DERBYCON VII LEGACY
LOUISVILLE 2017 KENTUCKY

EDR, ETDR, Next Gen AV is all the rage, so why am I ENRAGED?

Looks like Tod Beardsley (Fellow Austinite Rapid7)

Michael Gough – Founder
MalwareArchaeology.com
IMFSecurity.com

LOG-MD
Discover it

MalwareArchaeology.com

Malware Archaeology

Who am I

- Blue Team Defender Ninja, Malware Archaeologist, Logoholic
- I love “properly” configured logs – they tell us Who, What, Where, When and hopefully How

Creator of

“Windows Logging Cheat Sheet”

“Windows File Auditing Cheat Sheet”

“Windows Registry Auditing Cheat Sheet”

“Windows Splunk Logging Cheat Sheet”

UPDATED

“Windows PowerShell Logging Cheat Sheet”

“Malware Management Framework”

Malware Archaeology

- Co-Creator of **“Log-MD” – Log Malicious Discovery Tool** LOG–MD
  - **With @Boettcherpwned – Brakeing Down Security PodCast**
- **@HackerHurricane** also my Blog

LOG–MD
Discover it

MalwareArchaeology.com

Malware Archaeology

Why are we here?

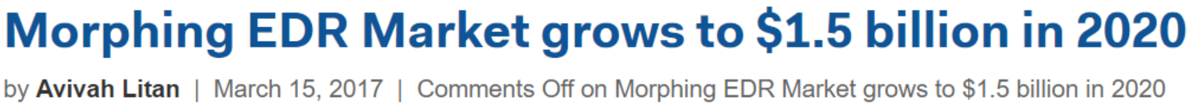
- Anti-Virus is not cutting it

MY EXPECTATIONS JUST GET LOWER AND LOWER.
THAT'S GREAT!
EVENTUALLY I'LL BE ABLE TO MEET ALL OF THEM!
mimiandeunice.com

- Actually AV provides me a lot
- Alerts me to large campaigns, hours or days later, old stuff and infected USB drives

Why are we here?

- AV’s lack of being able to catch today’s threats
- But also because logging was inadequate in Windows until 3 years ago (2014) when Process Command Line logging was added



Morphing EDR Market grows to $1.5 billion in 2020

by Avivah Litan | March 15, 2017 | Comments Off on Morphing EDR Market grows to $1.5 billion in 2020

- This lack of good logging and details left an opportunity for vendors to create tools that captured Command Line (ETL) Logs and join them with other details, like Intel, and behavior
- Many of the EDR tools use command line logging as a major component into what is going on with the endpoint

Why are we here?

- We evaluated a bunch of EDR solutions
- We had some VERY surprising findings
- Found and opened bugs with several vendors, yup we got by them
  - ***Are you shocked?***

- We only used 3 malware sample types
  - Only ONE vendor solution caught all 3

- We were surprised at what gave us the most artifact details, it wasn't even close

- Here is what we found and you should know

Our Malware Samples

Symantec Official Blog

Kovter malware learns from Poweliks with persistent fileless registry update

- Kovter
  - Some call it “Fileless Malware” – Psst it’s not fileless
  - Stored components in the registry
  - Mshta used to launch javascript and calls PowerShell

Symantec Official Blog

Dridex: Financial Trojan aggressively spread in millions of spam emails each day

- Dridex
  - Uses valid MS signed binaries and side loads a bad Dll from a directory in user space
  - Morphs on each reboot, new binary and Dll hash

Home › Malware

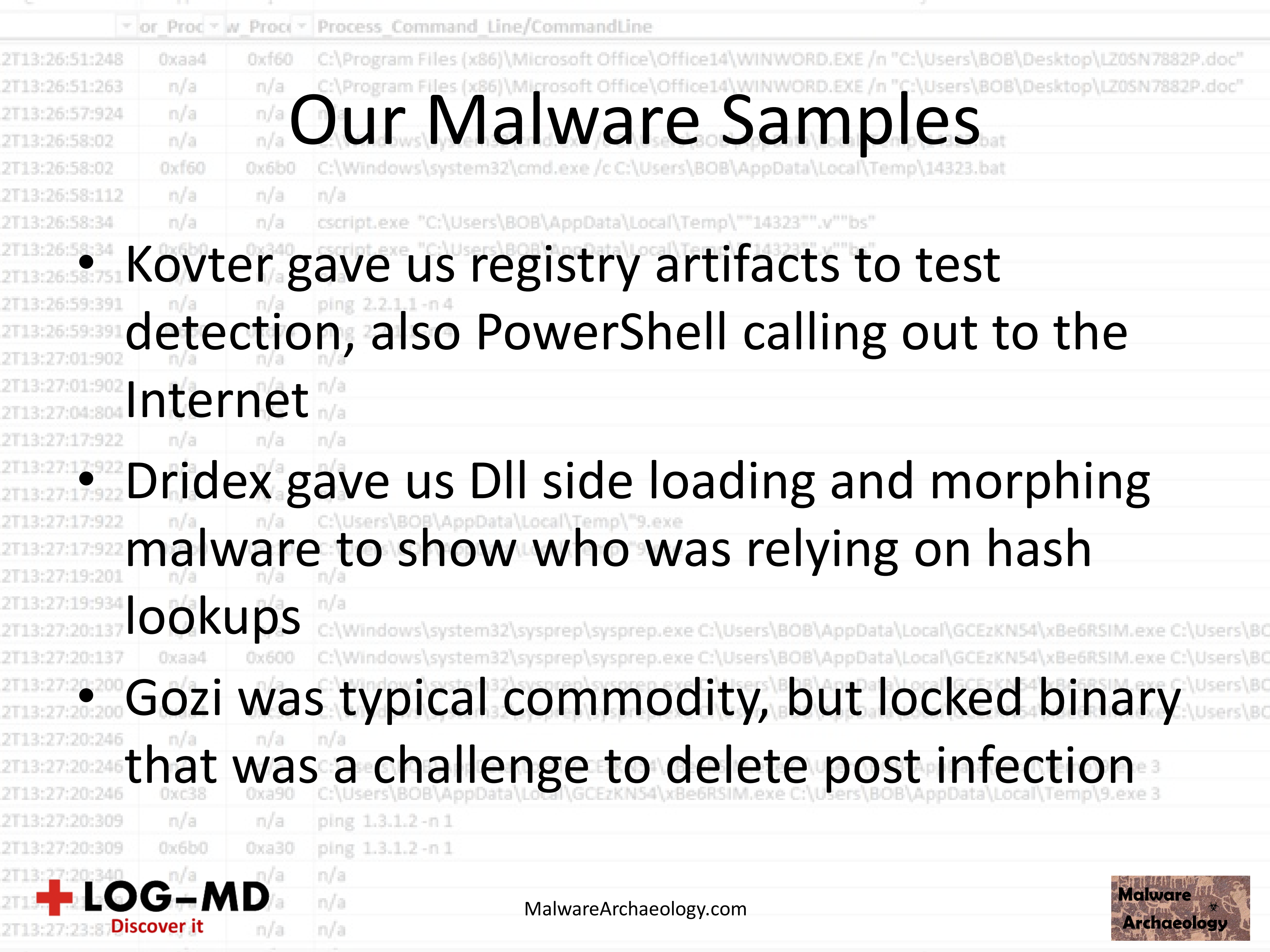
Gozi Banking Trojan Targets Windows 10's Edge Browser

By SecurityWeek News on February 19, 2016

- Gozi
  - Typical commodity malware
  - Run key, files on disk, locked the binary when infected

Our Malware Samples

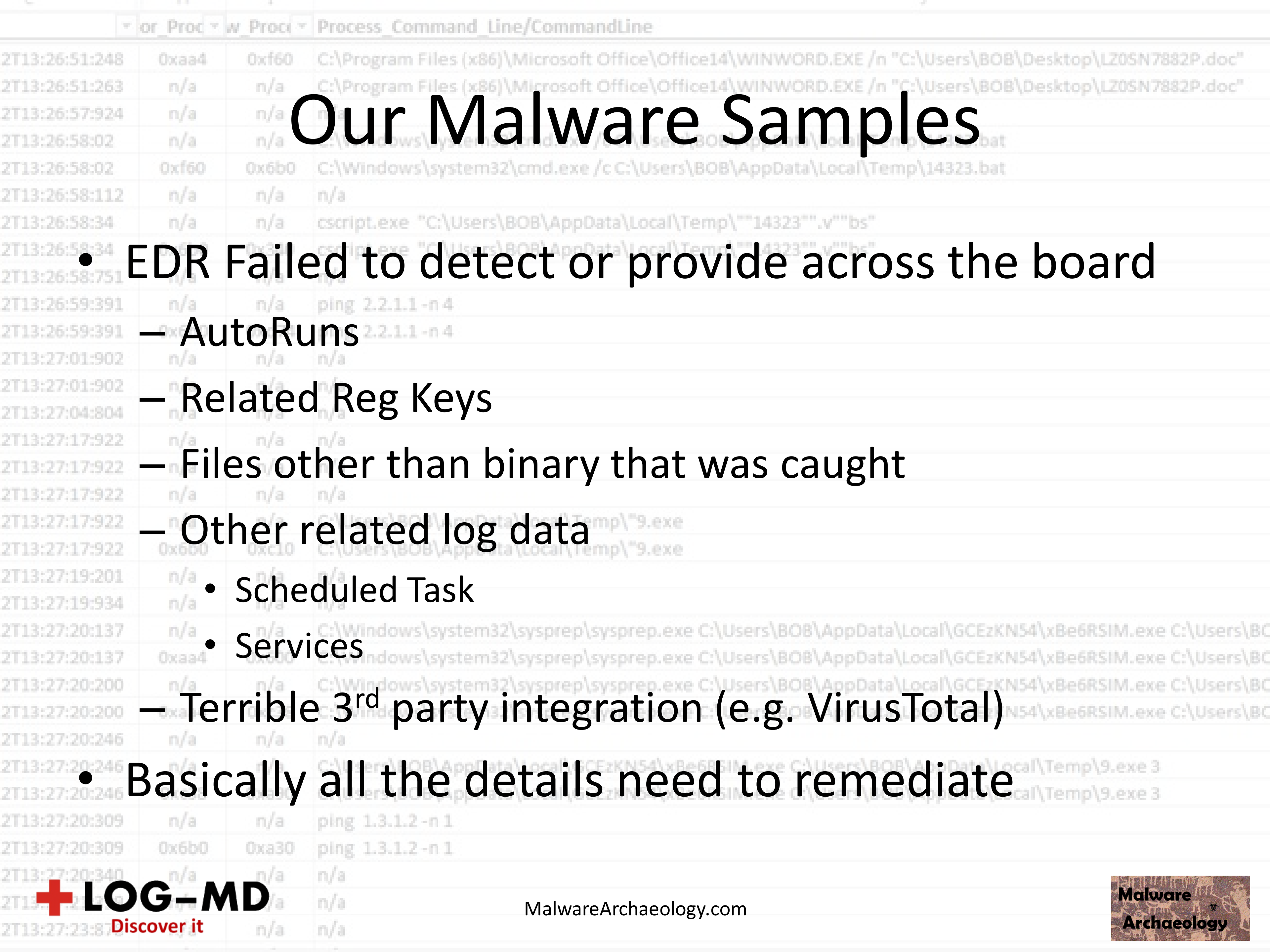
- Kovter gave us registry artifacts to test detection, also PowerShell calling out to the Internet
- Dridex gave us Dll side loading and morphing malware to show who was relying on hash lookups
- Gozi was typical commodity, but locked binary that was a challenge to delete post infection



```
           or_Proc  w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4   0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a     n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a     n/a     [illegible]
2T13:26:58:02   n/a     n/a     [illegible]
2T13:26:58:02   0xf60   0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a     n/a     n/a
2T13:26:58:34   n/a     n/a     cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0   0x340   [illegible]
2T13:26:58:751  [illegible]
2T13:26:59:391  n/a     n/a     ping 2.2.1.1 -n 4
2T13:26:59:391  [illegible]
2T13:27:01:902  n/a     n/a     n/a
2T13:27:01:902  [illegible]     n/a
2T13:27:04:804  [illegible]     n/a
2T13:27:17:922  n/a     n/a     n/a
2T13:27:17:922  [illegible]
2T13:27:17:922  [illegible]
2T13:27:17:922  n/a     n/a     C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922  [illegible]
2T13:27:19:201  n/a     n/a     n/a
2T13:27:19:934  [illegible]     n/a
2T13:27:20:137  [illegible]     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137  0xaa4   0x600   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  [illegible]
2T13:27:20:200  [illegible]
2T13:27:20:246  n/a     n/a     n/a
2T13:27:20:246  [illegible]
2T13:27:20:246  0xc38   0xa90   C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a     n/a     ping 1.3.1.2 -n 1
2T13:27:20:309  0x6b0   0xa30   ping 1.3.1.2 -n 1
2T13:27:20:340  n/a     n/a     n/a
[illegible]                     n/a
2T13:27:23:8[illegible]  n/a    n/a
```

Our Malware Samples

- EDR Failed to detect or provide across the board
  - AutoRuns
  - Related Reg Keys
  - Files other than binary that was caught
  - Other related log data
    - Scheduled Task
    - Services
  - Terrible 3rd party integration (e.g. VirusTotal)
- Basically all the details need to remediate



```
               or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4   0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a     n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a     n/a     n/a
2T13:26:58:02   n/a     n/a     C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60   0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a     n/a     n/a
2T13:26:58:34   n/a     n/a     cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0   0x3[illegible]   cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751  n/a     n/a     n/a
2T13:26:59:391  n/a     n/a     ping  2.2.1.1 -n 4
2T13:26:59:391  0x[illegible]   [illegible]   ping  2.2.1.1 -n 4
2T13:27:01:902  n/a     n/a     n/a
2T13:27:01:902  n/a     n/a     n/a
2T13:27:04:804  n/a     n/a     n/a
2T13:27:17:922  n/a     n/a     n/a
2T13:27:17:922  n/a     n/a     n/a
2T13:27:17:922  n/a     n/a     n/a
2T13:27:17:922  n/a     n/a     C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922  0x6b0   0xc10   C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201  n/a     n/a     n/a
2T13:27:19:934  n/a     n/a     n/a
2T13:27:20:137  n/a     n/a     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137  0xaa4   0x6b0   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200  n/a     n/a     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200  0xa[illegible]   [illegible]   [illegible]N54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246  n/a     n/a     n/a
2T13:27:20:246  n/a     n/a     C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  [illegible]   [illegible]   C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a     n/a     ping  1.3.1.2 -n 1
2T13:27:20:309  0x6b0   0xa30   ping  1.3.1.2 -n 1
2T13:27:20:340  n/a     n/a     n/a
2T1[illegible]  n/a     n/a     n/a
2T13:27:23:8[illegible]  n/a     n/a     n/a
```

