Weekly Intelligence Summary

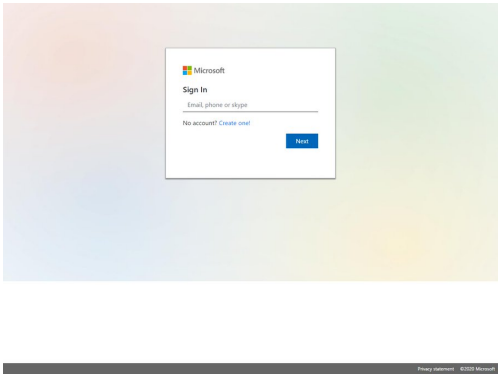
May 15, 2020 (TLP: WHITE)

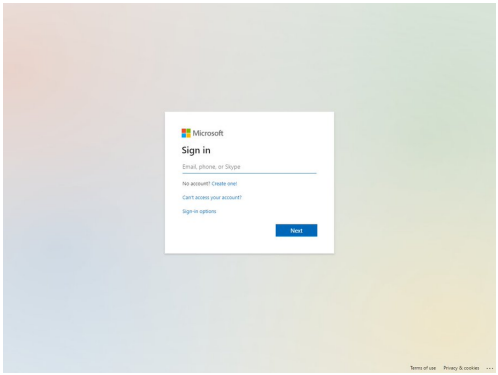
In the spotlight this week:

- Microsoft finally take some efforts to help Office 365 users to defence targeted phishing or BEC attacks by changing their login page with more sign-in options. They also disclosed attackers technique by sending email that carry a PDF attachment on OnneDrive to ask user to sign in fake AD page to capture users' credentials (assume users not turned on #MFA)
- PaloAlto published a blog to discuss the SilverTerrie group – the Nigerian cyber criminals launching BEC attacks campaigns recklessly included targets including government healthcare agencies, local and regional governments, large universities with medical programs/centers, regional utilities, medical publishing firms, and insurance companies. We are handling cases in #HongKong
- US-CERT published IOCs a MAR of malware variant has been identified as COPPERHEDGE. This is the reason why you can see there is a hung increase in number of sample collections on our http://dashboard.cisp.org.hk platform. #ForIocLovers
- Fortune 500s (#HK) in the crosshairs. Maze ransomware or ChaCha was first observed in May 2019 and has targeted organizations in North America, South America, Europe, Asia, and Australia.

(cisp-id:7901) May 7, 2020

The new Azure AD sign-in page was announced in February and started rolling out in April. The phishing campaigns show how fast attackers can adapt to changes in the experiences they mimic. One phishing campaign used emails with the subject line "Business Document Received". The emails carry a PDF attachment that poses as a OneDrive document requiring the user to sign in. The link points to a phishing site that spoofs the new sign-in page. https://twitter.com/MsftSecIntel/status/1260975503340482560





(cisp-id:7907) May 7, 2020

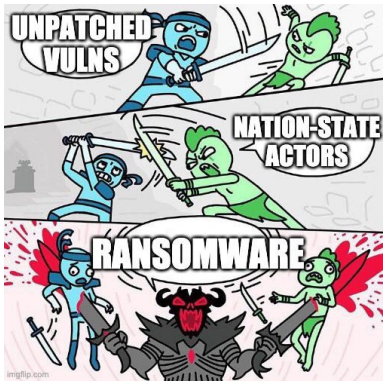
Focusing on one of the most active subsets of the global threat landscape, Palo Alto Networks Unit 42 tracks Nigerian cyber criminals involved in Business Email Compromise (BEC) activities under the name SilverTerrier. Over the past 90 days (Jan. 30 – Apr. 30), we have observed three SilverTerrier actors/groups launch a series of 10 COVID-19 themed malware campaigns. These campaigns have produced over 170 phishing emails seen across our customer base. While broad in their targeting, these actors have exercised minimal restraint in terms of targeting organizations that are critical to COVID-19 response efforts. Specifically, we find it alarming that several of these campaigns recklessly included targets at government healthcare agencies, local and regional governments, large universities with medical programs/centers, regional utilities, medical publishing firms, and insurance companies across the United States, Australia, Canada, Italy, and the United Kingdom.

https://unit42.paloaltonetworks.com/silverterrier-covid-19-themed-business-email-compromise/

(cisp-id:7969) May 12, 2020
The Malware Analysis Report is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD). Working with U.S. Government partners, DHS, FBI, and DoD identified Remote Access Tool (RAT) malware variants used by the North Korean government. This malware variant has been identified as COPPERHEDGE. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.
https://www.us-cert.gov/northkorea
https://www.us-cert.gov/ncas/analysis-reports/ar20-133a

