Shimcache Flush!

BlueteamOps · Follow

1 min read · May 27, 2020

1

> *A cleanup routine that can be performed by threat actors to flush the Shimcache to remove traces of their malicious activities.*

Shimcache aka AppCompatCache is a high valued artefact used for forensic analysis during cyber breaches. It holds records to detect evidence of execution or even existence of PEs. Latest OSs can hold up to 1024 entries (older entries gets rolled over). The parser of my choice is https://github.com/EricZimmerman/AppCompatCacheParser.

Below are the commands which can be executed by threat actors on endpoints/servers to flush the cache. Note that changes to the cache is only written during reboot or shutdown of the OS (even if you run the following flush commands). Therefore, you will still be able to obtain forensic evidence via a memory dump. This will provide data prior to last reboot of the system.

Written by BlueteamOps

Follow

81 Followers

Janantha Marasinghe's Research

More from BlueteamOps

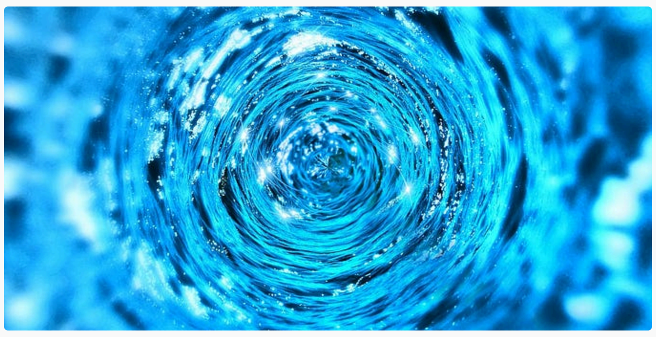
```
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 15
LockoutDuration = 15
AllowAdministratorLockout = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
NewAdministratorName = "Administrator"
NewGuestName = "Unwanted"
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableAdminAccount = 0
EnableGuestAccount = 0
[Event Audit]
AuditSystemEvents = 0
AuditLogonEvents = 0
AuditObjectAccess = 0
AuditPrivilegeUse = 0
```

BlueteamOps

Secedit and I know it!

First, let's talk a bit about auditpol.exe, previous occasions of it being misused and...

Nov 24, 2022 1



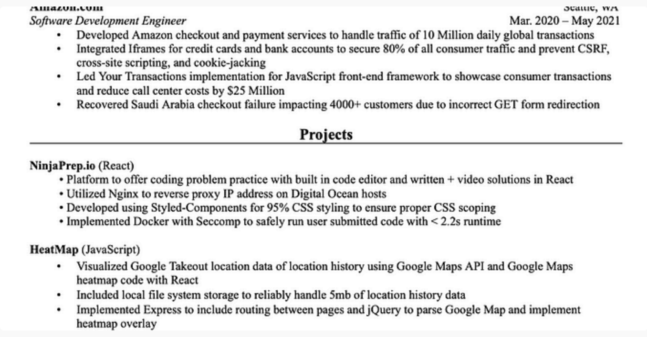
BlueteamOps in Detect FYI

Detecting 'Dev Tunnels'

latest tunnel in town

Oct 23, 2023 3

Recommended from Medium



Amazon.com Seattle, WA
Software Development Engineer Mar. 2020 – May 2021

- Developed Amazon checkout and payment services to handle traffic of 10 Million daily global transactions
- Integrated Iframes for credit cards and bank accounts to secure 80% of all consumer traffic and prevent CSRF, cross-site scripting, and cookie-jacking
- Led Your Transactions implementation for JavaScript front-end framework to showcase consumer transactions and reduce call center costs by $25 Million
- Recovered Saudi Arabia checkout failure impacting 4000+ customers due to incorrect GET form redirection

Projects

NinjaPrep.io (React)
- Platform to offer coding problem practice with built in code editor and written + video solutions in React
- Utilized Nginx to reverse proxy IP address on Digital Ocean hosts
- Developed using Styled-Components for 95% CSS styling to ensure proper CSS scoping
- Implemented Docker with Seccomp to safely run user submitted code with < 2.2s runtime

HeatMap (JavaScript)
- Visualized Google Takeout location data of location history using Google Maps API and Google Maps heatmap code with React
- Included local file system storage to reliably handle 5mb of location history data
- Implemented Express to include routing between pages and jQuery to parse Google Map and implement heatmap overlay

Alexander Nguyen in Level Up Coding

The resume that got a software engineer a $300,000 job at Google.

1-page. Well-formatted.

Jun 1 25K 484

Nathan Hueck

KQL, XQL, and Splunk script to identify executable files in the…

We can begin with comprehensive approach to identifying executable files in the Window…

Jun 7

Lists

Staff Picks
755 stories · 1416 saves

Stories to Help You Level-Up at Work
19 stories · 852 saves

Self-Improvement 101
20 stories · 2961 saves

Productivity 101
20 stories · 2506 saves

Austin Starks in DataDrivenInvestor

I used OpenAI's o1 model to develop a trading strategy. It is…

It literally took one try. I was shocked.

✦ Sep 15 5.3K 140

Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling…

✦ Jun 18 1.6K 54

See more recommendations