2017 年 8 月 18 日，星期五

一周威胁综述（8 月 11 日至 8 月 18 日）

本文概括介绍 Talos 在 8 月 11 日至 8 月 18 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.Agent-6335676-0**
  Office 宏下载程序
  这是一种具有混淆性的 Office 宏下载程序，它会尝试下载恶意负载可执行文件。其执行过程通常为 Word -> Shell 功能 -> CMD -> PowerShell 下载和执行。

- **Doc.Dropper.Agent-6335671-0**
  Office 宏下载程序
  这是一种具有混淆性的 Office 宏下载程序，它会尝试下载恶意负载可执行文件。

- **Doc.Macro.JunkCode-6335442-0**
  Office 宏
  此恶意 Office 宏经过混淆，增加了分析难度。这些宏有时会生成似乎像是指令的空操作。这些空操作（无用）指令会生成可被检测到的构件。

- **Win.Trojan.Expiro-6335658-0**
  木马
  此样本是一种木马。它利用自动调试技术扰乱自动分析和手动调试。此样本需要正确安装沙盒才能运行。

- **Win.Trojan.Ovidiy-6333880-0**
  木马
  Ovidiy（全称为 Ovidiy Stealer）是一种目前仍在活跃开发的 Windows 木马，用于窃取凭证。虽然它在性质上属于模块化程序，但是它的主要目标是网络浏览器会话中的凭证。它有一些命令与控制 (C2) 功能，而且会向外传输特定的主机信息。该木马本身是以 .NET 语言编写的，目前发现的多个样本基本都使用各种针对 .NET 二进制文件的打包程序打包，以增加检测难度。

- **Win.Trojan.Tinba-6333828-1**
  木马
  Tinba 是一种轻量级银行木马，主要通过注入到网络浏览器的 javascript 代码窃取受害者的敏感信息。Tinba 的源代码已在 2014 年泄露到网上，恶意软件开发者可以十分轻松地利用和修改其功能。

威胁

Doc.Downloader.Agent-6335676-0

感染指标

注册表项

- 不适用

互斥体

- 不适用

IP 地址

- 78[.]47[.]139[.]102
- 193[.]227[.]248[.]241
- 104[.]160[.]185[.]215

域名

- campusassas[.]com
- campuslinne[.]com

创建的文件和/或目录

- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\qdvjnh.bat
- %SystemDrive%\Documents and Settings\Administrator\Local Settings\Temp\plzea.exe

文件散列值

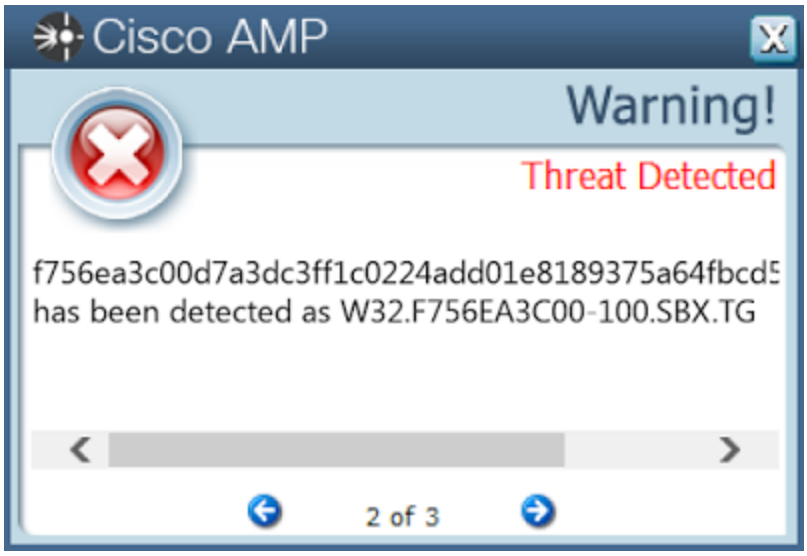
- 7ffabe10f4147ce48fc9ae40cdc7778d08ac7881b779743720e2c4313592445b
- c2a3dcd915905c09026044e8da533455a2742196e4294cfffc000c048c1ea9cc
- f756ea3c00d7a3dc3ff1c0224add01e8189375a64fbcd5c97f551d64c80cbdba

