RAPID7

Quarterly Threat Report: 2019 Q3

Scripting techniques, “living off the land,” and targeting RDP and SMB

Executive Summary

The 2019 Q3 Threat Report leverages data from the Rapid7 Insight cloud, Managed Detection and Response engagements, and projects Sonar and Heisenberg to analyze threat events across industry segments and organization size, while also aligning to the MITRE ATT&CK™ Framework. Why? By essentially combining data with a common taxonomy on attacker methods, we hope it’ll inform more effective measures you can take to mitigate those dangers.

Highlights for this quarter include:

Third-party software and PowerShell

Cmd.exe, powershell.exe, and ADExplorer were the top three executables we saw across MITRE ATT&CK tactics.

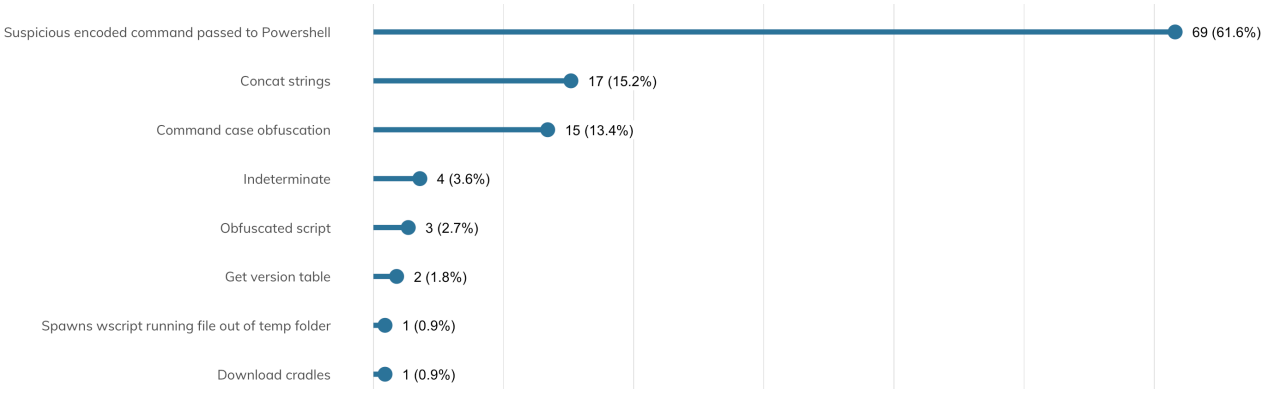
Phishing is still #1

The initial access tactic of the attacker kill chain still often starts with tried and true methods.

Probes, and now attacks, against RDP servers

We saw increased network traffic to Project Heisenberg honeypots coinciding with news of the attacks exploiting the BlueKeep vulnerability.

2019 Q3 Powershell Usage Alerted



Read the full Q3 2019 Threat Report to dive deeper into these key findings and what they could mean for your organization:

rapid7.com/threat-report