2017 年 9 月 15 日，星期五

一周威胁综述（9 月 8 日至 9 月 15 日）

本文概括介绍 Talos 在 9 月 8 日至 9 月 15 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.Agent-6336340-0**
  Office 宏下载程序
  这类下载程序使用 VBA 中的字符串混淆来构建 shell 下载命令，并通过 VBA Shell 函数执行命令。

- **Doc.Macro.Obfuscation-6336210-0**
  Office 宏
  这一类型的 Office 宏文档采用同样的混淆技术来阻止快速分析。大部分脚本内容由未使用的字符串和注释组成。

- **Doc.Trojan.Valyria-6336191-0**
  木马
  这类下载程序使用 VBA 中的字符串混淆为 powershell 命令构建下载命令，并通过 VBA Shell 函数执行命令。

- **Rtf.Exploit.CVE_2017_0199-6335035-0**
  漏洞攻击
  这些样本是包含嵌入式 OLE2 对象的 RTF 文档。创作者试图通过在 RTF 文档中的对象数据之间插入假命令来混淆 OL2E 对象，而实际的 OLE2 对象则包含指向另一个文档的链接。如果链接的文档是 .hta 文件，则会在 RTF 文档的环境中下载并执行该文件。此漏洞攻击利用的是已知漏洞 CVE-2017-0199。

- **Win.Malware.Cmig-6336177-0**
  加壳程序
  Cmig 是一种加壳程序，可用于混淆银行木马等大量恶意负载。Cmig 最近一次出现是在近期的网络钓鱼活动中，相关文件名包括“Transfer_copy.pdf.scr”和“(PO) No.2029243EL0003.exe”等。

- **Win.Malware.Ursnif-6336328-0**
  木马/下载程序
  Ursnif 的用途是从受感染的主机窃取敏感信息，但也可用作恶意软件下载程序。通过近期以日本收件人为目标并使用 XLS 下载程序附件进行攻击的恶意垃圾邮件活动，可以看出其感染率有所提高。此特定变体依靠极长的主函数来脱壳，导致 CFG（控制流图）的节点超过 1000 个。它还需要依靠 API 攻击和额外的 API 解析进行处理，才能将脱壳的代码复制到堆中进一步执行。

- **Win.Trojan.Agent-1356499**
  木马
  此样本是企图与外部服务器进行通信的木马。我们所分析的样本经过加壳，并且能够进行反 VM 检查。不过，这些样本是在检测环境中运行的。在分析过程中，样本联系了多个域，其中包括 VirusTotal。出乎意料的是，这些样本上传了一个样本供扫描。此外，这些样本还修改了 IDT 并下载了其他文件。

- **Win.Trojan.Symmi-6336247-1**
  木马
  该样本为 Symmi 的一种变体，它会创建额外的二进制文件，并通过创建计划任务以及在 AppInit_DLLs 注册表值中添加恶意 DLL 的路径（使其能被加载到系统中运行的每个用户模式进程中）而持久驻留在系统中。

威胁

Doc.Downloader.Agent-6336340-0

感染指标

注册表项

- 不适用

互斥体

- \BaseNamedObjects\Global\VLock

IP 地址

- 216[.]239[.]38[.]21
- 216[.]239[.]34[.]21
- 88[.]150[.]140[.]232
- 216[.]239[.]32[.]21
- 185[.]99[.]2[.]75
- 5[.]133[.]179[.]13
- 78[.]47[.]139[.]102
- 103[.]27[.]235[.]82

- 192[.]168[.]1[.]255
- 192[.]168[.]1[.]1
- 216[.]239[.]36[.]21
- 127[.]0[.]0[.]4
- 93[.]171[.]217[.]7
- 192[.]168[.]1[.]248

域名

- 12[.]242[.]40[.]8[.]zen[.]spamhaus[.]org
- myexternalip[.]com
- ipinfo[.]io
- tregartha-dinnie[.]co[.]uk

创建的文件和/或目录

- \Users\Administrator\Documents\20170913\PowerShell_transcript.PC.hwKj6yIW.20170913092128.txt
- \Users\Administrator\Documents\20170913\PowerShell_transcript.PC.EvG+kj6G.20170913092130.txt
- %AppData%\winapp\Modules\systeminfo64
- %SystemDrive%\DOCUME~1\ADMINI~1\LOCALS~1\Temp\697359.cvr
- %AppData%\winapp\Modules\injectDll32
- %TEMP%\ytkqvnx_o.exe
- %AppData%\winapp\qbmw.exe
- %TEMP%\CVR40C2.tmp.cvr
- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\rcnx.exe
- %AppData%\winapp\group_tag
- %WinDir%\Tasks\services update.job
- %TEMP%\gytdgo9.bat
- %AppData%\winapp\Modules\injectDll64_configs\dpost
- %System32%\Tasks\services update
- %AppData%\winapp\Modules\injectDll64_configs\dinj
- %AppData%\winapp\xsjpumw_n.exe
- %AppData%\winapp\palv.exe
- %AppData%\winapp\Modules\injectDll64
- %AppData%\winapp\Modules\systeminfo32
- %AppData%\winapp\client_id
- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\wvzyhlyh.bat
- %AppData%\winapp\Modules\injectDll64_configs\sinj

文件散列值

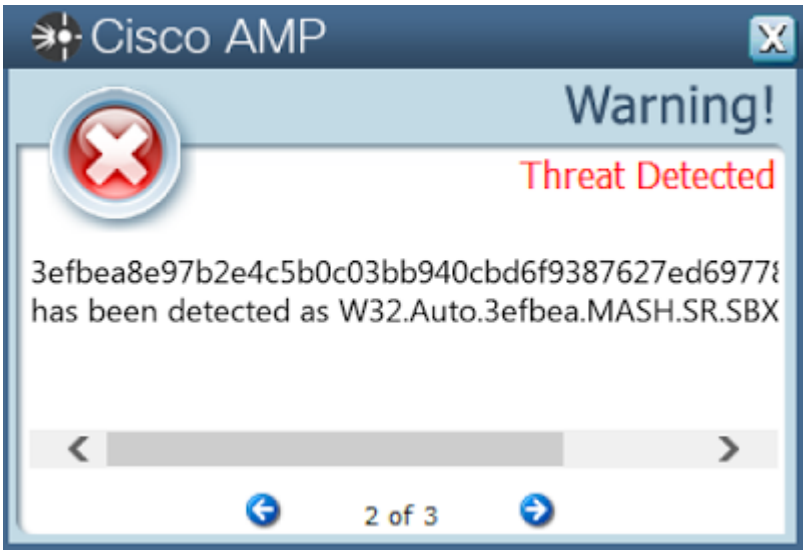
- 3efbea8e97b2e4c5b0c03bb940cbd6f9387627ed6977844bcc69613738089caa
- a8d06bd505e658dd9274b4c8ba0805d8c9b19ee65a8eb7fe6a3c388487dc0875

