illumio

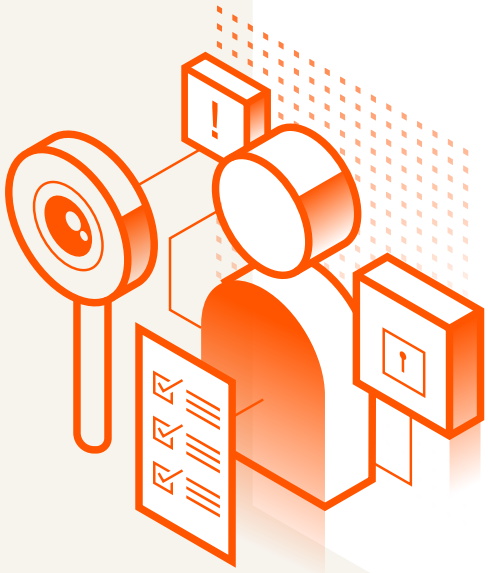
EBOOK

Living off the Land

How cyberattackers exploit native tools — and how security teams can fight back

Contents

Ghost-like threats: what is living off the land in cybersecurity?



In nature, “living off the land” means surviving only on what’s around you by hunting, gathering, and adapting to the environment. In cybersecurity, attackers are doing much of the same.

Living-off-the-land (LOTL) attacks[1] use legitimate tools built into the operating system — like PowerShell, PsExec, WMI, SSH, and AppleScript. These tools, or native binaries, are programs or scripts that come pre-installed with the operating system. Attackers use them to collect credentials, move through networks, and steal sensitive data — often without adding any new malware.

Native binaries — or LOLBins — were never meant for cybercrime. IT and security teams trust these tools and use them every day. That trust and the lack of obvious malware allow attackers to hide for weeks or even months.

LOTL attacks are especially dangerous in complex hybrid, multi-cloud environments like healthcare, manufacturing, government, and financial services. These sectors often have legacy systems, limited visibility, and broad admin privileges.

This e-book shows how LOTL attacks work, why they’re effective, and how defenders can fight back — using visibility, segmentation, and controls that don’t depend on detecting malware alone.

Why have (LOTL) attacks become such a dominant threat?

A 2025 Bitdefender[2] review of 700,000 security incidents found that 84% of major breaches involved LOTL tactics. Ransomware has also embraced the approach. Modern gangs have moved past smash-and-grab encryption to multi-stage, stealthy operations that rely on trusted tools already in the environment.

Why the shift? Because LOTL works — and it’s hard to stop. Attackers can:

- Hide in plain sight, blending into routine admin activity and evading traditional defenses
- Adapt to any environment, from cloud platforms to legacy servers
- Exploit tools so essential that removing them would hurt daily operations
- Linger undetected long enough to map networks, spread, and steal data
- Evade antivirus and EDR by avoiding tell-tale malware files
- Move laterally with minimal noise, keeping a low profile until the damage is done

[1] U.S. Department of Health & Human Services. “Living Off the Land Attacks (TLP:CLEAR).” February 2023.
[2] Bitdefender. “How Analyzing 700,000 Security Incidents Helped Our Understanding of Living Off the Land Tactics.” June 2025.

Evolution of LOTL: two decades of tradecraft

Fileless malware and LOTL tradecraft may seem new, but they've been evolving for more than 20 years. What began with in-memory worms has grown into today's complex campaigns and zero-day exploits.

For defenders, it helps to know the key incidents where LOTL tactics played a central role — whether for espionage, destruction, or ransom:

