

2017 年 3 月 3 日, 星期五

上周 (2 月 27 日至 3 月 3 日) 恶意软件汇总

本文概括介绍 Talos 在过去一周内观察到的最常见威胁。不同于我们的其他博文, 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、危害表现, 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。

Win.Ransomware.Cerber-5901829-0

勒索软件

Cerber 是一种勒索软件变体, 它会加密用户的个人数据 (例如 Office 文档、照片和音乐)。Cerber 还会尝试窃取浏览器历史记录。如果 Cerber 无法访问 C2 服务器特定域名, 它会通过 TCP 在端口 6892 上对特定 IP 地址范围执行 Ping 操作。

危害表现

创建的注册表项

| 密钥 | 值名称 | 值数据 |
|---|-------------------------------|--|
| HKEY_USERS\Software\Microsoft\Windows\ShellNoRoam\MUICache | C:\WINDOWS\system32\mshta.exe | Microsoft (R) HTML 应用主机 |
| HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager | PendingFileRenameOperation | \\??\C:\001984854a008441d5a880410dd582a0ee6f68bbc0068abeab1f4df1ae0b8af9.exe |

修改后的注册表项

- 不适用

创建的互斥体

- shell.{3EB72F14-EB8C-7844-D6B0-CDB105275440}

创建的文件

Cerber 在它加密文件的所有位置以及以下位置的磁盘上投放一个名为 README.hta 的文件：

- %HOMEDRIVE%\README.hta
- %APPDATA%\Microsoft\Windows\Cookies\Low\README.hta
- %ALLUSERSPROFILE%\Sample Pictures\README.hta
- %ALLUSERSPROFILE%\Cookies\README.hta
- %HOMEPATH%\Contacts\README.hta
- %HOMEPATH%\Desktop\README.hta
- %TEMP%\README.hta

请注意：此列表并不详尽。

IP 地址

- 104.16.149.172
- 194.165.16.0/24
- 194.165.17.0/24
- 194.165.18.0/24
- 194.165.19.0/24

域名

攻击者使用 DGA 算法生成所使用的主机名和域名。目前，攻击者访问的主机如下：

- vyohacxzoue32vvk.[a-z0-9]{6}.(bid | top)
- btc.blockr.io

使用正则表达式可以标识更常见的域：`[a-z0-9]{16}.[a-z0-9]{6}.(top|bid)`

示例：

- hjhqmbxyinislkkt.1mvku2[.]top

文件散列值

- 001984854a008441d5a880410dd582a0ee6f68bbc0068abeab1f4df1ae0b8af9
- f1246caf5b90ffaa5dc03d7c74be88c866627730e79c8da722799b11c576afaa
- bdb7527abf68bd948502dcbd8663382b822910344c21fce1ac9bc0036cb26274
- b48cec5ed5334f1526308bd9e40cde4877265fad488fd6d7935bd6b19edb196a
- 349ed9b9bd21ef37e31b062793b5648f87607b8815a32d425dca5a322d4e5b9e
- cd96f99b90ed85833ac19508d9c445a7352c971819e68073789aaf827fc21c2a
- c441013fcffe2b8bc71c4254882341883eab29db3eab05148c25b747113447ab
- 553d1a73ad634922ad77a317ca3ccd6a0b27a5d67b3429d0f08ea7c7b9967401