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

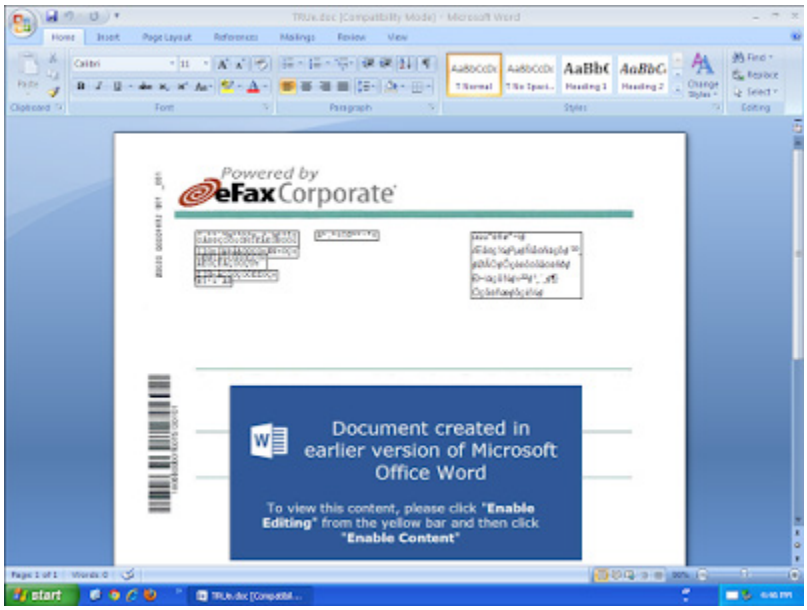
AMP



ThreatGrid

Umbrella

屏幕截图



Doc.Dropper.Agent-6335671-0

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

- iesimpianti[.]it
- janssen-st[.]de

创建的文件和/或目录

- %TEMP%\7E94\3F4A.bat
- %AppData%\Microsoft\Office\Recent\270700481.doc.LNK
- %AppData%\Microsoft\Office\Recent\fatt.348.LNK
- \Users\Administrator\Documents\20170810\PowerShell_transcript.PC.PbSYjzuP.20170810091133.txt
- %SystemDrive%\~$0700481.doc
- %AppData%\Microsoft\CHxRthlp\api-pntw.exe
- \TEMP\~$tt.348.doc
- %TEMP%\33513.exe
- %TEMP%\7E94\3F4A.tmp
- \TEMP\fatt.348.doc

文件散列值

- 5edbc08d4e919f7186aa2b8a6e3d49ef38035c2a55b6e226910fcc60fe26a335
- bbe5988f2470a296186ca43a76636fceb523b45273a32e83aa14a8cc1f4e3a8e
- acdae0dde63863e8be98935254c901439b5fc36fb45f974fd7ce7c298e3ca0ca
- b05c34ffdc8c82862b408a1f628b21bb08362de4340d768a08c511132ce7d34d
- cad134945e7f20e99efed18650d4a7c573f8902b32c10ae89639518f94e646d0
- 0752a00c66125520f78673e70af10123cb5b78fe4786d368f7beb586d5ce3531
- ffc6c04d292e6618826bb09c8c63a06af3993e7b6b14171c45c7b44619b4421a
- 758a4e1ea1fc0c9846d21f643013fd934fd23b187ca1fd32c90334ff48a60372
- 4111dc9ca29508aa89caf873ac9359ad579270c3b3025ab0ba8098dea9c3c459
- 0524147db311dedc4631e0749bb79865ac673763bd5ebc576855fcb9431de98b
- 0e5240bf70e304781511de29a000c308f675d6209735c118cd0054b519eaa096
- 09f89667dbbd0f72478f317aed5196f743693190aa3afe1f1cfccc67dad88fb6
- 4cf480e7bab22fdd7d64c43d8f18c3c5358c25fbd063bc2d2855885b886718ac
- 6ea7a564a6a7ba8f4c97e2eaefbedafab6dd1424d56716f1255b03f8b5879161
- 3728cecd2be075b09a3a6d8d8c5923fe14cf381e3070266cf05fa51585def305
- bec41e3e8d3093b58170d743ca905af81ed745a4828a42a9d39cd3373252a84d
- bd7ed9514afabc723da282f32ad1dcfe81796a83555b7b4a6738dd0254c06ccd
- 4b495c54056aa68e91fd481168a7ddc5d5a6cae713ab359777340f1ba901ae65
- b588aa1d5901e2ded7dfc9fe8efbd13304f2bed37086b5c9aa498fdffaed48ba
- 717f927b9c0b01a60eb94254d39ac5eeee24a2c10d0c59266252630202a36323
- 056bce922fab367aabfd43f5e85bb5397755db08afcc8c38d992ffb4fe8f766f
- 3ca148e6d17868544170351c7e0dbef38e58de9435a2f33fe174c83ea9a5a7f5
- 6250f069e1268801cb3afaee2523df1aca628fa791a666f1d05b6cb981913461
- 1496ddfb94f11120267fe9d6bf233ba4726754bebf3075340496a144777a6539
- 5f1827ab138eb25289a1a76910f5dc9c96aed87dd8aa2db7e3b0d310267a5a67
- d08c719c8ea6e5d7546e6449e6aed748ce74359e7c0dbd1f9bd08e2e8b795c68
- 168c49c8207019008bdf746d0fa4ab33a154277c5fe50fd4900e9d77ec6a2e7d
- e92710c582f71c4a9cb127774fa4cce0d8abb837a38d50d22d17ef7061646c92
- f20256df607a29ef83bd035ee27fc424307712e59298f54803150a88ea5c5ece
- 190cda0ade0c0348786652b7ee12fde595e12ab561d893224cfdafbd58ec7b75
- cccb32f7f0408b32f3ad7f5a75adf1b955ba83a712e59c64f16b07713a6b44b8
- 31b34ac21405f6450bef3c18249e83a7bc464dea5cd4fb239becfe0a800875a2
- db8ee4755c2b30756abb68e14e30b7c10d283b2f989fc7f3556f92389a2c32b9
- d26ebbc2bdf6a6b59d805f7f1e9a9b505b6ff6e8b99e254f9c5c36413142d3f8
- f2fbac0942b08720073373536520b471229c918474cabb63fd19c3d006caaa1b
- 366f1f331e940a462447e2b4abe9196ae7b977d281c2b9fe5e19bb0c2927b705
- 9859e621b4d259798b2813377f9cd1736497f51cb501c6b3ea44ccae57d4e4fa
- 94395a2b7bd0a120b55e39b3107f934f9b76faa9e2679dbae1237f69f2c3f1b9

