2017 年 7 月 7 日，星期五

一周威胁综述（6 月 30 日至 7 月 7 日）

本文概括介绍 Talos 在 6 月 30 日至 7 月 7 日观察到的最常见威胁。与之前的威胁聚焦一样，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 FireSIGHT 管理中心、Snort.org 或 ClamAV.net。

本周最常见的威胁包括：

- **Doc.Downloader.Generic-6332126-0**
  下载程序
  这种文档下载程序是在跟踪 Zbot 下载程序中的线索后发现的。它们依靠对 OOXML 格式的轻微混淆发动攻击，OOXML 格式在 Microsoft Word 中仍能成功加载，但是在特定沙盒环境中会阻止成功运行。这种下载程序还依赖于样本本身包含的 CDF 二进制文件内极易混淆的 JS 编码。大多数样本依靠重复使用十六进制字符串组合，进一步阻止对代码进行静态分析。

- **Doc.Dropper.Agent-6332127-0**
  Office 宏下载程序
  这是一种具有混淆性的 Office 宏下载程序，可利用 Powershell 下载恶意可执行文件负载。目前无法解析这些样本尝试执行下一阶段下载的主机。

- **Doc.Macro.Obfuscation-6331107-0**
  Office 宏
  恶意软件编写者将试图混淆 Office 文档中保存的宏代码来阻止检测或从表面上隐藏代码的意图。该签名会检测最近广泛使用的一种技术，通过使用大量算术运算来隐藏代码。

- **Win.Phishing.NikoLata-6332081-0**
  Web 诈骗网络钓鱼
  NikoLata 应用可反复将打开的浏览器窗口重定向到攻击者恶意控制的 http://bigpicturepop[.]com/redirect/57a764d042bf8 on the benign site bigpicturepop[.]com 站点。我们发现这些重定向会解析到色情站点、多个技术诈骗站点和其他站点。

- **Win.Ransomware.Nyetya-6331387-0**
  勒索软件
  Nyetya 是一种蠕虫病毒破坏性恶意软件，通过利用 EternalBlue 和 EternalRomance 的 Psexec、WMI 和 SMB 进行传播。有关该威胁的更多信息，请参阅我们的博文：

http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html 和 http://blog.talosintelligence.com/2017/07/the-medoc-connection.html。

- **Win.Trojan.Fileinfector-67**
  蠕虫病毒
  Win.Trojan.Fileinfector-67 是一种文件感染病毒，通过将其代码注入文件系统中任意类型的文件进行传播。

- **Win.Trojan.Fynloski-6332091-0**
  木马病毒
  Fynloski 是一种木马病毒，可用于将其他恶意软件分发到受感染的计算机。这些样本是自解压 cab 存档，并且释放的二进制文件会继续产生混淆。实际编码以 mov 指令解包在堆栈上。

- **Win.Trojan.Siggen-6261194-0**
  木马
  这是一种 .Net 恶意软件，其中包含反侦测虚拟环境技术。如果受害者计算机有网络连接并且不是经过检测的环境，则该木马可将自己注入另一个程序并尝试与 CnC 服务器通信，

威胁
Doc.Downloader.Generic-6332126-0

感染指标

注册表键
- 不适用

互斥体
- Local\10MU_ACBPIDS_S-1-5-5-0-61147
- Local\10MU_ACBPIDS_S-1-5-5-0-58021
- \Sessions\1\BaseNamedObjects\Local\10MU_ACBPIDS_S-1-5-5-0-59580

IP 地址
- 119[.]28[.]71[.]78
- 109[.]86[.]76[.]58
- 37[.]115[.]165[.]159

域名
- hoefnen[.]xyz
- berasadot[.]top
- bagrati[.]top
- page[.]numberx[.]org
- au[.]forestllc[.]org

创建的文件和/或目录

- %TEMP%\iio322171.uu
- %AppData%\Microsoft\Windows\Temporary Internet Files\Content.IE5\7N5LGTOO\lsmkk2[1].exe
- %AppData%\Microsoft\Office\Recent\account_3166.LNK
- %AppData%\Microsoft\Office\Recent\statement_d0bwfa.LNK
- %AppData%\Microsoft\Templates\~$Normal.dotm

文件散列值

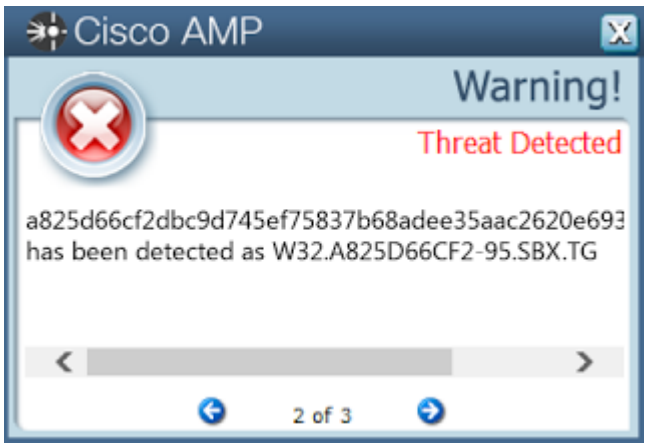
- a825d66cf2dbc9d745ef75837b68adee35aac2620e6933876d7662bf1f815a90
- ed62f5e6c396940a455a82a7a1864ac696fb00e576631b3293ec53bb4292700d
- 5788dbf3fef2fbf8f4dbe3edfe8ddc955c9741f6d7287f5d7427d0df53275108
- e2c4800a2a925ef71fe173269fe237bd2a43706e897c2de59f96ad5064a2389e
- bf544987ac6ee03cb089d54fac8c885bb4c02ef709576f46890d51335a15bef1
- 542abc75b0bba97deafa82b3424afb98beee71d71599345e659038a7dc969219

防护

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

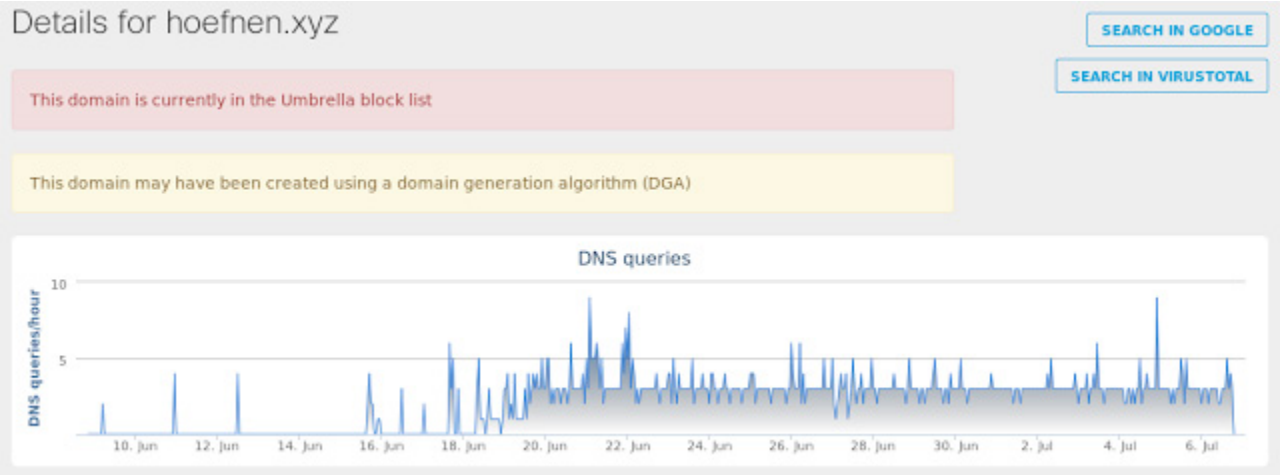
检测结果屏幕截图

AMP



ThreatGrid

Umbrella



屏幕截图


Please enable editing mode to view included documents.
SECURED BY RSA-4096
ENCRYPTED MESSAGE
This file is protected with RSA KEY.
To see this document you need to import key chain on your system. Please, double click on the icon below to start the import process immediately.
The file was generated by Microsoft Office SecurePoint on Feb 21, 2017.
RSA PROTECTED BLOCK
END PROTECTED BLOCK
Open Package Contents - Security Warning
Do you want to open this file?
Name: EF21H-1.js
Publisher: Unknown Publisher
Type: JavaScript File
Open
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?
Double-click or double-tap to edit OLE Package
Type here to search
6:04 PM
7/6/2017