2001	**Code Red & SQL Slammer Worms** Not classic LOTL, but these worms set the stage for in-memory execution. They exploited flaws in Microsoft IIS and SQL Server to run code in memory — no files written — a warning sign of today's fileless attacks.[3]
2017	**FIN7 Campaigns** The FIN7 group (Carbanak) hit hospitality, retail, and finance using PowerShell, WMI, and signed binaries. These were textbook LOTL operations — fileless and embedded in native tooling.[4]
2017	**NotPetya** NotPetya was a destructive global attack that used PsExec and PowerShell for lateral movement. It blurred the line between ransomware and cyberwarfare, and LOTL helped fuel its rapid spread.
2018–2021	**Ryuk Ransomware** Ryuk hit hospitals, municipalities, and enterprises, using PowerShell, WMI, and native tools for lateral movement.[5]
2020	**SolarWinds SUNBURST** In this renowned supply chain attack, attackers compromised the Orion software update, embedding malware into trusted software. They used WMI, PowerShell, and DNS tunneling to move laterally — hiding in plain sight. The U.S. formally attributed this attack to Russia's SVR.[6]
2021–2023	**LockBit Ransomware** LockBit hit critical infrastructure, including Accenture, healthcare, and government targets. It used native Windows tools — PowerShell, schtasks, PsExec, and WMI — to persist and spread without dropping malware.[7]
2023	**Volt Typhoon (China-affiliated APT)** Volt Typhoon targeted U.S. critical infrastructure, running almost entirely on LOTL — with legitimate tools like PowerShell, scheduled tasks, and command-line utilities to stay hidden.[8]
2023	**Medusa Ransomware** Medusa hit healthcare, education, and public sector targets. It used tools like schtasks and cmd.exe for lateral movement and persistence without relying on malware files.[9]
2025	**SharePoint ToolShell Exploitation** Attackers exploited two zero-days (CVE-2025-53770 and CVE-2025-53771) in on-prem SharePoint. State-backed groups deployed ransomware using built-in tools like PowerShell, BITSAdmin, and cmd.exe — no malware dropped.[10]

[3] U.S. Government Accountability Office (GAO). Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures (GAO-01-1073T). September 2001.

[4] MITRE. "FIN7 (Group G0046)." April 2024.

[5] Blumira. "Ryuk Ransomware Targets Healthcare Organizations." November 2020.

[6] CISA, NSA & FBI. "NSA-CISA-FBI Joint Advisory on Russian SVR Targets U.S. and Allied Networks." September 2021.

[7] Cybersecurity and Infrastructure Security Agency (CISA), FBI & NSA. "Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization (AA22-277A)." October 2022.

[8] CISA, NSA & FBI. "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection (AA23-144A)." May 2023.

[9] CISA, FBI & MS-ISAC. "#StopRansomware: Medusa Ransomware (AA25-071A)." March 2025.

[10] Microsoft. "Disrupting Active Exploitation of On-Premises SharePoint Vulnerabilities." July 2025.

Fileless malware: attacks with no footprint

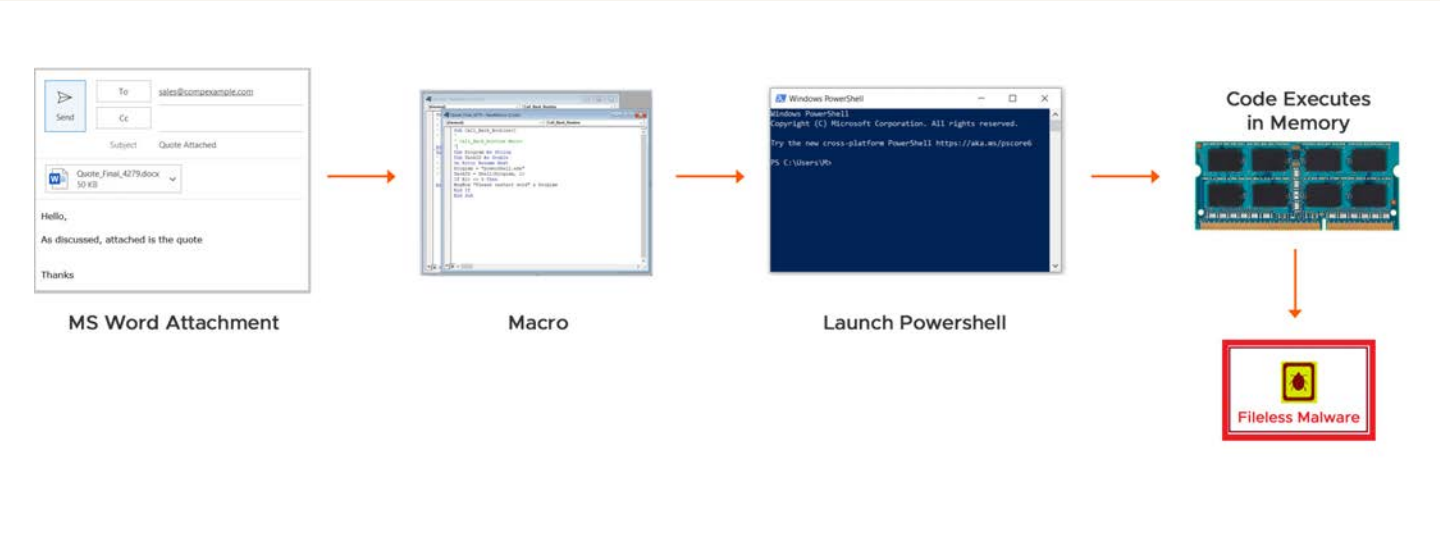
Fileless malware and living off the land (LOTL) attacks are a natural match — both avoid leaving a trail. Instead of dropping files onto a hard drive, attackers run their code directly in memory, often through trusted tools like PowerShell, WMI, or built-in scripting engines. This means there's no file for antivirus to scan, and in many cases, logs don't capture the activity.