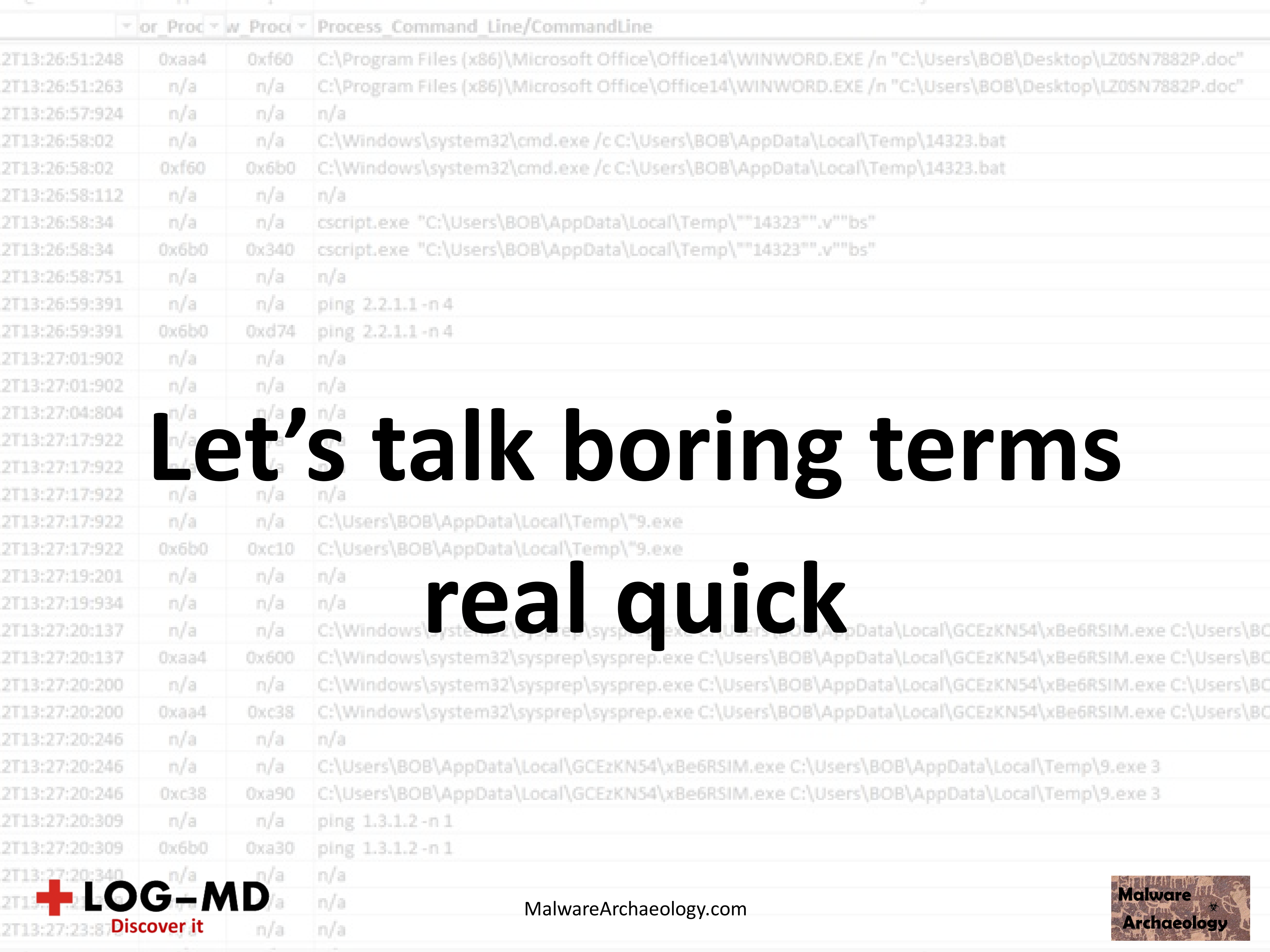
LOG-MD Discover it

MalwareArchaeology.com

Malware Archaeology

Our Baseline

- We have an IPS, it is surprisingly good
- The IPS alerted us to the system being infected for all 3 samples
- But an IPS alert gives you no details about the endpoint, so we have to investigate
- So we knew EDR needed to at least alert us that something was up, hopefully with details
- When on or ***off*** the corporate network



```
               or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248 0xaa4    0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263 n/a      n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924 n/a      n/a     n/a
2T13:26:58:02  n/a      n/a     C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02  0xf60    0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112 n/a      n/a     n/a
2T13:26:58:34  n/a      n/a     cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34  0x6b0    0x340   cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751 n/a      n/a     n/a
2T13:26:59:391 n/a      n/a     ping  2.2.1.1 -n 4
2T13:26:59:391 0x6b0    0xd74   ping  2.2.1.1 -n 4
2T13:27:01:902 n/a      n/a     n/a
2T13:27:01:902 n/a      n/a     n/a
2T13:27:04:804 n/a      n/a     n/a
2T13:27:17:922 n/a
2T13:27:17:922
2T13:27:17:922 n/a      n/a     n/a
2T13:27:17:922 n/a      n/a     C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922 0x6b0    0xc10   C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201 n/a      n/a     n/a
2T13:27:19:934 n/a      n/a     n/a
2T13:27:20:137 n/a      n/a     C:\Windows                                  pData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137 0xaa4    0x600   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200 n/a      n/a     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200 0xaa4    0xc38   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246 n/a      n/a     n/a
2T13:27:20:246 n/a      n/a     C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246 0xc38    0xa90   C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309 n/a      n/a     ping  1.3.1.2 -n 1
2T13:27:20:309 0x6b0    0xa30   ping  1.3.1.2 -n 1
2T13:27:20:340 n/a      n/a     n/a
2T1                     n/a     n/a
2T13:27:23:8            n/a     n/a
```

Let's talk boring terms real quick

LOG-MD Discover it

MalwareArchaeology.com

Malware Archaeology

Boring stuff first - Terms

Gartner and others defined these terms

ETDR – Endpoint Threat Detection & Response

The term used 2 years ago

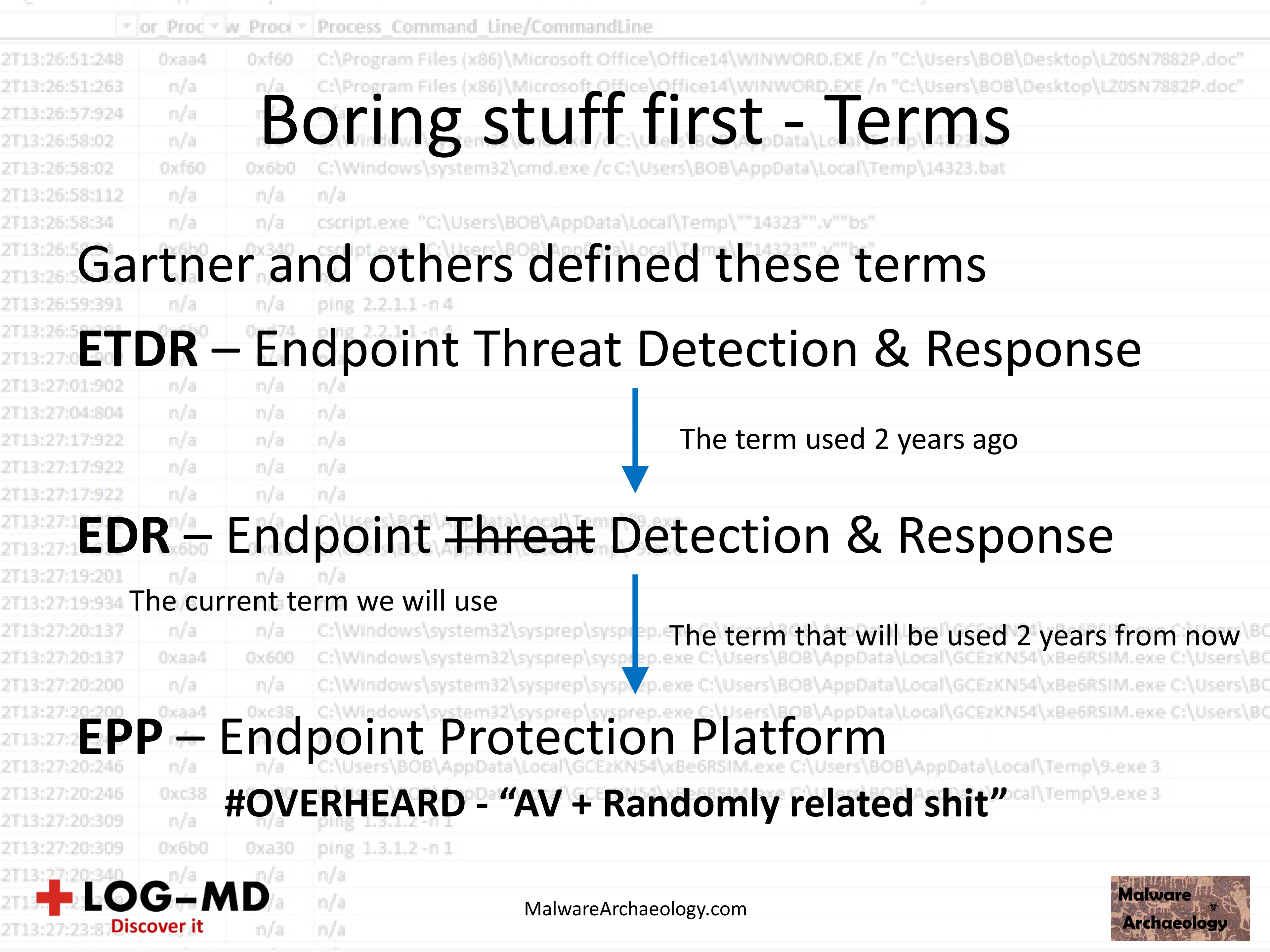
EDR – Endpoint ~~Threat~~ Detection & Response

The current term we will use

The term that will be used 2 years from now

EPP – Endpoint Protection Platform

#OVERHEARD - "AV + Randomly related shit"



```
or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4  0xf60  C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a    n/a    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a
2T13:26:58:02   n/a
2T13:26:58:02   0xf60  0x6b0  C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a    n/a    n/a
2T13:26:58:34   n/a    n/a    cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:59:391  n/a    n/a    ping 2.2.1.1 -n 4
2T13:27:01:902  n/a    n/a    n/a
2T13:27:04:804  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:19:201  n/a    n/a    n/a
2T13:27:19:934
2T13:27:20:137  n/a    n/a    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137  0xaa4  0x600  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  n/a    n/a    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  0xaa4  0xc38  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246  n/a    n/a    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  0xc38
2T13:27:20:309  n/a
2T13:27:20:309  0x6b0  0xa30  ping 1.3.1.2 -n 1
2T13:27:20:340  n/a    n/a    n/a
```

LOG-MD Discover it

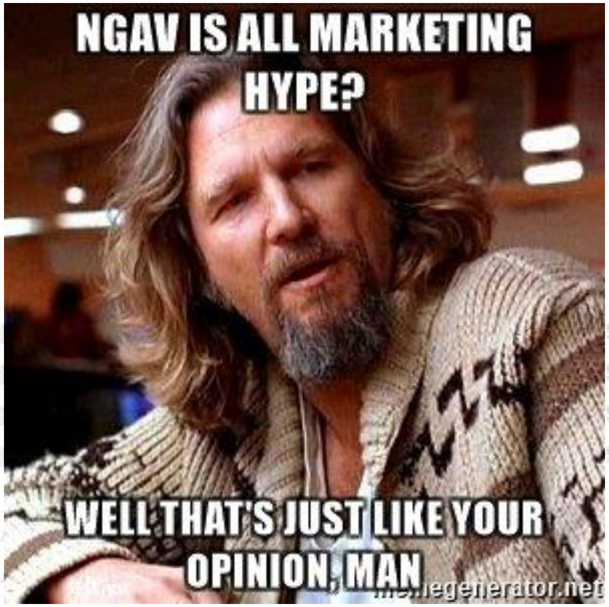
MalwareArchaeology.com

Malware Archaeology

Boring stuff first - Terms

Next-Gen AV

- Might have evolved from vendors trying to get the PCI certification


NGAV IS ALL MARKETING HYPE?
WELL THAT'S JUST LIKE YOUR OPINION, MAN
memegenerator.net

- It is a dead term, or so Gartner wants it to be
  - So we agree to kill it, because AV is AV

Endpoint Protection Platform (EPP) Definition

End Point Protection Platforms (EPP) are enterprise security platforms that protect PCs, mobile devices and server environments from malware, spyware, rootkits, trojans and worms. Platforms may include technologies such as:

- signature based malware/spyware detection and removal
- personal firewalls
- host based intrusion prevention systems (HIPS)
- application whitelisting
- data protection (e.g. file encryption)
- malicious website blocking
- file reputation systems
- security management and reporting

- In short, EPP products typically employ a cocktail approach to protect devices and servers from malware.

#OVERHEARD - “AV + Randomly related shit”

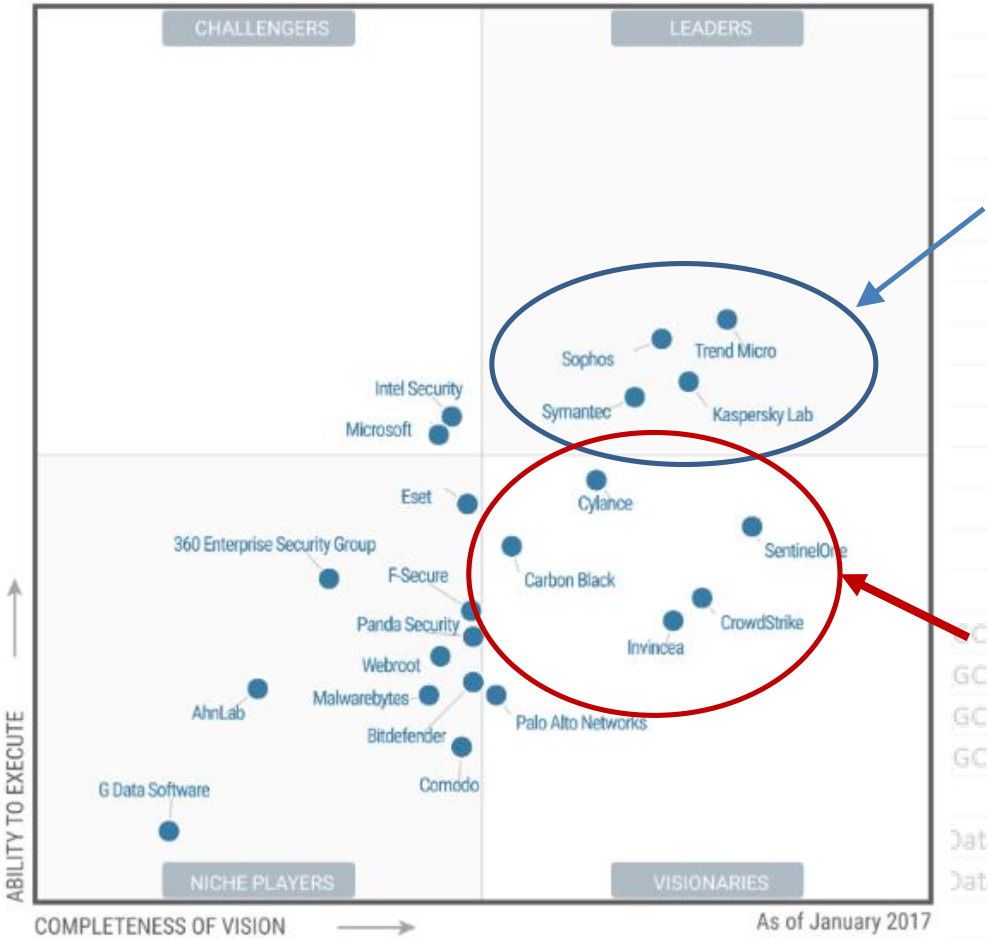
arch.simplicable.com

Endpoint Protection Platform (EPP) Definition

- Gartner
  - An endpoint protection platform (EPP) is a solution that **converges endpoint device security functionality into a single product that delivers antivirus, anti-spyware, personal firewall, application control and other styles of host intrusion prevention** (for example, behavioral blocking) capabilities into a single and cohesive solution…

