IDA

Anatomy of a Cyberattack: Standardizing Data Collection for Adversarial and Defensive Analyses

Jason Schlup, Vikram Kulkarni,
Shawn Whetstone, Walter Dodson III

Institute for Defense Analyses
Operational Evaluation Division
DATAWorks 2019

IDA | Bottom Line Up Front

- Cybersecurity is **difficult**
  - Technology changes rapidly
  - Cybersecurity affects everyone
  - Cyber activity generates tremendous amounts of data
- Problem: How can we predict network resiliency and suggest improvements?
- Uniform terminology and easily digestible reporting enable effective cyber defense
  - Find trends in attackers
  - Identify security weaknesses
  - Improve cyber situational awareness

How hard is cybersecurity?

- Attackers need one success, you must defend your **entire** network ***and*** trash!

http://www.commitstrip.com/en/2019/02/04/open-door/

IDA | Cyberattacks in the news

- **Consumers/PII**
  - Yahoo (3 billion)
  - Marriott (500 million)
  - Equifax (143 million)
  - Target (110 million)
  - OPM (26 million)
- **Infrastructure**
  - Baltimore 911 services
  - Ukrainian power grid
  - German steel mill
  - British NHS
  - D.C. police cameras
- **Internet of Things (IoT)/Hardware**
  - Fish tanks
  - Spectre/Meltdown
  - Routers (VPNFilter)
- **Sensitive Data/IP Theft**
  - Oklahoma Dept. of Securities
  - US Navy contractors
  - Sony Pictures

IDA | Why is this hard to counteract?

- **Technology moves quickly**
  - New breaches daily, information/exploits traded
  - Minimal hardware/software requirements
  - Systems not designed with cybersecurity in mind

[1]

- **Defense evasion built into tools**
  - Hackers only need one success, even if it's "trash"

[2]

- **"Big data" problem**
  - Local, remote, cloud-based data
  - Cross-domain (cyber-physical-social)

[1] – Kali Linux. www.kali.org. *Accessed Feb. 2019.*
[2] – Metasploit. www.metasploit.com. *Accessed Feb. 2019*.

IDA | Defending a network and looking forward

- IDA looks at past cyber exercises for trends
  - Collect qualitative data (reports, logs, sensor data, emails, …)
- Requires common taxonomy and methods
  - MITRE ATT&CK™ framework[1]
  - Other choices available
    - NSA, NIST, or Lockheed Martin
- Develop quantitative measures

[1] – MITRE ATT&CK™ (Adversarial Tactics, Techniques, and Common Knowledge)

IDA | Data collection methodology

- IDA primarily focuses on DOT&E operational tests and Cyber Assessment Program (DoD networks)