Doc.Dropper.Agent-6332127-0

感染指标

注册表键

- 不适用

互斥体

- 不适用

IP 地址

- 77[.]123[.]218[.]185

域名

- aninasmeesmase[.]com
- iitttyense[.]com
- monenanshca[.]com
- onasnenekaskeeee[.]com
- iianem[.]com
- mmmzmzlll[.]com
- oppasnndnew[.]com
- tranasportnmme[.]com
- uuunasn[.]com

创建的文件和/或目录

- \TEMP\request.doc
- \TEMP\~$equest.doc
- \Documents and Settings\Administrator\Recent\request.lnk
- %AppData%\alnyliz.exe

文件散列值

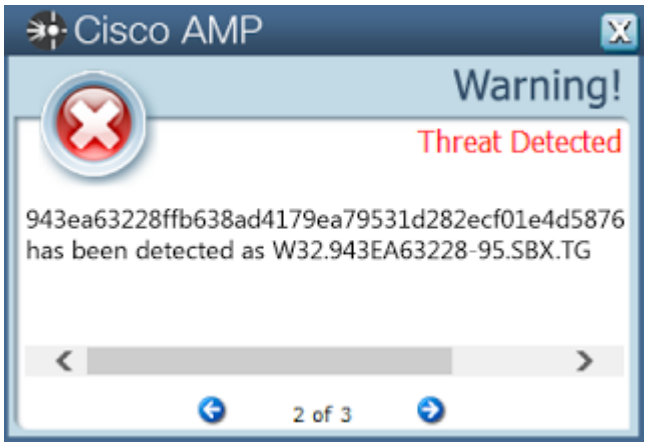
- 17d6dc47409d9a49ff9e0af92088213e1fe7d8cac1f69d73892d229b76395c43
- 4daaadac1d8dfa337f8e13cff2e3af24cbe6aa97877f3cec1e140507e9f20f19
- 53e6613c677e5498367a85b43569c81fd4d6d8c211ace257749a7c4f49bdf632
- 8f6515daea52d6b0e02b113f0357801d55f7d74dc113ab76055ad835ede11002
- 943ea63228ffb638ad4179ea79531d282ecf01e4d58764eb7bb0c3329a82b1ea
- 97597a498ab5b13b1fe3cb52e41eee108d91364b31895f896c884c36e28e0d59
- a0ccac6ea86fcdbae485abbf7f4374591ae4617cc78b09cb2e13657ad45a9b7e
- dad0a717b8fe07b9fc60d7a31deff159814c1c33702256a23e882bac0b50e94a
- df159704ed213a2f6ebf4087006acd2502aecc586b6828ae5222688cf9c20745

防护

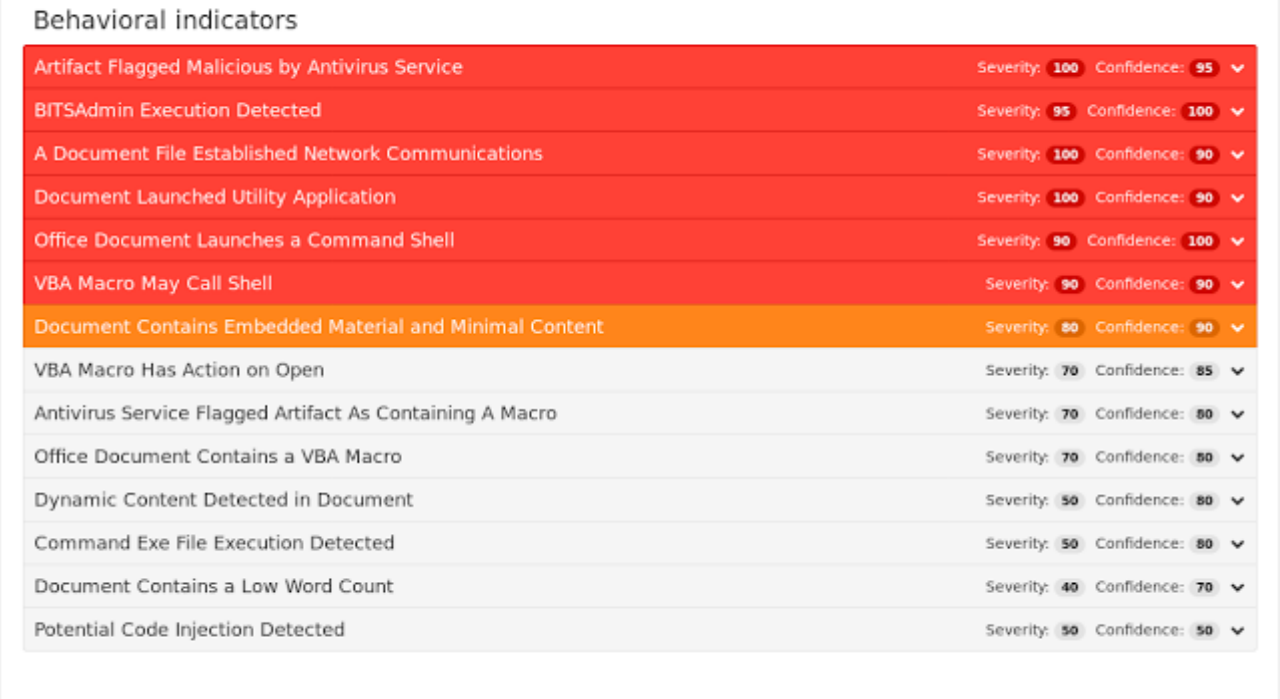
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

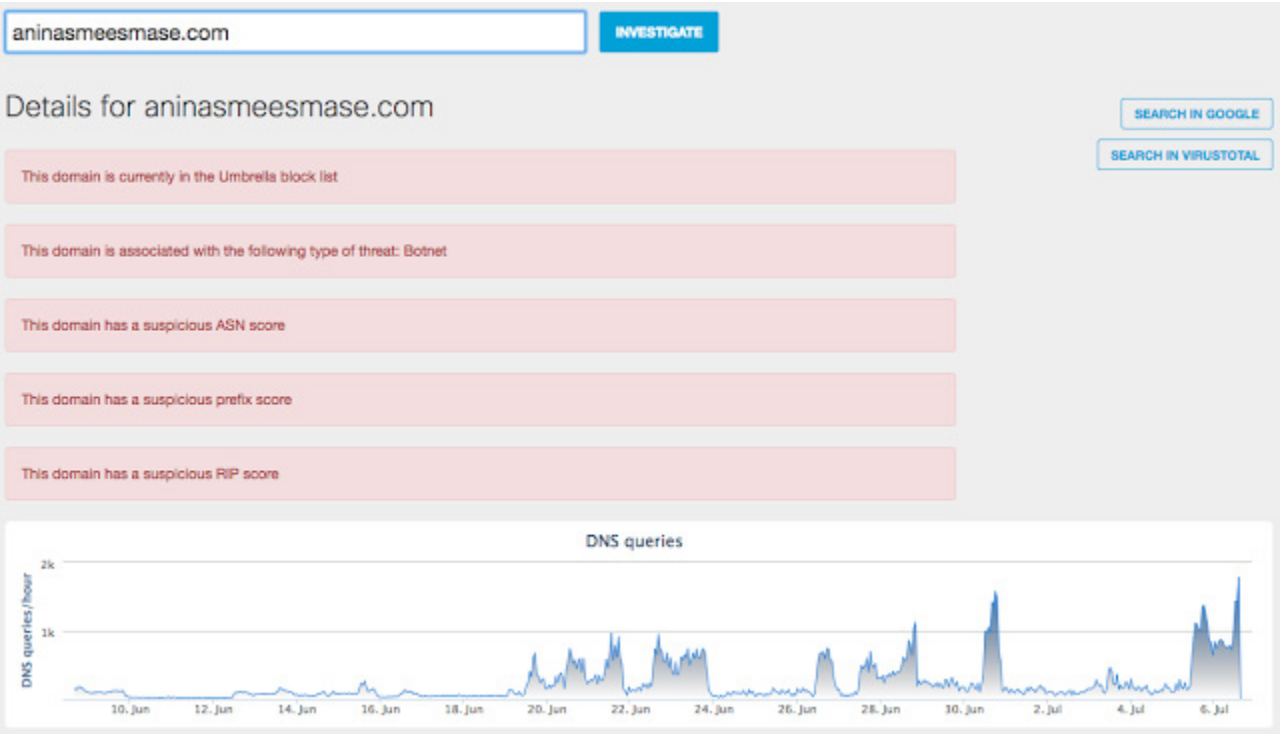
AMP



ThreatGrid



Umbrella



Doc.Macro.Obfuscation-6331107-0

感染指标

注册表键
- 不适用

互斥体
- 不适用

IP 地址
- 185[.]165[.]29[.]36

域名
- 不适用

创建的文件和/或目录
- \Users\Administrator\Documents\20170705\PowerShell_transcript.PC.0WdK03OL.20170705095145.txt

