LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Threat Intelligence Briefing Mylobot

OVERALL CLASSIFICATION IS

UNCLASSIFIED

TLP:WHITE

12/13/2018

Agenda

Overview

- Characteristics
  - A Two-Stage Botnet
  - Defensive Manuevers
  - Offensive Manuevers
  - Second Stage
  - Attribution
  - IOCs

Possible Affects on Healthcare's Enterprise

- Vulnerability Impact
- Cyber Threats

Preventative Measures

Conclusion

Makeuseof.com

Slides Key:

👤 Non-Technical: managerial, strategic and high-level (general audience)

⚙ Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- Mylobot's Characteristics
  - A Two-Stage Botnet
    - First Stage: This botnet lies dormant within the infected system for 14 days before it beacons its command-and-control servers

➢ Two Defensive Manuevers-Incorporates several obfuscation techniques:

Executes from victim PC's memory
Anti-virtual machine
Anti-sandbox
Anti-debugging
Encrypts resource files
Delay mechanisim
Code injection
Process hollowing*
Reflective Executable (EXE)*

The Inquirer

Obfuscation Techniques

- Process hollowing- occurs when a process is created in a suspended state then its memory is unmapped and replaced with malicious code. Similar to Process Injection, execution of the malicious code is masked under a legitimate process and may evade defenses and detection analysis

Tools for Prevention: AppLocker & Dell Authority Management Suite

- Reflective Executable (EXE)- allows excutable files to be executed directly from memory, rather than from a computer's disk drive, thereby further avoiding detection

Tools for Prevention: System Monitor (SysMon) & Process Monitor (ProMon)

Second Iteration of Defensive Manuevering- Mylobot will:

- Shut down firewall ports
- Disable Windows Defender
- Disable Windows Updates

DeepInstinct.com

Offensive Tactics

Mylobot's Third Iteration-

- The Offensive Manuever- Seek and Destroy Campaign:

- The botnet unleashes a seek and destroy campaign on the infected computer for any other malware that my be present on the system.

- Mylobot scans the system’s Application Data folders for common malware files and folders, and if it finds a certain file or process, Mylobot terminates it.

- Mylobot not only seeks to enslave unsuspecting computers but maintains its money-making scheme by ridding the infected systems of other malware.

Hackread.com

Second Stage of Mylobot

Payloads- Mylobot has the capability, once the system is infected, to execute any type of payload. From ransomware to cryptomining, the victim has no control.

Five months after its discovery, Mylobot has been spotted to download Khalesi on the infected system. Khalesi was one of the top five downloadable malware in the first half of 2017.

Possible Capabilities:

-keylogger

-screen scraper

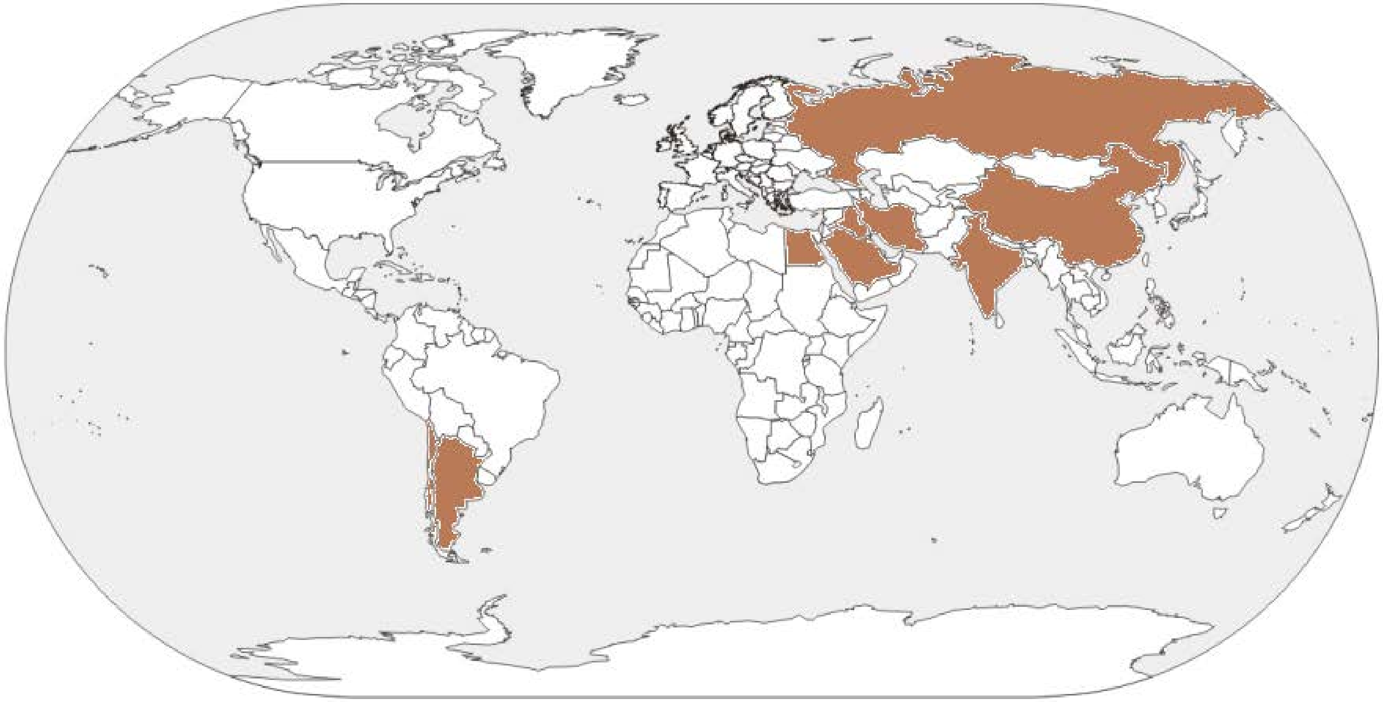
-spyware

-adware

TechSecurity.News

Attribution

Mylobot is not attributed to a known APT or FIN group at this time



Countries where majority of Mylobot's infrastructure IPs were located in analysis

Attribution

Other Clues to the Possible Origins of Mylobot:

- Asian character set and layouts
- Monetized motivation
- Malware collaboration

Mylobot's Indicators of Compromise

TLP:WHITE

Known C2 Domains and IPs

46.166.173.180

74.222.19.63

70.36.107.38

74.222.19.103

70.36.107.39

Downloader IP

138.128.150.133

File Hashes

9f930b106c1d1ddcb832a86e14c0474d3d2e6c22b0d3408fccfa8347d7f4e7c4

4ca8ef5d00bde49659ca97faf2a2a47445e6a3e82c151f18f0923392826d5af0

f6ac0ea45ccf7faded0fe03c13f356b82d03a9fc13a89194935ad75b8186275c

b7245ed896cd4199b410a326e1295aafb3e23c3311d301b1cdaf964cf7c008d9

NetFormation.com

Possible Affects on Healthcare's Enterprise

Vulnerability Impact

- Windows based environments

Cyber Threat Possibilities

- The botnet could be created to spread malware, launch DDoS attacks, and power ransomware campaigns

Patching & Prevention

- Be very cautious of downloading files you are unsure of with maintaining and mandating User Education and Training
- Keep a close eye on your network analytics for spikes or unauthorizations that differs from your baseline
- Diversify your network's products

References

“'Mylobot' botnet now downloading second-stage malware meant to siphon data,” November 14, 2018, accessed December 3, 2018; https://www.cyberscoop.com/mylobot-botnet-now-downloading-second-stage-malware-meant-to-siphon-data/

“Mylobot is sophisticated malware on the hunt for PCs to enslave,” June 21, 2018, accessed December 3, 2018; https://www.theinquirer.net/inquirer/news/3034597/mylobot-is-sophisticated-malware-on-the-hut-for-pcs-to-enslave

“What Is Mylobot Malware? How It Works and What to Do About It,” July 9, 2018, accessed December 3, 2018; https://www.makeuseof.com/tag/mylobot-malware/

“CenturyLink's Threat Research Labs blocks one-two punch of botnet,” November 15, 2018, accessed December 3, 2018; https://www.fiercetelecom.com/telecom/centurylink-threat-research-labs-blocks-one-two-punch-botnet

“Mylobot botnet delivers one-two punch with Khalesi malware,” November 14, 2018, accessed December 3, 2018; https://www.gurufocus.com/news/770443/mylobot-botnet-delivers-onetwo-punch-with-khalesi-malware

“Mylobot Malware Brings New Sophistication to Botnets,” June 20, 2018, accessed December 3, 2018; https://www.darkreading.com/vulnerabilities---threats/mylobot-malware-brings-new-sophistication-to-botnets/d/d-id/1332100

“Meet MyloBot malware turning Windows devices into Botnet,” June 25, 2018, accessed December 3, 2018; https://www.hackread.com/meet-mylobot-malware-turning-windows-devices-into-botnet/

“New Windows malware wants to add your PC to a botnet - or worse,” June 23, 2018, accessed December 3, 2018; https://www.komando.com/happening-now/466839/new-windows-malware-wants-to-add-your-pc-to-a-botnet-or-worse

“Meet MyloBot – A New Highly Sophisticated Never-Seen-Before Botnet That’s Out In The Wild,” June 20, 2018. accessed December 3, 2018; https://www.deepinstinct.com/2018/06/20/meet-mylobot-a-new-highly-sophisticated-never-seen-before-botnet-thats-out-in-the-wild/

“Mylobot: Windows malware wants to add your PC to a botnet – or worse,” June 20, 2018. accessed December 3, 2018; https://techsecurity.news/2018/06/mylobot-windows-malware-wants-to-add-your-pc-to-a-botnet-or-worse/

Conclusion

Upcoming Briefs

- Mobile Devices in the Health Sector
- Cryptomining Landscape
- Various APT/FIN Groups

Analyst-to-analyst webinars are available

Questions / Comments / Concerns?

HHS HC3 Email Address: HC3@hhs.gov