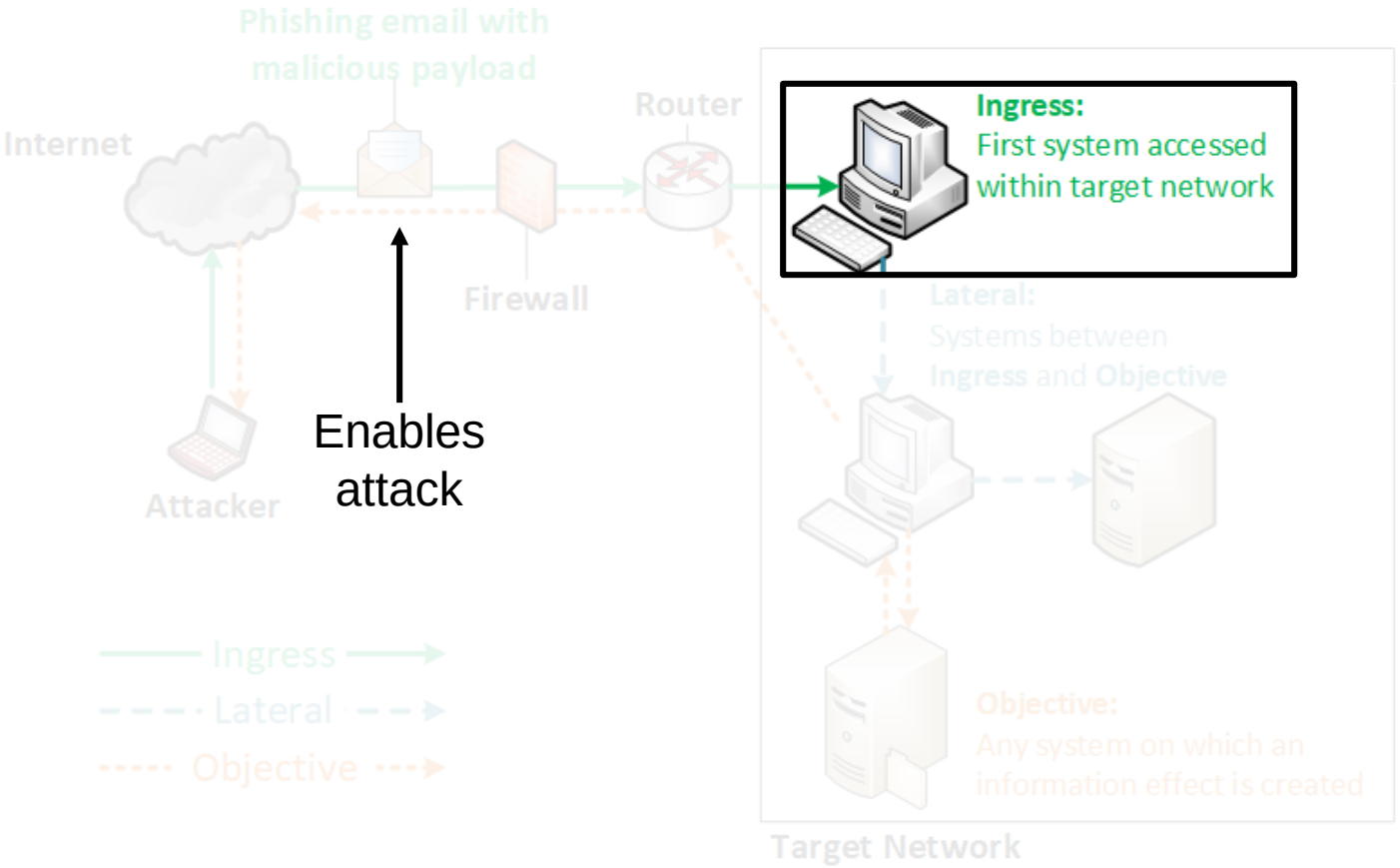
- Penetration testing, Red Teaming
  (Cooperative Assessment) (Adversary Simulation)

- Record attack threads
  - Attacker actions and defensive detections

- Interviews and follow-up

IDA | Example attack thread

- First analysis to achieve cyber picture



NOTE: Notional data is used on this slide.

IDA | Example attack thread – Notional data

- IDA bins actions according to ATT&CK framework
  - Enables analysis of attack threads

We work here

	Target IP	Tactic	Technique	Details	Tool	Tool Type	Detected?
Attack Thread 1	10.10.1.4	Initial Access	Spearphishing Attachment	An email is sent with malicious executable	Email	Native	No
	10.10.1.4	Execution	User Execution	A legitimate user executed the payload	Cobalt Strike	Foreign	No
	10.10.1.4	Execution	Scripting	Batch file is launched from user interaction	Cobalt Strike	Foreign	No
	10.10.1.4	Execution	Rundll32	Batch file launches CS DLL payload via Rundll32	Cobalt Strike	Foreign	No
	10.10.1.4	Persistence	Registry Run Keys / Start Folder	Write new batch file to user's Startup folder	Cobalt Strike	Foreign	Yes
	10.10.1.4	Command and Control	Commonly Used Port	Uses DNS port 53	Cobalt Strike	Foreign	No
	10.10.1.4	Command and Control	Standard Application Layer Protocol	Operating over DNS	Cobalt Strike	Foreign	No

Notional data set

NOTE: Notional data is used on this slide.
Attack from MITRE ATT&CK Evaluation 1.
https://attack.mitre.org/. *Accessed Feb. 2019*

Data analysis – Notional data

- **Look across attack threads**
  - Was the attack detected?
  - What factors determine detection?