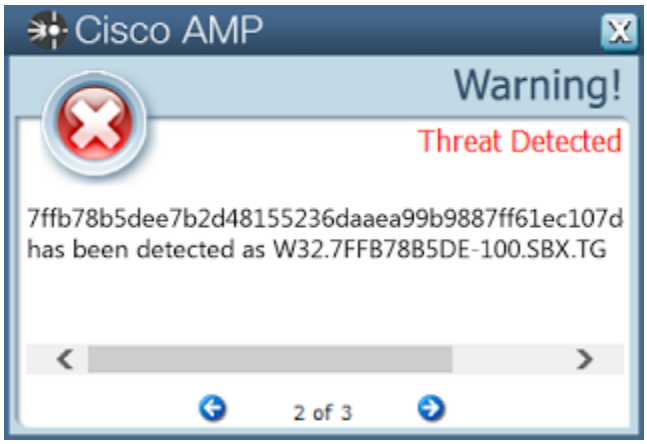
文件散列值
- 7ffb78b5dee7b2d48155236daaea99b9887ff61ec107d48a2522c951795f3353
- af89ebcecc2478cb5f90696aa75aaa3dca27c4928265b4b6833e95b5672d7a0a
- 1a3bd5acc39ff619417fc217786f8b6338348a1f5eda994cbd03a5d014d351b8
- 8db59629e0b972ca9aa4da3dd56278340dc1f4ad7849e536bd2a1dc2c8ec59ff
- 1e56463b3aebc9fdf435ca3910a7db4e5a1c9f7b6568da5ced62b2451345eb68
- 0696df98c9074fc4c05454149e9a9ce7f3bfec9d19852691a49919027aa2be05
- 01d024ae353d2c4349fb13bfff1417e77ee2f85c75834f91762f80ca1d25a0c9
- f38d35b8be18d3efe2394929184ad41e9e7c1f699bbc5cdebc4783b159075c66
- c5ceecdc491077b8db797d1c65eed03efed8ea28cd0ee5d0926e3fa591920426
- 441e093374df7b806bf883d564810c8733b5f664add7baa4a8b7df6c49b04dcf
- 403589bd4b2c275564aac4382800eaf5836ff61817ddb76afb9b7c7f24b0c0e9
- ef4685089d285ce677bc2aa2f2490dd25120d2af19fb6d2570adb03f0a5a3e7a
- 1d7bd5817b240a053cac0c6b3af1d848ed4b03e6bd334bd2e040800215d8d601
- dc4c028949fdd43c7d67fe085e4c85a62633a38e49a510e71d41270008fd29fa
- c07cdfd59b7ea1bdd2a6e267df60300bf23b1888f0582ef050946d0cba571f08
- 6cea69fa05cbf2a0db2ca40684ccbf3e4ea4744f5f6ae27655871d35cc6c85bd
- ec988f1b09c617c1b609e25aea76e7afa871bb2188accd75f3dd24d0834c5c47
- 29013332f09195261f8be7fd43674e4e5132a28744ed52a45d787646a6e8659f
- c30d4d4b41d7f690762ef26ffdbf14c7eff7ce92e7b8cfa87f5182bb057f05a2
- ee97cf5279ca40e5e3d879f4a8e0fdec6b3a5fb7547ece74252c72419df0a6fd
- 877107ecf0a698fad3a210289777dc647650c493f11cb384044a879efb3f16fb
- 123abdbf3c470dde32d7cbfa97e0393eaf602a3befa8050dfe8738a1c4b14768
- 124e908d1670ede9541b4f0ed6376dd03c62d1cf7b0ff22943a7fa3be90ce238
- ff7706bdd749accba1ea5c49903fb200af7fb3edf3e95d5f9686e78ec699847e
- 470918fd1ed47e4454af807c3b14b55314cb07a86d053ff83f3233628f08bd8e

防护

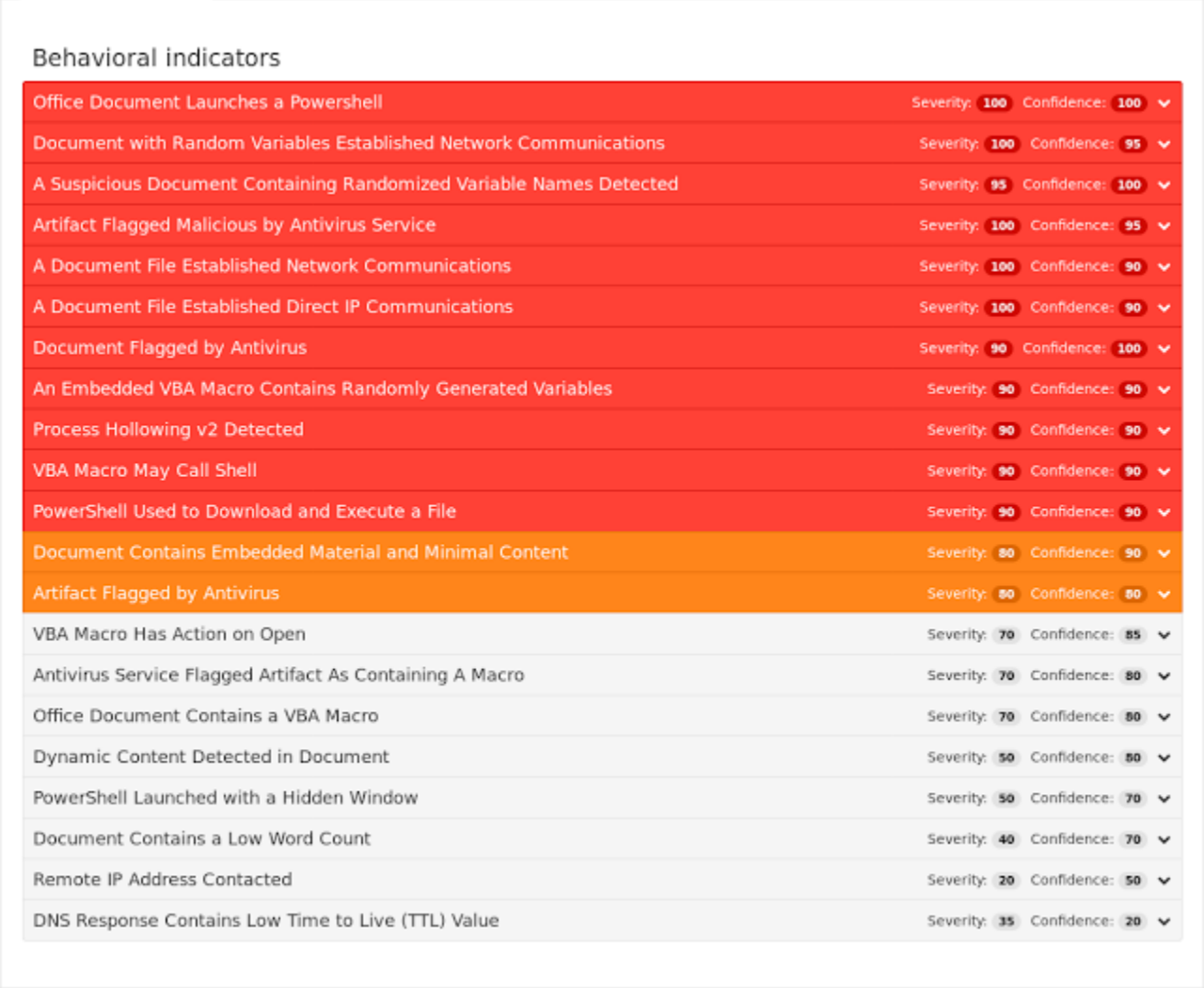
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