By relying on tools already present in the operating system, attackers can blend into normal traffic and system activity. They can move laterally, harvest credentials, and exfiltrate data without triggering obvious alerts. This makes them hard to detect, hard to block, and even harder to prove after the fact.

Key advantages include:

- No custom kernel modules required
- Use of trusted, native OS tools
- Minimal system resource use
- No large malware files to deploy
- Difficult to detect in network traffic
- Limited forensic evidence left behind

The result is an attack that can persist for weeks or months, hiding in plain sight while quietly stealing or destroying valuable data.



AN EXAMPLE OF FILELESS MALWARE FLOW

LOTL across operating systems

While Windows operating tools are the most frequent LOTL target, attackers are also exploiting trusted, native tools on macOS and Linux.[11] Here's a look at commonly abused utilities across major operating systems:

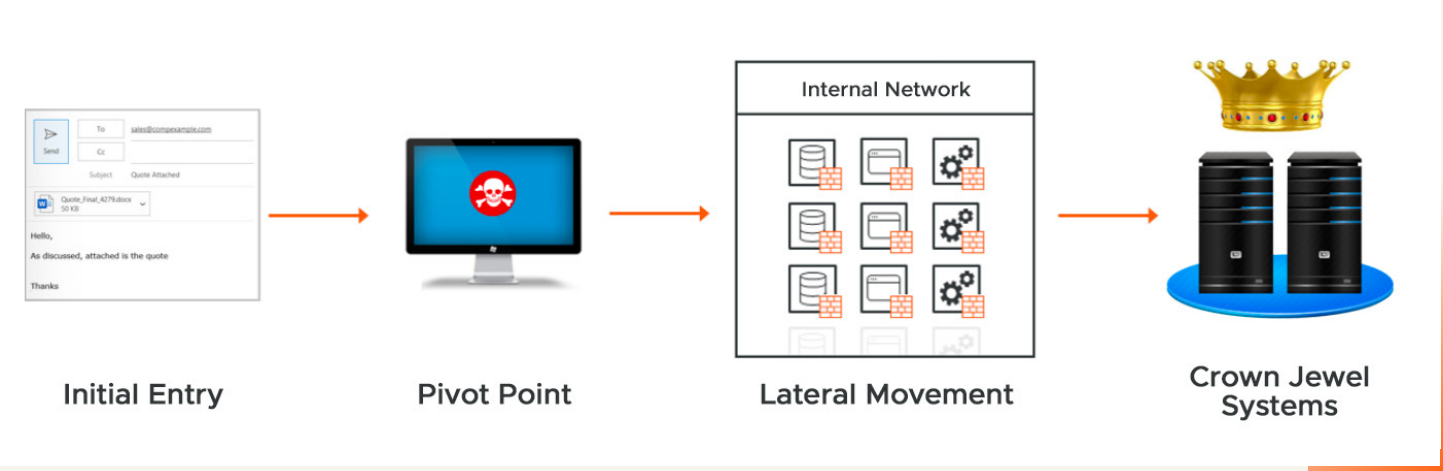
OPERATING SYSTEM	TOOL	PURPOSE IN ATTACK CHAIN
Windows	`PowerShell`	Reconnaissance, downloading payloads, executing commands
	`WMI`	Lateral movement, remote code execution
	`PsExec`	Executes commands across networked systems
	`netsh`	Alters firewall rules to allow malicious traffic
	`certutil`	Downloads and decodes payloads using a trusted binary
	`BITSAdmin`	Moves files and executes payloads over low-profile channels
	`schtasks`	Maintains persistence or triggers delayed execution
	`rundll32 / regsvr32`	Executes code via system DLLs to bypass application controls
macOS	`osascript / AppleScript`	Executes scripted tasks or commands; used for persistence
	`launchd / launchctl`	Loads background services or daemons at startup
	`cron`	Schedules recurring execution of scripts or payloads
Linux	`bash`	Executes shell scripts and commands, often in memory
	`cron`	Maintains persistence via scheduled task execution
	`ssh`	Enables lateral movement or remote access
	`systemd / init` scripts	Starts malicious services or scripts during boot