防护

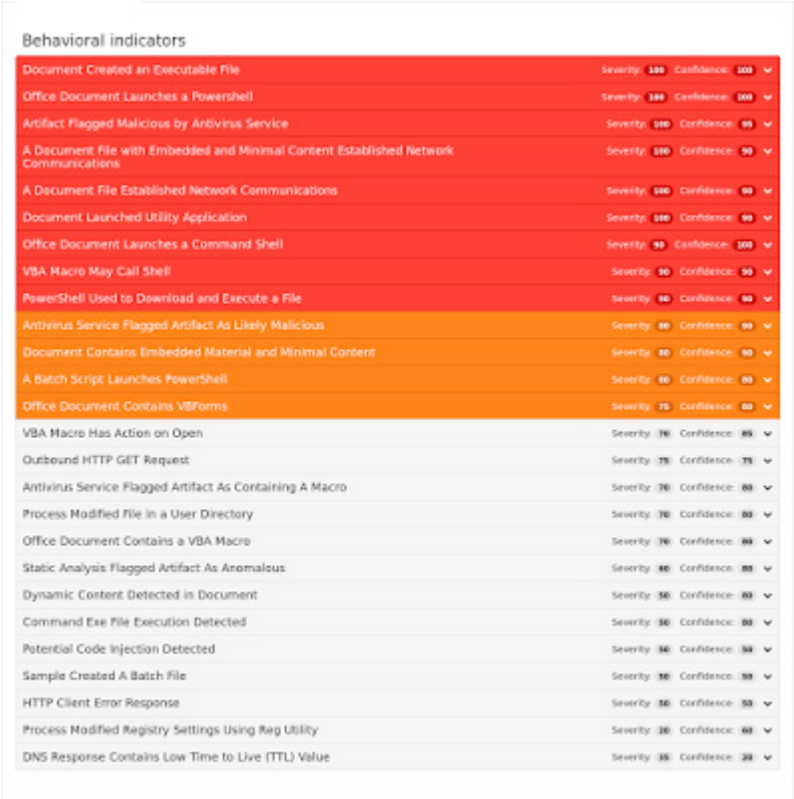
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

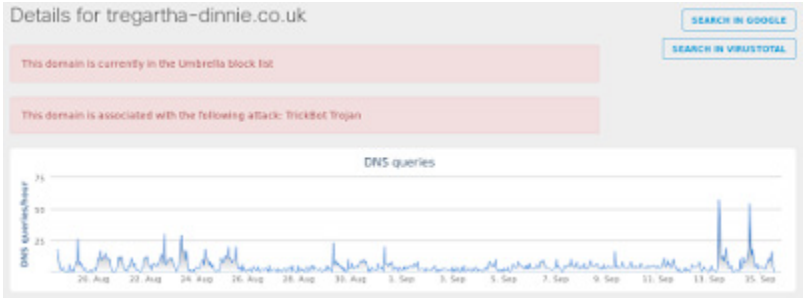
AMP



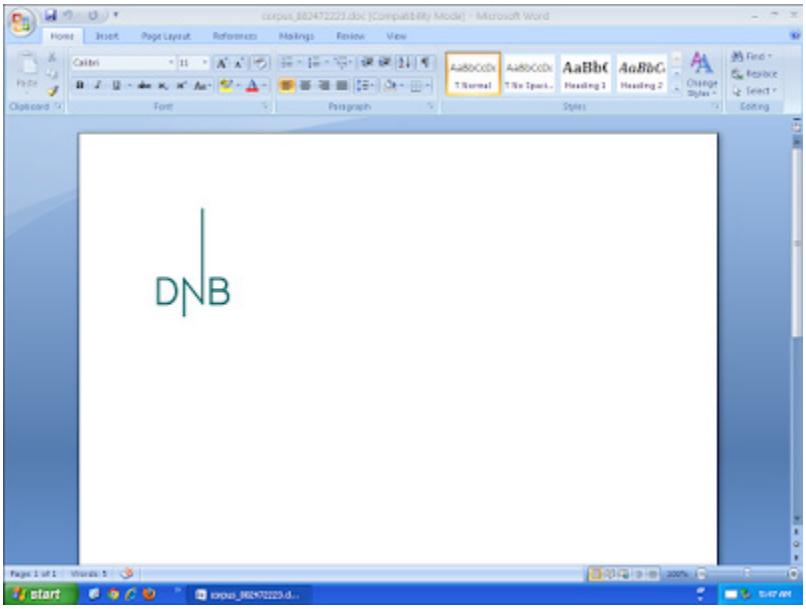
ThreatGrid



Umbrella



屏幕截图



Doc.Macro.Obfuscation-6336210-0

感染指标

注册表项

- **<HKCU>\SOFTWARE\MICROSOFT\OFFICE\14.0\WORD\RESILIENCY\STARTUPITEMS**
  - **值：**dz~
- **<HKCU>\SOFTWARE\MICROSOFT\OFFICE\14.0\WORD\RESILIENCY\STARTUPITEMS**
  - **值：**oy~
- **<HKCU>\SOFTWARE\MICROSOFT\OFFICE\14.0\WORD\RESILIENCY\DOCUMENTRECOVERY\42D7BE7E**
  - **值：**42D7BE7E

互斥体

- 不适用

IP 地址

- 52[.]173[.]193[.]166
- 174[.]136[.]52[.]222

域名

- tmsgroup[.]mx

创建的文件和/或目录

- %TEMP%\myfileepepe.exe
- \TEMP\propuesta_de_trabajo_795370.doc
- \Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\40DVD2HR\sound[1].htm