- 11a375d808fe0d440bbb6808766fc648a210b5621ae80908673b4f358ebae8ff
- 623c520afc9b32b4777accd9cb9b4422f49a53fc9fe6ff7dc21b7ffd783563ed
- bc753af8a4b203091fb6924e8f88a180e259ac77500eb056b7d04d840ee884e4
- ffde0727f1b487d1a7b84912a2d923e5a7e5443673bee34e89acfd70ef7b1918
- 182dee2062bbbefad0090da61a8b4bdf9d95fa7db621fac9725ad165505b4f1b
- d5ffa9e5b51342eb7c6df5fe7cd60d95ad74955617524148b6e20bc054f0d151
- 938986cb2e87323e482e9d772200157abcacbbe9f962f197276555f750b24c25
- e5ecdb92220696f09ad3500d8e52da3ecfb4f6e00cce6d0a9f224b30e7071394
- b48e859aa8e297cf0bf6bb312c8845f18c4b822e84f6196ffde4d6a08530efd7
- d2c8cc05a9ff073b7cf20026dee5f75a40125babb3c511e22627c9b2e4cf4c44
- 435b6935c28a3aad18a0d065c5ed851b797ae6963ae151b96628fff6d1bd8b59
- 63e1232a12bf86e1bdf9c1527b64eb3e6ae7cd1edb29ce9e2d518912e42d53aa
- 515e6c0cc23d0f8ff7a57737fbc1a7f06cdc86a46985086f91e39afa6d884da7
- c8e32211dc0e0f5477d5424831f1261786adbca862c63f581d88d4448ecdbf1a
- 1180dac56afb5cdb93f910f4f1e9abcb2584462186ec26b7cc7fae8ae4d99db4
- 082496e6e7f49099ac4fe0f6d0652c3a8a2b87f54b05fcf1efef9e006cfa57a7
- 8fd920aa1a4d2b7e7082758c3fe6212fa664258862bfd05ca977a7e01456a2bf
- facb0523eb66f1b2262a81a5fb898c4ab3012c3ade377833906a43d5942ceff0

防护

| 产品 | 保护 |
|-------------|----|
| AMP | ✓ |
| CWS | ✓ |
| 邮件安全 | ✓ |
| 网络安全 | ✓ |
| Threat Grid | ✓ |
| Umbrella | ✓ |
| WSA | ✓ |

