Modern Phishing Defeated by Plain Old Logs

ART AZARENKO

Agenda

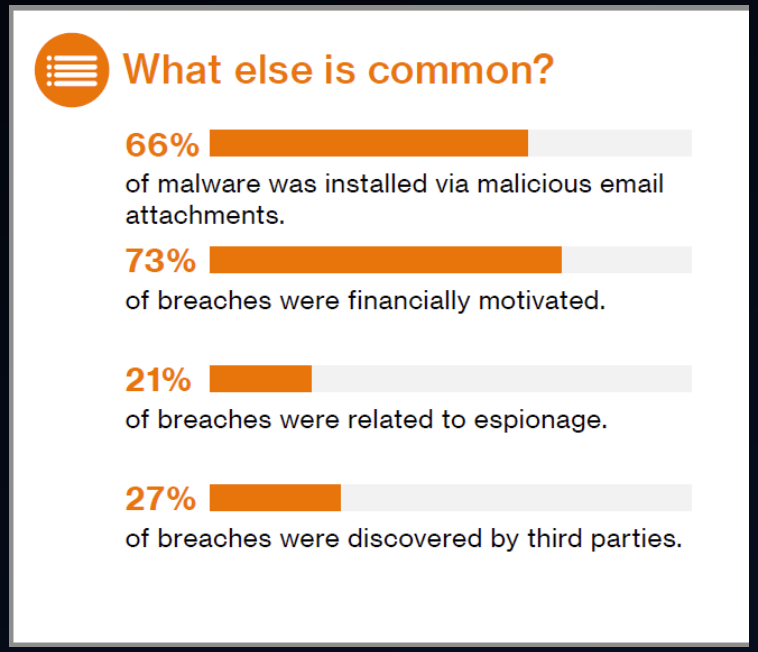
- Introduction - whoami
- Modern Phishing
- Defense Mechanisms
- Demo
- Q&A

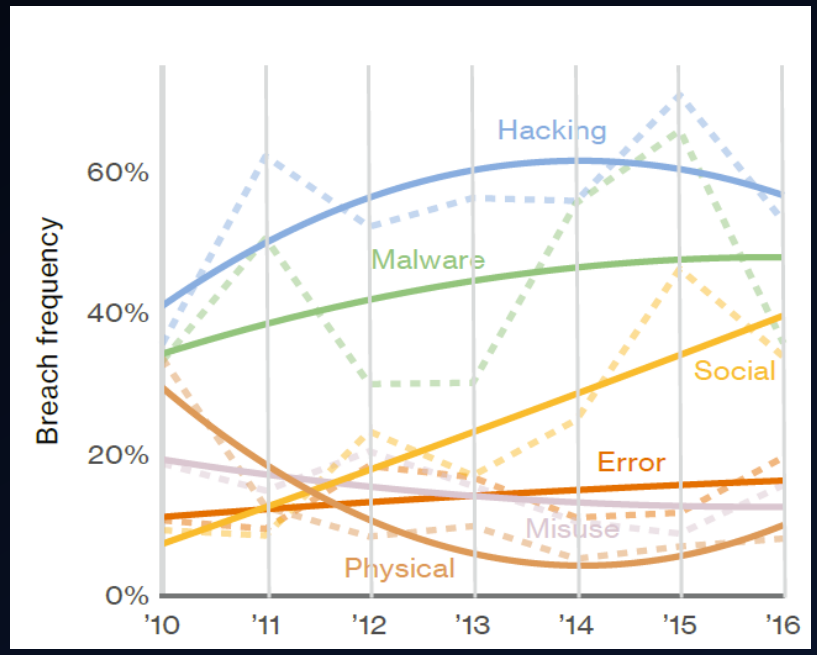
Introduction

- Art Azarenko
- GCFA, GCFE, #143745
- Security Analyst, TDS Inc.
- Art.Azarenko@tdsinc.com
- linkedin.com/in/artazarenko

