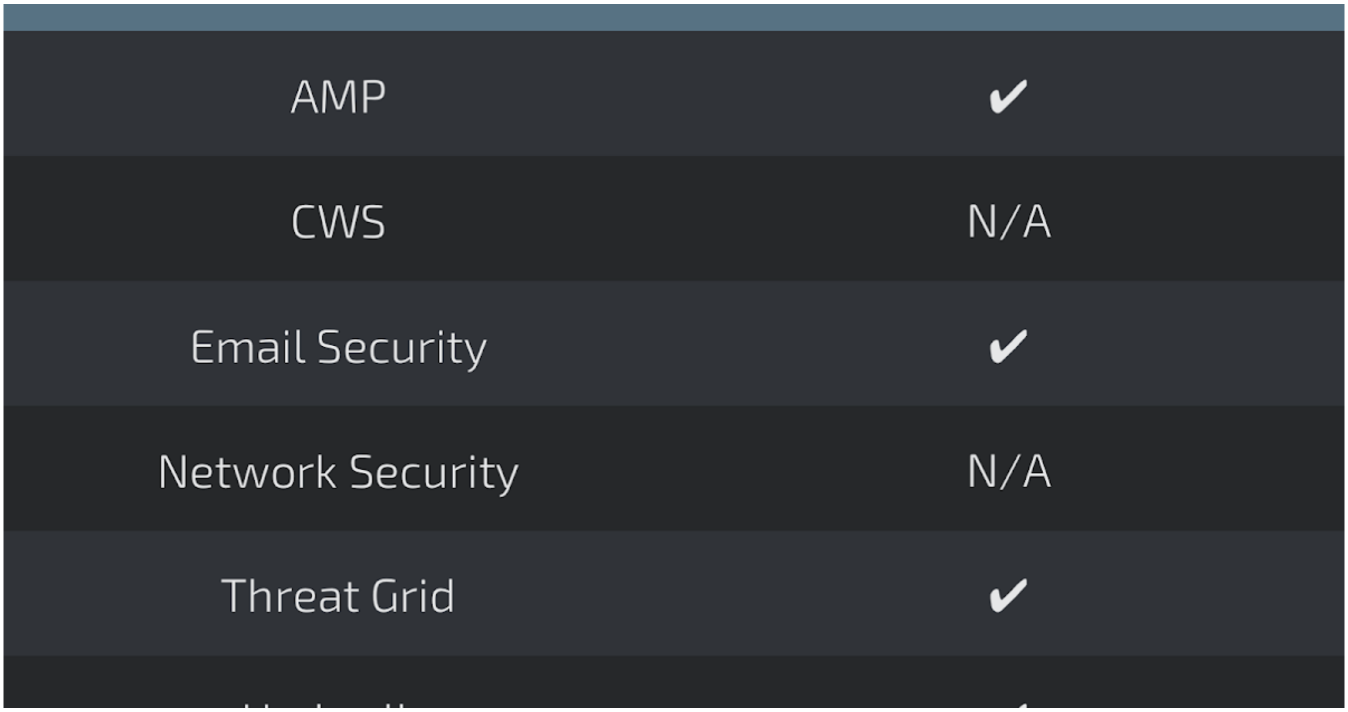
# Threat Round-up for Mar 24 - Mar 31

blog.talosintelligence.com/2017/03/threat-roundup-0324-0331.html



| | |
|---|---|
| AMP | ✔ |
| CWS | N/A |
| Email Security | ✔ |
| Network Security | N/A |
| Threat Grid | ✔ |

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between March 24 and March 31. As with previous round-ups, this post isn't meant to be an in-depth analysis. Instead, this post will summarize the threats we've observed by highlighting key behavior characteristics, indicators of compromise, and how our customers are automatically protected from these threats.

As a reminder, the information provided for the following threats in this post is non-exhaustive and current as of date of publication. Detection and coverage for the following threats is subject to updates pending additional threat or vulnerability analysis. For the most current information, please refer to your FireSIGHT Management Center, Snort.org, or ClamAV.net.

This week's most prevalent threats are:

- **Win.Ransomware.Cerber-6162243-1**
  Windows ransomware
  Cerber is a popular ransomware family that continues to undergo active development to continue being dropped in the wild. It still drops multiple ransom notes, including a desktop wallpaper as a warning post. Unfortunately, these recent samples are protected with heavy crypters.
- **Win.Trojan.Wabot-6113548-0**
  Backdoor
  This is an IRC worm written in Delphi. The code is not obfuscated. It drops several files in the system32 directory, and a text file with the word "marijuana" written in ASCII art to the root of the system drive. After waiting for some time, it will try to connect to an IRC server and join the channel '#HelloThere'. From there it receives backdoor commands.
- **Doc.Macro.HeuristicReplaceFuncs-6169546-0**
  Macro Obfuscation Technique
  To prevent quick understanding and basic detection of malicious macros developers use different obfuscation techniques to hide the macro's functionality
- **Doc.Macro.ReplaceFuncs-6171292-0**
  Macro
  This sample is a Microsoft Word document that uses a macro to launch a PowerShell script to download and execute another executable payload. Unfortunately, this secondary payload was unavailable at the time of this execution report.

- **Js.Trojan.Diplugem**
  Adware
  This family installs browser extensions in your browsers without your permission. It's main functionality is to show advertisements in different ways, such as opening tabs, potentially interfering with usual navigation.
- **Doc.Macro.ObfuscatedObj**
  Macro Obfuscation Technique
  This obfuscation technique utilizes macro string operations to prevent direct static detection of the string WSCRIPT.SHELL, which is the object used to execute commands outside of the Office system. As an obfuscation technique, these droppers are being discovered delivering payloads of all sorts and sizes.
- **Win.Trojan.VBCryptLaser**
  Trojan/Info stealer
  This malware is mainly an information stealer and it is able to detect an instrumented environment such as a sandbox. Moreover, the malware injects itself in legitimate processes and it persists reboot by invoking either Javascript or mshta . This family is highly obfuscated and considering its behavior is a variant of the infamous Kovter trojan.
- **Win.Virus.Virut-6171773**
  Virus
  This is a virus which is well know for opening back door on TCP Port 80 using the irc server ircd.zief.pl allowing remote attacker to download and execute additional files. It's looking for firewall and antivirus instances, as well modifying host file and internet explorer proxy settings.
- **Win.Ransomware.Spora-6172235**
  Ransomware
  This ransomware is encrypting files and not adding any specific extensions. It's also deleting volume shadow copy to avoid system restore point. It install a startup link and modify internet explorer proxies and create an html file with a dynamic filename. One difference with other ransomware is that no network traffic is generated as everything is done locally.

## Win.Ransomware.Cerber-6162243-1

### Indicators of Compromise

**Registry Keys**

N/A

**Mutexes**

N/A

**IP Addresses**

54.87.5.88

**Domain Names**

- api[.]blockcypher[.]com
- hjhqmbxyinislkkt[.]1efxa8[.]top

**Files and or directories created**

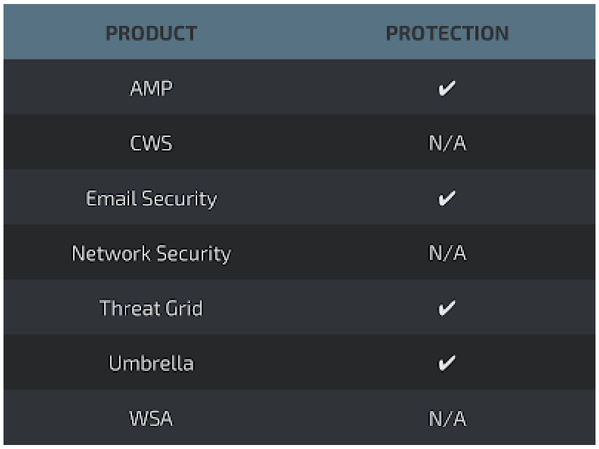
- %APPDATA%\Microsoft\Outlook\<RANDOM_FILENAME>.8a2a
- %APPDATA%\Microsoft\Outlook_HELP_HELP_HELP_1YI7CF_.hta
- %APPDATA%\Microsoft\Outlook_HELP_HELP_HELP_2NN4UMV_.png
- %USERPROFILE%\Desktop_HELP_HELP_HELP_J81LBSA_.hta
- %USERPROFILE%\Desktop_HELP_HELP_HELP_L1JAF_.png
- %APPDATA%\Microsoft\Outlook_HELP_HELP_HELP_6MTGJWJ_.png
- %APPDATA%\Microsoft\Outlook_HELP_HELP_HELP_LKCGK3Y_.hta

**File Hashes**

- dc184001af08dd043150c350c94304041b2c8e995ce62f05f846d776b450f80f
- 57288de46d603910b1d6eb88390a4b7083b3f060e75bd76023a8a13f7c40633f
- c0ab4ccdef7ad4fb6b1af396a29cbb4220dc720acfec091fa5d6484656fec63f

- ca7d955a40f2d7a969245884fffd0189402b05af3f9896d10e476cbdaa1b0829

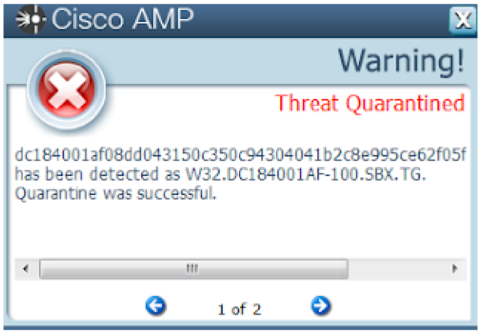
## Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | N/A |
| Email Security | ✔ |
| Network Security | N/A |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | N/A |

## Screenshots of Detection

### AMP

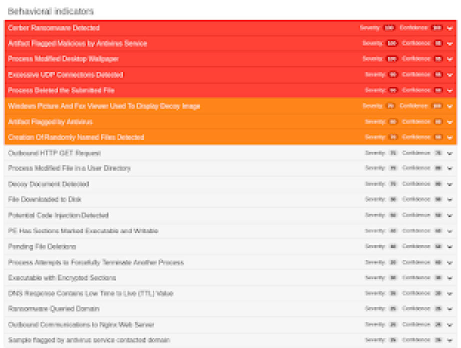


Warning!