[11] Startup Defense. "Living Off the Land (LOTL) Attacks: The Invisible Threat Lurking in Plain Sight." August 2025.

How LOTL attacks unfold

While the LOTL tactic can do an extraordinary job of hiding inside normal activity, it usually unfolds like other breaches. Here's how they typically play out:

- **Initial access:** The attacker slips in via phishing, social engineering, insider threats, or another common method.
- **Reconnaissance:** Once inside, they map the environment — looking for weak points, assets, and paths to escalate.
- **Lateral movement:** Using native tools, they quietly hop between systems, avoiding alarms as they go.
- **Privilege escalation:** They grab admin access to unlock sensitive systems and deeper control.
- **Malicious activity:** With control in hand, they exfiltrate data, create backdoors, tamper with settings, or execute payloads.
- **Obfuscation:** All the while, they hide in plain sight and conceal their malicious activities.



THE ATTACK CHAIN: FROM INITIAL ENTRY TO CROWN JEWEL SYSTEMS.

Why lateral movement is central in LOTL attacks

After gaining initial access, attackers rarely stop at a single system. They use that foothold as a pivot point — moving laterally across the network in search of high-value targets such as databases and systems housing sensitive customer data. This lateral movement is a hallmark of living-off-the-land attacks. The native OS tools and protocols — such as SSH on Linux and Unix, or Remote Desktop Protocol (RDP) and WMI on Windows — let attackers remotely discover and access other systems without raising alarms. Once they've reached the crown jewel systems, the next phase begins: data exfiltration. And all of it can happen without deploying traditional malware.