- 5df3016ba1cfd870d1d72e75ab9ec1d0a08a7e11d9fe7ec6b32fa0ce468206e7
- 5624e26cace481fa4144f5ccd5bdcc7b5c3d42c035c88250312833041cf55807
- b0610f20ce7be29f5864a02d72bcfa54e215d3159bf381d05fac58d2fa703f0d
- 1c364ed502fa3710d9fa3c5a4a2ac6688bea3610acee2a6f958220d8ffca908b
- 36472a674c751c65c15cbaab276c0fba8f3f1709750473b24e5d3c21e468617f
- 0419cd8e5884e2918c5f0746d54efe2e2d9f0385523ecdbc395200df4004d87a
- 29a7f99f81dd37bcbd196d635837c01d2aa48045ce4efd999a6d0da92bfbe917
- 6451b45a4f8bdccdbce6bcd14e5fda1f976c81efed2c4dfd028386cce31250d1
- 7a703a5e7f30a1621e204669ffefe91f22a1619814c4ef40872cd750cffb9125
- 5de158f2b9e0039b76588fd190565bcf4e02398ec8bff57d1c55bcc1626de5f3
- f8913513ec19ea386cb812e5e7249d44a4e4a3092fbfcea23fce692d7ed88970
- 6dc6070451995a7dae4d5b741e291ce525aec2cf3144d9fdb8484f39079ef9e2
- 4808a9fc9a33cf5df06d5a56f85b6e2dfdb8fc5fbb4cbd2ede05488dd566f6f5
- eb99cecc433a5134414024c98c227f52bae7660343a36469ccf0e6a8f5af4a6d
- b3dc9a164f1548ca0fd4618dbaae44c6a9ea05f66aafcf67758d9985b1409cb0
- e14472604877ad85c119703225fb6086053bcaa2ebae60d38762bbdd192e2244
- e631b1dd070f71e53dd7b5c36a1921c027257f0c79bc7964551f27d0f4ece78b
- e342cae3c710674f0e73ea2ed1e72085d790a653e249e1b5e4d8e6696e110041
- 9f404502e944f4cd76b902abf67717054732528a9399e23b3d90e2825316818d
- f6c2aea9dbc12ff2dbf77637560093234465cdae03c40ee4f0afcf8365ebfab7
- b3fffd7e92a3bb920456b149717c353c8779e45a947c0e756889956c6bc48d7a
- 45112ef00b7d34a471655f3a7318fd2b69de1ade1889647839ff897c6e6f1c67
- 9d52dd2437d0408e5971598b44c5dc1e1475004241bb5928d1eaee9a9aea51e1
- 947ec2662ab377aca91f9ccb5b2a0e823ab5b814be719494c5cb8f0e7e228252
- d076c672bdb9bd3b738edb882560482bebde469d02acd1ccda11e9c9cb6feaeb
- dcfddf26b9699622bde12c6b64a78e5446172e57c5a29c3ea0267a0df85bc1e3
- 0db7513e4ec8cea44afdce2d37991f5f9cbde0bb779856c10d9ffa75bed53d0f
- b1e4e3be5dd686424763f39f8930e28044a9cda7a48d8962ba6e8978ef532fa0
- 31755c56408a13f44d620971a60342bb0170ad78217c923c518fe4b58b4da365
- 27772ef48d027d7e23e1f78d8ea86cb1bbcf4240cd59a8dc7ebc82f8a3a8b6dd
- a31cbc1ce4abaa2ba7cab9ff97e1f647c3b1264c9cb7db0e20c74d151db2634d
- c685f1c782e6b9250035f922ebc80400f2d6515e5f343a933c6c12920eb89e92
- 5dd873a5cd07c4ac6edc7bfad7c92e1111cbddab5e72de96291e2990e0ab62e0
- 8c43427b886d65c06a43f823511f0927b85dc5956dc7bd1bd16c59af548db6b8
- 2aaf7791ed0a57e48c3d363b46ba5247e78a2290549bfd7f98793e9bee4c3e55
- 9b6d3e01584f4d1238a55050c7ffad0e14299e911db8497b81529bd58afa4bc7
- d526ffe1710b4b39866bebceb3660e1386e41df17b13a6055078b0ce7db74fbe
- 425e004b3c9034aa17071b137ca1d4ae7a35dde5f588c05295e491b716125e2a
- 8c4813043fa78b4aec7ada10556ddbe06eedbc81b115e4ff08371d8ee132d645
- c7cab605153ac4718af23d87c506e46b8f62ee2bc7e7a3e6140210c0aeb83d48

