iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78394

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Behavioral Profiling of Living-off-the-Land (LotL) Commands for Threat Hunting

Pallavi Ramkrishna More
Senior Cybersecurity Engineer, Cybersecurity Research & Operations

Abstract: ***Living-off-the-Land (LotL) attacks are an increasing cybersecurity issue in the contemporary world as cybercriminals use legitimate system tools to carry out malicious tasks without detection by traditional signature-based detection. PowerShell, WMI, certutil and rundll32 are some native utilities that allow the attacker to execute, persist and exfiltrate data without installing traceable malware binaries.***

In this study, the researcher suggests a behavioral profiling technique to identify malicious use of LotL commands by threat hunting using telemetry. The analysis uses command-line logs, relationship of processes, and pattern of execution taken out of Windows event logs and endpoint telemetry. Strict behavioral characteristics like command chaining, coded payload markers, unorthodox father-child process associations and recurring frequencies are harvested in order to model suspicious command sequences.

The correlation of these indicators of behavior with the adversary techniques reported in the MITRE ATT&CK framework allows the proposed approach to identify stealthy attack behaviors proactively. Empirical studies show that behavioral profiling can substantially enhance the ability to detect and offer viable information to undertake advanced threat hunting tasks.

Keywords: Living-off-the-Land (LotL) Attacks, Behavioral Profiling, Threat Hunting, Command-Line Telemetry Analysis, Endpoint Security Analytics

I. INTRODUCTION

One of the most advanced and disguised methods of contemporary cyber intrusion has become Living-off-the-Land (LotL) attacks. Compared to conventional malware attacks which entail the installation of malicious binaries on the victim systems, LotL attacks use the already existing legitimate tools, scripts and administrative utilities within the operating system to carry out malicious activities.

They often use trusted system features like PowerShell, Windows Management Instrumentation (WMI), command-line tools and system administration tools to run commands, perform reconnaissance, lateral movement across the networks, and get out with valuable information.

Since most of them are legitimate and used regularly by the system administrators, malicious activities may integrate into the normal system operations, and they may hardly be detected by the usual signature security systems [1][2]. In most instances, the malicious code is run fully in memory so that little disk-based forensic evidence remains and thus, attackers are able to circumvent antivirus and endpoint protection software that uses file-based detection methods [3]. This type of attacks is similar to fileless malware where attackers use scripting engines or in memory execution instead of malware files that are executable on their own [2]. Consequently, security experts become more and more vulnerable to the challenge of separating a lawful administrative activity and an act of malicious command execution.

Modern-day threat actors and organized cybercrime networks have implemented LotL methods since they enable attackers to circumvent detection systems, survive in networks with intrusions, and hone quietly over an extended time. Besides, the idea of Living-off-the-Land is strongly correlated with adversarial techniques that are reported in the modern threat intelligence models, in which malicious actors use so-called Living-off-the-Land Binaries (LOLBins) to accomplish malicious goals without triggering any security-related alarm [4]. As endpoint automation and cloud infrastructure, as well as remote administration tools, have grown quickly, the exposure to such command-based exploitation has grown dramatically, and LotL techniques have become a core focus of current cybersecurity research and threat-hunting activities [5].

