Enterprise Forensics and Response

Introduction to Tools and Techniques

IR PROACTIVE

Gerry Johansen

Principal

IR Proactive

@irproactive

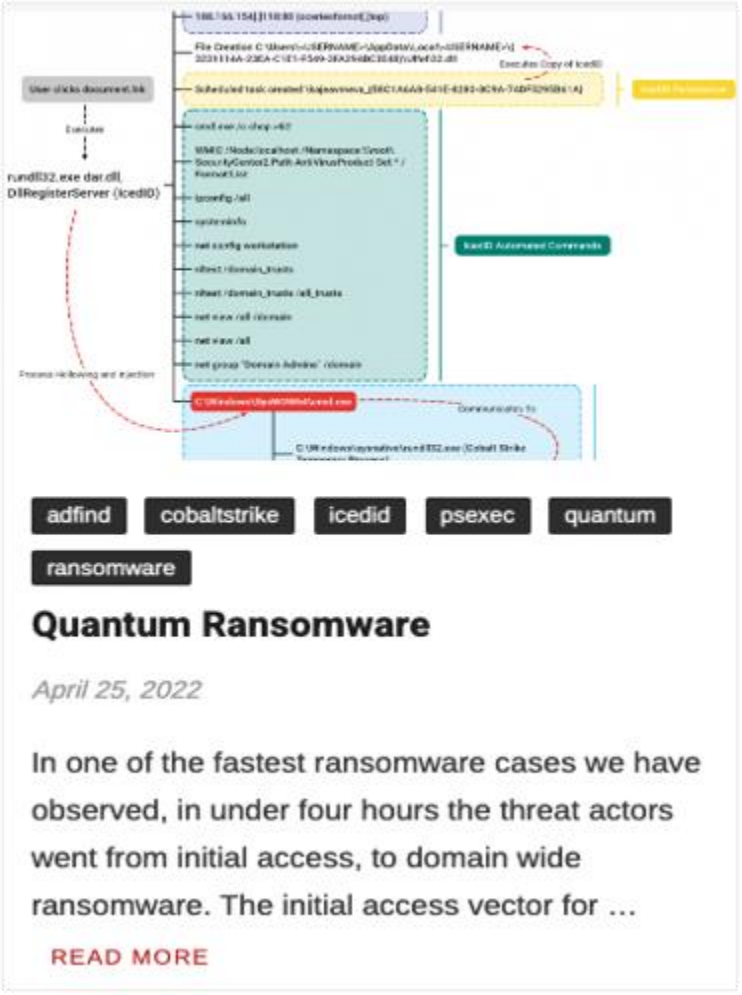
10+ Years of Incident Response, Digital Forensics and Threat Intelligence

BS – Justice and Law Admin, MA– Information Assurance, GCTI, GCFA, GNFA, GRID, CISSP Detective / Task Force Agent (FBI)

Rapid City, South Dakota

What is the problem?

- Time from initial execution to foothold is measured in hours
- Attackers continue to develop their TTPs: Macros to Mark of the Web
- Combination of scripted & hands on keyboard
- Even the best defenses don’t work 100%
- Response teams cannot wait



Where are we?

- We no longer have the luxury to wait
- It takes time to escalate to a full IR engagement
- Retainer SLOs or SLAs can run from 4 hours to ‘best effort’
- In the time it takes to get everyone aligned, what damage could we suffer?

What can we do?

- Incorporate forensic techniques that focus on identifying: Initial Access, Execution, Lateral Movement, Command and Control
- Use forensic techniques to support decision in the IR process
- Examine the IR process into two broad processes:
    - Identify & Contain
    - Investigate & Expel

What are we talking about?

Computer Forensics

Who?

Tracing activity on a system to identify a perpetrator

- Dead box Forensics
- Detailed process
- Time is plentiful

Digital Forensics

What?

