Azure LoLBins: Protecting against the dual use of virtual machine extensions | Microsoft Security Blog

By Ram Pliskin

Published: 2021-03-09 · Archived: 2026-04-05 14:39:51 UTC

Azure Defender for Resource Manager offers unique protection by automatically monitoring the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. In this blog, we will look into the threats that are caused by "Living off the land Binaries" (LoLBins).

The term "Living off the land," or LoL in short, is used to describe attackers leveraging built-in utilities to carry out attacks. LoLBins usually refer to pre-installed Windows or Linux binary tools that are normally used for legitimate purposes, but on compromised resources, can be leveraged by attackers. This tactic challenges defenders aiming to distinguish between the dual uses of these tools.

The usage of LoLBins is frequently seen, mostly combined with fileless attacks, where attacker payloads surreptitiously persist within the memory of compromised processes and perform a wide range of malicious activities. Together with the use of legitimate LoLBins, attackers' activities are more likely to remain undetected.

Attackers are increasingly employing stealthier methods to avoid detection. Evidence for a variety of campaigns has been witnessed. Please find a detailed overview of how such an attack unfolds, along with recommendations on how to detect malicious LoLBins' activities on Windows.

Azure LoLBins

The concept of LoLBins is not limited to traditional operation systems. In this post, we explore different types of Azure Compute virtual machine extensions, which are small applications that provide post-deployment configuration and automation tasks on Azure Virtual Machines. For example, if a virtual machine requires software installation, anti-virus protection, or to run a script inside of it, a virtual machine (VM) extension can be used.

Custom Script Extension downloads and executes scripts on Azure Virtual Machines, Anti-Malware extension for Windows warps different configuration types and applies them into Windows Defender, and VMAccess Extension manages administrative users, SSH keys and enables recovery features such as resetting the administrative password of a virtual machine (VM).

All these extensions serve thousands of administrators coming to orchestrate their Azure fleet. But in cases where an attacker assumes certain roles within a subscription, these Azure built-in capabilities will come in handy bypassing any network defense lines. Therefore, we named them Azure LoLBins.

How does it work?

Every image on Azure Marketplace contains an Azure guest agent implanted into it (VM Agent). The guest agent is a secure, lightweight process that manages VM interaction with the Azure Fabric Controller. The VM Agent has a primary role in enabling and executing Azure Virtual Machine extensions. Without the Azure VM Agent, VM extensions cannot be run.

The Guest Agent is responsible for managing VM extension operations such as installing, reporting status, updating individual extensions, and removing them. Extension packages are downloaded from the Azure Storage extension repository by the guest agent through communication with Azure fabric (over channel to 168.63.129.16).

To perform its tasks, the guest agent runs a Local System. Consequently, payloads of extensions, such as Custom Script Extension and Run Command, run on Azure Virtual Machines with extensive privileges on the local computer.

Impact

In this section, we will examine several behaviors we recently witnessed that demonstrate the exceptionality and potential strength of the VM extensions, making the specific Azure IAM roles, containing the rights to call them a lucrative target for attackers.

Case 1: Custom Script Extension

Custom Script Extension downloads and executes scripts on Azure Virtual Machines. This extension is useful for post-deployment configuration, software installation, or any other configuration or management tasks. Scripts can be downloaded from Azure Storage or GitHub, or provided to the Azure portal at extension run time. The Custom Script Extension can be run using the Azure CLI, PowerShell, Azure portal, or the Azure Virtual Machine REST API.

Usage of Custom Script Extension was seen spanning across different customers to fetch an executable from the same GitHub repository. We followed the traces to GitHub, finding the repository in question being publicly accessible allowed us to confirm the suspicion. The code intention within the executed payload (*hack1.sh, see snippet below)* is to mine cryptocurrency.

This behavior was observed across multiple customers from different countries within a noticeably short timeframe, together with the GitHub repository being inactive increased our suspicion this activity should not be

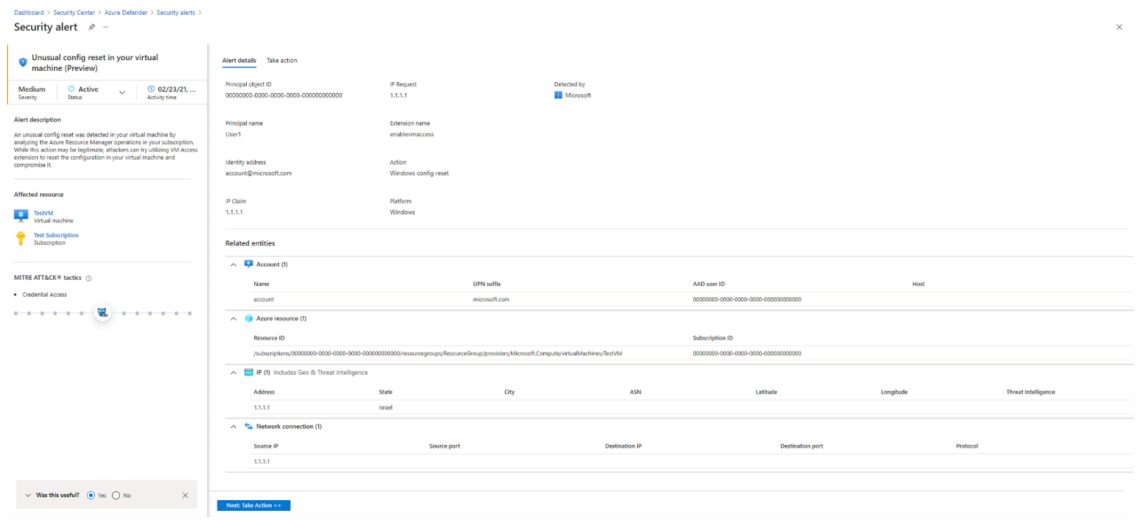
associated with normal pen-test, red-team, or intended activity.