Phishing / Social Engineering Data

- 2017 Verizon Data Breach Investigations Report
- Top 3 Threats: Hacking, Malware, and Social

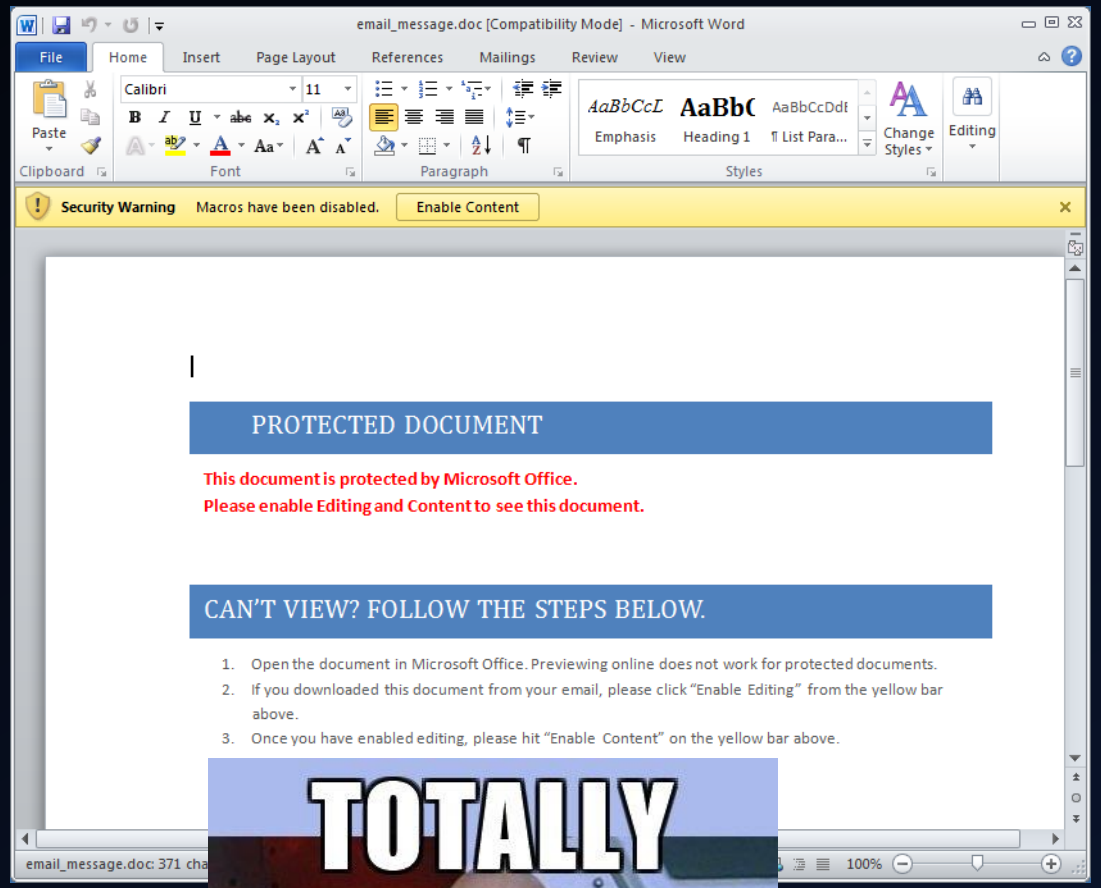




http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

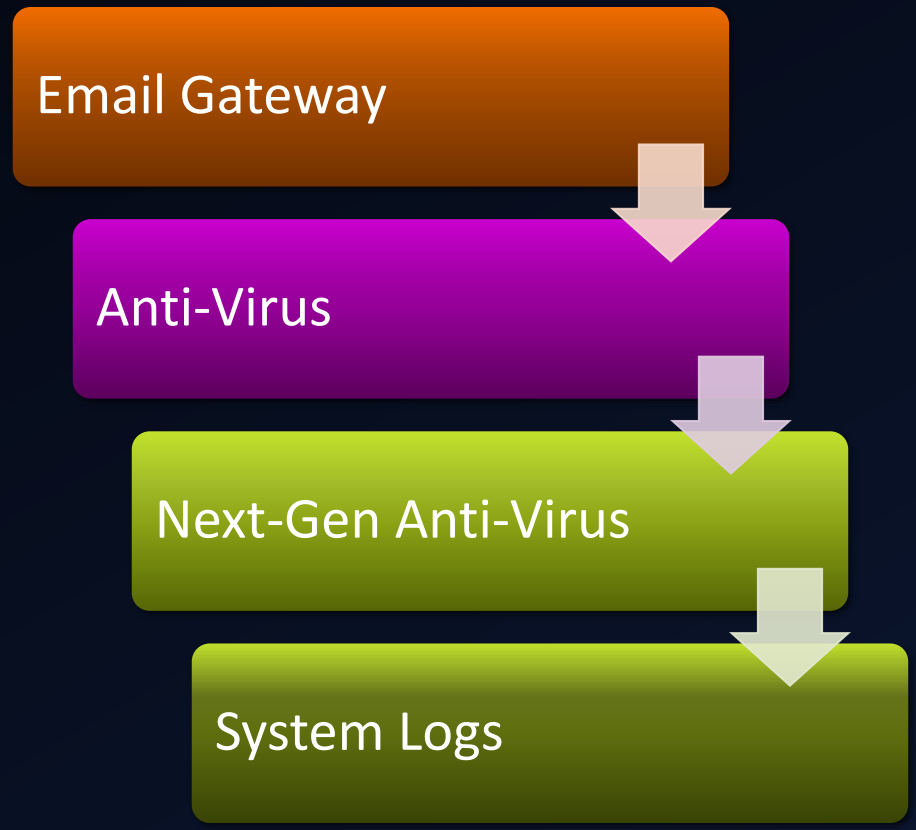
Malicious Attachments

- Productivity Applications containing malicious macros/scripts:
  - Microsoft Office files
  - Adobe PDF files
- How do attackers succeed?