Threat Quarantined

dc184001af08dd043150c350c94304041b2c8e995ce62f05f has been detected as W32.DC184001AF-100.SBX.TG. Quarantine was successful.

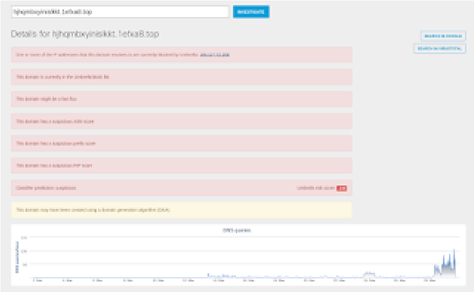
### ThreatGrid



Behavioral indicators

- Cerber Ransomware Detected
- Artifact Flagged Malicious by Antivirus Service
- Process Modified Desktop Wallpaper
- Excessive UDP Connections Detected
- Process Deleted the Submitted File
- Windows Picture And Fax Viewer Used To Display Decoy Image
- Artifact Flagged by Antivirus
- Creation Of Randomly Named Files Detected
- Outbound HTTP GET Request
- Process Modified File in a User Directory
- Decoy Document Detected
- File Downloaded to Disk
- Potential Code Injection Detected
- PE Has Sections Marked Executable and Writable
- Pending File Deletions
- Process Attempts to Forcefully Terminate Another Process
- Executable with Encrypted Sections
- DNS Response Contains Low Time to Live (TTL) Value
- Ransomware Queried Domain
- Outbound Communications to Nginx Web Server
- Sample flagged by antivirus service contacted domain

### Umbrella

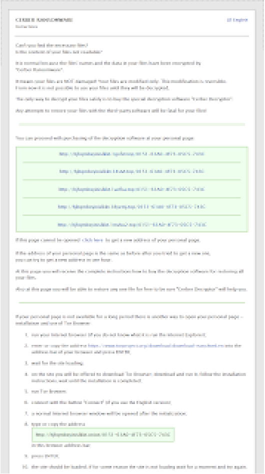


hjhqmbxyinislkkt.1efxa8.top

Details for hjhqmbxyinislkkt.1efxa8.top

[illegible]

### Malware screenshot(s)



## Win.Trojan.Wabot-6113548-0

### Indicators of Compromise

**Registry Keys**

HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\shell
is changed to point to the malware binary

**Mutexes**

\BaseNamedObjects\sIRC4

**IP Addresses**

N/A

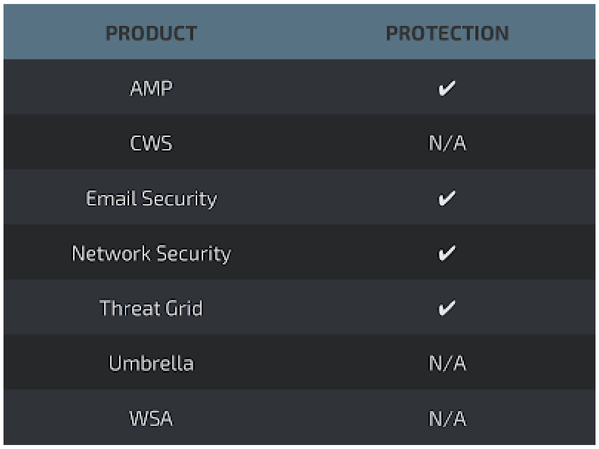
**Domain Names**

uk[.]undernet[.]org

**Files dropped**

- %System32%\sIRC4.exe
- %SystemDrive%\marijuana.txt
- %System32%\DC++ Share (several files are created in this directory)
- %SYSTEM32%\xdccPrograms (several files are created in this directory)

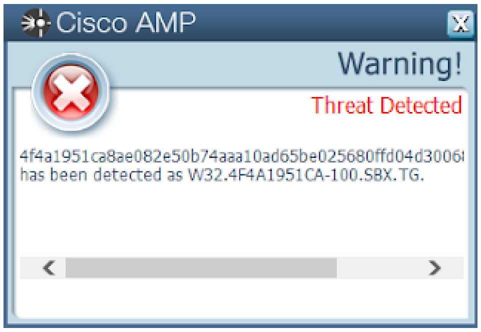
**Coverage**



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | N/A |
| Email Security | ✔ |
| Network Security | ✔ |
| Threat Grid | ✔ |
| Umbrella | N/A |
| WSA | N/A |

### Screenshots of Detection

#### AMP

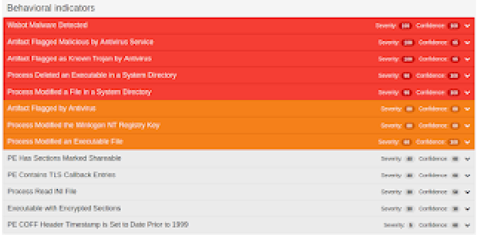


Warning!

Threat Detected

4f4a1951ca8ae082e50b74aaa10ad65be025680ffd04d3006
has been detected as W32.4F4A1951CA-100.SBX.TG.

#### ThreatGrid



Behavioral indicators

Wabot Malware Detected Severity: [illegible] Confidence: [illegible]

Artifact Flagged Malicious by Antivirus Service Severity: [illegible] Confidence: [illegible]

Artifact Flagged as Known Trojan by Antivirus Severity: [illegible] Confidence: [illegible]

Process Deleted an Executable in a System Directory Severity: [illegible] Confidence: [illegible]

Process Modified a File in a System Directory Severity: [illegible] Confidence: [illegible]

Artifact Flagged by Antivirus Severity: [illegible] Confidence: [illegible]

Process Modified the Winlogon NT Registry Key Severity: [illegible] Confidence: [illegible]

Process Modified an Executable File Severity: [illegible] Confidence: [illegible]

PE Has Sections Marked Shareable Severity: [illegible] Confidence: [illegible]

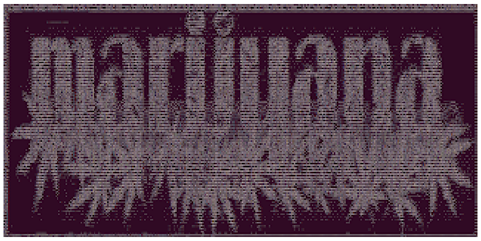
PE Contains TLS Callback Entries Severity: [illegible] Confidence: [illegible]

Process Read INI File Severity: [illegible] Confidence: [illegible]

Executable with Encrypted Sections Severity: [illegible] Confidence: [illegible]

PE COFF Header Timestamp is Set to Date Prior to 1999 Severity: [illegible] Confidence: [illegible]