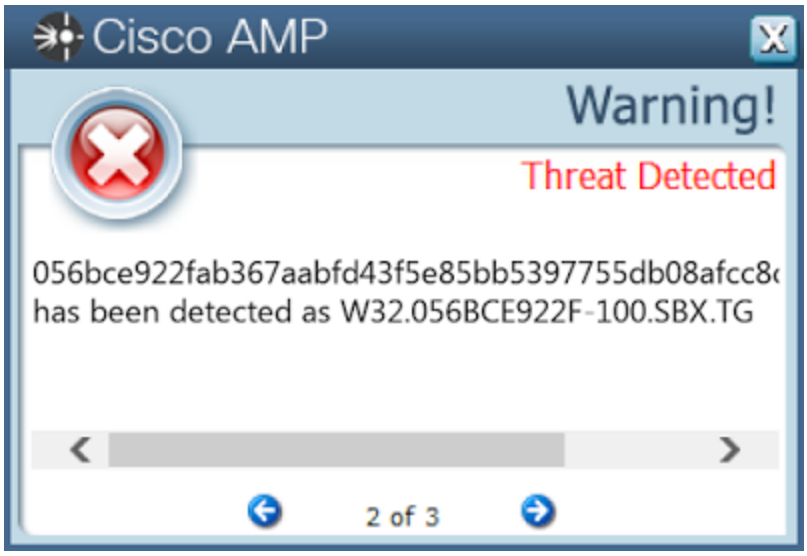
- d52318c1f83d086fcb94b8ae7288f2acb85f6e441c66a3f1d09365a1018c80bd
- 44b6060a5406112556049bd3efef8d876fe335bb4aa0f0a6f7d0210184918c71
- 4e812653205426b75038ce2796be5b254b61ee02da376462f3ad1ac23d898282
- 454ed2ca7a116ad34864d4e8b232dcb50c063ffbd70f23753262aabb6b34d24e
- bf958c7ba44b9dfdcba50eeb6f7b59fe3bd2948f1ab1a7c8ee0f162b7cac3b2c
- de0e7aae207f7a7a1f242d849bb61c7f4e98d84f74b228439d296e6a46b2f812
- 712a907f98efa76de2b349c90084fbef6d40d9df32a41df98fc62e19fab5329d
- 3d081fe6a220b546af09139fda7deceb5e7f16b52fb47d15ff4e69bab9175734
- f0b670afe4781d3e8899bf742fbd613636424681f56c4388168acea84ea344af
- 976c6ce6c484aef7d0d801c2f5ee31c984136d91636656a7e5425fbc4e848029
- 37e79b45ee53bc266d3602ec2cb79762a3c6360b5c173e89da045491150dbfb1
- a4692d62273960b017d80e2b3ee9befe9b186d0609dbf4aedd1dcaf6d3aef671
- c3e6a58e8a68518ffb43ee9026508b6520016e8d7096bf94ec2d1ed5cd328d76
- e8290589cab3707f80ada754a31263e239b870dac5bdece15bf2e331cae5acf1