  - Using SMTP servers with good sender reputation
    - Bypassing spam filters
  - New phishing campaign
    - No signatures
  - Encryption (password in the email)
    - User education



Defense Mechanisms

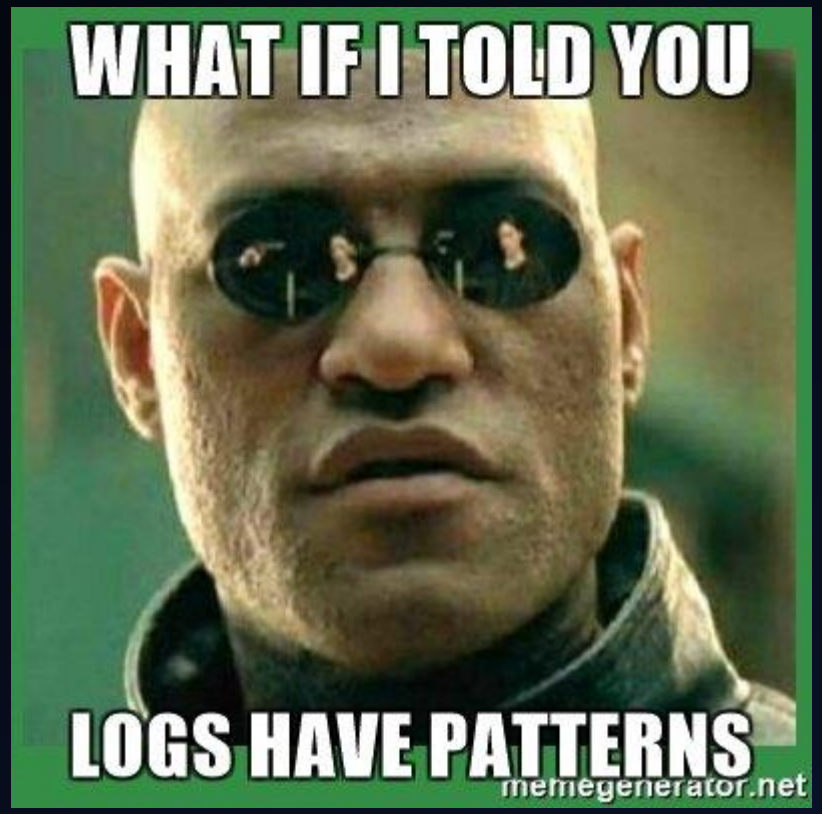
- Sender Reputation – Score
- Attachment analysis – Signature
- Threat Intelligence – Signature
- Anti-Virus – Signature
- Next-Gen Anti-Virus - Pattern
- Logs – Pattern



