When Good Tools Break Bad: Living off the Land (LotL) Attacks

A **Living off the Land (LOTL)** attack is a cyber-attack technique where threat actors exploit **legitimate, pre-installed operating system utilities, administrative tools, and trusted applications** to execute malicious operations. Instead of introducing external files or custom malware that could trigger defensive alerts, attackers use the system's own environment to hide in plain sight.

Detecting a trusted tool doing something malicious is like finding a specific needle in a shipping container of needles. Since you can't simply rely on what the file is (since powershell.exe or certutil.exe are completely legitimate), you have to look at **context, intent, and behavior.**

So how do you find this in your environment? Ask four simple questions.

Who sent you? • What are you saying? • Who are you talking to? • Is this normal for you?

1 "Who Sent You?" (Parent-Child Process Relationships)

In an operating system, programs don't just appear out of nowhere; they are launched by other programs. The relationship between the parent program and the child program is one of the most reliable ways to spot a good tool breaking bad.

- **Normal Behavior:** explorer.exe (the Windows desktop interface) spawns notepad.exe because a user double-clicked a text file.
- **Breaking Bad Behavior:** outlook.exe (Microsoft Outlook) or winword.exe (Microsoft Word) suddenly spawns powershell.exe or cmd.exe. There is almost zero legitimate reason for a word processor to launch a command-line interface.

2 "What are You Saying?" (Abnormal Command-Line Arguments)

When system administrators use tools like PowerShell, they write clear, standard scripts. When malicious actors use them, they try to hide their tracks directly inside the command line using specific flags and obfuscation.

Trusted applications break bad when they use arguments designed to hide activity:

- **Hidden Windows:** Running a tool with -WindowStyle Hidden or -W Hidden so the user can't see a window pop up.
- **Bypassing Execution Policies:** Using -ExecutionPolicy Bypass or -EP Bypass to force PowerShell to run unauthorized code.
- **Base64 Encoding:** Using -EncodedCommand followed by a massive string of random-looking characters (e.g., aW52b2tlLXdlYnJlcXVlc3Q...). This is a huge red flag; it means the attacker is trying to hide their malicious script from text-based logging.

3 "Who are You Talking To?" (Unusual Network Activity)

Many built-in administration tools have no business talking to the public internet, or at least not to unverified, external IP addresses.

- **Normal Behavior:** certutil.exe connects to a known Microsoft domain to verify a security certificate.
- **Breaking Bad Behavior:** certutil.exe connects to a random, newly registered IP address in another country to download a .txt file (which is probably an encrypted malware payload).
- **The Notepad Test:** If notepad.exe or calc.exe (Calculator) suddenly requests an outbound internet connection, it's a definitive sign of **process injection**—an attacker has forced malicious code to run inside the memory space of that trusted app.

4 "Is This Normal for You?" (User Context and Baselines)

Behavioral analytics software creates a baseline of what "normal" looks like for every user account and system in a network. When a trusted tool violates that baseline, it has probably broken bad.

- **The HR Account:** If a computer belonging to someone in Human Resources suddenly opens cmd.exe and runs network discovery commands like net view, whoami, or nltest /dclist, it triggers an immediate alarm. HR employees don't map network domains; attackers pretending to be HR employees do.
- **Time Anomalies:** A trusted backup script running at 2:00 AM is normal. A trusted administrative tool suddenly executing a bulk file-read command on a sensitive database at 2:00 AM on a Sunday is not.

We need these tools to administer our systems properly, but keep an eye out for Breaking Bad.

THE ATOM GROUP

New Hampshire DoIT

The Municipal Cyber Defense Grant is a collaboration between The ATOM Group, LLC, and the New Hampshire Department of Information Technology. It serves all New Hampshire-based municipal governments, schools, and public sector organizations. For more information about the MCDP Program and the free services we provide, please visit us at https://www.theatomgroup.com/mcdp