97

Mapping and Understanding Cybercrime Operations

Jesse Sowell, Department of International Affairs, Bush School of Government and Public Service

T3: TEXAS A&M TRIADS FOR TRANSFORMATION
A President's Excellence Fund Initiative

Background: Chasing Cybercriminals

Combatting cybercrime is often a game of cat and mouse. Attackers develop strategies to compromise systems for economic or political gain and defenders identify the new tools, techniques, and processes (TPPs) used by these actors and mitigate on-the-fly (Sowell 2018). A challenging contributing factor in this space is the continuing evolution and adaptation of malware as cybercriminals work to identify novel compromise vectors and evade existing network and services defenses. A further contributing factor is the professionalization of malicious tool development, in particular the commodification TTPs in service of crimeware-as-a-service (CaaS, see Sood and Endbody (2013)). Consider the evolution of Mirai as an illustrative instance, responsible for one of the largest distributed denial of service (DDoS) attacks on record:

- August 2016: Mirai surfaces as known malware in August 2016 (Antonakakis *et al*, 2017)
- September 2016: Mirai attacks OVH, one of the largest DDoS on record (Krebs, 2017)
- October 2016: Mirai attacks Dyn, taking down services such as the New York Times, Twitter, and Spotify (Krebs, 2016a, 2016b)
- October 2016: Mirai source code is released and Mirai is commodified, with new variants introduced (Krebs, 2017)
- After the first 7 months of Mirai in the wild, 33 cybercrime operational networks emerged launching more than 15,000 DDoS attacks (some against one another) (Antonakakis *et al* 2017)

Conventional technical analyses have shown that Mirai is rather simple in terms of software and relies on well-known vulnerabilities. With limited exceptions (such as (McCoy et al, 2012)), most technical work focuses on fingerprinting malware binaries and characterizing malicious traffic patterns.

This work complements the valuable technical work by exploring the structure of cybercrime networks from the perspective of communities of operational cybersecurity experts at threat intelligence firms and network providers. These actors are on the frontlines of emerging types of malware and regularly investigate the structure of cybercrime operational networks. These actors have a deep understanding of cybercrime operational networks, but most of this is tacit knowledge, developed through experience dealing with these networks but not necessarily formally documented.

The objective of this work is to investigate how these actors share knowledge of cybercrime operational networks, their incentives, and the challenges of formalizing this process in service of collaborations with domestic and international law enforcement and other organizations and institutions involved in combatting cybercrime. This work integrates technical understandings of how malware functions and the institutional economics of transnational operational epistemic communities that maintain this body of knowledge. Building on Sowell's previous work on cybersecurity operations and planned adaptation (2018), this work aims to prescribe possible avenues of enhanced collaboration that will make better use of operational capabilities in mitigating and remediating transnational cybercrime.

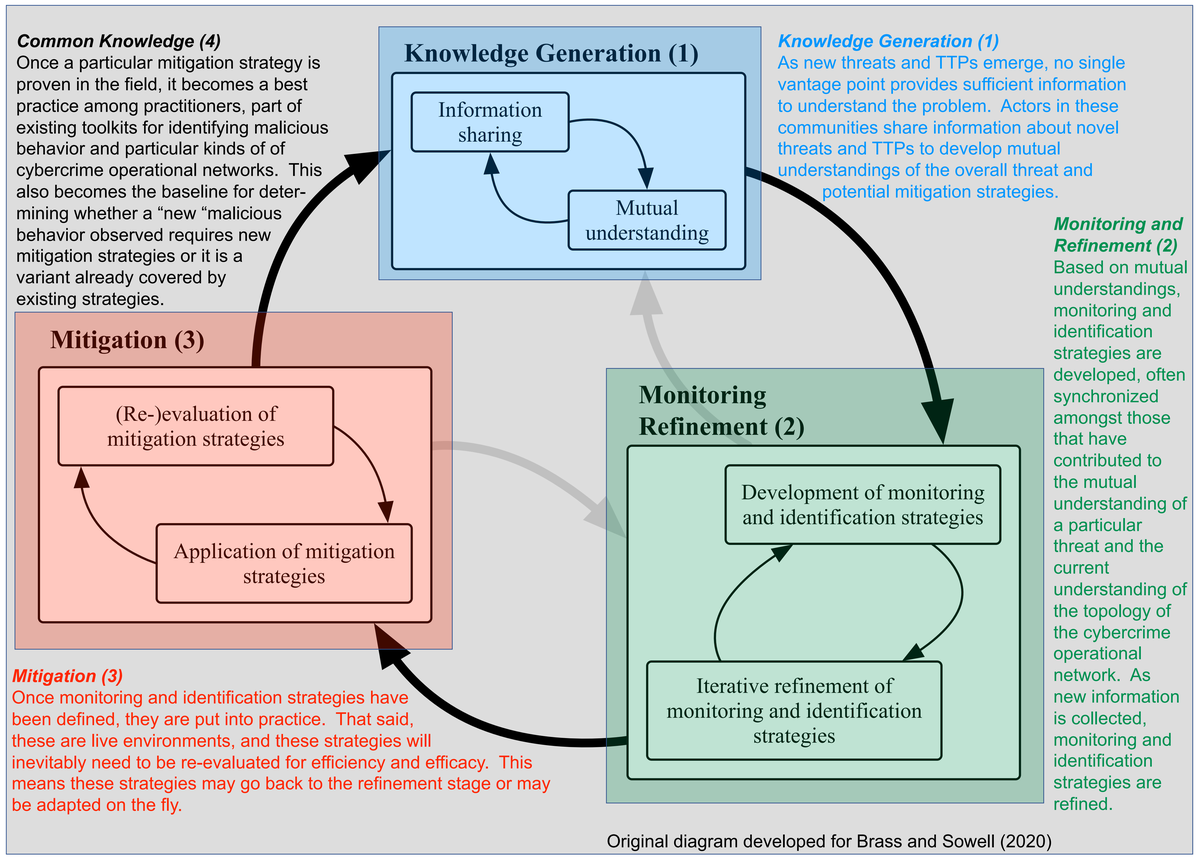
Research Design: Eliciting Tacit Knowledge