#### Malware Screenshot



## Doc.Macro.HeuristicReplaceFuncs-6169546-0

### Indicators of Compromise

#### Registry Keys

N/A

### Mutexes

N/A

### IP Addresses

N/A

### Domain Names

www[.]cleverdotl[.]top

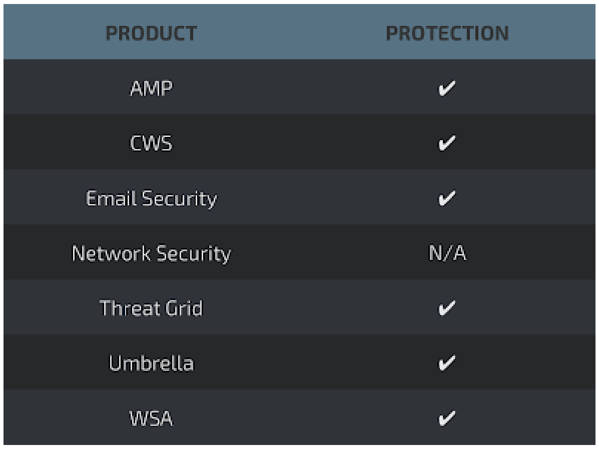
### Files and or directories created

N/A

### File Hashes

- d183f2200ed5f510888a80e95d99aa5a3c8408dee7f0c9b8330fc52fb0592dce
- ee6284d966eb9f510a1b44ef6ba435048729c8ce8a741fb33575d5b1b6d347f5
- bafa3a9e5b2f290eabce23811c6309209d281f31bc6eee25b4eb739bce1800ce
- 1480d45ed9841d055e4e04ade87f7785b3006fb62c8060616ed7507185df2b77
- 13d61439ede67b78a536ea3c510534db0ab7d295ef1275645b7981814909d0db
- b70497f0e50fcbfe83a7b92021db30e14f3fd6a829ab9948f828d46048cdbdd6
- 42ddcf96146d3be84bf36abe71fd6780abf79aa1ccb2ba65093c9b46a3d76b03
- 1fdb9f23b2d7dbe849f38f79f88449fe3f327e76585b202d914718036245c469
- 9948928059c4676f6b6f8519fc39eaab89a027159577dbc3ceac4833ef35167f
- 3fd05d08c135075d2f4a72652746bc42e359b9d1658d4f3b41d5f95bb7216649
- db7d22c806ca4a305a317df58a65bef8e2195bb0a8ac223313a8a18c37f5c143
- 5ee9f3b87db48f41eaaffd9a7fc9cc76920dd498237a23e1ad7585f4e2be02d8
- 6dfb35527b23ca769510228498c8de68cfc93d5c2b83246d8e9b338d2717481f
- fe257b7da01cfc247564f2e7b36b19b8af548c2f3ffbee2b9d8d552a71502d78
- dec3c2f1b1de6d70fc566f036ab320decc88ed5418e429feae45189e458bf5e4
- d4175848a03cab54f856d41c51ac4ede18c01382a5ebc4ed40c4e27f2e45244b
- c19a7af6c3846bd433765c027149ff838482a55624a5e603d395ad83d6f24129

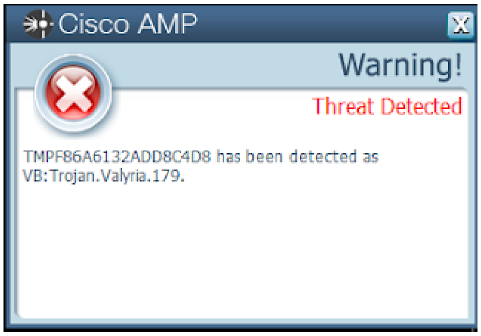
## Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | N/A |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

## Screenshots of Detection

### AMP



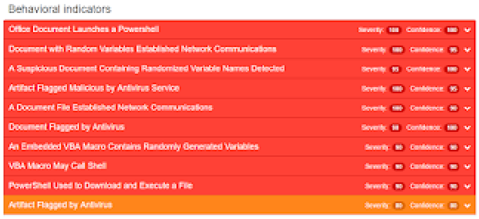
Cisco AMP

Warning!

Threat Detected

TMPF86A6132ADD8C4D8 has been detected as VB:Trojan.Valyria.179.

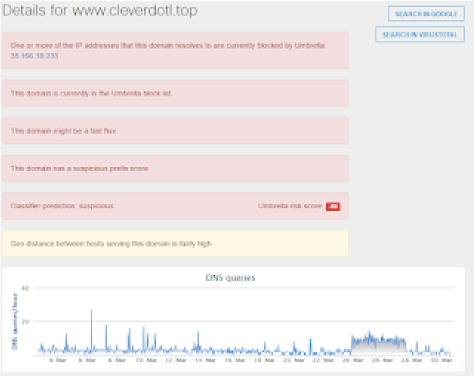
## ThreatGrid



Behavioral indicators

| | | |
|---|---|---|
| Office Document Launches a Powershell | Severity: [illegible] | Confidence: [illegible] |
| Document with Random Variables Established Network Communications | Severity: [illegible] | Confidence: [illegible] |
| A Suspicious Document Containing Randomized Variable Names Detected | Severity: [illegible] | Confidence: [illegible] |
| Artifact Flagged Malicious by Antivirus Service | Severity: [illegible] | Confidence: [illegible] |
| A Document File Established Network Communications | Severity: [illegible] | Confidence: [illegible] |
| Document Flagged by Antivirus | Severity: [illegible] | Confidence: [illegible] |
| An Embedded VBA Macro Contains Randomly Generated Variables | Severity: [illegible] | Confidence: [illegible] |
| VBA Macro May Call Shell | Severity: [illegible] | Confidence: [illegible] |
| PowerShell Used to Download and Execute a File | Severity: [illegible] | Confidence: [illegible] |
| Artifact Flagged by Antivirus | Severity: [illegible] | Confidence: [illegible] |

## Umbrella



Details for www.cleverdotl.top

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 35.166.18.233

This domain is currently in the Umbrella block list

This domain might be a fast flux

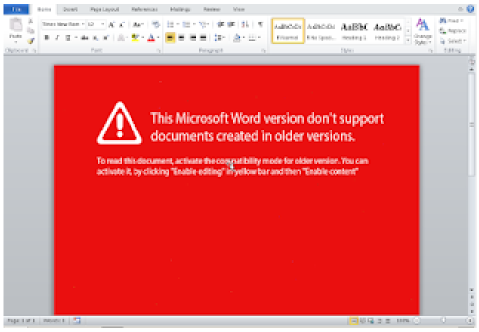
This domain has a suspicious prefix score

Classifier prediction: suspicious

Umbrella risk score [illegible]

Geo distance between hosts serving this domain is fairly high

## Malware Screenshot



This Microsoft Word version don't support documents created in older versions.

To read this document, activate the compatibility mode for older version. You can activate it by clicking "Enable editing" in yellow bar and then "Enable content"

---

## Doc.Macro.ReplaceFuncs-6171292-0

### Indicators of Compromise

### IP Addresses

35.166.163.174

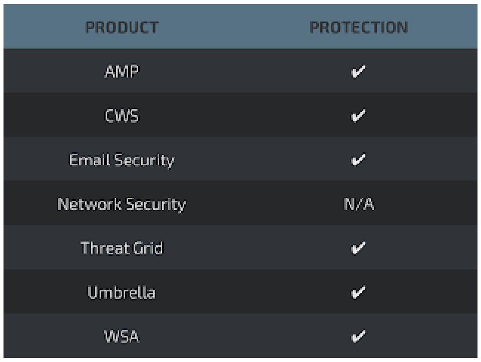
### Domain Names

otweeytl[.]bid

### File Hashes

77bccf5e4175d11971399f89abe0256c230e1757a3d0804737b14a0ac839890b

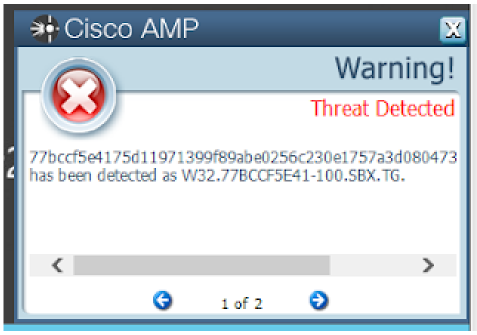
## Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | N/A |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

## Screenshots of Detection

### AMP

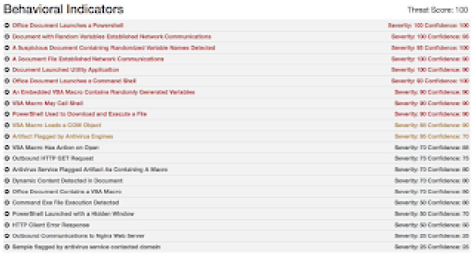


Warning!

Threat Detected

77bccf5e4175d11971399f89abe0256c230e1757a3d080473
has been detected as W32.77BCCF5E41-100.SBX.TG.

### ThreatGrid

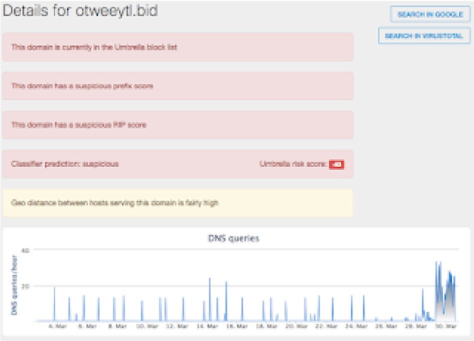


Behavioral Indicators

Threat Score: 100

| | |
|---|---|
| Office Document Launches a Powershell | Severity: 100 Confidence: 100 |
| Document with Random Variables Established Network Communications | Severity: 100 Confidence: 95 |
| A Suspicious Document Containing Randomized Variable Names Detected | Severity: 85 Confidence: 100 |
| A Document File Established Network Communications | Severity: 100 Confidence: 90 |
| Document Launched Utility Application | Severity: 100 Confidence: 90 |
| Office Document Launches a Command Shell | 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 Loads a COM Object | Severity: 80 Confidence: 90 |
| Artifact Flagged by Antivirus Engines | Severity: 90 Confidence: 70 |
| VBA Macro Has Action on Open | Severity: 70 Confidence: 88 |
| Outbound HTTP GET Request | Severity: 75 Confidence: 75 |
| Antivirus Service Flagged Artifact As Containing A Macro | Severity: 70 Confidence: 80 |
| Dynamic Content Detected in Document | Severity: 70 Confidence: 90 |
| Office Document Contains a VBA Macro | Severity: 70 Confidence: 80 |
| Command Exe File Execution Detected | Severity: 50 Confidence: 90 |
| PowerShell Launched with a Hidden Window | Severity: 50 Confidence: 70 |
| HTTP Client Error Response | Severity: 50 Confidence: 90 |
| Outbound Communications to Nginx Web Server | Severity: 20 Confidence: 20 |
| Sample flagged by antivirus service contacted domain | Severity: 25 Confidence: 25 |