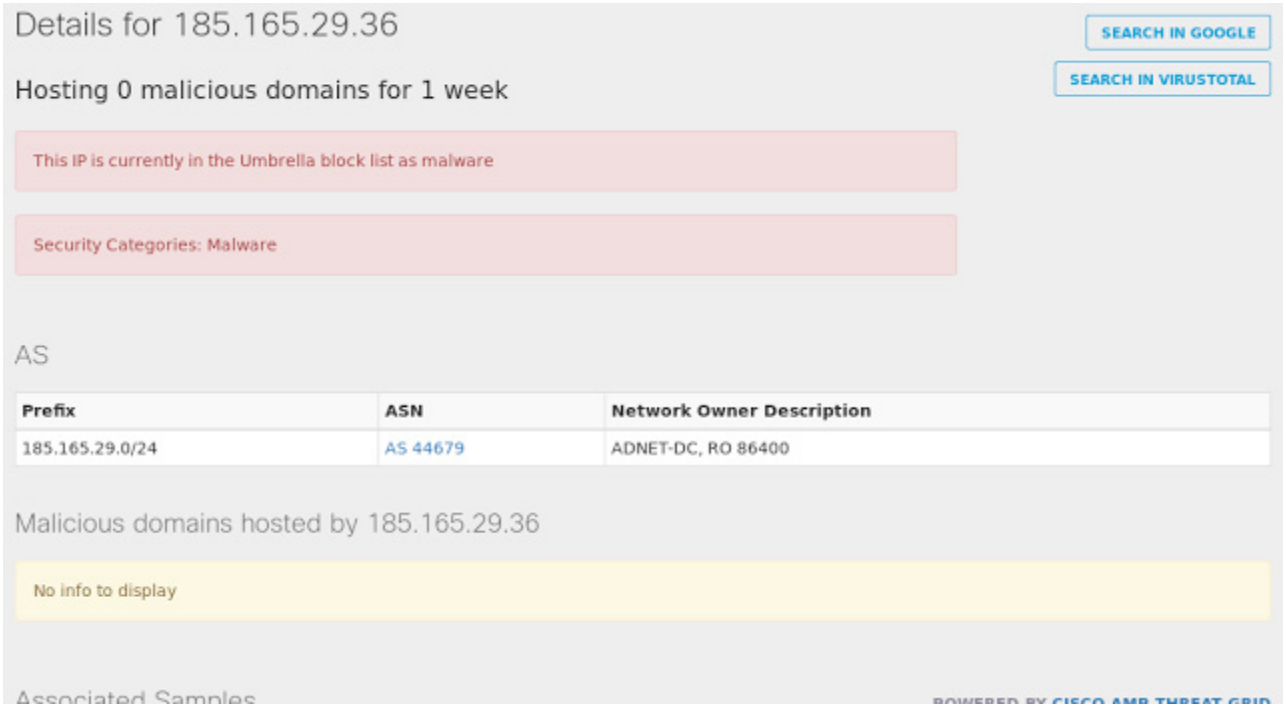
AMP



ThreatGrid


Behavioral indicators
Office Document Launches a Powershell Severity: 100 Confidence: 100
Document with Random Variables Established Network Communications Severity: 100 Confidence: 95
A Suspicious Document Containing Randomized Variable Names Detected Severity: 95 Confidence: 100
Artifact Flagged Malicious by Antivirus Service Severity: 100 Confidence: 95
A Document File Established Network Communications Severity: 100 Confidence: 90
A Document File Established Direct IP Communications Severity: 100 Confidence: 90
Document Flagged by Antivirus Severity: 90 Confidence: 100
An Embedded VBA Macro Contains Randomly Generated Variables Severity: 90 Confidence: 90
Process Hollowing v2 Detected Severity: 90 Confidence: 90
VBA Macro May Call Shell Severity: 90 Confidence: 90
PowerShell Used to Download and Execute a File Severity: 90 Confidence: 90
Document Contains Embedded Material and Minimal Content Severity: 80 Confidence: 90
Artifact Flagged by Antivirus Severity: 80 Confidence: 80
VBA Macro Has Action on Open Severity: 70 Confidence: 85
Antivirus Service Flagged Artifact As Containing A Macro Severity: 70 Confidence: 80
Office Document Contains a VBA Macro Severity: 70 Confidence: 80
Dynamic Content Detected in Document Severity: 50 Confidence: 80
PowerShell Launched with a Hidden Window Severity: 50 Confidence: 70
Document Contains a Low Word Count Severity: 40 Confidence: 70
Remote IP Address Contacted Severity: 20 Confidence: 50
DNS Response Contains Low Time to Live (TTL) Value Severity: 35 Confidence: 20

Umbrella



屏幕截图

Win.Phishing.NikoLata-6332081-0

感染指标

注册表键
- 不适用

互斥体
- 不适用

IP 地址
- 176[.]31[.]115[.]114

域名
- bigpicturepop[.]com

创建的文件和/或目录
- 不适用

文件散列值
- 0033e8aa040b150f10aae632940f5e975fdd8c9f3c50e3390655c4098a41a4a0
- 0899df6fe90b23914cf7bfaabf5b52eb61565f529006e1f8ae5c1c3603eb9120
- 0a222dac8daabd8f2ba8825519ad65916f88ad194caf3a0bde754cf49bc41699
- 102113176eeb0d8b170adda4fe1fc531d54bc8b8faa8aa0cbc8968acc478d2ee
- 237fdfef4a1dc47ebf3119ba0f16ea6f780acab50d964816f1d00c7340246366
- 338dcfc2a8933338210abb98144ec4d50907130b24c59b00307d1e37e89eeaab
- 34d135535a27eb46f4eefb5c62cf98f86a246cb1b8328206e300667e149d5e20
- 3727278e0326aa8726e8320d75b2224b601d575e49147befec4089fde72c8b6c
- 378be621adbd9655c1e8f439134b99da4eecddf41b09f3484496663cc2ea393f
- 3cb106ce8f4015abe7b2789f2675b5b4dc266b8c976bb79b4a9e50599ab822ba
- 466f3aaa5c69515cfeb0900d4c0487aa2c1e12fcc8d8bf2ed730ca56a22943ca
- 49e513841ef91b0b3cb3d58fe1d7e2c75373800c7c5062653905126bd1c586e3
- 61d79e963c2f1762920d1c8729d0e604cae6050cfc36bddc309fb9ffbecc0182
- 713353bc597075e577b738f843e9372444f8ed0010efc11ff80303dc9656f96b
- 7bb0b281ee6cd0d0859c51c4866528c1de8d36a337ef8449bde7422da6e7b908
- 857699fe734788e94f2fa7bf025211426c44aa065143ab98b55ab2864424fb8d
- 8fa890ae7063262b8092da0fff281cb11b633dd83e1f228351d187a07e51c248
- 90d993829351a41644966a191100eb7971c7fc886dfdcb2c023e6c7fb43900f9
- 9a60e3fc1c6e903f089b56c852b050f04dcbab6adf0bd44215e310b0b2663de6
- a41812691e197802b49cf1c6b1fcbf7d4f933a87032f3edd22e9e003749c5f21
- a7c803f8e2d17980b71ee3e895953e699da2cf316a70b1f76d5279f0af433235
- b1a0201a3d9529d966509111e6704f4bda521e26fc8142345e3f61712a64df55
- baf999647eb654bda2447ab3f017e634813fa3b01a656bda998178d17cfd0c1c
- bdb1b6aef20ec375f6f85c4f19a0d04228287e59dccbc72aaa79df1b9cbf9fc8
- c16b026d16e9ef8574dbb1e0f92b802ffb19ccb41cfe957246ffeba98b82f3df