文件散列值

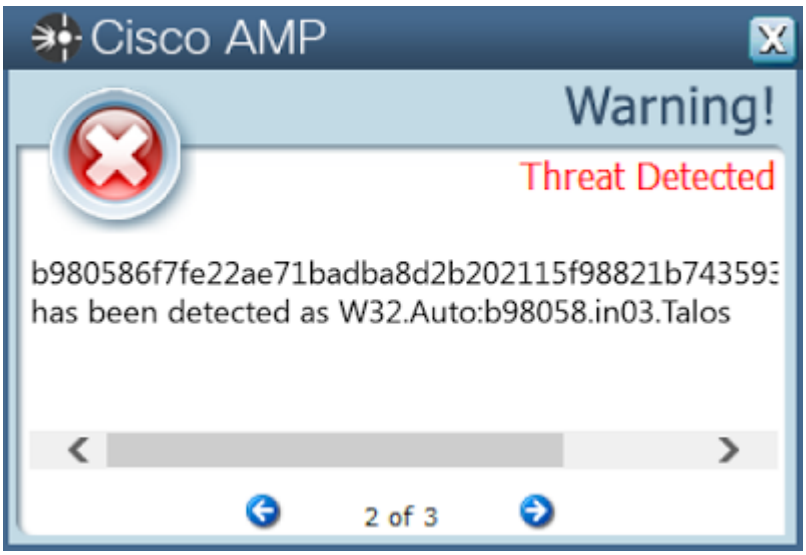
- b980586f7fe22ae71badba8d2b202115f98821b743593ca36e15387fbda4f361
- 0dd881a73d020780715e7a4ee943288fe5174ff27ae3ae90405785e8f584c225
- 179d8ad5e80d814aa8d04633ac9c624b60f2273e50dcd6ae5fd7441522ea714e
- 52568babc56f75ce343d9d8bf5ecb51af0a6d9d31fa60a2875b116a81064ee78
- 6891e0c2fe9c3b7bf9c02fbd81950c60118df47cf8e7d80ca92853fae72d9178
- 7df129105042ea8a4270ca975b97456bc819264864bf2992538a2558c3da9146
- 9416f466a01d60b4bccaf8658b0a78bbe84a8de3a1bc1abb77e541e224a6c197
- ad07da4920298c11f896748053f37a1a532d7b10077af762f4e0b8ca60d6b4a2
- b2158897b2fcd2ab2e6304c5c9da2d7af506356ded5b9e63d4421c5565d11123
- d0b4b36c3c50c58869ae58f34c9d05c4ae8333e20d29b6c35d85cc85a5d7e38c
- d4a60bcec8d6317d30262bfaa2d5c425c60d1cc42827f37b2fc7fbb5795a1557
- e03707413922ee8af0178296855bda42f2e0e86f1e34a63022dfd6e582cecd61
- e9e03d8cf474e69197beefecdb5db453740cb4349535dffe4476febee8e5fc8b
- 012852f831aa5af389baf81195874e6423d87959989787fc6921823c1bfbe293
- 1a0d042c3e9c5a0e3b36981e436b30cf5b40139f61877f6011a2c6b8934dc5fa
- 321fb4eb45e839e819b923aebb59c20368dd5c232e1a429fd4a41b8ee70d785c
- 3d27ace6341c0756a8a57f915e6e71fd7fd21661f1b2f0b4019199f5ae5ac30d
- 40e07a6ac949b795a75c679811ace193aa3b53dcb29c4b88ca936b6a47a1f04d
- 428810965b8c6bb09b66c83369382106d76be71f5e706622f862afd130008fdb
- 4c45540ba41c37f6c4cc0c4385139b63e56e58798c1c3ac94ea9cfca15ab8a98
- 4f4e875d64ecbc8f2aa485118d64419c9070b237171805acd9de5b04594f524e
- 51e75edc5abe46280a4ef590047bb0bf4ab0d409da07711cbd2917b4ce103c59
- 5329d1922d2e40d124aea198b8b19baa2382b52f8990f2112a396a4f6250f765
- 582e025a0a45e73aa4568cbef75d53f402dd48a941256730ffb0dacfab5ac71b

防护

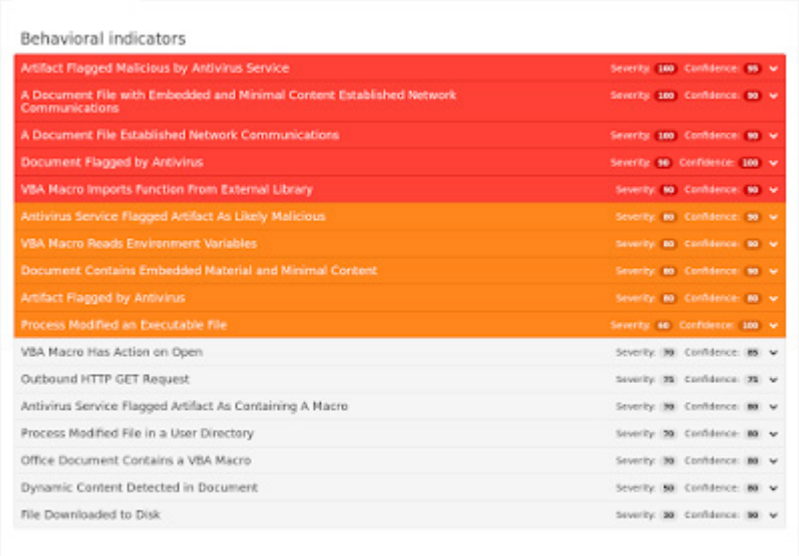
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

