Weekly Intelligence Summary

Apr 30, 2020 (TLP: WHITE)

The cyber-attacks and vulnerabilities seem to be affected by the COVID-19 lockdowns. Microsoft is on the spotlight after last week's Microsoft Online Tech Forum HK.

- Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams… CyberArk make a good comparison reference to the vulnerability of Teams and Zoom for the online meeting solutions which are heavily used by Hong Kong communities and business entities. Interesting to find this news is not attracted much public concerns in Hong Kong.
- HK SFC finally and being the first Hong Kong regulator posted a WFH instructions/guidelines for Hong Kong financial institutions. Their circular covering 2 areas: Remote access to internal network and systems and use of videoconferencing platforms. The circular addressed the use of Zoom, but not Microsoft Teams. 👍
- Microsoft Threat Protection Intelligence Team said: Using an attack pattern typical of ***human-operated ransomware campaigns***, attackers have compromised target networks for several months beginning earlier this year and have been waiting to monetize their attacks by deploying ransomware when they would see the most financial gain. We have published and confirmed similar findings 3 weeks ago.

(cisp-id:7884) April 29, 2020

In light of the increased use of remote office arrangements, the Securities and Futures Commission (SFC) reminds licensed corporations (LCs) to assess their operational capabilities and implement appropriate measures to manage the cybersecurity risks associated with these arrangements.

When staff work remotely, they may access the LC's internal network and systems from outside the office and hold meetings through videoconferencing platforms. This circular sets out examples of controls and procedures to assist in the protection of LCs' internal networks and data. LCs are reminded that the following examples are not exhaustive. They should implement and maintain measures which are deemed appropriate to the situation and commensurate with the size and complexity of their operations. The circular covering: (A) Remote access to internal network and systems & (B) Use of videoconferencing platforms.
https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=20EC37

(cisp-id:7874) April 29, 2020

Remote spring: the rise of RDP brute force attacks, Kaspersky said in Securelist blog.

With the spread of COVID-19, organizations worldwide have introduced remote working, which is having a direct impact on cybersecurity and the threat landscape. One of the most popular application-level protocols for accessing Windows workstations or servers is Microsoft's proprietary protocol — RDP. The lockdown has seen the appearance of a great many computers and servers able to be connected remotely, and right now we are witnessing an increase in cybercriminal activity with a view to exploiting the situation to attack corporate resources that have now been made available (sometimes in a hurry) to remote workers.
https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

(cisp-id:7881) April 28, 2020

Microsoft Threat Protection Intelligence Team said: Ransomware groups continue to target healthcare, critical services; here's how to reduce risk. At a time when remote work is becoming universal and the strain on SecOps, especially in healthcare and critical industries, has never been higher, ransomware actors are unrelenting, continuing their normal operations. The ransomware