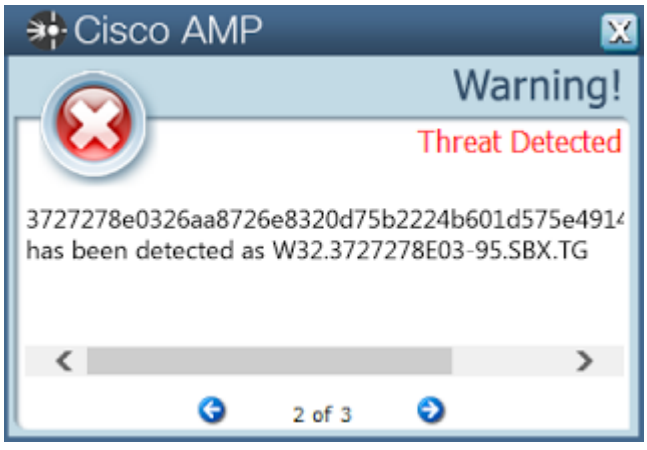
- cb3f34148beb2763a71b1727916490ac9e8825a68f60c296ebd98c4ec7bbfb6c
- cb891c0462de4eb8aa98c0af2ca4c70ea3e8ceb5f804af9c4b3a01abcfef82c9
- cdb21c6a6a47a508b5bf05f1f4e49b1a550cacec2452657fb9f094b2f0de9890
- ce397649edb82756667a63c26de24373992b84bbc4cf80353f5117876acebb2d
- eb024d54b61073e674d06c53fdc1523156d75268eaf9aff20070364df4ab0760
- ef509c6ac1fae60d57f773e4087b0412d3f08edbb19dc93218b183724bd64d83
- f1adbdee86076c202ab5d5783c9e8d5873b76a88a86a81ad10c275884303eaff

防护

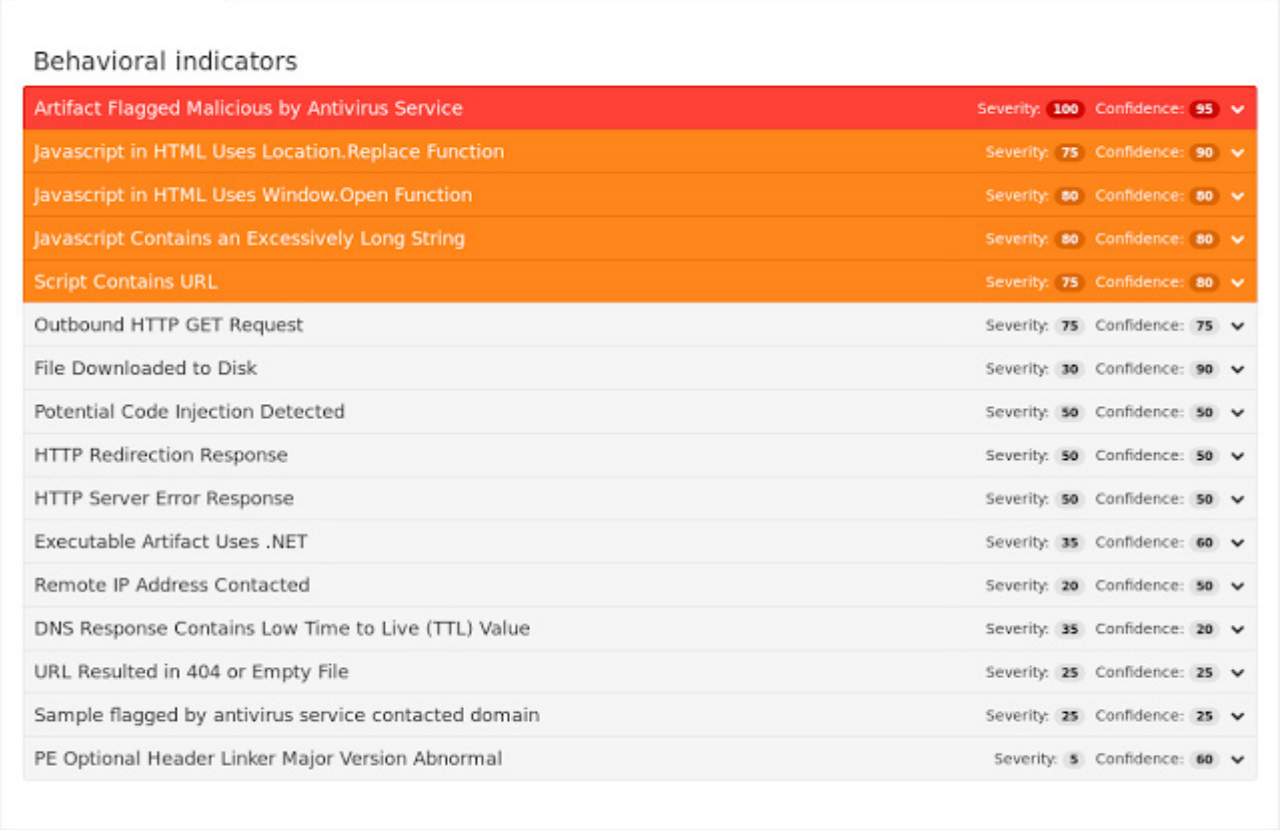
产品	保护
AMP	✔
CWS	不适用
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	不适用

