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 and scary! I could find a secret place that important data can be hidden in as well as the malwares! I want to share it with you as some malware writers might already know about this. It is actually another Microsoft weird feature!

In order to create a dotty directory and monitor its behavior, follow me:

1- Open the Windows Command Line (cmd.exe).

2- Go to a test directory.

3.0- Now, insert the following commands and hit Enter:

md ..::$index_allocation –> (Tested in Win XP)

md ….::$index_allocation

md ….::$index_allocation

md irsdl

md irsdl.::$index_allocation

md irsdl..::$index_allocation

3.1- You can use "echo test > " instead of "MD" if you have any

MongoDB NoSQL Injection with Aggregation Pipelines
June 23, 2024
Cookieless DuoDrop: IIS Auth Bypass & App Pool Privesc in ASP.NET Framework (CVE-2023-36899 & CVE-2023-36560)
August 8, 2023
Anchor Tag XSS Exploitation in Firefox with Target="_blank"
August 1, 2023
Thirteen Years On: Advancing the Understanding of IIS Short File

problem.

4- Now get a directory list from the folder that you are currently in (by using “Dir”)

5- In order to open each of these directories use “CD DirName::$Index_Allocation”.

cd …::$index_allocation

6- You can create some files inside these directories as well.

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)

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 “..”.

Name (SFN) Disclosure!
July 31, 2023
My MDSec Blog Posts so far in 2020/2021!
October 31, 2020
File Upload Attack using XAMLX Files
September 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
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

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 directories might be accessible by IIS.

Note 2: I experienced a crash in Windows Explorer in Win7 during playing with these directories.

Note 3: Norton Internet Security 2011 in Win 7 could find and delete the EICAR virus inside these folders. It's not tested on the other things.

Note 4: Windows XP did checkdisk after a restart.

Note 5: You can do the same to create a file by using "echo > …::$Data". And delete it by "del *.*".

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
August 12, 2018

BLOG TAGS

.Net Framework
Anti-XSS bypass
AntiXSS bypass
ASP.NET
bug bounty
bugbounty
bypass
Challenge
deserialisation
deserialization
ecommerce
ExternalInterface
ExternalInterface.call
file upload
file upload bypass
file uploader bypass methods
file uploader security bypass
financial
flash
flash xss
guideline
iis
IIS File Extension Security Bypass
iis short file name
IIS Tilde bug
IIS tilde feature
IIS tilde vulnerability

jar protocol machine.config machinekey penetration testing RCE request encoding sharepoint Short name scanner SQL Injection Unrestricted 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 */u/albinowax*

How to create a Burp Suite Extension from SCRATCH (Python) July 23, 2024 */u/Electronic_Village_8*

A commonly overlooked xss vector July 18, 2024 */u/Puzzleheaded-Put-693*

REDDIT NETSEC CHANNEL FEED

Attacking APIs using JSON Injection October 21, 2024

1-click Exploit in South Korea's biggest mobile chat app October 20, 2024

Finding Vulnerability Variants at Scale October 17, 2024

Call stack spoofing explained using APT41 malware 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