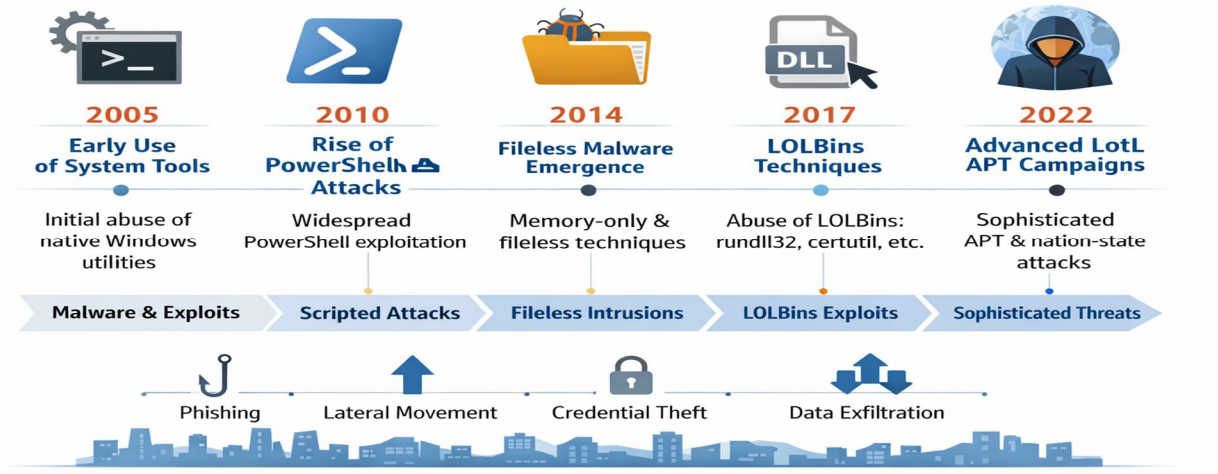


Figure I. Evolution of Living-off-the-Land (LotL) Attacks

This growing dependence on the Living-off-the-Land method has led to massive economic and functional losses in the business sector in the world at large. Since such attacks use the legitimate system tools, organizations usually cannot identify them before the attacker has achieved persistence or stolen important data. It has been estimated that hundreds of thousands of systems in the world have been targeted by fileless and LotL-style attacks which have cost the world economy billions of dollars in key cyber incidents alone [6]. Among the brightest ones is the case of NotPetya cyberattack, which is based on credential harvesting and use of legitimate administration tools to spread throughout enterprise networks and create disastrous havoc among companies and infrastructure around the globe [7]. The consequence of the attack saw multinational companies in the logistics, healthcare, finance, and manufacturing sectors affected, indicating how attackers can use trusted system utilities to create mass operational events. In addition to major ransomware attacks, LotL is prevalent in espionage and financial cybercrime and advanced persistent threat activities. Since attackers use trusted binaries and not malicious executables, most organizations fail to notice the initial phases of the compromise until the attack escalates into the data stealing or sabotaging of the system. This covert working system has enabled the criminals to stay unnoticed on network systems over long durations, even weeks and months, which heightens the financial and reputational harm that the targeted organizations may suffer [1][8].

These attacks are growing at an alarming rate and this situation demonstrates a complete paradigm change in cyber-offensive methods. Traditional malware campaigns targeted the deployment of malicious executables that could be spotted using signatures or even by means of static analysis. Modern attackers, by contrast, are increasingly relying on the legitimate tools being used in a behavioral fashion to turn otherwise trusted system capabilities into attack mechanisms. This transformation has been partly fuelled by the advancements in the defensive systems including antivirus and endpoint detection systems, which have compelled the attackers to resort to less open methods of operation [4]. LotL attacks are also known to allow attackers to be able to complete several steps of the cyber kill chain such as reconnaissance, credential theft, privilege escalation, lateral movement, and data exfiltration, with just built-in utilities and scripts [8]. Since such operations are similar to the normal operations of an administration, only sophisticated telemetry analysis and behavioral threat-hunting strategies can be used to differentiate between a nefarious activity and the normal operations of a system. As a result, cybersecurity scientists and practitioners have started paying attention to behavioral profiling of patterns of command execution, process relationships, and command-sequence anomalies as a technique of identifying such attacks. Learning how legitimate commands are used as weaponry by attackers and the behavioral patterns of abnormally using commands have thus become research areas that are of critical importance in current threat detection and proactive cyber defense interventions [5].

II. HOW LIVING-OFF-THE-LAND (LOTL) ATTACKS WORK

Living-off-the-Land (LotL) attacks are attacks where tools that are a legitimate part of a system and trusted binaries, which are already present in an operating system, are used to execute the malicious behavior. Instead of causing a network to execute new malware files, attackers rely on the available in-built utilities such as PowerShell, Windows Management Instrumentation (WMI), command-line interpreters and other administration tools to execute commands and download payloads, laterally traverse a network and steal sensitive information.

These are good components of operating system and they are used extensively by the system administrators in performing normal maintenance and automation. Therefore, security solutions are more likely to consider their deployment as a common practice of the system and will allow attackers a chance to confuse malice with a just administrative process. In the most typical LotL attack, the attacker gets the first entry with the help of phishing messages, hacked credentials, or code bugs. As soon as they are in, they begin executing system commands to record system information, identify privileged accounts as well as enumerating network resources. These activities are founded on trusted applications, and hence the attack can proceed without any conventional antivirus or signature-based detection system. Scripting environments and command-line utilities also imply that the attacker can directly invoke malicious instructions in memory with only slight generation of files that can be discerned on disk. The operations model of such nature enables the adversaries to be persistent, add privileges, and pursue lateral movements in enterprise environments and become difficult to be detected with the conventional security systems.

A real life situation of this kind of attack pattern can be witnessed in the Active Directory (AD) environment where the attacker abuses administrative tools which are normally used to administer the system. An example of such can be seen when a user has already been compromised by phishing or stealing his/her credentials, a PowerShell-based search of the domain users and group membership can be done with the following types of commands: Get-ADUser or net group Domain Admins /domain. The reconnaissance stage is similar to the common methods of AD attacks such as credential harvesting and privilege discovery with the only difference being the tools. In a typical attack of malware, attackers will utilize malware to steal credential or exploit kits to achieve reconnaissance. Quite to the contrary, a LotL attacker does so by using the built-in administrative utilities to make it appear like the action is legal as appears in system logs. Once reconnaissance is complete, attackers can then be able to escalate the privileges either through stealing the credentials in memory or abusing the scheduled tasks and service settings. Now, techniques similar to the Kerberos based attacks such as Kerberoasting or Pass-the-Ticket are applicable to obtain background privileges and expand access into the domain environment. Lateral movement is also a stage, which demonstrates that LotL techniques are not unique and that they resemble other popular attacks on Active Directory. An example is that the attackers can use wmic, PsExec or remote PowerShell session to provide commands to other network computers. This step appears analogous to the lateral movement in credit-based attacks like Pass-the-Hash, where the attackers gain access to compromised credentials and then submit them to authenticate them to numerous systems. In case of LotL, however, there are legitimate administrative programs that the actions are performed using rather than home-cooked malware frameworks. Similarly, the mechanisms of persistence such as scheduled activities or changes in registers or services installations can be utilized in the assurance of long term access in the domain controller or other important infrastructure systems.

