2017 年 9 月 29 日，星期五

一周威胁综述（9 月 22 日至 9 月 29 日）

本文概括介绍 Talos 在 9 月 22 日至 9 月 29 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.Downloader.Jrat-6336393-1**
  下载程序
  包含嵌入式 OLE 对象的恶意 Office 文档，嵌入式 OLE 对象主要为可执行文件或 Java JAR 模块，用于与某个域通信并下载其他恶意代码。

- **Doc.Dropper.Agent-6336814-0**
  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.DownloadExe-6336397-0**
  Office 宏
  这类下载程序使用硬编码的 URL 在设备上下载并执行样本。VBA 未经过混淆处理，只包含足以完成任务的功能。

- **Doc.Macro.VBSDownloader-6336817-0**
  下载程序
  这些 Word 文档中的宏以 Base64 进行编码，并在执行时从经过混淆处理的 URL 列表下载其他恶意文件。

- **Win.Ransomware.TorrentLocker-6336835-0**
  勒索软件
  TorrentLocker 采用 AES 加密对受感染主机上的文件进行加密，然后要求以比特币支付赎金。通过替换字符并选择性解析部分字符，将代码从一系列字符串中脱壳，再将最后的转换结果写入堆栈待稍后执行。随后，投放生成的子进程和其他二进制文件。

- **Win.Spyware.CCBkdr-6336251-2**
  APT 供应链攻击
  5.33 版 CCleaner 在供应商签名前被侵入，并在嵌入后门模块的情况下分发。有关详细信息，请参阅 http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html 和 http://blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html

- **Win.Trojan.Beeldeb-6336738-0**
  木马
  Win.Trojan.Beeldeb-6336738-0 是自执行 AutoIT 脚本。恶意软件负载被注入投放的可执行文件中。不仅如此，恶意软件还会将自身添加到启动文件夹以便持久驻留在系统中。

- **Win.Trojan.Cossta-237**
  木马
  Win.Trojan.Cossta-237 是一种木马，它会下载其他文件并有可能接收操纵者的进一步指令。

- **Win.Worm.Untukmu-5949608-0**
  蠕虫
  此蠕虫是极度恶意的威胁并且包含多种反分析机制，例如反调试技术，以及在安全模式下亦可避免被删除。它在感染后会持久驻留在系统中，并禁用 cmd 和注册表编辑器。

威胁

Doc.Downloader.Jrat-6336393-1

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

- mike22[.]linkpc[.]net

创建的文件和/或目录

- %AppData%\Microsoft\Office\Recent\ITT Tender - ABB -3600002386- Provision of Supply and Installation.LNK

文件散列值

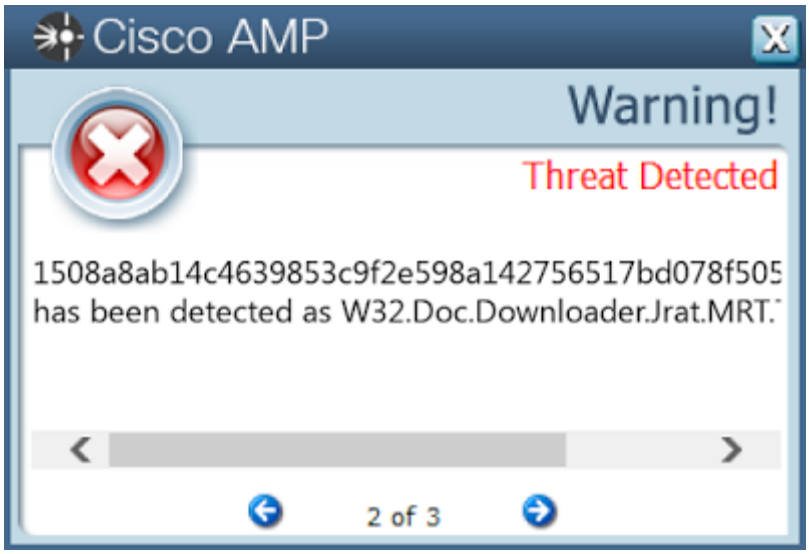
- 1508a8ab14c4639853c9f2e598a142756517bd078f505274b5783ddda8fed0a0
- 1570586012e23a7de3a8fd965bdc2d3a96175fd8a77d284827c1ed6d58944a7e
- 339ceac2076e833babc1ac838848ab2787af062835a24f05e0bf20ab1ec79ccf
- 6f276350ce399502dbf870702e1a09ee39b591b93ebface9d3214ce9822aed61
- 7dd8b4746bf2de079b3b66e9d5e0492cde0a3838311252176a8831c3fd64b33b
- 7e4ef415a75cea7d3d610c44c0fa51d0fba956cc8136784115641054cd470fa0
- 9394e12d1fe6d3627f5f928aff4a15699aa129e44fd4fd9eba29f6ad5a4f7556
- a5dfb783b89232fcc317194d267b8cf7204ae457d86eb5cdf703a656c03f1b71
- a601c81547e7180d284e2fa701599615070653cceaf63108a11c40821edbf024
- baba92ad2bf34ef95611656722344af6b60f731e7cdc4a341f64658837976899
- bb4793538712834408cd9b3b58c1edf8da81906ffc12e25766fb40ddabe1c383
- 50c1020efca0698519c89b468fc25926d1bad2eeb421482d9c17b6ab24535217
- d29a6afc4b35eef258116643694716 88a0ecd89fc2a5eb676de9c5518c9914f2
- db4d85d172b31413c1f93162053032a9a2e26b273dfdea8b7506ee8ca982e32f
- f745e3687dabecb07c033a70db4f8c2cb14b9fc75c896304f6e9ed4dc6e3a1ba
- fff6555400d65b28590cdde1a1f1a8731f02e8c21c1a9f167d53dc1054cc865a
- 522a804aeee581c63049d0a5983a558c2a3225c4b14814cf0acb8912b79260d6

防护

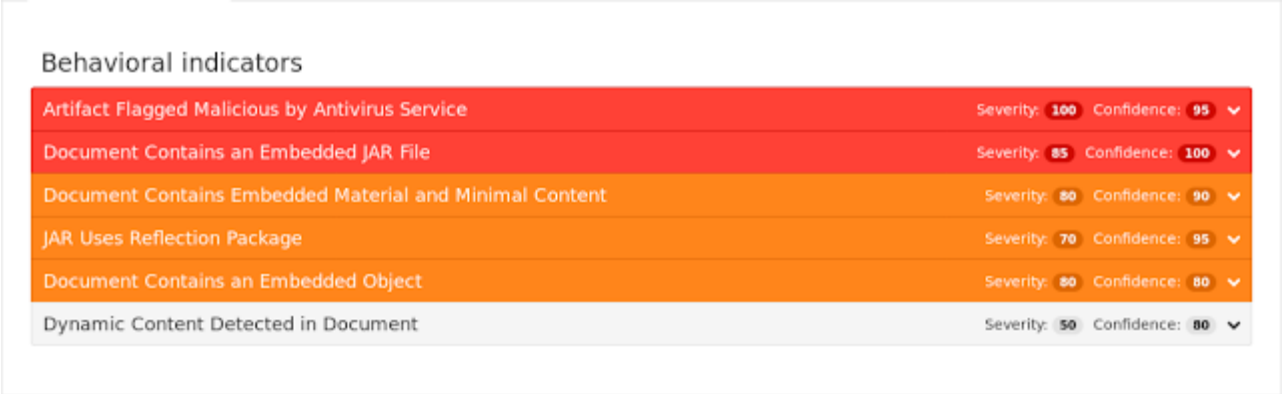
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

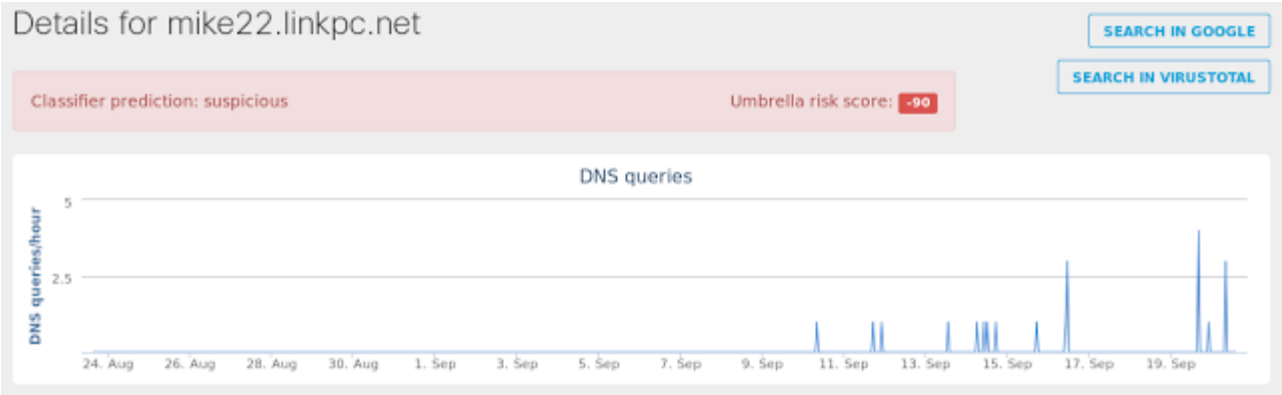
AMP



ThreatGrid



Umbrella



Doc.Dropper.Agent-6336814-0

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

- acsbaroda[.]com
- a[.]pomf[.]cat
- b[.]reich[.]io
- directlink[.]cz
- nusacitracipta[.]co[.]id
- u[.]teknik[.]io
- wallpaperbekasi[.]co[.]id
- www[.]b-f-v[.]info
- www[.]noosabookkeepers[.]com[.]au
- www[.]powerplusscable[.]com
- www[.]styrenpack[.]com

创建的文件和/或目录

- \Users\Administrator\Documents\20170920\PowerShell_transcript.PC.Pbzg9q9Z.20170920011010.txt
- \TEMP\Quotation_211.xls
- %AppData%\Microsoft\Office\Recent\Quotation_211.LNK
- %AppData%\Microsoft\Office\Recent\277336261.xls.LNK
- %AppData%\Jaty\WebHelper.exe

