Fireside Chat

Unit42 Views on Recent Trends in Security

unit42
PALO ALTO NETWORKS

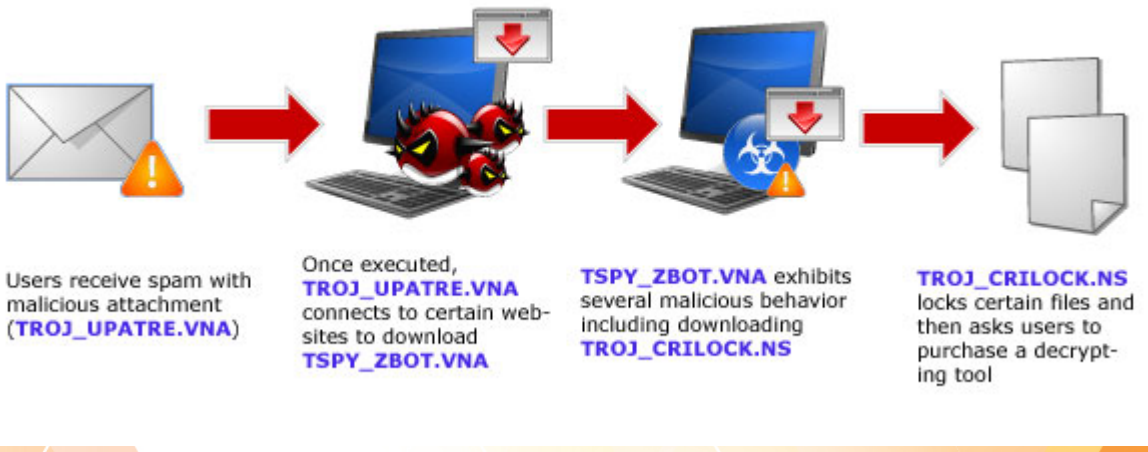
Overview

- Ransomware
  - Cryptolocker
- Industry Themes
  - Retail and POS Malware
  - Healthcare
- Desktop to Mobile
  - Wirelurker

unit42
PALO ALTO NETWORKS

Ransomware

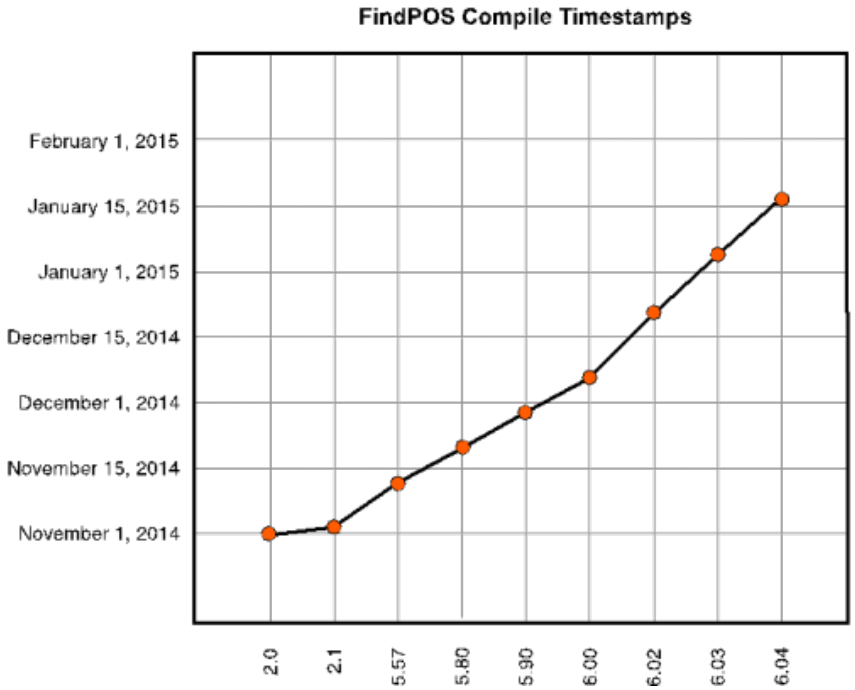
- In 2012, Symantec, using data from a command and control (C2) server of **5,700** computers compromised in one day, estimated that approximately 2.9 percent of those compromised users paid the ransom.
  - For a single C2 Server:
    Average ransom: $200 ➔ $33,060 profit per day ➔ $394,400 profit per month
- 2013 Variants: Xorist, CryptorBit, CryptoLocker
- 2014 Variants: CryptoDefense, Cryptowall
- Some variants encrypt not just the files on the infected device but also the contents of shared or networked drives.



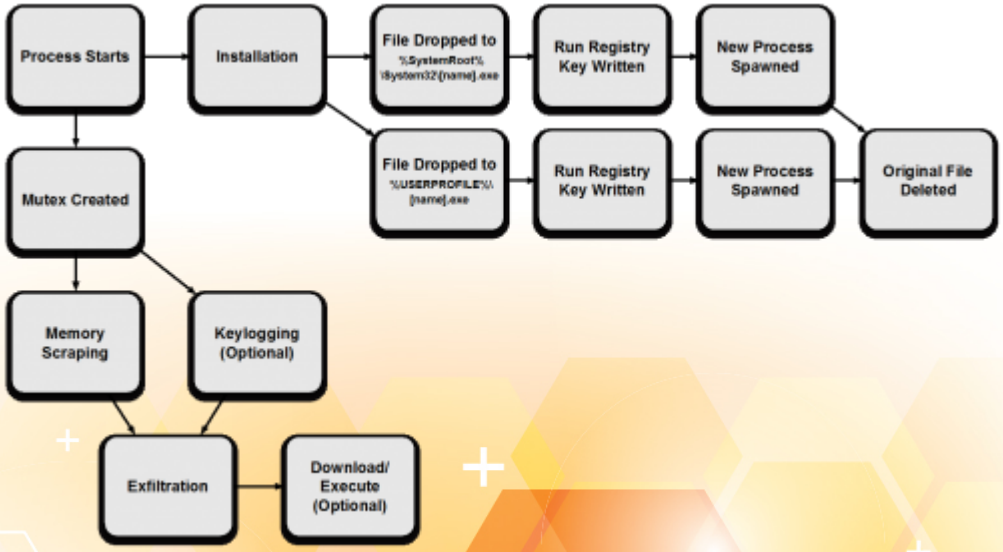
Source: https://www.us-cert.gov/ncas/alerts/TA14-295A

unit42 PALO ALTO NETWORKS

Retail Targets: Point of Sale Malware



Rapid Iteration and Evolution

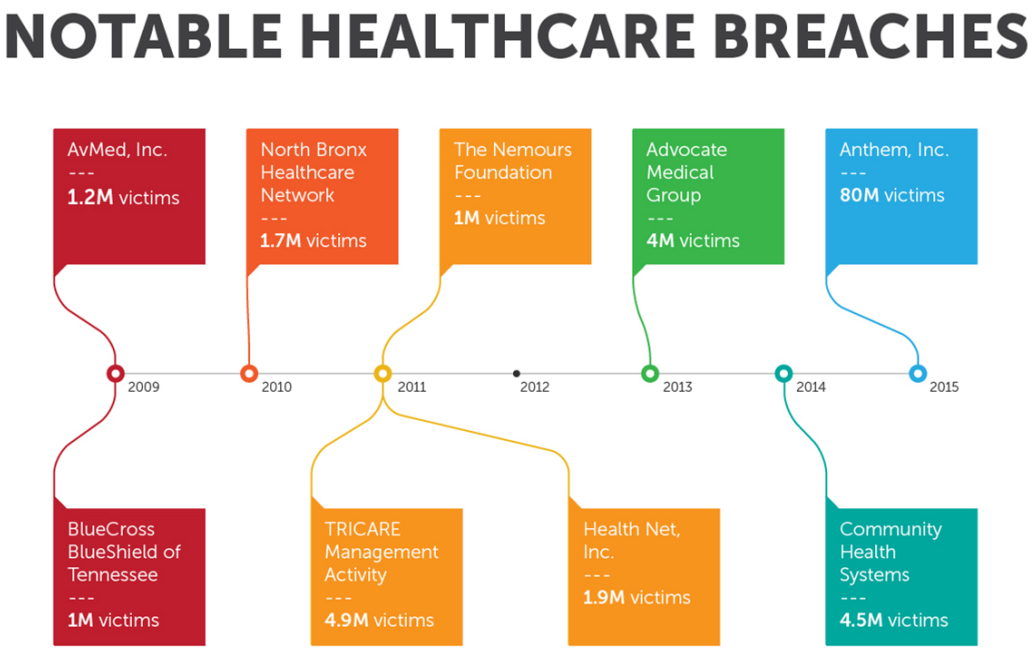


Simple and Efficient Execution

Source: http://researchcenter.paloaltonetworks.com/2015/03/findpos-new-pos-malware-family-discovered/

unit42 PALO ALTO NETWORKS

Healthcare



Source: http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/millions-affected-in-anthem-breach-healthcare-companies-prime-attack-targets

unit 42
PALO ALTO NETWORKS

Desktop to Mobile: WireLurker Attack