What actions did a threat actor take on a system or systems

- Combined Analysis
- Processes
- Time is a premium

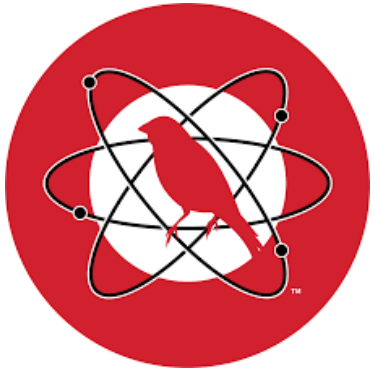
Enterprise Forensics

How?

How is the threat actor operating so we can kick them out

- Combined Analysis
- Plans / Playbooks
- Time is short

The tools



What is triage?

- In the medical context, it is determining what patients are savable based on their injury and the resources at hand: Mass Casualty situation
- Quickly patient assessment followed by a determination if the resources necessary to save their lives cannot be used for other patients
- In the Incident Response context, it is quickly analyzing key artifacts to determine if the system(s) has been compromised

What is triage?

- Most of the evidence is contained on less than 1% of the disk
- Can also be a quick assessment to extract the big three Tactics and Techniques: Initial access, Execution, Command and Control
- Our goal is to stop the attacker's access and pivot to Containment for:
  - Network access – aka North/South
  - Lateral movement – aka East/West
  - Credential use

How to triage?

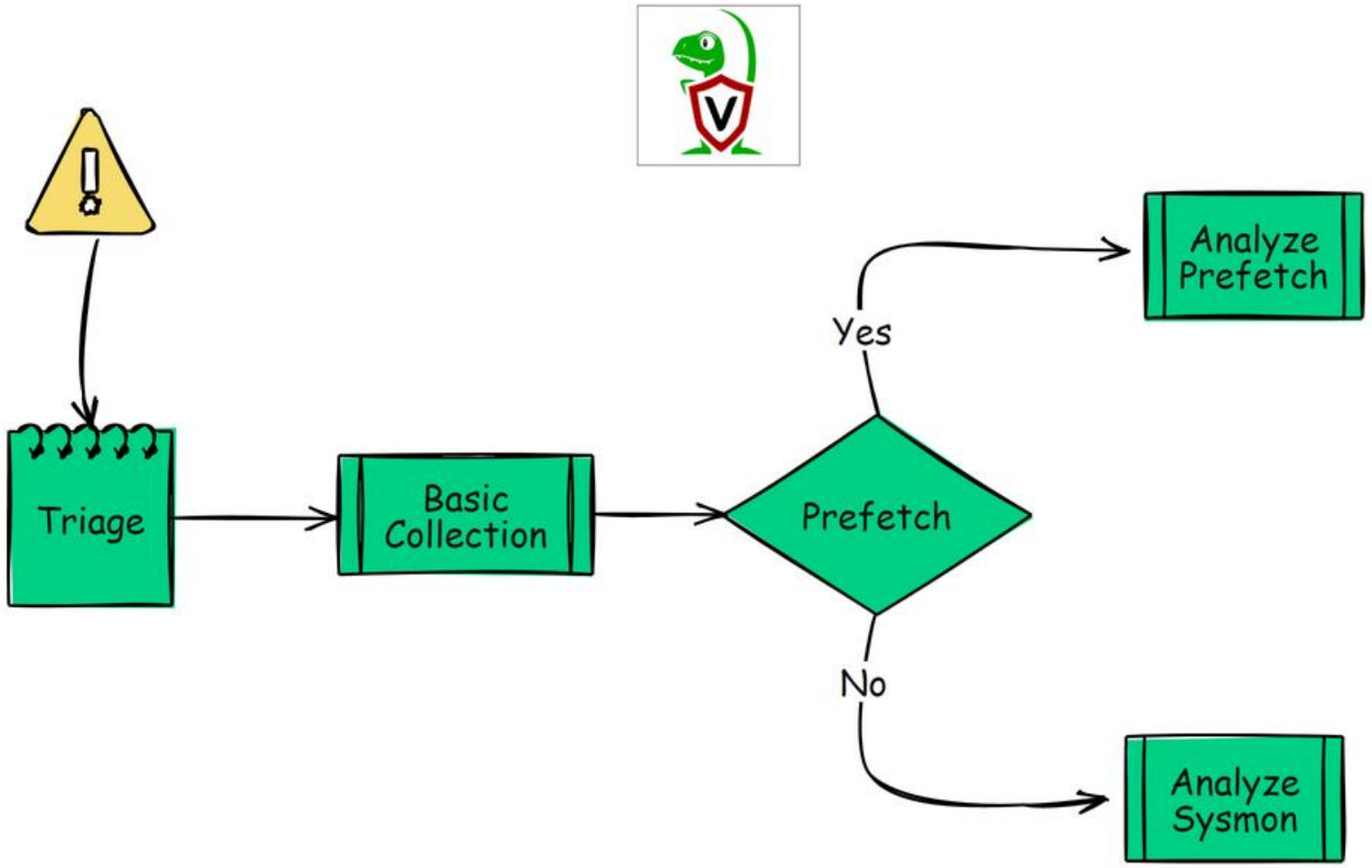
- Scripts
- Executables such as CyLR.exe or KAPE
- Manual extraction
- Locally vs Remotely – One scales, guess which one
    - Locally is good for small orgs, cannot access remotely, malware analysis
    - Remotely scales across a large enterprise but requires the capability to
- Identify key artifacts and analyze
- Alert → Collect → Analyze → Pivot
- The triage output focus on containment

