ActZero

THREAT INSIGHT

What is a "Living off the Land"(LotL) attack, and how can you manage the risk?

Attacks are bad enough when you're able to quickly detect and stop them, but when they get in and just sit there, they can be downright scary.

Lately, we're seeing a resurgence in threat actors leveraging an attack method called "Living off the Land", or LotL. In their 2020 Cyber Threatscape Report, Accenture provides a very clear picture of the increased use of LotL techniques by state-sponsored actors and other criminal groups. Essentially, adversaries are more often using legitimate admin tools to compromise secure environments undetected. The first access is typically accomplished by exploiting a vulnerability or tricking an end user. However, unlike traditional non-LotL attacks where the threat actor gets the endpoint to install some software (an executable virus), the adversary drops no files or executable. Rather, it uses existing tools on a victim's machine, drops malicious scripts or exploitive code code to use it against them. On Windows, most LotL attacks will use a malicious PowerShell at some point. Whereas on Linux, a LotL attack on a web server may use a webshell written in php. LotL may even use wget to launch a superset of fileless attacks. These are all within whitelisted system admin tools.

As the moniker Living off the Land would indicate, they're in no rush to 'cash in', operating with a 'canary in the coal mine perspective. "If the canary is still alive in a month", they know they're good to continue their attack largely undetected. Once the threat actors have access to your environment, they can run almost anything. It can reside in the RAM of your endpoint, as above, or it could even infiltrate a web server, for example, once run via Powershell. The actor uses this undetected dwell time to learn the infected host's environment, network, customers, and partners.

Why are Living off the Land attacks so successful?

Simply put, most detection solutions like Anti-virus, Anti-Spam Gateways and Next Generation Firewalls fail to detect LotL as they simply recognize the threat as 'Potentially Unwanted Programs' (PUPs) and 'Potentially Unwanted Modifications' (PUMs) at best, and don't block it. No alerting occurs as the applications involved are regularly used by users. When there is a PUP or PUM detection, they are often lost due to false positives. Threat actors leverage this lack of detection and dwell until detected by threat hunting.

What is the business impact?

LotL is very hard to detect in an automated fashion because the tools used are not malicious. Often they are core business tools. It's their stealth and how the tools are being used that make them malicious. While in your network adversaries can do considerable damage. From shutting down applications and systems, to stealing credentials and using them for lateral movement, to exfiltrating stolen data, this form of attack can have serious consequences. LotL attacks can also affect how you interact with peers/partners/etc., and 'jump up' to them through techniques like email compromise. You also might simply be patient zero, or the pawn used to take down your valuable business partner. It's no wonder that LotL is an often-used tool of choice to infiltrate the most secured and locked down businesses, where a max payout is achievable.

What proactive measures can you take? Unfortunately, there is no simple hardware or software solution for LotL attacks.

IT admins can start by implementing some partial detections. Use Application Control to prevent misuse of system tools admins, set software restrictions on each device which helps prevent things from running in places they shouldn't (Temp data and App data), implement rigid Endpoint Configuration and Management, or use implement endpoint behavior detection tools to block attacks. When it comes to detections, you could get hung up in the validation process, but identifying user anomalies like non-admin users setting up a Firewall Threat Defense are critical. Or, identifying when an executable shouldn't be running in a certain environment. Make no bones about it, this is very tough to do and will result in productivity impacts to your team if done at scale alone. Check out this article for some other tips and tricks.

You CAN try to manage LotL risk yourself, but HAVE you? WILL you?

Some choose to take on LotL themselves by building out a SOC, but the quantity of logs that need to be reviewed is immense, especially across multiple clients. Others turn to solutions that proclaim to offer Machine Learning (ML) and Artificial Intelligence (AI) capability that will solve LotL, but AI and ML alone can only pare down the data. Luckily, our ActZero customers get real, highly-trained, expert Threat Hunters as human-on-the-loop intervention.

Our threat hunters digest all of our ML output and provide the additional human intelligence to detect anomalies in whitelisted behaviours - like those presented by LotL footprint - that even ML and AI don't yet have the intuition to do. Maintaining good cybersecurity hygiene is also important. Our Hygiene report identifies risks, and provides actionable intelligence on how to mitigate them.

And finally, our optional vCISO solution can help you set up a Software Restriction Policy so that your unused or vulnerable apps can't serve as a fileless vector.

While there's no guarantee of catching all LotL threats, you can be assured that with ActZero's MDR, you've given yourself the best chance of success.

REQUEST A DEMO

Email: info@actzero.ai
Phone: +1.855.917.4981