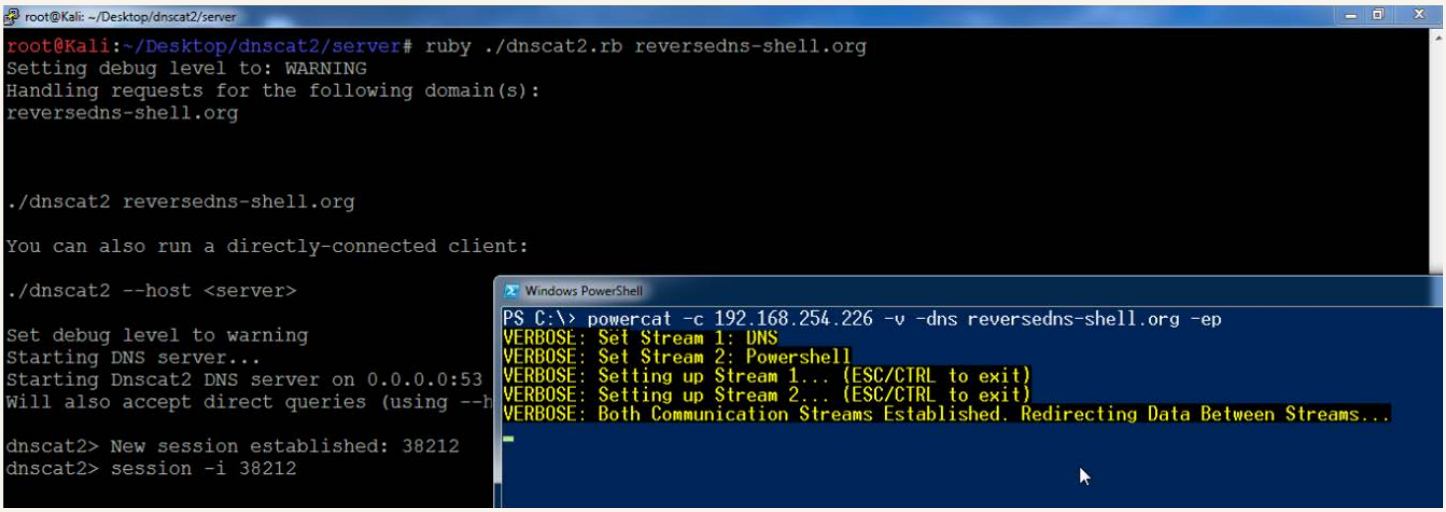
Data exfiltration: the final phase of a LOTL attack

After moving laterally to reach high-value systems, attackers finish by stealing the data. Sensitive files are quietly sent to their command-and-control servers.

In LOTL attacks, this step often blends into normal activity. Threat actors send stolen data through common protocols like DNS, ICMP, or HTTPS, so it looks like everyday traffic. For example, DNS tunneling tools can hide data inside DNS TXT records, slipping past standard alerts.

Because these protocols are trusted and used everywhere, spotting it is hard — especially when attackers hide their activity with obfuscation techniques.

Monitoring external data transfers is key to spotting exfiltration risks. Use tools that flag unusual workloads or large data movements and watch for traffic spikes, even if the total volume looks small. By comparing flow and byte counts, security teams can catch anomalies.



AN EXAMPLE OF A DNS TUNNELING TOOL USED TO HIDE DATA EXFILTRATION

Obfuscation techniques: staying hidden in plain sight

Attackers hide their actions by disguising commands and payloads.[12] A common trick is Base64 encoding, which turns readable commands into long strings of letters and numbers. Security tools have a harder time spotting threats, especially when the commands run through trusted tools like PowerShell or Bash.

They may also send data over encrypted channels such as HTTPS (TCP port 443), which are rarely blocked or closely inspected. When traffic is encrypted or disguised, even advanced defenses may have trouble telling safe and malicious activity apart. And once they're decoded, Base64-encoded commands run normally on the host device.

AN EXAMPLE OF BASE64 ENCODING

Staying power: how LOTL attacks maintain persistence

Fileless malware typically lives in memory — which means a system reboot would, in theory, wipe it out. But here's the catch: many targets, like critical servers, rarely reboot. And attackers know it.

To stick around even if a reboot does occur, threat actors often build in persistence. This ensures their tools or scripts automatically reload when the system restarts, allowing them to maintain access, move laterally, and continue malicious activity over long periods without being noticed.