What to Collect and Analyze

- Master File Table – dependent on knowing a rough date and time
- Prefetch Files
- User Journal
- Shimcach / Amcache
- Event Logs
  - Event ID 7045 for Execution
  - Event ID 4104 for PowerShell script Execution & Command and Control
  - Event ID 4624 for Lateral Movement
- Sysmon
  - ID 1 for execution
- Executables identified

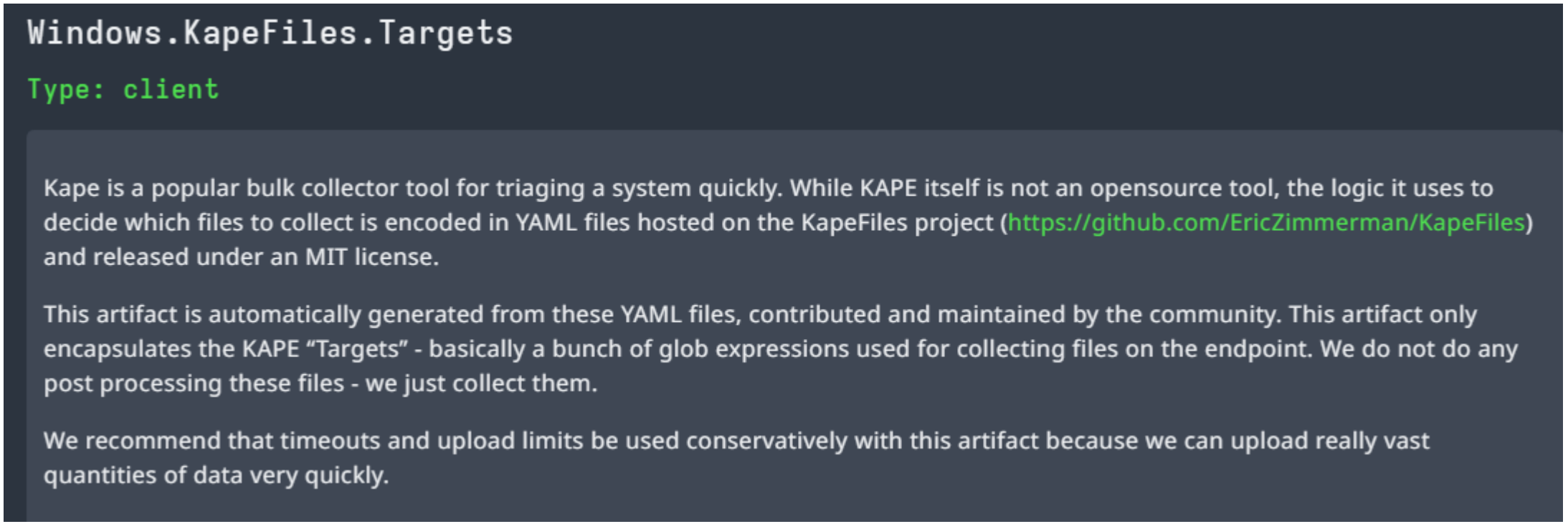
Velociraptor Triage Collection and EZ Tool Analysis