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	✔

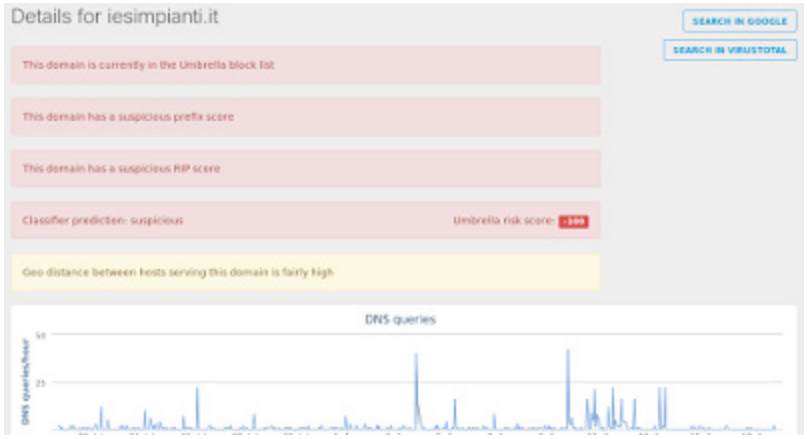
检测结果屏幕截图

AMP

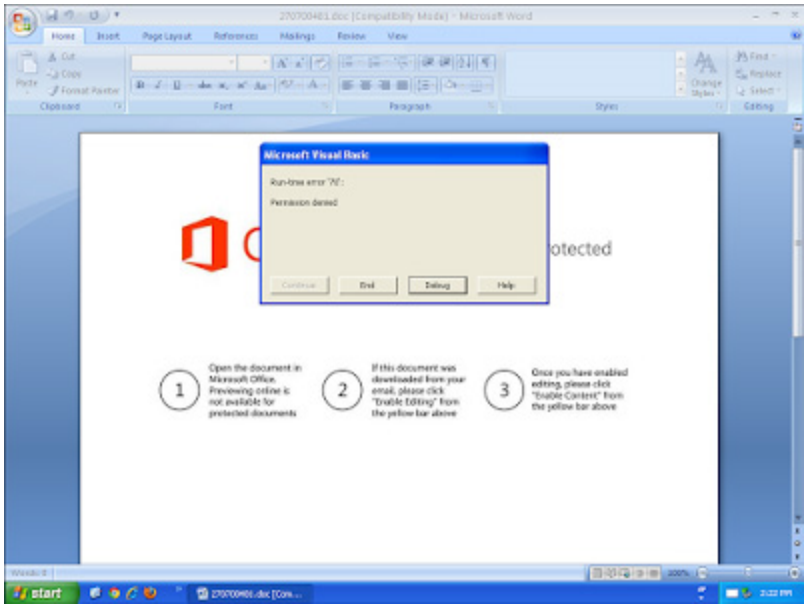


ThreatGrid

Umbrella



屏幕截图



Doc.Macro.JunkCode-6335442-0

感染指标

注册表项

- **<HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **值：**internat.exe

互斥体

- Local_!MSFTHISTORY!_

IP 地址

- 52[.]173[.]193[.]166
- 185[.]206[.]144[.]152
- 190[.]107[.]177[.]115

域名

- plantatulapiz[.]cl
- kalawatu[.]site

创建的文件和/或目录

- %TEMP%\CVRDF32.tmp.cvr

文件散列值

- a5eb0f2e7d972b47c5016dd755bfce2e794822ef6933ff9759fd70e72b137a16
- 404987cbcc932ba68aa9abd4607ea81ba4feb167c3f333c800a56cb2620ffd9f
- 046809ff996329f2bb539128d51a0c21179ac6d117688281dd927df4b0aaf85b
- 9679b02ca07d40f2d2d84445b5683fe2c1a135ecf73886d2ed27dc387b108417
- 3a79a33855731c0066016de8baf9ef6b946b06b1ce4fda28f3c68265afa6c89a
- 3b0997b98551548002dd9cd977cd3f881f0496ab2f86ef1a90d6c7a13765366c

