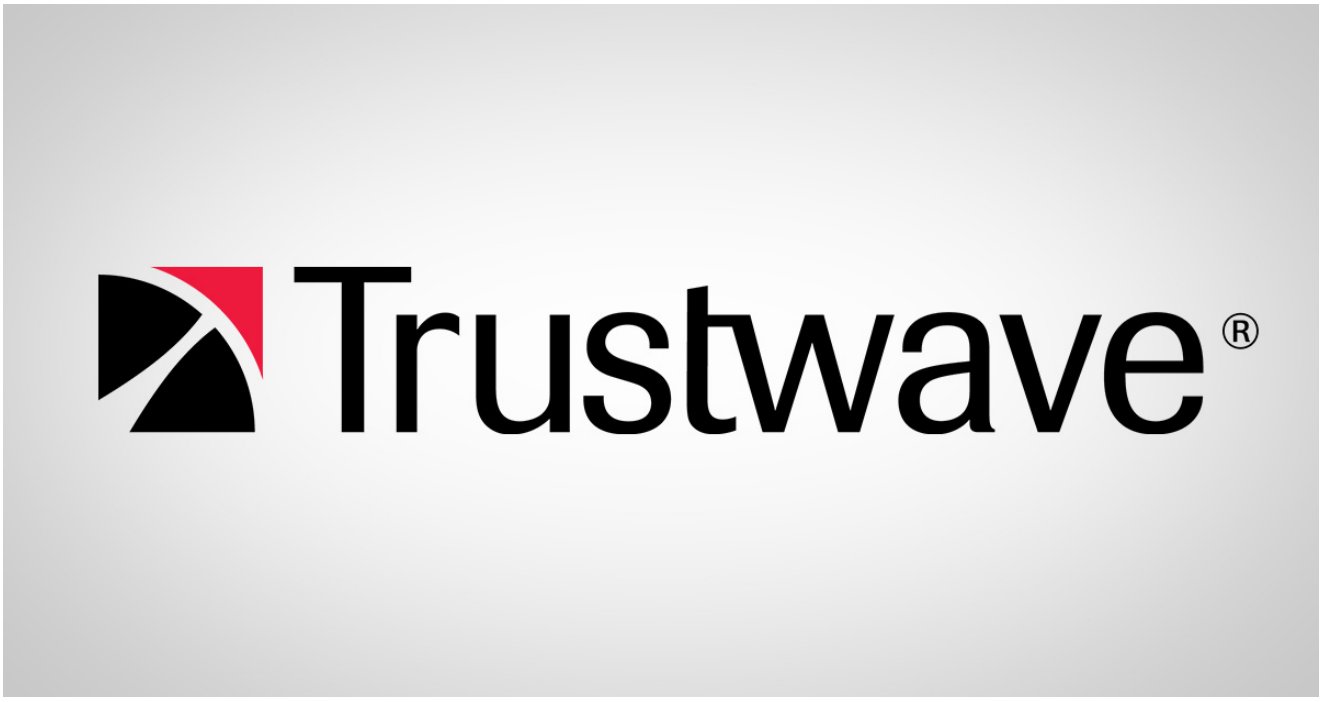
# The Curious Case of the Malicious IIS Module






Recently, we've seen a few instances of a malicious DLL that is installed as an IIS module making its rounds in forensic cases. This module is of particular concern as it is currently undetectable by almost all anti-virus products. The malware is used by attackers to target sensitive information in POST requests, and has mechanisms in place for data exfiltration. Encryption is circumvented as the malware extracts this data from IIS itself. This was seen targeting credit card data on e-commerce sites, however, it could also be used to steal logins, or any other sensitive information sent to a compromised IIS instance. *Please note that this is not related in any way to the recent 'Pony' malware that was reported. Pony targets the end-users, while this malware goes after the web servers themselves.*

One of my YARA rulesets that I created for this family of malware triggered, leading me to the following:

https://www.virustotal.com/en/file/587e784f8c54b49f25c01e0e8f71c205bd422e2b673fb7fbf28d721aa768e055/analysis/

As it turns out, this happens to be the original installer for the IIS module I'm referring to, and it seemed like the perfect time to throw a write-up together. I decided to write this post for a couple of reasons:

1. At the time of writing this post, anti-virus do not currently detect any of the IIS modules dropped by this malware. Even the installer is only picked up by a handful of anti-virus products, and in all cases it's simply generic heuristic detection. I'm using this post as a way of notifying anti-virus vendors so that specific detections for this malware may be written.
2. I think the malware is pretty neat.

