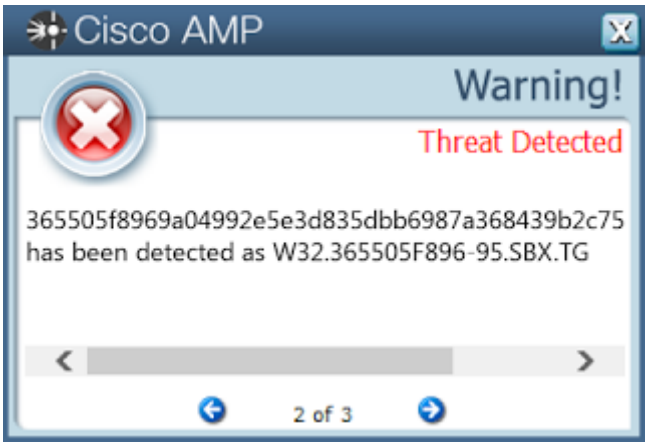
- 365505f8969a04992e5e3d835dbb6987a368439b2c757c24e59dc6daa13d60e6
- 47c364ac3d539ac0874e66b3f7cb0c5a87e3c67323156b082575fc926d1ecb13
- 6707d3ed970ced8091d64bbd0bc742e2d4d8f192e1e6c64ee9037451c04bca13
- 987cdbc17259f87a9e6b04c1d6c3c971f23c380f7da1a0d93ff79584230e5b7c
- b793ca990b4ebad46758253f8b3065334f923a7c077ce57c3b71308b6bd38422
- c78b70c786d299ecb97021fa4b989455852084ec3afc45f6e348a8a0489263df
- db8c2fa78a2751bafd2d1a95f778a725735d42854c901e42976d1599f75deef5

防护

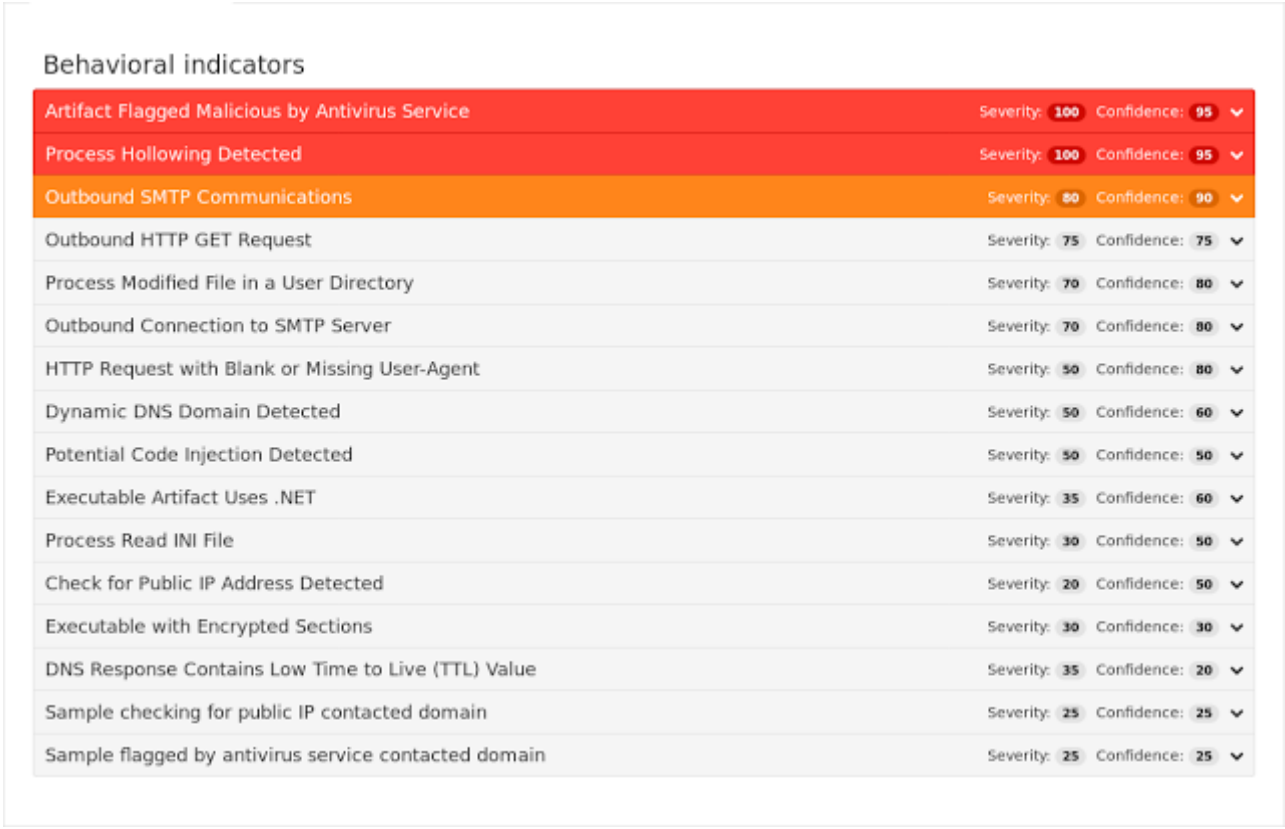
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



发布者：EDMUND BRUMAGHIN；发布时间：11:07

标签：恶意软件、威胁、威胁综述