检测结果屏幕截图

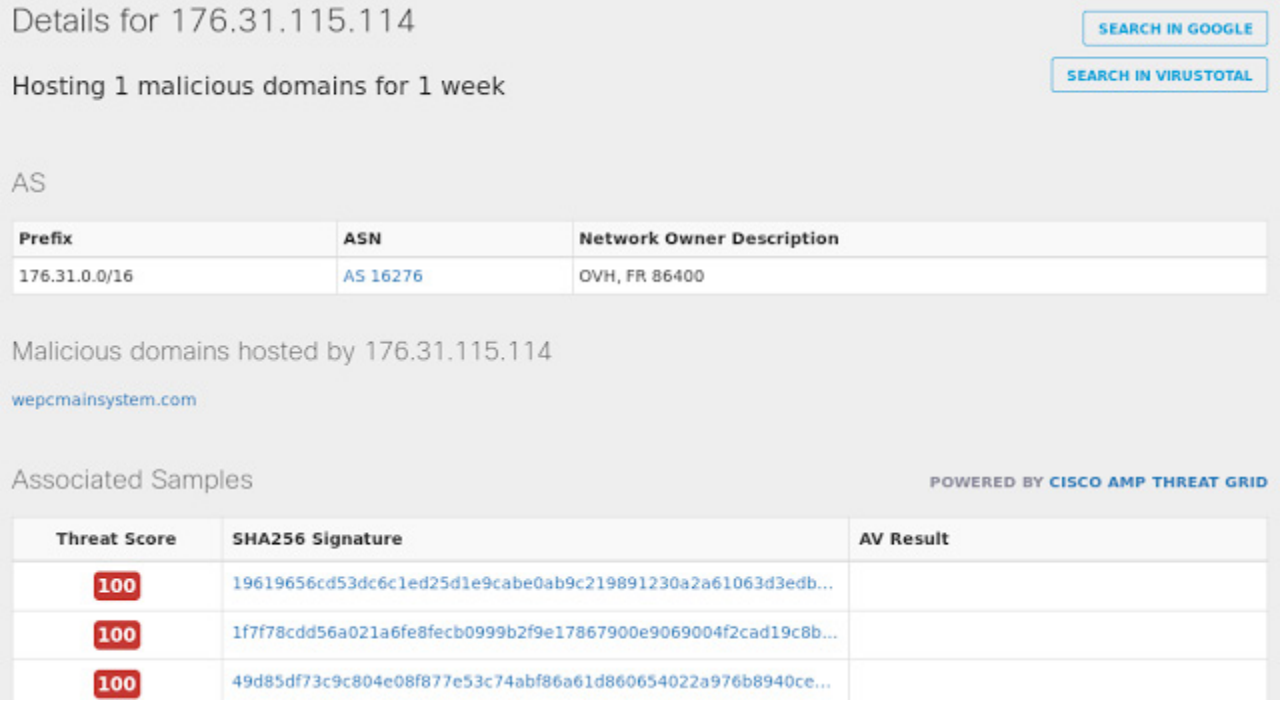
AMP



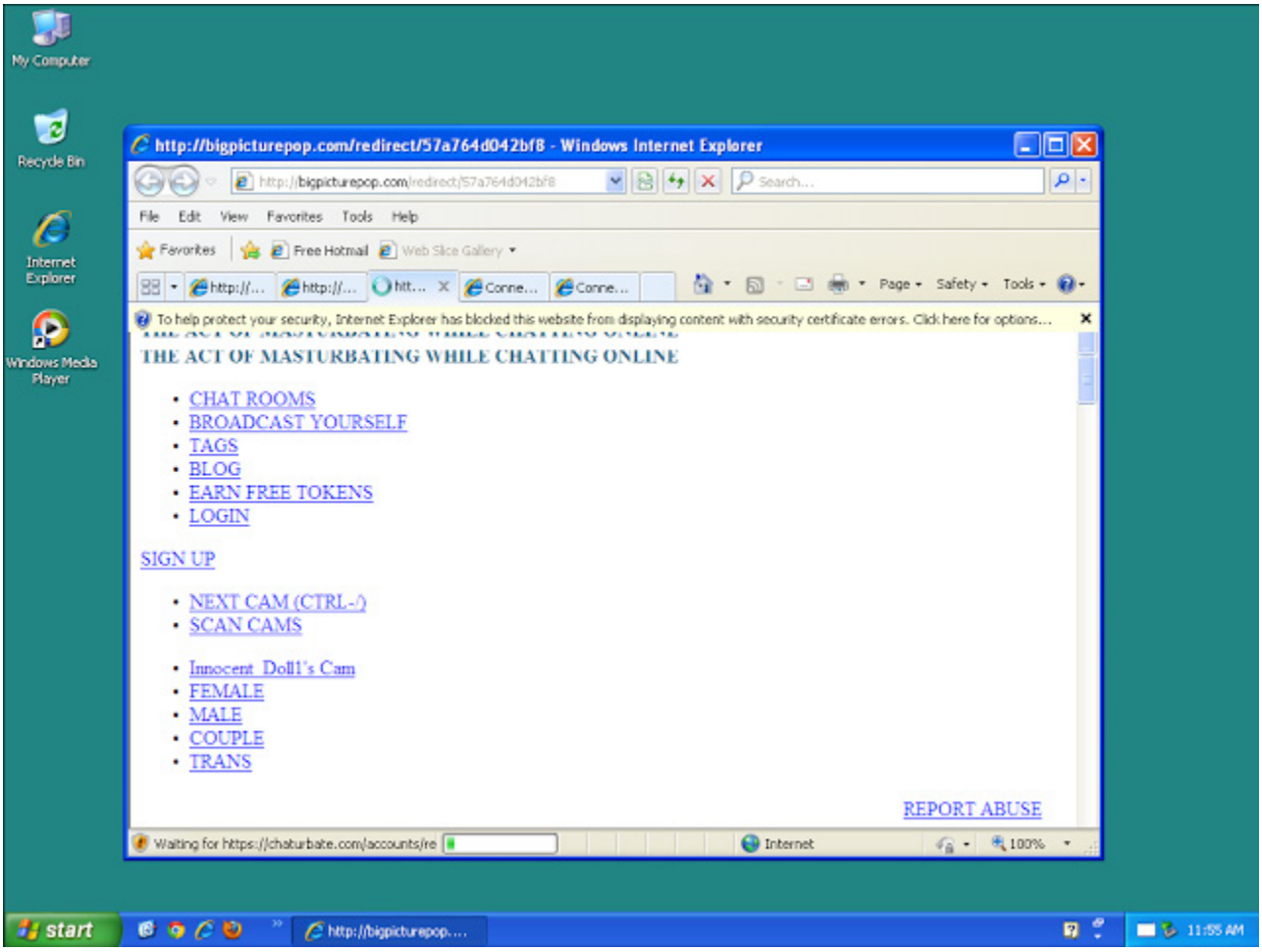
ThreatGrid



Umbrella



屏幕截图



Win.Ransomware.Nyetya-6331387-0

感染指标

注册表键

- 不适用

互斥体

- 不适用

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- %SystemDrive%\WINDOWS\perfc.dat

文件散列值

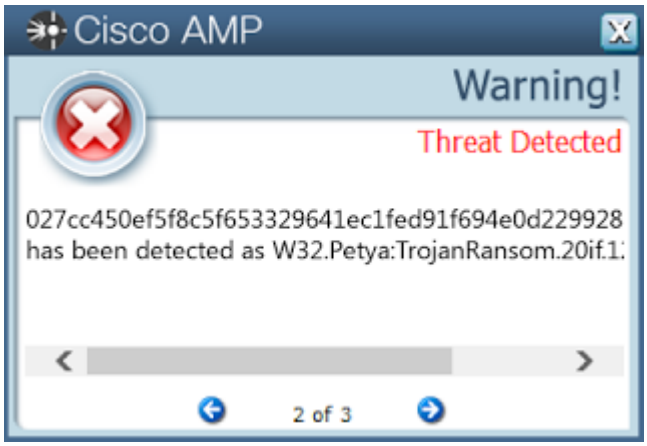
- 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
- eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998
- 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f

防护

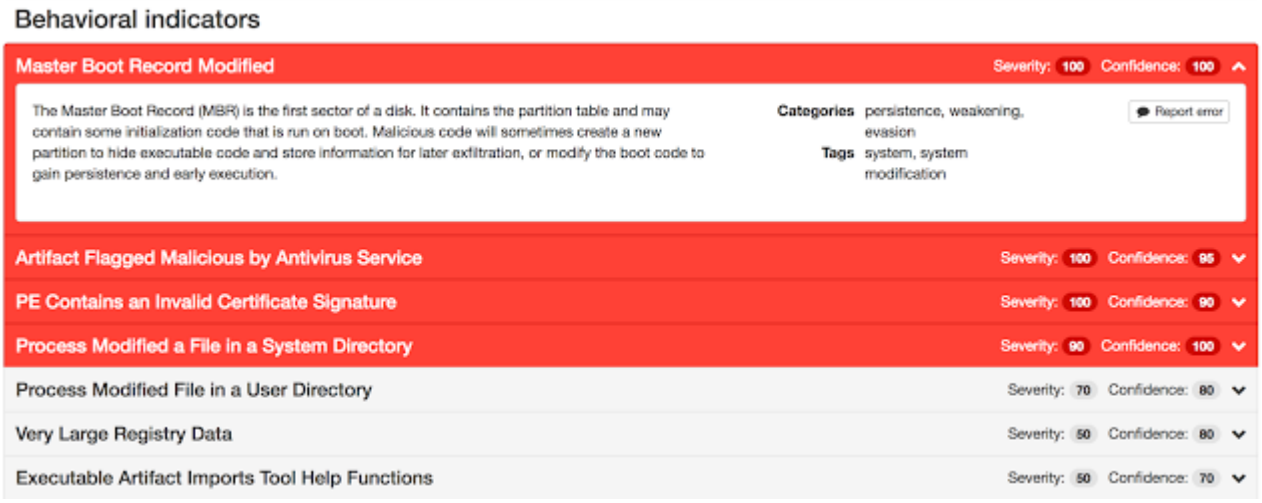
产品	保护
AMP	✔
CWS	不适用
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	不适用