So with that, let's talk about this thing. For the sake of my own sanity, I'm going to be referring to this malware as 'ISN' going forward, as this three character string is referenced in all of the malware's exfiltration commands.

Let's take a look at the installer first. The file can take a number of arguments, as you can see below:

- -path : [Location where malware is installed]
- -i : [List of URI paths to be targeted, such as '/sensitive.aspx'
- -u : [Uninstall malware]
- -is632 : [Manually instruct malware that victim is IIS6 32-Bit]
- -is664 : [Manually instruct malware that victim is IIS6 64-Bit]

In truth, the installer is quite simple. It has four embedded DLLs (in the PE resource section) that are dropped depending on the victim. There are IIS modules for the following:

- IIS6 32-Bit
- IIS6 64-Bit
- IIS7+ 32-Bit
- IIS7+ 64-Bit

Additionally, the ISN malware has a VBS file that is also embedded as a PE resource (See the reference section below for full output and VirusTotal link). This VBS file is used to install or remove the DLLs as an IIS module.

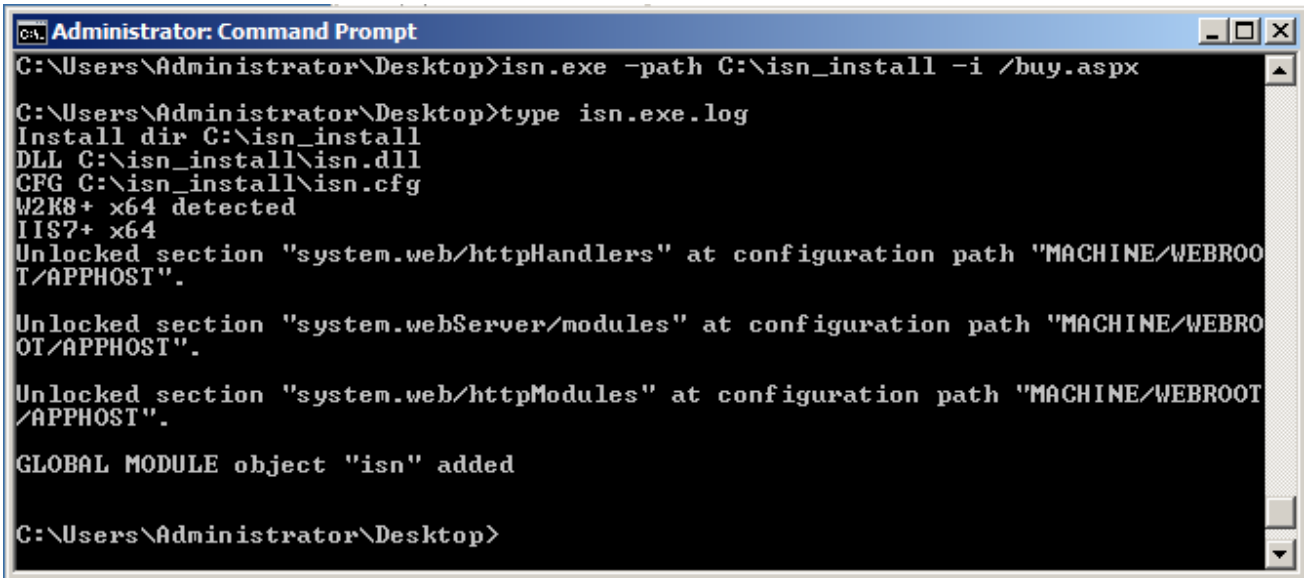
Once run, ISN will perform the following:

1. Drop the VBS file to the location specified by '-path', or the current working directory. This file is removed before the ISN installer is finished.
2. Create a configuration file ([filename].cfg) in the same directory. This file contains a list of
3. URIs that are targeted by the malware.
4. Detect the IIS version as well as the victim architecture.
5. Drop the appropriate DLL to the installation directory.
6. Call the VBS file in order to install the DLL as an IIS module.