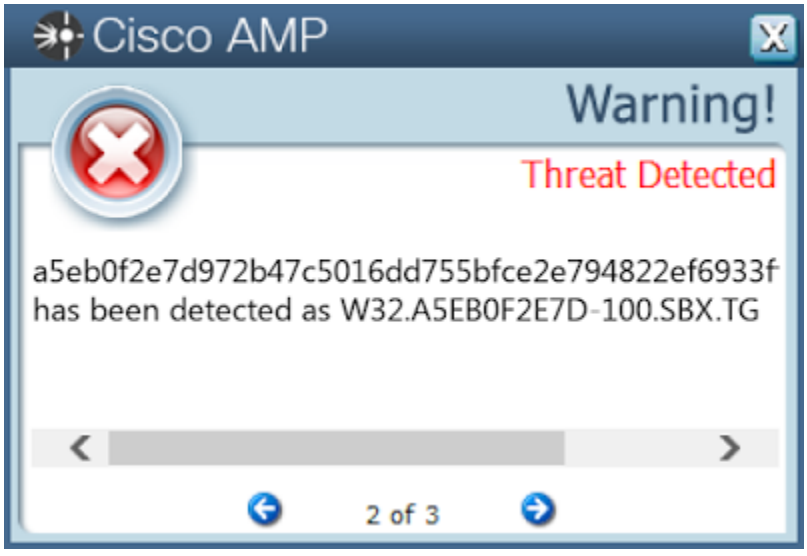
- 148b0ed81c95496d80778c7d3d093627a7395b76bf9b457f958201be66e8ea1f
- 9ba948417071478c1fa3fe89c46c19c56190f47f2ba141a446166eff5a71fbb4
- 1a1a48c35aee34ba91d83ae97865d75319112165ee8e7dad7cb7714ab57c40b7
- 5b1e2ebb1baa600fba198e5c233ebb431311c976ef23f5c2f2c74ff03392a824

防护

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

检测结果屏幕截图

AMP



ThreatGrid

Umbrella

Win.Trojan.Expiro-6335658-0

感染指标

注册表项

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

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

- \TEMP\60d2422af917cb8aa58c14b8b78d4af112c9c78343da8f7aa3fbcb87be1a4de0.exe

文件散列值

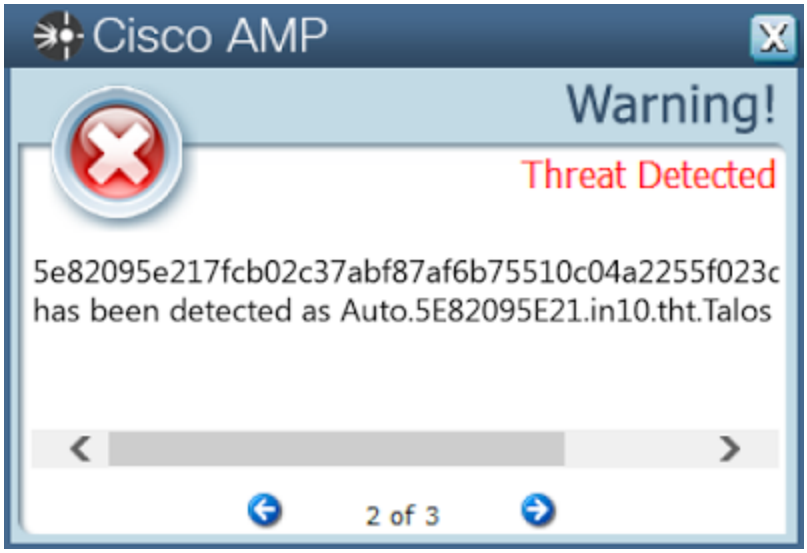
- 60d2422af917cb8aa58c14b8b78d4af112c9c78343da8f7aa3fbcb87be1a4de0
- 5fd134b6abe1473fd5a7f96c711a4270fbc364bc6e3b10b5b344e0a1bfb0e4d8
- 5f5e9e5952765887211883b42e508b4b14c62a1685092978f98c6619229796b5
- 5fe205ea4f5f975703e242e8079dc471a5363538535d76584e7138ed3fb67546
- 5ffa0097ebcba0e1921c6607a644e2649532ae07b1c7d6533a3cbef52ee51620