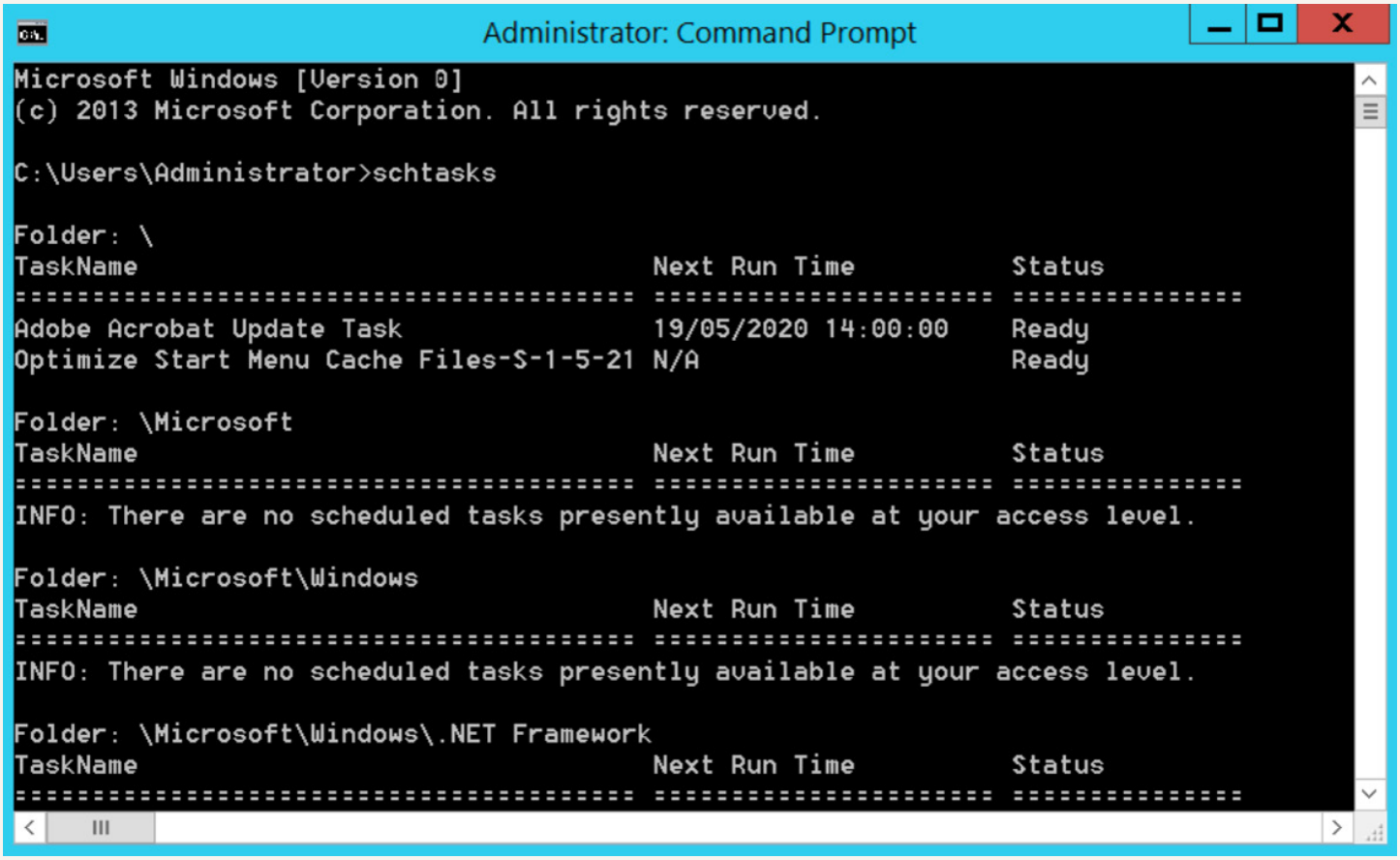
On Windows, attackers often use task scheduler (schtasks or at command) to trigger their code at startup. On Linux and Unix systems, they rely on startup scripts, cron jobs, or modifications to system services. These are all native tools, making them perfect for living-off-the-

[12] MITRE. "T1027: Obfuscated Files or Information." April 2025.

Why LOTL works so well for attackers

Living off the land gives attackers several clear advantages. With fileless malware, the attack stays light and leaves almost no footprint on the system. It runs in memory instead of on the hard drive, so normal scans often miss it.

These strengths make LOTL a favorite choice in many multi-stage attacks, from the first intrusion to final data theft.



A WINDOWS TASK SCHEDULER PERSISTENCE TECHNIQUE

Stopping LOTL requires visibility and instantly quarantining threats

Because LOTL attacks don't rely on traditional malware, stopping them means knowing what "normal" looks like. Security teams must be able to see how systems should communicate so that they can detect unusual behavior and quarantine threats in real time.