Attack Thread	Foreign Tool Use	Thread Detected?
1	88%	Yes
2	0%	Yes
3	23%	No
4	80%	Yes
5	0%	No
6	20%	No
7	13%	Yes
8	50%	Yes
9	20%	No

Notional data set

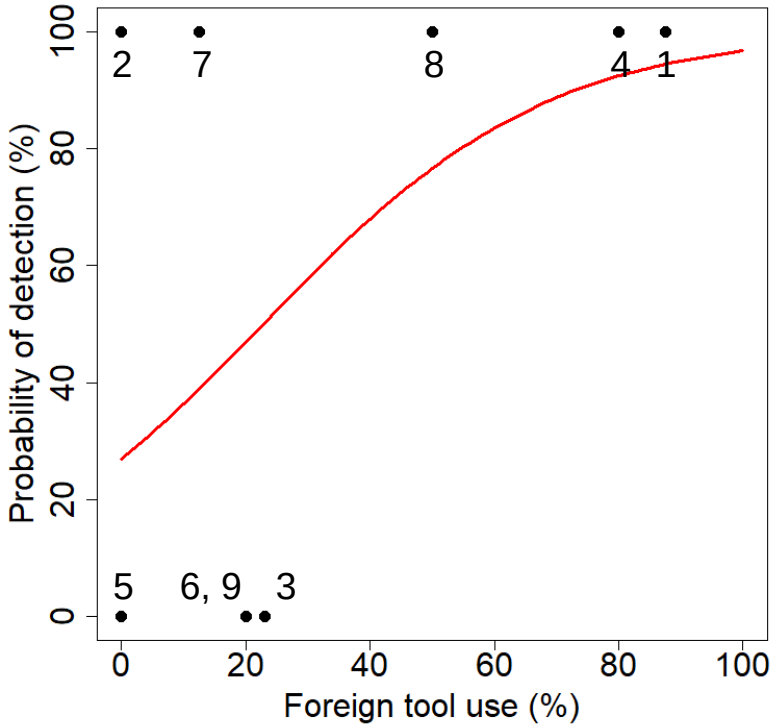
NOTE: Notional data is used on this slide.

IDA | Can use data for future prediction!

Logistic regression of data set

Attack Thread	Foreign Tool Use	Detected?
1	88%	Yes
2	0%	Yes
3	23%	No
4	80%	Yes
5	0%	No
6	20%	No
7	13%	Yes
8	50%	Yes
9	20%	No

Notional data set



Other controlling factors?

NOTE: Notional data is used on this slide.

IDA | Other factors?

- Other quantitative measures:
  - Specific tool use
  - Time-to-objective, time-to-detection