#OVERHEARD - “AV + Randomly related shit”

The EPP Magic Quadrant



Source: Gartner (January 2017)

The typical AV Suites Errrr… Platforms

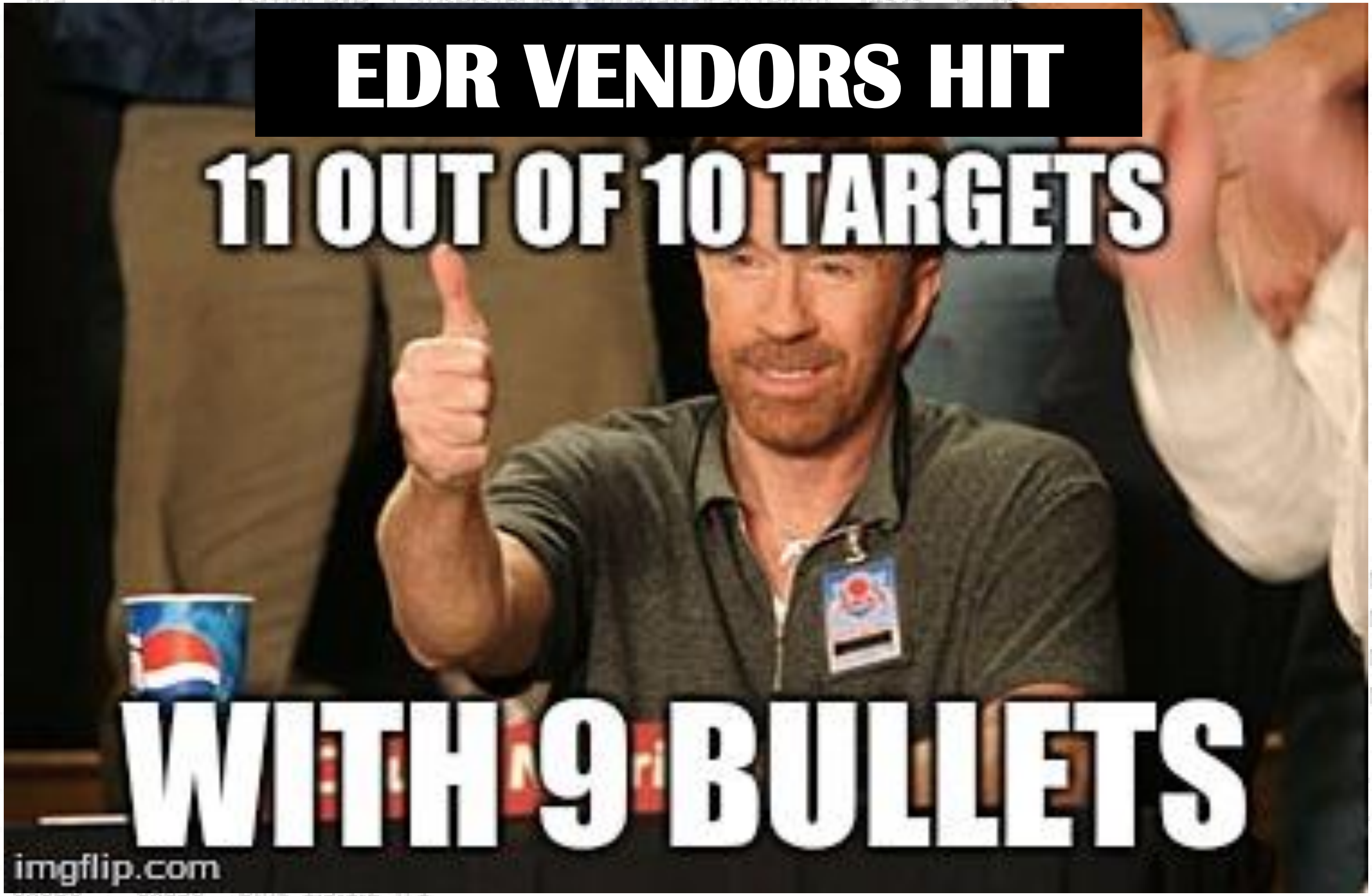
The up and coming EDR solutions

LOG-MD Discover it

MalwareArchaeology.com

Malware Archaeology

How I felt after weeks of testing

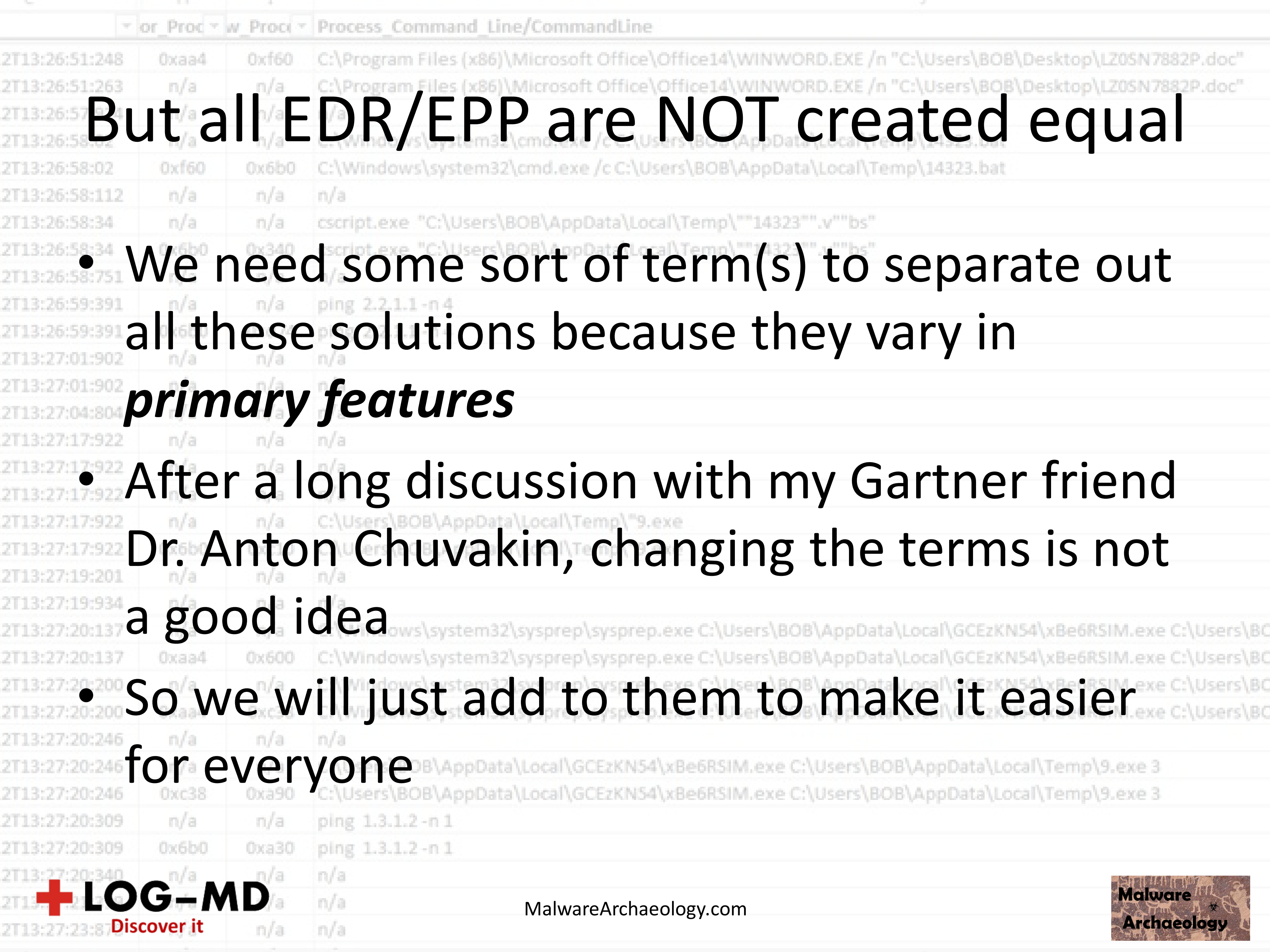


There are lots of vendors

cybereason	Bit9 + CARBON BLACK	CISCO fireAMP™	paloalto Traps	McAfee AR2-DAC
SECDO	TANIUM	RSA ECAT	SandBlast Check Point	Symantec SEP14
CYLANCE	CounterTack	FireEye HX MANDIANT	MORPHISEC	TREND MICRO OfficeScan XG
red canary	CYBERARK	SentinelOne	NYOTRON	INTERCEPT X SOPHOS
ENDGAME.	ENSILO	BUFFERZONE	MINERVA	KASPERSKY ANTI TARGETED KASPERSKY lab
Fidelis Cybersecurity	CROWDSTRIKE	IBM Trusteer	Malwarebytes ANTI-EXPLOIT	FORCEPOINT

But all EDR/EPP are NOT created equal

- We need some sort of term(s) to separate out all these solutions because they vary in ***primary features***
- After a long discussion with my Gartner friend Dr. Anton Chuvakin, changing the terms is not a good idea
- So we will just add to them to make it easier for everyone



```
               or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4   0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a     n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:58:02   0xf60   0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a     n/a     n/a
2T13:26:58:34   n/a     n/a     cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:59:391  n/a     n/a     ping 2.2.1.1 -n 4
2T13:27:01:902  n/a     n/a     n/a
2T13:27:17:922  n/a     n/a     n/a
2T13:27:17:922  n/a     n/a     C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201  n/a     n/a     n/a
2T13:27:20:137  0xaa4   0x600   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246  n/a     n/a     n/a
2T13:27:20:246  0xc38   0xa90   C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a     n/a     ping 1.3.1.2 -n 1
2T13:27:20:309  0x6b0   0xa30   ping 1.3.1.2 -n 1
```

LOG-MD Discover it

MalwareArchaeology.com

Malware Archaeology

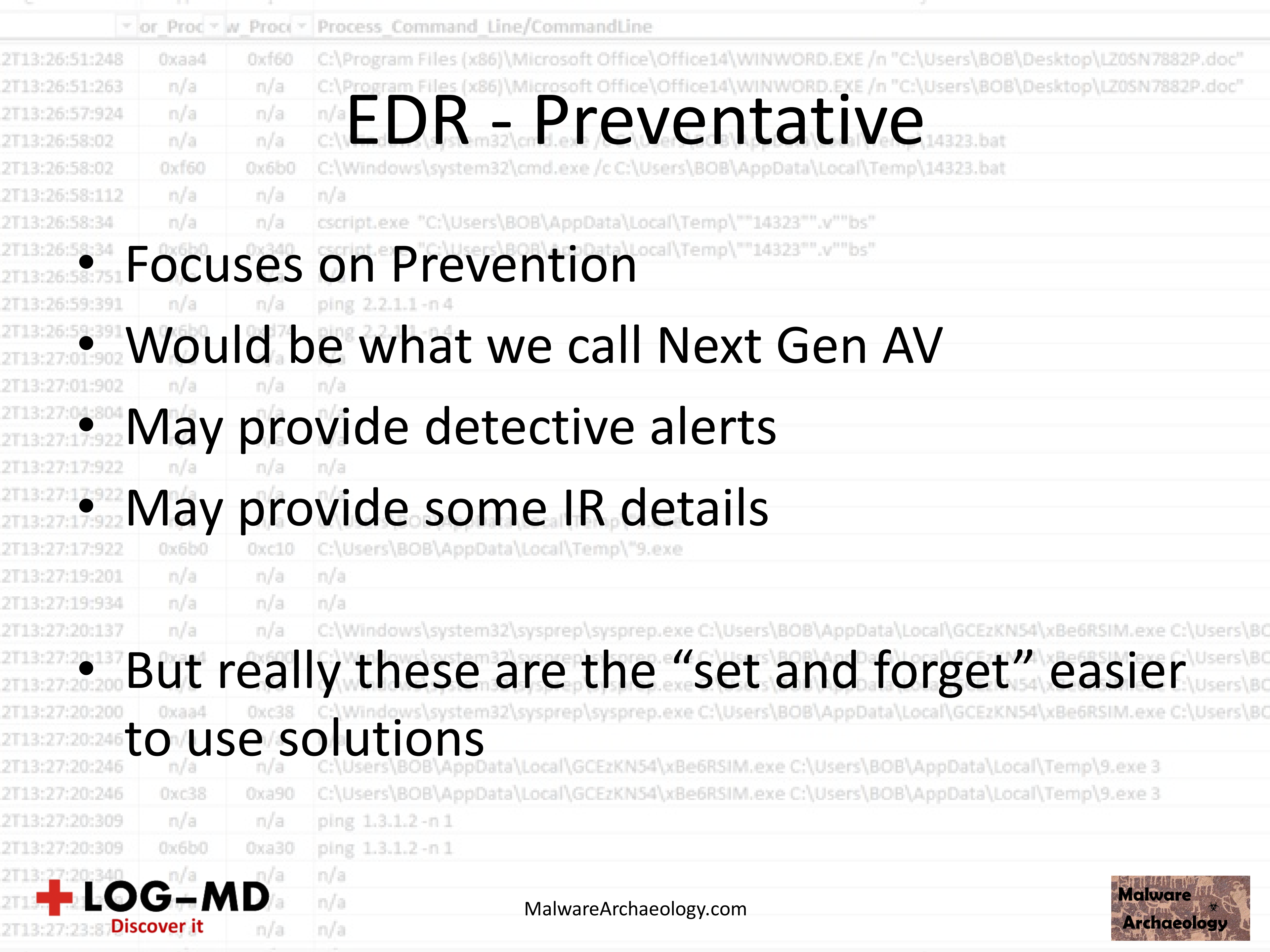
Improved Terms

- Use these two as they are current and the future
  - **EDR and EPP**
- We will add extensions so that we can break up the solutions into logical functions
  - **EDR – Preventative**
  - **EDR – Detective and Information**
  - **EDR – IR** or Incident Response
  - **EPP** – Has a Platform currently (Traditional AV)
  - **EPP – Eco Systems** – Mixes network with endpoint