### Umbrella



Details for otweeytl.bid

This domain is currently in the Umbrella block list

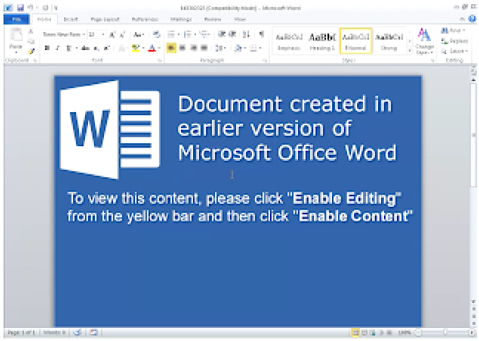
This domain has a suspicious prefix score

This domain has a suspicious RIP score

Classifier prediction: suspicious Umbrella risk score: [illegible]

Geo distance between hosts serving this domain is fairly high

### Malware Screenshot



Document created in earlier version of Microsoft Office Word

To view this content, please click "**Enable Editing**" from the yellow bar and then click "**Enable Content**"

## Js.Trojan.Diplugem

### Indicators of Compromise

**Registry keys**

- USER\$UUID$\Software\Classes\SystemFileAssociations\.aHTML\shell\Edit\command
- USER\$UUID$\Software\Classes\__aHTML\shell\Edit\command
- USER\$UUID$\Software\Classes\__aHTML\shell
- USER\$UUID$\Software\Classes\__aHTML\shell\Edit\ddeexec
- USER\$UUID$\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.aHTML
- USER\$UUID$\Software\Classes\__aHTML\shell\Edit
- USER\$UUID$\Software\Classes\SystemFileAssociations\.aHTML\shell\Edit
- USER\$UUID$\Software\Classes\SystemFileAssociations
- USER\$UUID$\Software\Classes\SystemFileAssociations\.aHTML
- USER\$UUID$\Software\Classes\SystemFileAssociations\.aHTML\shell\Edit\ddeexec
- USER\$UUID$\Software\Classes\.aHTML\OpenWithProgids
- USER\$UUID$\Software\Classes\.aHTML
- USER\$UUID$\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.aHTML\OpenWithProgids
- USER\$UUID$\Software\Classes\__aHTML
- USER\$UUID$\Software\Classes\SystemFileAssociations\.aHTML\shell

**Domain Names**

getlikemobj[.]info

**Files and or directories created**

- 0doGTj9XEZ5tbV5.dat
- 0doGTj9XEZ5tbV5.exe
- UtE5FnEWw87hxH.dll
- UtE5FnEWw87hxH.tlb
- UtE5FnEWw87hxH.x64.dll
- background.html
- content.js
- lsdb.js
- manifest.json
- uui.js
- bootstrap.js
- chrome.manifest
- bg.js
- Install.rdf

**Installed services**

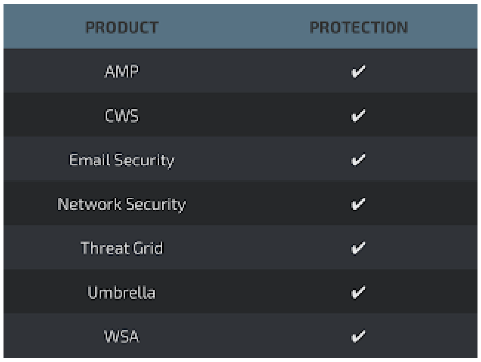
regsvr32.exe /u /s ".\\UtE5FnEWw87hxH.x64.dll"

**File Hashes**

- 0333de69ebe7ef58889c39c6ee10b33e8fa4299849c760e6f018bac5ae2212aa

- 9eb18b9091281aa25afa4ced079024a043913e179a03947f73dabe121f36dc2b
- 07e32a2e78410eb73f525032636894e82193d5806c85a132c7efd31a76abc862
- a441bf44fec8d08481920e240281afccdcef2f0cfadb681b7b6ce50be495fc01
- 0aa8272fc12da7273cdc3573ee4e78849fe187f01eca9cda4b7941de99d8bb83
- a6ac9b2e5211f3feb41a91a5c82992de483b56c142dc35e84439a965c8250f50
- 0591e02001c57dccc0062765240c0766fd24a2fb0af37a6e32a211ea202074b3

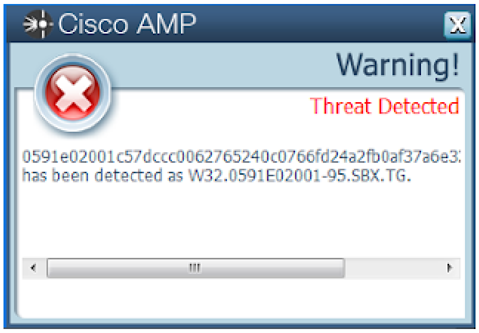
### Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | ✔ |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

### Screenshots of Detection

### AMP

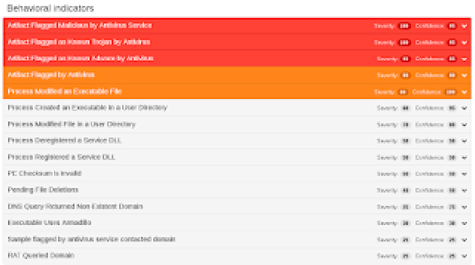


Warning!

Threat Detected

0591e02001c57dccc0062765240c0766fd24a2fb0af37a6e3
has been detected as W32.0591E02001-95.SBX.TG.

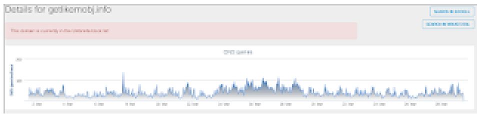
### ThreatGrid



Behavioral indicators

| | | |
|---|---|---|
| Artifact Flagged Malicious by Antivirus Service | Severity: [illegible] | Confidence: [illegible] |
| Artifact Flagged as Known Trojan by Antivirus | Severity: [illegible] | Confidence: [illegible] |
| Artifact Flagged as Known Adware by Antivirus | Severity: [illegible] | Confidence: [illegible] |
| Artifact Flagged by Antivirus | Severity: [illegible] | Confidence: [illegible] |
| Process Modified an Executable File | Severity: [illegible] | Confidence: [illegible] |
| Process Created an Executable in a User Directory | Severity: [illegible] | Confidence: [illegible] |
| Process Modified File in a User Directory | Severity: [illegible] | Confidence: [illegible] |
| Process Deregistered a Service DLL | Severity: [illegible] | Confidence: [illegible] |
| Process Registered a Service DLL | Severity: [illegible] | Confidence: [illegible] |
| PE Checksum is Invalid | Severity: [illegible] | Confidence: [illegible] |
| Pending File Deletions | Severity: [illegible] | Confidence: [illegible] |
| DNS Query Returned Non Existent Domain | Severity: [illegible] | Confidence: [illegible] |
| Executable Uses Armadillo | Severity: [illegible] | Confidence: [illegible] |
| Sample flagged by antivirus service contacted domain | Severity: [illegible] | Confidence: [illegible] |
| RAT Queried Domain | Severity: [illegible] | Confidence: [illegible] |

### Umbrella


Details for gedikemobj.info

## Doc.Macro.ObfuscatedObj

### Indicators of Compromise

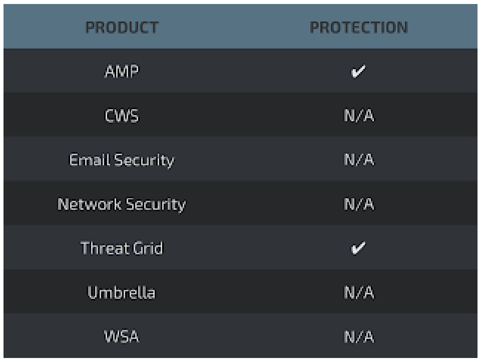
### File Hashes

Please note this is not an exhaustive list.

