

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](https://www.linkedin.com/in/artazarenko)



Phishing / Social Engineering Data

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



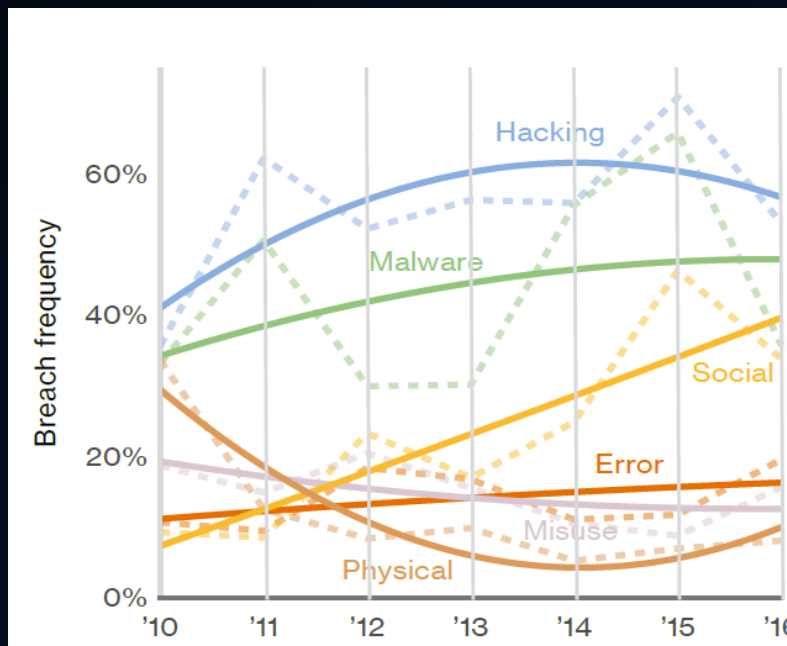
What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

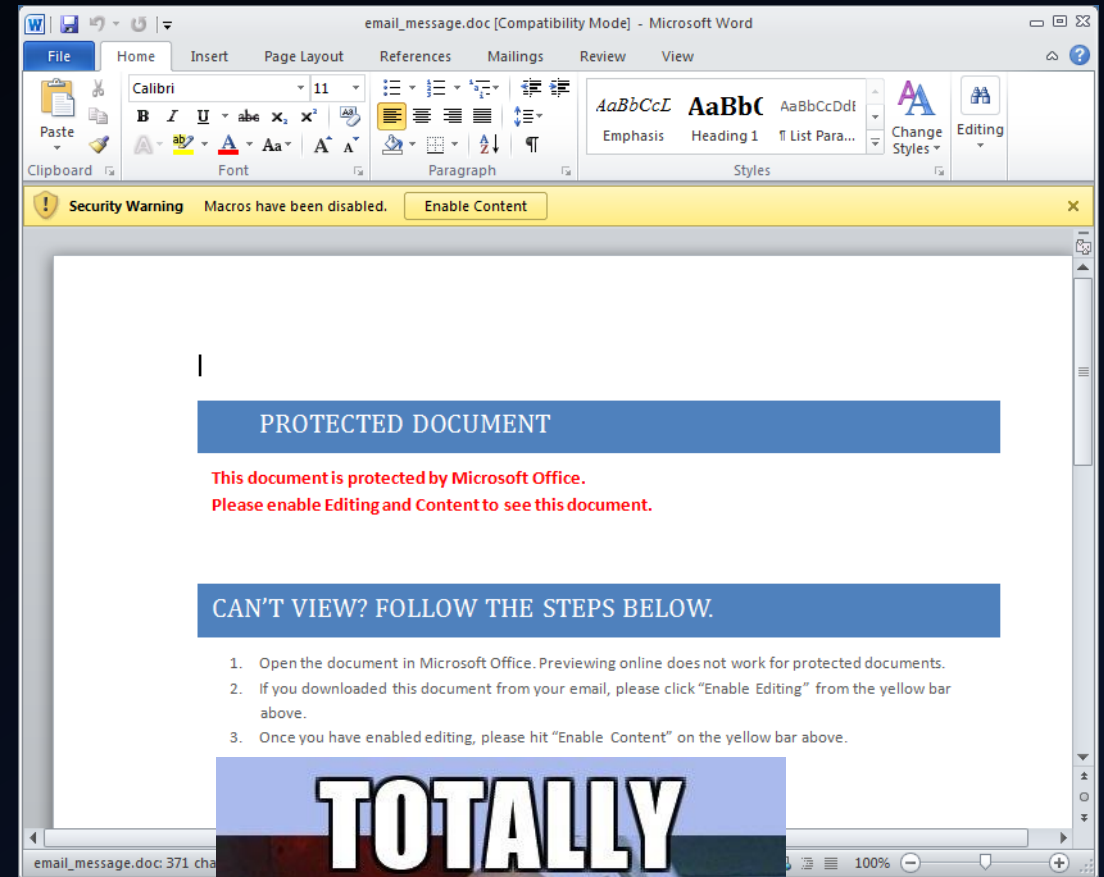
21% of breaches were related to espionage.

