

Cyber@UC Meeting 62

Finals Week :P

If You're New!

- Join our Slack: ucyber.slack.com
- **SIGN IN!** (*Slackbot will post the link in #general*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment
- Ongoing Projects:
 - Lab in ERC!



Announcements

- Everyone's busy with finals week!
- Cory's **VirtualBox tutorials** up on YouTube
- We got a nice managed switch for ERC 516.



Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** [@CyberAtUC](https://twitter.com/CyberAtUC)
- **Facebook:** [@CyberAtUC](https://facebook.com/CyberAtUC)
- **Instagram:** [@CyberAtUC](https://instagram.com/CyberAtUC)

For more info: cyberatuc.org



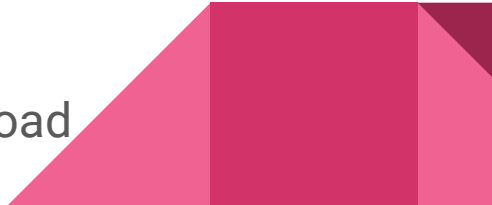
Weekly Content

Netspectre (a remote spectre attack)

- Found by security researchers
- All other forms of spectre have previously required local code execution
- Using an avx-based covert channel, attackers could steal data at a rate of 60 bits per hour
- Would allow the reading of arbitrary memory from the systems available on the network
- Works by measuring the response time of the machine by when sending specially crafted messages
- Was already patched in the initial Spectre Intel patch

<https://thehackernews.com/2018/07/netspectre-remote-spectre-attack.html>

Ghost in the Shell

- Named PowerGhost by Kaspersky
 - Stealthily establishes itself in a system and then spreads across large corporate networks
 - Infects workstations and servers
 - Data suggests that miners are replacing ransomware
 - PowerGhost is an obfuscated PowerShell script that contains the core code and add-on-modules
 - The miner, mimikatz, msvcp120.dll, and msucr120.dll, reflective PE injection module, and shellcode for EternalBlue exploit
 - Relies on fileless techniques to remain hidden
 - During infection, a one line shell script runs to download and run the miner
- 

Ghost in the Shell (continued)

- Running can be broken down into the following steps
 - Auto-self-updating
 - Propagation
 - Escalation of privileges
 - Establishing foothold in system
 - Payload
- Indicators of compromise listed at source link below

<https://securelist.com/a-mining-multitool/86950/>



Recommended Reading (leaks and breaches)

- <https://thehackernews.com/2018/07/data-breach-healthcare.html>
- <https://www.darkreading.com/attacks-breaches/unitypoint-health-reveals-14-million-patient-breach/d/d-id/1332457>
- <https://thehackernews.com/2018/07/dixons-carphone-data-breach.html>
- <https://thehackernews.com/2018/07/wikileaks-twitter-chats.html>
- <https://krebsonsecurity.com/2018/07/lifelock-bug-exposed-millions-of-customer-email-addresses/>
- <https://www.darkreading.com/threat-intelligence/reddit-warns-users-of-data-breach/d/d-id/1332458>



Recommended Reading

- <https://thehackernews.com/2018/07/android-cryptocurrency-mining.html>
- <https://thehackernews.com/2018/07/google-titan-security-key-fido.html>
- <https://thehackernews.com/2018/08/censored-google-search-china.html>
- <https://www.welivesecurity.com/2018/08/01/hp-offers-rewards-hacking-printers/>
- <https://www.welivesecurity.com/2018/07/31/onedrive-android-fingerprint-authentication/>
- <https://www.welivesecurity.com/2018/07/31/inmates-hack-tablets-free-credits-prison/>



Recommended Reading (Continued)

- <https://www.darkreading.com/endpoint/new-chrome-extension-alerts-users-to-hacked-sites/d/d-id/1332455>
- <https://thehackernews.com/2018/07/iphone-hacking-spyware.html>
- <https://thehackernews.com/2018/07/samsam-ransomware-attacks.html>
- <https://thehackernews.com/2018/07/kickico-cryptocurrency.html>
- <https://krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/>