- 00151e030408a5183d92132652d5a0c5eb2f9e073209cb7ee12060312c5f400c
- 01f9d4276b16af80bb29dd195d343e1844062f0d86115ec5ace3234cd510b403
- 033f7a9d6ed8cbb6ecb958c9db9ab7794d37c9e763b029329b2fdf431c172be4
- 03ade17b4ad71a395b4ba657171537d4e643f3686b7c1072208366bba26c9fdf
- 08aed8b4e7f420d1c08f7fa3de86143af13ba61313e5d98f7ce552e554c991b4
- 0a3693404f2b073d62c8b7bfbd4701fec0a2b6bb6efe7b91f274065e0b7540ff
- 0cb8d7a50e1e1d36be68bf6686f7772d1fc60f7a03ec9900d5abf842546b7ab8
- 0d1fd8c7ddf4abe530008971c2fe7f239c90052ad426ba480205c1e335db7966
- 0d69b76da355e4a7cb36976626d540cefd9ae8e1fd96f0c7ae7f7e582f1aa96e
- 125df53cab91b182b0c7d5cec5e310b3471e1b4f640edc8ec9c499f1f41df237
- 12b9b3f8c125a75653fe2e19f361d8a164e1c9d4653fd8690b4f197495cba580
- 19642ed34dc6e68b8a29075c3886027530d08351a588e1ccfa368df2ce2350dd
- 1c438d063a759da25a2517d4ca81f92606225d372143c978fa30cd4769025863
- 1d4d3da400696861a219e02ada9c730bf825484327322ea8a1b27ff7a3c11de4
- 1e316a875a347ae678fa11f12b08885e0b62a8abc3ca41cd7bed8f0d421c09a1
- 1e7ffa8b2f7b2dec0ff62a1ef51fe5a4adc6d11cf7e1d004d9e09dfdceaacb7a
- 1f49b218b1e4afb4b15124acd9c9a8eb8a1ba9d87fa91e8d255bb73c14a37f9f
- 25d93ab8a663df35b9752edc3bf7a1a2f563f626ff405f6b05386ad4df3fb776
- 2bcd02fc25eece8a348d96b80fa8933ff1411fd96f7e5116a14fc8d65ac2f4b8
- 2ca2cc8af7e0d37bdb2dbba9abf8399e4db695a7d6b31d050950a68d2635f260
- 2d8900fceeb3ec6a064420d662e7422d4ebc1230479b9c330661e10ef1b21881
- 2fe88a9c446bfb5cb93c948cfcb9d781a03a8422d5307e0ac4e987f16c46abd2
- 3393ddf44d6636bbc1d45c26b3a9c5073217a95d7506ddf7756e813e445a9ecb
- 348aee4ee9827c954854a496f24f2c4d2ba96853344884e8a5cf616d07d7236d
- 35582cb16758ed296fad554830cca279fce0d7512851ba0a382373f2d8ed32d2
- 368fc1d3fe0de1e9a73c7c5dd840d2f769e8c3d1a32a86390905d45e9ab2d9ff
- 3739cb9ef330544fc349da2c9cbc66151205904f625acda85bbe16152943830d
- 3a01219542a25bab989ffd78af40a4b13a636e9cdd50f92d659e9dbf253abf94
- 3becf2e1eb115dc2e41d947826b59ab8fd83b3f825b9cd3bb9f8003dd1d02416
- 48b565b639fa5d532b65246f82e66b325b7e8549f9bf04d27955a1b3a98fa281
- 53c50bf3bdfa58b66565071e82bb7ba40ac3cc344893b0aeeaa15502483ec3f6
- 54b5776a210ac4b6a00eca3efa2f0b665616f706a813cf29fe2ecf19cd90887c
- 5549e374040cd995939b24a8095c74e9fec188a04ca9a0189a289d3be0bfdc37
- 5617e4b5e25a41d5a491b3e36fcd165a1a7b999ea0de567ca63baec40b757ddf
- 5854de47ff6fedc84cc6fb73760763b8e427164bf3369e89d3e4b3b42483103d
- 5b34c3c2ec780258644c3245693dfef254cb91716c35ae33937f637bd8e04978
- 5d996e33e92e6f7b83867ccad52be72274bfd79d964bc4988043d91231369650
- 60979006e12a42b7f781adb2b1f8fe05836db0683abe0efc05b822dad5d1a9f7
- 6556d7052f3c3fafe15aa3ee81dbbb4b1caee88fd7e65788c1f90bfd940be7b0
- 69e7d856dc8e0b5508b8a4050c36451a0dc0164b856e1bd1efdbc6f8ec6de66e
- 709fe7d54e5ba52f2e45c4c62fdf1636ed64be0ae367bd992eb212aa234200cc
- 7120ecc9c04b8f9d93829210f3168b14cfecd45dec52478ff87d0ee86324cc0c
- 71715f32e3cb54756b39716f8dd33c503eabbb054f4a4e82d5e2b9a9b96ed46f
- 77d049ad71ea81f13e89d82ed398e59e95085d10cb0041eb6ef5ed48c0fd95e2
- 77d11af8d4b7f9e48764d285e801f1db3d7dffcd6a0ba17bb9bb75c178227b96
- 7dc0651c4258b079fe68acbddfcbedd89a94448bffbf4ca93c231fca171dda09
- 805d74474a13e5a3be13c73bb1d0dbb1b33dfc9dcaf067b4aea5d2a8584a29eb
- 80a05b5499539e7bbdd3dd34f04a940c5d36f8d44d7725c6530bf3872966a27a
- 85d95919960cab3788b587008fa49b61c230bbbe28cd9d000f0cb179abbbb0f5
- 896dc5b55cd8c0e160dc52ac9b21ed4c46da22ed3c369eb5dee856edb88f46e1
- 8caf0f703a108a6fec8d55e8f1a028814a3f26afb2f8a58a96576e1042f99874
- 8e8cd4aefc8422ba176d009d90ddcd65f72161a2576ab443f69480bb30050825
- 8f9292e116fb2a07838724e648e17d2a5e5e3e074232dbd83bfe624391acafee

- 9009b9ad9547af92f68b01f09200a043da6be1a65b274129a7c47532f3f966b0
- 99d311cef89fade4d29e3e33df256029841d59d2ee06579dbeac2c9519ef7cb3
- 9a80fde74d9e7674be309f44f6fa7b5e53f34a0d6f2fcc084d733c42bf95c4a5
- 9ba0d666293490f051b1612e6c8bd635dc382ae4e931fff5fe9ba7fa926d6b82
- a32c4d11737b59236b47b73fe20952a3827593b52f241100ba77648e60e1d42c
- a49705d9325ce8d87b1f24e92a3b64164ab0051eb3efbc0fc775d579959d9a62
- a69f4d4eddbd656a6ae061cc001ae245db87eced67015365cca1834179845290
- a8a449812c89915a1872aeed6424abdf7fc1f4b8d8ae35deee3f3c04104c2a79
- a9e9af82ef11cc51091426afd0784ad62c57dbeeecccd566f8cdf6be2fd8258e
- adb6155ed8d5b3e7c4a2c6fc58108382313b05f171336c52cb1ae7119dfee540
- ae01487921a5e8538f1599c3b0d467328992b32aace53b776180c6071bbae2fb
- aeb6e8a86ce9c7a9cfc0efe82038932ec1c9ca150279f151574233777b4ee69f
- b3551d5d465a7e7315a5c5ad15c99393f1dd77732ff2ddcbd96c0907c3b6e84b
- b402f8acfdbfd194baa2736b45b6529dbc2a6e523f7a7f15470765019387eb6d
- b47ba806ce07000e7fc3365da81afcd6783308e2077391f80e3a272d8090d95c
- b4d192f5122872145142b32a8c11253d70c83a5c23963da0c7f3408593e81238
- b55375ea1eac3f1967483e18c6b32cb5332d281975d54913c6fd3156129574f0
- b5df216db89067df157bab2c5e0042985e03aba5d1807551a069cf800b21d385
- b5ea73190ced08e3694d27d298a69f040cf70b05f21812f60334444102eb875e
- b798f6c32168e8c598af8b795924d42334dc1dbe9d5888125e39c0d3f03cda69
- b831e804d52760572bb4f77d9b62a2da6bbd6c7c4f5ddb0f1b5731e47fa784e7
- b9dd997c2f141fc0dea676b42dd962050f2886f2a1398a14f8e91498486eac90
- bbcf611f3d1da4aa31cd953d7372c50d8ce9a49af8664a86eb804adad390f0e6
- bcdd7ae916d59519521e9c3e96980092c0ad84db98b1f1301eee6899fa599769
- c3a0e9b007795db909245c18f597b4ece53dea011b088abd4f0717208dd3253c
- c3abbd74785fa3d8eb51f0f99fa568e566f864244ea2f4fda9971cda661036da
- ca4607f2cabdd6d3693ad3405085abd1e92112cf7a9fe56a2e52615778bfe79a
- cb10ef20a93542eb0e8ec1e9c921ad120454156c8ec5e431b3b1afa27afd8bbc
- cf0ee89b626684ed9f9f60823531dd1ed38cfd46395036209a274cadaf123575
- d10fa5c1a6bd4da0a3f9d0ee605fa906db9a7e0fe2cc213339d5af8cbee80855
- d20e3bad471429f04e0ca1b28fcf1177cac689394f39dcb20379935dbea883cc
- d314d825d85787833886b1a8c4cf882f8b25f268206e23372cdf3cc67d15e162
- d543f49808fc093e31f8282407d2b520678f041a5c43646b235116743b2e0eaf
- dafaa5c3d3ef49d1f17027cd33a6172b4ac35defaa12f136503200104eebfa1c
- db5e3b35e653690b164bb3aa7f9e8caa9e77f9233d846fbda27f616eb7334aff
- dccc34da745ee2d9464a643be8b4239f3f592498d5362b29dedb30c259878404
- dd926e46cf871d98cfb025896bbcb5a5c71025f5573f5ad1eb0ee77aa3bf5546
- ddc9d38524dc6f2ac918c5f0cb251cc2916f063835414bf34a58cc0c997acccf
- e4921ad4b0561e8c4dfbe0f72aff53d9bc06eaf177a9dbca7e538a6f1312ba1d
- e49328097b3531fb8981531e931b3cd1e2adcc22c8a89781260e0bd779705143
- e96d823ab4de0dde23a564e327d610d933051d6664df685278f85e6d096e25a5
- f3f8905a5ddc3074a367095a51662d4ac434dbe9e680d0b94bfa71f6b5875329
- f6c8e3c90fbc309e3d25c7b08609684e7ca16d93d7a568b702910222af9a4d4f
- f8ca6ffd131b738a30c90b486a839010a85a31d7675e090ea1c850529962bdfd
- f969874b93e7cd1fc2b14a750e4cc8fc778f70e9991a3109ace4e188d568442a
- fbeed70655a2eaf30ca878e1ddf4985a99a767a014adcd00a2150cc270315fe7
- fcc6f903c83a63e8579d1db1940d23294a13a288960d9d07052d978dff9b9e8c
- fe592fb50f84f5a8f10fd14a2a01a0c167a11c1c2242196e2b626a581ca5ac28
- ff198bf3509d1ff43c5529fdd16b160505117bec958363e7e385b4ca1bb4dc73

