Indications of Compromise
Cheat Sheet

The AMP for Endpoints indications of compromise (IOC) feature is a powerful incident response tool for scanning indicators across multiple computers.

Threat detected

One or more malware detections triggered on the computer.

Potential dropper infection

A single file is repeatedly attempting to download malware onto a computer.

Multiple infected files

Multiple files on a computer are attempting to download malware.

Executed malware

A known malware sample was executed on the computer. This can be more severe than a simple threat detection because the malware potentially executed its payload.

Suspected botnet connection

The computer made outbound connections to a suspected botnet command and control system.

[Application] compromise

A suspicious portable executable file was downloaded and executed by the application named, for example, Adobe Reader Compromise.

[Application] launched a shell

The application named executed an unknown application, which in turn launched a command shell, for example, Java launched a shell.

Generic IOC

Suspicious behavior that indicates possible compromise of the computer.

Suspicious download

An executable file was downloaded from an IP address using a nonstandard port. This is often indicative of malware droppers.

Suspicious cscript Launch

Internet Explorer launched a command prompt, which executed cscript.exe (Windows script host). This sequence of events is generally indicative of a browser sandbox escape, ultimately resulting in execution of a malicious Visual Basic script.

Suspected ransomware

File names containing certain patterns associated with known ransomware were observed on the computer. For example, files named help_decrypt were detected.

Possible webshell

The IIS worker process (w3wp) launched another process such as powershell.exe. This could indicate that the computer was compromised and remote access has been granted to the attacker.

Log in to your management console to view your IOCs.