

# LIVING OFF THE LAND ATTACKS

**How Adversaries are Using Native System Files  
Against You and What You Can Do to Block It**



# Introduction

---



## What Hidden Dangers are Lurking Within Your Systems?

Ever had a termite problem or know someone who has? Even though they seem small, they can do some major damage. Termites destroy wood by eating from the inside out. The destruction is often difficult to spot because these insects are hidden within the foundational structure of your home.

Most people are simply not trained to notice the subtle clues that indicate a much larger problem with the structural integrity of a house until it's too late.

You didn't invite them in. And you certainly don't want them to stay. But termites are opportunists, and they are living off the land you've provided.

Cybercriminals are like termites. They burrow in and start eating.

These adversaries see computer systems and networks as opportunities to live off the land. Once inside, they nibble away at your data by leveraging native tools already present in your system.

Working undercover, they hide their movement and infiltrate other systems on your network. Their use of legitimate tools makes it difficult to spot their activities until you've experienced significant loss.

## What is Living off the Land (LOTL)?

Living off the land (LOTL) is a technique widely used by attackers that involves the use of native tools and software to carry out malicious activities. They use legitimate tools like Microsoft-signed files and system launcher processes to hide and blend in with everyday network activity. This type of attack is also known as a malware-free attack.

**75% of attacks used to gain initial access to systems and networks were malware-free.**

**- 2024 Global Threat Report, CrowdStrike**

## Adversaries are Working Undercover

To avoid detection by endpoint security solutions, cybercriminals are moving away from malware and malicious attachments toward more subtle and effective attack methods. They are looking for gaps in protection and utilizing methods like credential phishing, password spraying, and social engineering to get into a system. Once the adversary has legitimate credentials, they can log in undetected and continue to harvest data for exploitation.

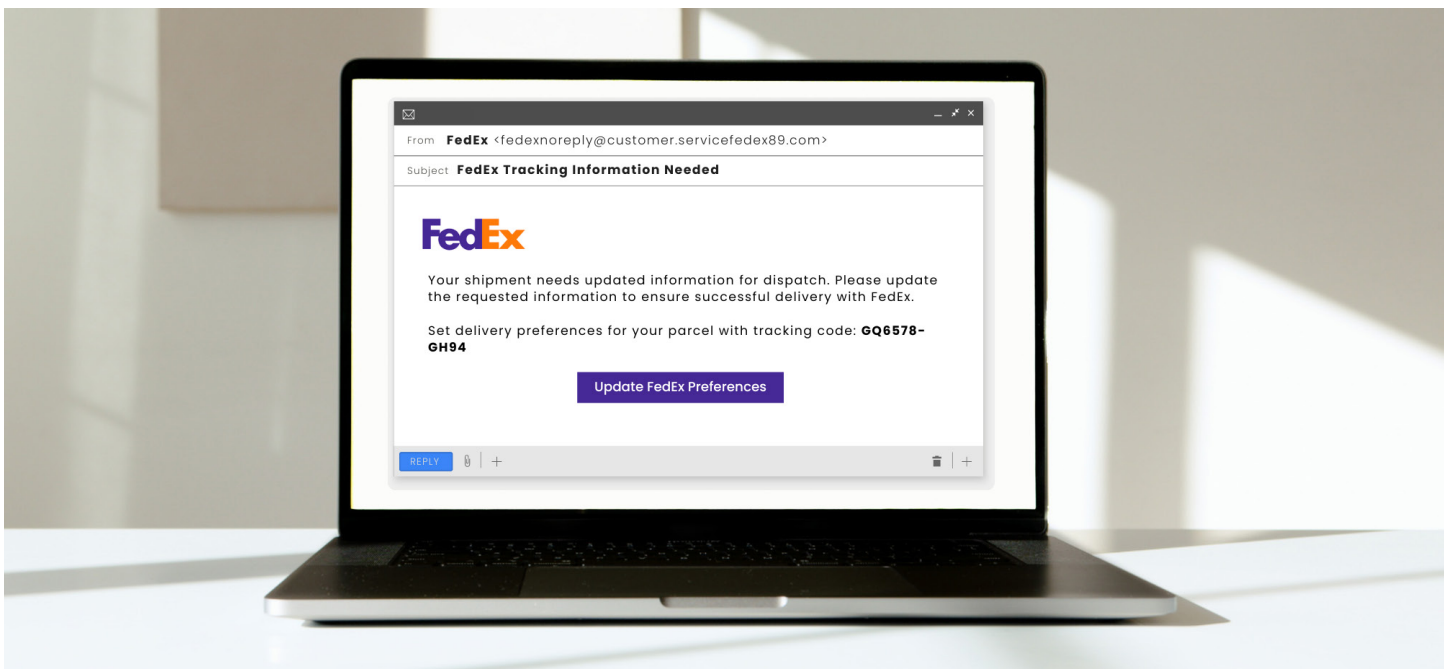
**Data breaches initiated with stolen or compromised credentials take nearly 11 months to identify and contain.**

