Is an Attacker Living Off Your Land?

By Samuel Greengard

Published: 2021-06-16 · Archived: 2026-04-05 19:00:17 UTC

(Image: Riverwalker via Adobe Stock)

Malware – and all of its various forms, including ransomware – has grown increasingly stealthy and sophisticated in recent years. Also on the rise: Its ability to fly under cybersecurity software's radar.

One of the primary reasons detecting and stamping out malware is so difficult is the rise of an attack method called living off the land (LotL). Despite conjuring up idyllic images of urban farming or sustainability, the term refers to a group of techniques that typically execute in shell code or scripts running in memory.

Attackers who "live off the land" make use of a system's own tools and utilities to conduct malicious activity. With these attacks, which don't use easily detectable malicious files, an attacker can lurk within a computer or network and avoid discovery by security tools.

Even if an attack is discovered, the binaries used are exceptionally difficult to eradicate. As a result, a LotL attack is particularly risky for victims.

Living Off the Land: A Brief History

The concept of using fileless malware, or malware that relies on legitimate programs to attack, first appeared around the start of the current century. Early examples of this approach include malware with names like Frodo, Code Red, and SQL Slammer Worm. However, these payloads were more of a nuisance than a real threat. Then, in 2012, a banking Trojan named Lurk appeared. Although it wasn't terribly sophisticated, it demonstrated LotL's potential.

In 2013, security researchers Christopher Campbell and Matt Greaber coined the LotL term to describe malware that hides within a system and exploits legitimate tools and utilities to cause damage. Over the past few years, the

scope and sophistication of these attacks has grown. In fact, as security firms have become better at identifying and blacklisting malicious files, fileless attacks have moved into the mainstream.

How Does Living Off the Land Work?

In a LotL attack, adversaries take advantage of legitimate tools and utilities within a system. This might include PowerShell scripts, Visual Basic scripts, WMI, PSExec, and Mimikatz. The attack exploits the functionality of the system and hijacks it for nefarious purposes. It may include tactics like DLL hijacking, hiding payloads, process dumping, downloading files, bypassing UAC keylogging, code compiling, log evasion, code execution, and persistence.

Cybercriminals use different methods and unleash different types of malware that fall into the general category of LotL. In many cases, they tap tools such as Poshspy, Powruner, and Astaroth that take advantage of LOLBins and fileless techniques to evade detection. Most attacks involve Windows binaries that mask malicious activities; however, LotL attacks can also affect macOS, Linux, Android, and cloud services.

The reason this approach works so well is because resources such as PowerShell and Windows Scripting Host (WScript.exe) offer capabilities that far exceed the needs of most organizations—and many of these features aren't switched off or removed when they're not required by an organization. Overall, more than 100 Windows binary tools represent a serious risk, according to GitHub.

What Do LotL Attacks Look Like?

Once attackers have invaded legitimate tools, such as PowerShell, they're able to tap other legitimate processes and code, including built-in scripting languages such as Perl, Python, and C++.

For example, an attacker might create a script that includes a list of targeted machines and, together with a PSExec account with executive privileges, copy and execute malware into peer machines. Another possible method of attack is leveraging a logon and logoff script via a Group Policy Object (GPO) or abusing the Windows Management Interface (WMI) to mass-distribute ransomware inside the network.

A similar approach uses malware to inject malicious code into a trusted running process like SVCHOST.EXE or use the Windows RUNDLL32.EXE application. This makes it possible to encrypt documents from a trusted process, cybersecurity firm Sophos reports. This tactic can evade some anti-ransomware programs that do not monitor or are configured to ignore encryption activity by default Windows applications.

Ransomware may also run from a NTFS Alternate Data Stream (ADS) to hide from both victim users and endpoint protection software, cybersecurity firm Malwarebytes Labs points out. Oftentimes, the entire attack takes place within a few hours or during the night when staff pay less attention to IT systems. Once the malware has encrypted files, the recipient winds up with a locked screen and a ransom note.

These attacks often appear to come out of nowhere because the actual file encryption is performed within a trusted Powershell.exe component. As a result, endpoint protection software may not detect the process because it appears to be legitimate, according to Sophos.

One of the most widely publicized LotL attacks occurred in 2017, when so-called Petya malware appeared. It initially infected a software accounting program in the Ukraine and then spread across companies. More recently,

the SolarWinds attack, a.k.a. SUNBURST, used LotL and other methods to plant malware in one of the security firm's software patches.

Reducing Risk Is Critical
There's no simple way to avoid the risk of an LotL attack. It's also difficult to determine who is initiating the attack because of the stealthy nature of the malware.

In general, the best defense is to ensure that unneeded components are switched off or removed from systems. Other strategies include setting up application whitelisting where possible, tapping behavioral analytics software, patching and updating components regularly, using multifactor authentication, and continuing to educate users about the risks associated with clicking email links and opening attachments.

About the Author

Freelance Writer

Samuel Greengard writes about business, technology, and cybersecurity for numerous magazines and websites. He is author of the books "The Internet of Things" and "Virtual Reality" (MIT Press).