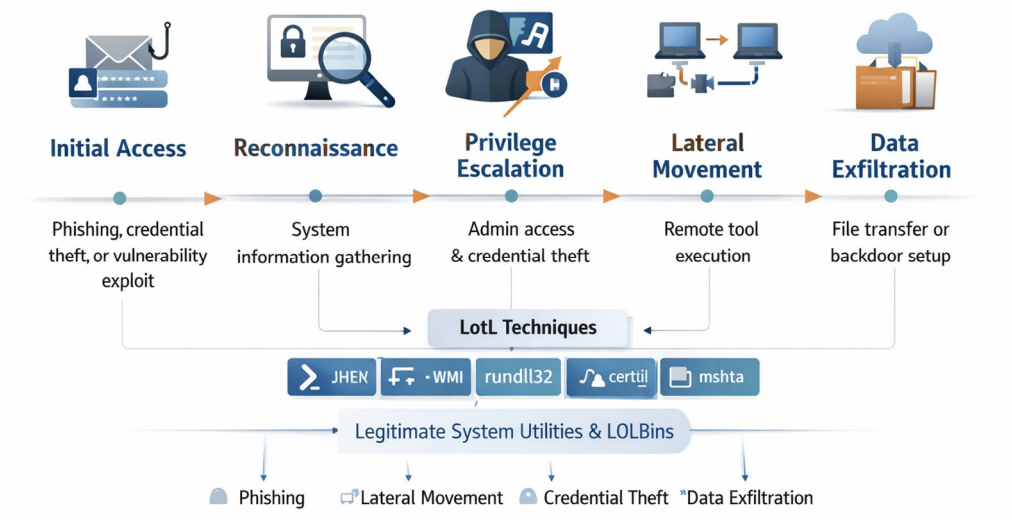


Figure II. Typical LotL Attack Workflow

The formal procedure that is characteristic of an average LotL attack aligns with the stages of typical cyberattacks. After getting into our system, attackers use system utility to perform reconnaissance action that could include system information, running processes and mapping internal network environment. The hostile side is able to automate such reconnaissance efforts using PowerShell or command line programs. Once the necessary information is collected, attackers make every effort to gain privileges that will allow them access to administrative privileges and expand their reach to the attacked environment.

Privilege escalation may be credential dumping, system registry setup or scheduled task abuse. Upon attaining escalation, the attackers move sideways through the network systems using the legitimate remote administration protocol or system management tools. During this step, the enemies can spread themselves across the network and identify the useful targets including database servers or domain controllers. The final stage is normally the exfiltration of the data or the ongoing development of the backdoors so that the attacker can access the environment on long-term basis. Because all phases utilise approved system resources, any maliciousness can only be observed through the aspect of context, i.e. command-line arguments, process relations or sequence execution.

