

Cyber@UC Meeting 78

Aaron McCanty visiting from Battelle

If You're New!

- Join our Slack: cyberatuc.slack.com
- Check out our website: cyberatuc.org
- **SIGN IN!** (*Slackbot will post the link in #general every Wed@6:30*)
- Feel free to get involved with one of our committees:
Content Finance Public Affairs Outreach Recruitment Lab
- Ongoing work in our research lab!




Announcements

- Looking for lab committee volunteers!
- Merchandise on the way, Online Shop
- CTF team training was this past Saturday
- We got MaaS (metal as a service) working in the lab!
- We're going to NorseRage's CTF at NKU on November 28th



Weekly News

StatCounter Hijacked Leads To Bitcoin Theft

- Gate.io crypto exchange compromised by their web analytics service, StatCounter
 - Malicious code found on >700k websites, bundled with traffic tracking code
 - Replaced tracking script with code target Gate.io customers
 - StatCounter is a bit old, but very popular real-time web analytics platform
 - Reported as being used in >2 million websites and >10 billion page views/month
 - Malicious code made to target a gate.io specific URI
 - Code replaced destination of bitcoin address with that of attacker's
 - Generated a new address everytime
 - Gate.io no longer uses StatCounter
 - Gate.io has not released stats on how many were affected
- 

VirtualBox Flaw, Escaping The Sandbox

- Vulnerability for Intel PRO 1000 MT Desktop network card when network mode is set to NAT, memory corruption
- OS type does not matter
- Poc published to GitHub, link in article
- Allows a malicious attacker with root privs in guest OS to escape and run arbitrary code in the application layer (ring 3, low privs) on the host
- Could leave host open to other vulnerabilities, like privilege escalation
- Not yet patched



Bleeding Bit

- Two new zero day vulns found by Armis, the guys who caught BlueBorne
- Allow arbitrary code execution and full C&C w/o auth
 - Ex. Insulin pumps, pacemakers, credit card readers, routers
- Vulns in bluetooth chips made by Texas Instruments
- Sending more traffic to the BLE chip causes a buffer overflow, allow malicious code execution, requires physical proximity
- Firmware update feature, Over the Air firmware Download (OAD)
- All Aruba devices share OAD password, obtainable by sniffing legitimate packets or reverse-engineering the firmware
 - Attacker can send a malicious firmware update
- Patches released last Thursday



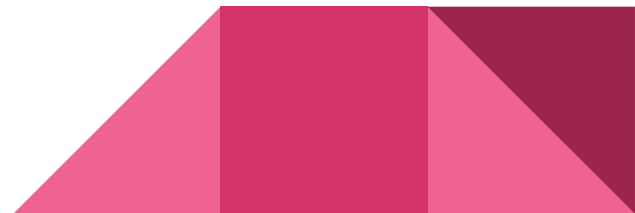
Recommended Reading

<https://thehackernews.com/2018/11/android-in-app-updates-api.html>

<https://krebsonsecurity.com/2018/11/u-s-secret-service-warns-id-thieves-are-abusing-usps-mail-scanning-service/>

<https://www.darkreading.com/vulnerabilities---threats/the-morris-worm-turns-30-/d/d-id/1333225>

<https://www.welivesecurity.com/2018/11/05/malware-1980s-brain-virus-morris-worm/>



Recommended Reading (continued)

<https://www.welivesecurity.com/2018/11/09/us-air-force-hackable-bug-bounty-program/>

<https://krebsonsecurity.com/2018/11/bug-bounty-hunter-ran-isp-doxing-service/>

<https://thehackernews.com/2018/11/gaming-server-ddos-attack.html>

<https://www.welivesecurity.com/2018/11/08/cyber-insurance-question/>

<https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/>

Recommended Reading (continued)

<https://thehackernews.com/2018/11/portsmash-intel-vulnerability.html>

<https://thehackernews.com/2018/11/self-encrypting-ssd-hacking.html>

<https://thehackernews.com/2018/11/woocommerce-wordpress-hacking.html>





**OUR FEATURE
PRESENTATION**