Case 2: VMAccess Extension

VMAccess Extension can create new administrator accounts, reset the password of an existing administrator account, reset the built-in administrator account and or reset the Remote Desktop service Configuration. Moreover, for Linux VMs, the extension can reset SSH public keys. Furthermore, similarly to other extensions, the VMAccess Extension can be executed through the Azure portal, Azure CLI, Powershell, or the Azure Virtual Machine REST API.

VM Access is extremely useful when managing your VMs. As an example, for Linux servers, an alternative would be to connect to the VM and execute the equivalent commands manually. Hence, it is one of the most accessible extensions due to its simplified user interface (UI) which you can access from the Azure Portal.

There is no doubt that the VMAccess Extension is a handy way for an attacker to gain initial access to VMs with elevated privileges. Such notorious usages of the extension may sometimes be difficult to notice. As an example, leveraging VM Access to create a common service user or modifying an existing one.



Case 3: Antimalware Extension

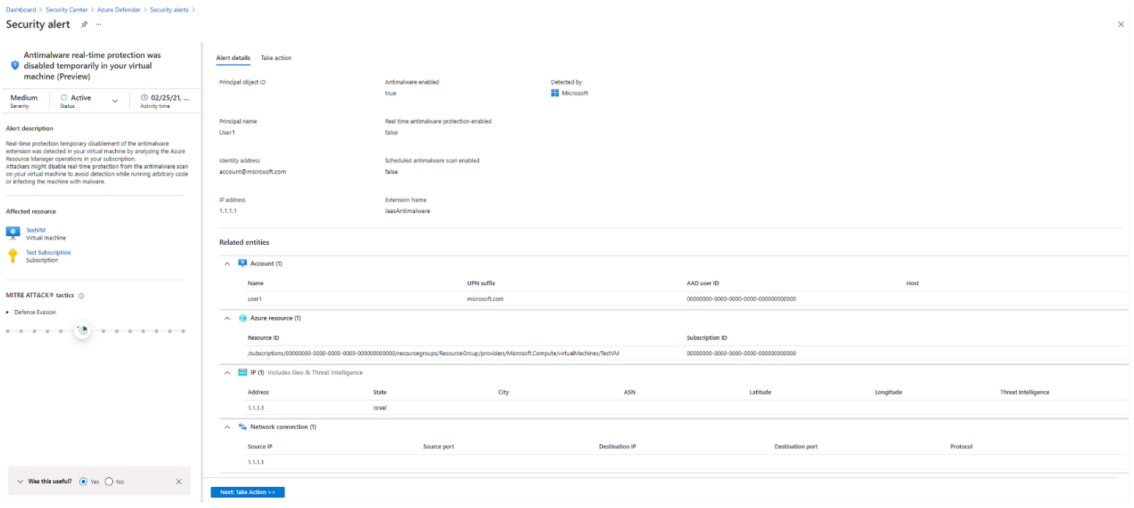
Microsoft Antimalware Extension for Azure is a free real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems. Microsoft Antimalware for Azure is a single-agent solution designed to run in the background without human intervention.

The Microsoft Antimalware for Azure solution includes the Microsoft Antimalware Client and Service, and when used in Windows environment with Windows Defender enabled, the extension will apply any optional configuration policies to be used by Windows Defender, the extension will not deploy any additional antimalware service.

While experimenting with Microsoft Defender for Endpoint alerts for Windows and usage of the Anti-Malware extension, we noticed a correlation between alerts fired on the node followed by API calls to Azure Resource

Manager. This orchestrates VM extensions, with configurations to the Anti-Malware extension that excluded the same alert-triggered payloads from being scanned in the future.

Using the Anti-Malware extension, attackers can potentially also disable the real-time protection before loading suspectable tools into the node or exclude specific files and directories for going unnoticed while conducting their malicious activity. Enjoying the benefit that Azure Resource Manager logs was rarely crossed in correlation to in-node telemetry.



Learn more

Microsoft recommends you implement detection and mitigation strategies to minimize exposure to new threats the Cloud brings. Azure Defender goes deep into dissecting attack techniques in order to define and build a depth protection plan.

Detection

Azure Defender has expanded its threat detection capabilities and recently introduced Azure Defender for Resource Manager, a new coverage for Azure deployment and management service. Every request to the Azure Resource Manager Endpoint on *management.azure.com* is logged and analyzed to reveal malicious intentions and threats.

Azure Defender for Resource Manager monitors all resource management operations performed in your organization performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Azure Defender runs advanced security analytics to detect threats and alert you when suspicious activity occurs. For a list of the Azure Defender for Resource Manager alerts, see the reference table of alerts.

Mitigation

Least privilege principle is a fundamental concept in Cloud environments. Ensuring that minimum access necessary to perform a legitimate operation would be granted to all identity types (human or non-human). A least privilege model for the cloud relies on the ability to continuously adjust access controls. We recommend

monitoring all access events and establish a decision-making framework that distinguishes between legitimate and excessive permissions.

Get started for free today

Protect your entire Azure environment with a few clicks and enable Azure Defender for Resource Manager. This offer is free during the preview period. Turn Azure Defender on now.

To learn more about Microsoft Security solutions and our Integrated Threat protection solution visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.

Source: https://www.microsoft.com/security/blog/2021/03/09/azure-lolbins-protecting-against-the-dual-use-of-virtual-machine-extensions/