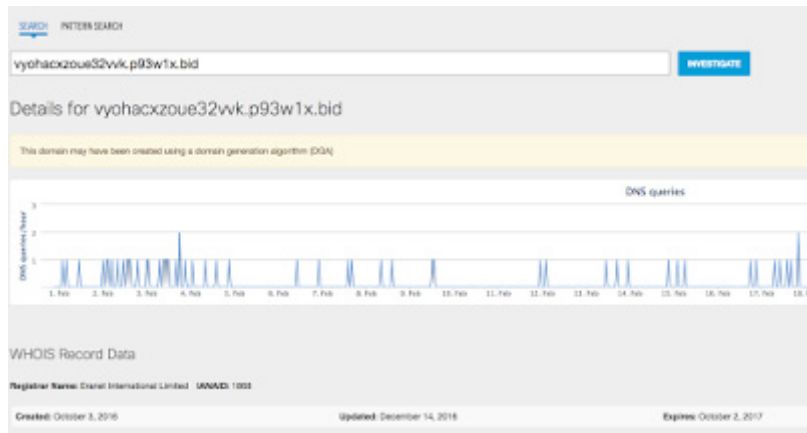
检测引擎

ThreatGrid

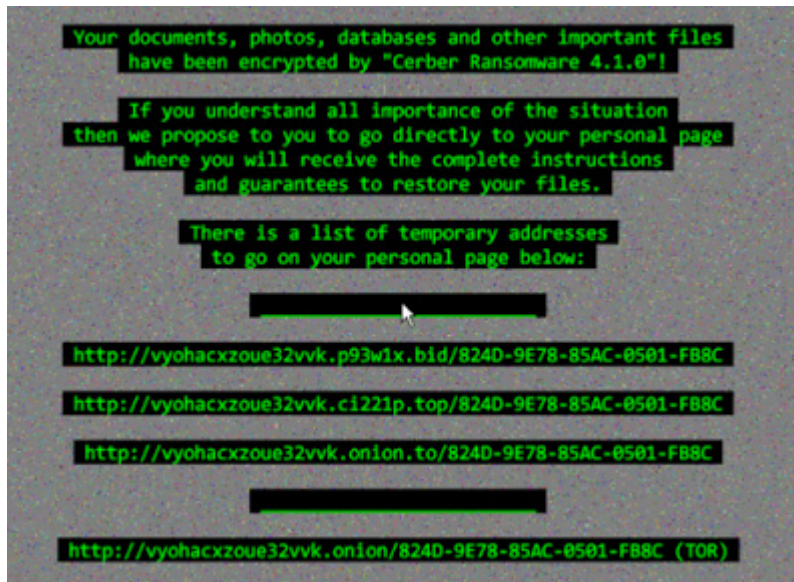
Behavioral indicators

| | |
|--|-------------------------------|
| Ransomware Backup Deletion Detected | Severity: 100 Confidence: 100 |
| Carber Ransomware Detected | Severity: 100 Confidence: 100 |
| WMI Used to Delete Shadow Copy | Severity: 95 Confidence: 100 |
| Artifact Flagged Malicious by Antivirus Service | Severity: 100 Confidence: 95 |
| Process Modified Desktop Wallpaper | Severity: 100 Confidence: 95 |
| Excessive Suspicious Activity Detected | Severity: 95 Confidence: 100 |
| Excessive UDP Connections Detected | Severity: 95 Confidence: 95 |
| Process Deleted the Submitted File | Severity: 95 Confidence: 95 |
| Process Modified a File in the Program Files Directory | Severity: 95 Confidence: 95 |
| Artifact Flagged by Antivirus | Severity: 95 Confidence: 95 |
| Creation Of Randomly Named Files Detected | Severity: 75 Confidence: 95 |
| Outbound HTTP GET Request | Severity: 75 Confidence: 75 |
| Process Modified the Internet Proxy Autoconfig Setting | Severity: 75 Confidence: 95 |
| Process Modified File in a User Directory | Severity: 75 Confidence: 95 |
| Decoy Document Detected | Severity: 75 Confidence: 95 |
| Process Disabled Internet Explorer Proxy | Severity: 75 Confidence: 75 |
| File Downloaded to Disk | Severity: 30 Confidence: 95 |
| DNS Query Returned Non-Existent Domain | Severity: 35 Confidence: 75 |
| Possible Double Flux Nameserver Detected (Beta) | Severity: 35 Confidence: 95 |
| Process Attempts to Forcefully Terminate Another Process | Severity: 35 Confidence: 95 |
| Executable with Encrypted Sections | Severity: 30 Confidence: 95 |
| DNS Response Contains Low Time to Live (TTL) Value | Severity: 35 Confidence: 35 |
| Ransomware Queried Domain | Severity: 35 Confidence: 35 |
| Outbound Communications to Nginx Web Server | Severity: 35 Confidence: 35 |
| Sample flagged by antivirus service contacted domain | Severity: 35 Confidence: 35 |

Umbrella



恶意软件屏幕截图



CERBER RANSOMWARE English

Introduction

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible, from now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

You can proceed with purchasing of the decryption software at your personal page:

<http://vyohacxzoue32vvk.p93w1x.bid/329A-AAEE-00B8-0501-F4E8>

<http://vyohacxzoue32vvk.ci221p.top/329A-AAEE-00B8-0501-F4E8>

<http://vyohacxzoue32vvk.onion.to/329A-AAEE-00B8-0501-F4E8>

If this page cannot be opened [click here](#) to generate a new address to your personal page.

At this page you will receive the complete instructions how to buy the decryption software for restoring all your files.

Also at this page you will be able to restore any one file for free to be sure "Cerber Decryptor" will help you.

Doc.Macro.Generic-5900096-0

宏下载程序

攻击者可以使用启用了宏的 Office 文档来在系统上下载恶意软件或执行恶意操作。此威胁重点利用宏代码中用于从外部来源下载恶意软件的一种常见方法。

危害表现

创建的注册表项

- 不适用

修改后的注册表项

- 不适用

创建的互斥体

- 不适用

创建的文件

- C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\<download_file>.exe

IP 地址

- 89.248.103.159

域名

- www.e-funciona.com

文件散列值

- 3641801c289e5f76ba3a10858567b15a46640ba26ea7d8402eff2016ad4067fc
- 607aaabcf0390969193e26f2e5c6ecec879686028ca39e29c1a4cf10267378
- 433f3d7209ca4be18b5afdef5651c46ec8f5f955a962f3faf7cc472108ff01d4
- 0e3cc78a6cc51199816d459ba6281e330fee7f4b6e0dd6f9d9c818874651cafa
- a8996fcc148fd2fd82c1551d3d874d7b4550fcab4ad4bdbdf7c5a7f0db7ec70a
- 21cb74721704ed761414a3929dec6d4723416594957a3c3b6075855e4f740729
- 1284cf7a0710e38584d430df6cdabda80c321a124b278e010ca0f2f70ba2e53b
- 1352bacc05c1f5414a1f1393c87044f533d2e3c293d42fae1753e3f55f6898ce
- 8f208af31938adbcbcf311317e43e14f8ab181b3038e399e2ba1dff2004c5378e
- f41e5af285ec67f0d08910a91434a5cac4edbcf0bb2713e7773ebe582ccd5d46
- aed55db2b5be215986d182743f07a64d450b26dc4f29007e9ae2192edaf3b924
- 9df62b06bb1c7ff1fcd863d072375c46f6c4132be9dbd89619be1e59993e4d94
- fcc21c98615be7118730e801e15122fad58a8fa75e7d27aff2917694fb465c61
- e89f1ae146aa47bbf5aff559d19b3a91453ef174759a3c4bb2a67c809f6e22c0
- ddaeeae452c0c61842316f574ef77fcd3fcb80df4afc4e22a444ec500663bef9
- dd7a69629cc7c0c975bdc18eee9e7b6c38e846854e6ac01900aa0d1ae332fe62
- d8f52f4f6c8b344dcc421577c77746f7175fb74fa1222578092e10b5c0be07be

