SECTOR 2018

MEMORY-BASED ATTACKS ARE ON THE RISE
HOW TO STOP THEM

Josh Fu | CISM, CISSP
Sales Engineer

WHAT IS IT?

AI

- Fileless
- Living-off-the-land
- Systems Memory

WHY NOW?

- Traditional AV
- Next Gen AV
- Still trying to steal your stuff

HOW IT WORKS

Getting the instructions into memory

MEMORY FOCUSED

- GOAL: Instructions in or data out
- STEP 1: Script or file on the endpoint
- STEP 2: Instructions get loaded
- STEP 3: Use system local applications

EXAMPLES

Docs and Browsers

WORD MACROS

- TOOLS: Word macros, PowerShell, Meterpreter, Mimikatz
- STEP 1: User opens a Word doc macros
- STEP 2: PowerShell does a second download
- STEP 3: Meterpreter and Mimikatz find and send credentials

```
.text:00401F2A loc_401F2A:                             ; CODE XREF: sub_401BF5+295↑j
.text:00401F2A                                         ; sub_401BF5+2A2↑j
.text:00401F2A                 push    104h            ; nSize
.text:00401F2F                 lea     eax, [esp+0BD4h+pszPath]
.text:00401F36                 push    eax             ; lpDst
.text:00401F37                 push    offset aWindirSystem32 ; "%windir%\\system32\\windowspowershell\\v1."...
.text:00401F3C                 call    ds:ExpandEnvironmentStringsA
.text:00401F42                 lea     eax, [esp+0BD0h+pszPath]
.text:00401F49                 push    eax             ; pszPath
.text:00401F4A                 call    ds:PathFileExistsA
.text:00401F50                 test    eax, eax
.text:00401F52                 jnz     short loc_401F7F
.text:00401F54                 push    [esp+0BD0h+var_BBC] ; pszPath
.text:00401F58                 call    sub_401B16
.text:00401F5D                 test    eax, eax
.text:00401F5F                 jnz     short loc_401F7F
.text:00401F61                 push    ds:ExitCode
.text:00401F67                 call    ds:GetLastError
.text:00401F6D                 push    eax
.text:00401F6E                 push    ds:ArgList      ; ArgList
.text:00401F74                 push    esi             ; Format
```

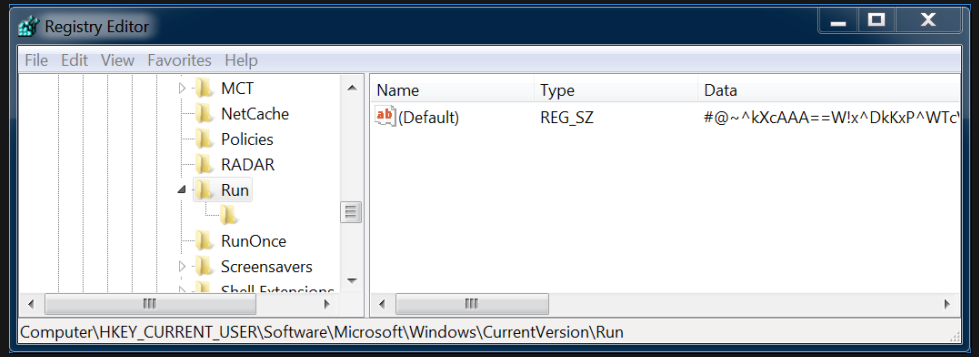
```
.text:00401B8D                 push    eax             ; lpExistingFileName
.text:00401B8E                 call    ds:CopyFileW
.text:00401B94                 test    eax, eax
.text:00401B96                 jz      short loc_401BED
.text:00401B98                 lea     eax, [ebp+NewFileName]
.text:00401B9E                 mov     [ebp+pExecInfo.lpFile], eax
.text:00401BA1                 lea     eax, [ebp+pExecInfo]
.text:00401BA4                 push    eax             ; pExecInfo
.text:00401BA5                 mov     [ebp+pExecInfo.fMask], 40h
.text:00401BAC                 mov     [ebp+pExecInfo.lpParameters], offset aQuietNorestart ; "/quiet /norestart"
.text:00401BB3                 call    ds:ShellExecuteExW
```

FLASH IN BROWSERS

- TOOLS: Your favorite browser, Flash
- STEP 1: Go to website
- STEP 2: Enable Flash
- STEP 3: Shellcode to Command Line in memory

KOVTER.EXE

- TOOLS: JavaScript, mshta.exe, WMI
- STEP 1: Write JS code to registry
- STEP 2: Execute mshta.exe
- STEP 3: Decrypt JS code
- STEP 4: Run new PowerShell script and inject shellcode into memory




```
Key:    HKCU\Software\Microsoft\Windows\CurrentVersion\Run
Value:  Null
Data:   rundll32.exe javascript:"\..\mshtml,RunHTMLApplication"; document.write("\74script
        language=jscript.encode><"+(new%20ActiveXObject("WScript.Shell")).RegRead("HKCU\\
        software\\microsoft\\ windows\\currentversion\\run\\")+"\74></script>)
```

