Since the December campaign, the actor has made several updates to how their tooling works. The newest campaign also has a new variable, MIXED_CREDFILES which contains only non-AWS credentials. Instead, C2 activity relies on a hardcoded username and password combination that are passed as arguments to the amazonaws command-line tool. The actor made the script more modular as it grew larger and more complex. The AWS functionality is now split into three smaller functions that are driven by the aws.sh script. The functions were not called. These changes indicate that these features are being actively developed, so we expect these changes to be included in the future.

In addition to the usual shell scripts, we observed the actor delivering a UPX-packed, Golang-based ELF binary. The binary is packed using a custom algorithm that is designed to evade detection by common static analysis tools. The binary includes a number of hooks that allow it to evade detection by other tools, such as signatures-based detection systems. The binary is also designed to be portable across different platforms, allowing it to be used on a wide range of systems.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.

The binary includes a number of features that are designed to make it difficult for security researchers to reverse engineer. These features include obfuscation techniques that make it difficult to understand the binary's structure, and anti-debugging techniques that prevent debugging tools from obtaining information about the binary's execution flow. The binary also includes a number of other features that are designed to make it more difficult for security researchers to analyze or decompile the binary.