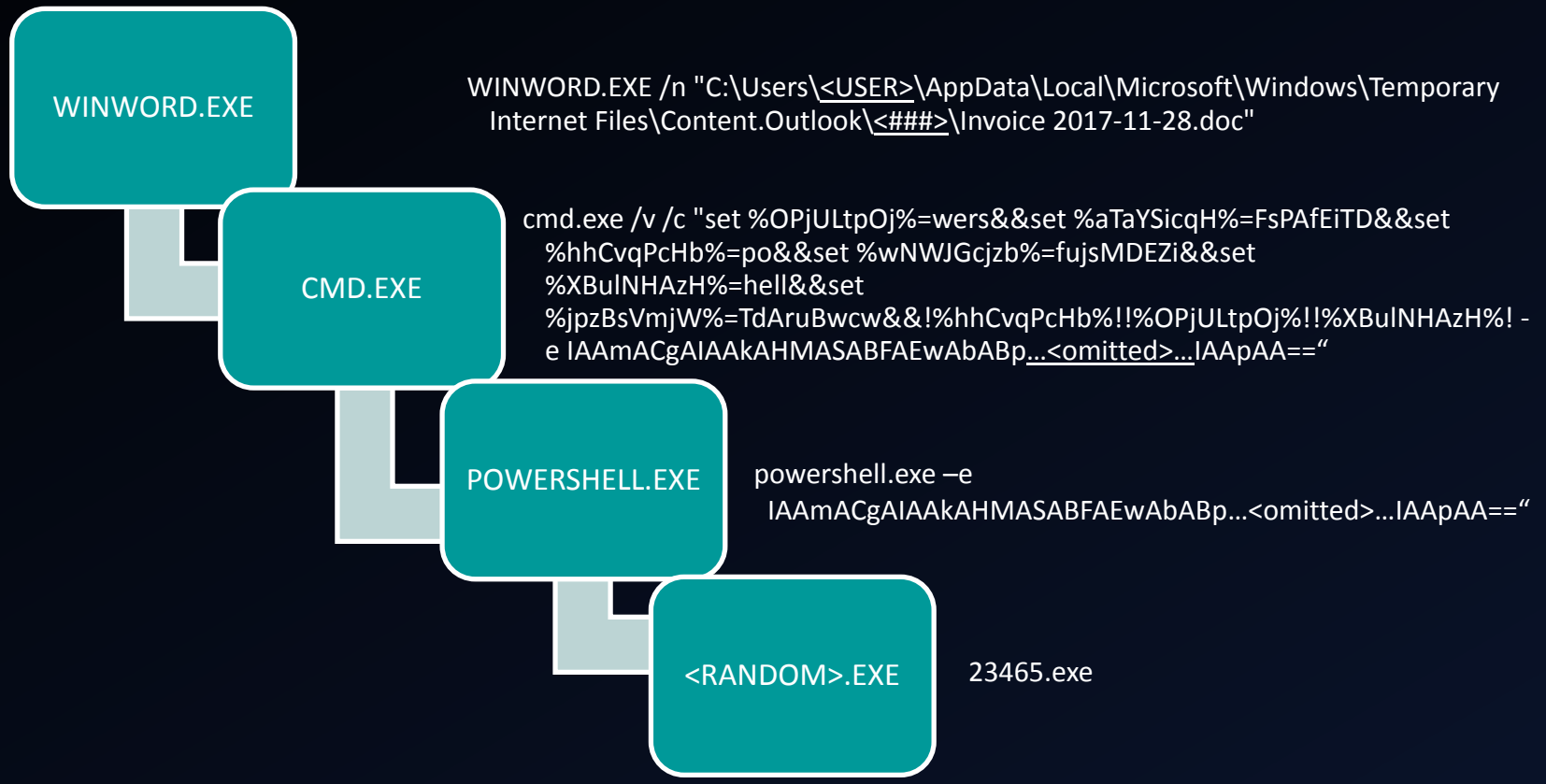
Signatures Vs. Patterns

- Anti-virus is dead!
  - Maybe not, but it’s hard to keep up with modern attacks
- Next-Gen Pattern Analysis
  - Evolving platforms, but require significant investment $$$

What about logs?

