Zeljka Zorz, Editor-in-Chief, Help Net Security
August 2, 2023

Attackers can turn AWS SSM agents into remote access trojans

Mitiga researchers have documented a new post-exploitation technique attackers can use to gain persistent remote access to AWS Elastic Compute Cloud (EC2) instances (virtual servers), as well as to non-EC2 machines (e.g., on-premises enterprise servers and virtual machines, and VMs in other cloud environments).

The success of this "living off the land" technique hinges on:

- Attackers gaining initial access to the machine (e.g., by exploiting an unpatched vulnerability on a public-facing instance/server), and
- The presence of the SSM Agent, a software component that enterprise sysadmins use to manage the endpoints from the AWS account using the AWS System Manager service

"After controlling the SSM Agent, the attackers can carry out malicious activities, such as data theft, encrypting the filesystem (as a ransomware), misusing endpoint resources for cryptocurrency mining and attempting to propagate to other endpoints withing the network – all under the guise of using a legitimate software, the SSM Agent," Mitiga researchers Ariel Szarf and Or Aspir explained.

Possible scenarios

The researchers have tried out two different scenarios, and the level access required for both is high. In the first scenario, the threat actor requires root access on targeted Linux machine or administrator privileges on the targeted Windows system, while in the second they must be able run as at least non-root privileged user on the targeted Linux machine or as administrator on the targeted Windows system.

"[In the first scenario], the attack is 'hijacking' the original SSM Agent process by registering the SSM Agent to work in 'hybrid' mode with a different AWS account, enforcing it to not choose the metadata server for identity consumption. Then, the SSM Agent will communicate and execute commands from attacker the owned AWS account," they explained.

In the second scenario, the attacker runs another SSM Agent process by using Linux namespaces or setting specific environment variables on Windows. "The malicious agent process communicates with the attacker's AWS account, leaving the original SSM Agent to continue communicating with the original AWS account."

And if the threat actor prefers not to use an AWS account to manage the agents, they don't have to: there's an SSM feature that can be abused to route the SSM traffic to an attacker-controlled server (i.e., not through AWS's servers).

Detection and prevention

Turning the SSM Agent into a remote access trojan enables attackers to compromise endpoints without getting spotted by installed security solutions. The C&C communications appear legitimate, there's no need to develop a separate attack infrastructure, and the SSM Agent can be used to manipulate the endpoint via supported features.

The fact that the SSM Agent is preinstalled on some popular Amazon Machine Images and is thus already installed and running on many existing EC2 instances widens the pool of potential targets for adversaries, the researchers pointed out.

Luckily, there are ways to detect the use of this technique. They include: keeping an eye out for new instance IDs, the use of specific commands, lost connections to SSM agents in the AWS account, new processes, and suspicious actions related to Sessions Manager in Amazon CloudTrail logs.

The researchers advise enterprise sysadmins to:

- Remove the SSM Agent binary from the allow list of their AV and EDR solutions, so that they can be examined and the behavior of processes analyzed for anomalous/suspicious behavior
- Integrate the outlined detection techniques into their SIEM and SOAR platforms to help with threat hunting.

“We strongly believe that threat actors will abuse this in real world attacks, if they don’t do that already. Because of that, understanding and mitigating the risks associated with its misuse is crucial to protect systems from this evolving threat,” they noted, and pointed out that the AWS Security team has also offered a solution to restrict the receipt of commands from the original AWS account/organization using the Virtual Private Cloud (VPC) endpoint for Systems Manager.

“If your EC2 instances are in a private subnet without access to the public network via a public EIP address or NAT gateway, you can still configure the System Manager service through a VPC endpoint. By doing so, you can ensure that the EC2 instances only respond to commands originating from principals within their original AWS account or organization. To implement this restriction effectively, refer to the VPC Endpoint policy documentation.

UPDATE (August 5, 2023, 05:20 a.m. ET):

“AWS software and systems are behaving as designed and there is no need for customers to take any action,” an AWS spokesperson commented for Help Net Security.

“The issues described in the Mitiga publication, titled ‘Mitiga Security Advisory: Abusing the SSM Agent as a Remote Access Trojan,’ require an actor to both obtain root level credentials and successfully access an EC2 instance in order to be leveraged. As a security best practice, we recommend AWS customers follow our documentation on properly configuring VPC Endpoints with AWS Systems Manager and to use global condition keys for VPC Endpoints and VPC Endpoint Policies to mitigate the risk of inappropriate access to EC2 instances.

More about

AWS | cloud computing | cloud security | enterprise | Mitiga | remote access trojan | research

Share

Featured news

Google on scaling differential privacy across nearly three billion devices

Lottie Player supply chain compromise: Sites, apps showing crypto scam pop-ups

North Korean hackers pave the way for Play ransomware

Don't miss

Google on scaling differential privacy across nearly three billion devices

Lottie Player supply chain compromise: Sites, apps showing crypto scam pop-ups

North Korean hackers pave the way for Play ransomware

IoT needs more respect for its consumers, creations, and itself

How agentic AI handles the speed and volume of modern threats