文件散列值

- 760d89498b3029b1c6fdc5feefa16170589a4b61414c6b1e9d76611031ab0bd5
- 19dc470f8c9a1a4e9e24707b68c43138178e81d4ec74e358941756667633c5b7
- 1d14387de0375c84c8c334fb4d29c8ec4e3c24cd9969bcd3acbb77cb65f77a11
- a80e8da4851eccfad1b8c2b930389a1980dcdab0d193073a4d3dac2d6a0e73d7
- f84e3b79c16a77db33d1f5ee66fa13d15f25fed78d219d77dfe83268650cd944
- d1e2655394e9ffd7f7d502840ace6b0de7369c938abee8c1ddc84dcf73486dd3
- 81b61e9dd4682b079e0b1df3250640c99e0228d4bdcbef5f18bf4bd8fedbff09
- 5af528ce89a31516eb1b5303b0789b56ab64ad16d7d15193c8b24b5ac3ff22a0
- a9fec7f8f911f431dd9934092903974c3206feefac7308f48087ab02fbc24927
- 93a1ddd820a187fd8db5ce8d595958fcfb34ea5c01b5971b359f318f8fe7bb3b
- 4eb507bf63d6273548238a6c7e6831b6b29363c1c37e9176b7c72a6c3faa862d
- cffb8b6c103a443159c94dadd5058c3c083d906600f0db6291ab0e2f4c005b68
- 127cae520479d08e0bfa1b569ace82203cd8154f49f7a8569bfbc54d4c8c6da8
- dfca64bac0dd845e4e0d98a0f0ce3ae235cddf2f6506fabb7923a2d5e0da3129
- c1f97901518b6dab1c4516a7f400430030011c26f52cd429299d4331938b70bd
- c3baeac24f2416d21e64df05b568600c3be76a6365e7cb5b8dbfdfe64ae95c46
- ac535056dcd65160165ad9e53bc5bc4e08b61ce129fb37d7f7b727c4e1a875df

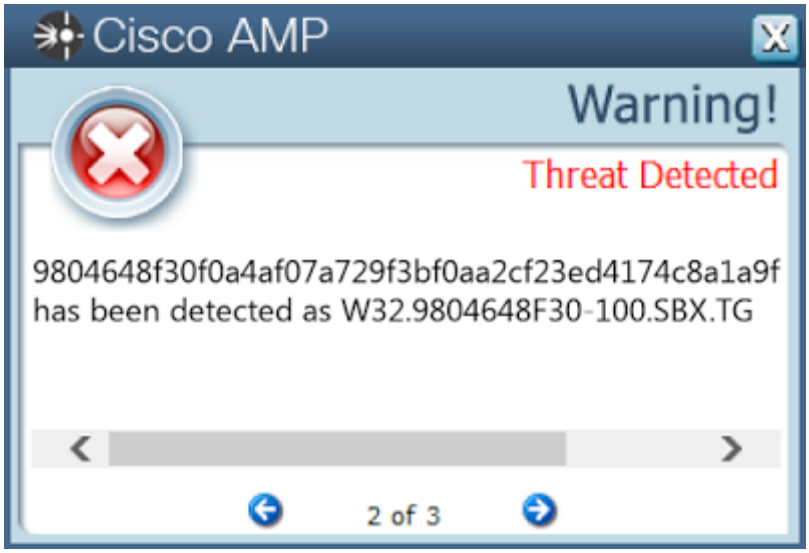
- af9f674bc5a26324b62f8c5a67f256b6133b2ec26a25a7c93564fe048ae4afd4
- 2b06143fffe0099302b2ec0b6f40b5aac115f37c61db32a3be6e0ed13d8eee85
- 2eba0e3bb658230fe8617038b6be0f58d042a8bb13dd4d9169e775263f82eab3
- 304c6f454f0efca218002c12009518c27e63186dd5de57b652cf2d4d14c7f0a4
- b75f01bb44d8a7f402bf01683230ff71138509344bd13d7c199855a321c26b30
- 5b5b1960bb43c0c115080b3393aaa263137141d53f6b173b24f6c08cbe86d2f8
- 51d6c81b77f098af1b463f72d236d44b21d873f3c8360004ac93ba803db620a9
- f4eb5c188028bd80eaf5e822fd6e80e6d2826215e6698668202b72aedabc3daf
- d8b26ec2609f02379d8b8489f0b52f060e1d5f2dea369dbb675c408c29f83401
- 81dea09c54a4f26cc078d1b341d5172ceeb5229861621e99552854c564747c83
- 80c8b5fad0efae1c96e51d97a3ae2ee0e3c9d802691e7178da29b12f23b0f2a0
- 5742ca6839d7b0b6e56f5406fcb744180bc76e81f7ebdc626b432ab3c1b3de81
- c1fb997c7dd23f0bb6f19e20029650fc890beca44fbe2f50e21a001b3aa1d319
- 2159c51a8951b68089524aec9cbb7ba171da57baf733bd12c7d7741d8f17e55b
- bef55fe81de1a2eb2c0a9e647619a483093b031f5c797d5a8e32bb787356e33a
- 7f0a79692fc21938be2f2acab035a56049a9444a8e380d62615546efd0862335
- e618be36548c349562bbdc6c4d68efcb2c86b4354037e9014fd91eea3ec0a0ca
- 100b1db7896fbd9c4415a96aed0383babbc43ac1f6ae589d408d39532ce9125b
- f48ecc2b672bc937370ef812eb1b23e3e76e680a2a96aff2d58af8331eb75cfe
- da2ee40c1fcf98c416132ddf8d4a533f387fcc2214772588bf2ab0967a7d1ede
- b5fd96e20d32e4f805c4b157037b8e382ff2ce3564fad2f5b3d3c7b6247ea1e2
- bfc11420c2e7d86d66ca3c4cd495a47b7882d6abbb7a8cc87a58ce9e3daaacaa
- 5f5e981122a6264042e5b79860200c894538cb134d2c93d3f15750ec9443c7f2
- 76a940a6ef4397c6b7c8d1ba0dca3e891c2d526f58c03c766d041b98a8791e54
- 5056b55b83863c4ac1ed6ee66e4d2dc0de8b56416dd96cf712f5b889aeff5cdf
- f9e29f39b89918fcf26237c5002cd98a2a001c37690720ba537eebd0e72a56cd
- 6264bc92083a561dd31c38fc752589eb7e8dd65fa2b6c792d2dd247b5f63ff98
- 544eac3c9205cc3ecaf57283c823050df3bfe4ce78d0c7e38592ef333cc8bdc8
- dce3ff33424c5e43795ffba7ad33ee8a301606e3c4406e2cd1d07cf6d789ac8e
- 633dd2217d33b8a60f3ca98905bb7119d7d63e8db50525452c5bfe5449b7885d
- 6386f608f5f0fb7007ecf808b9a96048c4fc1fe3c20637332b9da1e5094972c5
- 60d4c6a68368b14ce9aa0b6b3e8eb91e92f823f6524a49e4e7cc265353982898
- 9804648f30f0a4af07a729f3bf0aa2cf23ed4174c8a1a9ffd98694efb3c51e2c

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

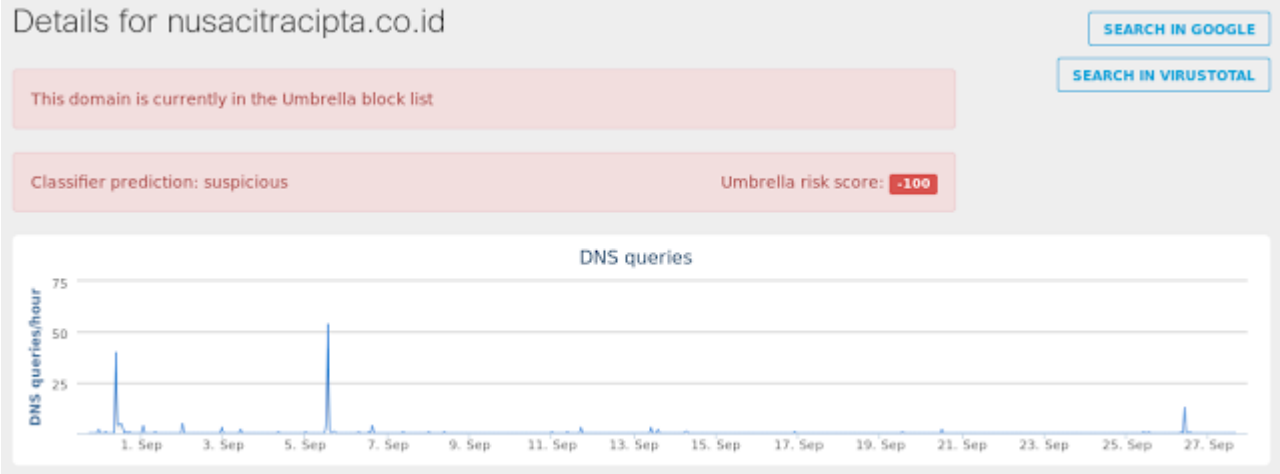
AMP



ThreatGrid

Office Document Launches a Powershell	Severity: 100 Confidence: 100
Document with Random Variables Established Network Communications	Severity: 100 Confidence: 95
A Document Requested an Executable via URL	Severity: 100 Confidence: 95
Document Contains VBA Macro With Random Variables And XOR Function	Severity: 100 Confidence: 95
A Suspicious Document Containing Randomized Variable Names Detected	Severity: 95 Confidence: 100
A Document File Established Direct IP Communications	Severity: 100 Confidence: 90
VBA Macro Uses Xor	Severity: 90 Confidence: 100
An Embedded VBA Macro Contains Randomly Generated Variables	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
VBA Macro Opens a Binary File	Severity: 80 Confidence: 100
Antivirus Service Flagged Artifact As Likely Malicious	Severity: 80 Confidence: 90
Artifact Flagged by Antivirus Engines	Severity: 95 Confidence: 70
An HTTP Request Was Made to a Numeric IP Address	Severity: 75 Confidence: 80
VBA Macro Has Action on Open	Severity: 70 Confidence: 85
Outbound HTTP GET Request	Severity: 75 Confidence: 75
Antivirus Service Flagged Artifact As Containing A Macro	Severity: 70 Confidence: 80
Office Document Contains a VBA Macro	Severity: 70 Confidence: 80
Office Document Contains an Internal Macro	Severity: 70 Confidence: 80
Static Analysis Flagged Artifact As Anomalous	Severity: 60 Confidence: 80
Dynamic Content Detected in Document	Severity: 50 Confidence: 80
PowerShell Launched with Execution Policy Bypass	Severity: 50 Confidence: 70
PowerShell Launched with a Hidden Window	Severity: 50 Confidence: 70
HTTP Client Error Response	Severity: 50 Confidence: 50
PowerShell Launched Without User Profile	Severity: 30 Confidence: 70
DNS Response Contains Low Time to Live (TTL) Value	Severity: 35 Confidence: 20

Umbrella



Doc.Macro.DownloadExe-6336397-0

感染指标

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 66[.]55[.]90[.]17
- 52[.]179[.]17[.]38

域名

- a[.]pomf[.]cat

创建的文件和/或目录

- \TEMP\~$L Receipt.doc
- %TEMP%\CVRFC94.tmp.cvr
- \TEMP\gkmgax.exe
- \TEMP\DHL Receipt.doc
- \srvsvc

