11.6.11 Malicious Code Facts

Malicious software (malware) is perhaps the most dangerous threat to any computing device. Malware can be created using a variety of programming languages and methods.

This lesson covers the following topics:

- Python
- Command shells
- Macros

Python

Python has become one of the most popular programming languages. First released in 1991, Python is designed to be easy to learn and read. It can be used on most operating systems including Windows, MacOS, and Linux. Python can also take advantage of open-source Python packages and repositories.

Many Remote Access Trojans (RATs) are designed using Python. Python makes it easy to implement libraries that allow the RAT to perform functions such as:

- Taking screenshots
- Enabling the webcam and viewing it remotely
- Making web requests
- Making phone calls

Python also makes it very simple to develop malicious code that can be run on many different systems and devices, including Android devices.

One of the main drawbacks to using Python for malware is the file size. Python files are larger than other common languages. Also, Python must be installed on a system for a Python script to run. This works for MacOS and Linux, but Windows doesn’t come with it installed. Python scripts can be converted to Windows compatible executables fairly easily though.

Command Shells

A shell provides an interface for users to access operating system functions and services. Shells are generally associated with command line interfaces, but they can have graphical interfaces also.

Because these programs provide access to core operating system functions, they are extremely dangerous when exploited.

Commands can be typed directly into the shell program or can be run from a script. A script is a plain-text document that has the commands typed out just like they would be in the shell. When the script is run, the commands are executed.

Two of the more heavily used shells are PowerShell and Bash. The following table describes these two shell programs:

Shell Program	Description

PowerShell	PowerShell is a management framework that Microsoft developed to replace Command Prompt and give users more power and control over the Windows system. PowerShell is built on the .NET framework and can now be run on multiple operating systems including MacOS and Linux. PowerShell uses cmdlets to execute commands. Cmdlets are tiny scripts that perform certain functions. Some cmdlets replace older commands and provide more advanced functions. Users can combine these cmdlets to develop scripts to automate tasks and configure just about anything in Windows. Malicious PowerShell scripts pose a major security threat. These scripts can run in the memory of the system which means they don't need a executable to run. ▪ An attacker can take advantage by running malicious PowerShell scripts in the background. ▪ This type of malware is known as *fileless malware.* Fileless malware is especially dangerous because many anti-virus programs are unable to detect it.
Bash	Bash is a command shell and scripting language used in most Linux distros and MacOS versions prior to Catalina. Bash was released in 1989 and is still heavily used. When a command is executed in Linux, Bash works in the background to execute the command using environment variables. Since many web servers run on Linux's Apache platform, malware can be designed in Bash to attack these systems. A well-known malware called Shellshock uses Bash commands to exploit a flaw within the Bash shell. The flaw allows an attacker to inject malicious commands.

Malware that exploits shell programs is using the operating system against itself, making this type of malware difficult to detect and prevent.

Keeping anti-malware up to date and training users to not click unknown links or run unknown programs is vital to staying safe.

Macros

Macros are similar to scripts in that they are little bits of code that are used to perform a series of steps or functions. Macros however are used inside specific applications. Many different programs can make use of macros, but the most common use of macros is in the Microsoft Office programs.

Microsoft Office programs use the Visual Basic for Applications (VBA) programming language to create and run macros. If the Office program is not configured properly, malicious VBA code can be used to open a shell on the Windows operating system. The shell can be used to perform malicious attacks.

In newer version of Microsoft Office, macros are disabled by default and a user must specifically allow them to run.

Copyright © 2022 TestOut Corporation All rights reserved.