Meeting 1/29/20

Introduced officers

Chase cyber security in the news

Went around the room introducing everyone

CYBER SECURITY CLUB

1/29/2020

NEED TO KNOW

- Department of Defense Scholarship
  - Due February 13th
  - https://www.iup.edu/DoDscholarship/
- Cyber Security Club Discord
  - https://discord.gg/gPeT4P4

NEW INTERNET EXPLORER BUG

- CVE-2020-0674
- A new Internet Explorer bug was found and is being executed in the wild
- The bug takes advantage of the way the JS scripting engine handles objects in memory
- The bug allows attackers to gain access to the PC and run arbitrary code as the current user
- Effectives IE 11 mainly, still possible on 10 and 9

EUROPEAN ENERGY COMPANIES ATTACKED

- A campaign of attacks was carried out again various European energy companies in what was thought to be a recon mission
- The open source tool PupyRat was used to carry out these attacks
- Though the malware is open source, it is prominently linked with the Iranian state backed group APT 33
- The events happened between November 2019 and January 2020
- Nothing has come of this yet

AWS ENGINEER SPILLED CRITICAL INFO ON GITHUB

- A repository was found on GitHub that contained critical AWS information
- There were multiple keys found for AWS services along with a file called rootkey.csv suggesting it gave root access to their account
- Things like passwords, logs, and documents labeled “Amazon Confidential” were found
- Documents in the repository were used to link the repository to an AWS employee
- The repository was left up for a total of 5 hours

NSA REVEALS CRITICAL WINDOWS FLAW

- The NSA was attributed for the first time ever on a Microsoft Vulnerability report for a new bug found that effects all versions of Windows
- This bug allows attackers to spoof digital signatures and run malicious code as signed from a trusted source
- It is not unusual for the NSA to report bugs to Microsoft, but this is the first time they did it publically
- Leaks from NSA vulnerabilities research in the past has lead to things like WanaCry and other variants of ransomware

MICROSOFT LEAKS USER DATA

- 250 Million customer records were leaked from a customer support data base
- This database was by a research team called Comparitech
- Information in the data base included customer email addresses, IP addresses, locations, Microsoft support agent emails, case numbers, resolutions, and remarks and internal notes marked as “confidential”.
- The leak was due to a misconfiguration of the security rules that controlled who had access to the database
- Microsoft claims this breach has nothing to do with their security of their cloud storage solutions