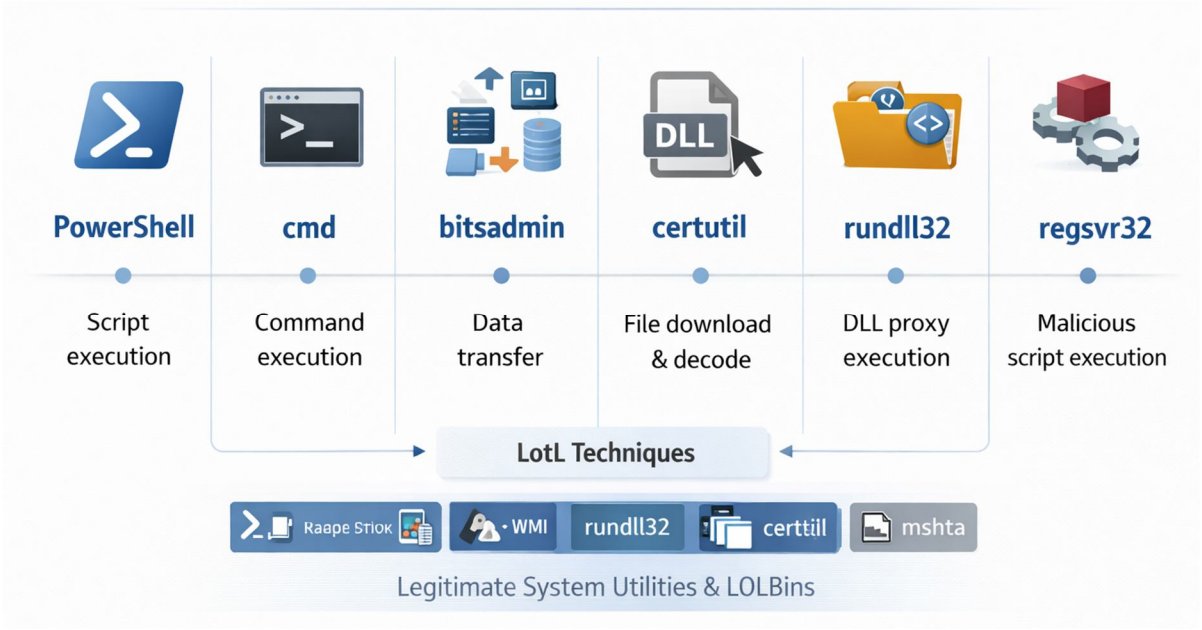


Figure III. Common Living-off-the-Land Binaries (LOLBins) Used in Attacks

Calls to special system utilities can be taken by hackers, which are known as Living-off-the-Land Binaries (LOLBins), to complete an illicit activity. These binaries are legal executables, that can be used to administer, but can equally be misused and can be used to perform illegal actions. Using PowerShell as an example, the language can run coded scripts and even load downloadable payloads directly into memory to bypass file based detection strategies. Similarly on remote servers file transfer may be conducted through such utility as certutil or encrypted/deencrypted messages that will be moved. Other tools that will help the attacker to use legitimate system process to execute malicious code with the impact of covering the malicious activity as a normal system operation are also available like rundll32, mshta and regsvr32. The binaries are signed and hence default installation of operating systems is comprised with these binaries and therefore they cannot be easily identified to raise security alerts when executed. Thus, the trusted utilities provide the attackers with a chance to be not noticed and invisible at different stages of an attack campaign. Such binaries and their usage pattern is therefore required in establishing abnormal usage and execution of commands as well as in identification of potential Lotl activity on enterprise systems. Monitoring of command-line parameters, execution paths and process dependencies involving these tools may also be helpful during threat-hunting efforts, and in identifying behavioral anomalies.

III. LOTL COMMAND TAXONOMY

The attacks of Living-off-the-Land (LotL) have primarily been based on the exploitation of operating system native legitimate command line utilities along with administrative binaries. Such instructions are actual administrative functions to the system administrators as system administration, system automation, remoteness administration and troubleshooting. But, the enemies use the same to do the devilish deeds without leaving any significant footprint. In a business environment, which is mostly windows based infrastructure and centralized infrastructure of identity such as active directory, attackers normally use command line interfaces to conduct reconnaissance, privilege escalation and subsequent lateral movement, using the network systems. Such tools are categorized according to their use in an attack lifecycle such as command execution, the harvesting of credentials, the establishment of persistence, defense evasion, and data exfiltration, in this LotL taxonomy.

This type of knowledge of this taxonomy would be more useful to security analysts and threat hunters to study the command telemetry and discern between normal administrative processes and possible malicious sequences of commands. Because the majority of these commands are digitally signed and are embedded into executable code in the operating systems, they are now often identified through behavioral profiling and examination of the arguments of the commands, the routes of execution, as well as connections of them with processes, instead of being identified by the mere finding of the command.

Attackers often also communicate with the operating system using command-line interfaces (e.g. Windows Command Prompt, PowerShell scripting). These interfaces allow administrators to directly access system resources and administration utilities, allowing attackers to do complex system operations at low overhead. As an example, system processes may be listed by issuing commands using the command prompt such as to list contents of the network configuration, to modify registry settings or to download remote payloads. Since these activities are similar to normal administrative operations, security surveillance devices usually fail to distinguish between authorized and malicious execution of commands in the system. Attackers in most instances will combine several commands together to automate the attack phases, the reconnaissance phase, privilege escalation phase and the lateral movement phase. This chain command behavior develops patterned behavior which can be reviewed by the behavioral profiling systems. Through investigating the interactions of commands, and access to system resources, process hierarchies and network communications, threat hunters have the ability to detect abnormalities, which are telling of possible misuse of approved utilities. Breaking these commands into functional groups also allows reaching detection rules and behaviour models that drives proactive threat-hunting activities in enterprise settings.