27% of breaches were discovered by third parties.



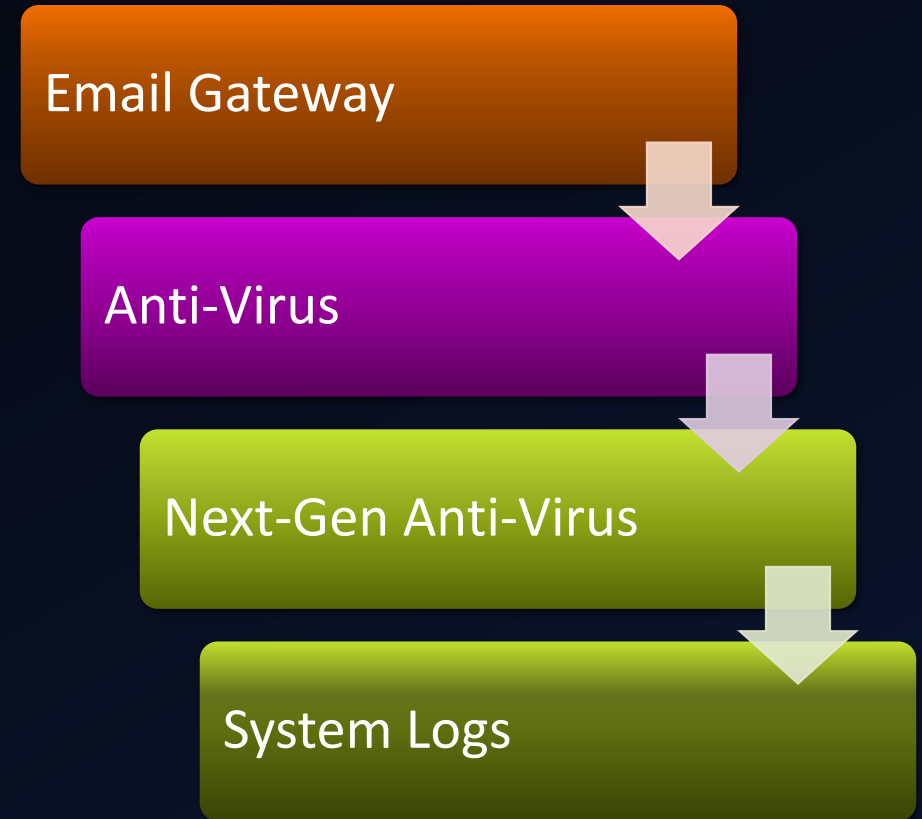
Malicious Attachments

- 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

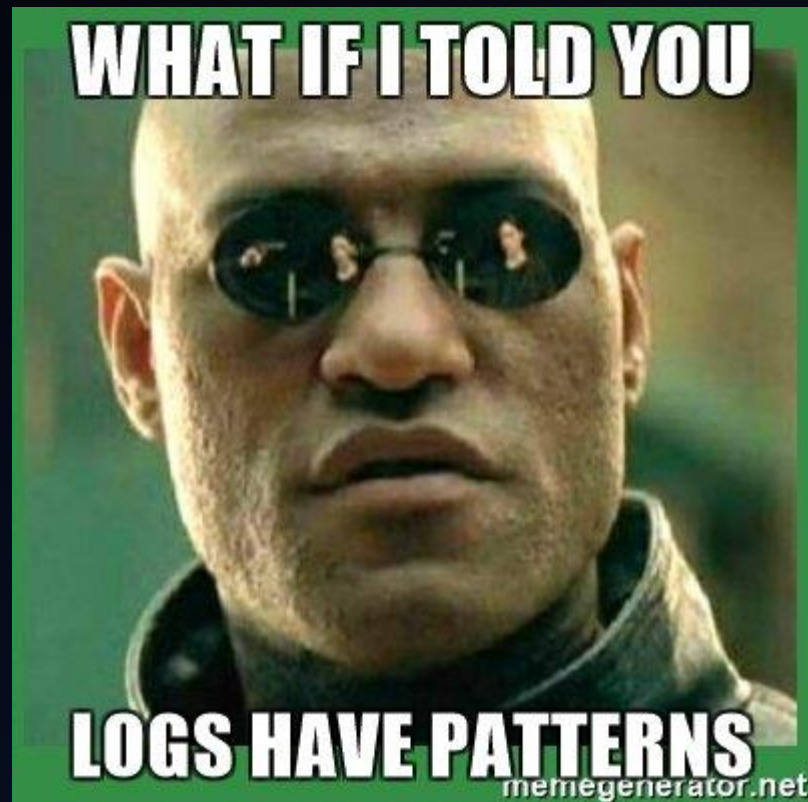
- Sender Reputation – **Score**
- Attachment analysis – **Signature**
- Threat Intelligence – **Signature**
- Anti-Virus – **Signature**
- Next-Gen Anti-Virus - **Pattern**
- Logs – **Pattern**



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?