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.Ovidiy-6333880-0

感染指标

注册表项

- **<HKLM>\SOFTWARE\MICROSOFT\TRACING\6838BCE2F6C831414DF831040FC14287_RASAPI32**
  - **值：**EnableFileTracing
- **<HKLM>\SOFTWARE\MICROSOFT\TRACING\6838BCE2F6C831414DF831040FC14287_RASMANCS**
  - **值：**ConsoleTracingMask
- **<HKLM>\SOFTWARE\MICROSOFT\TRACING\6838BCE2F6C831414DF831040FC14287_RASAPI32**
  - **值：**EnableConsoleTracing
- **<HKLM>\SOFTWARE\MICROSOFT\TRACING\6838BCE2F6C831414DF831040FC14287_RASAPI32**
  - **值：**FileTracingMask
- **<HKLM>\Software\Microsoft\WBEM\CIMOM**
- **<HKCU>\Software\Microsoft\SystemCertificates\My**
- **<HKLM>\System\CurrentControlSet\Services\EventLog\System\Schannel**
- **<HKLM>\Software\Microsoft\SystemCertificates\CA**
- **<HKLM>\Software\Microsoft\SystemCertificates\Disallowed**
- **<HKLM>\Software\Microsoft\SystemCertificates\TrustedPeople**
- **<HKLM>\Software\Microsoft\SystemCertificates\trust**
- **<HKLM>\Software\Microsoft\Tracing\6838bce2f6c831414df831040fc14287_RASMANCS**

互斥体

- 不适用

IP 地址

- 104[.]27[.]132[.]79
- 104[.]27[.]133[.]79

域名

- ovidiystealer[.]ru

创建的文件和/或目录

- 不适用

文件散列值

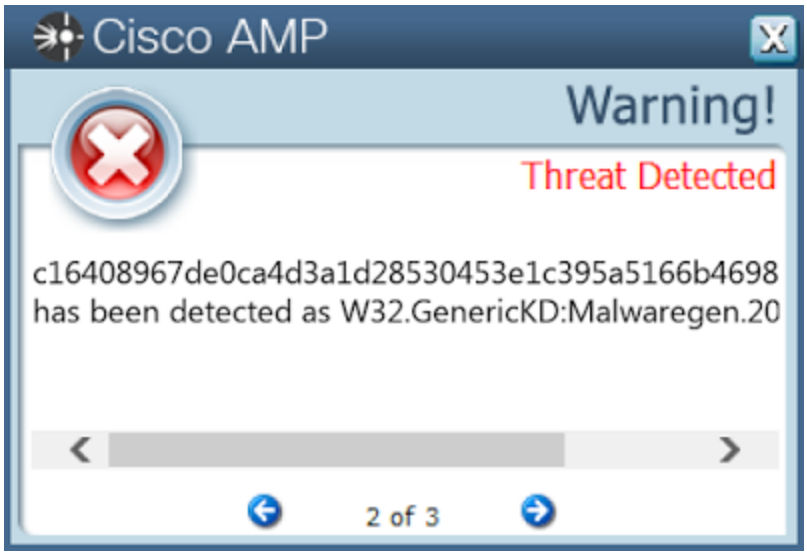
- c16408967de0ca4d3a1d28530453e1c395a5166b469893f14c47fc6683033cb3
- 062bd1d88e7b5c08444de559961f68694a445bc69807f57aa4ac581c377bc432
- 22fc445798cd3481018c66b308af8545821b2f8f7f5a86133f562b362fc17a05
- 80d450ca5b01a086806855356611405b2c87b3822c0c1c38a118bca57d87c410
- 8f6939ac776dac54c2433b33386169b4d45cfea9b8eb59fef3b922d994313b71

防护

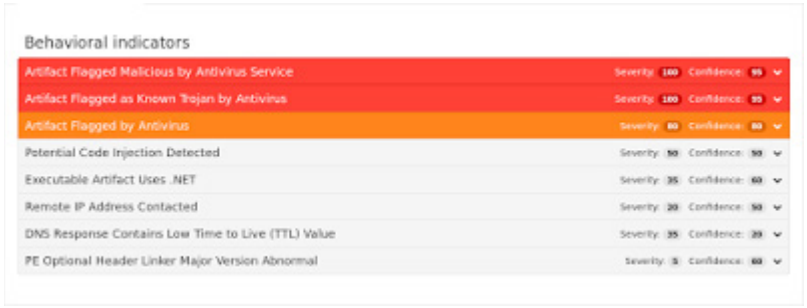
产品	保护
AMP	✔
CWS	✔
邮件安全	不适用
网络安全	不适用
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Umbrella