The malicious IIS module is installed as whatever the name of the executable is. For my demonstration, I've named the malware 'isn.exe', which results in the following:

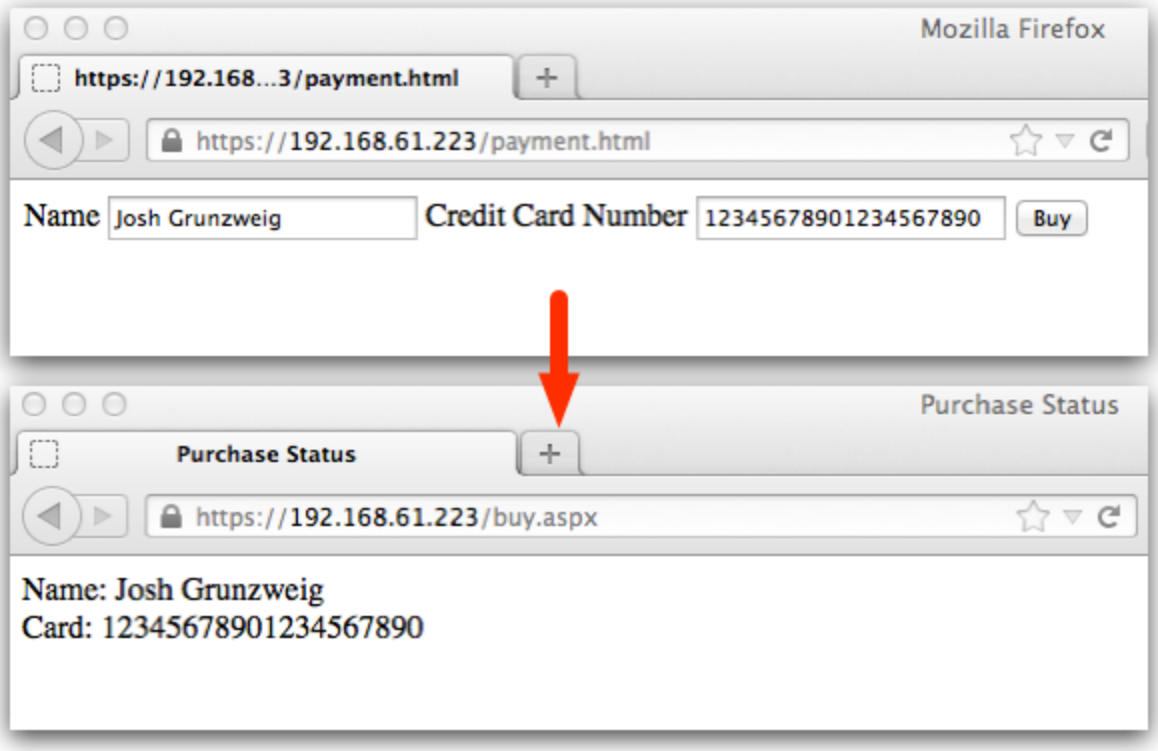
| | | | |
|---|---|---|---|
| HttpLoggingModule | %windir%\System32\inetsrv\log... | Native | Inherited |
| IsapiFilterModule | %windir%\System32\inetsrv\filt... | Native | Inherited |
| IsapiModule | %windir%\System32\inetsrv\isa... | Native | Inherited |
| isn | C:\isn_install\isn.dll | Native | Local |
| OutputCache | System.Web.Caching.OutputCa... | Managed | Inherited |

As the installation process takes place, a log file named '[filename].log' is created and a number of debugging statements are written to it.