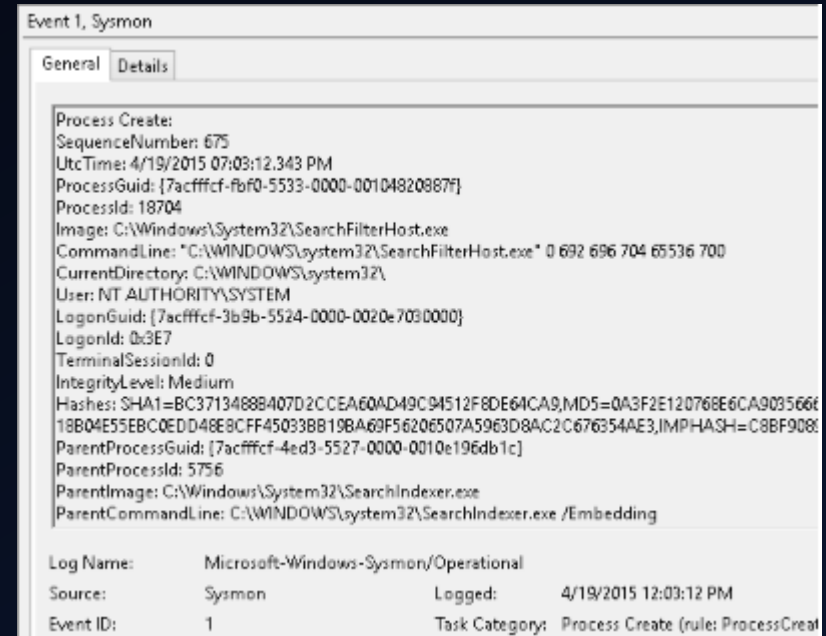


Malicious Attachment - Process Execution



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>



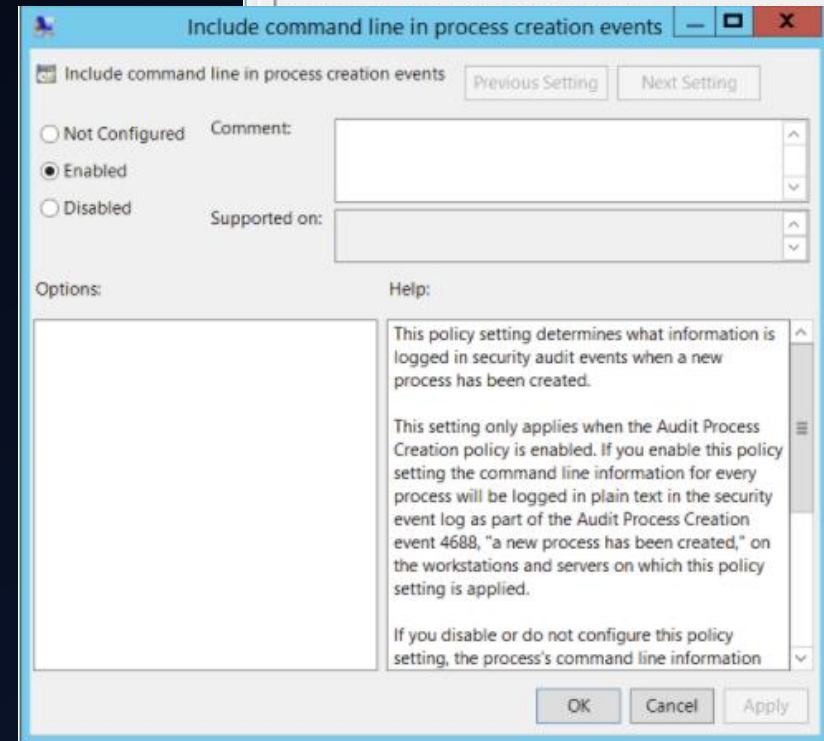
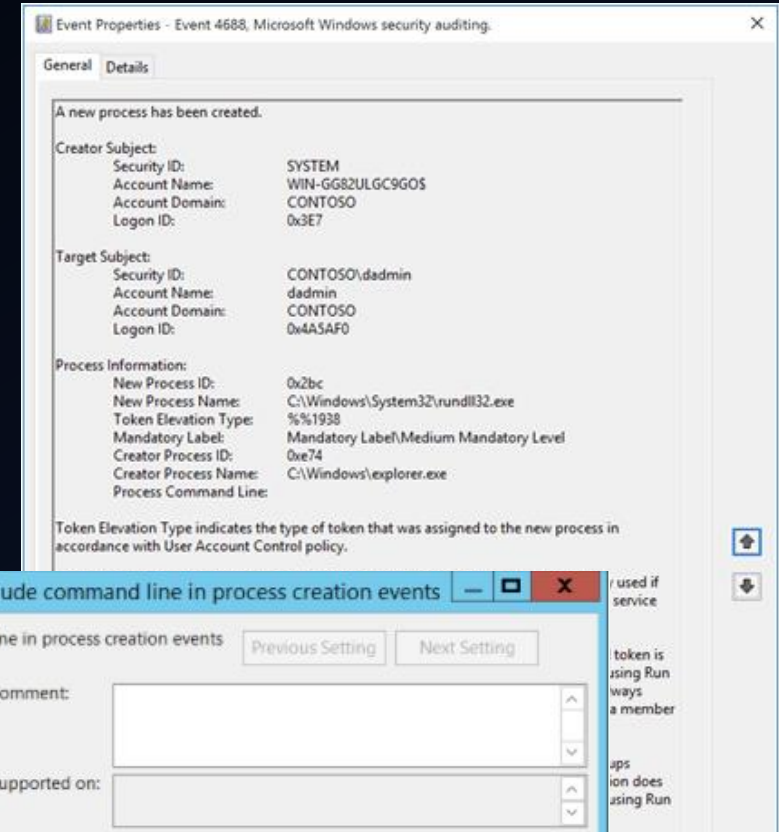
The screenshot shows a Windows Event Viewer window titled "Event 1, Sysmon". The "Details" tab is selected, displaying the following information:

```
Process Create:
SequenceNumber: 675
UtcTime: 4/19/2015 07:03:12.343 PM
ProcessGuid: {7acffcf-fb0-5533-0000-00104820887f}
ProcessId: 18704
Image: C:\Windows\System32\SearchFilterHost.exe
CommandLine: "C:\Windows\System32\SearchFilterHost.exe" 0 692 696 704 65536 700
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {7acffcf-3b9b-5524-0000-0020e7030000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: Medium
Hashes: SHA1=BC37134888407D2CCEA60AD49C94512F8DE64CA9,MD5=0A3F2E120768E66CA903566618B04E55EBC0EDD48E8CFF450338B198A69F56206507A5963D8AC2C676354AE3,IMPHASH=C8BF908E
ParentProcessGuid: {7acffcf-4ed3-5527-0000-0010e196db1c}
ParentProcessId: 5756
ParentImage: C:\Windows\System32\SearchIndexer.exe
ParentCommandLine: C:\Windows\system32\SearchIndexer.exe /Embedding
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 4/19/2015 12:03:12 PM
Event ID: 1 Task Category: Process Create (rule: ProcessCreat

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\\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