Workflow: Endpoint Triage



KAPE Files

- Windows.KapeFiles.Targets



KAPE Files – Basic Collection

_BasicCollection	Basic Collection (by Phill Moore): $Boot, $J, $J, $LogFile, $MFT, $Max, $Max, $T, $T, Amcache, Amcache, Amcache transaction files, Amcache transaction files, AppCompat PCA Folder, Desktop LNK Files, Desktop LNK Files XP, Event logs Win7+, Event logs Win7+, Event logs XP, GatherLogs, LNK Files from C:rogramData, LNK Files from Microsoft Office Recent, LNK Files from Recent, LNK Files from Recent (XP), Local Service registry hive, Local Service registry hive, Local Service registry transaction files, Local Service registry transaction files, NTUSER.DAT DEFAULT registry hive, NTUSER.DAT DEFAULT registry hive, NTUSER.DAT DEFAULT transaction files, NTUSER.DAT DEFAULT transaction files, NTUSER.DAT registry hive, NTUSER.DAT registry hive XP, NTUSER.DAT registry transaction files, Network Service registry hive, Network Service registry hive, Network Service registry transaction files, Network Service registry transaction files, PowerShell Console Log, Prefetch, Prefetch, RECYCLER - WinXP, RecentFileCache, RecentFileCache, Recycle Bin - Windows Vista+, RegBack registry transaction files, RegBack registry transaction files, Restore point LNK Files XP, SAM registry hive, SAM registry hive, SAM registry hive (RegBack), SAM registry hive (RegBack), SAM registry transaction files, SAM registry transaction files, SECURITY registry hive, SECURITY registry hive, SECURITY registry hive (RegBack), SECURITY registry hive (RegBack), SECURITY registry transaction files, SECURITY registry transaction files, SOFTWARE registry hive, SOFTWARE registry hive, SOFTWARE registry hive, SOFTWARE registry hive, SOFTWARE registry hive (RegBack), SOFTWARE registry hive (RegBack), SOFTWARE registry transaction files, SOFTWARE registry transaction files, SOFTWARE registry transaction files, SOFTWARE registry transaction files, SRUM, SRUM, SYSTEM registry hive, SYSTEM registry hive, SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry hive (RegBack), SYSTEM registry transaction files, SYSTEM registry transaction files, Setupapi.log Win7+, Setupapi.log Win7+, Setupapi.log XP, Start Menu LNK Files, Syscache, Syscache transaction files, System Profile registry hive, System Profile registry hive, System Profile registry transaction files, System Profile registry transaction files, System Restore Points Registry Hives (XP), Thumbcache DB, UsrClass.dat registry hive, UsrClass.dat registry transaction files, WindowsIndexSearch, XML, XML, at .job, at .job, at SchedLgU.txt, at SchedLgU.txt

