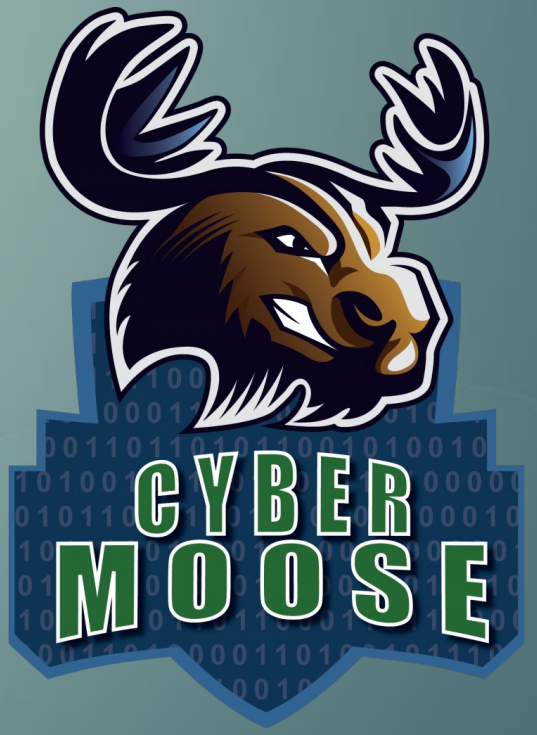
Catching the Guerrilla: PowerShell Counterinsurgency