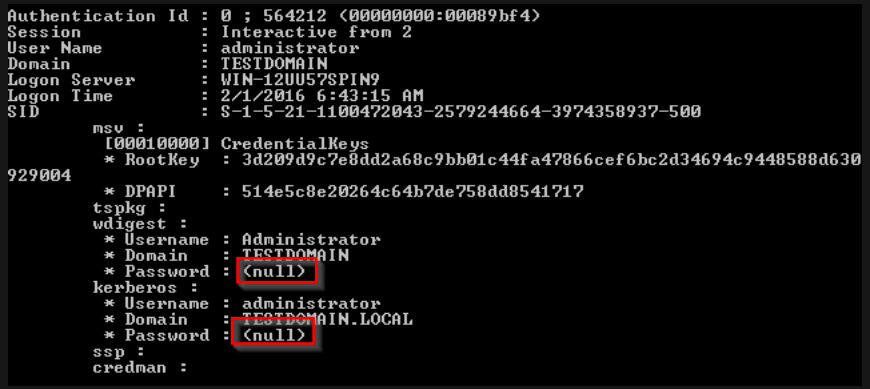
```
a.Environment("Process"))("a")="iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String('ZnVuY3Rp...=='")));
e=a.Run(p+" iex $env:a",0,1);
}
catch(e)
{log("scriptexcept_"+e.message);
close();
}};
close();
```

STOPPING THESE ATTACKS TODAY

How to protect yourselves without an EDR solution

BE VIGILANT

- Patching
- Block certain websites and requests
- Restrict macros usage
- Defend against Mimikatz
- Use SIEM to watch for strange traffic
- Memory forensic tools



STOPPING THESE ATTACKS TOMORROW

How to protect yourselves with scale and automation

ENDPOINT DETECTION AND RESPONSE

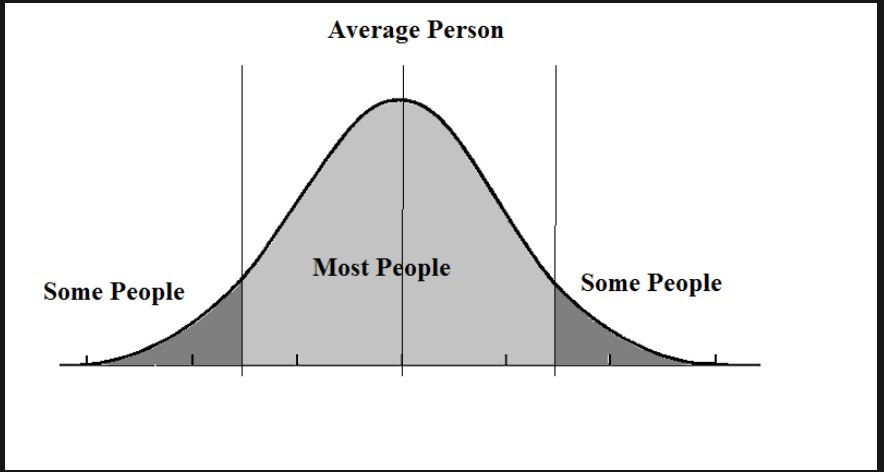
- Automate protections
- People, Process, Technology – What's yours?
- Crowded market
- Consider AI-based EDR

THE ROLE OF AI

How to protect yourselves with scale and automation

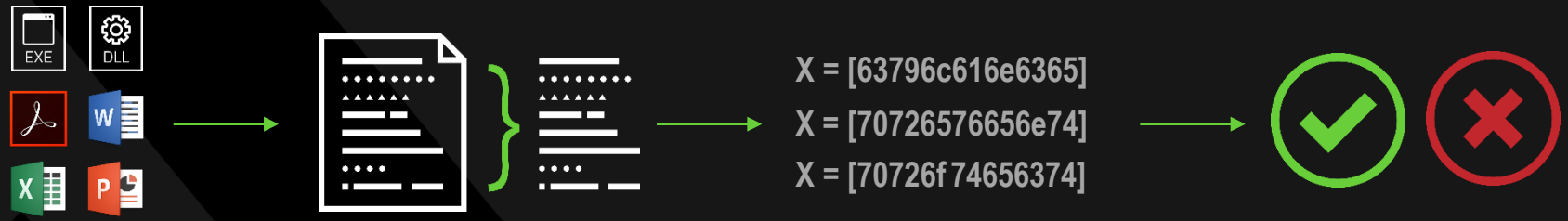
WHY AI IS NECESSARY FOR INFOSEC

- The Information Security Industry is at a -100% unemployment rate. There are 2 job openings for every reasonably qualified candidate.
- We are starving for qualified talent.
- AI allows seasoned veterans to reduce spending time on mundane tasks
- AI allows new entrants to punch above their weight class



HOW DO WE DO IT?

