Anti-Fingerprinting Suggestions Using Mainly "Living Off The Land Techniques" to Increase the Business Costs of Advanced Persistent Threats and Data Harvesters

Copyright © 2026 Peter Bentley, School of Computing and Engineering, University of Gloucestershire, Cheltenham, UK

***Abstract* –** This paper suggests ways to affect attacks of Advanced Persistent Threats (APT) and Data Harvesters on computer systems. It uses mainly "Living Off The Land" techniques. These techniques are applied to Microsoft Windows and Linux machines. They include, but are not restricted to, modifying IP Addresses, MAC addresses and Languages and they may affect the Mechanism of Action of any unauthorised software.

Keywords –Microsoft Windows; Linux; Fingerprinting; Finger Printing; IP Address; MAC Address, Language; Time Zone; Browser; Volume Serial Number; Malvertising.

1. Introduction

This paper is the seventh in an infrequently issued series of Monographs (University of Gloucestershire, 2026).

The cyber security industry publishes the outcome of their analysis of Advanced Persistent Threats (APT) mainly in the form of white papers. Bentley (2021) distilled over 3,300 documents and this paper is an extension of that research.

APTs and legitimate websites may collect computer specific data, for example user agent, operating system. APTs may use this data to ensure continuity of attack.be used for computer APT attack Bentley (2021). Data harvesters may also use the same but for different business reasons (coveryourtracks.eff.org, 2026). This paper explores ways to change such information to increase the business costs of APTs and data harvesters. It is acknowledged that this may affect, for example, banking apps and that there are other ways of obscuring origin e.g. TOR, which bring with it other challenges.

The work was performed on a dual boot machine: one partition used a Linux system built from a free repository (LINUX.ORG, 2024) and linked repositories (DistroWatch.com, 2024): and the other a Windows system. All work was performed on the Linux partition however, the Windows partition was affected by one piece of software. For security reasons full details of the operating systems are withheld.

Much of this work is based on private infrastructure and use may vary by machine and network. It mainly uses Living Off The Land techniques i.e. software that is part of the operating system and not bespoke. One dedicated program was written.

This paper does not claim completeness but provides suggestions to increase the business costs of APTs and data harvesters

This paper is agnostic towards the origin and intent of APTs.

2. Literature Review

Computer fingerprinting collects a variety of data. It may include IP Address, Browser/User Agent type and version, screen resolution and colour depth, Timezone, Language (What is My Location, 2026) and this data may be hashed for ease of retrieval and storage. Clearly any change in any of the collected data changes the hash (Mainguet, 2009).

Bentley (2021) introduces the concept of software Mechanism of Action and links this to a modified Courses of Action Matrix as described in from the Lockheed Martin Kill Chain (2011)

Bentley (2021) highlights at least three uses computer specific information that have been seen in attacks: the Volume Serial Number (VSN) as a bot id to verify the machine is the correct target and as a basis for an encryption key; the MAC Address used as an RC4 encryption key. Bentley also documents harvesting of IP address and computer name. It is acknowledged that for MAC address of the computer an attacker must be on that computer. Software is available from Microsoft to change the VSN (Microsoft, 2016). This is number of the form xxxx-xxxx but elsewhere it is claimed that the VSN is located at position 72 for 8 places on the Windows Master Boot Record (Sammes and Jenkinson, 2007). Any combination of collected data could provide a bot id but APTs may circumvent the problem by providing a unique value, generated prior to the attack. Wilson (2003) provides an algorithm for obtaining the VSN from the date when the disc was formatted. However, this no longer applies (Forensic Focus, 2026).

It is desirable to stop attackers installing malware and extracting data. Any way defenders can achieve this may increase the APT's business costs.

Malvertising is the term for malicious advertising. Some APTs use legitimate online advertising to identify victims and deploy malware (Juniper, 2018).

MAC addresses are block allocated to manufacturers (IEEE, 2026).

An HTML file with JavaScript was created to fingerprint the machine on which it runs. The output of this may be found in the Appendix. Unfortunately, there are no references in this paper for

this code. The code was developed as background interest before this paper was imagined. However, the code was initially generated using AI and enhanced by using code fragments found searching the web.