- ba20e30a94e8a815bddfc099df321cdad7d72927f944cb20ec200bf0291d3398
- b195291047d3c48738c48bbb604f4c5e85aec9dd03ccae29924acc7cff9a03a6
- 8a6f159fa8d744a384ab0dd5047de64e3bf6e99065afd35e96f42fb832230f9b
- 814b26f19c396af49ba0d39d434ab30c994984426996dc11c6f7418d80648609
- 70a18da4a41d5aa74b943f8c9a0572e8324d66826f64de7ea548e58a89cacia5
- 4e21a3b4ebc76407f70f2b9d9e3a30eec54e4fbeaa64020ac0648873c52b5905
- 4b895aaf6631ae677efc53ba9e416a444bc78df3cd2e3da400aa2968a9ae8db2
- 4b759728a284da96aefe30ea5f4b668d96dccc8c2f9630bf6786eb26b5650a06

解决方案

| 产品 | 保护 |
|-------------|----|
| AMP | ✓ |
| CWS | ✓ |
| 邮件安全 | ✓ |
| 网络安全 | ✓ |
| Threat Grid | ✓ |
| Umbrella | ✓ |
| WSA | ✓ |

检测引擎

ThreatGrid

Behavioral Indicators

| | |
|--|------------------------------|
| A Document Requested an Executable via URL | Severity: 100 Confidence: 95 |
| Artifact Flagged Malicious by Antivirus Service | Severity: 100 Confidence: 95 |
| Dridex Variant Detected | Severity: 90 Confidence: 100 |
| A Document File Established Network Communications | Severity: 100 Confidence: 90 |
| VBA Macro Uses Xor | Severity: 90 Confidence: 100 |
| Document Flagged by Antivirus | Severity: 90 Confidence: 100 |
| VBA Macro Imports Function From External Library | Severity: 90 Confidence: 90 |
| VBA Macro Opens a Binary File | Severity: 90 Confidence: 100 |
| Artifact Flagged by Antivirus | Severity: 80 Confidence: 90 |
| 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: 85 |
| Dynamic Content Detected in Document | Severity: 70 Confidence: 90 |
| Process Modified the Internet Proxy Autoconfig Setting | Severity: 70 Confidence: 90 |
| Process Modified File in a User Directory | Severity: 70 Confidence: 90 |
| Office Document Contains a VBA Macro | Severity: 70 Confidence: 90 |
| Process Disabled Internet Explorer Proxy | Severity: 70 Confidence: 70 |

Umbrella

SEARCH PATTERN SEARCH

www.e-funciona.com **INVESTIGATE**

Details for www.e-funciona.com

SEARCH IN GOOGLE
SEARCH IN VIRUSTOTAL

DNS queries

WHOIS Record Data

Registrar Name: Interdominios, Inc. IANAID: 818 Last retrieved March 2, 2017 [GET LATEST](#)

Created: April 4, 2011 Updated: April 5, 2016 Expires: April 4, 2017 [Raw data](#)

SEARCH PATTERN SEARCH

www.e-funciona.com/~esoporte/43/8: **INVESTIGATE**

PART OF WWW.E-FUNCIONA.COM

DETAILS FOR www.e-funciona.com/~esoporte/43/83.exe

SEARCH IN GOOGLE
SEARCH IN VIRUSTOTAL

Associated Samples POWERED BY CISCO AMP THREAT GRID

| Threat Score | SHA256 Signature | AV Result |
|--------------|---|---------------------------|
| 95 | e8911ae146aad7bb5a7f559d19b3a91453ef174759a3c4bb02a67c... | Doc.Macro.Generic-5900096 |