TABLE 1
Taxonomy Of Common Living-Off-The-Land Commands

Category	Command / Tool	Typical Legitimate Use	Malicious Abuse in LotL Attacks
Command Execution	PowerShell	Script automation and system management	Execution of encoded payloads or remote scripts
System Enumeration	cmd / net	User and system information retrieval	Reconnaissance of domain users and privileges
Remote Administration	WMI / wmic	Remote system management	Lateral movement across network systems
File Transfer	bitsadmin	Background file transfer	Downloading malicious payloads
Encoding & Data Handling	certutil	Certificate management	Payload encoding, decoding, and covert downloads
Proxy Execution	rundll32	Running DLL components	Execution of malicious DLL code
Script Execution	regsvr32 / mshta	Registering system components	Execution of remote scripts or malicious payloads
Persistence	schtasks	Task scheduling	Establishing persistent backdoors

IV. BEHAVIORAL CHARACTERISTICS OF LOTL COMMANDS IN ENTERPRISE TELEMETRY

Analysis of Living-off-the-Land (LotL) commands used during behavioral analysis has turned out to be a key element of modern threat detection of enterprises due to the inability of conventional signature-based systems to identify the difference between administrative functions and command execution in terms of malicious intent. Because attackers abuse trusted system binaries including PowerShell, Windows Management Instrumentation (WMI), and command-line interpreters, the distinguishing factor between good and bad activity is seen in the execution of those commands and not the command itself. Telemetry in the enterprise environment, which can be gathered based on endpoint detection platforms, system log, and network monitoring systems, offers useful behavioral information that aids in identifying suspicious command use.

Such indicators are abnormal command-line arguments, abnormal parent-child process relationships, unexpected contexts of command execution and anomalous time series execution pattern. An example would be the execution of PowerShell scripts by applications like Microsoft Word or web browsers which could be evidence of a malicious chain of macro execution and not as an example of legitimate administrative use. On the same note, when administrative commands are high-frequency and executed on several positions on various hosts in a brief duration, it can signify automated lateral movement in a compromised network. Contextual information including user identity, execution privileges, network connections, and process lineage are also captured by behavioral telemetry and are useful to help analysts determine abnormal activity patterns. Through these behavioral indicators, security teams are able to identify covert adversarial actions that use legitimate system utilities at minimum false positives that are a by-product of normal administrative tasks. Therefore, command telemetry behavioral profiling is very vital in threat hunting, as organizations can predict and identify suspicious behavior before it develops into a massive compromise.

TABLE 2
Behavioral Indicators Of Living-Off-The-Land Commands In Enterprise Telemetry

Behavioral Feature	Description	Example Indicator	Potential Threat Implication
Parent–Child Process Relationship	Analysis of which process launched the command execution	PowerShell launched by Microsoft Word	Possible macro-based attack or phishing payload execution
Command-Line Arguments	Inspection of parameters passed to commands	Encoded PowerShell commands using Base64	Obfuscation used to hide malicious scripts
Execution Frequency	Number of times a command executes within a short time window	Multiple PowerShell executions within seconds	Automated attack scripts or lateral movement
Execution Context	Privilege level or user account executing the command	Domain admin executing unusual commands	Potential credential compromise
Temporal Behavior	Time pattern of command execution	Administrative commands executed at unusual hours	Suspicious after-hours activity
Process Chain Length	Number of processes spawned sequentially	winword → powershell → cmd → rundll32	Multi-stage attack execution chain
Network Connectivity	Network communication initiated by commands	PowerShell downloading files from external IP	Payload retrieval or command-and-control activity
Host Propagation Pattern	Commands executed across multiple hosts	wmic executing commands on several machines	Lateral movement within enterprise network
System Resource Access	Access to registry, memory, or sensitive files	certutil accessing encoded payload files	Possible staging of malicious components
Persistence Behavior	Repeated execution or task scheduling	schtasks creating recurring tasks	Establishing persistence on compromised systems

V. PROPOSED BEHAVIORAL PROFILING FRAMEWORK FOR LOTL THREAT HUNTING

The proposed behavioral profiling system will be capable of detecting Living-off-the-Land (LotL) attacks with the behavior of command execution, rather than basing on a few, specific detection guidelines or relying on the static signature. Seeing how the attackers exploit legitimate system utilities such as PowerShell, command prompt utilities and administrative binaries, the

framework focuses on the context and behavioral telemetry data collected on enterprise endpoints. The framework operates in a multi-stage pipeline, which includes, gathering of telemetry, feature extraction, modelling of behaviour, anomaly identification and correlation between anomalies and threat-hunting. Initial data observed on the endpoint logs are process creation events, command-line arguments, user context, and network connections as observed by monitoring systems such as windows event logs, Sysmon and endpoint detection platforms. These logs are further broken down to identify the behavioral patterns such as frequency of commands, relationship between parent and child process, chain patterns of command and patterns of privilege context and pattern of network communication. The framework is built on the behavioral profiles through the combination of all these features and hence they are a normal functioning in the enterprise environment in administration. Then the deviation of these baseline behaviors can be detected through machine learning models to steer security teams to determine tendentious command-based attack that would otherwise be tallied as legitimate. This approach modifies the rule that is similar to the detection to behavioral anomaly detection to allow threat hunters to reveal suspicious command sequence that might indicate a potential compromise.