**- Source; IBM Security, 2023 Cost of a Data Breach Report**

# How LOTL Attacks Evade Your Defenses and Deliver Payload to Attackers

## Preying on Human Emotions

Cybercriminals often start their attacks by preying on human emotions.



This scenario may sound familiar. Picture this:

You receive an email or a text from FedEx. The message states that you have a package delivery that needs to be scheduled. Included in the message is a tracking code and a link. Perhaps you really are waiting for something—and it's urgently needed—so you ignore your gut feeling that this message seems a little off. You click the link, and it takes you to a "FedEx" page where it asks you to fill in your username and password.



If you entered your credentials, the scammer now has your account information—which may include your company credit card number or other sensitive information.

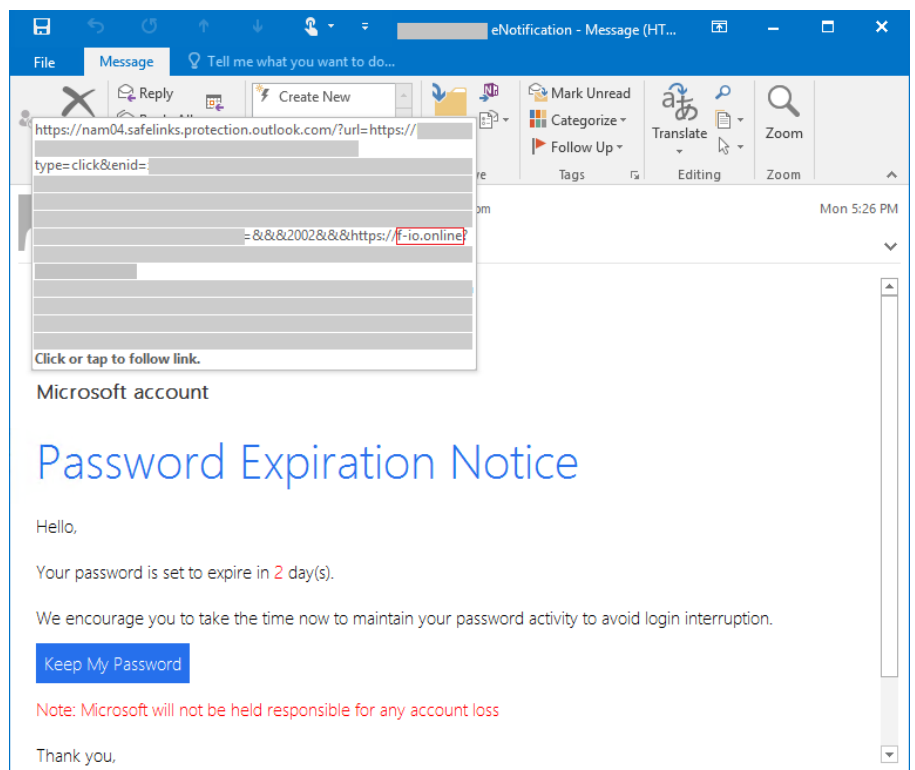
Using those stolen credentials, bad actors can now log into your FedEx account and legitimately gain access.

## Relying on Human Error

**95% of all cybersecurity issues can be traced to human error.**

**– Source: 2022 Global Risks Report, World Economic Forum**

Another common credential phishing scam involves your Microsoft 365 account at work. Impersonating Microsoft, adversaries start by sending you an email about your account and try to lure you into clicking a malicious link. For example, the email may state that your password will expire in 2 days and urges you to click a “Keep My Password” button to prevent account loss.