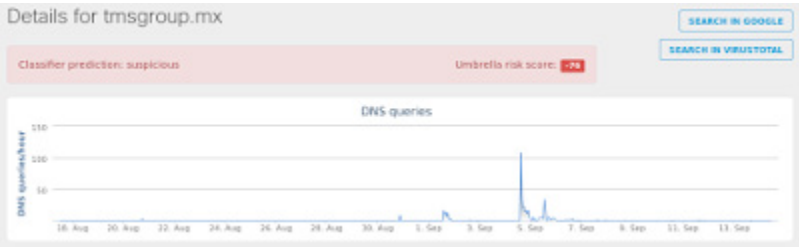
AMP



ThreatGrid



Umbrella



Doc.Trojan.Valyria-6336191-0

感染指标

注册表项

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

互斥体

- 不适用

IP 地址

- 不适用

域名

- workupe[.]us
- kekeoffer[.]com

创建的文件和/或目录

- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\vhost.exe

文件散列值

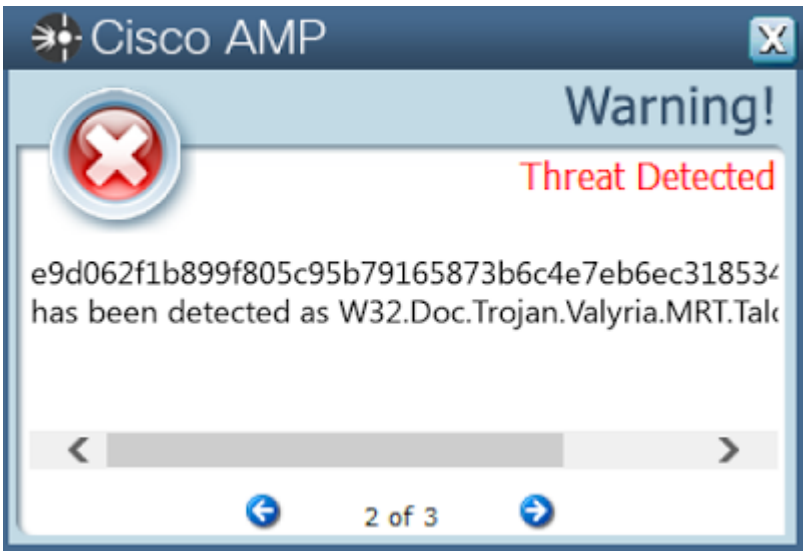
- 02a384b45673cf0c1e7dbe129fa397d92d43add25b22b080b4308def418e7927
- 0e0edccb33a141f7a9f2f57590c33eb22b599f3b2a070bf930083b5d0053fdb2
- 2c421d3fe1bce958f7a47ffa6a74ee7b6b6d0e90c95e230eced7a883d9db2505
- 31a70dff6c1abfc4a0074a72e2e45ad6e50cdb8cf9ab023655f21d4c770d6946
- 4c16cda58dbd96b74579eafe2a73740c6d98d588bdebee6a3830140d1326aafd
- 532b0c407a2c8ae3adf7c148ae64e63d8dd92fb624802d3f3992e87445274a73
- 568f8b461fe97728ebca0231b5b8b00bc85de9909ab83c7d2fc60d134739819f
- 59400bc70eab4810a1b7a5c8556879315cdc2233b51e812587fe259a3dde69a6
- 64b2b883632292f6d1bbbba7c95973a3f47c36bf70c940f262caaeb3422786c4
- 68edb052cd861ebe7dad58a9923723c1ed711ec4d965ba13a3cf10d70a90d11f
- 6df3fb420cba5fb279edfc1724af82cfd28a63c7121fb123846db6edf1594a17
- 7291b9989f4ef506f1792dd4bae6d7f8b1d4f7c770295552a05acf38a41c0b26
- 764b5f6e36f12e80dd801db166f6c1357745a1c7a5526c00e1a1eb057624f56c
- 7eed89f56f776f61421242f428edc4a93bd250e8b98fe44b6f71a67ec8a3fb08
- 80c33e29b5221557070d70c81c72b0866a7a916490fdc2bee4644f057e844283
- 8263c8ab8cf63264e39de0c237e26c7f08e36427ec47e0699f7ff8726af40db5
- af2229c42175b9c6591427f82619564c8a8a1fcb1fa3f912502b098563c12643
- af91e3a9413567bbea70a7d91b3ea4377608d0120a0e8feccab149dd2b4e497b
- b6ba50de7e2573d32975f60905d3fcd3a67bd57d5f2925a3cf7fddefae174c6e
- c9210ef989809971703aea1b0d12b83aa85fcc7e0547b877b6645456d4945051
- e9d062f1b899f805c95b79165873b6c4e7eb6ec3185347ec0d67e2d30caff67b
- f543e6e17ca16d883f3da521b9c8e0070ab7a1ee6c83eb8bca701bea7af6385f

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

Rtf.Exploit.CVE_2017_0199-6335035-0

感染指标

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 172[.]16[.]1[.]57

域名

- www[.]supernaturalspells[.]co[.]za

创建的文件和/或目录

- 不适用

文件散列值

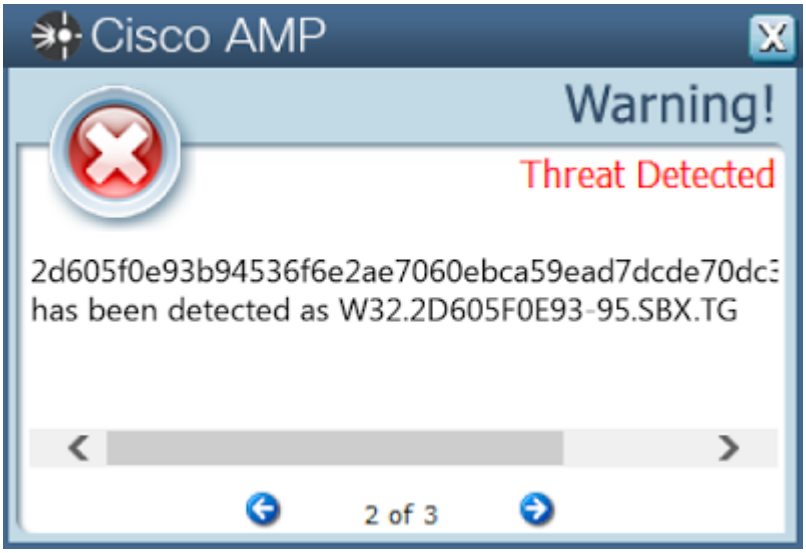
- 2d605f0e93b94536f6e2ae7060ebca59ead7dcde70dc3ea5dc99d2ed5a391afa
- 9b366a6ab581517c6d62c5195e606eba6cb764ff813df7c247f34455af7db567
- 148c4c8b544dce269b28f6d5166ff65a72d365045ce02ca36f0554834a07d7a5
- 29c4a742042b6065bc4e30c1d06c0b8b83218c87d922c024f172fc39764d1d5d
- dc730f033912235910103a20eb1c46f4c4c50e221d985a156fb7ef384c5b1bc4

