Threat Analysis Report

Summary

Threat Level	Malicious
URL	http://lifescience.sysu.edu.cn/filees/guuu16pesche.asp
MD5 Hash Identifier	5573641A9E543C104E9D58FD6AFA141D
File Type	application/url
URL Submitted	2015-07-22 15:54:21
Duration	39 seconds
Sandbox Replication	25 seconds
Screenshots	2

Engine Analysis

Engine	Threat Name	Severity
GTI File Reputation	---	Unverified
Gateway Anti-Malware	---	Unverified
Anti-Malware	---	Unverified
YARA		
Custom Rules		Unverified
Sandbox	Malware.Dynamic	Very High
Final		Very High

Sample is malicious: final severity level 5

Behavior Classification

Networking	Very High
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	Informational
Spreading	Informational
Hiding, Camouflage, Stealthiness, Detection and Removal Protection	Informational
Exploiting, Shellcode	Unverified
Persistence, Installation Boot Survival	Unverified
Data spying, Sniffing, Keylogging, Ebanking Fraud	Unverified

Dynamic Analysis

Action	Severity
ATTENTION: connection made to a malicious website (see Web/URL reputation for details)	Very High
Cracks a URL into its component parts	Informational
Read data from a handle opened on previous URL's request	Informational
Set a filter function to supersede the top-level exception handler (http://msdn.microsoft.com/en-us/library/vstudio/x85tt0dd.aspx)	Informational
Downloaded data from a webserver	Unverified
Connected to a specific service provider	Unverified

GTI Web/URL Reputation

Connected Sites: 3

URL	Port	Reputation	Category Name	Risk Group	Functional Group
LIFESCIENCE.SYSU.EDU.CN	**80**	**Minimal Risk**	**Entertainment**	**Productivity**	**Entertainment/Culture**
LIFESCIENCE.SYSU.EDU.CN/FILEES/GUUU16PESCHE.ASP	**80**	**High Risk**	**Malicious Sites**	**Security**	**Risk/Fraud/Crime**
WWW.RELATIETHERAPIE-RIJSWIJK.COM	**80**	**Minimal Risk**	**Blogs/Wiki**	**Productivity**	**Information/Communication**

Processes Analyzed

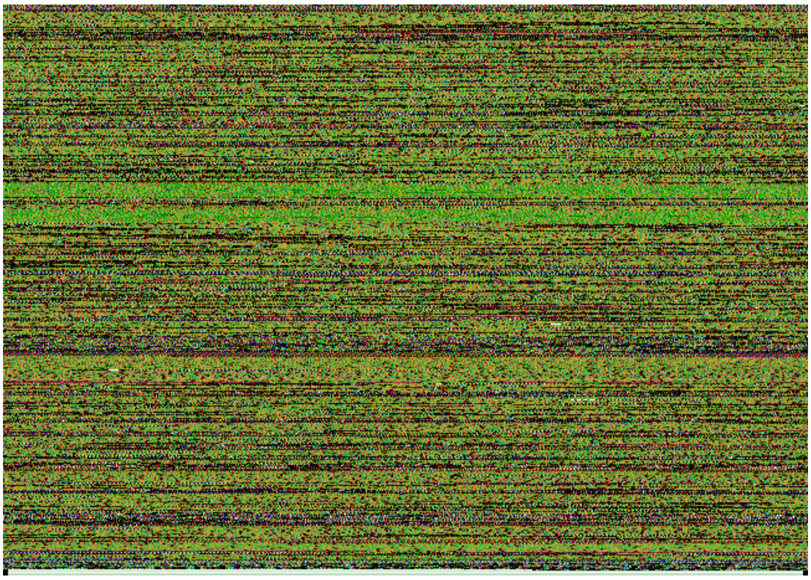
Name	Reason	Severity
http://lifescience.sysu.edu.cn/filees/guuu16pesche.asp	loaded by MATD Analyzer	Very High

Screenshots

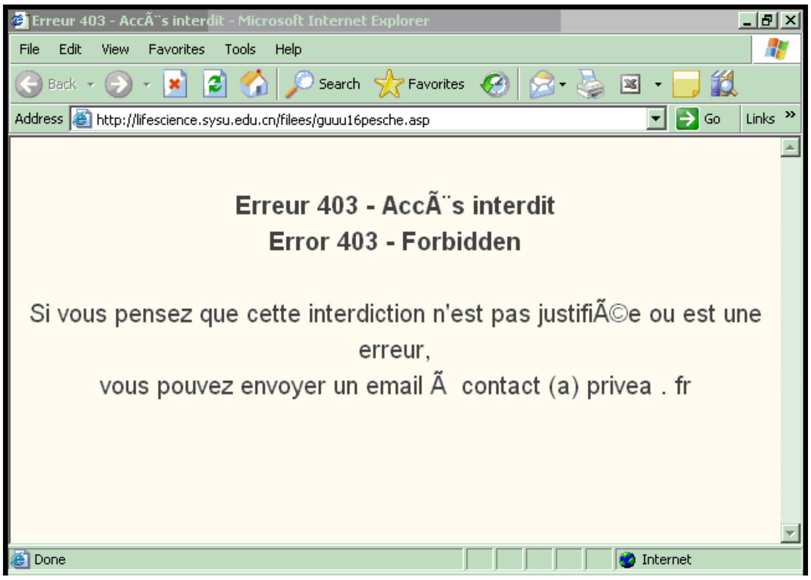
Note: a pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample

Images: 2

1ab036.jpg



1a8d2e.jpg



Erreur 403 - AccÃ¨s interdit - Microsoft Internet Explorer

http://lifescience.sysu.edu.cn/filees/guuu16pesche.asp

Erreur 403 - AccÃ¨s interdit
Error 403 - Forbidden

Si vous pensez que cette interdiction n'est pas justifiÃ©e ou est une erreur,
vous pouvez envoyer un email Ã contact (a) privea . fr

---

http://lifescience.sysu.edu.cn/filees/guuu16pesche.asp

Run-Time Dlls: 2

kernel32.dll

ws2_32.dll

File Operations: 3

Files Opened

File Name	Access Mode	File Attributes
C:\notexist.htm	**Read**	**Normal**

Files Read

Reads data from a handle opened by the InternetOpenUrl, FtpOpenFile, or HttpOpenRequest function

Other

Retrieved the full path for the module

Registry Operations: 9

Registry Opened

HKCR\.htm

HKCR\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Old Icon\htmlfile

HKCR\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Old Icon\htmlfile\DefaultIcon

HKCR\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Old Icon\htmlfile\ShellEx\IconHandler

HKLM\SOFTWARE\Microsoft\Windows Script\Features

HKLM\Software\Microsoft\COM3

Registry Read

HKCR\.htm

HKCR\CLSID\{42042206-2D85-11D3-8CFF-005004838597}\Old Icon\htmlfile\DefaultIcon

HKLM\Software\Microsoft\COM3 COM+Enabled

▶ Process Operations: 18

Process Created

Process Name	Module
{00000323-0000-0000-C000-000000000046}	
{0000032A-0000-0000-C000-000000000046}	
{00021401-0000-0000-C000-000000000046}	
{18DF081C-E8AD-4283-A596-FA578C2EBDC3}	
{42042206-2D85-11D3-8CFF-005004838597}	
{42AEDC87-2188-41FD-B9A3-0C966FEABEC1}	
{5B4DAE26-B807-11D0-9815-00C04FD91972}	
{6C736DB1-BD94-11D0-8A23-00AA00B58E10}	
{750FDF0E-2A26-11D1-A3EA-080036587F03}	
{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}	
{7B8A2D95-0AC9-11D1-896C-00C04FB6BFC4}	
{7EB5FBE4-2100-49E6-8593-17E130122F91}	
{871C5380-42A0-1069-A2EA-08002B30309D}	
{9BA05972-F6A8-11CF-A442-00A0C90A8F39}	
{A5E46E3A-8849-11D1-9D8C-00C04FC99D61}	
{DBC80044-A445-435B-BC74-9C25C1C588A9}	
{FF393560-C2A7-11CF-BFF4-444553540000}	

Other

Enabled an application to supersede the top-level exception handler

▶ Network Operations: 17

DNS Queries

Converted a long value from TCP/IP network order to host byte order

Socket Activities

Obtained the local name (address) for a socket

Other

Cracked the URL into its component parts: HTTP://LIFESCIENCE.SYSU.EDU.CN/FILEES/GUUU16PESCHE.ASP

Enumerated IE Cache to f4 identifier

Headers: accept-language: en-us, HeaderLength: ffffffff, Optional: , OptionalLength: 0

Headers: referer: http://lifescience.sysu.edu.cn/filees/guuu16pesche.asp, HeaderLength: ffffffff, Optional: , OptionalLength: 0

Initialized the WinINet functions, Agent name: mozilla/4.0 (compatible; msie 6.0; windows nt 5.1; sv1), Access type: PRECONFIG Flags: ASYNC

Opened a HTTP or FTP session for a given site: LIFESCIENCE.SYSU.EDU.CN

Opened a HTTP or FTP session for a given site: WWW.RELATIETHERAPIE-RIJSWIJK.COM

Retrieved header information associated with the HTTP request

Set an Internet option: 3a

Set an Internet option: 3c

Set an Internet option: 3e

Set an Internet option: 44

Set an Internet option: 56

Verb: get, ObjectName: /1127/ugg-fr.js, Version: , Referer: , Flags: 400000, Context: 1aec30

Verb: get, ObjectName: /filees/guuu16pesche.asp, Version: , Referer: , Flags: 400000, Context: 17f830

▶ Other Operations: 1

Others

Retrieved information about a locale specified by a identifier

Analysis Environment

Microsoft Windows XP Professional Service Pack 3 (build 2600, version 5.1.2600)

Internet Explorer version: 6

Microsoft Office version: 2003

PDF Reader version: 9.0

No Flash player installed

No Flash player plugin installed

Platform Version 3.4.8.96.50610

Baitexe activated but not infected