Key defenses include:

- **Lateral movement detection.** Track how systems talk to each other to catch attackers moving inside the network.
- **Behavioral threat detection.** Use analytics to flag abnormal use of native tools that might blend in with routine work.
- **Alert prioritization.** Filter out the noise and focus on suspicious patterns in trusted processes.
- **Rapid containment using segmentation.** Isolate compromised assets quickly, protecting critical assets, without waiting for malware signatures, to stop LOTL before it spreads.
- **Protecting the crown jewels.** Apply segmentation to shield critical assets, cut off attack paths, and make malicious activity easier to detect.

LOTL security: using built-in defenses for Zero Trust

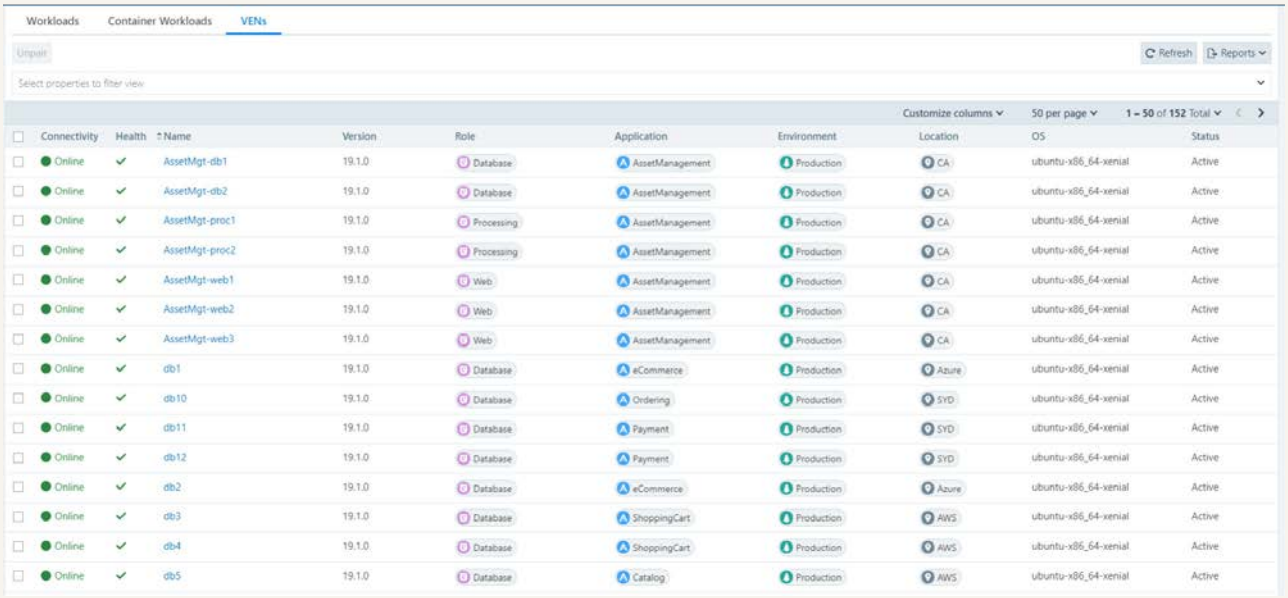
Attackers use the tools already on your systems. Defenders can do the same — but to protect, not to do harm. Living-off-the-land security (LOTLS) means using the security features built into modern systems to apply Zero Trust without adding complexity.

Examples:

- Windows: Windows Filtering Platform (WFP)
- Linux and Unix: IPTables
- AIX and Solaris: IPFilter

These built-in firewalls can be managed from one place — on-premises or in the cloud — to control traffic on each workload, not just at the edge of the network.

By labeling assets by environment, app, or role, teams can group workloads in a logical way. They can then write, test, and model policies before turning them on without breaking normal operations or depending on network layout.



AN EXAMPLE OF THE WINDOWS FILTERING PLATFORM (WFP)

Some systems also have built-in IPSec, which encrypts traffic between workloads. This is a big help for older apps that don't have encryption.

For LOTLS to work well in Zero Trust, it should give teams:

- Clear, context-rich telemetry
- A visual map of workload traffic
- Built-in firewall and IPSec support
- Central control that works at scale

And it should do all this without extra kernel modules or agents. By "living off the land," defenders get speed, scale, and performance from tools they already have. This uses native defenses to enforce microsegmentation policies, blocking lateral movement and stopping threats before they reach key systems.