防护

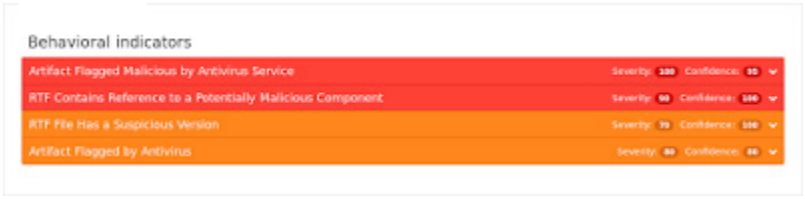
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

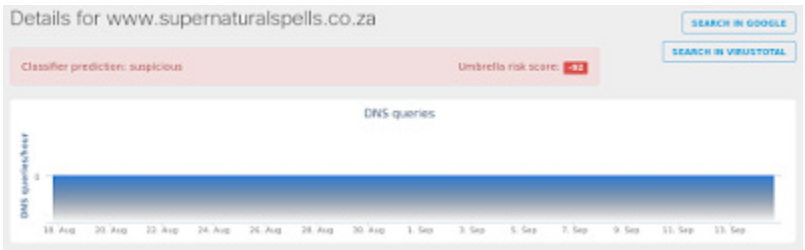
AMP



ThreatGrid



Umbrella



Win.Malware.Cmig-6336177-0

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

- 不适用

创建的文件和/或目录

- 不适用

文件散列值

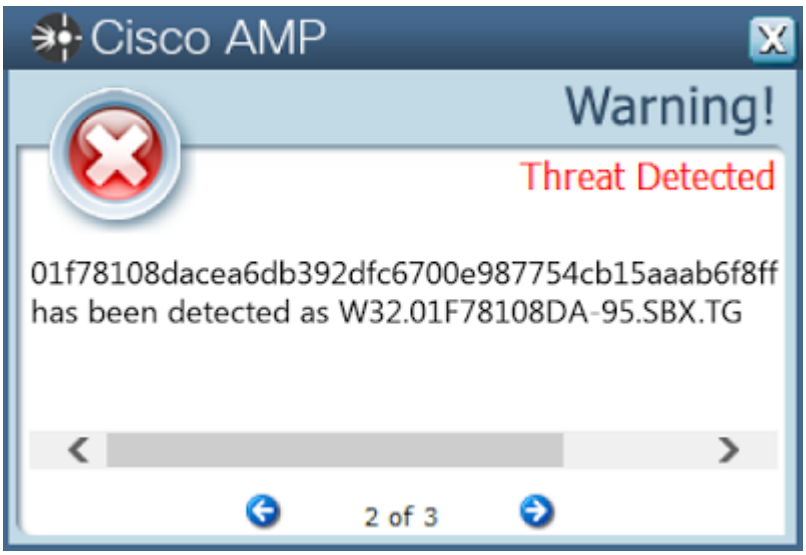
- 01f78108dacea6db392dfc6700e987754cb15aaab6f8ff85ae9349f4fcef1044
- 05baa0dc22cf5b14b5a8e70c4a0183c50f366da7916fdee0f1b26835f48e43c1
- 0898ded2110056e9bc720860640282384f08d4064918322cf99c6e79554208f6
- 09e7612bce428fb51593cfc286d7e9904a1c372771a7ad1870538a4a72046d15
- 12b2c3dd430777d50966f542668eb022b2871a3c2ec77003911080fa90c32c5b
- 14eeda627d8c65edea9e8c7b3a02f381079f1c28be3f1408a0f6f4f0968da27c
- 1828387d77ccd498e318dc2bdf580a51ef8161dfda186651cb4c6300aea6ecf5
- 251984e04c9654cab912e5ab74f510c808a3fd34bc10d81f20eef7350dc51339
- 28c5bd99d92cf80443f93cb12344cade4e9685a89e936d490b9e04edd6207f1a
- 2b9d669d44fb21199c4ad9f51566d641cb1613907c1a8f66c49c3a0766fbd386
- 2fe55bd75831905bd35b0928ecd70f064330311ec0749bda01cff595b9af6b27
- 359c0c9d53f14552ede1a37f73b4554f8fa8004ec0a25a6b6741dfd4f2df5682
- 3706c1b476c5a7093dbf71f51daa053d817668b854b99ef8ab939f2498fe253f
- 3d3d7e837aafbd8f42ade61f867114cc28af14c5d4ace788f351df0ad58cadf1
- 3ee7edf180cc44da6f2f79f90cc965dddb0eee97e32d9e340e873c71ce3d57e0

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	不适用
WSA	不适用

检测结果屏幕截图

AMP



ThreatGrid

Win.Malware.Ursnif-6336328-0

感染指标

注册表项

- **<HKLM>\SOFTWARE\Microsoft\DirectDraw\MostRecentApplication**

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

- 不适用

文件散列值

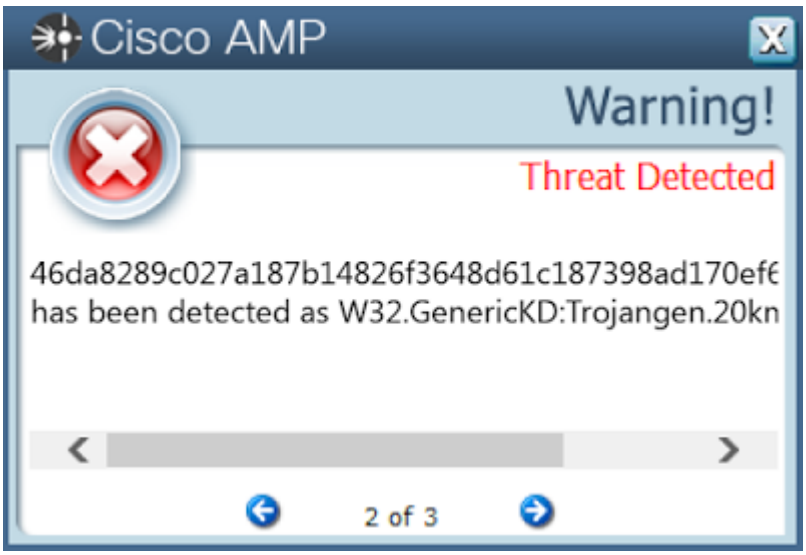
- 46da8289c027a187b14826f3648d61c187398ad170ef60ec3311b5dae3b52d61
- 6f2af5771522f2ce3843f57c2a72a2451e0b73a71505cd50abad031267915be3
- a753a288318dd38709ac1c26374cdc1fdb930b8476788d2868a1cae79cc8f352