Once you click the link, threat actors use open redirects from legitimate domains to take you to an attacker-owned infrastructure where they can harvest your credentials and later gain a foothold in your system.

**Some threat actors gain access by injecting malicious code or cross-site scripting into web browsing to open vulnerabilities in your system.**

## Exploiting Known Vulnerabilities in Your System

Once inside your system, attackers know exactly where to go and hide while they dig for information. They seek out popular IT administration tools, Microsoft developer tools, and other system files and use them to their advantage.



Threat actors manipulate commands, execute processes, modify source codes, and establish pathways to move throughout your network. Because they are using files that have special validation or Microsoft-signed certificates, it masks their movements.

### How do threat actors escape detection in LOTL attacks?

- » Antivirus is programmed to look for **bad files** and **signatures**.
- » Endpoint detection and response (EDR) looks for **malicious activity**.
- » LOTL attacks are **fileless** and they operate within **normal system activity**.

### How threat actors get their reward:

Now the attacker really starts feasting as they take advantage of the time and anonymity they've established.

### Here are some of the methods they use to get their loot:

- » Launching executables that reveal sensitive information including personal identifying information and other system credentials.
- » Creating their own accounts to maintain system access.
- » Escalating privileges so they can get inside other accounts and systems.
- » Gaining domain administrator privileges to pull password data for the most powerful systems.

## What motivates them? What is the end game?

Some adversaries use the information they gain to further their attack while others sell the stolen information to other bad actors. There really is no rhyme or reason.

It doesn't matter the size of your organization. It doesn't matter if you're based in New York City or rural Iowa. It's doesn't matter if you're a financial institution, school, or nonprofit dedicated to helping the homeless.

**Cybercriminals are opportunists.** They do not discriminate. They will use any vulnerability and exploit any opening to get what they want: credentials, data, identities. These items all have monetary value.

## Looking for Easy Money

There are more than **1 billion Windows installations** around the globe.

If an adversary nets just \$100 from each successful data breach, they only need to be successful .001% of the time to net \$1 million.



# LOTL Attack Tools: A Quick Reference Guide

---



## What is fileless malware?

**It's a sneaky way for cybercriminals to get access into your system through the back door. Instead of installing malicious files that can be detected by Antivirus software, this type of memory-based attack activates tools already built into your operating system and works under the "protection" of these trusted files.**

Let's explore some of the tools these LOTL attackers are using against us.



## LoLBins

- 🔒 **What:** Binaries are non-malicious files that are local to the operating system
- 🔒 **Population:** Nearly 200 files
- 🔒 **Target:** Microsoft-signed files such as Certutil, AddinUtil, and Windows Management Instrumentation Command-line (WMIC)
- 🔒 **How:** Bypasses process or signature-based defenses to gain persistence or escalate privileges. Leveraged in a range of attacks including code execution and file operations like downloading, uploading, and copying, and password stealing.
- 🔒 **Evades Detection:** Antivirus, Application Control, and Digital Certificate Validation

## Registry Run Keys

- 🔒 **What:** Run keys and services are part of the registry that runs the Windows operating system.
- 🔒 **Population:** 7 keys
- 🔒 **Target:** System launcher process including Run, RunOnce, RunServices, and Setup
- 🔒 **How:** Executes arbitrary commands defined in the Registry. Adversaries loop malicious programs so they run each and every time Windows is started. Rootkits mask and bury files in the Windows registry which are difficult to remove.
- 🔒 **Evades Detection:** Antivirus, Antispyware

## Cross-Site Scripting (XSS) Attacks

- 🔒 **What:** Injects malicious code into vulnerable web applications, especially functions that accept user input like forms, search bars, and comment boxes
- 🔒 **Population:** Unknown
- 🔒 **Target:** Users of compromised web applications
- 🔒 **How:** Uses Trojans to modify site content and trick users into providing credentials and other sensitive information. It steals session data to gain unauthorized access into accounts.
- 🔒 **Evades Detection:** Manipulates JavaScript, VBScript, and other client-side languages of trusted company websites to trick visitors into providing sensitive data.