- %AppData%\Microsoft\Office\Recent\runme.doc.LNK
- %SystemDrive%\~$runme.doc
- %AppData%\Microsoft\Office\Recent\DHL Receipt.LNK

文件散列值

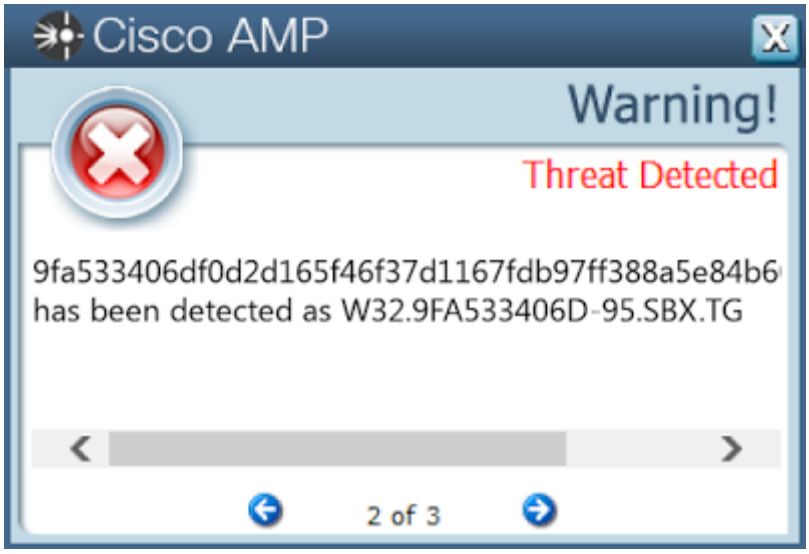
- 9fa533406df0d2d165f46f37d1167fdb97ff388a5e84b60bfd75921c6f44ff6c
- 74805a5b0a8171f723627c8b061805a6c9c098e7ce1ea83378a774769bc7a1c6
- f861caffda478a4227bf06323ef32407f774274cdacf2e5e23506d67a08cd89c
- 9fa533406df0d2d165f46f37d1167fdb97ff388a5e84b60bfd75921c6f44ff6c
- 0ef4406f5608ad25b4c61d37b6ece1b71c2738814528af550dde14917d2cb4e3
- f8dcc75be0d1354741606663aebb95e477fe1d4e46246e677fc0e414b7dd354f
- 216f09c6eff72fae7d6511a73be7530e80980ff6305e4dd2656c96aec29f242e
- 265de60479b8d8bd46b56a7bec778d6ef9c62a9053e42c6a632d52cdc16a9490

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

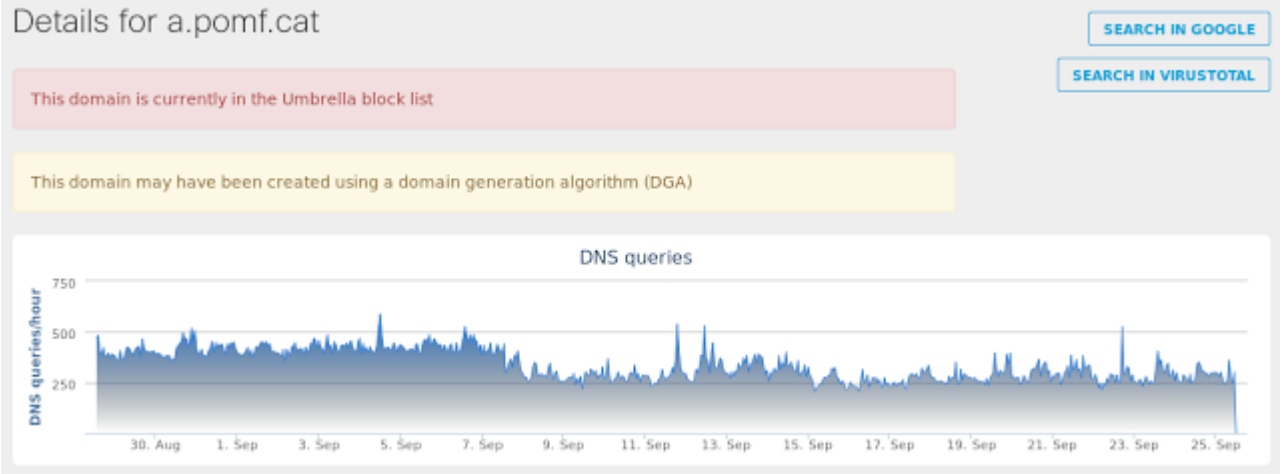


ThreatGrid

Behavioral indicators

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 Flagged by Antivirus	Severity: 90 Confidence: 100
VBA Macro May Call Shell	Severity: 90 Confidence: 90
Antivirus Service Flagged Artifact As Likely Malicious	Severity: 80 Confidence: 90
Document Contains Embedded Material and Minimal Content	Severity: 80 Confidence: 90
Artifact Flagged by Antivirus	Severity: 80 Confidence: 80
Process Modified an Executable File	Severity: 60 Confidence: 100
Script Contains URL	Severity: 75 Confidence: 80
VBA Macro Contains URL	Severity: 75 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
DNS Response Contains Low Time to Live (TTL) Value	Severity: 35 Confidence: 20

Umbrella



Doc.Macro.VBSDownloader-6336817-0

感染指标

注册表项

- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass

互斥体

- Global\MTX_MSO_AdHoc1_S-1-5-21-2580483871-590521980-3826313501-500
- Local\ZonesLockedCacheCounterMutex
- Global\MTX_MSO_Formal1_S-1-5-21-2580483871-590521980-3826313501-500
- \BaseNamedObjects\Global\I9B0091C
- RasPbFile
- Local\WinSpl64To32Mutex_e39d_0_3000
- Local\MSCTF.Asm.MutexDefault1
- \BaseNamedObjects\MD99F8B3

- Local\10MU_ACB10_S-1-5-5-0-58054
- Local\ZonesCacheCounterMutex
- Local\10MU_ACBPIDS_S-1-5-5-0-58054
- Global\552FFA80-3393-423d-8671-7BA046BB5906
- \BaseNamedObjects\Global\M9B0091C

IP 地址

- 50[.]63[.]119[.]1

域名

- lymanite[.]com

创建的文件和/或目录

- %SystemDrive%\~$c69c4b9785cdc861c8fae99998a1ad011cf2e98456a1891bd29bcc990897f0.doc
- \TEMP\gescanntes-Dokument-07170222835.doc
- \Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{24E5C5A3-7CF5-41D8-94C1-47B41F61C27E}.tmp
- %AppData%\Microsoft\Office\Recent\fac69c4b9785cdc861c8fae99998a1ad011cf2e98456a1891bd29bcc990897f0.doc.LNK
- %TEMP%\64388.exe
- %AppData%\Microsoft\Templates\~$Normal.dotm
- \TEMP\~$scanntes-Dokument-07170222835.doc
- %AppData%\Microsoft\Office\Recent\gescanntes-Dokument-07170222835.LNK
- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\42994.exe
- %AppData%\Microsoft\Office\Recent\Local Disk (C).LNK
- %TEMP%\CVR26FE.tmp.cvr
- \Users\Administrator\Documents\20170926\PowerShell_transcript.PC.sJClvqz1.20170926112823.txt

文件散列值

- fac69c4b9785cdc861c8fae99998a1ad011cf2e98456a1891bd29bcc990897f0
- 0274541153434372cb7c0bdc7f55c5b70a48ab0c22907611a89139d2073826bf
- 12b2acf3a81b16850fec270f521ba9b749a340f1357f225e495462822409da12
- 1d1407735650c83e62a561a1ea5cdc798aa1cdc92653f5e722dc8b22b5ed9a7c
- 2b4bbedb5119cd52c44fe035ee5b00b520792db60207ffd6ce3cdc339901346d
- 476e8075ba4866c0a78253dcb19961b28f150aa207d50b575b0d07fdcca4aa13
- 477bbf5395742a4e45331d71c6de3191729fbbf5914457ccfef7eb9d3e8697c7
- 4cfd3f25f178f5ae5dd5c5438a4bc3cd0af2ca712a5a59388612697d4b4424d4
- 5bb5975dd0b781d5fab3721ae66463e64825fccfdcf876bcb8899c2571ed04f4

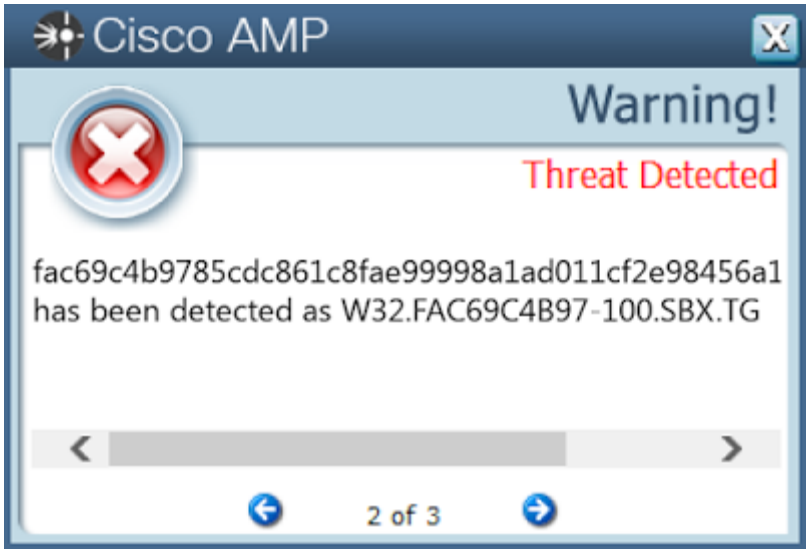
- 5dc91a43bfcf5f4b4c2a759220e9eacec671bc275572b6feeca274d9c4836829
- 61411a7a585f12f1d3e60eb084e9dac648217b922a3d68ce4024b26a6fcce3cc
- 69b35b1bffd2d36c06d4598de38fa4364e726044623d89bc73fc1e9b31f57e71
- 6c0bf54da7ee15bf99b7ff6be57ee8331d8335a1d15513227c6ada04c841c4de
- 71cc8b291e0a1ad38ed9142eb112f56c4a8a3eb00d130bfa27e5c40a08bc9e43
- 75eb214657020fd9b6f2d533d3c12724cf1de2adbb925d7abfd744e6ff73633d
- 7cc1a551e6060d0e7a38423a2247edd4a84b6cca927f996d2bc056269dedb6e6
- 908b6ea63e3e916377fe0319886bf4b55c7aaddde27292b9dce5930eede5622a
- a2fe92fa39d6b0f9dbfebd83be179524fadb87b11e555eee96c606af7d34ce73
- b6bfdbfcbb5097912ad8bdf9cec2592a162a27b7c367193d1fdd10d9db5182dc
- b7651bd99dda94f6bf962b473872690ee145c38546cd7b3f8bb477976d9a8617
- c77d0bee9502f8d4c3afc1729a7ab9721ffce9bf2b7759d086e436370af4ff5c
- d621d5dea6a95c31650a4c46aaf507625a8e18f33b5a4a22e8a801c25dc77a49
- d919139e4965ad6c55b7f08e2f919aac5fd8deb0fd90cf65f2bd4a4aa5bd2dd8
- d9c9e1fece032140a4754096b08a4eb147598a36f8b582c796b8764ff6cd9a91
- df5c68270b14d82a523a503a717de1ccfe1739c62956e7a58aa8441f117b7344