EDR - Preventative

- Focuses on Prevention
- Would be what we call Next Gen AV
- May provide detective alerts
- May provide some IR details

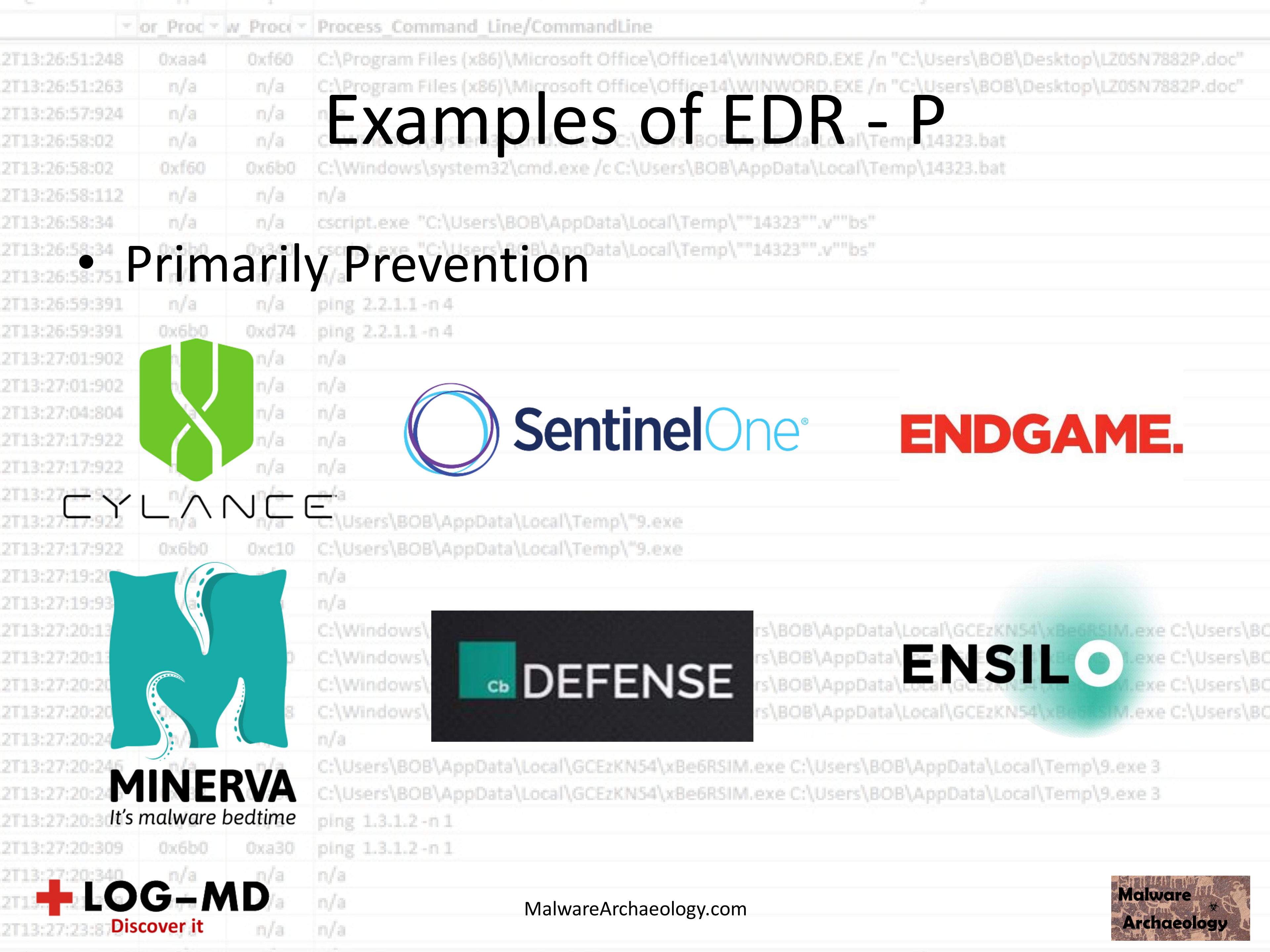
- But really these are the “set and forget” easier to use solutions



```
           or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4  0xf60  C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a    n/a    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a    n/a    n/a
2T13:26:58:02   n/a    n/a    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60  0x6b0  C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a    n/a    n/a
2T13:26:58:34   n/a    n/a    cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0  0x340  cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751  n/a    n/a    n/a
2T13:26:59:391  n/a    n/a    ping 2.2.1.1 -n 4
2T13:26:59:391  0x6b0  0xd74  ping 2.2.1.1 -n 4
2T13:27:01:902  n/a    n/a    n/a
2T13:27:01:902  n/a    n/a    n/a
2T13:27:04:804  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922  0x6b0  0xc10  C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201  n/a    n/a    n/a
2T13:27:19:934  n/a    n/a    n/a
2T13:27:20:137  n/a    n/a    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137  0xaa4  0x600  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200  n/a    n/a    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200  0xaa4  0xc38  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246  n/a    n/a    n/a
2T13:27:20:246  n/a    n/a    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  0xc38  0xa90  C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a    n/a    ping 1.3.1.2 -n 1
2T13:27:20:309  0x6b0  0xa30  ping 1.3.1.2 -n 1
2T13:27:20:340  n/a    n/a    n/a
2T1[illegible]  n/a    n/a    n/a
2T13:27:23:8[illegible]  n/a  n/a  n/a
```

Examples of EDR - P

- Primarily Prevention



	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	[illegible]
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x3[illegible]	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:2[illegible]	[illegible]	[illegible]	n/a
2T13:27:19:93[illegible]	[illegible]	[illegible]	n/a
2T13:27:20:1[illegible]	[illegible]	[illegible]	C:\Windows\[illegible]rs\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:1[illegible]	[illegible]	[illegible]	C:\Windows\[illegible]rs\BOB\AppData\[illegible].exe C:\Users\BO
2T13:27:20:2[illegible]	[illegible]	[illegible]	C:\Windows\[illegible]rs\BOB\AppData\[illegible].exe C:\Users\BO
2T13:27:20:2[illegible]	[illegible]	[illegible]	C:\Windows\[illegible]rs\BOB\AppData\Local\GCEzKN54\x[illegible]SIM.exe C:\Users\BO
2T13:27:20:24[illegible]	[illegible]	[illegible]	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:2[illegible]	[illegible]	[illegible]	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:3[illegible]	[illegible]	[illegible]	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T1[illegible]	[illegible]	n/a	n/a
2T13:27:23:8[illegible]	[illegible]	n/a	n/a

CYLANCE

SentinelOne

ENDGAME.

MINERVA
It's malware bedtime

Cb DEFENSE

ENSILO

LOG-MD
Discover it

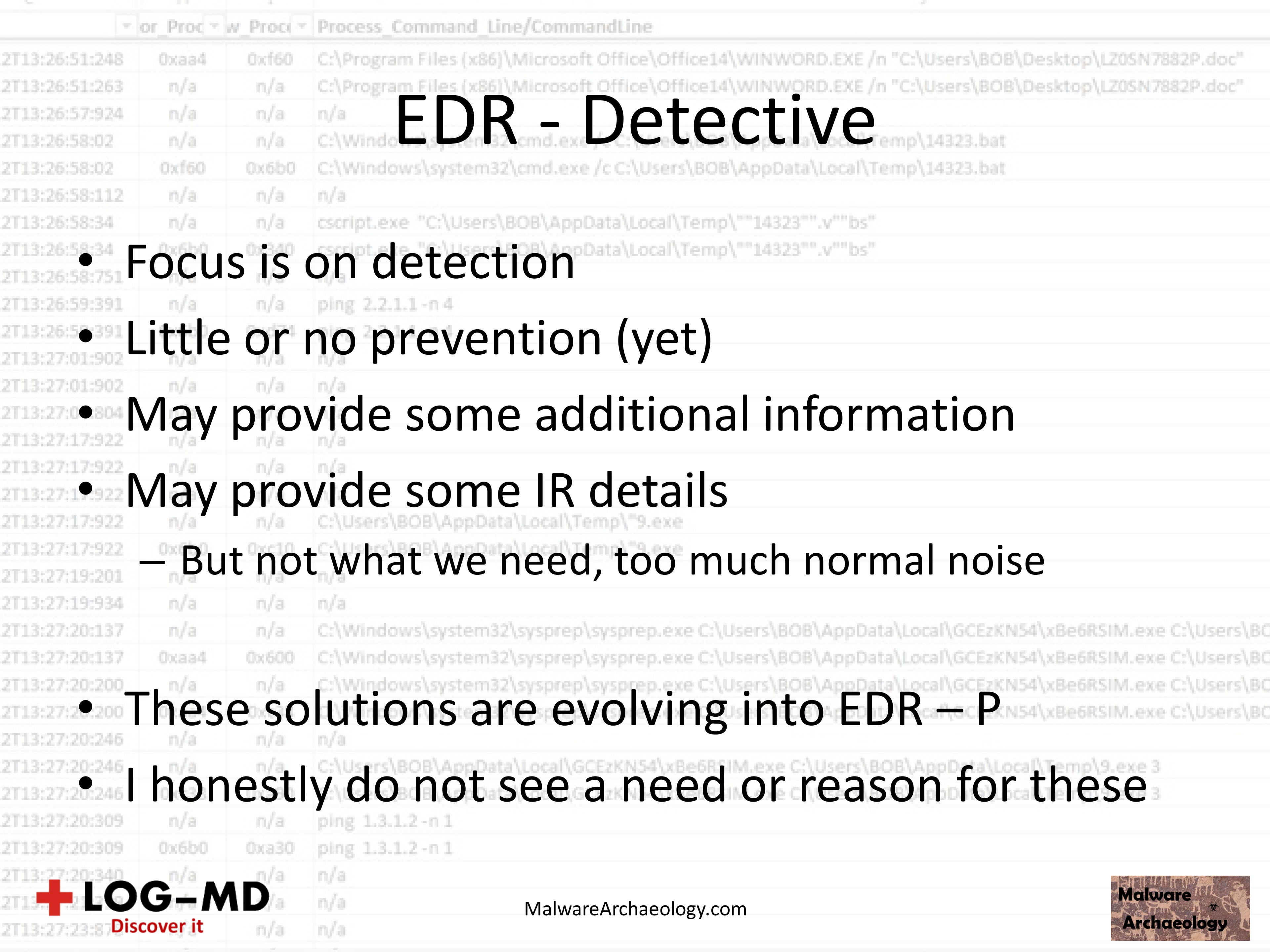
MalwareArchaeology.com

Malware Archaeology

EDR - Detective

- Focus is on detection
- Little or no prevention (yet)
- May provide some additional information
- May provide some IR details
  - – But not what we need, too much normal noise

- These solutions are evolving into EDR – P
- I honestly do not see a need or reason for these



	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windo[illegible]cmd.exe [illegible]emp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x840	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	[illegible]	[illegible]	[illegible]
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:5[illegible]391	[illegible]	[illegible]	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:0[illegible]804	[illegible]	[illegible]	[illegible]
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:1[illegible]922	[illegible]	[illegible]	[illegible]
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	[illegible]	[illegible]	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:2[illegible]200	[illegible]	[illegible]	[illegible]KN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:2[illegible]246	[illegible]	[illegible]	[illegible] 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T1[illegible]	[illegible]	[illegible]	n/a
2T13:27:23:8[illegible]	[illegible]	n/a	n/a

Examples of EDR - D

- Primarily Detective and Information

cybereason

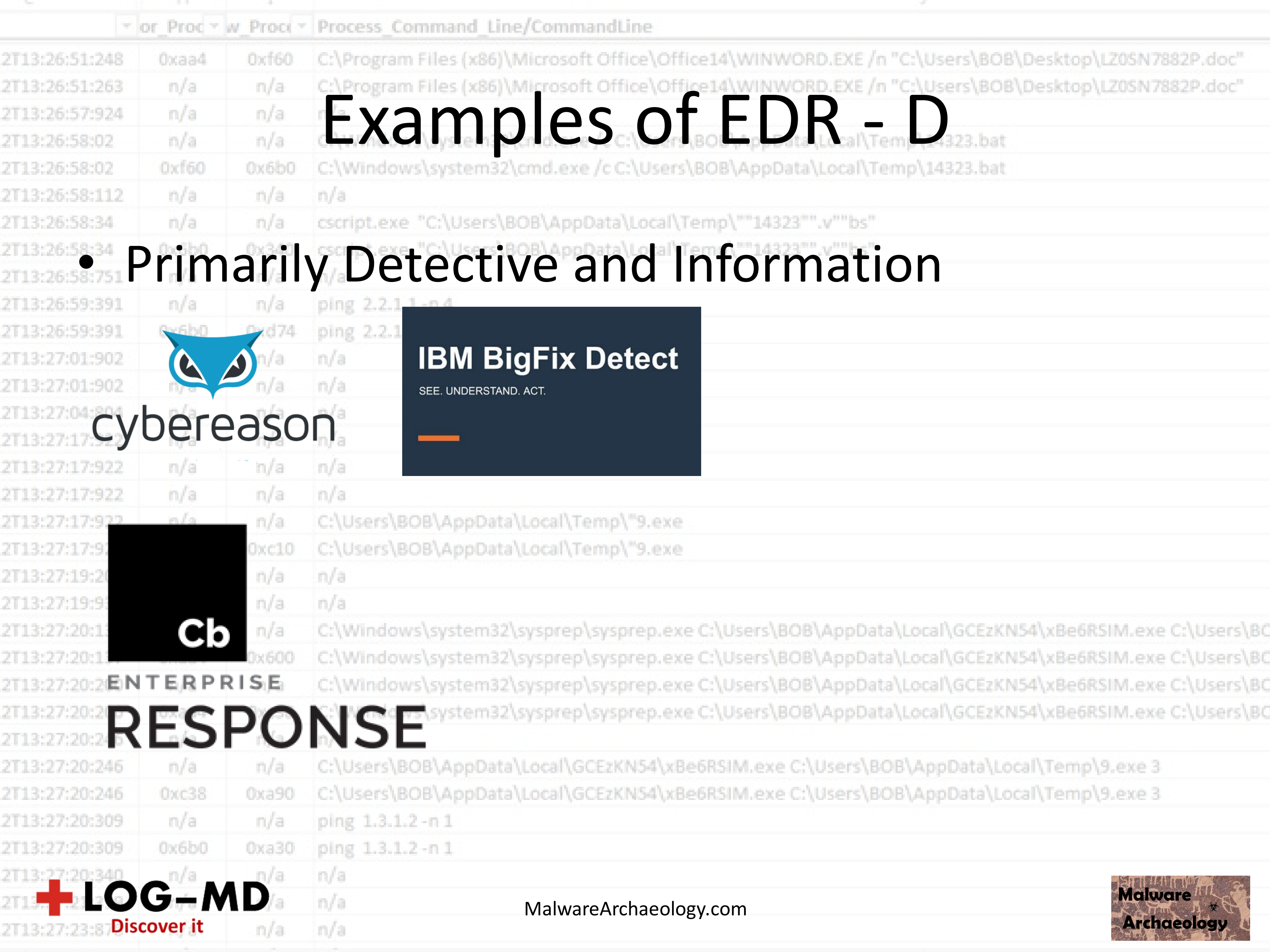
IBM BigFix Detect

SEE. UNDERSTAND. ACT.