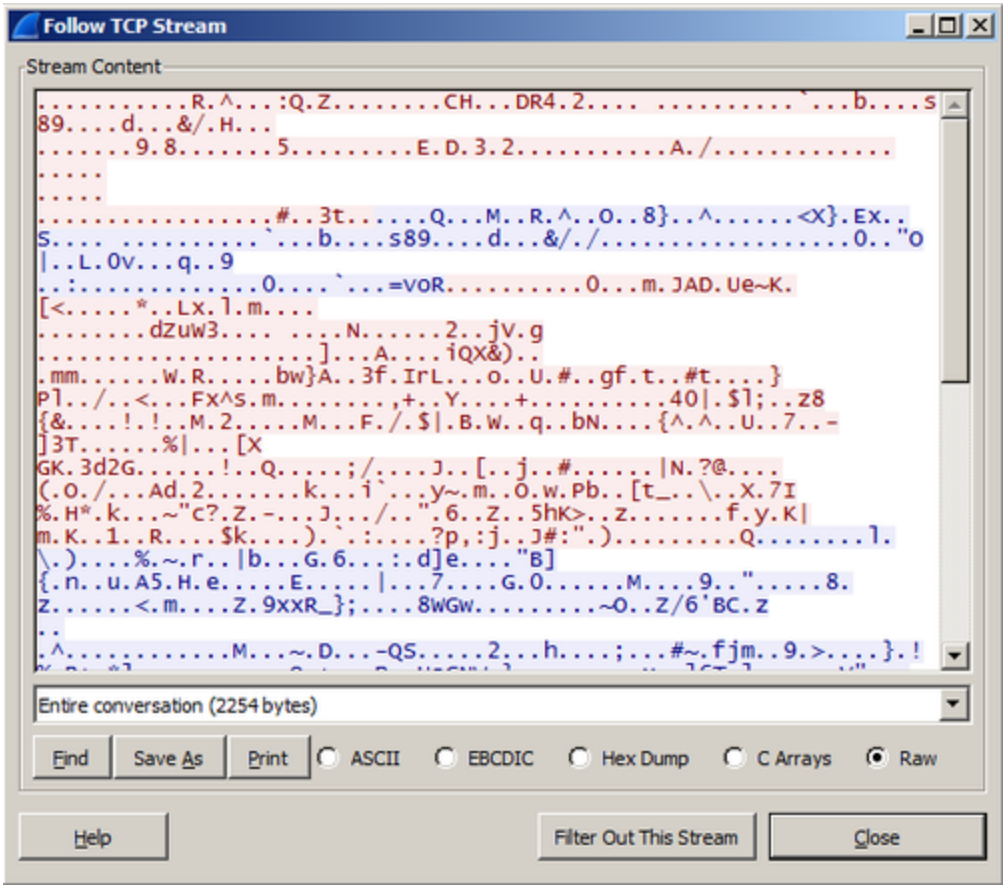



Once the module is successfully installed, it will monitor the URIs specified in the configuration file and dump any POST requests encountered to the '[filename].log' file. The module will also monitor the QUERY_STRING parameter, and can accept a number of commands. I've setup a simple IIS instance to demonstrate how this process takes place.

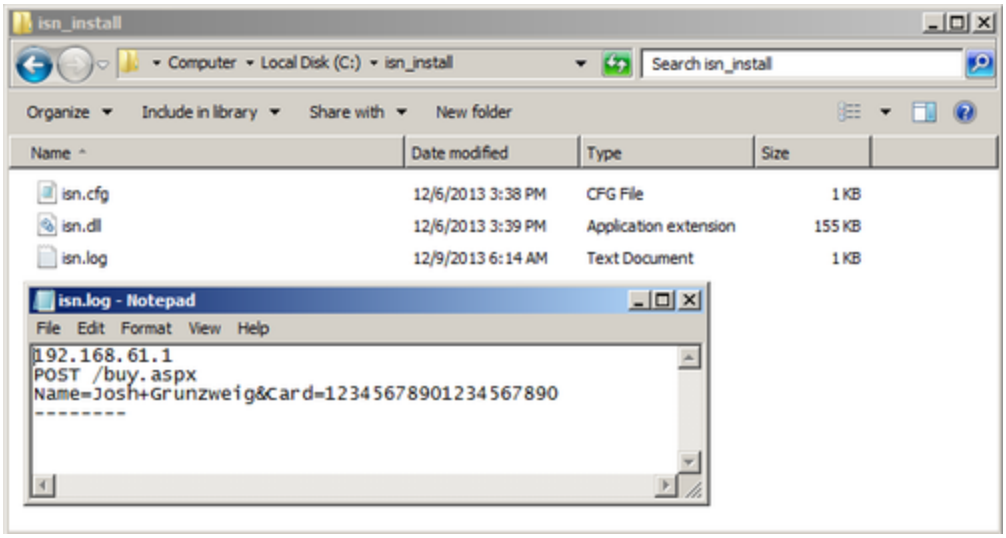
As we can see below, I've created a simple web form that would mimic an actual e-commerce site. A user would enter their name and credit card number and submit the information, which is simply replayed back to them in '/buy.aspx'.




I've also setup a self-signed certificate so that all of the communicate takes place over SSL.



However, this transaction took place on an IIS instance with the ISN malware. The configuration has been set to track POST requests to '/buy.aspx'. As we see below, when this POST request occurs, the ISN malware creates a log file with this information stored in the clear.