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

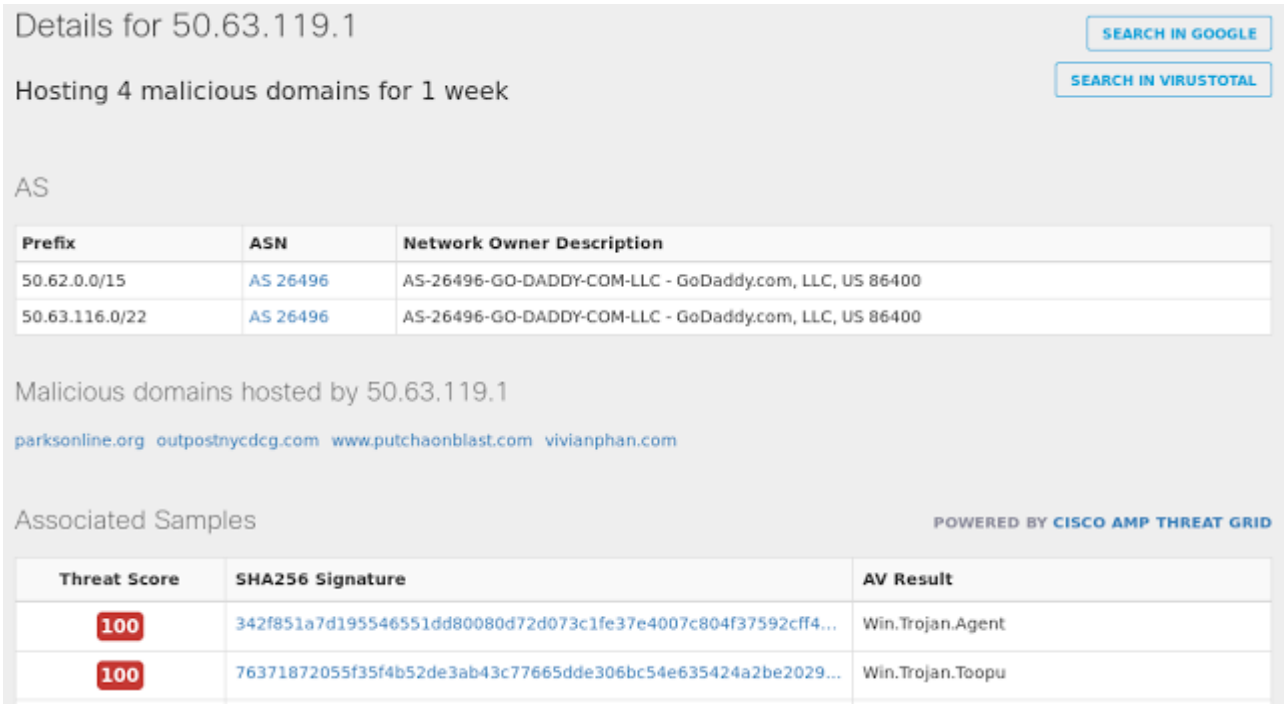

Cisco AMP
Warning!
Threat Detected
fac69c4b9785cdc861c8fae99998a1ad011cf2e98456a1
has been detected as W32.FAC69C4B97-100.SBX.TG
2 of 3

ThreatGrid

Behavioral indicators

Document Created an Executable File	Severity: 100 Confidence: 100
Document Properties Store Base64 Encoded String	Severity: 95 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 with Embedded and Minimal Content Established Network Communications	Severity: 100 Confidence: 90
A Document File Established Network Communications	Severity: 100 Confidence: 90
An Embedded VBA Macro Contains Randomly Generated Variables	Severity: 90 Confidence: 90
Antivirus Service Flagged Artifact As Likely Malicious	Severity: 80 Confidence: 90
Document Contains Embedded Material and Minimal Content	Severity: 80 Confidence: 90
VBA Macro Accesses Document Properties	Severity: 75 Confidence: 90
File Name of Executable on Disk Does Not Match Original File Name	Severity: 80 Confidence: 80
Process Modified an Executable File	Severity: 60 Confidence: 100
VBA Macro Has Action on Open	Severity: 70 Confidence: 85
Outbound HTTP GET Request	Severity: 75 Confidence: 75
Antivirus Service Flagged Artifact As Containing A Macro	Severity: 70 Confidence: 80
Process Modified File in a User Directory	Severity: 70 Confidence: 80
Office Document Contains a VBA Macro	Severity: 70 Confidence: 80
Downloaded PE Executable	Severity: 60 Confidence: 90
Static Analysis Flagged Artifact As Anomalous	Severity: 60 Confidence: 80
PowerShell Used With Encoded Command	Severity: 60 Confidence: 70
Dynamic Content Detected in Document	Severity: 50 Confidence: 80
File Downloaded to Disk	Severity: 30 Confidence: 90
Potential Code Injection Detected	Severity: 50 Confidence: 50
Executable with Encrypted Sections	Severity: 30 Confidence: 30

Umbrella



Details for 50.63.119.1

SEARCH IN GOOGLE

SEARCH IN VIRUSTOTAL

Hosting 4 malicious domains for 1 week

AS

Prefix	ASN	Network Owner Description
50.62.0.0/15	AS 26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US 86400
50.63.116.0/22	AS 26496	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US 86400

Malicious domains hosted by 50.63.119.1

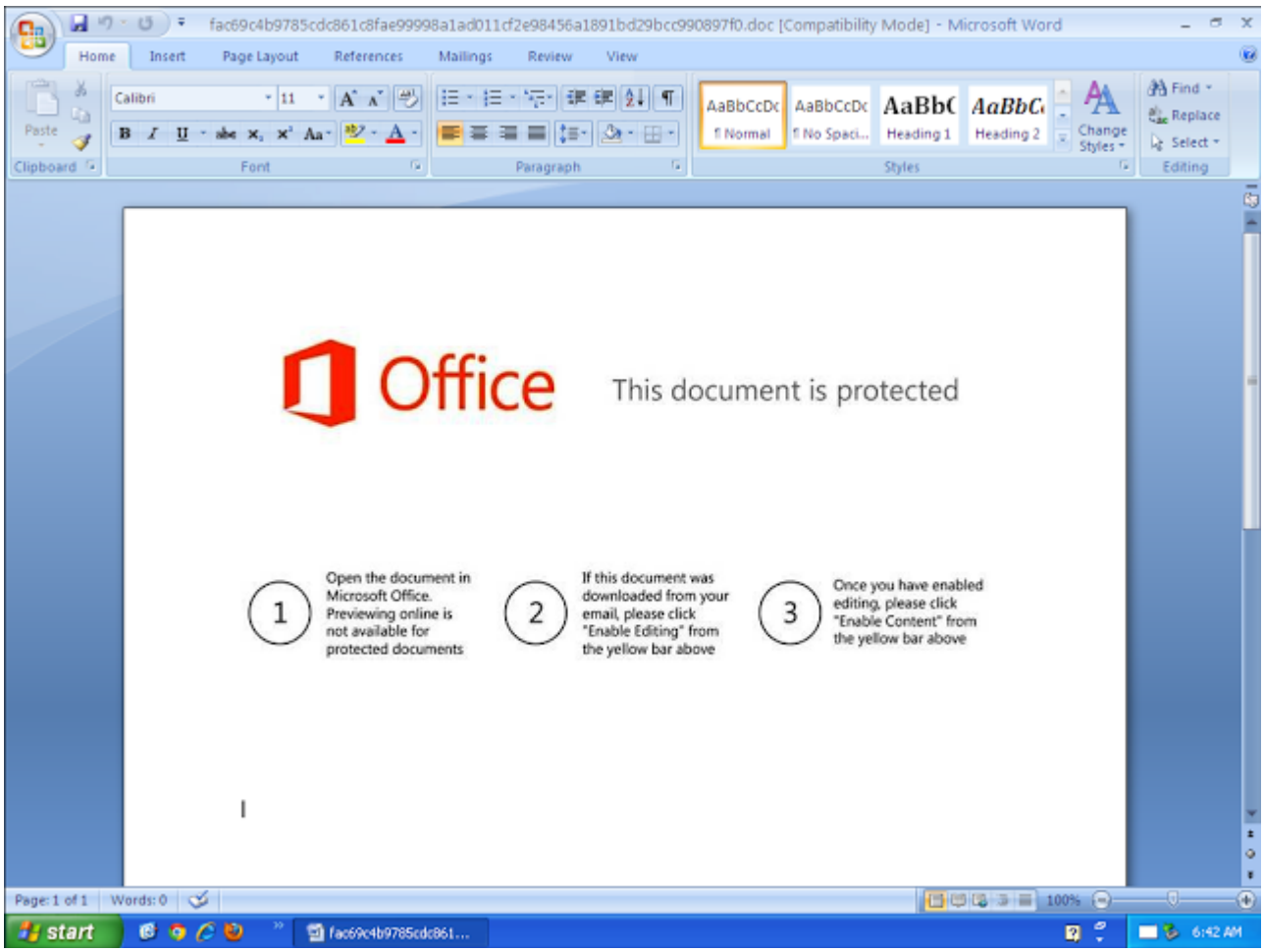
parksonline.org outpostnycdcg.com www.putchaonblast.com vivianphan.com

Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	342f851a7d195546551dd80080d72d073c1fe37e4007c804f37592cff4...	Win.Trojan.Agent
100	76371872055f35f4b52de3ab43c77665dde306bc54e635424a2be2029...	Win.Trojan.Toopu

屏幕截图



Win.Ransomware.TorrentLocker-6336835-0

感染指标

注册表项

- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**etejasix
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**ProxyEnable

- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**AutoConfigURL
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**ProxyOverride
- **<HKLM>\SYSTEM\CurrentControlSet\Services\VSS\Diag\Shadow Copy Optimization Writer**
- **<HKLM>\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

互斥体

- \BaseNamedObjects\Global\otydesuxofyjyxufexycaga
- Global\otydesuxofyjyxufexycaga
- \BaseNamedObjects\Global\yjacitumaxicuqexyfitywoqewyquwy
- qazwsxedc
- Global\yjacitumaxicuqexyfitywoqewyquwy

