Analyzing crimeware and underground economies (pointers and rough notes)

Objective: awareness/understanding of attacker goals/models related to crimeware.

Approach: explore a selection of introductory papers on Internet underground economies + malware services.

1. **Underground/illicit markets for Internet goods and services**

   Motoyama [11], IMC 2011: analysis of 6 (beyond-IRC) **underground Internet markets**
   – from DB records of persistent web forums/social nets (e.g., vetted-members only) leaked by outside parties

   Franklin [2], CCS 2007: nature and causes of the wealth of Internet miscreants
   – earlier analysis of open, **IRC-based underground markets**, based on 7-month study
   – *miscreant*: "a person whose behaviour is bad or breaks the law"

2. **Spam-based services/ecosystems**

   Kanich [5], CCS 2008/C.ACM 2009: empirical analysis of **spam marketing chains** + conversion rates
   – infiltrates Storm botnet, analyze campaigns to: propagate Trojan malware, and online-sell pharmaceuticals

   Grier [3], CCS 2010: a separate study on **spam in Twitter**

   Levchenko [9], Oakland 2011: deeper analysis of **spam monetization chain** and its weak links
   – apparent *payment bottleneck/chokepoint*: a small number of banks are relied on for monetization

   Kanich [6], Usenix Security 2011: analysis to better **characterize spam-advertised revenue**

   McCoy [10], Usenix Security 2012: empirical analysis of 3 online **pharmaceutical affiliate programs**

3. **Pay-per-install (PPI) model/networks**

   Caballero, Usenix Security 2011 [1]: outsourcing and **commoditization of malware distribution** via PPI
   – overview of the PPI model/ecosystem + infiltration of 4 PPI services

   Kotzias [7], CCS 2015: **falsely-certified PUPs**, through abuse of Windows Authenticode code-signing tools

   Kotzias [8] + Thomas [12], both at Usenix Security 2016
   – **explore unwanted software/PUPs**, their prevalence + role of commercial PPI networks in distributing them

   Grier [4], CCS 2012: explores driveby download to install malware, providing an **exploit-as-a-service model**
   – infection by browser/plugin compromise can be considered separately from driving traffic to a site
   – analyzes dataset of malicious URLs + malware binaries they deliver + identifies monetization approaches
   – driveby downloads aided by exploit kits (sets of browser exploits), which enable a **driveby-PPI service**

References

[1] Juan Caballero, Chris Grier, Christian Kreibich, Vern Paxson. Measuring pay-per-install: The commoditization of malware distribution. USENIX Security, 2011. https://www.usenix.org/legacy/events/sec11/tech/full_papers/Caballero.pdf

[2] Jason Franklin, Adrian Perrig, Vern Paxson, Stefan Savage. An inquiry into the nature and causes of the wealth of internet miscreants. CCS 2007, pp.375-388. https://courses.cs.duke.edu/fall15/compsci590.2/papers/ccs07_franklin_eCrime.pdf

[3] Chris Grier, Kurt Thomas, Vern Paxson, Chao Michael Zhang. @spam: The underground on 140 characters or less. CCS 2010, pp.27-37.

[4] Chris Grier, Lucas Ballard, Juan Caballero, Neha Chachra, Christian J. Dietrich, Kirill Levchenko, Panayiotis Mavrommatis, Damon McCoy, Antonio Nappa, Andreas Pitsillidis, Niels Provos, M. Zubair Rafique, Moheeb Abu Rajab, Christian Rossow, Kurt Thomas, Vern Paxson, Stefan Savage, Geoffrey M. Voelker. Manufacturing compromise: the emergence of exploit-as-a-service. CCS 2012, pp.821-832.

[5] Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, Stefan Savage. Spamalytics: An empirical analysis of spam marketing conversion. *Commun. ACM* 52(9): 99-107, 2009. Earlier version in: CCS 2008, pp.3-14, http://users.umiacs.umd.edu/~tdumitra/courses/ENEE757/Fall14/papers/Kanich08.pdf

[6] Chris Kanich, Nicholas Weaver, Damon McCoy, Tristan Halvorson, Christian Kreibich, Kirill Levchenko, Vern Paxson, Geoffrey M. Voelker, Stefan Savage. Show me the money: Characterizing spam-advertised revenue. USENIX Security, 2011.

[7] Platon Kotzias, Srdjan Matic, Richard Rivera, Juan Caballero. Certified PUP: Abuse in Authenticode code signing. CCS 2015, pp.465-478.

[8] Platon Kotzias, Leyla Bilge, Juan Caballero. Measuring PUP prevalence and PUP distribution through pay-per-install services. USENIX Security, 2016, pp.739-756.

[9] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, Stefan Savage: Click trajectories: End-to-end analysis of the spam value chain. IEEE Symp. Security and Privacy 2011, pp.431-446. http://www.icir.org/christian/publications/2011-oakland-trajectory.pdf

[10] Damon McCoy, Andreas Pitsillidis, Grant Jordan, Nicholas Weaver, Christian Kreibich, Brian Krebs, Geoffrey M. Voelker, Stefan Savage, Kirill Levchenko. PharmaLeaks: Understanding the business of online pharmaceutical affiliate programs. USENIX Security, 2012, pp.1-16.

[11] Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, Geoffrey M. Voelker. An analysis of underground forums. IMC 2011, pp.71-80. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ffe8e68bca8505b168e15de3161d70db87dcfa37

[12] Kurt Thomas, Juan A. Elices Crespo, Ryan Rasti, Jean Michel Picod, Cait Phillips, Marc-Andr Decoste, Chris Sharp, Fabio Tirelo, Ali Tofigh, Marc-Antoine Courteau, Lucas Ballard, Robert Shield, Nav Jagpal, Moheeb Abu Rajab, Panayiotis Mavrommatis, Niels Provos, Elie Bursztein, Damon McCoy: Investigating commercial pay-per-install and the distribution of unwanted software. USENIX Security, 2016, pp.721-739.