Building a Threat-Based Cyber Team

Anthony Talamantes | Manager, Defensive Cyber Operations
Todd Kight | Lead Cyber Threat Analyst

Sep 26, 2017 | Washington, DC
Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.
Johns Hopkins University Applied Physics Lab

University Affiliated Research Center
Sponsors include DOD, NASA, DHS, IC
6,000+ staff
$1.5 B revenue
Common Themes

- Change in **Threat Landscape**
- The **Philosophy** of Security Posture vs. Capability Posture
- The value of making multi-faceted change in **Technology, People, and Process**
- Implementing new **Core competencies** including Research, Adaptive Red Team, DevOps, Analytics
Cyber Attack 2009

- APT targeted JHUAPL

- 5 unique pieces of malware on disk
  - Backdoor, Password dumpers, Network exploration utility

- 13 accounts compromised
  - Domain Administrator

- Unclassified data exfiltrated

- Operational impact
  - 2 Weeks disconnected from the Internet
Build Resilient Security Infrastructure

**Technology**
- Legacy SIEM
- Anti-Virus
- IPS/IDS
- Blackhole/Sinkhole
- Sandboxes
- Application Whitelisting

**Philosophy**
- Response
- Signature based
- Alert based
- Mitigation focused
- Tool focused
- IOC focused
- Limited data ingestion

**Security Posture**

**Capability Posture**
Cyber Maturity Evolution

- Philosophy Changing
  - Use Cases
  - Behaviors
  - Visibility focused

- Capability Posture

- Cyber Operations
  - Response
  - Triage
  - Mitigation

- Threat Intel
- Behavioral
- Hunting
Heartbleed

- CVE-2014-0160 (Common Vulnerability & Exposures)
- Publicly disclosed in April 2014
- Vulnerability in the OpenSSL cryptography library
- When it is exploited it leads to the leak of memory contents from the server to the client and from the client to the server
- What is in memory?
  - Encryption keys
  - Usernames
  - Passwords
  - Session Keys
  - Session Cookies
APL Unclassified Network

Internet

APL Public DMZ

VPN

Virtual Machines

APL Internal

QUSER.EXE
The Landscape is Changing

Emergence of New Methodologies
Defense Partner – March IR Collaboration

Never Let a Good Incident Go to Waste

- Extensive use of commercial cloud and SSL
  - Command & Control
  - Exfiltration
  - Distributing malware
  - Constantly changed infrastructure
- PowerShell
  - Reflective injection into memory
  - Lateral movement
  - Reconnaissance
- Persistence
  - Windows Management Instrumentation (WMI)
  - Scheduled tasks
  - Registry (RunOnce)
- Actor’s actions on network – more agile than incident responders

Defenders had limited network visibility

Living off the Land
Change in **Philosophy**

- **Threat Focused Cyber Operations**
  - Research and identify Threats targeting your organization
  - Target advanced tactics, techniques and procedures of adversary
  - Emulate threat in your environment
  - Develop hunting and analytics techniques

- **Changes, Challenges & Culture**
  - What is behavioral monitoring anyways?
  - Mitigation vs Detection
    - Not everything can be mitigated
    - Value in Visibility
  - What is Threat Intelligence?
    - More than indicators of compromise

[Diagram showing Threat Intelligence, Threat Emulation, Behavioral Artifacts, Malware Analysis, AV, Sinkhole, IPS, Firewall]
Defensive Cyber Operations Inception

**Philosophy**
- Use Cases
- Data Analysis
- Behaviors
- Visibility based
- Agility
- Enrichment
- Automation
- Independence
- DevOps

**Technology**
- Splunk
- EDR

**People**
- New skillsets
- New approach

**Process**
- Hunting
- Agility

**Vehicle For Change**
Change in Technology

Legacy SIEM implementation
- A few specialists creating content
- Very static and signature content
- Run scheduled reports for data analysis
- Only acquire logs that you need

Splunk
- All analysts creating content
- Dynamic & behavioral content
- Google like query language for agility
- More visibility means more data
Change in People

Traditional Cyber Skillset
- Firewall Management
- IPS/IDS administrator
- Implementing rule/signature rulesets
- Strong network competencies
- Dead box forensics
- Implement mitigations

Adaptive Skillset
- Data manipulation capabilities
- OS internals
- Malware & memory analysis
- Strong research skills
- Collaborative teams
- Red Team skills
- Constant development of skills
Analysts followed procedures
- Responded to alerts
- Followed playbooks
- Implemented mitigations

Analysts Performing Analysis
- Hunting for anomalies
- Researching threats
- Understanding adversary tradecraft
- Emulating threats
- Developing new analytics, content & alerts
- Understanding context
Putting It All Together
Research
What are the adversary’s doing?

- **Blue sky threats**
  - What if…
  - Based on our environment and Threat Intel
  - LoE, ROI, Likelihood

- **Threat Intelligence**
  - Research threat actors
  - Tradecraft research
  - Emerging capabilities

- **Threat Models**
  - Behaviors
  - **Adversary profiling**

---

5. HAMMERTOSS processes the decrypted commands, which may instruct the malware to conduct reconnaissance, execute commands via **PowerShell**, or upload data to a cloud storage service.

Invoke-WmiMethod -Class Win32_'whoami', $null
Get-WmiObject -Class Win32_Net
powershell.exe -NonInteractive -ExecutionPolicy Bypass -EncodedCommand 2gB1AG4AYwB0AGkAbwBuACAAb1AHIA2gBDAHIAKAAkAGMAAcgBUAHIALAAgACQA2ABhAHQ
Adaptive Red Team

- Proof of concept
  - Predictive
  - Research driven

- Threat Emulation
  - Lateral movement
  - Privilege escalation
  - Persistence methodologies
  - Initial code execution

- External Adaptive RT
  - Comprehensive attack & response lifecycle
DevOps

- Scripting
  - Forensic tool development
  - Data parsing
  - Orchestration
  - Enrichment

- Application Development
  - Threat Tracking System
  - REnigma

- Content Creation
  - Use Case Development
  - Compound Correlation
  - YARA development
Analytics

- Proactive Threat Hunting
  - Process behaviors
  - Network behaviors
  - Account behaviors

- Uniqueness/Rareness/Newness
  - Email
  - FQDN

- Gap analysis
  - Visibility
  - Technology
  - People

- Content review
  - Threat scoring
  - Prioritization
Challenges & Wins
Challenges

- Splunk Core is not a traditional SIEM
  - Uniqueness identifiers
  - Tagging events
- Expensive Live queries
- Sub-Search limitations
- An imperfect start is better than a perfect unimplemented plan
- Leverage existing talent in Cyber Operations
- Managing larger data sets – the cost of visibility
- Solving the same problems differently
Wins

- Leveled analyst playing field
- APT targeting
- DMZ Breach
- Red Team
- No formal Splunk training
Adaptive Red Team Exercise
The Fruits of Our Labor

- Hits on existing custom developed content
- Anomalies associated with credential theft
  - Mimikatz
- RPC & SMB baseline drift
  - Lateral movement
  - AD Reconnaissance
- Privileged account usage
  - Uniqueness
  - Rareness
- Bubble-Up Analytics
  - Aggregation of lower fidelity events of interest
  - Threat models
Summary

Key Takeaways
Summary

Philosophy

People Centric

Data Centric

Research Centric
Questions
Don't forget to rate this session in the .conf2017 mobile app