IP 地址

- 不适用

域名

- wrygsxi[.]zotebsca[.]net
- atawgce[.]zotebsca[.]net
- adez[.]zotebsca[.]net
- uluxkqopy[.]zotebsca[.]net
- efedaluc[.]zotebsca[.]net
- mxed[.]zotebsca[.]net
- omywuw[.]zotebsca[.]net
- imjmawfcoja[.]zotebsca[.]net
- evycoroz[.]zotebsca[.]net
- erivequt[.]zotebsca[.]net
- aqyjo[.]zotebsca[.]net
- usuhazepug[.]zotebsca[.]net
- avev[.]zotebsca[.]net

- fhuga[.]zotebsca[.]net
- uqydjnwn[.]zotebsca[.]net
- evehasuruzo[.]zotebsca[.]net
- ypyhi[.]zotebsca[.]net
- epabojyluko[.]zotebsca[.]net
- iqesex[.]zotebsca[.]net
- ywapivuqexe[.]zotebsca[.]net
- ihodi[.]zotebsca[.]net
- rtacin[.]zotebsca[.]net
- aliragifut[.]zotebsca[.]net
- eztcu[.]zotebsca[.]net
- ukajusi[.]zotebsca[.]net
- okypag[.]zotebsca[.]net
- ubapimiwdj[.]zotebsca[.]net

创建的文件和/或目录

- %WinDir%\edaraxoz.exe
- %AppData%\uqetukykopefyvij\02000000
- %AllUsersProfile%\uqetukykopefyvij\02000000
- %AppData%\uqetukykopefyvij\01000000
- %AllUsersProfile%\uqetukykopefyvij\01000000
- %AppData%\uqetukykopefyvij\00000000
- %AllUsersProfile%\uqetukykopefyvij\00000000
- %WinDir%\ukavdnlj.exe

文件散列值

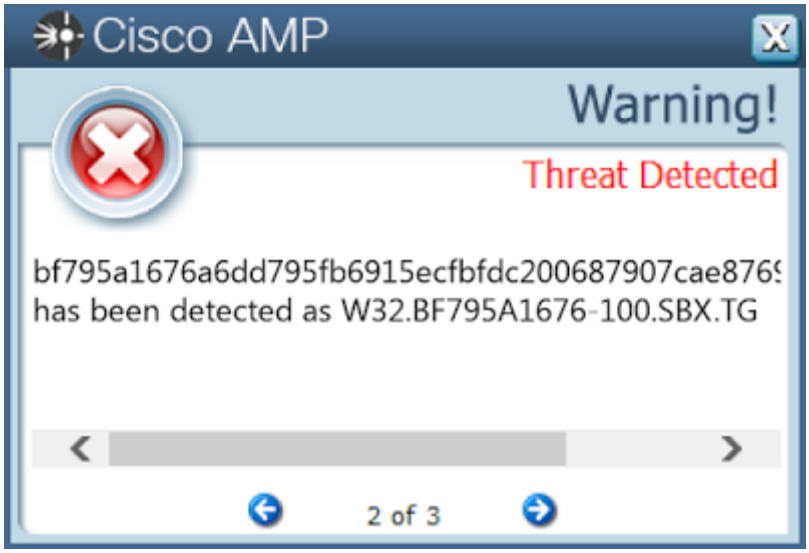
- 1a78a5c1c4ebb8a0047cbb4a8a27782212603d71cae2aeb033bceab76795a294
- 4312486eb32d7edc49d437a598d7e0453e8c9d1222b8b9ba429c73e0598db1a9
- 58f36594d9502e3e8e135d0a449e5c07a62ae6fcd34a32c5c4d9243cb28d958b
- 5c66755aeeed65c21c8d9774baebd79c962311a57b733cb19d4d2bb6a0eb52c3
- ae7a23e9b4c2645c26dce4a83a97953fa5ca008570aa9ac32e0826369593a099
- ba4fe6e91aae42e7a12747422443a361201898a4a5d2454472cf8d42b8d5cc52
- bf795a1676a6dd795fb6915ecfbfdc200687907cae8769c55b9e26328b026f88
- cc07ae7275b177c6882cffce894389383ca2c76af5dc75094453699252c9c831

防护

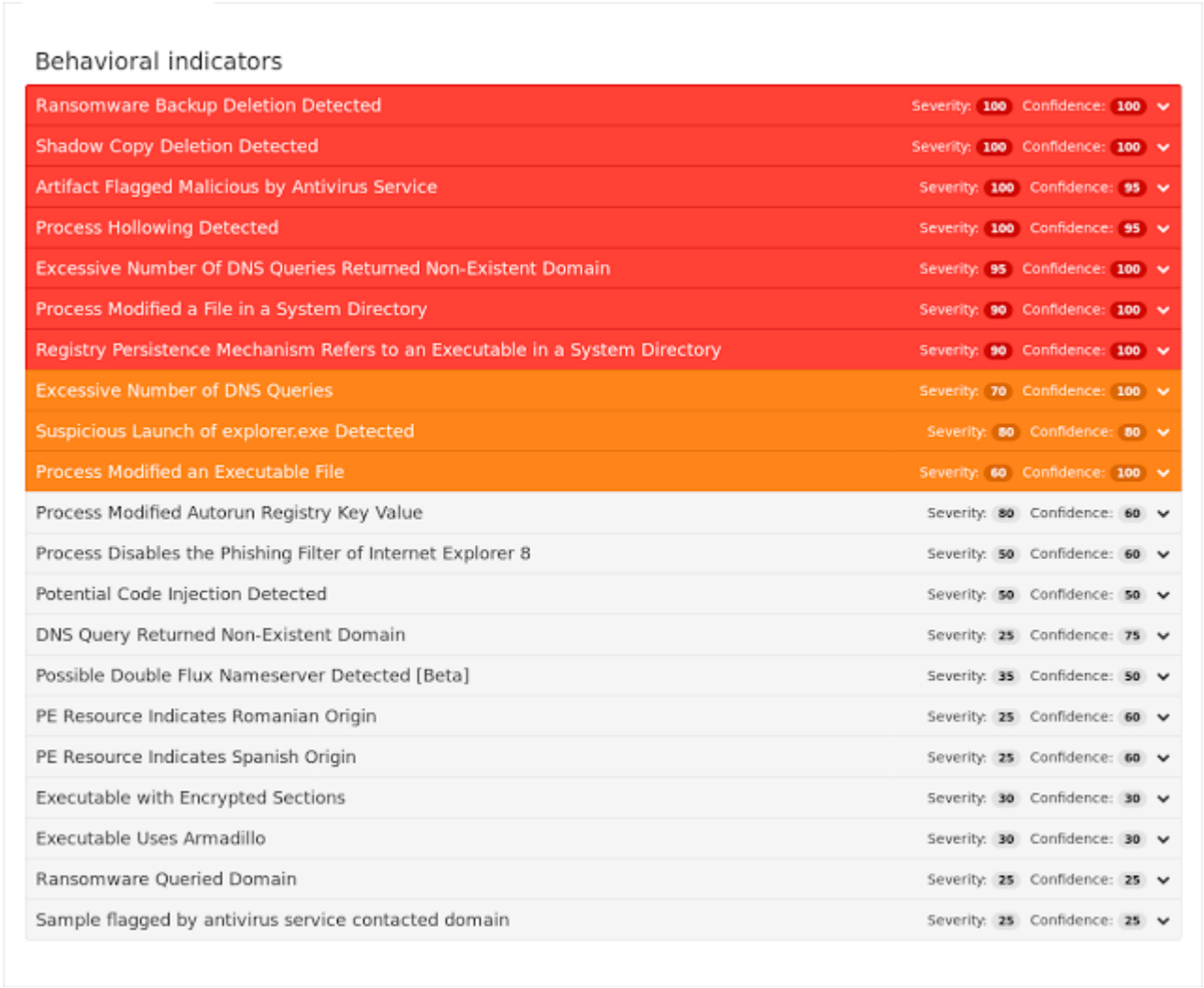
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

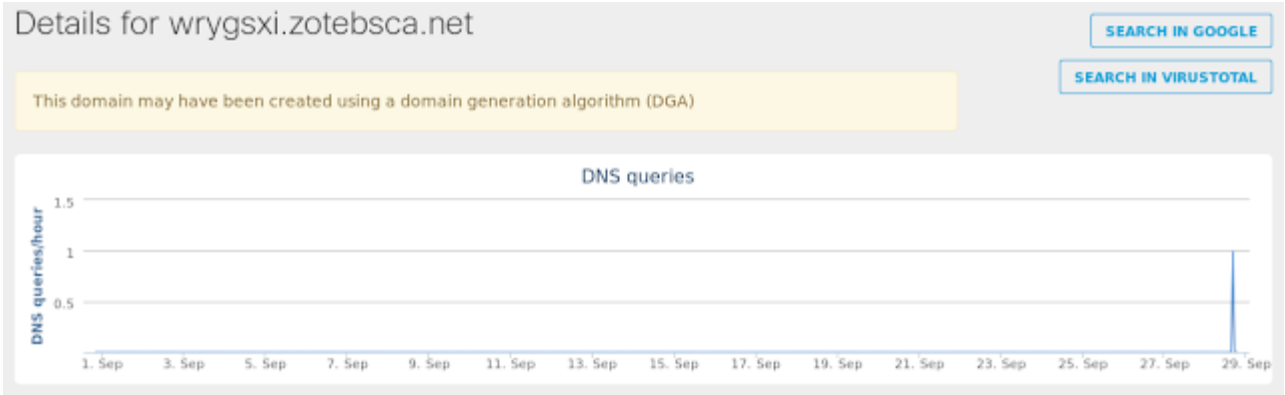
AMP



ThreatGrid



Umbrella



Win.Spyware.CCBkdr-6336251-2

感染指标

注册表项

- **<HKLM>\HKLM\SOFTWARE\Piriform\Agomo**
  - **值：**NID
- **<HKLM>\HKLM\SOFTWARE\Piriform\Agomo**
  - **值：**TCID
- **<HKLM>\HKLM\SOFTWARE\Piriform\Agomo**
  - **值：**MUID

互斥体

- 不适用

IP 地址

- 216[.]126[.]225[.]148

域名

- 不适用

创建的文件和/或目录

- 不适用

文件散列值

- 04622bcbeb45a2bd360fa0adc55a2526eac32e4ce8f522eaeb5bee1f501a7d3d
- 1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff
- 30b1dfd6eae2e473464c7d744a094627e5a70a89b62916457e30e3e773761c48
- 53c6ad85a6b0db342ce07910d355dad53765767b4b9142912611ec81bee0f322
- 6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9
- 8562c9bb71391ab40d4e6986836795bcf742afdaff9a936374256056415c5e25
- 8a8485d2ba00eafaad2dbad5fad741a4c6af7a1eedd3010ad3693d128d94afab
- dbf648e5522c693a87a76657e93f4d44bfd8031c0b7587f8b751c110d3a6e09f
- 07fb252d2e853a9b1b32f30ede411f2efbb9f01e4a7782db5eacf3f55cf34902
- 128aca58be325174f0220bd7ca6030e4e206b4378796e82da460055733bb6f4f
- 27a098761e8fbf4f0a7587adeee8eb787c0224b231b3891fa9323d4a9831f7e5
- 2bc2dee73f9f854fe1e0e409e1257369d9c0a1081cf5fb503264aa1bfe8aa06f
- 2c020ffa3436a69a1b884b5b723909c095e5e58406439287ac4c184a3c3c7da7