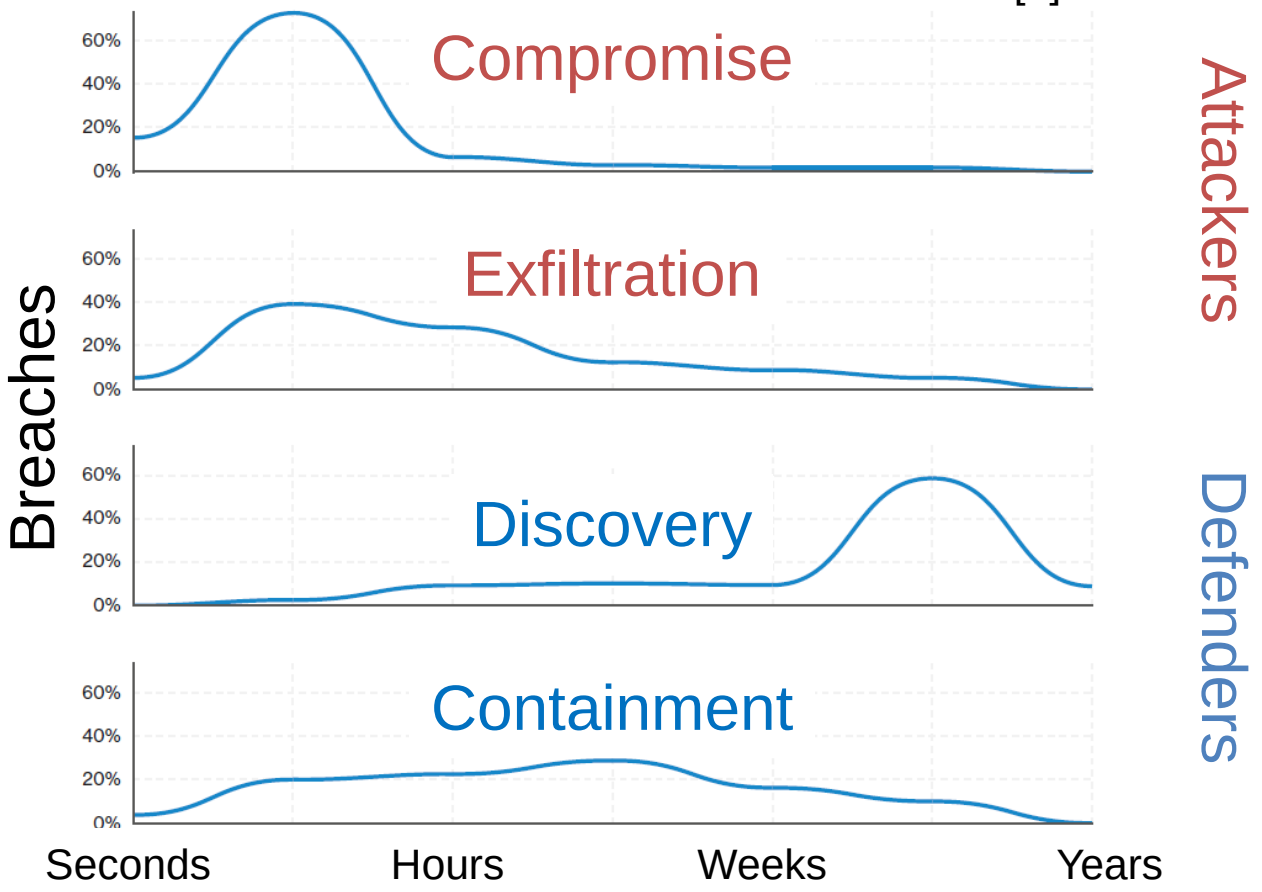
Attack Thread	Foreign Tool Use	PowerShell Use	Time-to-Objective (hr)	Factor 4	Factor 5	Detected?
1	88%	30%	1	…	…	Yes
2	0%	10%	4	…	…	Yes
3	23%	0%	0.2	…	…	No
4	80%	90%	0.2	…	…	Yes
5	0%	20%	0.1	…	…	No

Notional data set

NOTE: Notional data is used on this slide.

- Cybersecurity is asymmetric

[1]



[1] – *Data Breach Investigation Report*, Verizon, 2018.

Conclusions

- Cybersecurity is asymmetric
- If you can't prevent the attack, at least detect it
  - What factors influence detection?
  - How can we increase detections?
- Use common taxonomy to categorize attacker behavior
- Inform defenses based on the findings

BACK-UP SLIDES

IDA | MITRE ATT&CK framework

- 11 tactics, 200+ techniques, and common knowledge
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Exfiltration
  - Command and Control
- Information on 78 known groups

https://attack.mitre.org/. *Accessed Feb. 2019*