Cb

ENTERPRISE

RESPONSE



```
               or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4    0xf60    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a      n/a      C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a      n/a
2T13:26:58:02   n/a      n/a                                        C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60    0x6b0    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a      n/a      n/a
2T13:26:58:34   n/a      n/a      cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0             cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751                    n/a
2T13:26:59:391  n/a      n/a      ping 2.2.1.1 -n 4
2T13:26:59:391  0x6b0    0xd74    ping 2.2.1
2T13:27:01:902           n/a      n/a
2T13:27:01:902           n/a      n/a
2T13:27:04:804                    n/a
2T13:27:17                        n/a
2T13:27:17:922  n/a      n/a      n/a
2T13:27:17:922  n/a      n/a      n/a
2T13:27:17:922           n/a      C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:9             0xc10    C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:2             n/a      n/a
2T13:27:19:9             n/a      n/a
2T13:27:20:1             n/a      C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:1             0x600    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:2                      C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:2                                 system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:2
2T13:27:20:246  n/a      n/a      C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  0xc38    0xa90    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a      n/a      ping 1.3.1.2 -n 1
2T13:27:20:309  0x6b0    0xa30    ping 1.3.1.2 -n 1
2T13:27:20:340  n/a      n/a      n/a
2T1                               n/a
2T13:27:23:8             n/a      n/a
```

LOG-MD Discover it

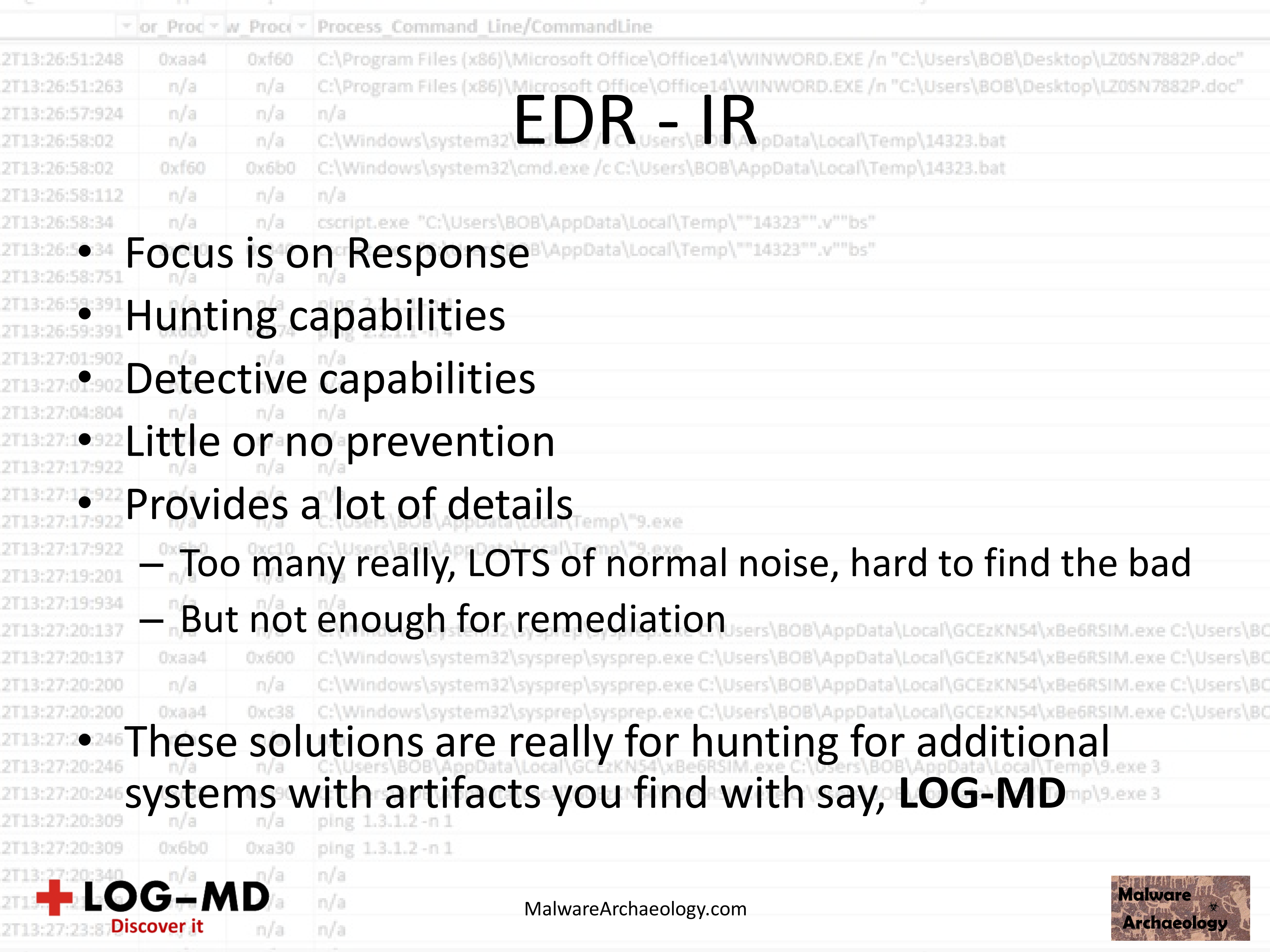
MalwareArchaeology.com

Malware Archaeology

EDR - IR

- Focus is on Response
- Hunting capabilities
- Detective capabilities
- Little or no prevention
- Provides a lot of details
  - Too many really, LOTS of normal noise, hard to find the bad
  - But not enough for remediation

- These solutions are really for hunting for additional systems with artifacts you find with say, **LOG-MD**



```
                 or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248   0xaa4     0xf60    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263   n/a       n/a      C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924   n/a       n/a      n/a
2T13:26:58:02    n/a       n/a      C:\Windows\system32\[illegible] C:\Users\[illegible]pData\Local\Temp\14323.bat
2T13:26:58:02    0xf60     0x6b0    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112   n/a       n/a      n/a
2T13:26:58:34    n/a       n/a      cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:[illegible]34 [illegible] [illegible] [illegible]B\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751   n/a       n/a      n/a
2T13:26:5[illegible]391 n/a    n/a      ping 2.2.1.1 -n 4
2T13:26:59:391   0x6b0     [illegible] ping 2.2.1.1 -n 4
2T13:27:01:902   n/a       n/a      n/a
2T13:27:0[illegible]902 [illegible] [illegible] [illegible]
2T13:27:04:804   n/a       n/a      n/a
2T13:27:1[illegible]922 [illegible] [illegible] [illegible]
2T13:27:17:922   n/a       n/a      n/a
2T13:27:1[illegible]922 n/a    n/a      n/a
2T13:27:17:922   n/a       n/a      C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922   0x6b0     0xc10    C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201   n/a       n/a      n/a
2T13:27:19:934   n/a       n/a      n/a
2T13:27:20:137   n/a       n/a      C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137   0xaa4     0x600    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200   n/a       n/a      C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200   0xaa4     0xc38    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:[illegible]246 [illegible] [illegible] [illegible]
2T13:27:20:246   n/a       n/a      C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246   [illegible] [illegible] [illegible]mp\9.exe 3
2T13:27:20:309   n/a       n/a      ping 1.3.1.2 -n 1
2T13:27:20:309   0x6b0     0xa30    ping 1.3.1.2 -n 1
2T13:27:20:340   n/a       n/a      n/a
2T1[illegible]   [illegible] n/a    n/a
2T13:27:23:8[illegible] [illegible] n/a n/a
```

LOG-MD
Discover it

MalwareArchaeology.com

Malware Archaeology

Examples of EDR - IR

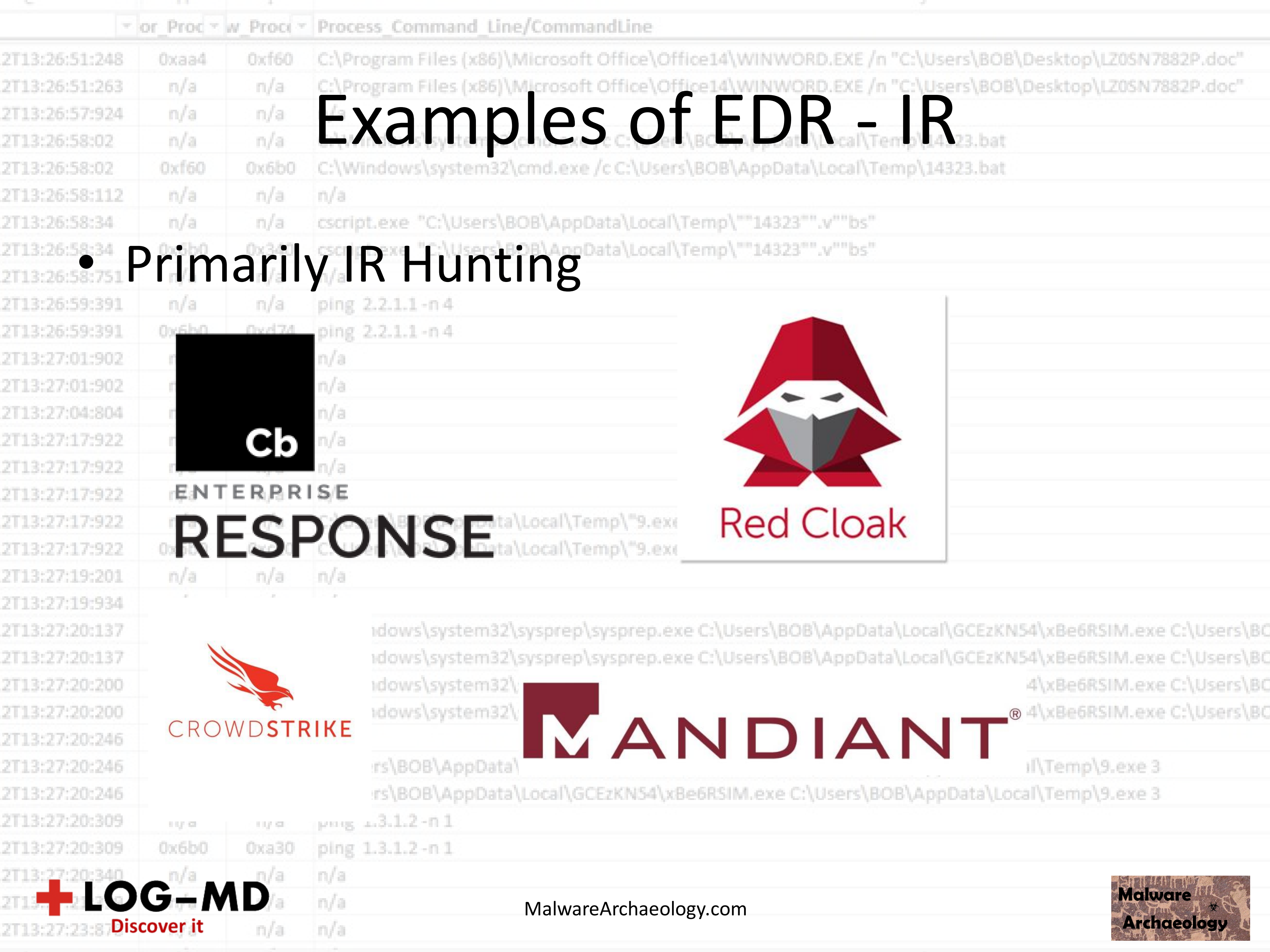
- Primarily IR Hunting

Cb
ENTERPRISE
RESPONSE

Red Cloak

CROWDSTRIKE

MANDIANT®



```
       or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4   0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a     n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a     n/a
2T13:26:58:02   n/a     n/a     C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60   0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a     n/a     n/a
2T13:26:58:34   n/a     n/a     cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0   0x3     cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751  n/a     n/a     n/a
2T13:26:59:391  n/a     n/a     ping  2.2.1.1 -n 4
2T13:26:59:391  0x6b0   0xd74   ping  2.2.1.1 -n 4
2T13:27:01:902                  n/a
2T13:27:01:902                  n/a
2T13:27:04:804                  n/a
2T13:27:17:922                  n/a
2T13:27:17:922                  n/a
2T13:27:17:922
2T13:27:17:922                  C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922  0x              C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201  n/a     n/a     n/a
2T13:27:19:934
2T13:27:20:137                    ndows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137                    ndows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200                    ndows\system32\                                   4\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200                    ndows\system32\                                   4\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246
2T13:27:20:246                    rs\BOB\AppData\                                   l\Temp\9.exe 3
2T13:27:20:246                    rs\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a     n/a     ping  1.3.1.2 -n 1
2T13:27:20:309  0x6b0   0xa30   ping  1.3.1.2 -n 1
2T13:27:20:340  n/a     n/a     n/a
2T1                     n/a     n/a
2T13:27:23:8            n/a     n/a
```

EPP - Eco Systems

- These are total solutions
- Yes, Platforms
- Endpoint
- Web Gateway
- Network
- Email
- Etc.

Examples of EPP – Eco Systems

- Covering the endpoint, network, web, email

CISCO AMP Threat Grid

CISCO SOURCEfire

CISCO Cisco Umbrella

RSA ECAT
Endpoint Threat Detection
Expose More. Analyze Faster. Respond Better.
EMC
RSA

FireEye™

MANDIANT®

```
                 or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248   0xaa4     0xf60    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263   n/a       n/a      C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924   n/a       n/a      n/a
2T13:26:58:02    n/a       n/a      C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02    0xf60     0x6b0    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112   n/a       n/a      n/a
2T13:26:58:34    n/a       n/a      cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34    0x6b0
2T13:26:58:751   n/a
2T13:26:59:391   n/a
2T13:26:59:391   0x6b0
2T13:27:01:902   n/a
2T13:27:01:902   n/a
2T13:27:04:804   n/a
2T13:27:17:922   n/a
2T13:27:17:922   n/a
2T13:27:17:922   n/a
2T13:27:17:922   n/a
2T13:27:17:922   0x6b0
2T13:27:19:201   n/a
2T13:27:19:934   n/a
2T13:27:20:137   n/a                                                      4\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137   0xaa4                                                    4\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200   n/a                                                      4\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200   0xaa4                                                    4\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246   n/a
2T13:27:20:246   n/a                                                      l\Temp\9.exe 3
2T13:27:20:246   0xc38     0xa90    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309   n/a       n/a      ping 1.3.1.2 -n 1
2T13:27:20:309   0x6b0     0xa30    ping 1.3.1.2 -n 1
2T13:27:20:340   n/a       n/a      n/a
2T1                        a        n/a
2T13:27:23:87              n/a      n/a
```

What did we expect?

