# Weekly Intelligence Summary

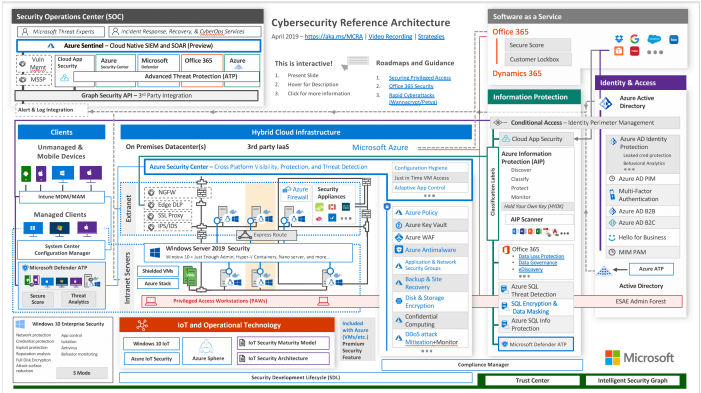
Apr 17, 2020 - COVID-19 is still in the spotlight this week:

Zoom's privacy and security woes are still flowing around Hong Kong communities. Two big global FSIs are on the list of a 500k Zoom accounts found for sales on the dark web. Other stuffs should attract more attentions:

- (cisp-id:7799) Both NTT and Microsoft are offering free protection to healthcare industry in APAC regions. Beware security vendors, I think Microsoft has a big plan (MCRA) on expanding their security solutions: Sentinel, Azure AD, Windows Defender ATP, Windows 10 VBS, Office 365 ATP (Fig. 1)
- (cisp-id:7770, cisp-id:7815) The #SFO breach!! - "What information was involved? At this time, it appears the attackers may have accessed the impacted users' usernames and passwords used to log on to those personal devices." This incident shows actors' TTP (#Magcart, #Dragonfly?) like the attacks in British Airways (or CX). If critical infrastructure, including HK Airport, MTR, Hospitals, PLC/HK Electric, HKEX, think that their networks are running an inside private network (unlike : http://faog.org.hk (cisp-id:7798) ); therefore they are well protected by existing technologies. That kind thinking may have some issue as refer to this incident.
- (cisp-id:7808) BEC, target phishing, Trickbot/Ryuk are still evolving.
- (cisp-id:7804) COVID-19 is the key enabler for VPN-routers (cisp-id:7813) exploit researches. 0-days come out including US-CERT (cisp-id:7817) and FBI (cisp-id:7812) issued alerts.

(cisp-id:7799) April 14, 2020

Microsoft AccountGuard for Healthcare is a security service offered at no cost for healthcare providers on the front line of care combatting COVID-19, including hospitals, care facilities, clinics, labs, and clinicians, as well as pharmaceutical, life sciences, and medical devices companies that are researching, developing, and manufacturing COVID-related treatments, and non-governmental organizations (NGOs), and international non-governmental organizations (INGOs) (collectively, COVID-19 Responders). The service is designed to help these highly targeted customers protect themselves from cybersecurity threats.
https://thehill.com/policy/cybersecurity/492675-microsoft-offers-free-cybersecurity-services-to-protect-health-groups




(Fig. 1 – Microsoft Cybersecurity Reference Architecture)

(cisp-id:7804) April 15, 2020

Multiple fiber routers are being compromised by botnets using 0-day. 360.cn claims that

“这是我们过去 30 天内的第 3 篇 IoT 0-day 漏洞文章，之前我们还披露了 DrayTek Router 在野 0-day 漏洞分析报告[1]，LILIN DVR 在野 0-day 漏洞分析报告[2]。我们观察到僵尸网络存在相互竞争获取更多的 Bot 规模的情况，其中有些僵尸网络拥有一些 0-day 漏洞资源，这使它们看起来与众不同。我们正在研究并观察 IoT Botnet 使用 0-day 漏洞传播是否是一个新趋势。”

https://blog.netlab.360.com/multiple-fiber-routers-are-being-compromised-by-botnets-using-0-day-en/

*(Interesting to see 360.com paying attentions on IoT devices and routers. Unlike other security researchers, they put high attention on devices produced by Taiwan (https://www.draytek.com and https://www.meritlilin.com/en/product/category/50), India (https://www.netlink-india.com). Actually, there are two devices from Taiwan under their surveillance, I assume it is a coincident*
***Updates: Our honeypot catches CVE-2020-8515: DrayTek scans using https://www.exploit-db.com/exploits/48268)***

(cisp-id:7808) April 14, 2020

By the Intel 471 Malware Intelligence team. One of the more notable relationships in the world of cybercrime is that between Emotet, Ryuk and TrickBot. This loader-ransomware-banker trifecta has wreaked havoc in the business world over the past two years, causing millions of dollars in damages and ransoms paid. Our Malware Intelligence team receives a lot of great questions from our clients on this subject, so we thought it would be good to do a Q/A style blog covering some of the more general questions.
https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/amp/
*(https://dragonadvancetech.com/reports/Ransomware%20Playbook_v3.3.pdf)*

