GRIT BLOG

SUPERNOVA SolarWinds .NET Webshell Analysis

Posted by: GuidePoint Security 6 min read

Published 12/14/20, 9:30am

Introduction

The recently announced supply-chain compromise of SolarWinds and FireEye illustrated many of the thre investigation, with particular focus being placed on the SUNBURST SolarWinds Orion implant, the memory malware dropper, and usage of Cobalt Strike's BEACON module. However, in the IOCs listed by FireEye as .NET webshell named SUPERNOVA was identified with no supplemental analysis as to its method of opera indications of this webshell being present in an environment.

The GuidePoint Security Digital Forensics and Incident Response Practice closely monitors the on-going t emerging state-of-the-practice to ensure that the most up-to-date information and methods are being ut provide to our clients. To that end, this post will describe the SUPERNOVA webshell's operation in-depth, webshell's activity can be detected within your organization.

Overview

The SUPERNOVA webshell is an anonymous code C# webshell written in .NET C# that is specifically written for usage on SolarWinds Orion servers. It is deployed as a DLL module that masquerades as a SolarWinds web service that returns the current logo image for display by the SolarWinds Orion application. In normal operation, this webshell performs the operation of returning the appropriate logo image as requested by other elements of the Orion application, requiring a specific set of parameters to be present in the HTTP GET Request for any of the malicious code to execute. This allows the webshell to remain undetected until such time as the attackers decide to utilize it.

The parameters required for webshell remote code execution include the C# code intended to be compiled and executed by the .NET C# compiler, the C# class to be called, the method within that class to be executed, and the parameters to pass to the requested method. Upon receiving an HTTP GET Request with the necessary parameters supplied, the webshell will collect the parameters and pass them to an additional C# method added by the attacker which will perform the compilation and memory-resident execution of

commonly used web languages, such as PHP, ASP, or Java. Anonymous code webshells utilizing a compiled code language indicate a significant level of sophistication within the threat group that employs them.

Analysis Detail

SUPERNOVA is implemented as a modification to the existing 'app_web_logoimagehandler.ashx.b6031896.dll' module of the SolarWinds Orion application. The purpose of this module, in it's legitimate form, is to return the logo image configured by the user to various web pages of the SolarWinds Orion web application. This is done through the ProcessRequest() method of the LogoImageHandler class. In legitimate operation, this class only contains the ProcessRequest() and LogoImageHandler() methods, a private static Log object, and public boolean parameter IsReusable. The malicious additions made by the threat actors include:

- An extra try/catch block at the beginning of the ProcessRequest() method
- An extra method called DynamicRun()

Now, to discuss each of these in detail, beginning with the ProcessRequest() try/catch block.

ProcessRequest() Try/Catch Block

As the ProcessRequest() method is the primary driver method that parses the incoming HTTP Request, this was the most appropriate place for the attacker to implement code to parse and handle the webshell parameters passed to SUPERNOVA. As such, the attacker's implemented their argument-handling code in a try/catch block at the very beginning of the ProcessRequest() method. This code block is shown below:

Figure 2: Attacker-Implemented Argument-Handling Try/Catch Block

The attacker-implemented try/catch block can be broken down into two primary segments, one concerni
another concerning the webshell output. The first are the parameter instantiations, in which the code de
parameters exist in the HTTP Request, and if they do, then extract the values of those parameters to stri
parameter names. The four attacker parameters, and their purposes, are as follows:

- "codes": Stores anonymous C# code to be compiled and executed by the webshell
- "clazz": Stores the .NET C# class name that the attacker wants to instantiate as part of this executic
- "method": The specific method to be executed within the requested .NET C# class being instantiated by the "clazz" parameter
- "args": A newline-delimeted list of arguments to pass to the executing method requested by the "method" parameter

The second segment is comprised of the last two lines of the try{} block, which involves setting values within the Response object of the HttpContext 'context' object. As this Response object is the data that will be sent back to the attacker in the HTTP Response, this serves as the output mechanism for this webshell. The first instruction sets the HTTP Response Content-Type Header Value to 'text/plain', indicating that the HTTP Response body will consist of plain-text content; this is commonly observed webshell operation.

```
context.get_Response().set_ContentType("text/plain")
```

Figure 2: Setting of the HTTP Response Content-Type Header

Since the second instruction both executes and outputs the result to the Response object, the try{} block completes and the result is returned to the attacker.

Next, we discuss the attacker-implemented DynamicRun() method.

DynamicRun() Method

The DynamicRun() method added by the attacker is where the actual compilation and execution of the requested class and method take place.