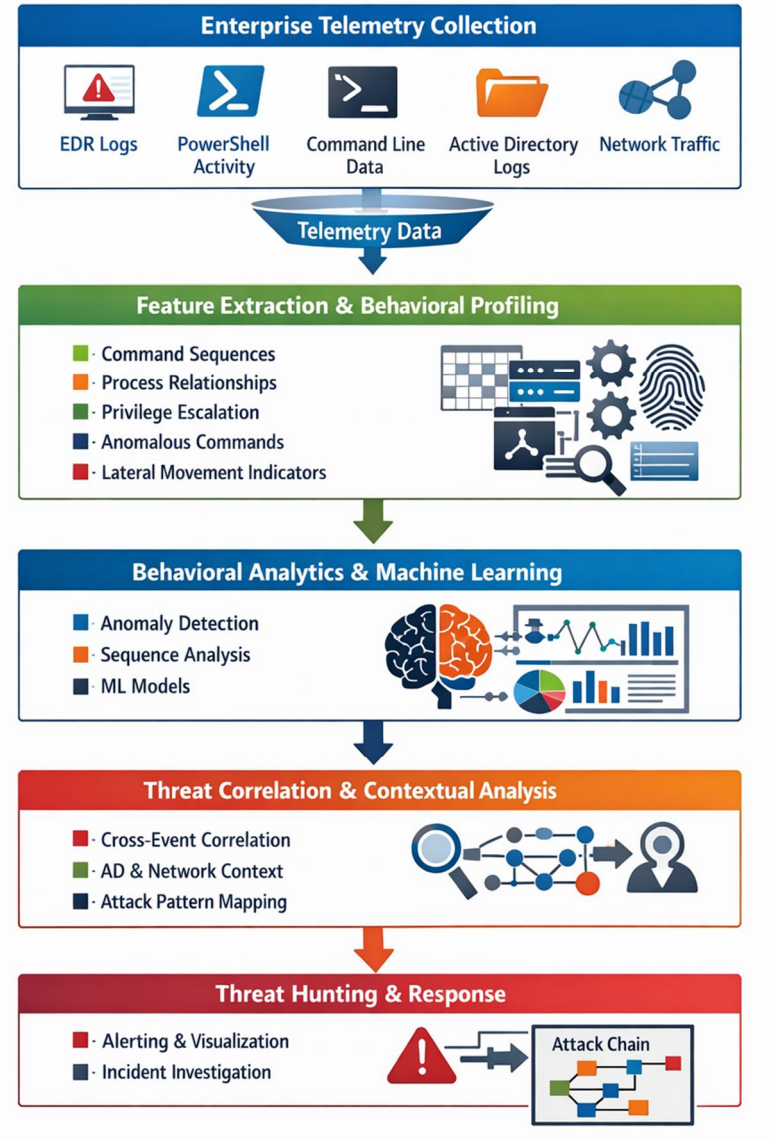


Figure IV: Neural Behavioral Analysis Model for LotL Detection

The neural behavioral analysis model is a key factor in defining the abnormal command performance in enterprise conditions. Under this model, the telemetry aspects based on endpoint logs are converted into structured datasets which reflect behavioral patterns of command utilization.

Options like order of command sequences, frequency of execution, privilege level, process relations and network activity are coded into feature vectors and fed as input to machine learning algorithms. Normal operational patterns can then be learned by the neural networks or sequence based models that occur in the enterprise systems and deviation can be identified which could signify malicious activity. To illustrate, an example of a sequence of commands C- winword - powershell - certutil - rundll32 can be an example of a suspicious chain of execution that is usually linked to fileless malware delivery. In case the model notices such anomalies, it creates alerts, which may be investigated by using threat-hunting workflows. In the long run, the ongoing enterprise telemetry-driven learning enhances the model to identify the legitimate administrative operations and malicious command sequences and the former and lowers the false positives and improves the detection accuracy.

Behavioral threat analysis involves identifying the mapped anomalies with the established adversarial methods and attack phases. After the behavioral profiling model has detected the suspicious command sequences, these actions can be traced to other phases of the attack lifecycle, such as reconnaissance, privilege escalation, lateral movement, and data exfiltration. Threat analysis entails analysis of contextual telemetry including originating user account, infected systems, command arguments, and network destinations of suspicious commands. Through the correlation of these indicators, the analysts will be able to identify whether the identified activity is benign administrative activity or an active intrusion attempt. It is also capable of mapping observed behaviors to adversarial techniques reported in threat intelligence frameworks that can enable security teams to see a bigger picture of the attack campaign. Combining behavioral detection and threat intelligence, thus, allows proactive threat hunting, in which the analyst looks into suspicious patterns before the attacker can accomplish their goals.