检测结果屏幕截图

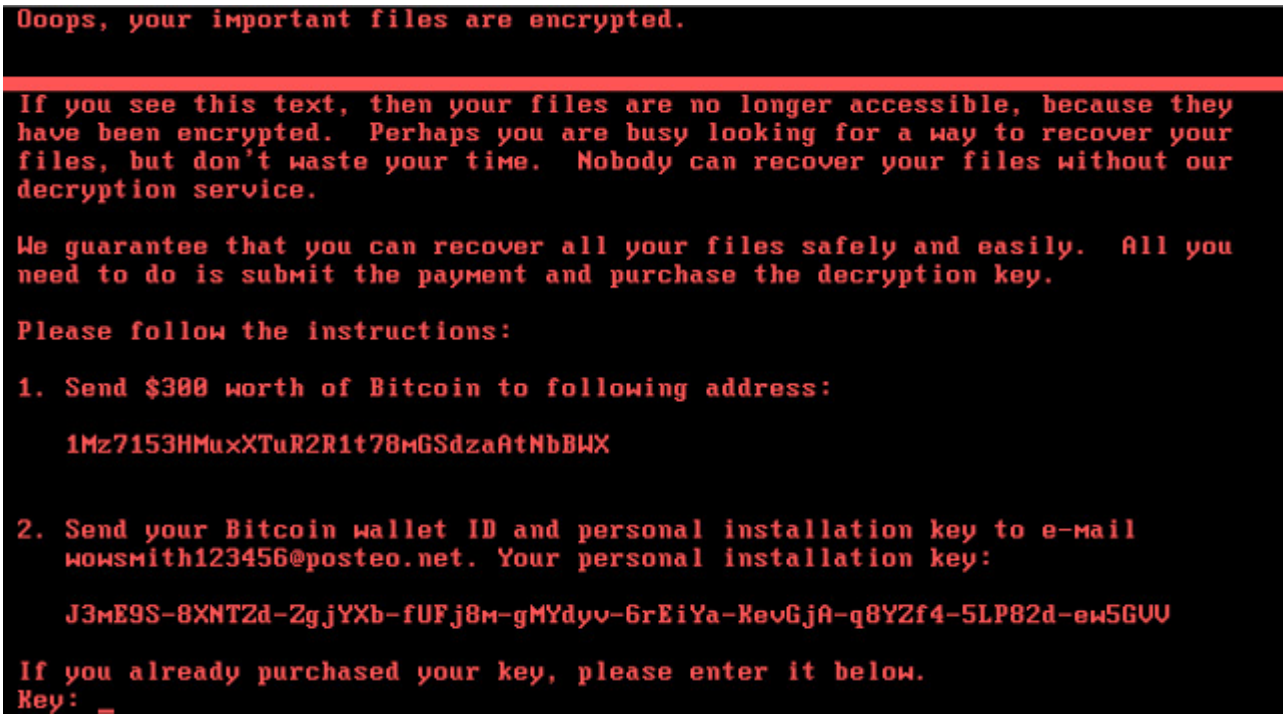
AMP



ThreatGrid



屏幕截图



Win.Trojan.Fileinfector-67

感染指标

注册表键

- 不适用

互斥体

- 不适用

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- %SystemDrive%\c2d124b8466cec6b3e47c4\i386\mxdwdrv.dll
- %AppData%\Adobe\Acrobat\11.0\Security\directories.acrodata
- %AppData%\Adobe\Acrobat\8.0\AdobeSysFnt08.lst
- %CommonProgramFiles%\Microsoft Shared\Filters\VISFILT.DLL
- %SystemDrive%\AUTOEXEC.BAT
- %System32%\wdi\LogFiles\WdiContextLog.etl.001
- %SystemDrive%\CONFIG.SYS
- %AppData%\Adobe\Acrobat\10.0\Security\CRLCache\48B76449F3D5FEFA1133AA805E420F0FCA643651.crl
- %AppData%\Adobe\Acrobat\11.0\JSCache\GlobData
- %SystemDrive%\c2d124b8466cec6b3e47c4\amd64\msxpsinc.gpd
- %AppData%\Adobe\Acrobat\11.0\Security\CRLCache\A9B8213768ADC68AF64FCC6409E8BE414726687F.crl
- %SystemDrive%\c2d124b8466cec6b3e47c4\i386\filterpipelineprintproc.dll
- %AppData%\Adobe\Acrobat\11.0\JSCache\GlobSettings
- %AppData%\Adobe\Acrobat\10.0\Security\addressbook.acrodata
- %SystemDrive%\c2d124b8466cec6b3e47c4\i386\xpssvcs.dll
- %AppData%\Adobe\Acrobat\7.0\Updater\udstore.js
- %AppData%\Adobe\Acrobat\7.0\UserCache.bin
- %AppData%\Adobe\Acrobat\10.0\ReaderMessages
- %AppData%\Adobe\Acrobat\11.0\TMDocs.sav
- %AppData%\Adobe\Acrobat\11.0\assets\assets-140109170701Z-78340
- %AppData%\Adobe\Acrobat\7.0\Collab\RSS
- %SystemDrive%\c2d124b8466cec6b3e47c4\i386\msxpsdrv.inf
- %AppData%\Adobe\Acrobat\11.0\TMGrpPrm.sav
- %AppData%\Adobe\Acrobat\10.0\JavaScripts\glob.settings.js
- %AppData%\Adobe\Acrobat\8.0\Preferences\AutoFillDefaults.dat

- %AppData%\Adobe\Acrobat\8.0\Synchronizer\adobesynchronizersu80
- %AppData%\Adobe\Acrobat\8.0\AdobeCMapFnt08.lst
- %CommonProgramFiles%\Microsoft Shared\Filters\msgfilt.dll

文件散列值

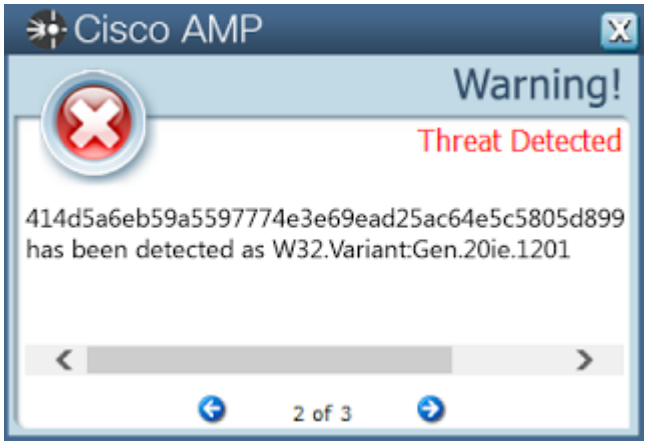
- 414d5a6eb59a5597774e3e69ead25ac64e5c5805d899886fc4c53ed0e4b1960d
- f9f0449bd2187f8a69a2e8a2eebae77c45d422900a762664847f4b097796bec5
- aab0014dbda65fb1ae5340a8b6da731aaa3215bb340c7df80b5b033ad2533001
- 29ba1dae0c75b5d67de2fb832a65a0a8d226f9585f1a3e334926259065355618

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.Fynloski-6332091-0

感染指标

注册表键

- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**c4f40c367320fcdc570a23c70d18a343
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**c4f40c367320fcdc570a23c70d18a343
- **<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**

互斥体

- 不适用

IP 地址

- 不适用

域名

- 不适用

创建的文件和/或目录

- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\c4f40c367320fcdc570a23c70d18a343.exe
- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Startup\x.vbs
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\x.vbs
- %TEMP%\IXP000.TMP\1.xyz

文件散列值

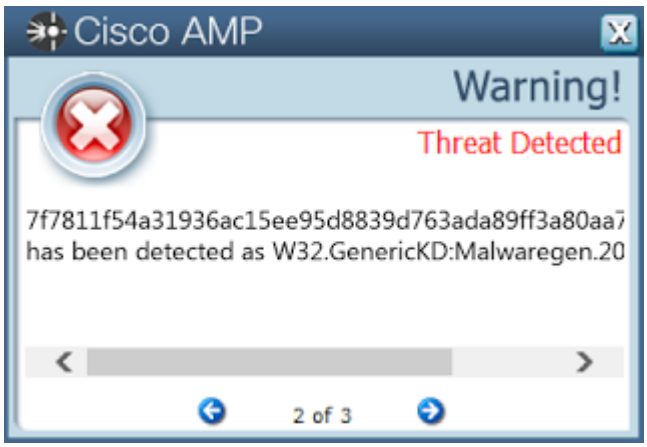
- 7f7811f54a31936ac15ee95d8839d763ada89ff3a80aa7479c7ea670b1a382c5
- 1b2149951adf10d725ad54bd262b4bcc7ca44be5986ce1414fa95082606811c8
- 7e9a837489b93a6f16385bd4e604923a1e4fa9c72a7d0ee1017037f26b02ed90
- 7077931eaa70834cb3a9862b6e405ea945459fda20d60ceb83b54a0e4a9f209f
- 77654b410cf65ec4e4e7b46cdef9c0df8397349cb351fa070bc9b64bdd6e83e1
- 83768ae6bc29747d33f106d36d12f59771a0333a997bd4b6eeaadd6b0a586f63
- e9642b9759686add2d022f0f3ac0ae5c2f5efe6a2cc5bef57f9480acb4792e6b
- ca006c5f27586648e44c1204f49ac555f9f4ddfd5a74af19104b031fd241adf8
- ad8472fbcf4ba8f6e9c7c275a64cdf364dabebdb7b9fc950cecce980a551ba48
- b3ea382eb9047ad9ba10956dbd580e70d08d027ca49504a78a24d98aed623de5
- e8415def78f91ca7b6e6dab7e6efc24eedeaf8f363af66b59b4fe1bc5ed24384

