How analyzing 700,000 security incidents helped our understanding of Living Off the Land tactics - Help Net Security

By Help Net Security

Published: 2025-07-01 · Archived: 2026-04-05 20:18:33 UTC

This article shares initial findings from internal Bitdefender Labs research into Living off the Land (LOTL) techniques. Our team at Bitdefender Labs, comprised of hundreds of security researchers with close ties to academia, conducted this analysis as foundational research during the development of our GravityZone Proactive Hardening and Attack Surface Reduction (PHASR) technology.

The results reveal adversaries' persistent and widespread use of trusted system tools in most significant security incidents. While this research was primarily for our internal development efforts, we believe these initial insights from Bitdefender Labs are valuable for broader understanding and we are sharing them now, ahead of a more comprehensive report.

Data analysis and initial findings

To figure out exactly how common LOTL binaries are, we analyzed 700,000 security incidents from our Bitdefender GravityZone platform along with telemetry data (legitimate usage) from the last 90 days. Security incidents were not simple alerts, but correlated events, and we analyzed the whole chain of commands to identify how frequently attackers are using LOTL binaries. The result? 84% of major attacks (incidents with high severity) involved the use of LOTL binaries. For validation, we also examined our MDR data and found a consistent trend: 85% of incidents involved LOTL techniques.

The most abused tool? Netsh.exe

While LOTL tools are a well-covered topic (including our tech explainer), most prior analysis has been based on experience, not hard data. We based our analysis on the frequency of tools usage, instead of how much damage they could cause. We were hoping to discover binaries that are frequently abused yet rarely used for legitimate purposes.

What was quite visible immediately is that the tools popular with attackers are also very popular with administrators. The usual suspects like *powershell.exe*, *wscript.exe*, and *cscript.exe* were all present. However, one of the more surprising findings was that *netsh.exe* was the most frequently abused tool, appearing in one-third of major attacks. While checking firewall configurations is a logical initial step for attackers, this clearly demonstrates how data analysis can spotlight trends that human operators might instinctively disregard.

1. Netsh.exe – Administrators use this command-line utility for management of network configuration, including firewalls, interfaces, and routing.

2. PowerShell.exe – Often referred to as the "Swiss Army Knife" of Windows management, PowerShell is a versatile command-line shell and scripting language.

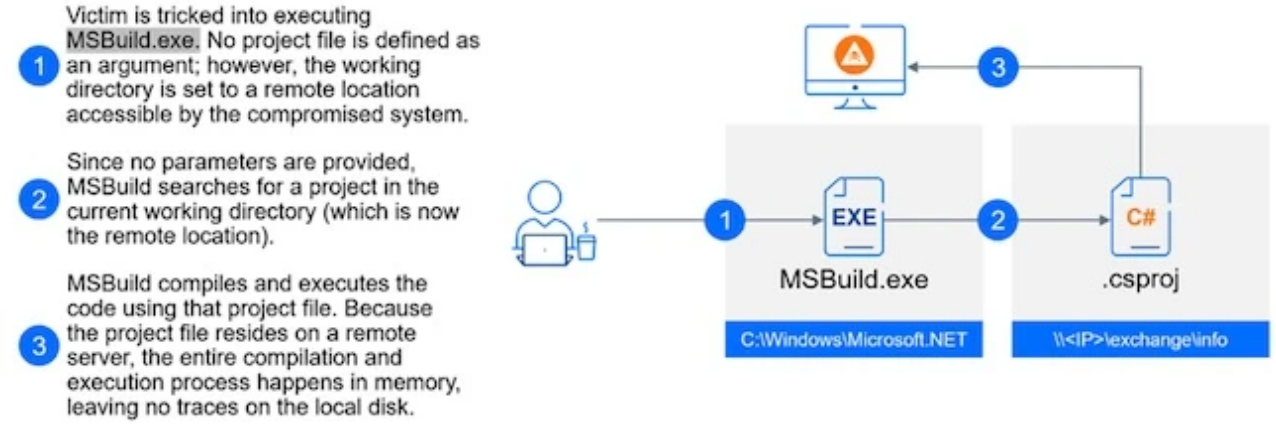
3. Reg.exe – This command-line tool allows administrator to query, change, add, or remove registry entries, and threat actors frequently use it to establish persistence.

4. Csc.exe – The Microsoft C# Compiler is a command-line tool for compiling C# source code into executable assemblies (.exe files) or dynamic link libraries (.dll files).

5. Rundll32.exe – This system utility loads and executes functions exported from DLL files. Often used for DLL sideloading attacks.