1-1 of 1 < >

Win.Trojan.Infostealer-5900674-0

木马（凭证窃取程序）

Infostealer 是一种 Windows 木马，用于窃取通过 Mozilla Firefox 和 Google Chrome Web 浏览器提交的凭证。它使用 SQLite 数据库存储获取的凭证。我们观察的样本是用 Delphi 编写的，并且使用 UPX 进行压缩。由于在运行时没有明显的网络流量，因此我们怀疑被窃取的凭证就存放在本地位置，以供执行攻击的其他组件投放该木马。

危害表现

创建的注册表项

- 不适用

修改后的注册表项

- 不适用

创建的互斥体

- \BaseNamedObjects\CTF.LBES.MutexDefaultS-1-5-21-2741372430-2673733078-4290318639-500
- \BaseNamedObjects\CTF.Compart.MutexDefaultS-1-5-21-2741372430-2673733078-4290318639-500
- \BaseNamedObjects\CTF.Asm.MutexDefaultS-1-5-21-2741372430-2673733078-4290318639-500
- \BaseNamedObjects\CTF.Layouts.MutexDefaultS-1-5-21-2741372430-2673733078-4290318639-500
- \BaseNamedObjects\CTF.TMD.MutexDefaultS-1-5-21-2741372430-2673733078-4290318639-500
- \BaseNamedObjects\CTF.TimListCache.FMPDefaultS-1-5-21-2741372430-2673733078-4290318639-500\MUTEX.DefaultS-1-5-21-2741372430-2673733078-4290318639-500

创建的文件

- %TEMP%\sqlite3.dll

- %SystemDrive%\history.txt
- %APPDATA%\moz.tmp
- %TEMP%\0.tmp
- %TEMP%\31379.tmp
- %SystemDrive%\pass.txt

IP 地址

- 不适用

域名

- 不适用

文件散列值

- 68f794cefe42c5b746abea703856036fed7ceaf571220874d8b70782d8d81569
- 2940298afc9b926b95a501ae12b28024b2e070eabffe28ca3da0f08f33c2c6c8
- 62aa96177f224e58362278d3424f90ebd4512b61214a36024685b0c7704ec60a
- 6850b01820037dbf2264f43140ff7780c35abef14d8c6e6bd8da9248a1b88943
- 864f375840c009d6260e2ac143dd09404e262b012e1ee4a16902f99004cbc862
- 68f794cefe42c5b746abea703856036fed7ceaf571220874d8b70782d8d81569
- a38ac23db7f5c3343285e3a17d48823756c56e9a946e56fdd9612265c40f9f99
- c8badfa7fe40d9bc10a33c118a75b920b4eb8f2f3d831376c095ba02515c7176
- e8e697802bf0219cb54ab97910d436ef2e7dbe1c2a4abf0b406a42e2507265c1

解决方案

| 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 |

检测引擎

ThreatGrid

Behavioral indicators

| | | | |
|---|---------------|----------------|---|
| Artifact Flagged Malicious by Antivirus Service | Severity: 100 | Confidence: 95 | ▼ |
| File Name of Executable on Disk Does Not Match Original File Name | Severity: 80 | Confidence: 80 | ▼ |
| Process Modified File in a User Directory | Severity: 70 | Confidence: 80 | ▼ |
| PE Has Sections Marked Executable and Writable | Severity: 40 | Confidence: 60 | ▼ |
| PE Contains TLS Callback Entries | Severity: 40 | Confidence: 60 | ▼ |
| Process Read INI File | Severity: 30 | Confidence: 50 | ▼ |
| Executable with Encrypted Sections | Severity: 30 | Confidence: 30 | ▼ |
| Executable Packed with UPX | Severity: 30 | Confidence: 30 | ▼ |
| Executable Imported the IsDebuggerPresent Symbol | Severity: 20 | Confidence: 20 | ▼ |
| PE COFF Header Timestamp is Set to Date Prior to 1999 | Severity: 5 | Confidence: 60 | ▼ |