KAPE Files – SANS Triage

_SANS_Triage	SANS Triage Collection (by Mark Hallman): $Boot, $J, $J, $LogFile, $MFT, $Max, $Max, $T, $T, AVG AV Logs, AVG AV Logs (XP), AVG AV Report Logs (XP), AVG FileInfo DB, AVG Persistent Logs, AVG Report Logs, AVG lsdbj2 JSON, ActivitiesCache.db, Addons, Addons XP, Amcache, Amcache, Amcache transaction files, Amcache transaction files, Ammyy Program Data, AnyDesk Logs - ProgramData - *.conf, AnyDesk Logs - ProgramData - *.trace, AnyDesk Logs - ProgramData - connection_trace.txt, AnyDesk Logs - System User Account, AnyDesk Logs - User Profile - *.conf, AnyDesk Logs - User Profile - *.trace, AnyDesk Logs - User Profile - connection_trace.txt, AnyDesk Videos, AppCompat PCA Folder, Application Event Log Win7+, Application Event Log Win7+, Application Event Log XP, Application Event Log XP, Avast AV Index, Avast AV Logs, Avast AV Logs (XP), Avast AV User Logs, Avast Icarus Logs, Avast Persistent Data Logs, Avira Activity Logs, Avira Security Logs, Avira VPN Logs, Bitdefender Endpoint Security Logs, Bitdefender Internet Security Logs, Bitdefender SQLite DB Files, Bookmarks, Bookmarks, Bookmarks, Box Drive Application Metadata, Box Sync Application Metadata, Chrome Cookies, Chrome Cookies XP, Chrome Current Session, Chrome Current Session XP, Chrome Current Tabs, Chrome Current Tabs XP, Chrome Download Metadata, Chrome Extension Cookies, Chrome Favicons, Chrome Favicons XP, Chrome History, Chrome History XP, Chrome Last Session, Chrome Last Session XP, Chrome Last Tabs, Chrome Last Tabs XP, Chrome Login Data, Chrome Login Data XP, Chrome Media History, Chrome Network Action Predictor, Chrome Network Persistent State, Chrome Preferences, Chrome Preferences XP, Chrome Quota Manager, Chrome Reporting and NEL, Chrome Sessions Folder, Chrome Shortcuts, Chrome Shortcuts XP, Chrome SyncData Database, Chrome Top Sites, Chrome Top Sites XP, Chrome Trust Tokens, Chrome Visited Links, Chrome Visited Links XP, Chrome Web Data, Chrome Web Data XP, Chrome bookmarks, Chrome bookmarks XP, Cisco Jabber Database, ComboFix, Cookies, Cookies, Cookies, Cookies XP, Current

KAPE Files – Kape Triage

KapeTriage	Kape Triage collections that will collect most of the files needed for a DFIR Investigation. This module pulls evidence from File System files, Registry Hives, Event Logs, Scheduled Tasks, Evidence of Execution, SRUM data, SUM data, Web Browser data (IE/Edge, Chrome, Mozilla history), LNK Files, Jump Lists, 3rd party remote access software logs, 3rd party antivirus software logs, Windows 10 Timeline database, and $I Recycle Bin data files. (by Scott Downie): $Boot, $J, $J, $LogFile, $MFT, $Max, $Max, $T, $T, AVG AV Logs, AVG AV Logs (XP), AVG AV Report Logs (XP), AVG FileInfo DB, AVG Persistent Logs, AVG Report Logs, AVG lsdbj2 JSON, ActivitiesCache.db, Addons, Addons XP, Amcache, Amcache, Amcache transaction files, Amcache transaction files, Ammyy Program Data, AnyDesk Logs - ProgramData - *.conf, AnyDesk Logs - ProgramData - *.trace, AnyDesk Logs - ProgramData - connection_trace.txt, AnyDesk Logs - System User Account, AnyDesk Logs - User Profile - *.conf, AnyDesk Logs - User Profile - *.trace, AnyDesk Logs - User Profile - connection_trace.txt, AnyDesk Videos, AppCompat PCA Folder, Application Event Log Win7+, Application Event Log Win7+, Application Event Log XP, Application Event Log XP, Avast AV Index, Avast AV Logs, Avast AV Logs (XP), Avast AV User Logs, Avast Icarus Logs, Avast Persistent Data Logs, Avira Activity Logs, Avira Security Logs, Avira VPN Logs, Bitdefender Endpoint Security Logs, Bitdefender Internet Security Logs, Bitdefender SQLite DB Files, Bookmarks, Bookmarks, Bookmarks, Chrome Cookies, Chrome Cookies XP, Chrome Current Session, Chrome Current Session XP, Chrome Current Tabs, Chrome Current Tabs XP, Chrome Download Metadata, Chrome Extension Cookies, Chrome Favicons, Chrome

Live Demo

Velociraptor and EZ Tools

Thank You

For Your Time & Attention