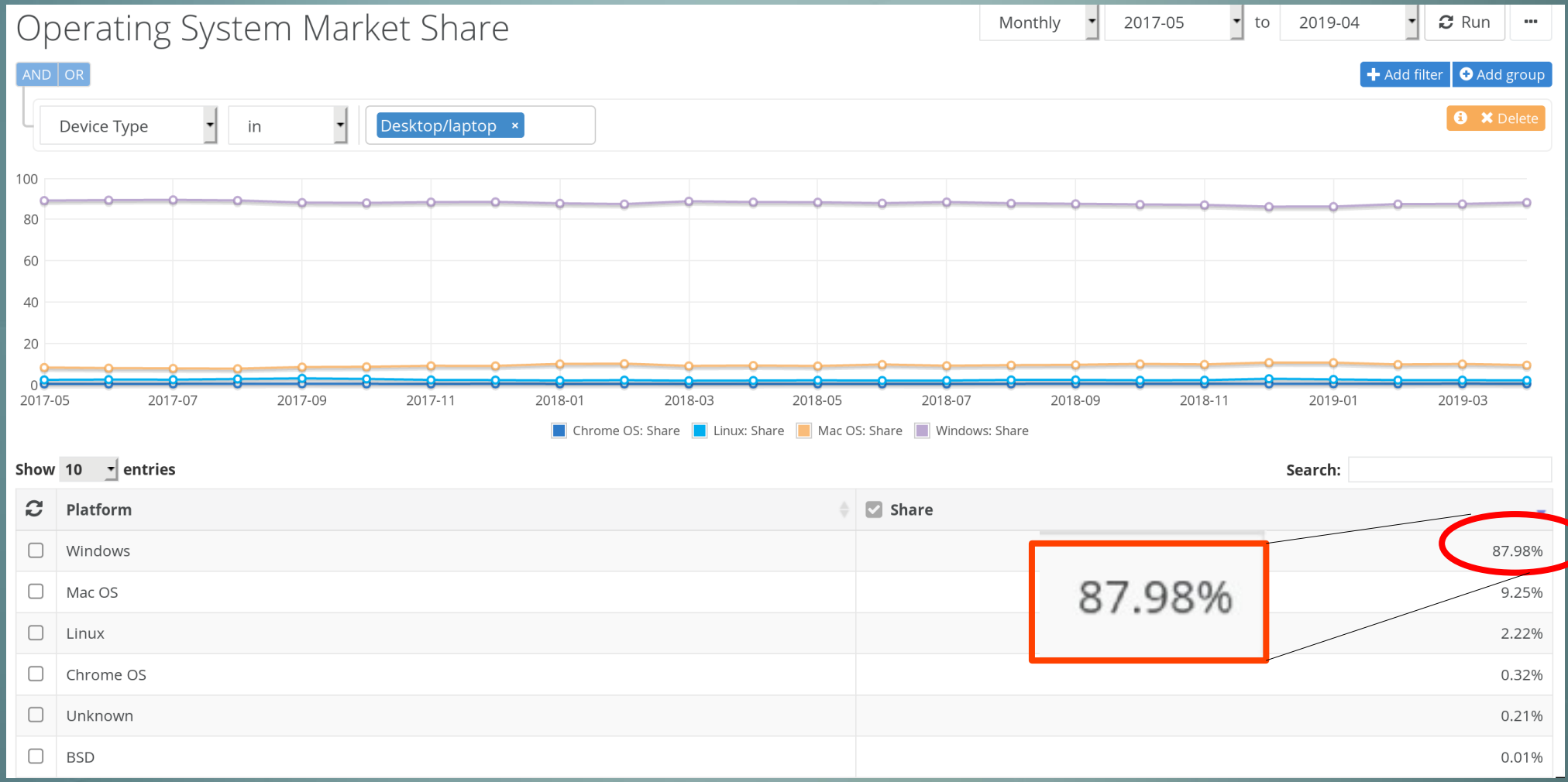
Aaron Sawyer
Intern
InfoSec Innovations



The Problem

- Most of the Attack Surface Consists of Windows
- Only Two Options For Defenders: Watch or Kill

Windows Market Share



Large Number of Vulnerability Classes

- SMB/NetBIOS
  - EternalBlue (MS17-010)
    - EternalBlue + Mimikatz = NotPetya
  - Cornficker (MS08-067)
  - NetBIOS DoS (CVE-2017-0174)
  - Auxiliary Vulnerabilities (CVE-2018-7445)

Large Number of Vulnerability Classes

- TrueType Fonts
  - ATMFD.dll

    Patched in Windows 10 1607

    CVE-2017-8483 shows that ATMFD.dll can still be fuzzed

- Old Protocols, new tricks...

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/14/2019
MITRE CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

Security Update Guide > Details

CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/14/2019
MITRE CVE-2019-0708

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

On this page

Why Not Switch?

- Switching over legacy software
- Training employees on new systems
- Windows is here to stay

New PowerShell Stuff

- Unix Philosophy
- Larger Framework
- Here’s a small taste...

PRACTICAL DEMO

Why so short?

- Written with the UNIX philosophy
  - Simple
  - Short
  - Clear
  - Modular
  - Extensible
- This produces a tool that’s easy to customize

Malware Detected!

Program is acting ‘weird’

Containment Options:

- Kill it
  - What if it’s on a production server?
  - What if it’s an accounting tool? (SEC compliance)
- Watch it
  - “the time from first action in an event chain to initial compromise of an asset is most often measured in seconds or minutes.”[1]

PS-Suspend

- PS-Suspend can do this, but:
- Requires local installation of PSExec Utils on every target system
- Thousands of instances in some cases...