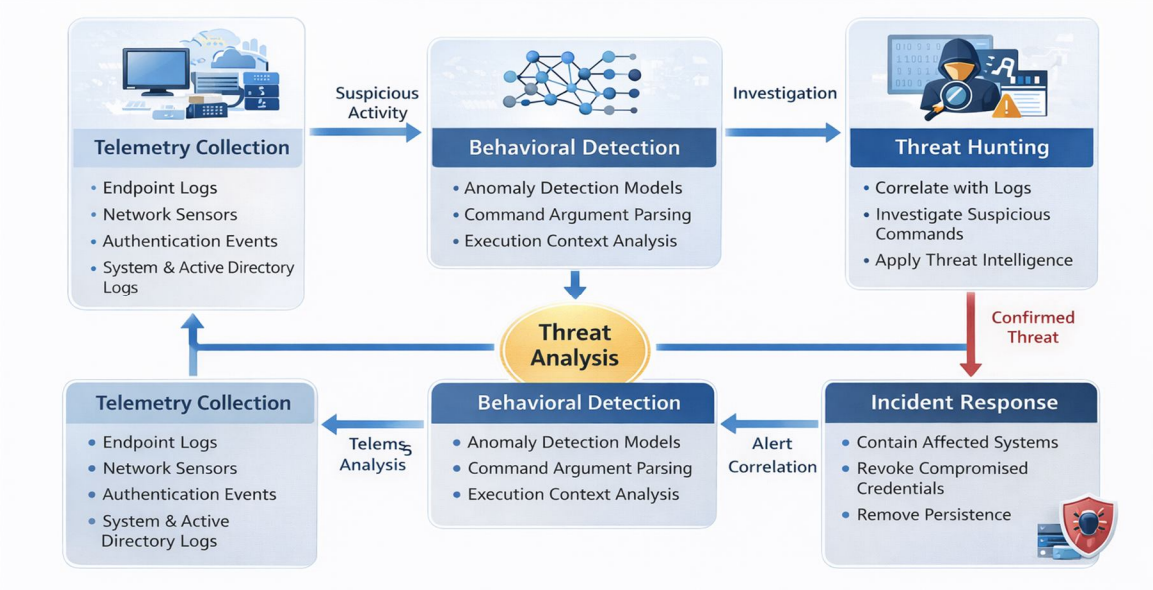


Figure V: Threat Analysis Workflow for LotL Command Detection

This flow diagram shows how behavioral analysis can be used to transform enterprise telemetry into threat intelligence that can be acted upon. Information gathered on endpoints and network sensors is initially processed using behavioral detection models which determine patterns of suspicious commands. These alerts are subsequently processed by threat-hunt teams who compare them with system log, user activity and network traffic in order to detect the extent of the possible compromise. In case of malicious activity being established, incident response teams start to put in place containment actions which includes isolating the impacted systems, terminating the compromised credentials and eliminating the persistence mechanisms. Through behavioral analytics coupled with formal threat-hunting processes, companies can identify sneaky LotL attacks further into the intrusion chain and mitigate the effects of more complex command-based cyberattacks by a substantial margin.