防护

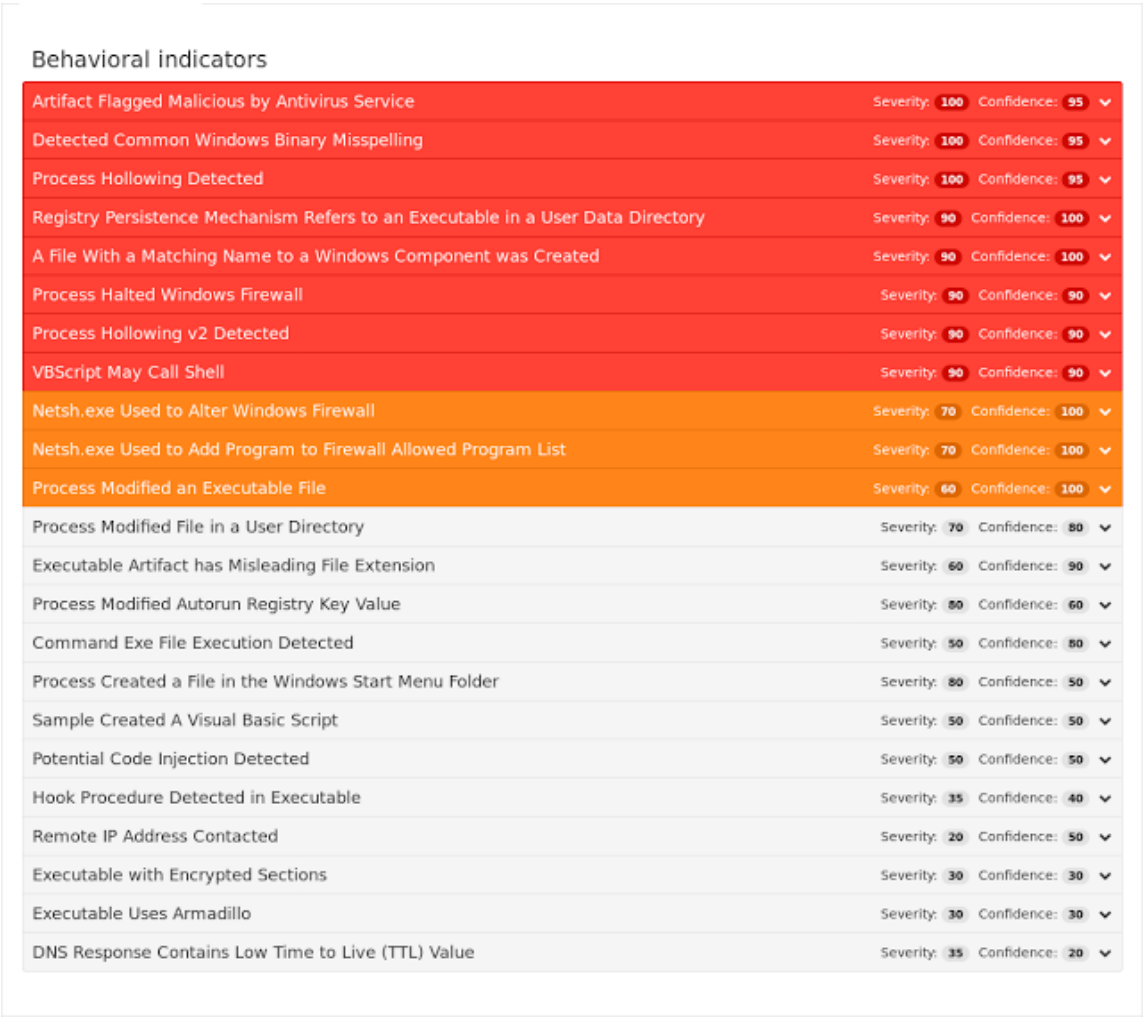
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Win.Trojan.Siggen-6261194-0

感染指标

注册表键

- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\MPSSVC\PARAMETERS\PORT KEYWORDS\DHCP**
  - **值：**Collection

互斥体

- Local\MSCTF.Asm.MutexDefault1

IP 地址

- 13[.]65[.]245[.]138

域名

- time[.]windows[.]com

创建的文件和/或目录

- \TEMP\filename.exe
- %System32%\wdi\{ffc42108-4920-4acf-a4fc-8abdcc68ada4}\{debd4f12-5573-4e21-a11a-2adccd61a055}\snapshot.etl
- %System32%\wdi\LogFiles\WdiContextLog.etl.001
- %System32%\wdi\{533a67eb-9fb5-473d-b884-958cf4b9c4a3}\{bc3d8877-b46d-4746-b041-b538af5e2cf0}\snapshot.etl

文件散列值

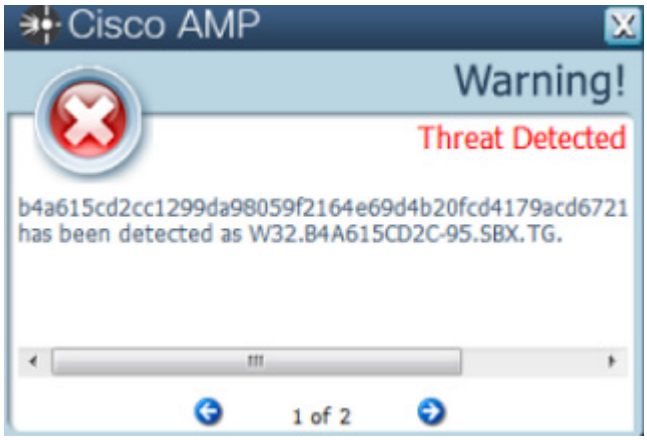
- b4a615cd2cc1299da98059f2164e69d4b20fcd4179acd672153e6533b9c95709
- f59c0ffee54d23875a039b546a1827c3bc40c45aee5a4887e6c8515e96d4169f
- e38d7a959a6957ae51733a4f8b28e7514c4f1cbb5faf2f6314d7b17c69eef155
- b3cd047683dc8944c9d9765d2e73c25c5ac1b7bba39f6b4ff748849b9a3d091b
- 4bcadb728a4948f945738f4d704c3f63525952ce8e6894aa6634de6e33a0d961

防护

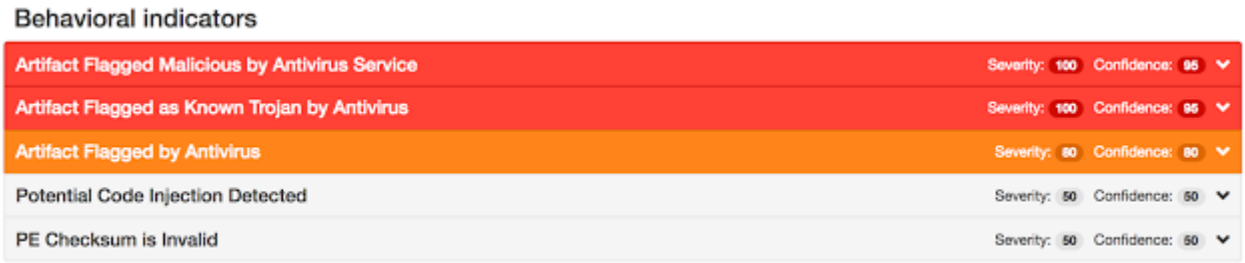
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



发布者：EDMUND BRUMAGHIN；发布时间：0:30
标签：防护、恶意软件、威胁综述