As mentioned earlier, the popularity of tools among attackers often reflects their popularity with legitimate administrators. This general trend held true for the most part, but some notable exceptions appeared. Specifically, threat actors leverage tools like *mshta.exe*, *pwsh.exe*, and *bitsadmin.exe* but administrators rarely use them.

While most LOLBins are very familiar to those experienced in system administration, there is another category of abused tools that is not so well understood. These tools, such as csc.exe, msbuild.exe (Microsoft Build Engine), or ngen.exe (.NET Native Image Generator), are primarily used by developers, and can fly under the radar of security monitoring focused solely on traditional system administration binaries.



An example of MSBuild.exe abuse from our Unfading Sea Haze research

The temptation of simple solutions

Our research revealed another unexpected observation: The widespread use of *PowerShell.exe* in business environments. While nearly 96% of organizations in our dataset legitimately utilize PowerShell, our initial expectation was that its execution would be limited primarily to administrators. To our surprise, we detected PowerShell activity on a staggering 73% of all endpoints. Further investigation revealed that PowerShell is frequently invoked not only by administrators (and their pesky logon/logoff scripts), but also by third-party applications running PowerShell code without a visible interface.

A similar pattern emerged with *wmic.exe*. This tool, popular around the year 2000, has largely been superseded by PowerShell for administrative purposes – and is slated for decommissioning by Microsoft. However, we were

surprised to find its regular usage across many workstations. Analyzing the data, it became clear that *wmic.exe* is still commonly employed by a multitude of third-party applications to gather system information.

Geographical analysis also revealed intriguing differences in tool usage. For example, *PowerShell.exe* showed a notably lower presence in APAC (Asia-Pacific), at just 53.3% of organizations in our dataset. This stands in sharp contrast to EMEA, where our analysis indicated a much higher adoption rate of 97.3%. Conversely, while PowerShell usage was lower in APAC, *reg.exe* was more frequently present in this region compared to all other geographical areas.

This underscores the importance of nuanced understanding, as even tools appearing outdated or unused can be critical for specific functions and disabling them can cause unforeseen disruptions.

You can't live with them, you can't live without them

The LOTL reality that we "can't live with them, and can't live without them" directly informed the development of our Bitdefender GravityZone Proactive Hardening and Attack Surface Reduction (PHASR) technology. Recognizing the inherent risks and potential for disruption in simply blocking these essential tools, PHASR adopts a more nuanced and intelligent approach: individualized endpoint hardening through action-based control.

PHASR goes beyond blocking entire tools, it also monitors and stops the specific actions attackers use within them. By analyzing the behavior of processes like *powershell.exe*, *wmic.exe*, or *certutil.exe*, PHASR distinguishes malicious intent from legitimate use. For instance, PHASR allows PowerShell to execute regular scriptswhile proactively blocking its attempts to run encrypted commands or tamper with critical system configurations.

Consider *WMIC.exe* again. Instead of blocking the entire tool, which could disrupt legitimate operations, PHASR differentiates between its legitimate use for system information retrieval and its abuse for lateral movement or process manipulation. This action-level blocking, combined with the layered analysis of user and attacker behavior, enables tailored protection without business disruption.

PHASR's effectiveness lies in its architecture, which incorporates hundreds of granular rules informed by known attacker playbooks and our extensive threat intelligence. The engine continuously learns by establishing a baseline of typical user and application behavior on each endpoint. This learned behavior is then constantly compared against known malicious patterns and emerging threats. Intelligent analysis allows PHASR to not only detect and report suspicious activity but also to proactively block access to specific tools or even parts of their functionality when their use deviates from the established baseline and aligns with malicious indicators. This proactive blocking occurs seamlessly, without requiring constant manual policy adjustments or fine-tuning, ensuring robust protection against even novel LOTL attacks.

Conclusion

The words of "gg," the BlackBasta ransomware group leader, chillingly underscore the central challenge revealed by our analysis of 700,000 security incidents. *"If we use standard utilities, we won't be detected… We never drop tools on machines."* The staggering 84% prevalence of Living off the Land (LOTL) techniques in major attacks directly validates this adversary perspective.

Attackers are demonstrably successful in evading traditional defenses by expertly manipulating the very system utilities we trust and rely on daily—and threat actors operate with a confident assertion of undetectability. This stark reality demands a fundamental shift towards security solutions like Bitdefender's PHASR, which moves beyond blunt blocking to discern and neutralize malicious intent within these tools.