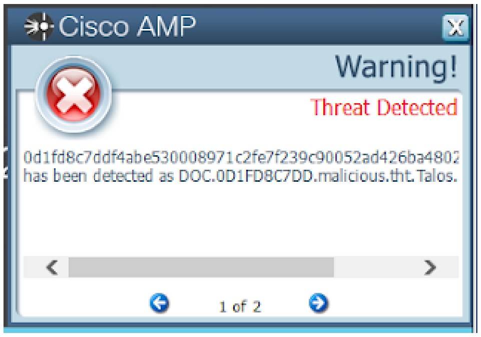
## Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | N/A |
| Email Security | N/A |
| Network Security | N/A |
| Threat Grid | ✔ |
| Umbrella | N/A |
| WSA | N/A |

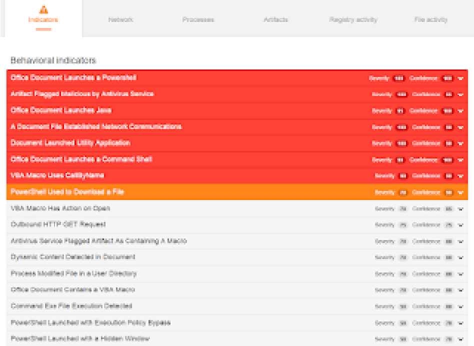
### Screenshots of Detection

#### AMP



0d1fd8c7ddf4abe530008971c2fe7f239c90052ad426ba4802
has been detected as DOC.0D1FD8C7DD.malicious.tht.Talos.

#### ThreatGrid



Behavioral indicators

| | | |
|---|---|---|
| Office Document Launches a Powershell | Severity [illegible] | Confidence [illegible] |
| Artifact Flagged Malicious by Antivirus Service | Severity [illegible] | Confidence [illegible] |
| Office Document Launches Java | Severity [illegible] | Confidence [illegible] |
| A Document File Established Network Communications | Severity [illegible] | Confidence [illegible] |
| Document Launched Utility Application | Severity [illegible] | Confidence [illegible] |
| Office Document Launches a Command Shell | Severity [illegible] | Confidence [illegible] |
| VBA Macro Uses CallByName | Severity [illegible] | Confidence [illegible] |
| PowerShell Used to Download a File | Severity [illegible] | Confidence [illegible] |
| VBA Macro Has Action on Open | Severity [illegible] | Confidence [illegible] |
| Outbound HTTP GET Request | Severity [illegible] | Confidence [illegible] |
| Antivirus Service Flagged Artifact As Containing A Macro | Severity [illegible] | Confidence [illegible] |
| Dynamic Content Detected in Document | Severity [illegible] | Confidence [illegible] |
| Process Modified File in a User Directory | Severity [illegible] | Confidence [illegible] |
| Office Document Contains a VBA Macro | Severity [illegible] | Confidence [illegible] |
| Command Exe File Execution Detected | Severity [illegible] | Confidence [illegible] |
| PowerShell Launched with Execution Policy Bypass | Severity [illegible] | Confidence [illegible] |
| PowerShell Launched with a Hidden Window | Severity [illegible] | Confidence [illegible] |

## Win.Trojan.VBCryptLaser

### Indicators of Compromise

#### Registry Keys

- **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\DisableOSUpgrade**
  This key is created and set to 1. In this way, the malware prevents any OS upgrade
- **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\OSUpgrade\ReservationsAllowed**
  Key necessary to disable any OS update. It is set to 0.
- **HKEY_USERS\Software\[a-z]{8}\[a-z]{10}**
  This registry key contains an encrypted copy of the malware binary.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
  The persistance method invokes at every login Javascript code.

#### Mutexes

N/A

**IP Addresses**

- 185.117.72.90
- 12.190.56.53
- 104.193.109.67
- 133.28.94.49
- 19.131.186.114
- 109.152.13.49
- 46.248.138.70
- 36.150.95.154
- 151.126.133.167
- 49.117.103.250
- 145.85.32.96
- 244.159.110.110
- 8.19.53.244
- 218.255.128.133
- 110.200.102.30
- 161.133.250.103
- 216.115.112.112
- 93.10.53.55
- 214.28.222.43
- 194.59.147.179
- 206.213.193.26
- 140.192.50.4
- 170.54.3.5
- 202.161.197.181
- 3.166.202.197
- 187.23.153.218
- 69.81.37.149
- 138.142.156.77
- 97.207.252.167
- 153.74.137.236
- 32.144.23.231
- 203.4.193.199
- 193.212.108.131
- 27.32.23.117
- 116.67.48.94
- 236.43.120.190
- 248.100.151.74
- 140.178.134.108
- 71.40.250.251
- 2.170.194.13
- 188.121.121.90
- 103.182.107.224
- 238.44.206.248
- 185.196.78.227
- 241.117.137.46
- 27.184.52.156
- 17.100.187.246
- 142.159.223.136
- 53.154.160.76
- 74.112.68.147
- 150.158.250.75
- 153.11.186.249
- 83.172.78.89
- 89.50.100.129
- 252.84.7.113
- 112.84.131.231
- 156.116.8.163

- 109.137.79.244

**Domain Names**

- puresourcecollective[.]com
- appollobafh[.]com

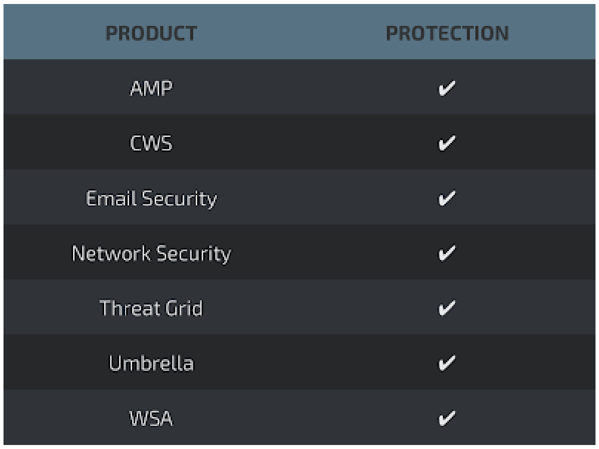
**Files and or directories created**

N/A

**File Hashes**

- 2acfab58519552eaed08a1a40cf92368e28b3a665b7d6851b47e38f2bd8f598e
- 3e2f71a4dd6bc8e866325ccee3d780b029532e83d5aef69825d1a583205a6f4c
- 455f53b882d1648694d8b8cbcc625c2ee2a5f7400f0db70bd7385284304751f4
- 56ded612854f90cf5ba70daba78308a9e46198444ea3b63b0c2707c6776a1b4d
- 58f3fd45631a08818d44c8c7f555f46d2817d4ef804a8faf80c47faa388e436f
- 68f3ed6d61556fd899e95d2b5b43a266cd23fb763b6e1f02dff2e2d62a27a41f
- 6a9b132e407edec1c06ebec33a47ff0a1f44968679f88c2584c380d033b748e3
- c2bacb6a9ddf8eca886f083c9f52d8979cfd29b3f0b97fbb0c76ca86373562a8
- Faa87134b84133b85c42cb1997c96b04021b2848369599e555b100981fbc7cad

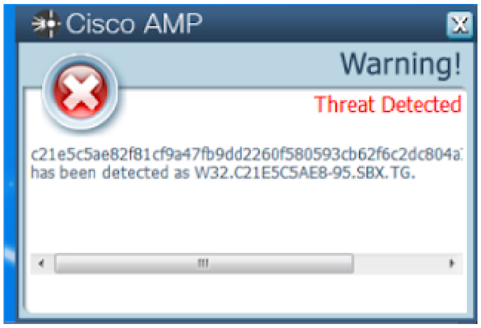
## Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✓ |
| CWS | ✓ |
| Email Security | ✓ |
| Network Security | ✓ |
| Threat Grid | ✓ |
| Umbrella | ✓ |
| WSA | ✓ |

## Screenshots of Detection

### AMP

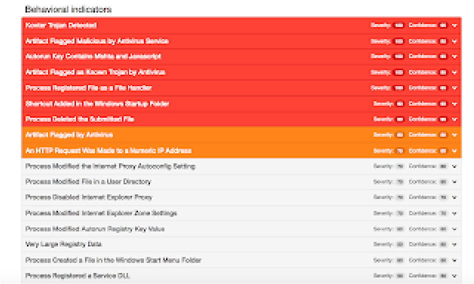


Warning!