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.Agent-1356499

感染指标

注册表项

- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASAPI32**
  - **值：**ConsoleTracingMask
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**AutoDetect
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASMANCS**
  - **值：**FileDirectory
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**UNCAsIntranet
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASAPI32**
  - **值：**FileTracingMask
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**ProxyEnable
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASAPI32**
  - **值：**FileDirectory
- **<HKU>\.DEFAULT\SOFTWARE\CLASSES\LOCAL SETTINGS\MUICACHE\34\52C64B7E**
  - **值：**LanguageList

- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\CONNECTIONS**
  - **值：**SavedLegacySettings
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**IntranetName
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASMANCS**
  - **值：**FileTracingMask
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASMANCS**
  - **值：**EnableFileTracing
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS**
  - **值：**ProxyServer
- **<HKU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections**
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASAPI32**
  - **值：**MaxFileSize
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASAPI32**
  - **值：**EnableConsoleTracing
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASMANCS**
  - **值：**EnableConsoleTracing
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**ProxyBypass
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP**
  - **值：**IntranetName
- **<HKU>\S-1-5-21-2580483871-590521980-3826313501-500_CLASSES\LOCAL SETTINGS\MUICACHE\34\52C64B7E**
  - **值：**LanguageList
- **<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>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASAPI32**
  - **值：**EnableFileTracing
- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\CONNECTIONS**
  - **值：**DefaultConnectionSettings
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASMANCS**
  - **值：**MaxFileSize
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\TRACING\RASMANCS**
  - **值：**ConsoleTracingMask
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CTLs**
- **<HKCU>\Software\Microsoft\SystemCertificates\My**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\SMARTCARDROOT\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CRLs**
- **<HKLM>\System\CurrentControlSet\Services\Tcpip\Parameters**
- **<HKLM>\Software\Wow6432Node\Microsoft\EnterpriseCertificates\Root**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUST\Certificates**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CRLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CRLs**
- **<HKCU>\Software\Microsoft\SystemCertificates\trust**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\CA\CRLs**
- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\SmartCardRoot**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\Certificates**
- **<HKCU>\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CTLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CTLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA\Certificates**
- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\TrustedPeople**
- **<HKLM>\Software\Wow6432Node\Microsoft\EnterpriseCertificates\Disallowed**
- **<HKCU>\Software\Policies\Microsoft\SystemCertificates\CA**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CTLs**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\ROOT\CTLs**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CRLs**

- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CTLs**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST\Certificates**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CRLs**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CTLs**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CTLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\TRUST\CRLs**
- **<HKCU>\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CTLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CTLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\Certificates**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\Certificates**
- **<HKLM>\Software\Wow6432Node\Policies\Microsoft\SystemCertificates\trust**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\DISALLOWED\CTLs**
- **<HKLM>\Software\Wow6432Node\Microsoft\Tracing\RASAPI32**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\Certificates**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\SMARTCARDROOT\CTLs**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CRLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST\Certificates**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUST\Certificates**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CRLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA\CTLs**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA\CTLs**
- **<HKCU>\Software\Microsoft\SystemCertificates\Root**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CRLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CRLs**

- **<HKLM>\System\CurrentControlSet\Control\SecurityProviders\Schannel**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\TRUSTEDPEOPLE\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\SMARTCARDROOT\Certificates**
- **<HKCU>\Software\Microsoft\SystemCertificates\CA**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CTLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\SMARTCARDROOT\CTLs**
- **<HKCU>\Software\Microsoft\SystemCertificates\SmartCardRoot**
- **<HKLM>\Software\Wow6432Node\Policies\Microsoft\SystemCertificates\TrustedPeople**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA\CRLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CRLs**
- **<HKLM>\System\CurrentControlSet\Services\EventLog\System\Schannel**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\Certificates**
- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\Root**
- **<HKCU>\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\CA\CTLs**
- **<HKLM>\Software\Wow6432Node\Microsoft\Tracing**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\Certificates**
- **<HKLM>\Software\Wow6432Node\Microsoft\EnterpriseCertificates\TrustedPeople**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\ROOT\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\TRUST\Certificates**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\Certificates**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CTLs**
- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\AuthRoot**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CRLs**

- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CRLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CTLs**
- **<HKCU>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness**
- **<HKCU>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CTLs**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\DISALLOWED\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\CA\Certificates**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\ROOT\CRLs**
- **<HKLM>\Software\Wow6432Node\Microsoft\EnterpriseCertificates\CA**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CTLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\TRUST\CRLs**
- **<HKCU>\Software\Policies\Microsoft\SystemCertificates\TrustedPeople**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\DISALLOWED\CRLs**
- **<HKLM>\Software\Wow6432Node\Microsoft\Tracing\RASMANCS**
- **<HKLM>\Software\Wow6432Node\Policies\Microsoft\SystemCertificates\CA**
- **<HKCU>\Software\Policies\Microsoft\SystemCertificates\trust**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CTLs**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\TRUST\CTLs**
- **<HKLM>\Software\Wow6432Node\Policies\Microsoft\SystemCertificates\Disallowed**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\SMARTCARDROOT\Certificates**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\Certificates**
- **<HKCU>\Software\Policies\Microsoft\SystemCertificates\Disallowed**
- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\Disallowed**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\TRUSTEDPEOPLE\Certificates**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE\CTLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CTLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\ROOT\Certificates**
- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\trust**

- **<HKLM>\Software\Wow6432Node\Microsoft\SystemCertificates\CA**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\SMARTCARDROOT\CRLs**
- **<HKCU>\Software\Microsoft\SystemCertificates\TrustedPeople**
- **<HKLM>\Software\Wow6432Node\Policies\Microsoft\SystemCertificates\Root**
- **<HKLM>\Software\Wow6432Node\Microsoft\EnterpriseCertificates\trust**
- **<HKCU>\Software\Microsoft\SystemCertificates\Disallowed**
- **<HKLM>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CTLs**
- **<HKCU>\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED\CRLs**
- **<HKLM>\SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA\CRLs**
- **<HKLM>\SOFTWARE\MICROSOFT\ENTERPRISECERTIFICATES\TRUSTEDPEOPLE\CTLs**

互斥体

- Local\c:!users!administrator!appdata!local!microsoft!windows!history!history.ie5!
- Local\WininetConnectionMutex
- Local_!MSFTHISTORY!_
- Local\ZonesLockedCacheCounterMutex
- RasPbFile
- Local\c:!users!administrator!appdata!local!microsoft!windows!temporary internet files!content.ie5!
- Local\ZonesCacheCounterMutex
- Local\WininetStartupMutex
- Local\WininetProxyRegistryMutex
- Local\c:!users!administrator!appdata!roaming!microsoft!windows!cookies!