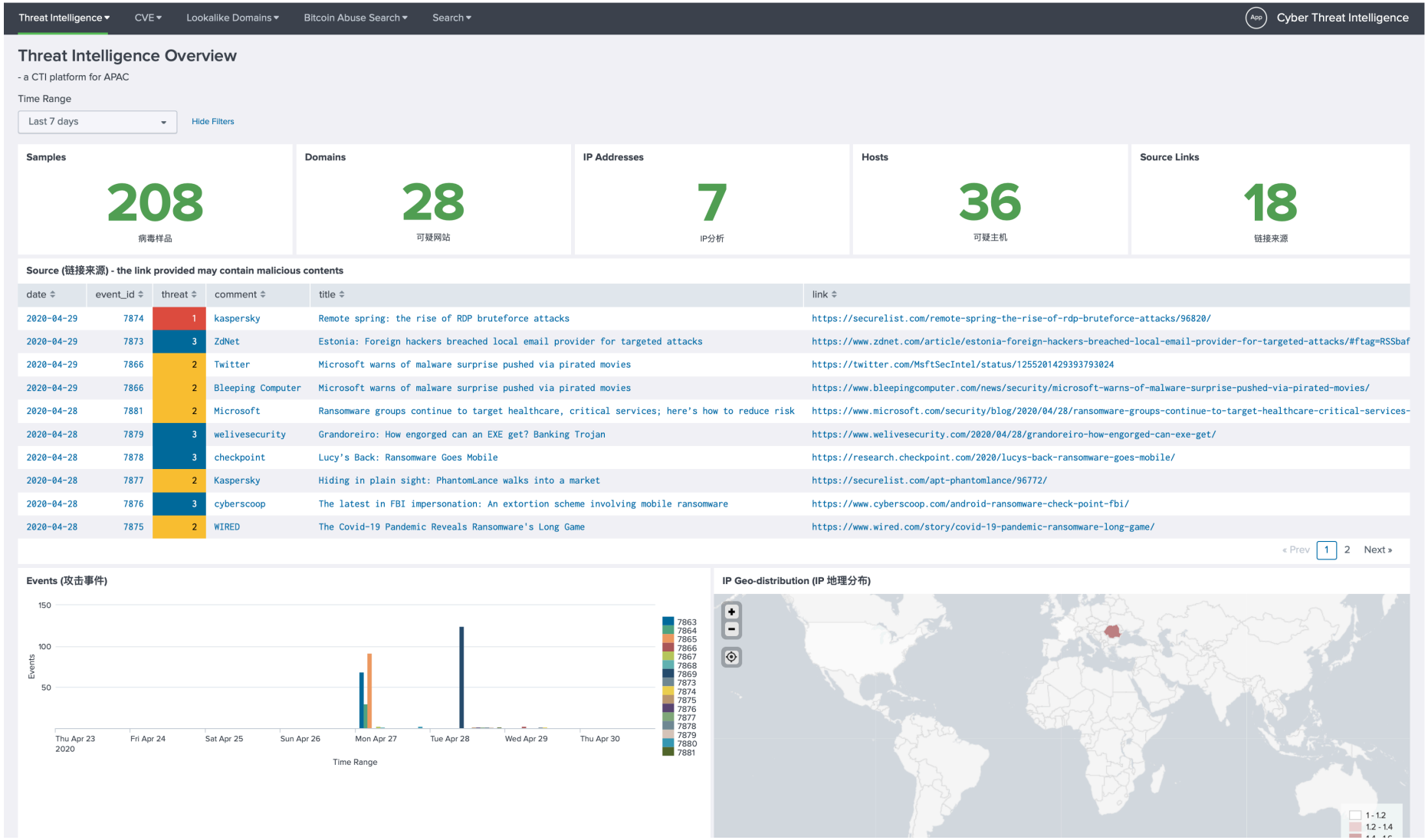
deployments in this two-week period appear to cause a slight uptick in the volume of ransomware attacks. However, Microsoft security intelligence as well as forensic data from relevant incident response engagements by Microsoft Detection and Response Team (DART) showed that many of the compromises that enabled these attacks occurred earlier. Using an attack pattern typical of human-operated ransomware campaigns, attackers have compromised target networks for several months beginning earlier this year and have been waiting to monetize their attacks by deploying ransomware when they would see the most financial gain.
https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

(cisp-id:7877) April 28, 2020
APT group OceanLotus try hiding in plain sight: PhantomLance walks into a market. In July 2019, Dr. Web reported about a backdoor trojan in Google Play, which appeared to be sophisticated and unlike common malware often uploaded for stealing victims' money or displaying ads. So, we conducted an inquiry of our own, discovering a long-term campaign, which we dubbed "PhantomLance", its earliest registered domain dating back to December 2015. We found dozens of related samples that had been appearing in the wild since 2016 and had been deployed in various application marketplaces including Google Play. One of the latest samples was published on the official Android market on November 6, 2019. We (Kaspersky) informed Google of the malware, and it was removed from the market shortly after. More information on PhantomLance is available to customers of Kaspersky Intelligence Reporting. For more information, contact intelreports@kaspersky.com.
https://securelist.com/apt-phantomlance/96772/

(cisp-id:7883) April 28, 2020
Microsoft Patches Dangerous Teams Vulnerability. CyberArk says issue would have allowed attackers to take over Teams accounts using a malicious GIF.
Microsoft has patched a dangerous vulnerability in its Teams collaboration platform that would have allowed attackers to potentially take control of an organization's entire roster of Teams accounts using a malicious GIF. The vulnerability is the latest to highlight the heightened risks that organizations face from having a high percentage of their employees work from home because of the COVID-19 pandemic.

Researchers from CyberArk discovered the vulnerability while examining Microsoft Teams' security this March. According to the security vendor, the problem had to do with how authentication information was handled when users shared or viewed images that were shared with them on the Teams platform.
https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/
https://www.darkreading.com/vulnerabilities---threats/microsoft-patches-dangerous-teams-vulnerability/d/d-id/1337665
https://thehackernews.com/2020/04/microsoft-teams-vulnerability.html

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



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