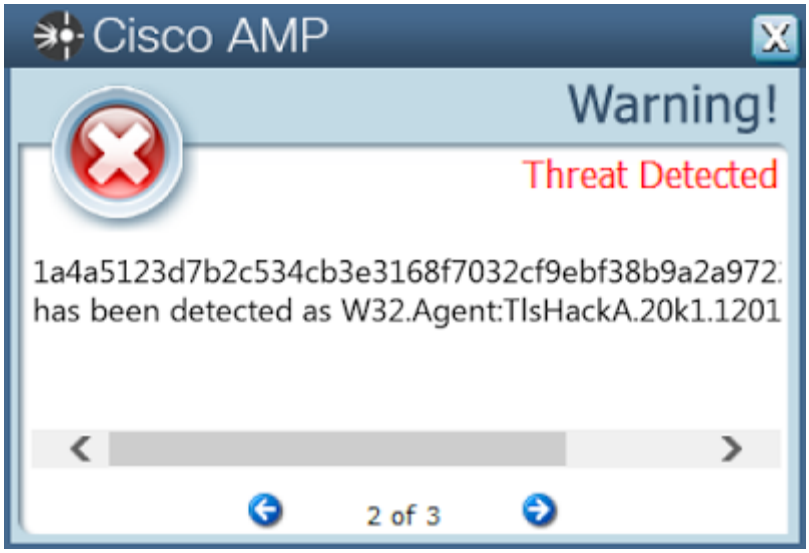
- 76cd0370af69d5c76e08673976972fee53764fca67f86fcf0db208b87b7341d6
- 8038ea1b72a720f86397fd2ee1f386bb832e5cbd8e12f97e11e0c787bde9e47e
- dc9b5e8aa6ec86db8af0a7aa897ca61db3e5f3d2e0942e319074db1aaccfdc83
- e8e02191c1b38c808d27a899ac164b3675eb5cadd3a8907b0ffa863714000e72
- f0d1f88c59a005312faad902528d60acbf9cd5a7b36093db8ca811f763e1292a

防护

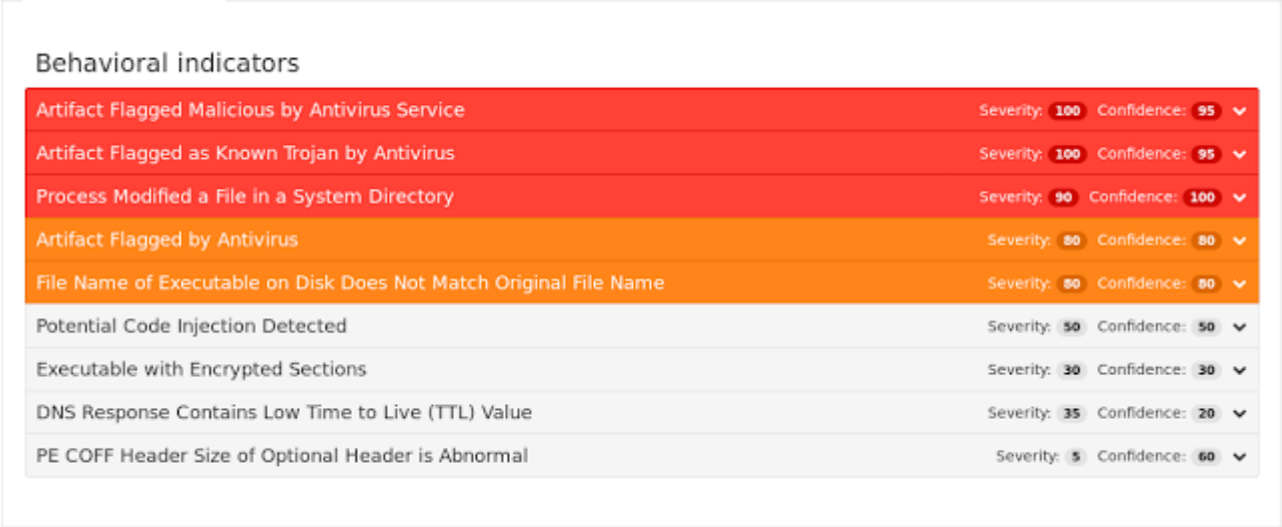
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

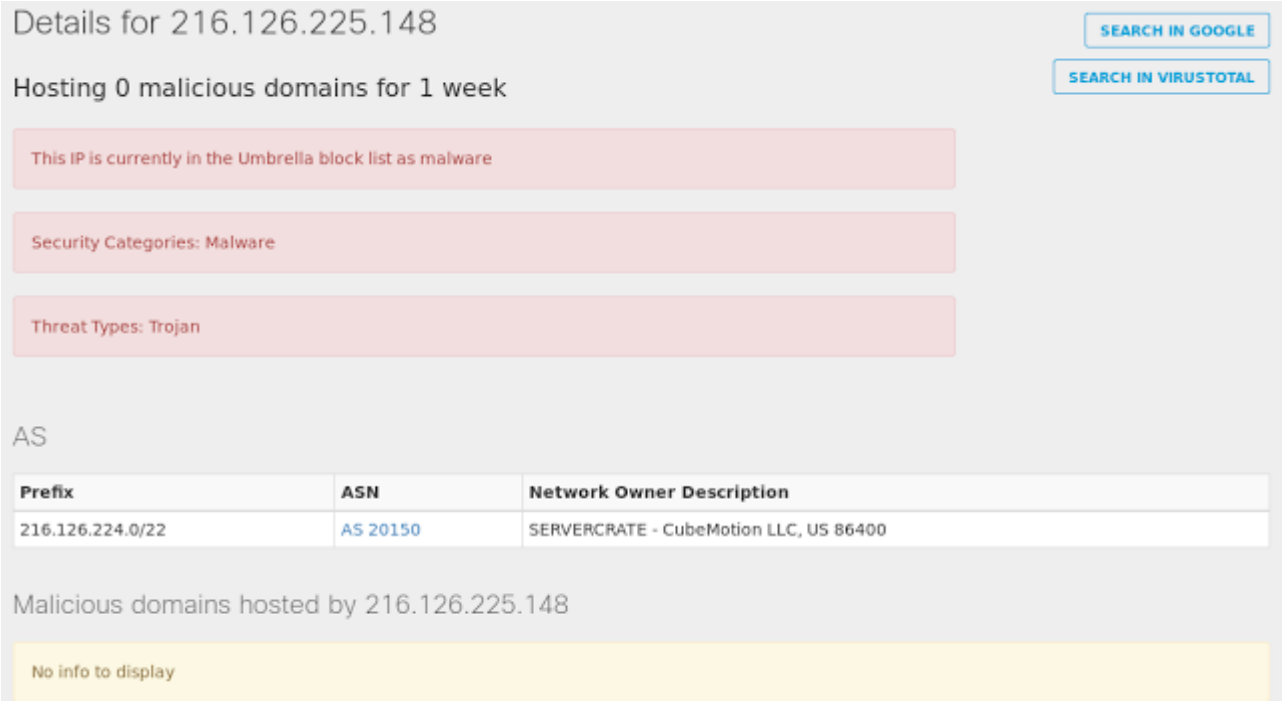
AMP



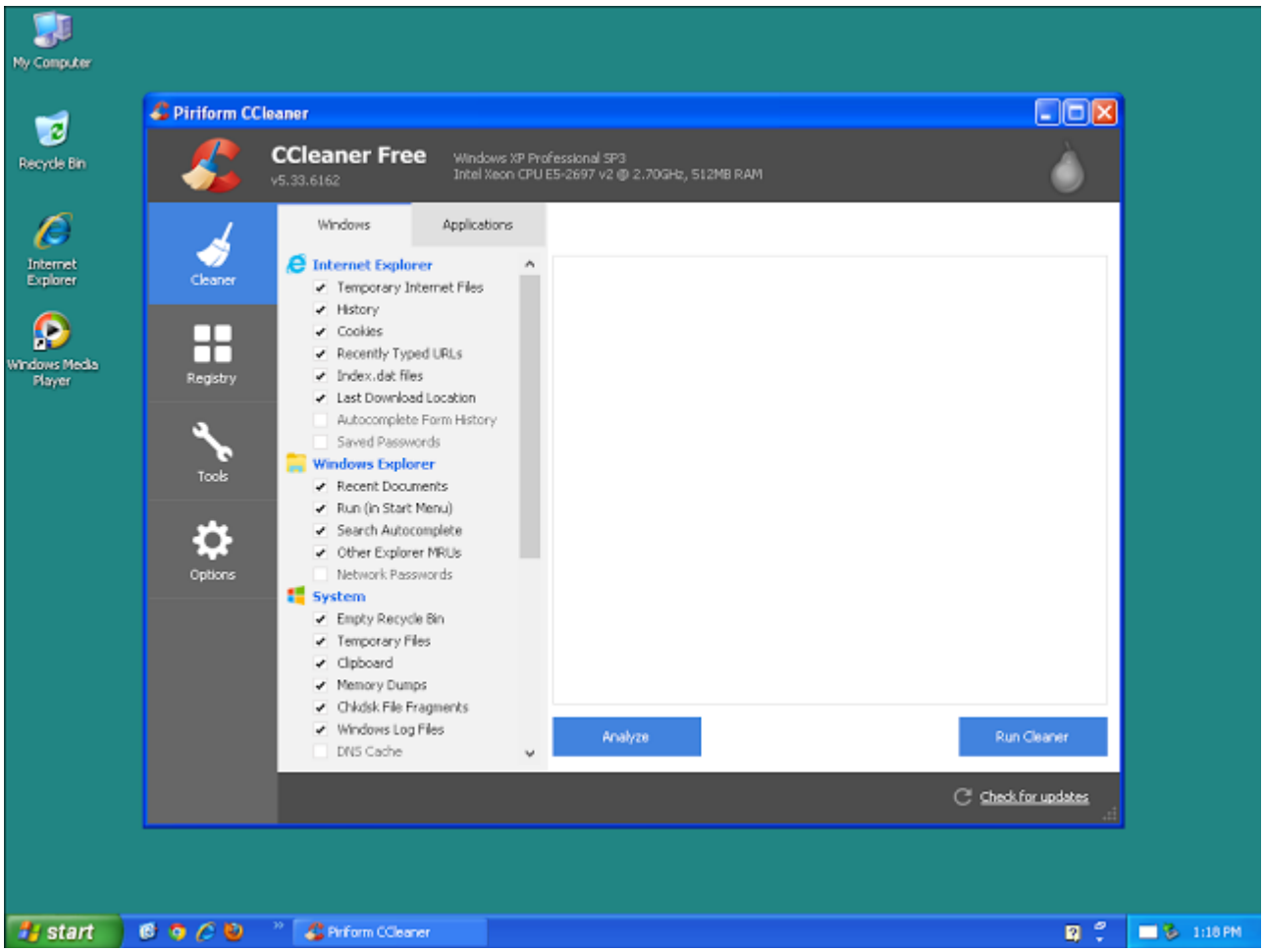
ThreatGrid



Umbrella



屏幕截图



Win.Trojan.Beeldeb-6336738-0

感染指标

注册表项

- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2**

互斥体

- \BaseNamedObjects\hTGfNaKIQ4lPz

IP 地址

- 41[.]45[.]138[.]91
- 156[.]203[.]64[.]64

域名

- microsoft[.]net[.]linkpc[.]net

创建的文件和/或目录

- %TEMP%\EqEhol.exe
- %TEMP%\JTVxon.txt
- %TEMP%\NJiSUL
- %AppData%\njisul\NJiSUL
- %AppData%\njisul\EqEhol.exe
- %AppData%\njisul\fXMIDZ.exe
- %AppData%\njisul\JTVxon.txt
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\gmail.lnk