IP 地址

- 216[.]58[.]217[.]68
- 216[.]58[.]217[.]78
- 216[.]58[.]218[.]132
- 216[.]58[.]218[.]142
- 74[.]125[.]34[.]46

域名

- www[.]virustotal[.]com
- google[.]com
- a6281279[.]yolox[.]net
- ghs-svc-https-c46[.]ghs-ssl[.]googlehosted[.]com
- www[.]google[.]com

创建的文件和/或目录

- \DAV RPC SERVICE

文件散列值

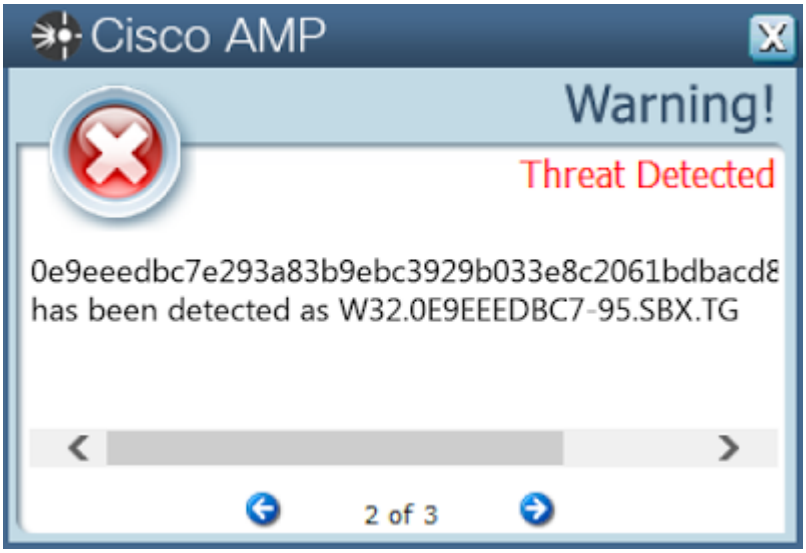
- 0e9eeedbc7e293a83b9ebc3929b033e8c2061bdbacd8f17cd29b12505d2e777b
- 55acc591f5c6c0d2313ddd4ba47c25fe3b81bbcb64b4ad77c4668dfcc559748c
- e26c807c8e5d5ba8b41de497a24da81b8db0325a0a2c64bb04ee7beaae12904b
- 5554e16e209aec408f7f7ba49caff85e568de76a05ebe41cf74002a7ca35d973
- 8b20f9e78855218c693ade8a89b9c74487304df9bfdbcdbe8c65b05bfaa5b71b
- b001932b6938223033229e9d5bfbb5754680ab786c927396bb540e1a6db1ba7a
- 768ef3bae40d69715d2cfe3948fe3e9b0adb047525e8fa6d067269e859d0832b

防护

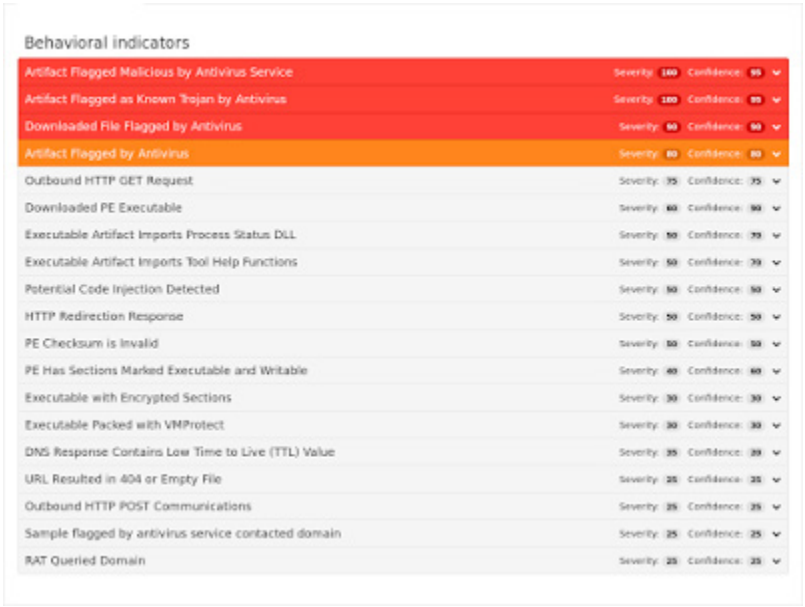
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

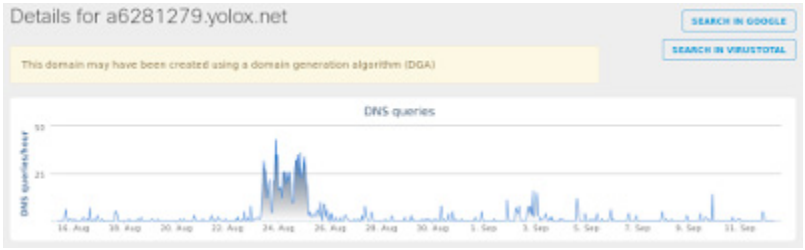
AMP



ThreatGrid



Umbrella



Win.Trojan.Symmi-6336247-1

感染指标

注册表项

- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{084FBB2E-F87B-4A87-B07B-817B5979A462}**
  - **值：**Triggers
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS**
  - **值：**LoadAppInit_DLLs
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\HANDSHAKE\{340E7911-BE16-495F-BCFC-77C4B88E2E62}**
  - **值：**data
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\COMPATIBILITYADAPTER\SIGNATURES**
  - **值：**aybbmte.job
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\COMPATIBILITYADAPTER\SIGNATURES**
  - **值：**aybbmte.job.fp
- **<HKLM>\SYSTEM\CONTROLSET001\SERVICES\MPSSVC\PARAMETERS\PORT KEYWORDS\DHCP**
  - **值：**Collection

- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{084FBB2E-F87B-4A87-B07B-817B5979A462}**
  - **值：**DynamicInfo
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{084FBB2E-F87B-4A87-B07B-817B5979A462}**
  - **值：**Path
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\AYBBMTE**
  - **值：**Index
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TREE\AYBBMTE**
  - **值：**Id
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{084FBB2E-F87B-4A87-B07B-817B5979A462}**
  - **值：**Hash
- **<HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS**
  - **值：**AppInit_DLLs
- **<HKLM>\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\HANDSHAKE\{340E7911-BE16-495F-BCFC-77C4B88E2E62}**

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%\Tasks\aybbmte
- %AllUsersProfile%\Mozilla\thfirxd.exe
- %System32%\config\TxR\{016888cc-6c6f-11de-8d1d-001e0bcde3ec}.TxR.blf
- %AllUsersProfile%\Mozilla\lygbwac.dll

文件散列值

- 10e8f34991079b2c40f2e72babdbd3d0fd97703870552061752b341b704153b3
- 17ae6bd9e77a9a783caf5bc398f03ff47691134f9a6c5600a903159057c78b17
- 2a6794ad2014b95abca5512d85f748aaaf08a1d1f9a7be3583987bd1523f5f1b
- 2c0f383fcc3b07a893fa0ce0cfbe025d31c6ebfe46979b129bd8090712256c42

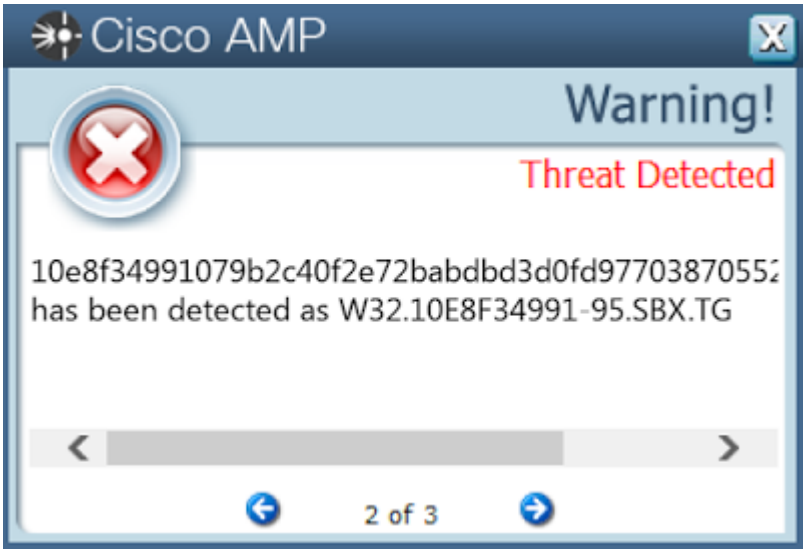
- 4395a481c0e8afbc60cd6bf4eef233bb2067485581a47e56ff310cb7466ee681
- 4763992ecb0dc5bbda30d2d00dd99927fb8aa2be759c9058f2dafb691ccf0f0b
- 54ac75db11197dc919f3574eefb88fe8b653de92ee5a6ed99cf00eb1b373d622
- 5542e1e52c63ceea56446d3c2f1f9c12adc60033d92289bb5d3450a40e02acd5
- 5917eb033004f3a29a3ac843f9c90844cab3cf0520e78e8739cc8cbfff83ef02
- 6c51d2e568f033b8a8c6764d54583da5af6fcec7a21d283e536063861c156ff4
- 7156221c0787b78866de2621828fa2ea48ebdba2b06219576337db8bf342c6cf
- 848993b12b05369d0873975aded55f837dc0a583c3839c05abe96bc4c3b68408
- 89c9a8a7f47bb27a175632ad48317b93fe8a2b59502c73371df48982168a70db
- 90e0adc73ca753d91fe32b1d3761c3f6f6e7216f3b77a87fdbe2a8e7f5e889fc
- 983f1a853f5f7f1c7aa2e687761ae736d2a4397884dfd455685bbc5ae1d0b2ef
- a6099ef0093736c0757c589890df229b39e4efbb38ebc63d460ea06186e09f69
- a94ef67587dde19950297b9b69e90254f16cd5e6653fc596524044377a2e1193
- c7fc560bff6d3fbc3a72355463836eaf9b3d7d18ade95ce72436926568626edc
- d6d82c71a400735446318832a57f7a2573cfa4073aa31ec6a8b742d43f93e9dd
- d778483fb3f3afdc4efd06ae0f605a53d7ee4e512459aa3b287cc246cc6097b5
- d8a3df456b94acea22b8ebeb4f7f860687dd6ab4ac2b687631b63342f7cbf927
- e5a8eba740a5acc1a6b5e11bb64be0be88a8556e48d78c292732048fa2c56003
- e76a23d8d8e16a6e1cd78e28ad875f5ca61221f3d0c44dddf750e5920dc5acc2
- e7eb60dd2d0830ae2d42a913afc5db98392a3d5846ef85ac32ec6fdd08b67fae
- fc30aafd75f5bcf3d4a73a6336ba1f2fb150a410712e32f5887d2afe8504f717

防护

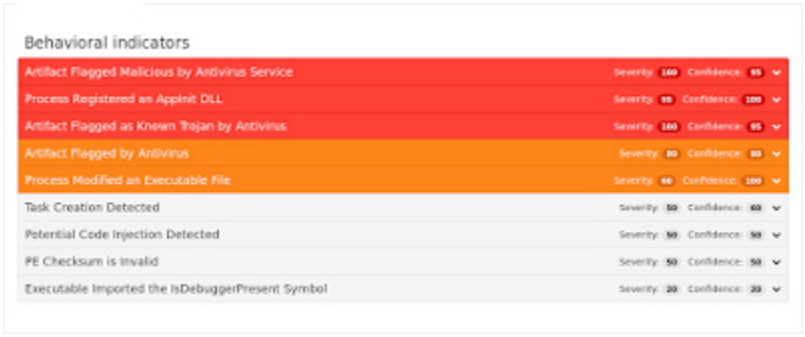
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	不适用
Threat Grid	✔
Umbrella	不适用
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



发布者：ALEXANDER CHIU；发布时间：16:10

标签：AMP、CLAMAV、防护、恶意软件、SNORT、一周威胁综述、UMBRELLA

分享此文