## Credential Dumping

- 🔒 **What:** Technique for obtaining account login and password information for a user's system
- 🔒 **Population:** 8 techniques
- 🔒 **Target:** Stored credentials available on the user's system including Local Security Authority Subsystem Service (LSASS), Security Account Manager (SAM), Active Directory Domain Services
- 🔒 **How:** After compromising a target with elevated privileges, bad actors dump as many credentials as possible and then extract credentials from memory or use techniques to leverage password hashes for authentication.
- 🔒 **Evades Detection:** Hijacks New Technology LAN Manager (NTLMv1) hashes, modifies Access Control Lists (ACLs) in your domain, and hides traffic in the LSASS.exe process.

## Known Accomplices to Credential Dumping Attacks

**Pass the hash (PTH):** In this exploit, an attacker steals a hashed user credential. Without cracking it, the attacker reuses it to create a new authenticated session on the same network.

**Pass the ticket (PTT):** Using a stolen Kerberos ticket-granting ticket (TGT), the attacker impersonates that user on a network and gains unauthorized access to resources.

**Overpass the hash:** A post-exploitation technique that enables an attacker to use a captured NTLM hash to authenticate to a service or server within an Active Directory domain.

**Golden ticket attack:** Manipulating the Kerberos authentication protocol utilized within Windows networks, a threat actor gains unrestricted access to an organization's entire domain.

## Mimikatz: These “cute cats” are master manipulators in disguise

(Mimikatz is French slang for cute cats)

Mimikatz is not malware. In fact, it was created by a French programmer in 2007 to show Microsoft that its authentication protocols were vulnerable to attack. Unfortunately, it is still being used today by threat actors to view and save authentication credentials and gain unauthorized access to systems. One of the reasons this tool is so dangerous is its ability to load the mimikatz DLL reflexively into memory.

According to SentinelOne, Mimikatz can be used in many ways, depending on the attacker’s goals and objectives.

### For example, it can be used to

- » Extract passwords and credentials from the system’s memory
- » Bypass authentication mechanisms
- » Escalate privileges on a system
- » Move laterally within a network

–Source: [SentinelOne](#)



# Time to Batten Down the Hatches

---



## Practical Ways to Reduce the Attack Surface and Stop Adversaries in their Tracks

Do you have a security system for your home? Many people have sensors installed on their doors and windows, so they are alerted if someone breaks into their house. Some go a step further and have video cameras set up to the system to get some evidence of the theft.

Imagine one day, you turn on the security system and leave the house, but you leave all the doors, windows, and garage bays open and unlocked. Oops!

You might get away with this a few times, but eventually someone is going to get in and steal something that's valuable to you. Maybe they get into your garage (where you don't have a camera or sensor set up) and steal your air compressor. But you don't notice it's missing until you need it.



The moral of this story? It's important to use all the security available to you to prevent theft. It's much better to keep the doors and windows closed and turn on your security system rather than just relying on one or the other for protection.

This is also true for IT security. Foundational security works best when you've plugged all the holes.

## Ensure System Entry Points Are Closed

Keeping the doors closed is used as a preventative measure in many situations. It helps maintain privacy and security in offices (think confidential meetings behind closed doors) and in fire safety situations, a closed door acts as a fire barrier to slow down the spread of flames.

Similarly, blocklisting is a barrier that keeps known undesirables out of your system's business. It identifies and bans known threats, including specific tools, applications, and IP or email addresses associated with malicious activity and prevents against unauthorized access.

## What is Blocklisting?

Given all the known vulnerabilities and easy targets we've discussed, blocklisting is an essential component to foundational security protection.

Blocklisting reduces the attack surface by blocking standard users and bad actors from using tools in the Windows Operating System that aren't needed for everyday use—but often used for malicious activity.

## **A blocking tool uses a curated, comprehensive list of attack vectors like LOLBins and Registry Run Keys and protects your system by:**

- 🔒 Denying bad actors from utilizing more than 200 known entry points into your system.
- 🔒 Preventing the nefarious use of Microsoft utilities and scripts that can be leveraged for LOTL attacks.
- 🔒 Giving you control to block additional tools and render them useless to bad actors.