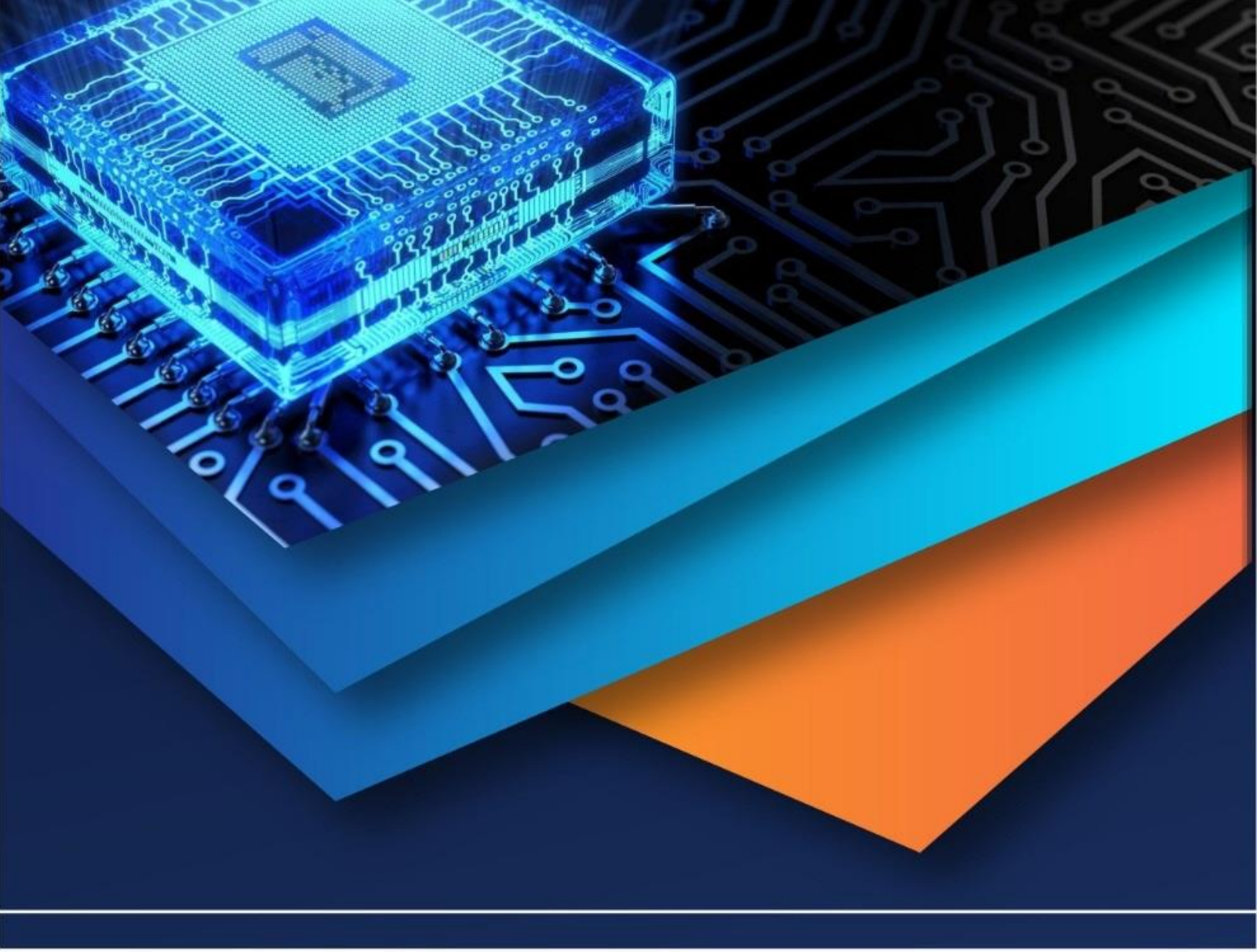
VI. CONCLUSION

Of interest to the modern approaches to cyberattacks is the Living- off-the-Land (LotL) attacks where an attacker calls on legitimate system utilities rather than resorting to the traditional malware. Attackers can conduct reconnaissance, privilege escalation, lateral movement, and data exfiltration with the assistance of established administrative tools, such as PowerShell, WMI, and command-line systems and remain difficult to detect with conventional security capabilities.

As discussed in this paper, the nature of operations of LotL attacks, and how the attackers take advantage of binaries that belong to the native system and utilize these binaries to inject malicious activity and the way they make the legitimate administration behave work as well. Through the examination of the patterns of enterprise telemetry and patterns of command execution, the paper developed a conclusion that behavioral profiling could be applied to provide the useful information to determine the application of such suspicious commands, which are hard to detect by other currently available systems of signature detection. The proposed model of behaviour profiling illustrates the applicability of testing situational pointers such as process relations, frequency of command, execution context, and network activity so as to identify abnormal behaviour in the enterprise settings. By integrating telemetry analysis, behavioral modeling, and threat-hunting processes, organizations will have a significant opportunity to improve the process of detecting stealthy command-based intrusions. In addition, visual processing applications such as radar-based behavioral indicators and threat analysis procedure patterns help security analysts to analyze complex telemetry patterns and prioritize investigations. Overall, the data presented in the paper suggests that behavioral analysis and preemptive threat hunting can be identified as the major components of the modern cybersecurity operations, particularly in the environment where the attackers increasingly utilize the Living-off-the-Land tactics to remain unnoticed and operational within the enterprise networks.

REFERENCES

[1] Al-Shaer, E., Duan, Q., & Jafarian, J. (2013). Random host mutation for moving target defense. Proceedings of the IEEE Security and Privacy Workshops, pp. 310–317. https://doi.org/10.1109/SPW.2013.41
[2] Behl, A., Behl, K., & Behl, K. (2017). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
[3] Bromiley, M., & Baker, A. (2020). Fileless malware: The stealthy cyberattack technique. SANS Institute Information Security Reading Room.
[4] Cimpanu, C. (2020). Living-off-the-land attacks are becoming the dominant attack technique. ZDNet Cybersecurity Report.
[5] CrowdStrike. (2022). The CrowdStrike Global Threat Report 2022. CrowdStrike Inc.
[6] Greenberg, A. (2018). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Doubleday.
[7] Greenberg, A. (2020). The untold story of NotPetya, the most devastating cyberattack in history. Wired. https://www.wired.com
[8] MITRE Corporation. (2023). MITRE ATT&CK: Adversarial tactics, techniques, and common knowledge. https://attack.mitre.org
[9] Palo Alto Networks. (2021). Unit 42 Threat Report: Fileless malware and Living-off-the-Land techniques. Palo Alto Networks.
[10] Symantec Corporation. (2019). Living-off-the-Land: Attackers use legitimate tools to compromise enterprises. Symantec Security Response.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY