Consuming Threat Intelligence More Effectively

Bri Rolston
GkChick Threat Research

March 2014

Geek Juju?

- Any experience in security?
  - Security operations
  - Code security
  - Incident response
  - Telecomm
  - Critical infrastructure
- Research area → threat intel

Research Biases

My hat is blue….

- Competitive nature of defense
- Operational threat intelligence
- Where my thoughts tend to wander….
  - Trends in malware use & creation
  - Attack surface
  - Attack vector
  - Attack style

Winning from behind the 8-Ball

Threat paradigm→ most threat talked about in military terms

- National security risk
  - Risk = f (Threat, Vulnerability, Consequence)
- Characterizing--> Taking the intent out of
  - Threat = f(Capabilities, Opportunities, Intent)
  - Capabilities = attack techniques & technologies
  - Opportunities = vulnerabilities & problem solving

Shifting Threat Perspective

Threat from industry perspective

- Operational risk
  - Risk = f (Probability, Impact)
- Priorities
  - People
  - Process
  - Technology

Attack Methodology Analysis (AMA)

Previous work in the threat space….

- Threat analysis technique designed for use on computer networks
- More responsive to dynamic state of target's threat profile
- Concentrates threat analysis efforts on known characteristics of the target
- Need to know potential threat of exploit technology rather than the potential threat of an adversary
- 4 stages of analysis process
  - Characterize system and its vulnerabilities
  - Isolate known attack capabilities
  - Research mitigation techniques for potential threats
  - Analyze gap between existing defensive posture and known exploits

Predictive Attack Path Analysis (PAPA)

They attack. I defend. Shiny object!

- **Miscellaneous studies**
  - LEAN & Six Sigma
  - Root cause failure analysis (RCFA)
  - Code security
- **Cyber defense would be more EFFICIENT if I**
  - Stop defending all targets the same way
  - Identify the high value targets on my network first
  - Evaluate the attack surface
- **Tools used**
  - Reversing off the target (software patent)
  - ATAC (attack styles, FSL, ATAC Life Cycle)
  - Adversarial tiers (not done yet)

ATAC Attack Style

Technology is a tool people use to get work done and to solve business problems.

Adversaries	Attack Work Flow	Attack Technology
• Have operational goals • Are creatures of habit • Solve problems uniquely • Plan attacks based on previous factors	• Makes it possible to characterize threat • Describes the life cycle & work • Drives selection of attack tech	• Shows how adversary solves problems • Can be used to identify most likely attack paths
ATTACK STYLE		

ATAC Life Cycle

Hackers have project managers, too.

Target Development	Exploitation & Pivoting	Attack Operations	Attack EoL
Design	Implementation	Maintenance	EoL
• Work planning • Identify ops goals • Develop attack strategy • Create tool kit	• Point of Entry (PoE) • Foothold • Elevate privilege • Pivot to next system	• Achieve ops goals • Shift in technical focus • Different technical needs than E&P • Lots of infra.	• End of technical work
• Network mapping • Vuln scanning • Spear-phishing	• 0-days • Pass the hash • Elev. of Priv. (EoP)	• C&C channels • Keystroke logging • Remote admin	• Clean up

Functional Security Layers (FSL)

We have the data. We need to make it actionable.

- User Roles & Responsibilities (UR&R)
- Physical comms components
- Network comms
- Firmware or embedded devices
- Operating system (OS)
- Virtualization
- Applications (COTS, 3rd party, GPL, etc.)
- Hosting, managed, or cloud services
- Custom or proprietary software
- Data & data stores

Night Dragon vs. Red October

Would response strategy for one be effective for the other?

- **Night Dragon**
  - Reported by McAfee in Feb 2011
  - 2009 – 2011
  - Ran against oil & gas internationally
  - Operational goal was exfiltration of strategic business data
  - Ended up pulling data from at least one ICS
  - PoE execution is beautiful (Tier 1)
- **Red October**
  - Reported by Kaspersky in Jan 2013
  - 2007 – 2013
  - Ran against govt, education, and diplomatic groups internationally
  - Operational goal was information gathering
  - Not ICS specific but still very cool
  - Rootkit & payloads (Tier 1)

Target Development

What technology was managed by the attacker long term?

- Workstations or laptops
- Mobile devices
  - iPhone
  - Nokia
  - Windows Mobile
- Removable disk drives
- Network devices
  - Cisco

Exploitation

How did they get on the network to begin with?

- PoE exploits
  - Exploits developed & used by other teams
  - Exploit code exactly the same
  - Changed out rootkit & payloads
- Initial PoE – 1st choice
  - Spear-phishing email with malicious attachment
  - Office vulns exploited
  - CVE-2009-3129
  - CVE-2010-3333
  - CVE-2012-0158
- Re-acquisition PoE – back up
  - Spear-phishing email redirecting to malicious PHP web site
  - CVE-2011-3544 (Rhino)

Pivoting

How did they pivot to the next stage targets?

- Harvested credentials for custom “Rainbow Tables”
- Custom payload module for identifying next stage targets
- Use browser, browser history, cached browser creds, & FTP client settings for pivot
- Stole creds from FTP client, browsers, mail clients, MS hash

Attack Operations: C&C

How did they get their work done?

- Multi-tiers to prevent take downs
- Lower tiers were proxies & did port forwarding
- At least 60 domains, multiple geo locations
- Infected hosts call out to C&C servers, which triggers download of payloads
- Comms handled by server-side scripts in "cgi-bin" directories (old school!)
- Different encryption algorithms for sending & receiving
- All rootkits have 3 C&C domains hardcoded in code
- C&C domains (old school crimeware!)
  - Dll-host-update.com
  - Msgenuine.net

Attack Operations: Payload

How did they get their work done?

- Dropper used to load rootkit
  - MSC.BAT
  - LHAFD.GCP
  - SVCHOST.EXE –main component
- Plug and play rootkit framework
- Checks to see if lose access to compromised hosts
- Checks for network access (old school!)
  - update.microsoft.com
  - www.microsoft.com
  - support.microsoft.com

Attack Style

How did the attacker use technology to do work?

- Registry trolling
- QA of malware operations
- Re-acquisition of targets
  - Alternate channels
  - Different PoEs
- Proxies to prevent takedown
- Criminal domains used circa 2003
- USB deleted file recovery
- Custom PnP payload loading

Defending Against Red October

Match defenses and detection to the attack life cycle.

- **Exploitation & Pivoting: PoE**
  - Anywhere PDF & MS Office are used
  - Any machine with JVM
- **Attack Operations: C&C**
  - Outbound web requests with encrypted content
  - DNS requests for known bad I.P.s or domains
- **Attack Operations: Payloads**
  - Registry trolling
  - SNMP polling of network devices
  - Outbound requests to Windows update sites
  - File integrity checks for Office, Adobe, and Java

Questions????

```
If questions = 0
    Then presentation = fail
End If
```

Contact Information

If you need to catch me after you're fully caffeinated…..

Bri Rolston

Chief Research Geek

GkChick Threat Research

gkchick@gmail.com