Soroush Dalili (@irsdl) Blog

A web application security ninja 🥷, a semicolon enthusiast!

A Dotty Salty Directory: A Secret Place in NTFS for Secret Files!

I was playing with "::$Index_allocation" and ":$I30:$Index_Allocation" in an NTFS partition to make a directory which ends with some dot characters (".") or just includes some dots!

The result was a bit interesting
data can be hidden in as well
malware writers might already
feature!

In order to create a dotty direc
1- Open the Windows Comman
2- Go to a test directory.
3.0- Now, insert the following c

```
md ..::$index_allocation
md ...::$index_allocatior
md ....::$index_allocatio
md irsdl
md irsdl.::$index_allocat
md irsdl..::$index_alloca
```

3.1- You can use "echo test > '
4- Now get a directory list from
5- In order to open each of the

```
cd ...::$index_allocation
```

6- You can create some files ir
7- Now use Windows Explorer to see these directories.

The result in **Windows XP:**
– The double dot ("..") directory is hidden and you cannot see it.
– In windows explorer, directories with a single dot at the end show the files which are inside a directory with same name but without any dot. For example: "irsdl." shows content of "irsdl". Directories with a double dot at the end show the files which are inside a directory with the same name but with a single dot. For example: "irsdl.." shows content of "irsdl.". And so on.
– In Windows Explorer, if you modify a directory with some dots at the end, the modification will be applied on a directory with a dot lesser than the modified directory. Therefore, if you delete "irsdl.", "irsdl" folder will be deleted instead!
– It is not possible to delete these directories by Windows Explorer. (use "del DirName::$Index_Allocation*.* & RD DirName::$Index_Allocation" instead)

Search

goDB NoSQL Injection with
regation Pipelines
23, 2024
kieless DuoDrop: IIS Auth Bypass &
Pool Privesc in ASP.NET Framework
E-2023-36899 & CVE-2023-36560)
st 8, 2023
nor Tag XSS Exploitation in Firefox with
et="_blank"
st 1, 2023
een Years On: Advancing the
erstanding of IIS Short File Name
N) Disclosure!
31, 2023
MDSec Blog Posts so far in 2020/2021!
ber 31, 2020
Upload Attack using XAML Files
ember 21, 2019
Uploading web.config for Fun and Profit 2
August 15, 2019
IIS Application vs. Folder Detection During Blackbox Testing
July 9, 2019
Danger of Stealing Auto Generated .NET Machine Keys
May 10, 2019
x-up-devcap-post-charset Header in ASP.NET to Bypass WAFs Again!
May 4, 2019
Exploiting Deserialisation in ASP.NET via ViewState
April 23, 2019
Yet Other Examples of Abusing CSRF in Logout
April 23, 2019
How to win BIG and even more!
April 17, 2019

In Windows 7:

– It is very similar to Windows XP. However, if you click on the directories by Windows Explorer, it may show you the content of a specific directory for all the Dotty ones.

– It is not also possible to create a folder with only double dots "..".

The directories which only contain several dots such as "…", show the content of their root directory although it is not so real!

Result:

Dotty directories are very good places to hide some files and data! It is not easy to be detected and it is not easy to be deleted! As malwares can use the same technique to hide themselves inside an NTFS partition, we should be very careful about it.

Notes:

Note 0: I might miss some other interesting points. Please let me know when you find one.

Note 1: some of these directori

Note 2: I experienced a crash

directories.

Note 3: Norton Internet Securit

inside these folders. It's not tes

Note 4: Windows XP did check

Note 5: You can do the same t

it by "del *.*".

This entry was posted in Security Post

Directory by Dot, File By Dot, Hidden F

← Skype Privacy Concern: It sends

numbers + URLs to its server!

Finding and Exploiting .NET Remoting over HTTP using Deserialisation

March 26, 2019

More research on .NET deserialization

December 19, 2018

Feel honoured to be there again after 8 years: Top 10 Web Hacking Techniques of 2017

December 19, 2018

Story of my two (but actually three) RCEs in SharePoint in 2018

December 19, 2018

ASP.NET resource files (.RESX) and deserialization issues

August 12, 2018

MS 2018 Q4 – Top 5 Bounty Hunter for 2 RCEs in SharePoint Online

August 12, 2018

WAF Bypass Techniques – Using HTTP Standard and Web Servers' Behaviour

st 12, 2018

hives

lect Year

OG TAGS

Framew ork Anti-XSS bypass XSS bypass ASP.NET g bounty bugbounty bypass llenge deserialisation serialization ecommerce nalInterface ExternalInterface.call e upload file upload bypass ploader bypass methods uploader security bypass financial sh flash xss guideline iis File Extension Security Bypass ort file name IIS Tilde bug IIS tilde feature e vulnerability jar protocol machine.config inekey penetration testing RCE quest encoding sharepoint rt name scanner SQL Injection stricted File Dow nload Unrestricted File Upload view state w af WAF bypass web.config XSS XSS Vulnerability ysoserial.net

REDDIT WEB SECURITY RESEARCH

How to turn a file write vulnerability in a Node.js application into RCE – even though the target's file system is read-only October 10, 2024 */u/albinowax*

Class Pollution in Ruby: A Deep Dive into Exploiting Recursive Merges October 3, 2024 */u/albinowax*

Exploiting trust: Weaponizing permissive CORS configurations October 1, 2024 */u/t0xodile*

Iconv, set the charset to RCE (part 3): Blind file read to RCE in PHP September 30, 2024 */u/cfambionics*

DNS poisoning in 30M domains caused by the Great Firewall September 27, 2024 */u/albinowax*

Splitting the email atom: exploiting parsers to bypass access controls August 23, 2024 */u/garethheyes*

Gotta cache 'em all: bending the rules of web cache exploitation August 22, 2024 */u/albinowax*

Listen to the whispers: web timing attacks that actually work August 8, 2024 *binowax*

to create a Burp Suite Extension from ATCH (Python) July 23, 2024 *ectronic_Village_8*

mmonly overlooked xss vector July 024 */u/Puzzleheaded-Put-693*

REDDIT NETSEC ANNEL FEED

cking APIs using JSON Injection tober 21, 2024

ck Exploit in South Korea's biggest ile chat app October 20, 2024

ing Vulnerability Variants at Scale tober 17, 2024

stack spoofing explained using APT41 vare October 17, 2024

CVE-2024-45844: Privilege escalation in F5 BIG-IP October 17, 2024

EXPLOIT-DB FEED

[webapps] dizqueTV 1.5.3 - Remote Code Execution (RCE)

[webapps] openSIS 9.1 - SQLi (Authenticated)

[webapps] reNgine 2.2.0 - Command Injection (Authenticated)

[dos] Windows TCP/IP - RCE Checker and Denial of Service

[webapps] Invesalius3 - Remote Code Execution

Soroush Dalili's blog asks for your consent to use your personal data to:

Personalised advertising and content, advertising and content measurement, audience research and services development

Store and/or access information on a device

Your personal data will be processed and information from your device (cookies, unique identifiers, and other device data) may be stored by, accessed by and shared with 134 TCF vendor(s) and 63 ad partner(s), or used specifically by this site or app.

Some vendors may process your personal data on the basis of legitimate interest, which you can object to by managing your options below. Look for a link at the bottom of this page to manage or withdraw consent in privacy and cookie settings.