Weekly Intelligence Summary

Apr 25, 2020 (TLP: WHITE)

COVID-19 is still in the spotlight this week. (cisp-id:7848) Google said.

- All VPN vulnerabilities, including Pulse Connect Secure, give adversaries ways to launch stealth attacks during COVID-19 period because all organizations are forced to allow their employees to WFH in the past months. I had post Orange [1] Tsai's SSL VPN vulnerability alert in 8/2019, however; this week I notice an ISP is proposing an *interesting* "SOC" service to a client by only monitoring the logs of that VPN box. In a Splunk event last year, a tier-1 HK organization complained that they paid millions but don't know what their out-sourced SOC can help them.
- Ransomware attackers are not only looking for a few hundred USD now but aggressively asking for bigger $$$. ***DoppelPaymer*** and ***Nightwalker*** ransomware will publish your data if you don't pay. Please don't tell me that there is ***NO*** data breach in your organization if a few servers were only infected with ransomware.
- As of 21/4, Threatpost told us, the IBM Data Risk Manager 0-days are still un-patched. This incident reminds me on 6/19 Reuters told us China hacked eight major MSSP in years-long attack [2]
- FireEye claims Vietnamese Threat Actors APT32 targeting Wuhan government

[1] https://blog.orange.tw/2019/08/attacking-ssl-vpn-part-2-breaking-the-fortigate-ssl-vpn.html
[2] https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers

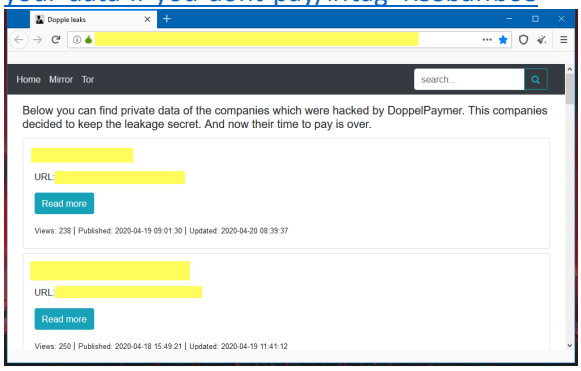
(cisp-id:7841) April 23, 2020

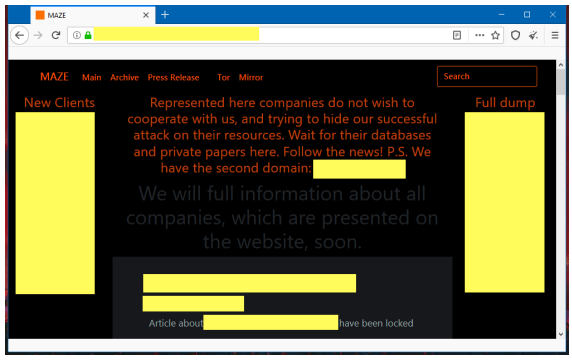
On April 6, 2020, three issues were discovered in Host Checker policy enforcement on Pulse Secure Pulse Connect Secure (PCS). These vulnerabilities were encoded as CVE-2020-11580 (No certificate Validation), CVE-2020-11581 (Command Injection), CVE-2020-11582 (DNS Rebindig). These vulnerabilities could allow a man-in-the-middle (MITM) attacker to perform a remote code execution (RCE) attack. CERT-EU is not aware of any malicious exploitation for those vulnerabilities, but we have to take into consideration that the file on which these vulnerabilities are built (tncc.jar) is not obfuscated in any way and the original source code can be obtained with almost any Java decompiler and customized in a malicious manner. (cisp-id:7839) CrowdStrike also discovered two distinct vulnerabilities in the Windows, Linux and macOS versions of the Palo Alto Networks GlobalProtect VPN client.
https://media.cert.europa.eu/static/SecurityAdvisories/2020/CERT-EU-SA2020-023.pdf
https://www.crowdstrike.com/blog/exploiting-escalation-of-privileges-via-globalprotect-part-1/

(cisp-id:7836) April 21, 2020

The security researcher Pedro Ribeiro, Director of Research at Agile Information Security, has published details about four zero-day vulnerabilities affecting the IBM Data Risk Manager (IDRM) after the company refused to address the issues. The IBM Data Risk Manager is an enterprise security product that aggregates feeds from vulnerability scanning tools and other risk management tools allowing to analyzed security events and data-related business risks. IBM weighed in on the problem this week, after a researcher went public with the bugs, one of which may end up being a zero-day issue — Big Blue is still investigating.
https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/
https://threatpost.com/rce-exploit-ibm-data-risk-manager-no-patch/154986/

(cisp-id:7831) April 21, 2020
The City of Torrance of the Los Angeles metropolitan area, California, has allegedly been attacked by the DoppelPaymer Ransomware, having unencrypted data stolen and devices encrypted. The attackers are demanding a 100 bitcoin ($689,147) ransom for a decryptor, to take down files that have been publicly leaked, and to not release more stolen files. In February 2020, DoppelPaymer created a site called "Dopple Leaks" that they used to publish the stolen data of victims who refuse to pay a ransom. (cisp-id:7828) Ransomware gangs are getting more aggressive these days about pursuing payments and have begun stealing and threatening to leak sensitive documents if victims don't pay the requested ransom demand, ZDnet said.
https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-hits-los-angeles-county-city-leaks-files/
https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/#ftag=RSSbaffb68