Blocklisting locks down these ports of entry into your system and blocks the passageways attackers use to move laterally throughout your network.



The amount of time between initial access and lateral movement of a threat actor is 83 minutes (Source: [Blackpoint Data](#))

### How do we know what to block?

- 🔒 Windows Defender Application Control (WDAC) is a Microsoft Windows 10/11 security feature that uses code integrity policies to restrict what code can run in both user mode and kernel mode. However, more than 40 files were left out of WDAC and are at risk of compromise by threat actors.
- 🔒 The Living Off the Land Binaries and Scripts (LOLBAS) project maintains an up-to-date list of every binary, script, and library that can be used for Living Off the Land attacks.

Visit <https://lolbas-project.github.io/> to view the complete list.

### Grant Access Only to Trusted Associates

Sometimes you have a need to let certain people pass through the door. Maybe they need to enter on a regular basis and since they have your trust, you grant them permissions and access.

In cybersecurity, this is known as **allowlisting**.

## What is Allowlisting?

Allowlisting permits approved applications, websites, and IP addresses to operate in a system or network environment. In this case, only preapproved applications and processes are allowed to run and access preidentified files. Allowlists can also manage which users and devices on your network have permission.

The challenge of allowlisting is that can be too time-consuming and complex to set up. It's difficult to create and maintain an allowlist that balances security needs with a list that is excessively strict and limits user productivity. Too permissive and you've expanded the attack surface.

## Leverage the Best of Both Worlds: How to Use Blocklisting and Allowlisting Together

To safeguard your organizations against potential security breaches, many organizations find that the best way to mitigate risk is to use a combination of blocklisting and allowlisting.

- » **Block** native Windows binaries that are rarely used by standard users to prevent bad actors from using them against you.
- » **Allow** specified processes to execute when required by defining rules and exceptions.

**There are more than 450,000 new malicious programs every day so it's important to keep your block list updated.**

—Source: [AV-TEST Institute](#)

# Reduce the Attack Surface with Privileged Access Management (PAM) and Blocklisting

---

Privileged access management (PAM) is a subset of cybersecurity that revolves around tools and methods for controlling the access and permissions for users, accounts, processes, and systems throughout an IT environment. Blocklisting is a natural extension of that.

## The benefits of privileged access management and blocklisting together include

- 🔒 Minimizes risk of malware infections and LOTL attacks.
- 🔒 Secures applications and operating system tools from outside intervention.
- 🔒 Eliminates an attacker's ability to exploit most known vulnerabilities.
- 🔒 Provides a forensics component so IT professionals can track down problems and write new rules to prevent future attacks.