Figure 4: DynamicRun() Attacker-Implemented Method

The majority of instructions in this method are just setup code for compilation of the requested class and method into something that can be executed in memory. However, some instructions stand out as significant or explanatory. First items of interest are instructions seven and eight.

```
7 val.set_GenerateExecutable(false);
8 val.set_GenerateInMemory(true);
```

Figure 5: Instructions Setting Memory-Resident Compiled Code Execution Only

Instruction seven tells the compiler not to create an executable on disk to load for execution of the comp
instruction eight telling the compiler to generate the compiled module within memory only. These two ins
that any requested compiled modules will not leave filesystem evidence for incident response analysts t
and methods were executed by the attacker using this webshell.


```
9 CompilerResults val2 = obj.CompileAssemblyFromSource(
   (CompilerParameters)(object)val, codes
);
```

Figure 6: Passing of Anonymous C# Code in "codes" to .NET Compiler and Compilation

Instruction nine passes the C# code contained in the "codes" string object parameter to the compiler, th
by the CompileAssemblyFromSource() method. This creates the memory-resident module for executing,
CompilerResults object.

```
16 object obj2 = val2.get_CompiledAssembly().CreateInstance(clazz);17 return
(string)obj2.GetType().GetMethod(method)!.Invoke(obj2, args);
```

Figure 7: Class Instantiation and Method Execution

Instructions 16 and 17 use the compiled module and instantiate its contained class referenced in the "clazz" parameter, then invokes the target method referenced in the "method" parameter with the attacker-supplied arguments referenced in the "args" parameter. The result of this method execution is stored in the return value of the method, and the DynamicRun() method terminates. The return value is the value that is used by the Write() method of the Response object that was discussed previously.

Detection

we would want to implement a ruleset or query that would key in on the existence of the four webshell parameters (“codes”, “clazz”, “method”, and “args”) for any inbound HTTP connections to logoimagehandler.ashx. An example of this logic in Lucene-syntax pseudo-query would be as follows:

```
direction:inbound AND
rotocol:http AND
uri.filename:logoimagehandler.ashx AND
uri.param:codes AND
uri.param:clazz AND
uri.param:method AND
uri.param:args
```

Figure 8: Pseudo-Query Logic for SUPERNOVA Webshell Access Identification

For the Response side, we would want to key in on the HTTP Response Content-Type Header value of ‘text/plain’ resulting from a HTTP Request to logoimagehandler.ashx.

```
direction:inbound AND
protocol:http AND
uri.filename:logoimagehandler.ashx AND
http.response.contenttype:text/plain
```

Figure 9: Pseudo-Query Logic for SUPERNOVA Webshell Access Response Identification

Logs

The access logs for the IIS web server hosting the SolarWinds Orion web application would be the best location in the log dataset to identify this activity. Here, we would take a similar approach as in Figure 8, attempting to identify HTTP R logoimagehandler.ashx in which the URI contains the “codes”, “clazz”, “method”, and “args” parameters. similar to the logic shown in Figure 8.

```
uri.filename:logoimagehandler.ashx AND
uri.query contains “codes” AND
uri.query contains “clazz” AND
uri.query contains “method” AND
uri.query contains “args”
```

Figure 10: Pseudo-Query Logic for SUPERNOVA Webshell Access Identification in IIS Logs

Conclusion

While webshells are a common access and persistence mechanism leveraged by attackers, characteristics of this specific webshell reiterate the targeted nature and sophistication of these specific attacks. The SUPERNOVA webshell was developed specifically for use on SolarWinds Orion systems, does not appear to repurpose code from other well-known webshells, contains various functionality to ensure limited identification or detection capabilities, and various other characteristics reemphasizing involvement from a nation-state sponsored actor. GuidePoint recommends utilizing the aforementioned detection capabilities, in combination with other IOC’s that have been released for other components of this threat, to ensure your organization has not been impacted.

Categories: BLOG CYBERSECURITY GRIT BLOG

Share

Related Articles

View All

GRIT BLOG

Analysis of the SolarWinds Supply Chain Attack

Posted by: Tony Cook

Published 12/22/20, 05:53pm

Read More 10 min read

CYBERSECURITY

Cybersecurity Week in Review: 12/7

Posted by: GuidePoint Security

Read More 6 min read

CYBERSECURITY

Quarterly GRIT Ransomware Report — Q3 2024

Posted by: Grayson North

Read More 2 min read

Be Informed + Reduce Risk.

Better protect your organization with our unmatched expertise and proven approach to cybersecurity.

Talk to an Expert

GuidePoint Security LLC
2201 Cooperative Way
Suite 225
Herndon, VA 20171

(877) 889-0132

Management (IAM)

Incident Response & Threat Intelligence

Managed Security Services

Network & Infrastructure Security

(SOC) Services

Staff Augmentation

Vulnerability Management & Penetration Testing

Managed Security

Strategic Security Program Management

Managed Security Services

Subscribe to Blog

Business Email*

I'm not a robot

reCAPTCHA
Privacy - Terms

SUBMIT