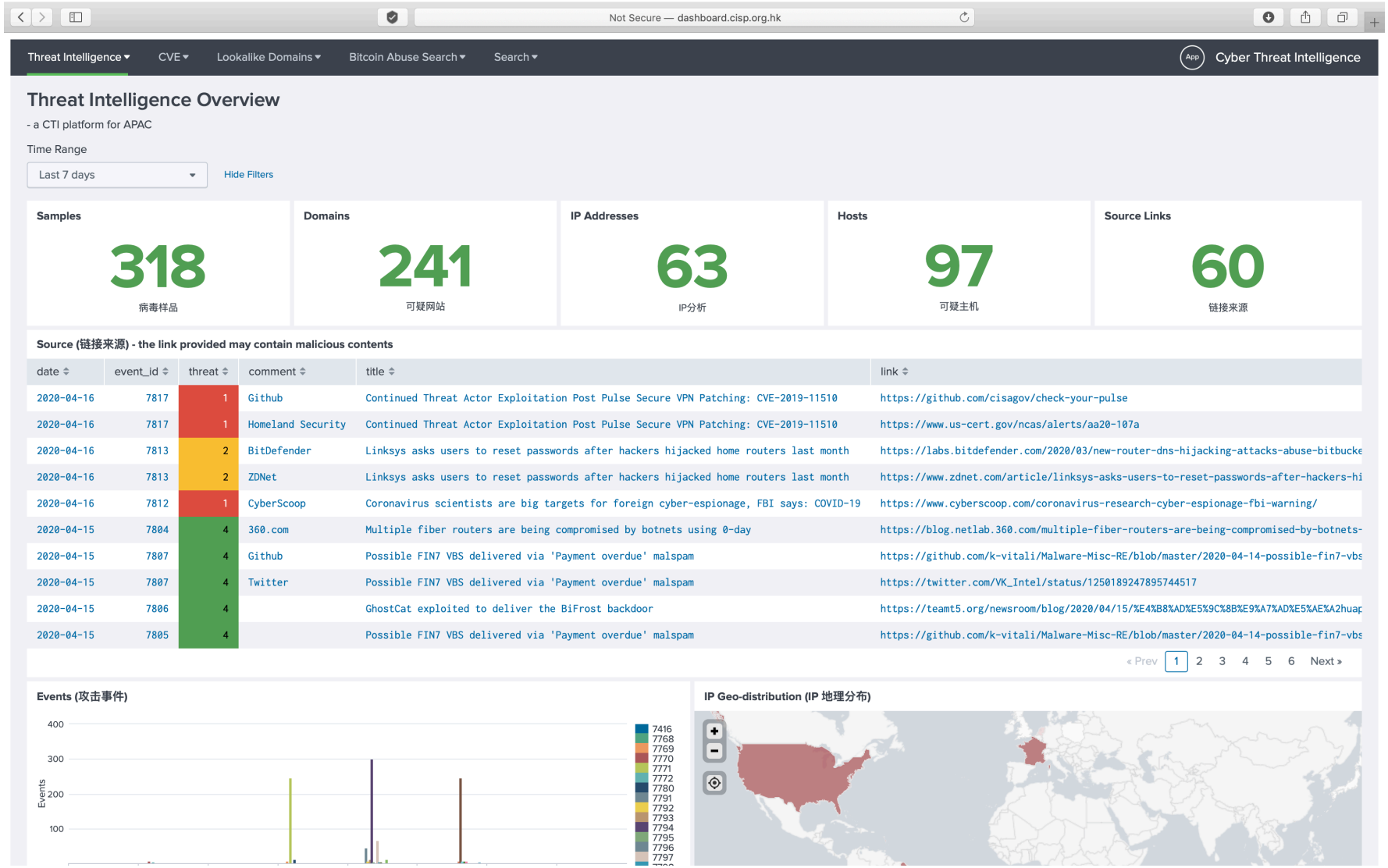
(cisp-id:7817) April 16, 2020

This Alert provides an update to Cybersecurity and Infrastructure Security Agency (CISA) Alert AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability, which advised organizations to immediately patch CVE-2019-11510—an arbitrary file reading vulnerability affecting Pulse Secure virtual private network (VPN) appliances. CISA is providing this update to alert administrators that threat actors who successfully exploited CVE-2019-11510 and stole a victim organization’s credentials will still be able to access—and move laterally through—that organization’s network after the organization has patched this vulnerability if the organization did not change those stolen credentials.

(cisp-id:7802) April 14, 2020

While the various COVID-19 themed phishing campaigns observed by Unit 42 are numerous, this blog seeks to provide a thorough picture and solid technical analysis of the cross-section between the various types of COVID-19 themed threats organizations may be facing during the ongoing pandemic. Specifically, we address a ransomware variant (EDA2) observed in attacks on a Canadian government healthcare organization and a Canadian medical research university, as well as an infostealer variant (AgentTesla) observed in attacks against various other targets (e.g, a United States defense research entity, a Turkish government agency managing public works, a German industrial manufacturing firm, a Korean chemical manufacturer, a research institute located in Japan and medical research facilities in Canada).
https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/

*Our Threat Intelligence Platform (http://dashboard.cisp.org.hk/) is ready for public access.*




*Get access? please send an email to: admin@dragonadvancetech.com*