文件散列值

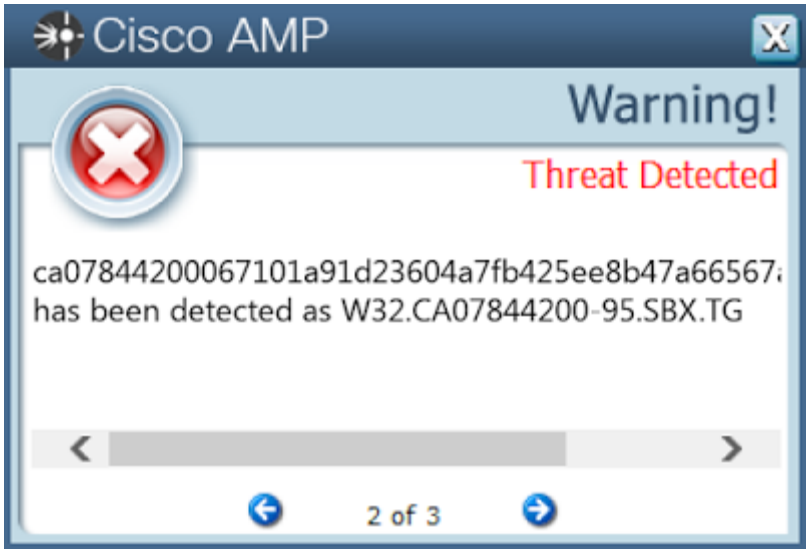
- bb8e4aec824aa052fdda739abb8472caf2bd6c34d1773248ea3072e5c024140a
- 2c89cbab497a1a5219b5d66f1ba39473b6ffc15ec4f53a2bb09c070a15a537e8
- 36e92852d67e66cb3c99312f107f83080605c2badf787108f619d6b54e6c85fc
- 1e76a00a1e6e4265ad5ff364d3139a62013a9628d90edd7e6a155e7f0a8193e8
- 07de12cf4c78151a0bdd6d8dcf8b5d0b91f51b606fd8ec0774e54fcb16e3440a
- e15dc2879dccd3c62d77169fe77d869455e61e2706006da829013d55b42107ba
- ca07844200067101a91d23604a7fb425ee8b47a66567a953103a9949f66d74cc
- c4cf29d4e6a6b905e08534108ab07318d5704d91df50c9d5477b998a19395eff
- a864f592f8fd01a57cf8302056a413e4a688f6cfa2beae8c5e136a40384f7b56
- eea366f807de6e4a0834e9fcf8dc0847b7ab4707314191448950a22cc0dbfa76

防护

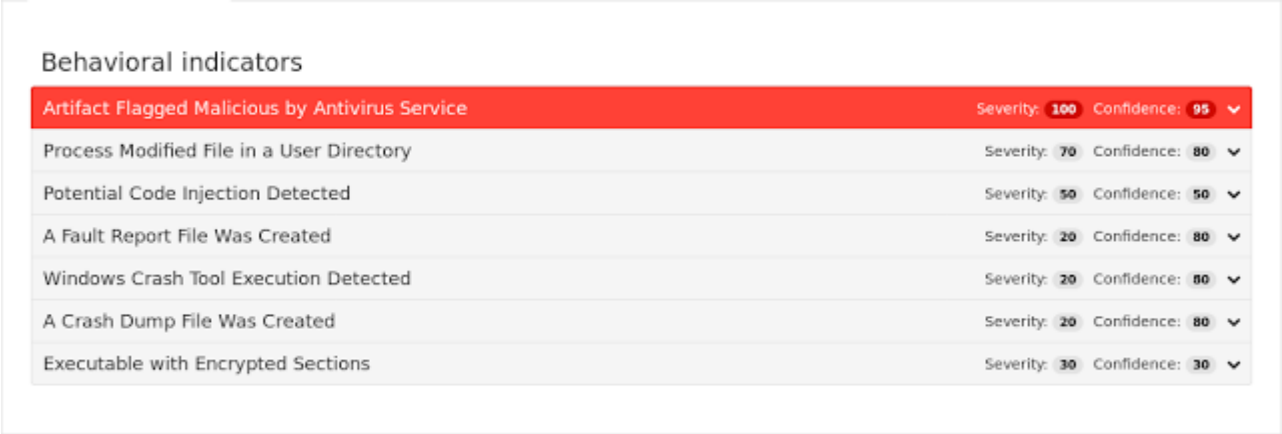
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Win.Trojan.Cossta-237

感染指标

注册表项

- **<HKLM>\SYSTEM\ControlSet001\Services\Alerter**

互斥体

- \BaseNamedObjects\44-41

IP 地址

- 不适用

域名

- wenrou88[.]3322[.]org

创建的文件和/或目录

- %SystemDrive%\Program Files\Microsoft Explorer\AAA.exe

文件散列值

- e8feccbab518346c0ec9ea3787f3b09994e41ca278aa537bc753fa1d6b40d1c4
- b955412a8b6ec7d48b70bc2ed05226755c2b418a075fd0e3f98ba52086caa495

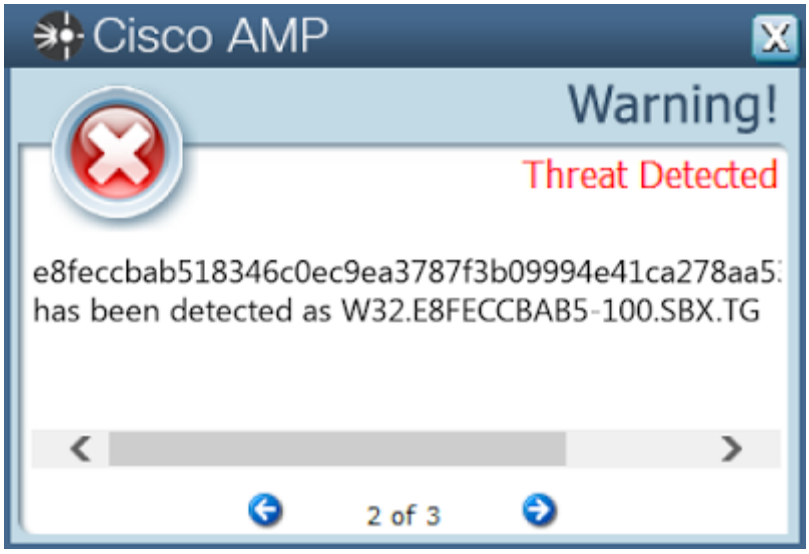
- de37309306863d4a1b6f12a9c6e047fd93a9645f8acdbcc2f36f65d00226af2d
- 2e3b79c0bc90f46218700afba5d5a55cb00832969a00f254ec113d342d76a992
- 38a58d5c41f91b483ae727e922039848e14410c485db577cd0e21ee28e8fa250
- 424e36fd9975a43f25fad06e0282833d1280bcd9e6d5ef8221dc322fd16fbaa0
- 83062a56de8404db9311d60c87cccc4c25a8887952e695e5ffa0ac2600606706
- 94bc3ce60f0750456467c4262543e1196eb8a3294fcd79441ef7250e8fdf7885
- 5ed30bc2f7412875ccba2ade6e124154eda0788d555978ab6b60a69dbdf0bac1
- f81a1362894fa49b7008cffe93365ef2158180be9a935ae17acc2bafa8f983d9
- 6e678b7d3a7a46f20a19079644f0d879f03b1cad83e441ca64a4c0d1076d9ebb
- f9e9a3d7b7bffae8cda1b3ff4c893933eff386b26fd035fa4bb61c7c31bf2690
- 53c7cececf2d29386f3184e588c5a0ec558292ff227891d3ce5605f82a5f9688
- dfbafa207c90d3d4e20dabe7620f901e1abe30fa0fa4dd06bfabe852f8f1f0bc

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

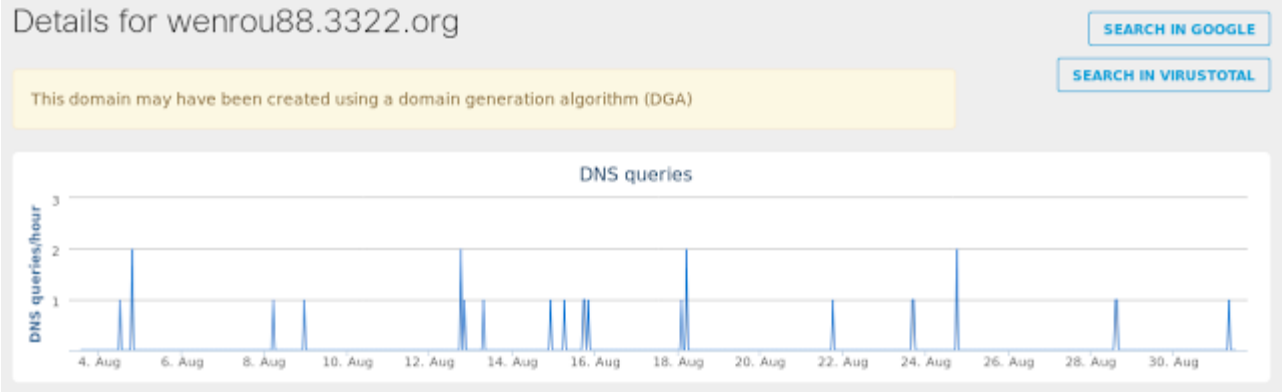


ThreatGrid

Behavioral indicators

Detected Trojan Added As Service	Severity: 100 Confidence: 100
Artifact Flagged Malicious by Antivirus Service	Severity: 100 Confidence: 95
Artifact Flagged as Known Trojan by Antivirus	Severity: 100 Confidence: 95
Process Deleted the Submitted File	Severity: 90 Confidence: 90
Process Modified a File in the Program Files Directory	Severity: 80 Confidence: 90
Artifact Flagged by Antivirus	Severity: 80 Confidence: 80
File Name of Executable on Disk Does Not Match Original File Name	Severity: 80 Confidence: 80
Process Modified an Executable File	Severity: 60 Confidence: 100
Executable Artifact Imports Tool Help Functions	Severity: 50 Confidence: 70
Potential Code Injection Detected	Severity: 50 Confidence: 50
Process Added a Service to the ControlSet Registry Key	Severity: 50 Confidence: 50
DNS Query Returned Non-Existent Domain	Severity: 25 Confidence: 75
Possible Double Flux Nameserver Detected [Beta]	Severity: 35 Confidence: 50
Hook Procedure Detected in Executable	Severity: 35 Confidence: 40
Executable Uses Armadillo	Severity: 30 Confidence: 30
Sample flagged by antivirus service contacted domain	Severity: 25 Confidence: 25
RAT Queried Domain	Severity: 25 Confidence: 25

