Botnets: detection & mitigation

I. Pustogarov

Cloud-hosted botnets

- Black Hat USA 2014 – "CloudBots: Harvesting Crypto Coins like a Botnet Farmer"
  - https://www.slideshare.net/rob.ragan/cloudbots-harvesting-crypto-currency-like-a-botnet-farmer
  - https://www.wired.co.uk/article/mining-botnet-in-amazon-cloud
- Build a botnet from freely available cloud services
  - What are the advantages/disadvantages?
    - Free, more resourceful, reputable IP blocks
    - Difficult to automate account creation?
  - Do we have enough services to exploit?
    - Amazon EC2, Google App Engine, CloudFoundry
- Can you use such a botnet?
  - Yes: network scanning, password cracking, DDoS, Crypto mining
- How about using "less-resourceful" smart devices?

Botnets from other resources

- How about using "less-resourceful" smart devices?
  - Smart-TVs, fridges, thermostats?
- How about compromised servers as bots?
- How to increase infection rate: search poisoning attack

TrickBot

Features and take-down efforts

Overview

- Developed in 2016, TrickBot targets Windows machines, offers "malware-as-a-service"
- Used to deliver the RYUK ransomware against state departments and hospitals in the United States; targeted many banks in the past; voting system ransomware
- Infected over 2 million computing devices around the world

Overview

- Capabilities include harvesting emails and credentials, banking trojans, and Bitcoin wallets (using the Mimikatz tool)
- Custom modules accompanied by a configuration file, and each module has a specific task; e.g., persistence, propagation, stealing credentials, ransom, mail searcher, SMB worm, password grabber, banking trojans, remote view and control (VNC)
- C&Cs are set up on hacked wireless routers

Spreading vectors

1. Email attachments, simple spam or spear-phishing (an Excel/Word file containing a malicious macro)

2. Also used: Emotet (another botnet) backdoor infection

3. Lateral infection: SMB attack (EternalBlue: https://en.wikipedia.org/wiki/EternalBlue)

Defense, persistence

- Disable Windows Threat Defender, McAfee AV
- Bot process is added to Start-up, Auto-start services
- Use encrypted loader and config files; a custom packer to obfuscate its functionality; signed loaders with stolen valid certificates

C&C, data collection

- C&C servers: used many regular routers/IoTs and PCs
- C&C backup communication: TOR hidden services, and EmerDNS (a blockchain based DNS service, see: https://emercoin.com/en/documentation/blockchain-services/emerdns/emerdns-introduction)

- Credentials from: Browsers ("man-in-the-browser" attacks), remote desktop clients, Active Directory, passwords stored by Outlook, Filezilla, and WinSCP, PuTTY; also collects email addresses

Disruption attempts

- U.S. military Cyber Command

- Sept 22, 2020: pushed out a new configuration file to Trickbot infected computers -- new malware control server's address is changed to 127.0.0.1

- Oct 1, 2020: stuffed millions of bogus records into the Trickbot control networks

Disruption attempts

- Microsoft (Oct 2020)
- Court order is used to take down the botnet C&C servers -- copyright claims
- Microsoft argued that Trickbot irreparably harms the company "by damaging its reputation, brands, and customer goodwill. Defendants physically alter and corrupt Microsoft products such as the Microsoft Windows products. Once infected, altered and controlled by Trickbot, the Windows operating system ceases to operate normally and becomes tools for Defendants to conduct their theft."
- Disabled most servers – check the status at https://feodotracker.abuse.ch/browse/trickbot/

Incident from summer/fall 2019

https://techcrunch.com/2019/09/01/police-botnet-takedown-infections/

https://decoded.avast.io/janvojtesek/putting-an-end-to-retadup-a-malicious-worm-that-infected-hundreds-of-thousands/

Police hijack a botnet and remotely kill 850,000 malware infections

Zack Whittaker @zackwhittaker / 6 months

Important details

- Retadup malware: cryptocurrency mining botnet controlling over 850,000 infected computers.
- Avast with the help of Cybercrime Fighting Center (C3N) of the French National Gendarmerie
- Abused a protocol flaw to send a self-destruct command to the malware process