- Some decent results
- We expected many or most of the solutions to catch what our IPS caught as that is what we would measure against, our baseline
- If the IPS caught something and alerted us to "**HEY! Look at that system!!!**"
- Then EDR should do the same
- And give us all kinds of details…

And what we were treated to after weeks of testing…

What we tested

- We did NOT test the following:
  - **Eco Systems** – we were not going to do a forklift upgrade and go all out on Cisco AMP, RSA ECAT, or Mandiant/FireEye
  - **EPP** – We did not test the typical AV with all the bells and whistles
  - **Sandbox solutions** – We know this would provide a lot of detail of what malware does on infection, but we have **LOG-MD** and with roughly 30% of malware that detects sandboxes, we opted not to go this route
  - Any Managed Service Providers

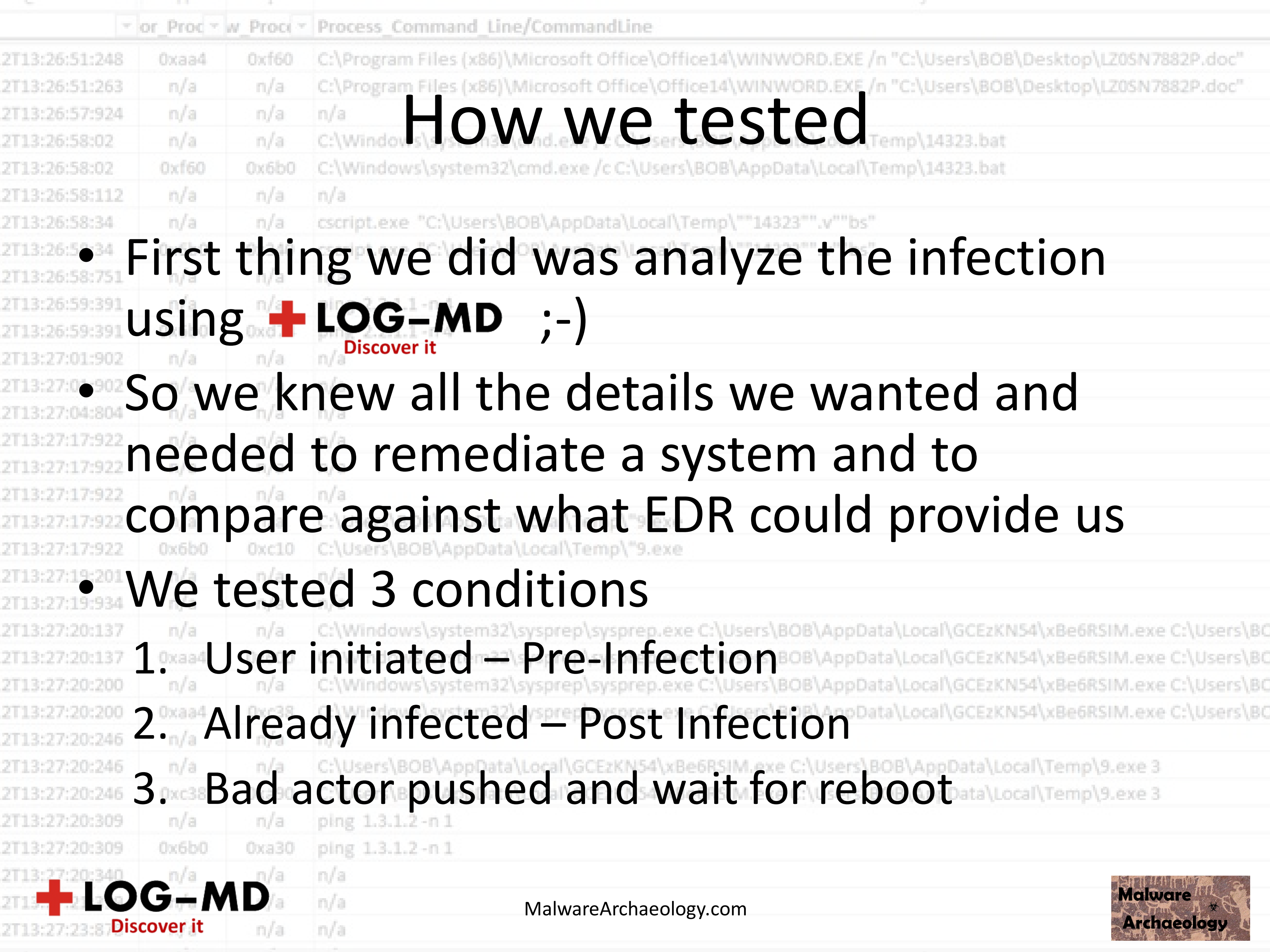
What we tested

- EDR – Preventative solutions (NG-AV)
- EDR – Detective and Information solutions
- EDR – Incident Response solutions

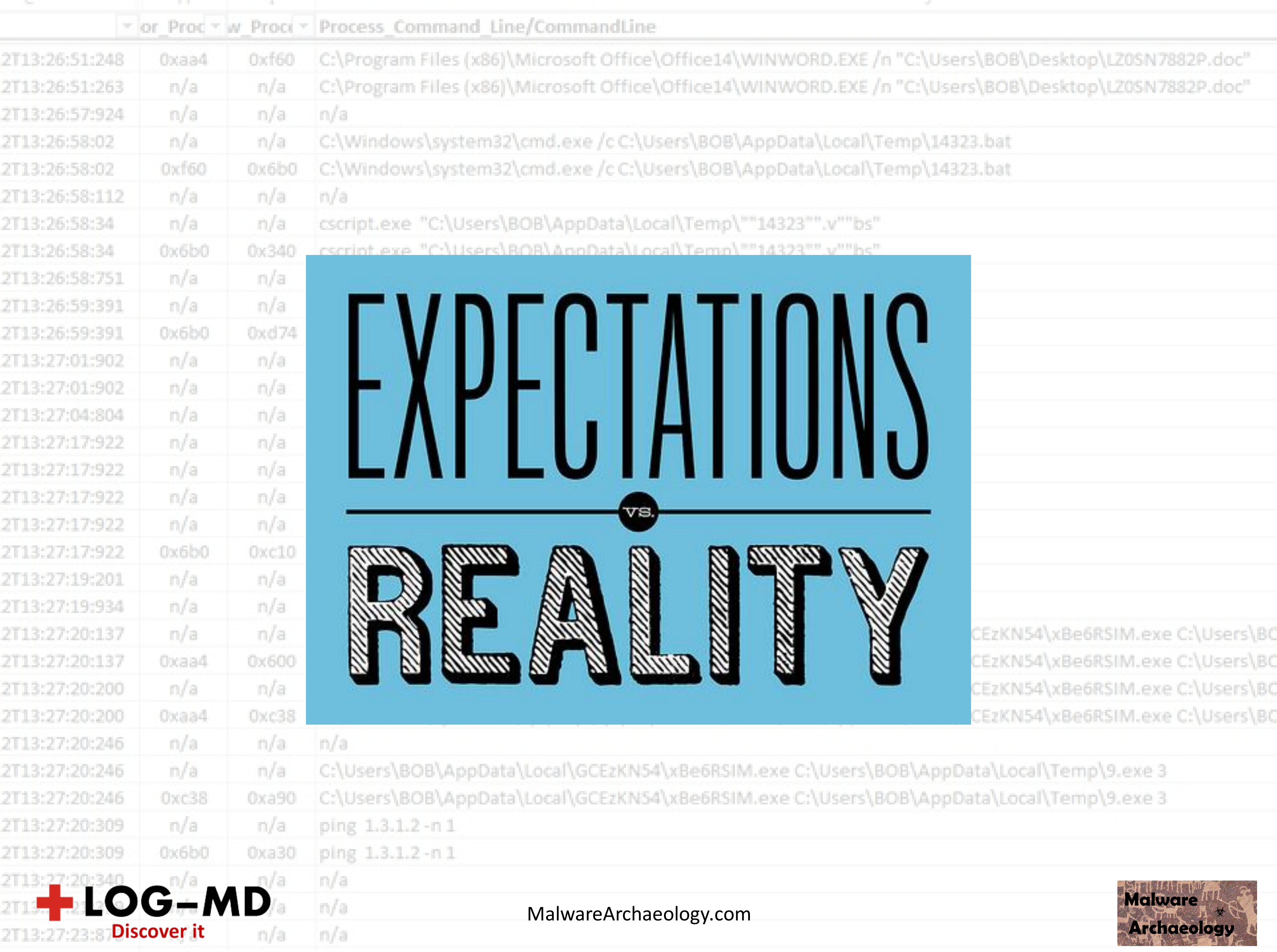
- The typical up and coming EDR solutions that InfoSec would own and manage

How we tested

- First thing we did was analyze the infection using LOG-MD Discover it ;-)
- So we knew all the details we wanted and needed to remediate a system and to compare against what EDR could provide us
- We tested 3 conditions
  1. User initiated – Pre-Infection
  2. Already infected – Post Infection
  3. Bad actor pushed and wait for reboot



```
               or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248 0xaa4    0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263 n/a      n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924 n/a      n/a     n/a
2T13:26:58:02  n/a      n/a     C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02  0xf60    0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112 n/a      n/a     n/a
2T13:26:58:34  n/a      n/a     cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34  [illegible]
2T13:26:58:751 n/a      n/a     [illegible]
2T13:26:59:391 n/a      n/a     ping 2.2.1.1 -n 4
2T13:26:59:391 0x6b0    0xd[illegible] ping 2.2.1.1 -n 4
2T13:27:01:902 n/a      n/a     n/a
2T13:27:0[illegible]902 n/a n/a n/a
2T13:27:04:804 n/a      n/a     n/a
2T13:27:17:922 n/a      n/a     n/a
2T13:27:17:922 [illegible]
2T13:27:17:922 n/a      n/a     n/a
2T13:27:17:922 [illegible]
2T13:27:17:922 0x6b0    0xc10   C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201 n/a      n/a     n/a
2T13:27:19:934 [illegible]
2T13:27:20:137 n/a      n/a     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137 0xaa4    [illegible] C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200 n/a      n/a     C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200 0xaa4    0xc38   C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246 n/a      n/a     n/a
2T13:27:20:246 n/a      n/a     C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246 0xc38    [illegible] C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309 n/a      n/a     ping 1.3.1.2 -n 1
2T13:27:20:309 0x6b0    0xa30   ping 1.3.1.2 -n 1
2T13:27:20:340 n/a      n/a     n/a
2T1[illegible] n/a      n/a     n/a
2T13:27:23:8[illegible] n/a n/a n/a
```



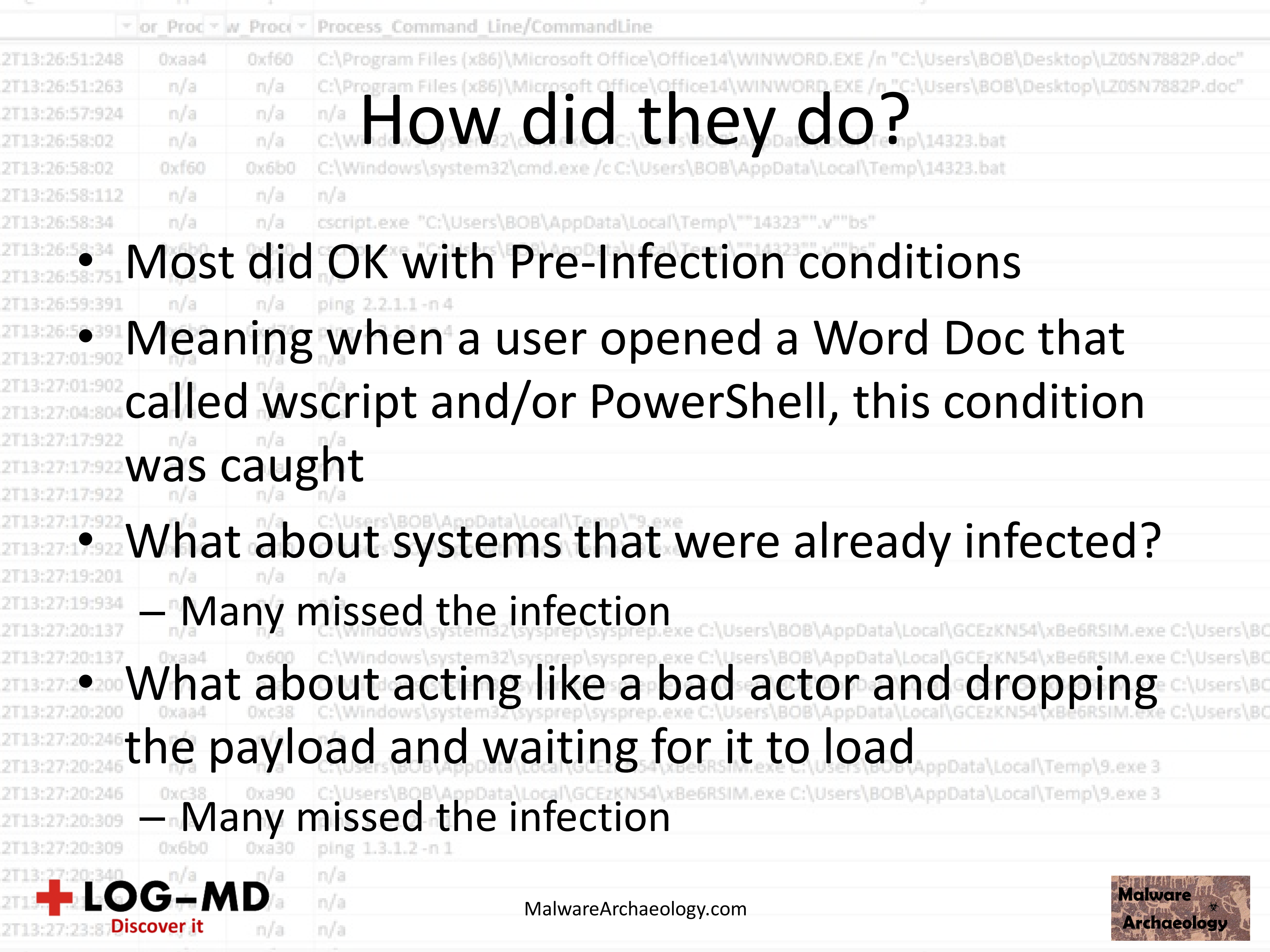
```
               or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4   0xf60   C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a     n/a     C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a     n/a     n/a
2T13:26:58:02   n/a     n/a     C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60   0x6b0   C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a     n/a     n/a
2T13:26:58:34   n/a     n/a     cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0   0x340   cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751  n/a     n/a
2T13:26:59:391  n/a     n/a
2T13:26:59:391  0x6b0   0xd74
2T13:27:01:902  n/a     n/a
2T13:27:01:902  n/a     n/a
2T13:27:04:804  n/a     n/a
2T13:27:17:922  n/a     n/a
2T13:27:17:922  n/a     n/a
2T13:27:17:922  n/a     n/a
2T13:27:17:922  n/a     n/a
2T13:27:17:922  0x6b0   0xc10
2T13:27:19:201  n/a     n/a
2T13:27:19:934  n/a     n/a
2T13:27:20:137  n/a     n/a     CEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137  0xaa4   0x600   CEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200  n/a     n/a     CEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200  0xaa4   0xc38   CEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246  n/a     n/a     n/a
2T13:27:20:246  n/a     n/a     C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  0xc38   0xa90   C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a     n/a     ping  1.3.1.2 -n 1
2T13:27:20:309  0x6b0   0xa30   ping  1.3.1.2 -n 1
2T13:27:20:340  n/a     n/a     n/a
2T1                     n/a     n/a
2T13:27:23:87           n/a     n/a
```

LOG-MD
Discover it

Malware Archaeology

How did they do?