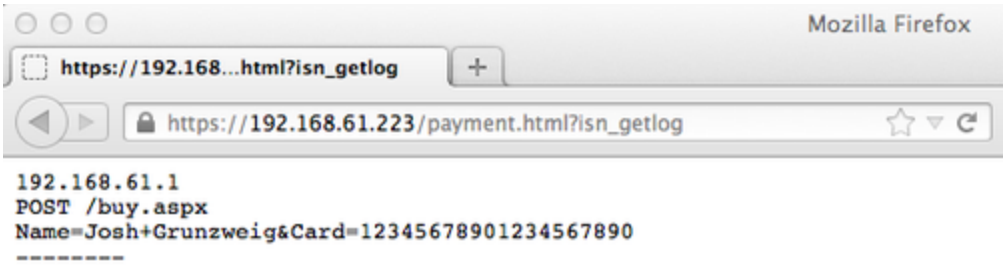



Now, I mentioned earlier that the ISN malware monitors QUERY_STRING parameters. Specifically, it will look for the following commands:

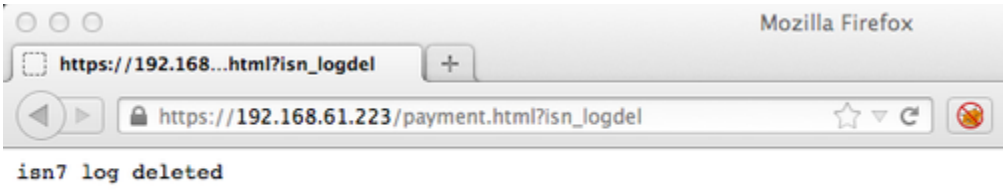
- isn_getlog – return the contents of the isn.log file
- isn_logdel – delete the isn.log file
- isn_logpath – return the path of the isn.log file

These commands can be sent remotely simply by providing them as a GET parameter.

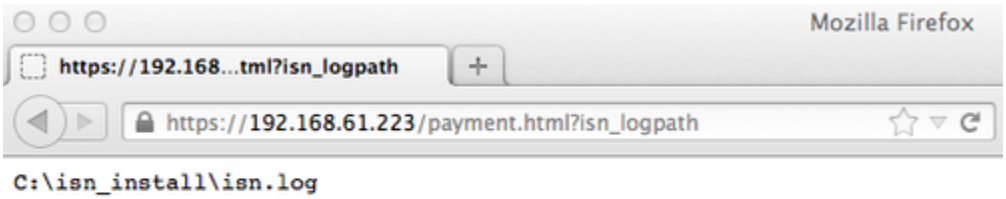
'isn_getlog' example:




'isn_logdel' example:




'isn_logpath' example:




Overall, this malware does not appear to be widely spread and has only been seen in a few forensic case instances. However, the extremely low detection rate in collaboration with the malware's targeted functionality makes this a very real threat.

Trustwave's WebDefend and ModSecurity can be used to both block the initial point of infection for this malware and detect whether sensitive user data such as credit card numbers appear in outbound data.

**Reference**

Installer (9/48) - https://www.virustotal.com/en/file/587e784f8c54b49f25c01e0e8f71c205bd422e2b673fb7fbf28d721aa768e055/analysis/

VBS File (0/49) - https://www.virustotal.com/en/file/688b80289a0c3771c7cee689c50a61b1c5215e8e5ac39a1120b3c7e4f4ada002/analysis/

IIS6 64-Bit (0/49) - https://www.virustotal.com/en/file/956ed56ecc574f68b637e22add7c8e3cb0deea3b1e0dd02abea165bfcb7e3786/analysis/

IIS6 32-Bit (0/47) - https://www.virustotal.com/en/file/9f501c052f2d4f4b0954f6060c7111f272ae29f9d88188d37c961c38e13e3905/analysis/

IIS7+ 64-Bit (0/46) - https://www.virustotal.com/en/file/c6847600910ab196652a38e94ecf592e645d43025d1d61b3710b2f715238307b/analysis/

IIS7+ 32-Bit (0/47) - https://www.virustotal.com/en/file/157174f0b9be66e3c9090c95efdd1dd23b19e42aa671758ebac5540a173f760c/analysis/

Content of VBS File - https://gist.github.com/jgrunzweig/7840987