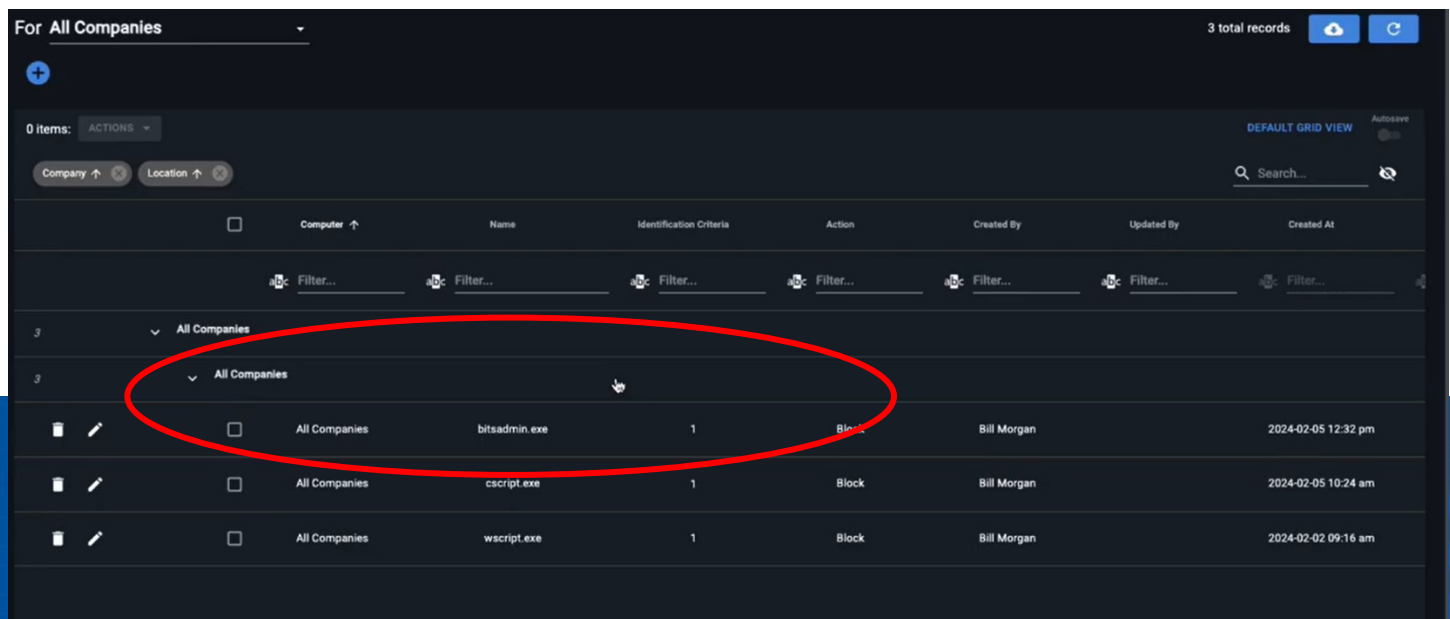


## How it Works

When using CyberFOX's AutoElevate and Blocker together, organizations can stop nefarious activity and gain insight into where the problem started to prevent future attacks.

Here's how blocklisting of a known Remote Access Trojan "bitsadmin" shuts down a potential attack in just three steps:

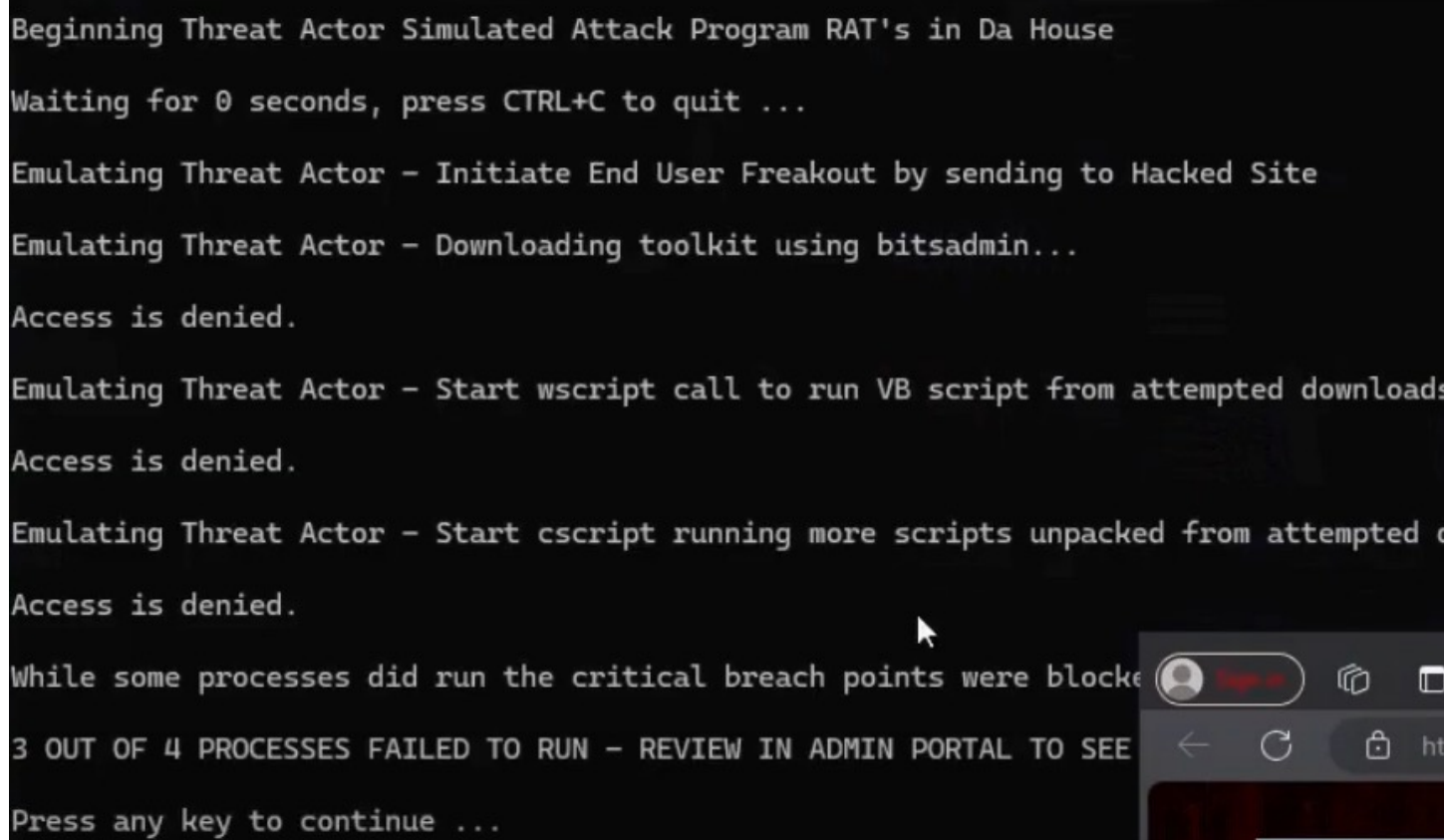
- 01.** This curated list of files includes the tool, bitsadmin.exe, so it will be automatically blocked from executing.