- Most did OK with Pre-Infection conditions
- Meaning when a user opened a Word Doc that called wscript and/or PowerShell, this condition was caught
- What about systems that were already infected?
  - Many missed the infection
- What about acting like a bad actor and dropping the payload and waiting for it to load
  - Many missed the infection



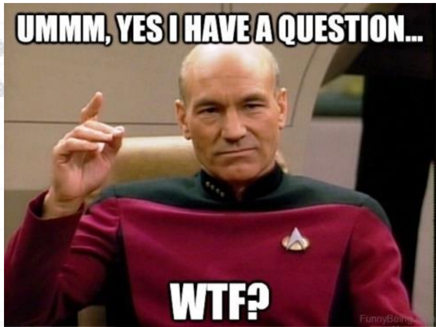
```
           or_Proc  w_Proc  Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4  0xf60  C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a    n/a    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a    n/a    n/a
2T13:26:58:02   n/a    n/a    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60  0x6b0  C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a    n/a    n/a
2T13:26:58:34   n/a    n/a    cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0  [illegible]  cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751  n/a    n/a    n/a
2T13:26:59:391  n/a    n/a    ping 2.2.1.1 -n 4
2T13:26:59:391  [illegible]  [illegible]  ping 2.2.1.1 -n 4
2T13:27:01:902  n/a    n/a    n/a
2T13:27:01:902  n/a    n/a    n/a
2T13:27:04:804  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  [illegible]  [illegible]  [illegible]
2T13:27:17:922  n/a    n/a    n/a
2T13:27:17:922  n/a    n/a    C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922  0x6b0  [illegible]  C:\Users\BOB\AppData\Local\Temp\9.exe
2T13:27:19:201  n/a    n/a    n/a
2T13:27:19:934  n/a    n/a    n/a
2T13:27:20:137  n/a    n/a    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137  0xaa4  0x600  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  [illegible]  [illegible]  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  0xaa4  0xc38  C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246  n/a    n/a    n/a
2T13:27:20:246  n/a    n/a    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  0xc38  0xa90  C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a    n/a    n/a
2T13:27:20:309  0x6b0  0xa30  ping 1.3.1.2 -n 1
2T13:27:20:340  n/a    n/a    n/a
2T1[illegible]  n/a    n/a    n/a
2T13:27:23:8[illegible]  n/a    n/a    n/a
```

LOG-MD
Discover it

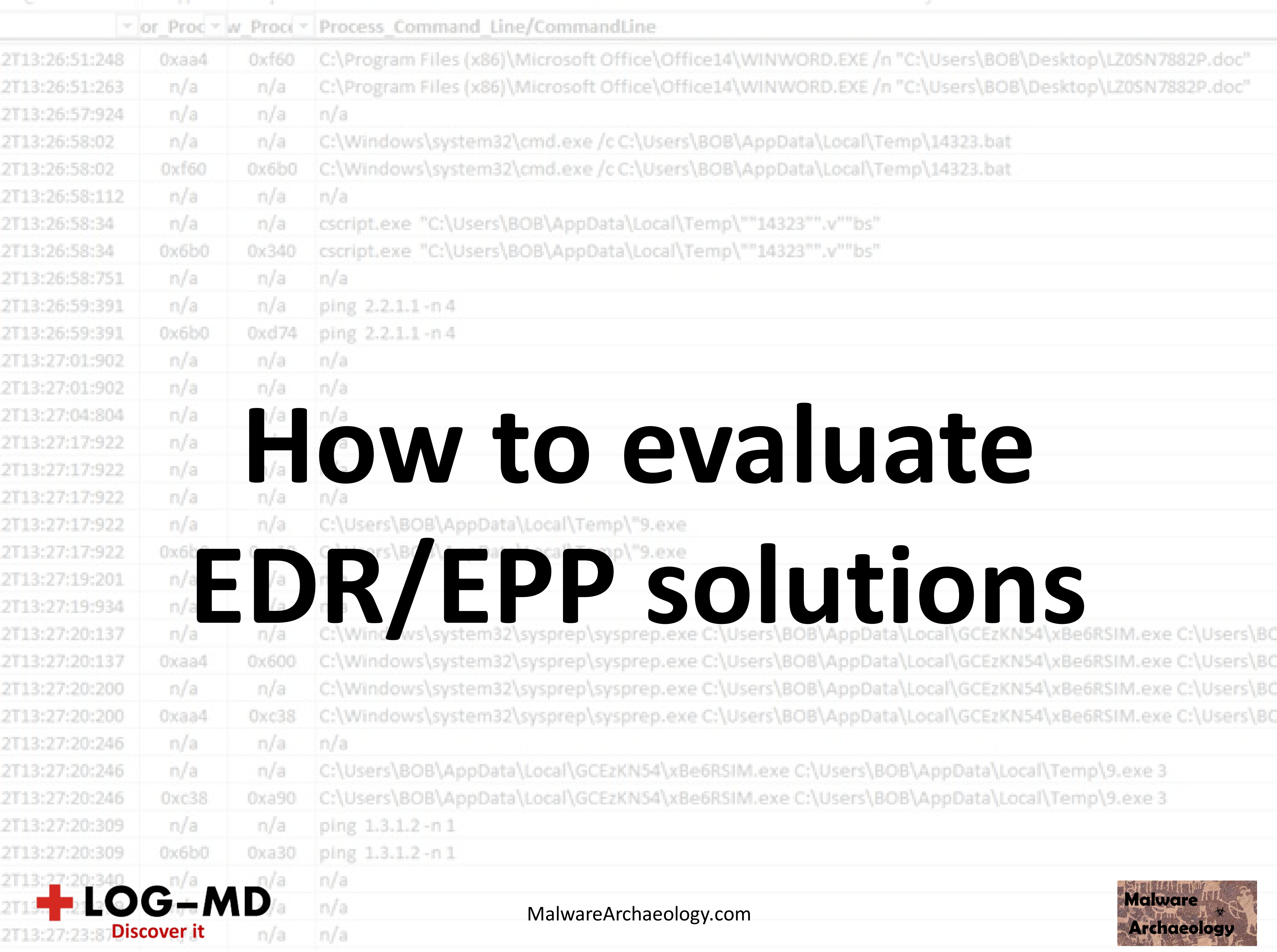
Malware Archaeology

How did they do?

- Kovter was missed by several solutions
  - When caught it was mshta calling PowerShell
- Dridex was missed by several solutions
  - Side loading by a signed MS binary is an issue
  - Morphing rendered hash lookups worthless
- Gozi was missed by a couple solutions
  - This is typical commodity so VERY lame to miss
- Really??? IPS did better than EDR???



How to evaluate EDR/EPP solutions



```
                 or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248   0xaa4     0xf60    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263   n/a       n/a      C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924   n/a       n/a      n/a
2T13:26:58:02    n/a       n/a      C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02    0xf60     0x6b0    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112   n/a       n/a      n/a
2T13:26:58:34    n/a       n/a      cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34    0x6b0     0x340    cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751   n/a       n/a      n/a
2T13:26:59:391   n/a       n/a      ping  2.2.1.1 -n 4
2T13:26:59:391   0x6b0     0xd74    ping  2.2.1.1 -n 4
2T13:27:01:902   n/a       n/a      n/a
2T13:27:01:902   n/a       n/a      n/a
2T13:27:04:804   n/a                n/a
2T13:27:17:922   n/a
2T13:27:17:922   n/a
2T13:27:17:922   n/a       n/a      n/a
2T13:27:17:922   n/a       n/a      C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922   0x6b                                       p\"9.exe
2T13:27:19:201   n/a
2T13:27:19:934   n/a
2T13:27:20:137   n/a       n/a      C:\Win  ws\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137   0xaa4     0x600    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200   n/a       n/a      C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200   0xaa4     0xc38    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246   n/a       n/a      n/a
2T13:27:20:246   n/a       n/a      C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246   0xc38     0xa90    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309   n/a       n/a      ping  1.3.1.2 -n 1
2T13:27:20:309   0x6b0     0xa30    ping  1.3.1.2 -n 1
2T13:27:20:340   n/a       n/a      n/a
2T1                        n/a      n/a
2T13:27:23:8               n/a      n/a
```

LOG-MD
Discover it

MalwareArchaeology.com

Malware Archaeology

```
             or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4    0xf60    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a      n/a      C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a      n/a      n/a
2T13:26:58:02   n/a      n/a      C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60    0x6b0    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a      n/a      n/a
2T13:26:58:34   n/a      n/a      cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   0x6b0    0x340    cscript.exe  "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751  n/a
2T13:26:59:391  n/a
2T13:26:59:391  0x6b0
2T13:27:01:902  n/a
2T13:27:01:902  n/a
2T13:27:04:804  n/a
2T13:27:17:922  n/a
2T13:27:17:922  n/a
2T13:27:17:922  n/a
2T13:27:17:922  n/a
2T13:27:17:922  0x6b0
2T13:27:19:201  n/a
2T13:27:19:934  n/a
2T13:27:20:137  n/a                                                          e6RSIM.exe C:\Users\BC
2T13:27:20:137  0xaa4                                                        e6RSIM.exe C:\Users\BC
2T13:27:20:200  n/a                                                          e6RSIM.exe C:\Users\BC
2T13:27:20:200  0xaa4                                                        e6RSIM.exe C:\Users\BC
2T13:27:20:246  n/a      n/a      n/a
2T13:27:20:246  n/a      n/a      C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246  0xc38    0xa90    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  n/a      n/a      ping  1.3.1.2 -n 1
2T13:27:20:309  0x6b0    0xa30    ping  1.3.1.2 -n 1
2T13:27:20:340  n/a      n/a      n/a
2T1                      n/a      n/a
2T13:27:23:87            n/a      n/a
```

Expectations

- Check your expectations

- Build a set of requirements
- What do you REALLY need???
- Expect that you may not be satisfied

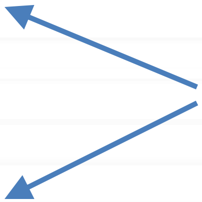
Test your SH*T

- I think their was shock, surprise and bewilderment that our testing found the amount of issues we did
- Do people actually test EDR???

- You REALLY need to test this stuff and decide for yourself what works
- Your requirements are NOT our requirements
- Solutions will change and/or improve over time, or not **Or we HOPE…**

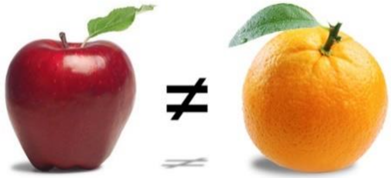
Suggested evaluation

- Determine what you REALLY need
  - EDR – P
  - EDR – D
  - EDR – IR
  - EPP
  - EPP - Eco System



Pick one, skip this one

- Test only the solutions in the area you need
  - Compare Apples to Apples



How to evaluate solutions

- Use malware you actually receive
  - Or ask us or people that can give you good samples
- NEVER use samples from the vendor, they know their stuff can catch it
- Use **LOG-MD** to evaluate your samples to discover the artifacts you will use to evaluate the solutions you select
- Create a short list of things you need or want

How to evaluate solutions

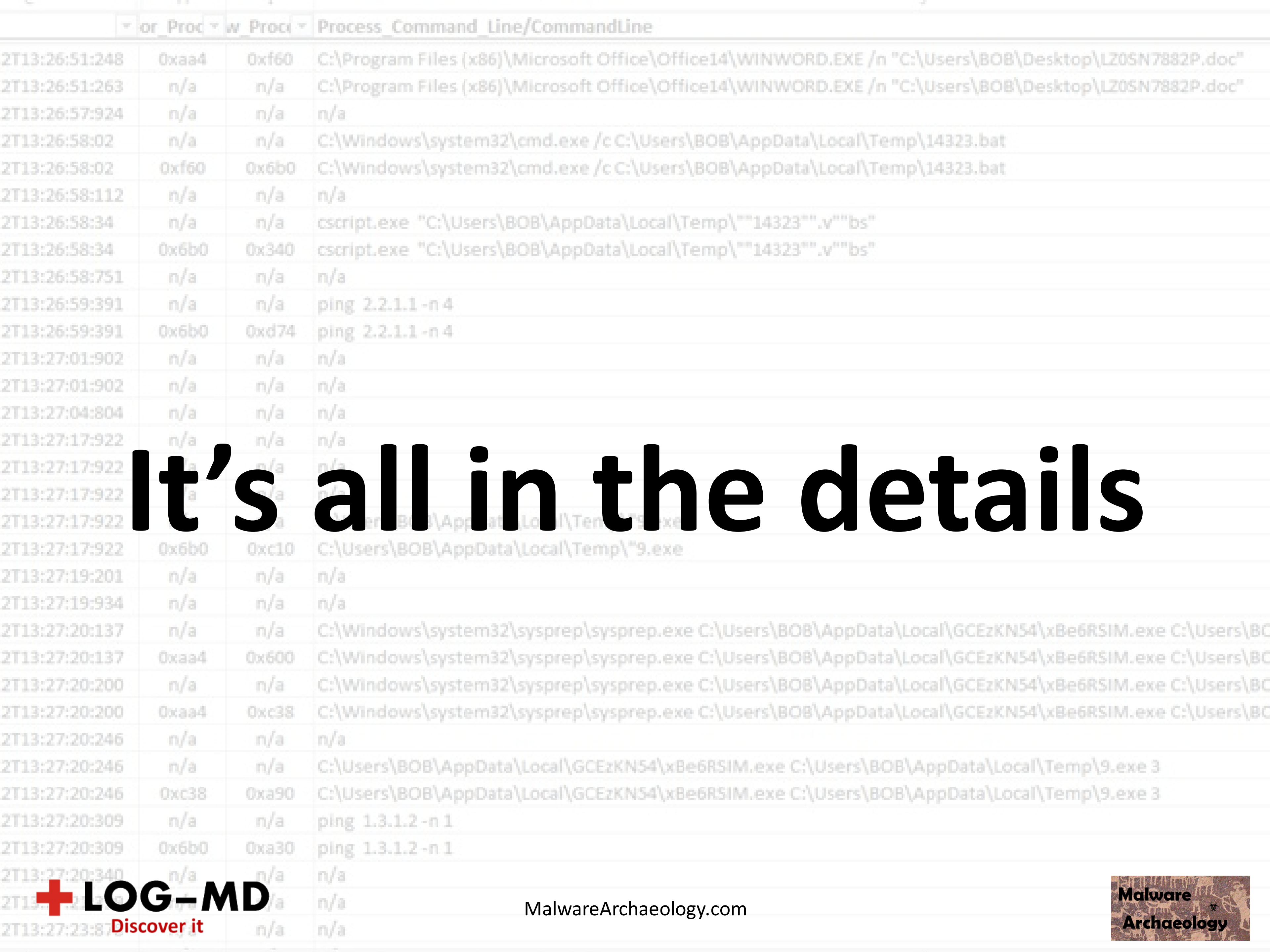
- How easy to use is the console / GUI
  - Many are very difficult or complicated to use
  - Tier 1 probably cannot use them so impacts your staffing
- Do you expect them to provide all the details you need to remediate?
  - They all sucked at this - seriously
  - You will know the system is infected and some details
  - But not everything you need to remediate
  - Which means you will need to investigate systems that trigger alerts to obtain all remediation details

How to evaluate solutions

- Test the damn stuff
  - You will be surprised

- What impact to your resources will it have
- Some are complete time sucks
  - Is this really what you need or want?
- Shouldn't this stuff save us time or at least automate some tasks and gain some efficiency?