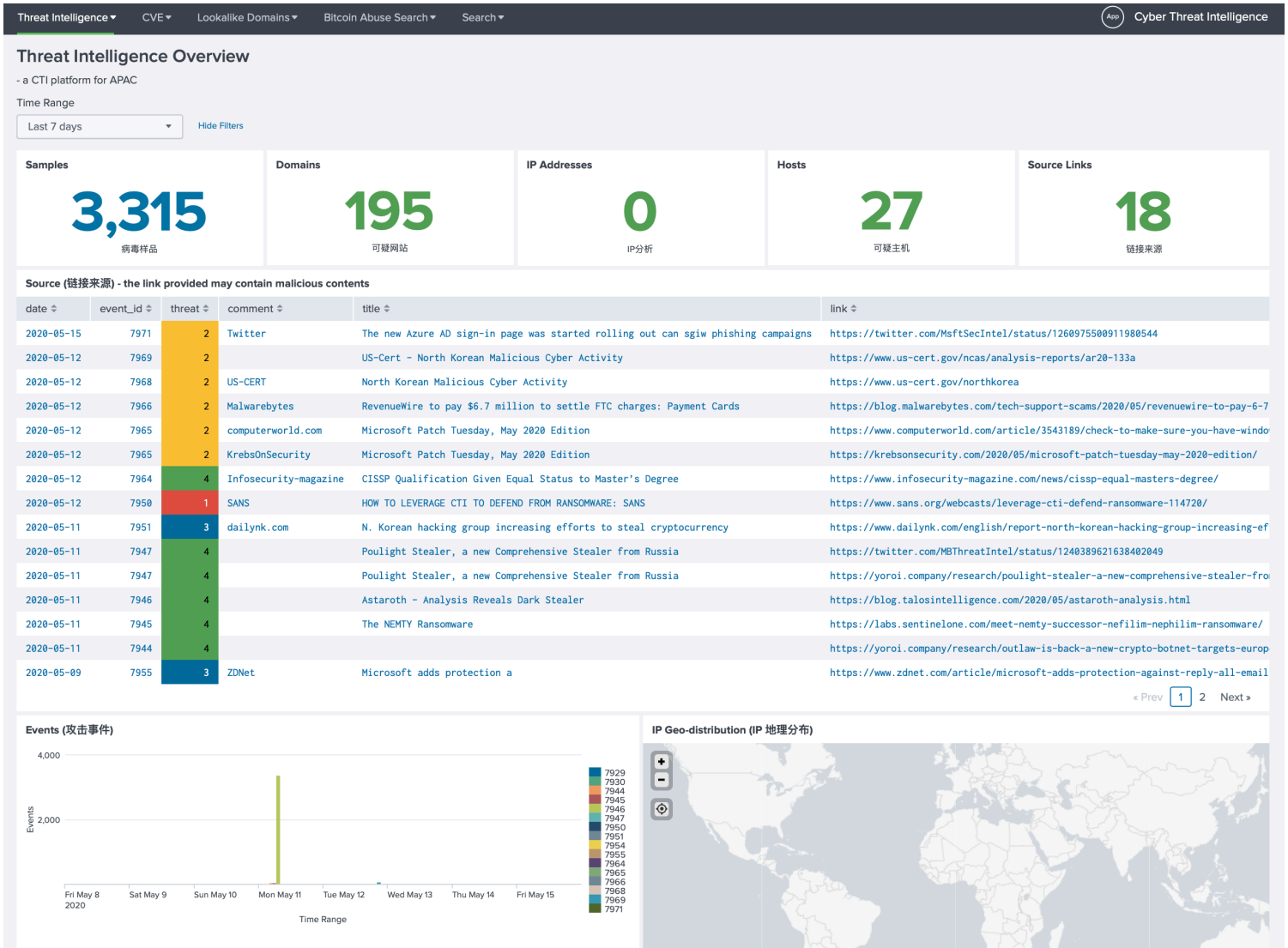
(cisp-id:7965) May 12, 2020
Brian Krebs said: Microsoft today issued software updates to plug at least 111 security holes in Windows and Windows-based programs. None of the vulnerabilities were labeled as being publicly exploited or detailed prior to today, but as always if you're running Windows on any of your machines it's time once again to prepare to get your patches on. But focusing solely on Microsoft's severity ratings may obscure the seriousness of the flaws being addressed this month.
https://krebsonsecurity.com/2020/05/microsoft-patch-tuesday-may-2020-edition/

(cisp-id:7930) May 9, 2020
Fortune 500s in the crosshairs: One of Maze's biggest scalps was the multibillion-dollar IT services company Cognizant, which has clients in the banking and oil and gas industries. Despite a reported denial of involvement from the hackers themselves, Maze's fingerprints were on last month's attack that disrupted Cognizant's work with its clients.
https://www.cyberscoop.com/maze-ransomware-mandiant-lessons-learned/



(cisp-id:7929) May 9, 2020
Maze ransomware, a variant of ChaCha ransomware, was first observed in May 2019 and has targeted organizations in North America, South America, Europe, Asia, and Australia. This ransomware is typically distributed via emails containing weaponized Word or Excel attachments. However, it has also been distributed via exploit kits. The malware first establishes a foothold within the environment. It then obtains elevated privileges, conducts lateral movement, and begins file encryption across all drives. However, before encrypting the data, these operators may exfiltrate the files to be used for further coercion, including public exposure.
https://unit42.paloaltonetworks.com/threat-brief-maze-ransomware-activities/

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



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