3. Commentary on Each Technique

A startup a script is run to invoke a number of scripts. The reason for this is that scripts contained within may be changed without affect the initial call. The following techniques are used:

3.1. Change IP Address

This is trivially done by switching the router on and off at least one a day. Any attack based on static IP address is disrupted.

3.2. Change Computer Name

A Linux script was written to change the hostname in /etc/hosts and /etc/hostname to a random word selected from a copy of the dictionary file /etc/dictionaries-common/words. This random word was selected by the pseudo-random number generator: number=$(($(date +%s%N)%(line_no-1))) where line_no is the number of lines in the dictionary file.

Later this was changed to a single, constant, word followed by an integer [0, 63]. The integer was generated by the pseudo-random number generator: number=$(($(date +%s%N)%64)). The reason for the change was that by providing a random number to the machine might make the APT think that the number of computers on the network is larger than there really are and waste their time looking for the other machines.

3.3. Time Zone Change

A script was written to randomly change the time zone.

3.4. Change of Language

This script changes the language used. This script contains hard coded values in two arrays for “lang” and “language” and values are randomly selected from each for the session. This changes the language variables LANG, LANGUAGE and variables starting “LC_”.

Values are hard coded to inhibit the use of unreadable languages.

3.5. Browser Change

A few browsers are installed on the Linux machine. A browser is suggested by generating a random number, again based on the date, and suggesting a browser to the user by a pop-up box. The user may, or may not, use this suggestion.

It is noted that each browser used generated a different user agent string.

3.6. Change Computer MAC Address

There were some problems generating a completely new MAC address. It is hypothesised that this is because they are block assigned to a manufacturer. To circumvent this script retains high order bits and only changes low order bits.

3.7. Inhibit Advertising

This is done by blocking websites which may, or may not, be those of advertisers by adding lines to the Linux file /etc/hosts or the Windows file C:\Windows\System32\drivers\etc\hosts using the loopback address 127.0.0.1 e.g.

127.0.0.1 www.bbc.co.uk

3.8. Disrupt Advertising

Some browsers permit command line searches. This script selects random words from the dictionary file and searches for them on the internet. This should add bias to harvested internet search data and, therefore, affect the algorithms that serve up advertisements.

With this technique it is possible to change the User Agent but not to any version of the User Agent.

3.9. Volume Serial Number Change

This was the only bespoke software. It is possible to access the Windows machine/partition from the Linux machine/partition.

Using the Linux tool “gparted “it is possible to view other partitions on the machine. The format of the partition name is /dev/sdax where x is a positive integer. One of these is the Windows partition. It is possible, using “sudo”, to read and write to this partition. This was achieved with a C program compiled using gcc.

The VSN was read from, modified and written to, the Windows Master Boot Record (MBR) for 8 hex characters from position 72 with 0xff; It was later returned to its original value. Overwriting all eight hex characters instead of the first four did not seem to affect machine operation. Although this test was not extensive the machine booted up and a browser was successfully used.

The algorithm described by Wilson (2003) was applied to one disc. The VSN could not be produced from the date in the $Volume record. Should a more rigorous value be needed, beyond overwriting with random values more forensic work would be needed.

4. Discussion

Ideally attackers' mechanisms of action should be managed as early as possible in the attack chain. For very little effort, changing the number of machines presented to attackers could easily run into the millions. Using Sections 3.2 – 3.5 apparently different machines can be presented to attackers or even data harvesters. For example, there may be C values for the computer name, L_1 values for lang, L_2 for language, T time zones and B browsers installed. Five of each presents 3,125 machines to attacker. Trivially extending the computer name value to 100 presents 62,500 machines. Multiply by the IP block size of the provider, the space of MAC addresses and the space of VSNs that may be generated and the number of machines becomes billions. In addition, several .iso files of different operating systems could be loaded into a virtual machine. Finally, multiply by the number of VPNs installed.

To reduce their footprint APTs or Data Harvesters may only retrieve a hash of the fingerprint. Any change in the data used in the hash changes that hash presenting an apparently different machine each time.

5. A Critique of this Work and Suggested Further Lines of Work

This paper does not claim complete success and contains issues for administrators. For example, static IP addresses or static MAC addresses CISCO (Unknown) may be needed for the business security or personal banking security.

Other computer variables may be changed to affect APTs and Data Harvesters.

