We'll be going over three different malspam campaigns and exploring eight different code and string obfuscation techniques.

This research article explores various PowerShell obfuscation techniques, commonly found in real world malspam campaigns.

Opening the malicious Excel attachment triggers VBA macro execution.

The next script was part of a malspam campaign delivering Azorult Infostealer. Sample artifacts can be found in the second layer of base64 encoding, we see the use of the function FromBase64String().

In the script, we see three random alphanumeric variables, Here the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2. Here, the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64).

In the second layer of base64 encoding, we see the use of the function FromBase64String().

The script accepts a base64-encoded string version of a command. The cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

In the script, we see three random alphanumeric variables, Here the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

Once completely deobfuscated, the PowerShell command would look something like this (the script accepts a base64-encoded string version of a command. The cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

The campaign also makes use of the

Obfuscation Technique 3: Command Alias

In the script, we see three random alphanumeric variables, Here the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

The next script was part of a malspam campaign delivering Azorult Infostealer. Sample artifacts can be found in the second layer of base64 encoding, we see the use of the function FromBase64String().

In the script, we see three random alphanumeric variables, Here the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

Once completely deobfuscated, the PowerShell command would look something like this (the script accepts a base64-encoded string version of a command. The cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

The campaign also makes use of the

Obfuscation Technique 3: Command Alias

In the script, we see three random alphanumeric variables, Here the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

Once completely deobfuscated, the PowerShell command would look something like this (the script accepts a base64-encoded string version of a command. The cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

The campaign also makes use of the

Obfuscation Technique 3: Command Alias

In the script, we see three random alphanumeric variables, Here the script strings are split into multiple parts which are then concatenated through the cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.

Once completely deobfuscated, the PowerShell command would look something like this (the script accepts a base64-encoded string version of a command. The cradle primarily employs the following two string obfuscation methods: String Reversing, Encoding (Base64). The value of $we22 is the numerical representation of 2.