Win.Trojan.Tinba-6333828-1

感染指标

注册表项

- **HKU\Software\Microsoft\Windows\CurrentVersion\Run**

互斥体

- \BaseNamedObjects\5E60878D

IP 地址

- 不适用

域名

- recdataoneveter[.]cc

创建的文件和/或目录

- %AppData%\5E60878D\bin.exe

文件散列值

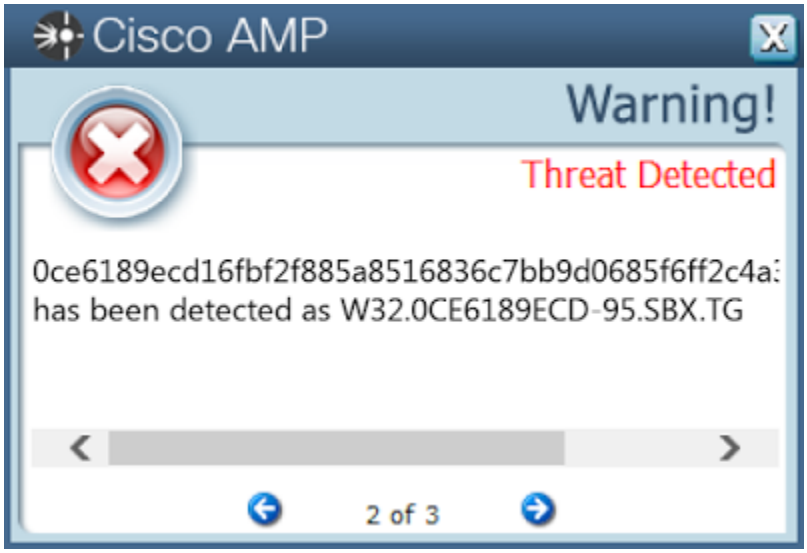
- 0ce6189ecd16fbf2f885a8516836c7bb9d0685f6ff2c4a3df80e236ef5d0d803
- 33fd66f4cee5bdd9f30eb2e5bd7a65367e10f55495c1122430685a8ff0d90fcc
- 51769c916a89522975cb1babb4c9c7b18f3530286c66f3d735751cbdac02a160
- 56f91537753491cd32a250428b146d7685362c762c7e8f39703b4cf6cd92c020
- 6fd80f8da071c3dc482314cbc994b22f105bce22acdad9e9bd86bae5abed53d9
- 7607a0e1be2a8f50959ef42b78edd156aa76741fdc8ee2be9d375610c0b130b2
- 7bbd6d3d6bf6e991e023395e3cb31c18b2a106eef036ad175736a17fb1099b39
- 856ed534a7c32ab7799756c33f7ee104718c89add001428a41dc57e8449167c8
- 968ff771eab9d14d1847f489f425e44532522c7b9fe7407b09d7cc594da0eb84
- e2776a037dcad9e2c752ac4f07dfae0412312ba9b1b748a48922ed572f83eb9c

防护

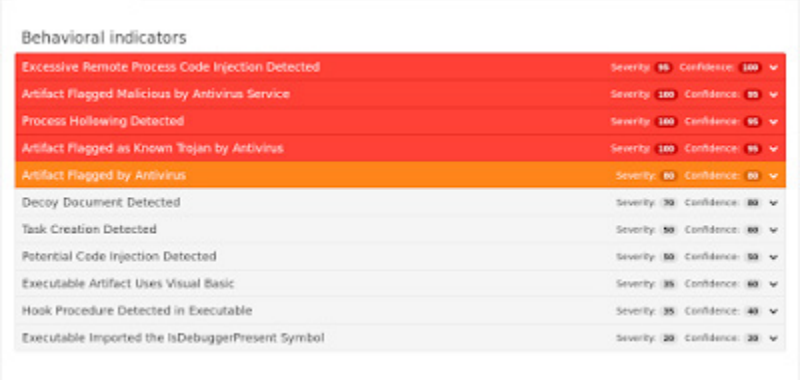
产品	保护
AMP	✔
CWS	✔
邮件安全	✔
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

检测结果屏幕截图

AMP



ThreatGrid



Umbrella

发布者：ALEXANDER CHIU；发布时间：14:15
标签：AMP、CLAMAV、防护、恶意软件、SNORT、一周威胁综述、UMBRELLA