It is noted that one can write to a Windows partition from a Linux partition. Should the latter be hidden then that demonstrates an attack technique. However, should an APT have been able to do this then there might be easier ways that they could attack.

6. Concluding Remarks

The paper has presented and discussed ways to disrupt APTs and Data Harvesters by changing machine variables that are used in computer fingerprinting. It does not claim 100% success but offers suggestions for simple scripts that any sysadmin may write and implement based on their wider business security needs.

References

Bentley, P (2021) The Treatment of Advanced Persistent Threat on Windows Based Systems p 120, p157, p186, p214-215, p231 Available at: https://eprints.glos.ac.uk/10332/ (Accessed: 12th July 2026)

CISCO (Unknown) Configuring Port Security https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011111.html (Accessed: 18th July 2026)

Coveryourtracks.eff.org (2026) See How Trackers View Your Browser Available at: /about https://coveryourtracks.eff.org/about (Accessed 26th July 2026)

DistroWatch.com (2024) DistroWatch.com Available at: https://distrowatch.com/

Forensic Focus (2026) NTFS Volume Serial Number TO date and time of creation Available at: https://www.forensicfocus.com/forums/general/ntfs-volume-serial-number-to-date-and-time-of-creation/ (Accessed 27th August 2026)

IEEE (2026) MAC Addresses Available at: https://standards.ieee.org/products-programs/regauth/mac/ (Accessed: 18th July 2026).

Hutchins, E. M., Clopperty, M. J. and Amin, R. M. (2011) 6th International Conference on Information Warfare and Security. The George Washington University, Washington, DC, USA 17-18 March 2011. Academic Conferences and Publishing International Limited.

Juniper (2018) Combating Malvertising and Drive-By Downloads Available at: https://www.juniper.net/content/dam/www/assets/white-papers/us/en/security/combating-malvertising-and-drive-by-downloads.pdf p 3 Accessed 22nd July 2026

LINUX.ORG (2024) Linux.org Available at https://www.linux.org/pages/download/

Mainguet, JF. (2009). Fingerprints Hashing. In: Li, S.Z., Jain, A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_60

Microsoft (2016) VolumeID v2.1 Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/volumeid (Accessed 18th July 2026).

Sammes, T. and Jenkinson, B. (2007) Forensic Computing a Practitioner's Guide. London 2010: Springer-Verlag. p 199, p387-388

University of Gloucestershire (2026) Repository Statistics Available at: https://eprints.glos.ac.uk/cgi/stats/report/authors/1f86d5cbc0df3f3cae58c198c0a1c27c/main Accessed 28th July 2026

What is My Location (2026) Browser Fingerprinting Explained: What Our Tool Actually Reveals Available at: https://whatismylocation.org/blog/browser-fingerprinting-explained (Accessed: 12th July 2026).

Wilson, Craig (October 2003 (updated June 2005)) Volume Serial Numbers and Format Date/Time Verification Available at: https://www.digital-detective.net/documents/Volume%20Serial%20Numbers.pdf (Accessed: 12th July 2026).

Appendix

Generated Fingerprint Hash is: <redacted>

Generated Fingerprint is ...

Browser ...

UserAgent: <redacted>

Language: <redacted>

Languages: <redacted>

Cookies Enabled: <redacted>

Do Not Track: <redacted>

Plugins: <redacted>

Hardware ...

Vendor: <redacted>

WebGL Vendor: <redacted>

WebGL Renderer: <redacted>

Device: <redacted>

Platform: <redacted>

Hardware Concurrency: <redacted>

Device Memory: <redacted>

Battery Information: <redacted>

Screen Resolution: <redacted>

Colour Depth: <redacted>

PixelRatio: <redacted>

Absolute ScreenWidth: <redacted>

Absolute ScreenHeight: <redacted>

Available ScreenWidth: <redacted>

Available ScreenHeight: <redacted>

Inner ScreenWidth: <redacted>

Inner ScreenHeight: <redacted>

Network and Time Zone ...

Online/Offline: <redacted>

TimezoneOffset Minutes: <redacted>

TimezoneOffset Hours: <redacted>

Timezone: <redacted>

Misc ...

Max Touch Points: <redacted>

Detected Fonts: <redacted>

MIMES types: <redacted>

Canvas: <redacted>