ALGORITHMIC SCIENCE AND MACHINE LEARNING



COLLECT (GOOD AND BAD)

EXTRACT FEATURES

TRAIN MODELS

Algorithm

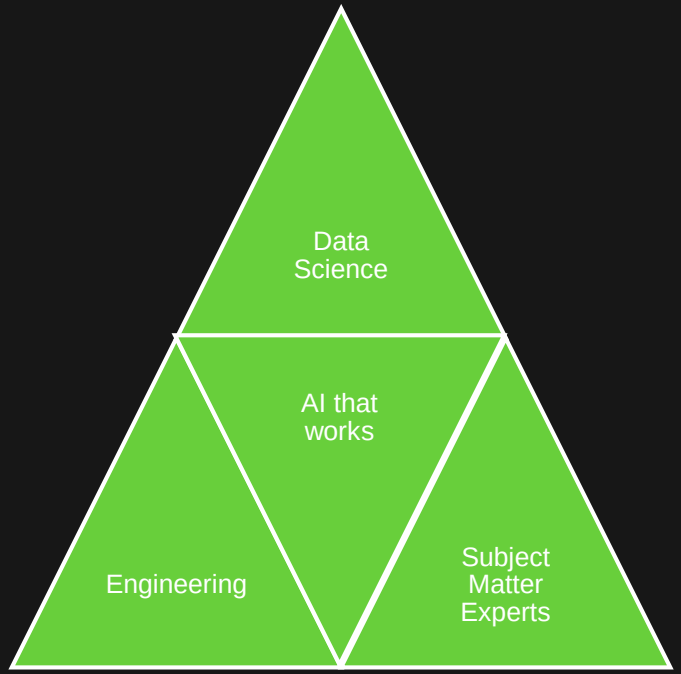
CYLANCE™

GENERATIONS OF AI

Gen	Runtime	Features & datasets	Human interactions	Robustness
1st	Cloud training Cloud prediction	Small (<1000) number of features. Human hand-picked. Small number of samples (<1M). Human labeled.	Easily interpretable (small)	Trivial. Bypass in minutes.
2nd	1st gen + Local prediction	Medium (<100k) number of features. Human hand picked. Medium (<100M) number of samples. Mostly human labels with some heuristic labels.	Large uninterpretable Human association indicators (TTM)	Easy. Bypass in hours.
3rd	2nd gen + Cloud enhanced models	Large (<3M) number of features. Mostly heuristic labels with some human labels. Large (1B+) number of samples. Mostly heuristics with some human labels.	Some interpretability w/ accurate visualization.	Moderate. Bypass in days.
4th	3rd gen + Local training	Active learning, feature suggestions.	Human feedback into model building.	Difficult. Bypass in weeks.
5th	4th gen + unsupervised local training	Semi-supervised feature discovery and data collection.	Human feedback optional; model provides interpretable insights	Extremely Difficult. Bypass in months.

WHY TEAMS CHOOSE CYLANCE

1. Lowers operational and infrastructure costs
2. Optimizes the team's ability to focus on "the important" vs. "the urgent"
3. Extends the system lifetime by multiple years
4. Reduces helpdesk calls and malware-related reimaging
5. 14.5 million endpoints protected and growing
6. Gives the security team their nights, weekends and family time back



TAKEAWAYS

- Manual efforts are possible, but automation is scalable
- AI is incredibly powerful at hard problem solving
- AI cannot simply be an add-on feature
- Prevention is possible
- Cylance provides predictive advantage

REFERENCES AND RECOMMENDED READING

- Cylance AI platform – www.cylance.com
- The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
- Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It
- Verizon Report for 2017 - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
- NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million - https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#4c5703e04f9a
- Mimikatz Overview, Defenses, and Detection - https://www.sans.org/reading-room/whitepapers/detection/paper/36780 AV-TEST Statistics - AV-TEST statistics https://www.av-test.org/en/statistics/malware/
- Best Machine Learning Resources for Starters - https://machinelearningmastery.com/best-machine-learning-resources-for-getting-started/
- Defending Against Mimikatz- https://jimshaver.net/2016/02/14/defending-against-mimikatz/
- A visual introduction to machine learning - http://www.r2d3.us/visual-intro-to-machine-learning-part-1/
- DEMYSTIFYING MACHINE LEARNING - https://www.infoworld.com/article/3068540/data-analytics/machine-learning-demystifying-linear-regression-and-feature-selection.html
- The wonderful and terrifying implications of computers that can learn - https://www.ted.com/talks/jeremy_howard_the_wonderful_and_terrifying_implications_of_computers_that_can_learn?language=en
- Deep Learning on GPU Clusters - https://www.youtube.com/watch?v=brui4N2orlI
- USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers - https://www.youtube.com/watch?v=bDJb8WOJYdA

Thank You | Q&A

fJosh Fu
cylance.com
Twitter: @cylanceinc and
@jfusecurity
jfu@cylance.com