Threat Detected

c21e5c5ae82f81cf9a47fb9dd2260f580593cb62f6c2dc804a
has been detected as W32.C21E5C5AE8-95.SBX.TG.

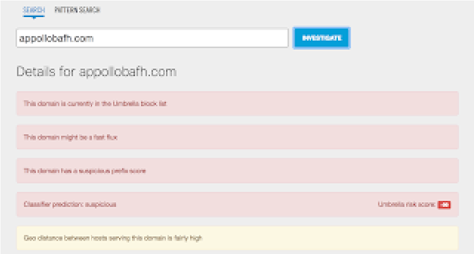
### ThreatGrid



Behavioral indicators

- Kovter Trojan Detected
- Artifact Flagged Malicious by Antivirus Service
- Autorun Key Contains Mshta and Javascript
- Artifact Flagged as Known Trojan by Antivirus
- Process Registered File as a File Handler
- Shortcut Added in the Windows Startup Folder
- Process Deleted the Submitted File
- Artifact Flagged by Antivirus
- An HTTP Request Was Made to a Numeric IP Address
- Process Modified the Internet Proxy Autoconfig Setting
- Process Modified File in a User Directory
- Process Disabled Internet Explorer Proxy
- Process Modified Internet Explorer Zone Settings
- Process Modified Autorun Registry Key Value
- Very Large Registry Data
- Process Created a File in the Windows Start Menu Folder
- Process Registered a Service DLL

## Umbrella



appollobafh.com

Details for appollobafh.com

This domain is currently in the Umbrella block list

This domain might be a fast flux

This domain has a suspicious prefix score

Classifier prediction: suspicious — Umbrella risk score: [illegible]

Geo distance between hosts serving this domain is fairly high

---

## Win.Virus.Virut-6171773

### Indicators of Compromise

**Registry Keys**

N/A

**Mutexes**

N/A

**IP Addresses**

N/A

**Domain Names**

- jl[.]chura[.]pl
- sys[.]zief[.]pl

**Files and or directories created**

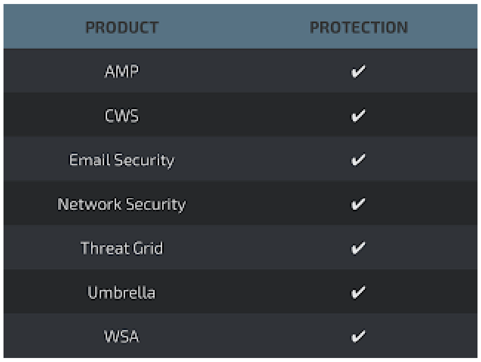
Modify host files

**File Hashes**

- a477f53caa2a04835db7e3e02238fd90b92930738e6d512543bb4b6114b28d81
- ef1070106dbad598487ddd22a8fe7d40d8cc30a49e8c48d19ea02c76497a062c
- 7075a7fb70a46dc02460abc92b890b6e9f43ab20e4d47d16435dc133c218cd42
- 128debd4fa18c3ad5ff49925ea3d8a3ccd013e82950cde429b09e8d58878f27c
- 1319090b4d1d8b9815005585ee3fa15ac1df4f2eca0e22e22bc317e52a520c4e
- bd92f8a83f0fbebc76749c41916fa212b75b386386c25e1203f53657adf07aac
- 6d71a5594dc5adc2bab1fd2ead630a705c7c0e02e2a5a20994584a1fb1effa4f
- ba9cdbb4b0f43daa78bd8cb9cc4f842fb970bdbf0ed012760a55e2df34778232
- fbb151befa1d287d49870fa9fc6254036452c4ca3e80da7bb19d529a8a4382ea
- 6f1cebb94490adcd133bba22a6ba9aafce96d84c76dc4007bbe5ff0c83431462
- 1f6984b9f0dc7009a91577b3868d8980c5ee47a161559f56878e5e80424e01a7
- a2d5c82fe41f613c159d6952c9ff3aa2a1b059ce4692e20292ba2e01effb2e9e
- 62796ad8ede80f59beb4f4b40d68cc4e5477cecd10f2b7993d25cdeac9535bd0
- 1c752622d01064f0adf1962e1d5671cff249be495bea9bbaf200fdfd2124f9b2
- db97b4f3aa56a8111d007c2581379d827e97994843d0d7b4d461ba151db52988
- b0b0ae2afa85dac9f3d289059a06cde24e33308dae64f11fa3ee68a93f8a6b67

- 6e27d1b6622efc68e98acc87e9356a78af7d942e0cba0d3aa97809cecec6bdf9
- 2a0ea00ae1634818d3d84d699a54ad9cb28c71dddf24b0340c9a6b1449d2d966
- 348713e66c6ddc09dbcf95ca50cfe384987031fc787249fa14d10aacdb3b7e1c
- d754e1fac2ae13b1cbc6d7beec8f37c1f304a52120e6e6878b06d8183f659c17
- 0e653eb48d3718b3abd3459386795a3802bde8aad920a33cc2d8d632138b0a61
- 8e431f2bf003132434c5fca097c60240fee7f1e9ca30bc7a063dabcd7d902841
- 683192a27d4316eb1073522de5fb3fa1e3923b5e7d6cdb979d4bd82ed317fa47
- 8f0058f2fa085a4cf8ee5dc01250aa18dd624187d527b5521438cfcda2a4fbe4
- b89927a14e2e54b2bd917904b38737ce96f3bc004215c5a0486fc0a96a6c47d5
- ebf6f32cf12e0839338564a6edef3d8ec8b7ebd1d93bc09c3359a69a4803460d
- 68ef4a3024eeadab44169cb292f897e66e57342dd65c9b63fda5fad6cb517e53

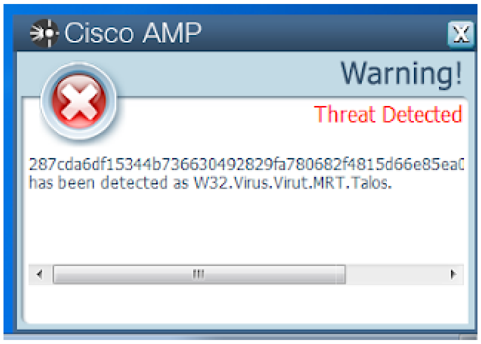
## Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | ✔ |
| Threat Grid | ✔ |
| Umbrella | ✔ |
| WSA | ✔ |

## Screenshots of Detection

### AMP

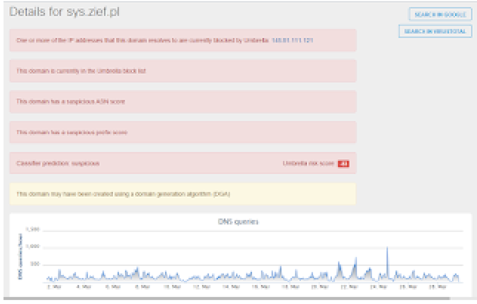


Warning!

Threat Detected

287cda6df15344b736630492829fa780682f4815d66e85ea
has been detected as W32.Virus.Virut.MRT.Talos.