Doc.Macro.Laroux-5893719-0

宏下载程序

攻击者可以使用启用了宏的 Office 文档在系统上下载恶意软件或执行恶意操作。此威胁重点利用该恶意软件系列中用于启动代码执行的一种常用方法。

危害表现

创建的注册表项

- N/A

修改后的注册表项

- N/A

创建的互斥体

- N/A

创建的文件

- 不适用

IP 地址

- 不适用

域名

- 不适用

文件散列值

- 0e6dcb17c222cf90bec20d6e2f4e7e8ce3c0a6ea3a9960e5914be4eb8dce6cab
- 155a0409cecdf0ac869ca2c15a2b55c746c6f940ee3d8a9f08a91554add7b2d
- d3678428b6939ed19211b5b88a079f33e556d4e547c5acb1eaa148366d0b6e6d
- 13853b3d52b4e19a7a4b1dfb620f6ee28fc02ff3fb6162ebfca3ee6219a30bbc
- 78fcadb4d82afe19799c4a47626a8faf75fc56ecde28bd250f33f90e79c65e42
- 949dcec4d0a79d1296366353794a275b0bea056bb099558f8c231afe8cb9adff
- be1e11932dd5820dc45e3fdcde360af6634dfc0da5cbf9de9b7a717de50b0ec9
- 529239d98ee139cc276daff5db157746a2a421cbe0f7bd870a8f10d51452bb20
- afd854fa48077adb87b3e700f6695c9d5ef74e77353328337ef7c591060f5f89
- d5111633f192a9a83cc39b4d8c9717a0d284a00acc1af4274f85319ac0034505
- 0d1a187f252848e219053845351c3b07d440587d55cc624b0b2d59419ea8a896
- 180caf6d44cdec9c977aac2f2bd2d15ba10477bcba7bccbaba720503dd5eb021
- 4701392544a60dc493e13179ab0b3a709217961353e6e404a40d2278b4dbd6d2
- 4c499c70249e9e953c0b63f13c3d2c368e07b04e0a44cb1b3fd05e4aa4f13f56
- 6921de7df37141ca093a24d1184e4812ce5883cc86383f6435d85ff561c58bc6
- b2de2b00c0494238c04784e7a03307d1680eee4f2e6a8b40df455bf91db8898a
- b332cde3d53ff68390f666f86f270ca005926ae66d47322fac839291518db1ef
- 1bc489abc45a3db159c2d43cb220f3f3e7aaa6d40eba49758150e40c3df03ff2
- 40e498704f3f4f807e807f59c0644e457e1690847d43dcbd43aa1b4d41b41e4a
- 5e930fe0323d09a4e7c10edbc8bf8d51e2826be344a3778695c7adb8eda10ca4
- 66d223fd0f0b2ce642755bb18f876e919c91dfedcdb84ffb79eba2de8b0e10eb
- 6abffacb8a95bf7d67fe7544f2020e90109be89a0a5ec754def98377b361e81f
- 6b03f59727e07f63340c1a1603538c107d2008c08fb34f3f47d6ecb352b391f0
- 7a2e044f1716d2236800dd4dd186cd5224abe779692cd5e0767714798aaa430a
- 7a750bd06456920deeb26929b5bfd8c9a7a0106c917e0aacd79b7b39ba505675

解决方案

| 产品 | 保护 |
|-------------|----|
| AMP | ✓ |
| CWS | ✓ |
| 邮件安全 | ✓ |
| 网络安全 | ✓ |
| Threat Grid | ✓ |
| Umbrella | ✓ |
| WSA | ✓ |

检测引擎

ThreatGrid

| Behavioral indicators | |
|--|------------------------------|
| Artifact Flagged Malicious by Antivirus Service | Severity: 100 Confidence: 95 |
| Document Flagged by Antivirus | Severity: 99 Confidence: 100 |
| VBA Macro May Hide Windows | Severity: 75 Confidence: 99 |
| Artifact Flagged by Antivirus | Severity: 80 Confidence: 80 |
| VBA Macro Has Action on Open | Severity: 76 Confidence: 85 |
| Antivirus Service Flagged Artifact As Containing A Macro | Severity: 76 Confidence: 88 |
| Process Modified File in a User Directory | Severity: 76 Confidence: 88 |
| Office Document Contains a VBA Macro | Severity: 76 Confidence: 88 |

发布者: ALEXANDER CHIU; 发布时间: 下午 5:05 

标签: AMP、CLAMAV、防护、邮件、恶意软件、SNORT、THREATGRID、UMBRELLA