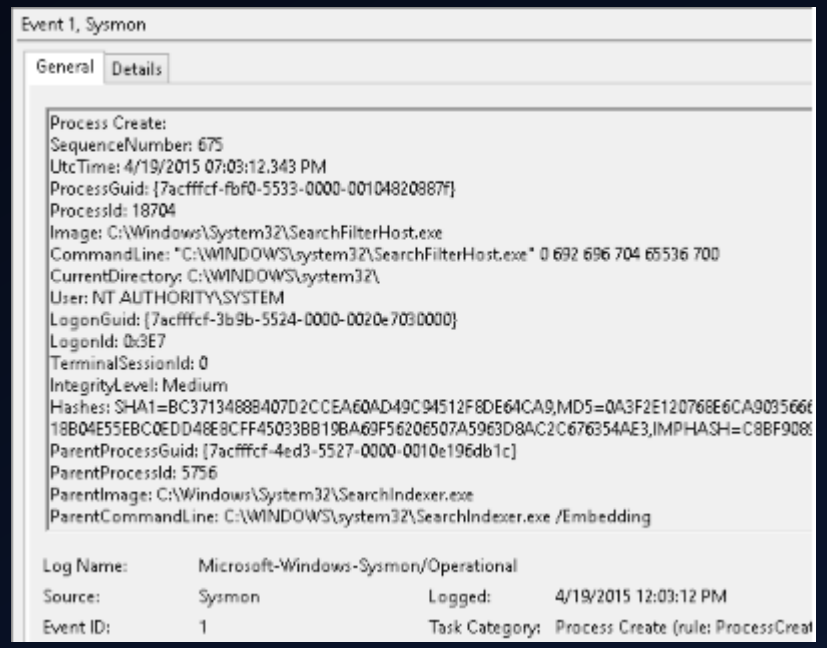


Malicious Attachment - Process Execution



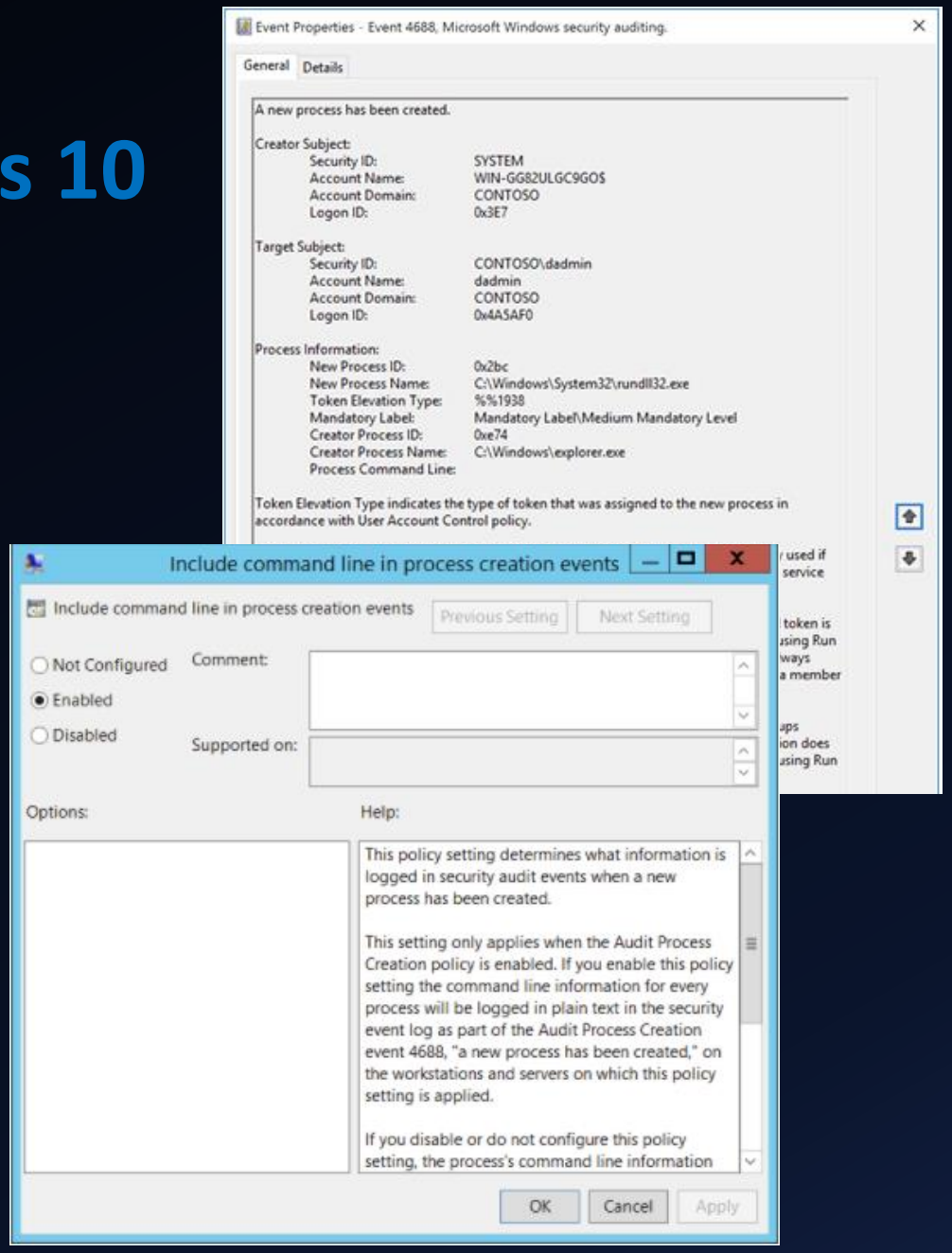
Log Pattern Analysis – Windows 7

- Sysmon – Windows Sysinternals
  - By Mark Russinovich and Thomas Garnier
  - Logs process creation with full command line for both current and parent processes.
  - Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
  - https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon



Log Pattern Analysis – Windows 10

- In addition to Sysmon, Windows 10 native logs contain parent process information
  - EventID:4688
  - Administrative Templates\System\Audit Process Creation\Include command line in process creation events



Demo Time!

More Patterns = More Alerts

- Enhancement levels depend on maturity
  - Level 1 – Basic Parent Process Correlation
    - Parent Process = WINWORD.EXE
    - New Process = CMD.EXE
  - Level 2 – Enhance Filename extraction
    - WINWORD.EXE /n "C:\Users\<USER>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\<###>\Invoice 2017-11-28.doc"
    - Filename = Invoice 2017-11-28.doc
  - Level 3 – Email Recipient Lookup
    - Search email gateway logs for similar attachment names
    - Recipients = john.smith@company.com, jane.smith@company.com


Q&A