It’s all in the details



	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	0x6b0	0xd74	ping 2.2.1.1 -n 4
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	[illegible]	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	0x6b0	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:200	0xaa4	0xc38	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BC
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	n/a	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
[illegible]	[illegible]	n/a	n/a
2T13:27:23:87	[illegible]	n/a	n/a

LOG-MD
Discover it

MalwareArchaeology.com

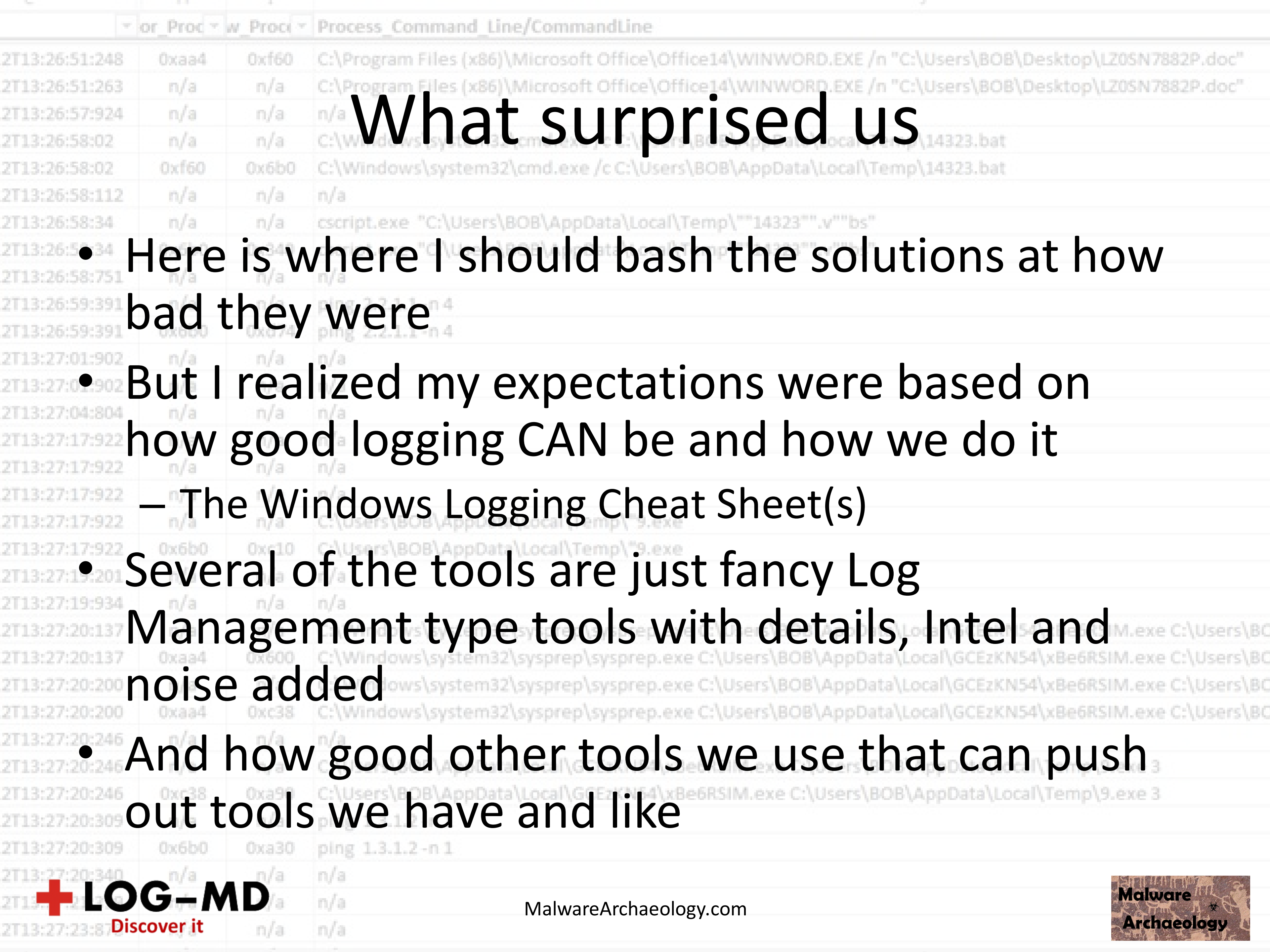
Malware Archaeology

What surprised us

- My expectations were that I would get some details more than AV or IPS gave us
  - This file is bad and this IP is infected
- I expected that we would get some details to help us know what infected the system and how…
- I was soooo disappointed…

What surprised us

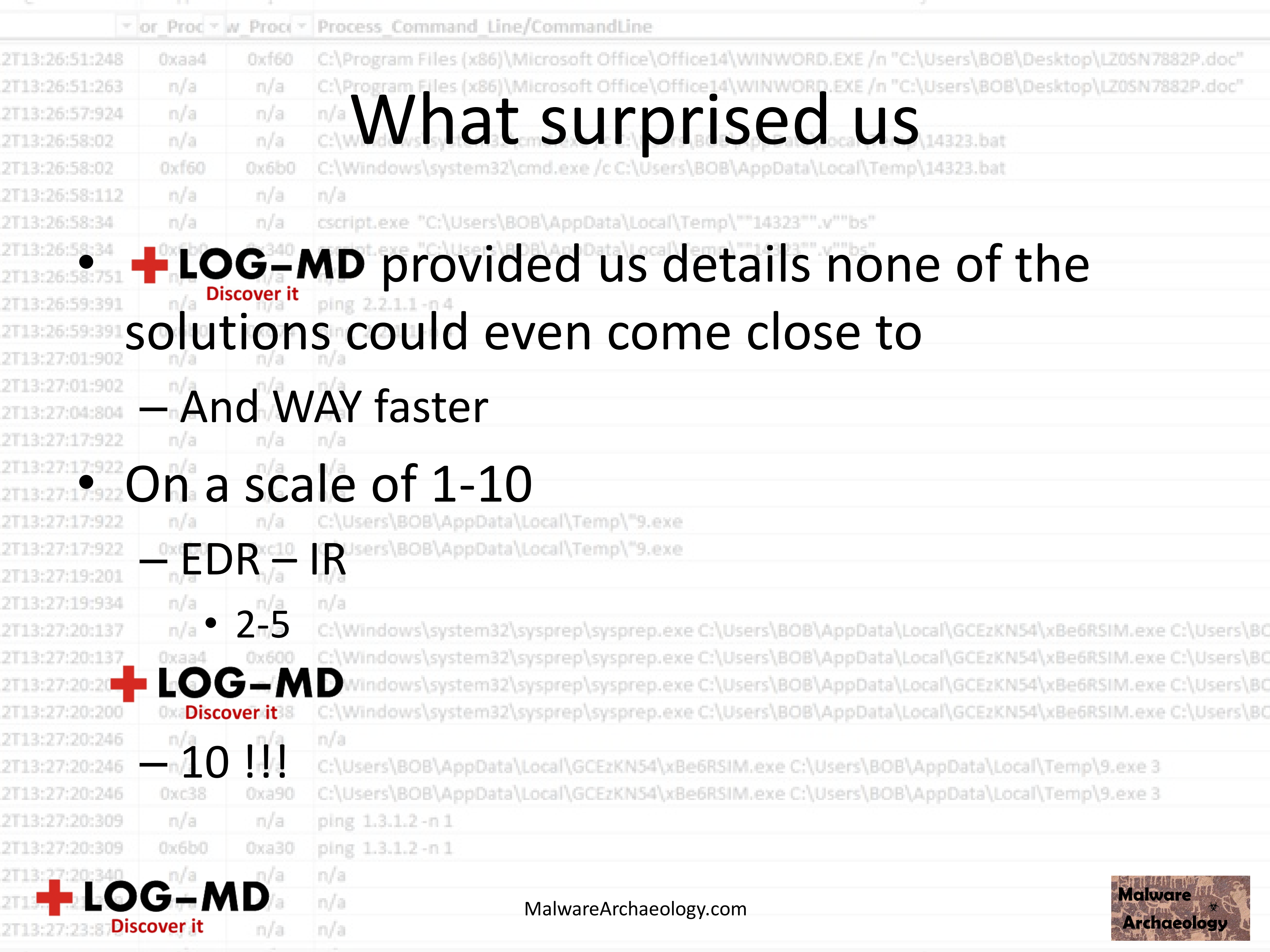
- Here is where I should bash the solutions at how bad they were
- But I realized my expectations were based on how good logging CAN be and how we do it
  - The Windows Logging Cheat Sheet(s)
- Several of the tools are just fancy Log Management type tools with details, Intel and noise added
- And how good other tools we use that can push out tools we have and like



```
               or_Proc   w_Proc   Process_Command_Line/CommandLine
2T13:26:51:248  0xaa4    0xf60    C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263  n/a      n/a      C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924  n/a      n/a      n/a
2T13:26:58:02   n/a      n/a      C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02   0xf60    0x6b0    C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112  n/a      n/a      n/a
2T13:26:58:34   n/a      n/a      cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34   [illegible]
2T13:26:58:751  n/a      n/a      n/a
2T13:26:59:391  n/a      n/a      ping 2.2.1.1 -n 4
2T13:26:59:391  0x6b0    0x674    ping 2.2.1.1 -n 4
2T13:27:01:902  n/a      n/a      n/a
2T13:27:01:902  [illegible]
2T13:27:04:804  n/a      n/a      n/a
2T13:27:17:922  [illegible]
2T13:27:17:922  n/a      n/a      n/a
2T13:27:17:922  n/a      n/a      [illegible]
2T13:27:17:922  n/a      n/a      C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922  0x6b0    0xe10    C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201  [illegible]
2T13:27:19:934  n/a      n/a      n/a
2T13:27:20:137  [illegible]xBe6RSIM.exe C:\Users\BO
2T13:27:20:137  0xaa4    0x600    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  [illegible]ows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200  0xaa4    0xc38    C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246  n/a      n/a      n/a
2T13:27:20:246  [illegible]
2T13:27:20:246  0xc38    0xa98    C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309  [illegible]
2T13:27:20:309  0x6b0    0xa30    ping 1.3.1.2 -n 1
2T13:27:20:340  n/a      n/a      n/a
2T1[illegible]           n/a      n/a
2T13:27:23:8[illegible]  n/a      n/a
```

What surprised us

- LOG-MD provided us details none of the solutions could even come close to
  - And WAY faster
- On a scale of 1-10
  - EDR – IR
    - 2-5
  - LOG-MD
  - 10 !!!



	or_Proc	w_Proc	Process_Command_Line/CommandLine
2T13:26:51:248	0xaa4	0xf60	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:51:263	n/a	n/a	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE /n "C:\Users\BOB\Desktop\LZ0SN7882P.doc"
2T13:26:57:924	n/a	n/a	n/a
2T13:26:58:02	n/a	n/a	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:02	0xf60	0x6b0	C:\Windows\system32\cmd.exe /c C:\Users\BOB\AppData\Local\Temp\14323.bat
2T13:26:58:112	n/a	n/a	n/a
2T13:26:58:34	n/a	n/a	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:34	0x6b0	0x340	cscript.exe "C:\Users\BOB\AppData\Local\Temp\""14323"".v""bs"
2T13:26:58:751	n/a	n/a	n/a
2T13:26:59:391	n/a	n/a	ping 2.2.1.1 -n 4
2T13:26:59:391	[illegible]	[illegible]	[illegible]
2T13:27:01:902	n/a	n/a	n/a
2T13:27:01:902	n/a	n/a	n/a
2T13:27:04:804	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	n/a
2T13:27:17:922	n/a	n/a	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:17:922	[illegible]	0xc10	C:\Users\BOB\AppData\Local\Temp\"9.exe
2T13:27:19:201	n/a	n/a	n/a
2T13:27:19:934	n/a	n/a	n/a
2T13:27:20:137	n/a	n/a	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:137	0xaa4	0x600	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:2	[illegible]	[illegible]	Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:200	[illegible]	[illegible]	C:\Windows\system32\sysprep\sysprep.exe C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BO
2T13:27:20:246	n/a	n/a	n/a
2T13:27:20:246	n/a	[illegible]	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:246	0xc38	0xa90	C:\Users\BOB\AppData\Local\GCEzKN54\xBe6RSIM.exe C:\Users\BOB\AppData\Local\Temp\9.exe 3
2T13:27:20:309	n/a	n/a	ping 1.3.1.2 -n 1
2T13:27:20:309	0x6b0	0xa30	ping 1.3.1.2 -n 1
2T13:27:20:340	n/a	n/a	n/a
2T1[illegible]	[illegible]	n/a	n/a
2T13:27:23:8[illegible]	[illegible]	n/a	n/a

After Testing - My Top 10 Tools

1. Log Management
   1. Of course with the “Windows Logging Cheat Sheet(s)”
2. Query the System
   1. I LOVE BigFix, Tanium, Grrr, OSQuery, Investigator
3. LOG–MD Discover it
4. n/a
5. n/a
6. n/a
7. n/a
8. n/a
9. n/a
10. n/a – Maybe one that implements the changes I am about to recommend

Recommendations to the Industry

- EDR – IR
  - Need a console that allows us to run say……… **LOG-MD** or other tool(s) of your choice
  - Not one by one, but automated on all the suspect systems we want to obtain more details
- Simpler consoles to address Tier 1 staff
  - Can have drill down for more detail
  - But focus at Tier 1 so I can share some of the load
  - Help me distribute the load across the team

Resources

- Websites
  - Log-MD.com The tool
- The "*Windows Logging Cheat Sheet(s)*"
  - MalwareArchaeology.com
- This presentation and others on SlideShare
  - Search for **MalwareArchaeology** or **LOG-MD**

Questions?

You can find us at:

- **Log-MD.com**

- **@HackerHurricane**
- **@Boettcherpwned**

- **MalwareArchaeology.com**
- **HackerHurricane.com (blog)**