FUJITSU

Monthly Cyber Threat Intelligence Bulletin

Cloudbleed is the latest in a string of vulnerabilities that should be of concern to enterprise IT security and a reminder us of the problems caused by user password reuse across corporate services and personal web sites and cloud services.
https://storify.com/jessicajown/online-info-blog-cloudflare-bug-spills-private-dat?utm_source=hs_email&utm_medium=email&utm_content=44790540&_hsenc=p2ANqtz-893CCGEC3qKOsmfMQw1Ks_PHpjA8zEsxuiPdM0dBwR9w6lUXmakCdhgBXMYMD1a7chpeIxEnXu8nSF-TTWkEC3XDjhww&_hsmi=44790540

DDoS attacks like this aren't the only ways in which botnets can be used by hackers. They can be used to perpetrate click fraud (defrauding online advertising services which pay by the click), evade spam filters, speed up password guessing, mine Bitcoins, or really anything else that would require a large network of computers working together.
http://principia-scientific.org/botnets-dangerous-downside-internet-things/?utm_source=hs_email&utm_medium=email&utm_content=44212517&_hsenc=p2ANqtz--ktJ0zh9QqrSfkHAcEzCPF2Bc80jYxMS45ZeuF7zTEss4zcj9YF3dNmMyDlcYEm5qhlR00ksMOfArkjLIZpK4nuFd4Gg&_hsmi=44212517

Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA.
http://www.organizedrage.com/2017/03/the-latest-wikileaks-disclosure-is.html?utm_source=hs_email&utm_medium=email&utm_content=44212517&_hsenc=p2ANqtz--hoDwT2hjmB5DL4BYOZeCnl2rj5Son5Ch708zIYQBUJ-adGwlAAd1ccM_ms-rXou4gjzjv-COPu_PVQC-TPzoIVJ07Xg&_hsmi=44212517

Kaspersky Lab researchers discovered StoneDrill with the help of Yara-rules created to identify unknown samples of Shamoon, they realised they were looking at a unique piece of malicious code that seems to have been created separately from Shamoon.
http://www.ilonggotechblog.com/2017/03/from-shamoon-to-stonedrill-advanced-new-destructive-malware.html?utm_source=hs_email&utm_medium=email&utm_content=44212517&_hsenc=p2ANqtz--1F4RsvKBBmC8l-o5E3W0MyJNw-8DvNRrRgHINnfTLvT4CnGD5gy11HW2NwxJu3VHs60mEJYsBhyAp1vgnkaviKo5tEw&_hsmi=44212517

The new version of Dridex (Dridex v4) is the first malware that uses the AtomBombing process to try and infect systems. It uses atom tables to copy its payload and some other related data into the memory space of a target process.
http://www.darkreading.com/attacks-breaches/new-version-of-dridex-banking-trojan-uses-atombombing-to-infect-systems/d/d-id/1328299

Criminal organization selling counterfeit sports apparel is engaging in spam to promote their retail websites. In addition to spam, we have shown that they are also using brute force attacks, targeting WordPress websites, from one of their spam servers which is hosted at a well known bullet proof host, Pp Sks Lugan, based in Ukraine.
https://www.wordfence.com/blog/2017/03/jersey-shore/?utm_source=hs_email&utm_medium=email&utm_content=43792312&_hsenc=p2ANqtz-_ZWvl1nM0YhDTOF57kKWxtUpYILmdx4c7Wd3tRijMVE2hY-oN9U_QkQUabosGCJqt61GX62zkZVLvNbuuX0MbkxUpBTA&_hsmi=43792312