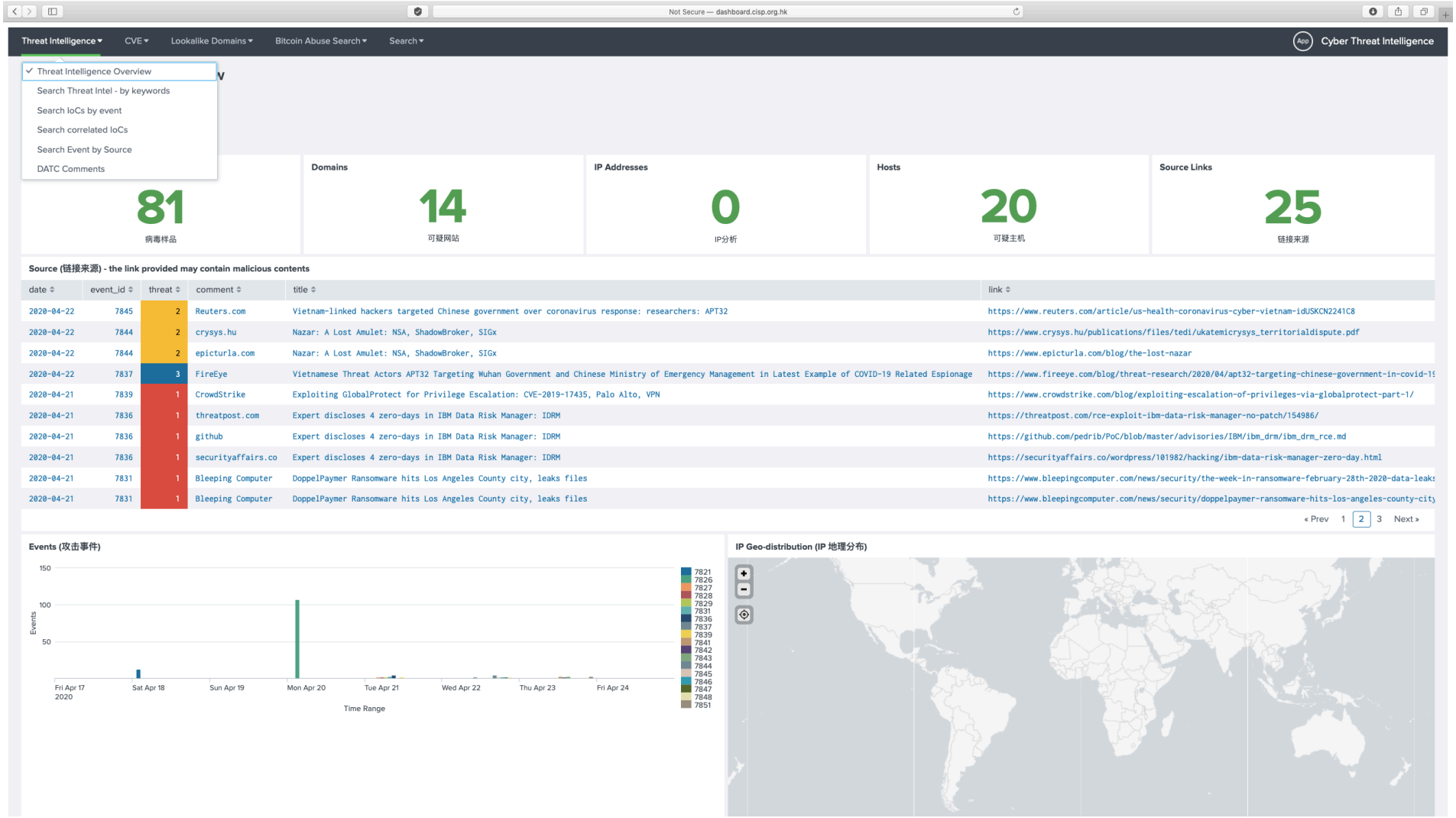
(Screenshots from ZDnet)

(cisp-id:7837) April 21, 2020
From at least January to April 2020, suspected Vietnamese actors APT32 carried out intrusion campaigns against Chinese targets that Mandiant Threat Intelligence believes was designed to collect intelligence on the COVID-19 crisis. Spear phishing messages were sent by the actor to China's Ministry of Emergency Management as well as the government of Wuhan province, where COVID-19 was first identified. While targeting of East Asia is consistent with the activity, we've previously reported on APT32, this incident, and other publicly reported intrusions, are part of a global increase in cyber espionage related to the crisis, carried out by states desperately seeking solutions and nonpublic information.
https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

(cisp-id:7846) April 21, 2020
Over the past few weeks, Morphisec Labs researchers identified a flaw in the Zoom application that can enable threat actors to voluntarily record Zoom sessions and capture chat text without any of the meeting participants' knowledge. The Zoom malware is even able to do this when the host has disabled recording functionality for participants. The trigger is a malware that injects its code into a Zoom process without any interaction of the user and even if the host did not enable the participant to record.
https://blog.morphisec.com/zoom-malware-can-record-meetings-attack-simulation-shows-how

(cisp-id:7851) April 21, 2020
If this scary scenario sounds familiar to you, it is because not so long ago, we released a report about a similar case investigated by CPIRT – An incident where attackers were able to divert $1M of funds, which were supposed to be transferred from a Chinese venture capital.
https://research.checkpoint.com/2020/ir-case-the-florentine-banker-group/

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



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