Turn insight into action and protect your organization today.

LOTL and fileless attacks thrive in flat networks and any hybrid cloud environments that lack strong lateral movement controls.

Illumio stops these tactics in their tracks — without adding complexity or slowing you down.

Talk to our security experts today to see how you can:

- Assess lateral movement risks
- Enforce policy and detect attacks
- Contain threats instantly

Schedule a demo and learn how Illumio can help you stop LOTL attacks before they spread.

Appendix

Major living-off-the-land cyberattacks (espionage + ransomware)

Attack / Campaign	Year	Type	LOTL Tools/ Commands Used	Description
Frodo Virus	1989	Early Fileless Malware	Memory-resident only	One of the first fileless viruses; lived in memory, intercepted DOS calls.[13]
Code Red Worm	2001	Worm / DoS	In-memory only, no files	Exploited IIS buffer overflow; executed in memory, evaded signature-based detection.[14]
NotPetya	2017	Destructive (pseudo-ransomware)	PsExec, WMI, PowerShell	Used legitimate tools for lateral movement; caused massive disruption in Ukraine and beyond.[15, 16]
FIN7 Campaigns	2017–2018	Espionage / Financial	PowerShell, WMI, signed binaries	Targeted retail and hospitality sectors using fileless techniques.[17]
Ryuk Campaigns	2018–2021	Ransomware	PowerShell, net use, WMI	Used manual intrusion and LOTL tools for lateral spread, paired with TrickBot access.[18]
Maze / Egregor	2019–2021	Ransomware + Data Exfiltration	PowerShell, netsh, task scheduler	Blended data theft and encryption; LOTL used for lateral movement and evasion.[19]
SolarWinds SUNBURST	2020	Espionage (APT)	PowerShell, WMI, DNS tunneling	Nation-state supply chain attack. Used native tools to blend in and avoid detection.[20]
Conti (HSE Ireland)	2021	Ransomware	PsExec, WMI, PowerShell	Used native Windows admin tools to encrypt Irish health systems. [21]

[14] U.S. Government Accountability Office. "Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures (GAO-01-1073T)." August 2001.

[15] Cybersecurity and Infrastructure Security Agency (CISA). "Alert TA17-181A: Petya Ransomware," June 2017.

[16] Wired. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." August 2018.

[17] MITRE ATT&CK®. "FIN7 (Group G0046)." April 2024.

[18] ANSSI – Agence nationale de la sécurité des systèmes d'information (France). "Ryuk Ransomware: French Cybersecurity Notice—PDF." February 2021.

[19] U.S. Department of Health & Human Services. "Maze Ransomware." June 2020.

[20] CISA. "Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise." May 2021.

[21] U.S. Department of Health & Human Services. "Lessons Learned from the HSE Cyber Attack." March 2022.

Attack / Campaign	Year	Type	LOTL Tools/ Commands Used	Description
LockBit (Accenture, others)	2021–2023	Ransomware	PowerShell, schtasks, rundll32	Used fileless persistence and native task scheduling for infection. [22]
BlackCat / ALPHV	2022–2024	Ransomware	PsExec, BITSAdmin, PowerShell	Used advanced, modular fileless payloads via native tooling.[23]
Volt Typhoon	2023	Espionage (China-affiliated APT)	PowerShell, netsh, cmd, schtasks	Used only LOTL tools to hide in critical U.S. infrastructure. No malware.[24]
SharePoint ToolShell Attack	2025	Ransomware	PowerShell, BITSAdmin, cmd.exe	Used zero-day (CVE-2025-53770); no malware files — all execution via trusted tools.[25]

[22] U.S. Department of Health & Human Services. "Maze Ransomware." June 2020.
[23] Trend Micro. "Attackers in Profile: menuPass and ALPHV/BlackCat." June 2024.
[24] Microsoft Threat Intelligence. "Volt Typhoon Targets US Critical Infrastructure with Living-Off-the-Land Techniques." May 2023.