The Trouble with Attribution

Travis Farral

Director of Security Strategy at Anomali

February 16, 2017

ANOMALI™

Sometimes cited for attribution…

- Non-English keyboard language
- Non-English strings in malware or non-English comments in scripts
- Use of The Onion Router (TOR) to anonymize network traffic
- Use of Virtual Private Servers (VPS) from a “shady” provider
- Use of a Virtual Private Network (VPN) provider that has been used in other attacks associated to particular actor or group
- Use of a foreign free webmail provider
  - Such as: QQ Mail, Yandex, or Mail.ru

Extra credit

- Use of Mimikatz or other widely available tools
- Use of PowerShell during exploitation or lateral movement
  - Such as the Empire framework (www.powershellempire.com)
- Use of URL shortening services such as Bit.ly to obfuscate malicious links
- Use of techniques such as fake landing pages for services like Gmail, Hotmail, or Yahoo mail
- Activities performed during business hours in Moscow or Beijing

What is attribution typically based on?

- A collection of mostly circumstantial evidence
  - Example: Russian keyboard, Russian comments, Russian timezone
- Overlap with tools and infrastructure used in other incidents
  - Particularly for tools only known to be associated to a single actor or group
- Actors aligned with motivations for the attack
- Non-public evidence from other collection sources
  - Forensic evidence
  - Subpoenaed evidence
  - Government sources and methods

Better for attribution

- Specialized tools only associated with a specific group
  - Source code unavailable outside the group
- Computer names
- SSH keys
- Use of very specific, non-publicly known techniques
  - The same **unique** account names, scripts, service names, etc.
- Infrastructure only known to be controlled by a single group
- Use of specific email addresses
  - For communication or DNS registration, etc.

What is *really* known?

- Is it really *attribution* to a specific actor or group?
- Or is it more “this attack bears similarities to this other attack”?
  - Neither of which may actually point to a specific actor
- “Motivations for this attack align with the possible goals of ________”
- True attribution strength may lie in non-public details
  - It’s a matter of faith in the institution delivering the attribution

In the end…

What does attribution do for me anyway?

How valuable is attribution?

- If you aren't using it as the basis for foreign policy decisions…
  - Nations have different reasons for leveraging attribution than companies
- Some considerations for attribution:
  - Know what an adversary is after
  - Useful towards counterintelligence
  - Aids predictive intelligence
- Otherwise…
  - Simply knowing as much as possible about observed attacks aids defense
  - Techniques used, tools used, infrastructure used, targeted users or infrastructure

Thank you!

Travis Farral

- travis@anomali.com
- @mivyx
- Linkedin.com/in/travisfarral
- Github.com/mivyx

- For more on attribution:
  - www.anomali.com/election

ANOMALI™