The screenshot shows the CyberFOX interface with a table of blocked files. A red circle highlights the first row, which lists 'bitsadmin.exe' for 'All Companies' with a 'Block' action. The table has columns for Computer, Name, Identification Criteria, Action, Created By, Updated By, and Created At. The first row is circled in red.

Computer	Name	Identification Criteria	Action	Created By	Updated By	Created At
All Companies	bitsadmin.exe	1	Block	Bill Morgan		2024-02-05 12:32 pm
All Companies	cscript.exe	1	Block	Bill Morgan		2024-02-05 10:24 am
All Companies	wscript.exe	1	Block	Bill Morgan		2024-02-02 09:16 am

- 02.** When a bad actor tries to initiate the bitsadmin executable, the blocking tool denies access and prevents the malicious scripts from running.



```
Beginning Threat Actor Simulated Attack Program RAT's in Da House
Waiting for 0 seconds, press CTRL+C to quit ...
Emulating Threat Actor - Initiate End User Freakout by sending to Hacked Site
Emulating Threat Actor - Downloading toolkit using bitsadmin...
Access is denied.
Emulating Threat Actor - Start wscript call to run VB script from attempted download
Access is denied.
Emulating Threat Actor - Start cscript running more scripts unpacked from attempted download
Access is denied.
While some processes did run the critical breach points were blocked
3 OUT OF 4 PROCESSES FAILED TO RUN - REVIEW IN ADMIN PORTAL TO SEE
Press any key to continue ...
```

- 03.** Using the AutoElevate monitoring tool, an IT professional can take a closer look at this event to determine where the attack came from and further investigate the incident.

Now that you've seen how easy it is for bad actors to hijack tools within your system and commit Living Off the Land (LOTL) attacks, we invite you to join us in the fight against them.

AutoElevate is a privileged access management (PAM) solution that helps organizations improve security and compliance by reducing the attack surface and providing granular control over user privileges. The Blocker feature in AutoElevate blocks 200+ native Windows applications, binaries, and .dll files that are typically used as LOTL attack vectors.