Umbrella



Win.Worm.Untukmu-5949608-0

感染指标

注册表项

- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\INSTALLER**
  - **值：**DisableMSI
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**System Monitoring
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\EXPLORER**
  - **值：**NoFolderOptions
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SYSTEM**
  - **值：**DisableCMD
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM**
  - **值：**DisableRegistryTools
- **<HKCU>\CONTROL PANEL\DESKTOP**
  - **值：**ScreenSaveTimeOut

- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\CABINETSTATE**
  - **值：**FullPathAddress
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**xk
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\WINDOWS NT\SYSTEMRESTORE**
  - **值：**DisableConfig
- **<HKLM>\SYSTEM\CONTROLSET001\CONTROL\SAFEBOOT**
  - **值：**AlternateShell
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\AEDEBUG**
  - **值：**Debugger
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\INSTALLER**
  - **值：**LimitSystemRestoreCheckpointing
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON**
  - **值：**Userinit
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**internat.exe
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM**
  - **值：**DisableRegistryTools
- **<HKCU>\CONTROL PANEL\DESKTOP**
  - **值：**SCRNSAVE.EXE
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\AEDEBUG**
  - **值：**Auto
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\WINDOWS NT\SYSTEMRESTORE**
  - **值：**DisableSR
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\ADVANCED**
  - **值：**HideFileExt
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\ADVANCED**
  - **值：**ShowSuperHidden
- **<HKCU>\CONTROL PANEL\DESKTOP**
  - **值：**ScreenSaverIsSecure
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**MSMSGS

- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**LogonAdministrator
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER\ADVANCED**
  - **值：**Hidden
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\ACTION CENTER\CHECKS\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.CHECK.0**
  - **值：**CheckSetting
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON**
  - **值：**Shell
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\EXPLORER**
  - **值：**NoFolderOptions
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**ServiceAdministrator
- **<HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System**
- **<HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\Explorer**
- **<HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run**
- **<HKLM>\SOFTWARE\CLASSES\lnkfile\shell\open\command**
- **<HKCU>\Control Panel\Desktop**
- **<HKLM>\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows NT\SystemRestore**
- **<HKLM>\SOFTWARE\CLASSES\batfile\shell\open\command**
- **<HKCU>\Software\Policies\Microsoft\Windows\System**
- **<HKLM>\SOFTWARE\CLASSES\piffile\shell\open\command**
- **<HKLM>\SYSTEM\CurrentControlSet\Control\SafeBoot**
- **<HKLM>\SOFTWARE\CLASSES\LNKFILE\SHELL\open**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState**
- **<HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\AeDebug**
- **<HKLM>\SOFTWARE\CLASSES\lnkfile**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Run**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer**
- **<HKLM>\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\Installer**
- **<HKLM>\SOFTWARE\CLASSES\exefile**

- **<HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon**
- **<HKLM>\SOFTWARE\CLASSES\exefile\shell\open\command**
- **<HKLM>\SOFTWARE\CLASSES\LNKFILE\shell**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\Policies\System**
- **<HKLM>\SOFTWARE\CLASSES\comfile\shell\open\command**

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

- %System32%\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
- %WinDir%\setupact.log
- %System32%\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
- %System32%\wdi\LogFiles\BootCKCL.etl
- %WinDir%\Tasks\SCHEDLGU.TXT
- %System32%\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90485d}\S-1-5-21-2580483871-590521980-3826313501-500_UserData.bin
- %System32%\wfp\wfpdiag.etl

文件散列值

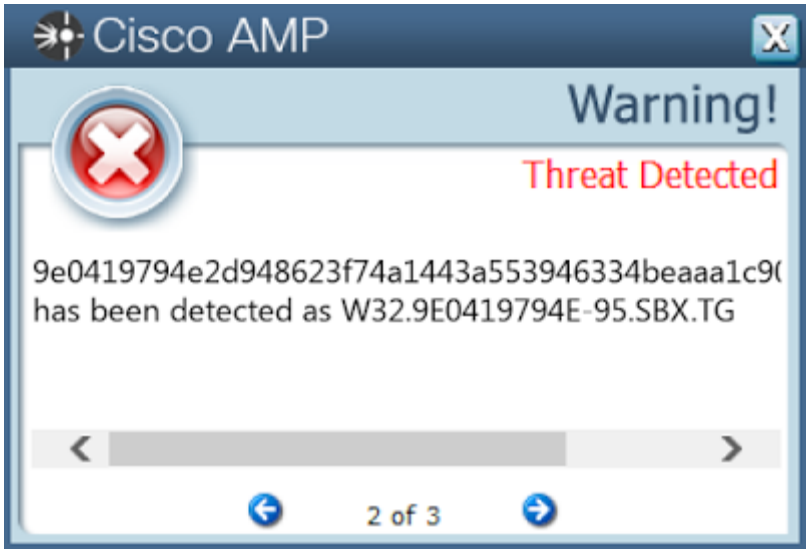
- 9e0419794e2d948623f74a1443a553946334beaaa1c902ddc2741b1586a3bd89
- 6735181a112e87550dba81d667012250ff78959cdfe4852043c35895a4a53635
- fdb82a1a0c8b84d22d87e373d37a09cbbee481eca77a695f0a42b0ce8e7d15fb
- 1c3d3774371a96d8dac17ef186e1d10e6520fc82d9325974f4191d437bfa106a
- c7e85bc2b8120dec204e5592ab9254e90030cf3a13a2281d047c1d0bcb878d10

防护

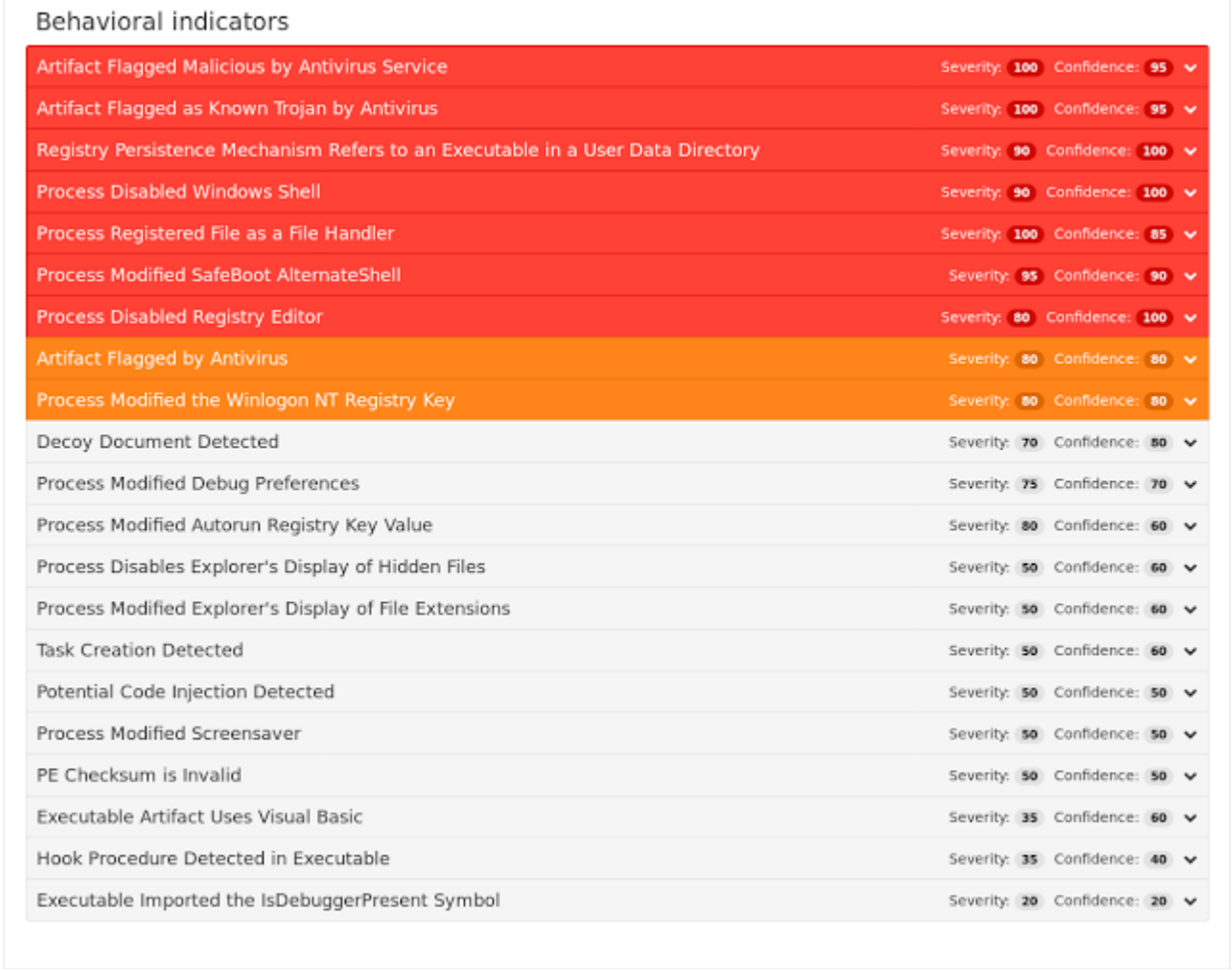
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



发布者：ALEXANDER CHIU；发布时间：16:56
标签：AMP、CLAMAV、防护、SNORT、一周威胁综述、UMBRELLA