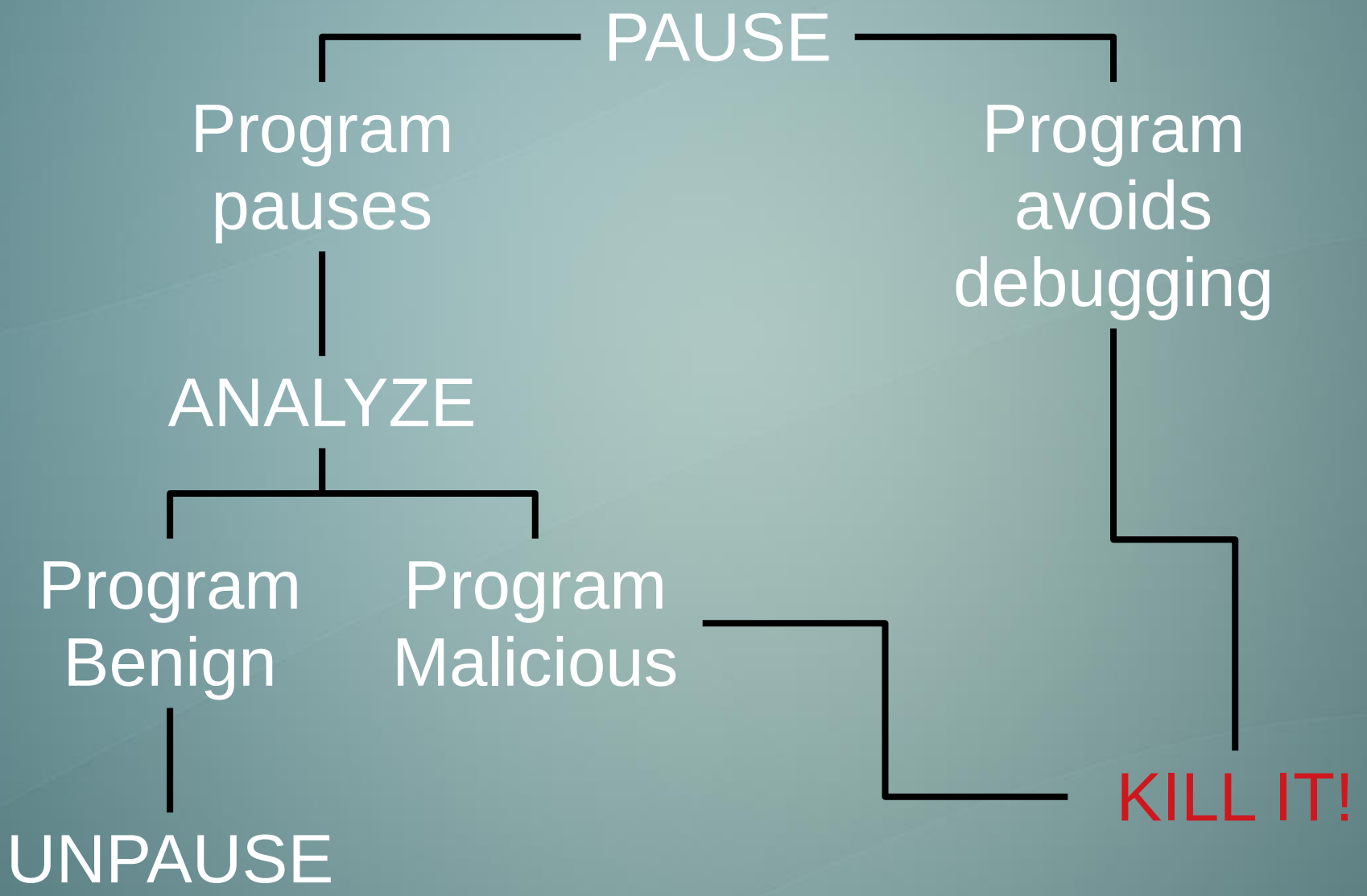
Pause-Process

- Accepts a PID as input
- “Pauses” that process by sending it to a debugger
- Works out of the box with no install on target system

Why?

- Pausing stops malicious activity
- If PID isn’t malicious, program can be unpaused
  - No harm done!

Why?


PAUSE
Program pauses
Program avoids debugging
ANALYZE
Program Benign
Program Malicious
KILL IT!
UNPAUSE

Larger Scope

- Can be deployed using WinRM/WMI triggering
- Behavioral signatures can be mapped to WQL
- Results can be cross-checked to a whitelist before automatic pausing

Use Case

- “Select all processes on a network where CPU consumption is higher than 95% for more than 3 seconds”
- Compare results to a whitelist
- Automatically pause and alert SOC analyst

Advantage of Pause-Process

- Signature matches crypto-miners
- Also matches rendering processes and compilers
- Killing would destroy someone’s work
- Pausing is Safer

Caveats

- Not good for time-sensitive processes
  - HFT
  - Manufacturing
- Currently requires a dedicated thread for each paused job

The Future of Pause-Process

- Spawn local background jobs for each paused thread
  - Eliminate SIEM overhead
- Debugging thread redirection
  - Reverse-Engineer Utility (i.e. GHIDRA)
- Slow process instead of pausing

Timed Out?

This talk is dedicated to my amazing wife.

Questions?

GitHub.com/CrashingStatic/Pause-Process

References

[1] Operating System Market Share. Net MarketShare. (Accessed May 30, 2019). https://www.netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22platform%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22platformsDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222018-05%22%2C%22dateEnd%22%3A%222019-04%22%2C%22segments%22%3A%22-1000%22%7D

[2] Verizon Data Breach Investigations Report (2018). pg 10. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[3] CVE-2019-0708. Microsoft CVE Announcement. 14 May 2019. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

[4] Jealous CVEs. "2600 | The Hacker Quarterly" Facebook Page. https://www.facebook.com/groups/majordomo