The art and craft of tracking cybercriminals is a kind of tacit knowledge: it is not something the analyst learns in a textbook, but rather what is learned in the field, and from other experienced analysts. To elicit this tacit knowledge, Dr. Sowell will be conducting interviews with cybersecurity practitioners and law enforcement to understand

- the process of sharing data and translating that into knowledge that can be applied to mitigation and remediation (figure below)
- the kinds of cybercrime operational networks observed on the ground, in particular how they have evolved and the challenges of keeping pace
- the gaps in the current state-of-the-art and how these are being remedied
- what organizational and institutional mechanism might fill these gaps

This work builds on a survey of technical tools, but the primary data comes from the actors on the ground. Dr. Sowell will be conducing:

- semi-structured interview among well-known practitioners and those new to the field
- workshops with practitioners on the ground to characterize the gaps, especially those related to collaboration and prosecution (remediation)



Original diagram developed for Brass and Sowell (2020)

Project Plan and Ongoing Work

The majority of the empirical work for this project is fieldwork: interviews and workshops with operational cybersecurity communities

Initially the project plan was as follows:
- background literature
- identify collaborators in cybersecurity operations community in first year of project
- interviews and workshops with cybersecurity operations community in year 2, in particular Summer 2020
- report and publications development in Fall 2020

Background literature on malware tools and CaaS
- malware tools bibliography (done, needs cleanup)
- CaaS (preliminary done, needs update)

Due to the COVID-19 pandemic, interviews and workshops planned for Summer 2020 were postponed. Sowell is currently working with partners in the operational cybersecurity community to schedule interviews and workshops for late Fall 2020 and Spring 2021, ideally holding in person workshops depending on conditions.

References

Antonakakis, Manos, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, et al. 2017. "Understanding the Mirai Botnet." In *Proceedings of the 26th USENIX Security Symposium*, 1093–1110. Vancouver, BC, Canada: USENIX Association. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

Brass, Irina, and Jesse H. Sowell. 2020. "Adaptive Governance for the Internet of Things: Coping with Emerging Security Risks." *Regulation & Governance* Special Issue on the Governance of Emerging Disruptive Technologies (early access). https://doi.org/10.1111/rego.12343.

Krebs, Brian. 2016a. "DDoS on Dyn Impacts Twitter, Spotify, Reddit." *Krebs on Security* (blog). October 21, 2016. https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/.

———. 2016b. "Hacked Cameras, DVRs Powered Today's Massive Internet Outage." *Krebs on Security* (blog). October 21, 2016. https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

———. 2017. "Reaper: Calm Before the IoT Security Storm?" October 23, 2017. https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/.

McCoy, Damon, Andreas Pitsillidis, Jordan Grant, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey Voelker, Stefan Savage, and Kirill Levchenko. 2012. "PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs." In , 1–16. Bellevue, WA: USENIX. https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/mccoy.

Sood, Aditya K., and Richard J. Enbody. 2013. "Crimeware-as-a-Service—A Survey of Commoditized Crimeware in the Underground Market." *International Journal of Critical Infrastructure Protection* 6 (1): 28–38. https://doi.org/10.1016/j.ijcip.2013.01.002.

Sowell, Jesse H. 2018. "Combining Capabilities in Cybersecurity Incident Response." Stanford, CA: Center for International Security and Cooperation, Freeman Spogli Institute for International Studies, Stanford University.