### Umbrella



Details for sys.zief.pl

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 148.81.111.121

This domain is currently in the Umbrella block list

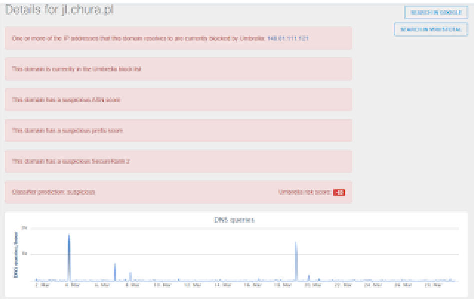
This domain has a suspicious ASN score

This domain has a suspicious profile score

Classifier prediction: suspicious

Umbrella risk score [illegible]

This domain may have been created using a domain generation algorithm (DGA)



Details for jl.chura.pl

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 148.81.111.121

This domain is currently in the Umbrella block list

This domain has a suspicious ASN score

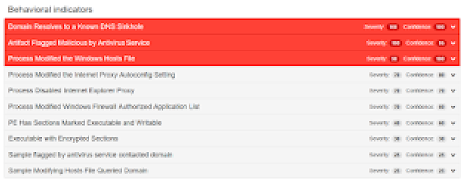
This domain has a suspicious prefix score

This domain has a suspicious SecureRank 2

Classifier prediction: suspicious

Umbrella risk score: 40

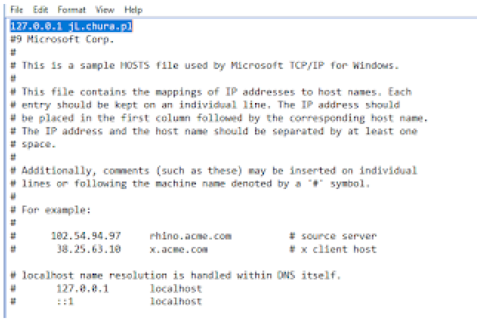
## ThreatGrid



Behavioral indicators

| | | |
|---|---|---|
| Domain Resolves to a Known DNS Sinkhole | Severity: 100 | Confidence: 100 |
| Artifact Flagged Malicious by Antivirus Service | Severity: 100 | Confidence: 95 |
| Process Modified the Windows Hosts File | Severity: 80 | Confidence: 100 |
| Process Modified the Internet Proxy Autoconfig Setting | Severity: 75 | Confidence: 80 |
| Process Disabled Internet Explorer Proxy | Severity: 75 | Confidence: 75 |
| Process Modified Windows Firewall Authorized Application List | Severity: 75 | Confidence: 80 |
| PE Has Sections Marked Executable and Writable | Severity: 40 | Confidence: 60 |
| Executable with Encrypted Sections | Severity: 30 | Confidence: 30 |
| Sample flagged by antivirus service contacted domain | Severity: 25 | Confidence: 25 |
| Sample Modifying Hosts File Queried Domain | Severity: 25 | Confidence: 25 |

## Malware Screenshot



```
127.0.0.1 jl.chura.pl
#9 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

---

---

## Win.Ransomware.Spora-6172235

### Indicators of Compromise

### Registry Keys

N/A

### Mutexes

\Sessions\1\BaseNamedObjects\m[0-9]{9}

### IP Addresses

N/A

### Domain Names

N/A

### Files and or directories created

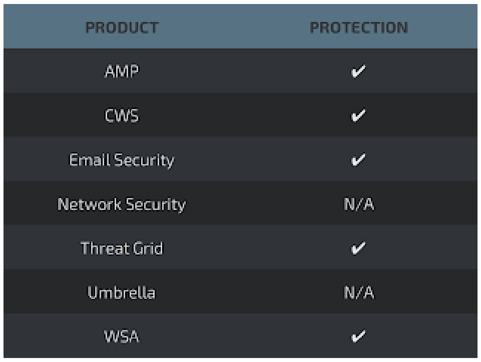
%APPDATA%\[A-Z0-9]{5}-[A-Z0-9]{5}-[A-Z]{5}-[A-Z]{5}-[A-Z]{5}.html

### File Hashes

- f8bf2eb6481164e4a8cae0dc1114044a9ba81d41350edd1be19021e2cbdab749
- 5e7a7f4ef9ba326e3650c4ee58bdfafb3661fa50f680d78d5868240120c553be
- b64639ae67147ff584507627713db60baf8050cedb9a7e4d3b68b521ca54ad36
- e849051316cc2cf869f80f66cd2b48b436d51cc7544bad3309774aebf101c889
- 81cc065fc899b98f774708d8176ad4319311ff8643138705b24fbeb439f6e0d0
- 6c191a684907ec323516c837f66cd7331acbdad65220b73dba9307dffaa284f9

- 8a8ebf400b190a6fabf6d0e5f6756dfd1d856395161e522a7efe43342531894e
- ec31d44d1c2eae34897001c41e14ed26c03d8acaabf00ee31183021f7a2fd141
- e1a3784ef065cea4a8c8402015028494c18e3cd235cbb13785d269452376b2f1
- 9232ac662ebf2460bc2eb68875b548eb2547f62c5f7799861cfc0bebf5bf1e53
- 23a91bb1cf1019f1b6aabfc249df42b57a76d78d09a33b39441206d62f416fc8
- b3b489585e8d6714ac05b79ae3e01cf3c93e51ebb5d16ccec2a6afcf4eb4c325
- c0f7e40dd057ab32aaecad7df71b22433ef7474a57e5a2e58ec7fd613dfc30b5
- a25bafcf74304d56beeb5395a0f801a743e27381ca95626f4720a48c966e3129
- 66449dde7d12706fb9ab6aafd690e077f5f37f11aa8b372a95d9e962763c7bc1
- e1f992137562f1cfe5d38f57f36ffac76dda729e102b6abaedda89970ba8c493
- 6072804f727f1f237b4fcdeec9428449311d3cc54d9e0d284a68d300f3c858f6
- 2432fad4d84816155ea80075d686896de32304c8f453c01b029ad21e7eb17b13
- 9c93758e4b5767edaebb8bb39e0b7566715e2b610d2117bc6e1acf2578c973f5
- 67342ca4bada435d4e8d03d65342434f70909f54d4951412e18c49aeb72dcf47
- 346cf5120e5d1512f879d14111254ba68e3eaa3d3ea6f02977cd835725521984
- 288384c983496978fdda879847525e26194761394d62febeb922284cbeba0c9d
- 722b92a1f10fd2cac878ab7f9e3a120d656a245e40cc13a0bc619eb63362768d
- 5a011ceb0bf539ac5cc7e89b85dd7b742d94093fe84153d647fa18f16e7cac06
- 0304ce1dbaf1cf933f7d63dc559101b5899af7e07fef52abc38de430a428fce2
- 1f63371f2b2a5f340ea3c4d211b1fe0d6197e3a00e87cae49e873ae8964e8810

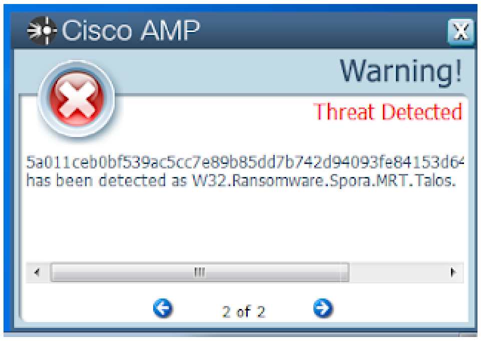
### Coverage



| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CWS | ✔ |
| Email Security | ✔ |
| Network Security | N/A |
| Threat Grid | ✔ |
| Umbrella | N/A |
| WSA | ✔ |

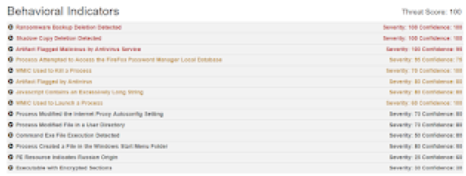
### Screenshots of Detection

### AMP



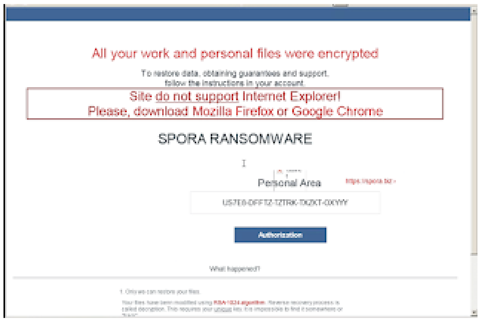
5a011ceb0bf539ac5cc7e89b85dd7b742d94093fe84153d64
has been detected as W32.Ransomware.Spora.MRT.Talos.

### ThreatGrid



| Behavioral Indicators | Threat Score: 100 |
|---|---|
| Ransomware Backup Deletion Detected | Severity: 100 Confidence: 100 |
| Shadow Copy Deletion Detected | Severity: 100 Confidence: 100 |
| Artifact Flagged Malicious by Antivirus Service | Severity: 100 Confidence: 80 |
| Process Attempted to Access the FireFox Password Manager Local Database | Severity: 95 Confidence: 75 |
| WMIC Used to Kill a Process | Severity: 70 Confidence: 100 |
| Artifact Flagged by Antivirus | Severity: 60 Confidence: 60 |
| Javascript Contains an Excessively Long String | Severity: 60 Confidence: 60 |
| WMIC Used to Launch a Process | Severity: 60 Confidence: 100 |
| Process Modified the Internet Proxy Autoconfig Setting | Severity: 70 Confidence: 80 |
| Process Modified File in a User Directory | Severity: 70 Confidence: 60 |
| Command Exe File Execution Detected | Severity: 50 Confidence: 80 |
| Process Created a File in the Windows Start Menu Folder | Severity: 60 Confidence: 80 |
| PE Resource Indicates Russian Origin | Severity: 25 Confidence: 60 |
| Executable with Encrypted Sections | Severity: 30 Confidence: 30 |

### Malware Screenshot



All your work and personal files were encrypted

To restore data, obtaining guarantees and support,
follow the instructions in your account.

Site do not support Internet Explorer!
Please, download Mozilla Firefox or Google Chrome

SPORA RANSOMWARE

Personal Area

https://spora.biz ›

US7E6-DFFTZ-TZTRK-TXZKT-OXYYY

What happened?

1. Only we can restore your files.

Your files have been modified using RSA-1024 algorithm. Reverse recovery process is called decryption. This requires your unique key. It is impossible to find it somewhere or "hack"