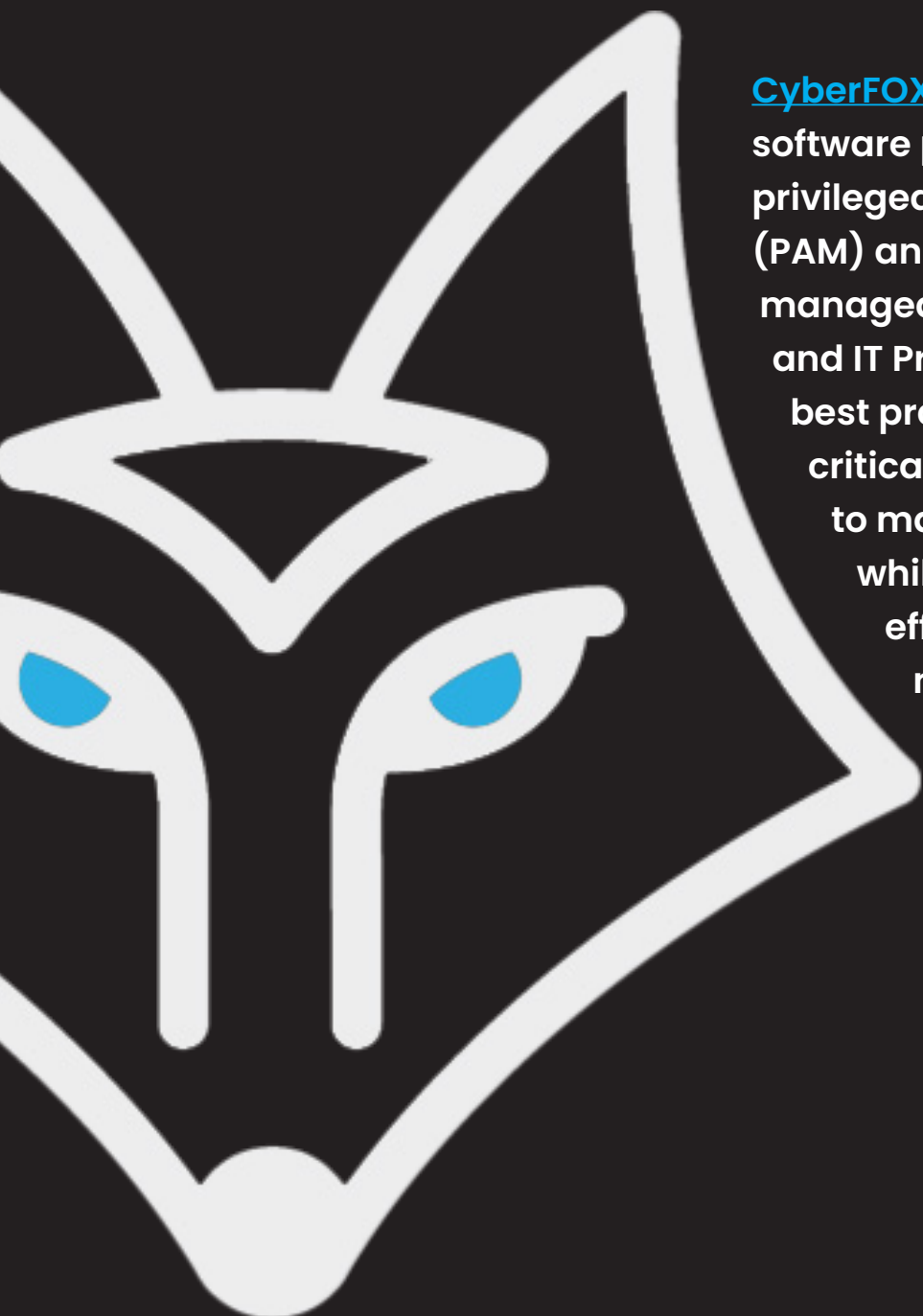
Blocker is an important component of PAM that prevents bad actors from leveraging these legitimate tools in the Windows Operating System to steal credentials, data, and identities.

Blocker obstructs these adversaries by curating a comprehensive list of attack vectors and empowering you to choose which items to block from executing.

### **With Blocker, you get:**

- » Enhanced Security
- » Easy Rule Management
- » Minimized False Positives

**Blocker keeps bad actors from living off your land.**



CyberFOX is a global cybersecurity software provider focused on privileged access management (PAM) and password management for managed service providers (MSPs) and IT Pros. Prioritizing cybersecurity best practices as a company like CIS critical controls, allows CyberFOX to make complex security simple while providing affordable and efficient solutions. To learn more about how CyberFOX helps protect MSPs and organizations visit [www.cyberfox.com](http://www.cyberfox.com).