Weekly Intelligence Summary

May 8, 2020 (TLP: WHITE), updated May 10, 2020

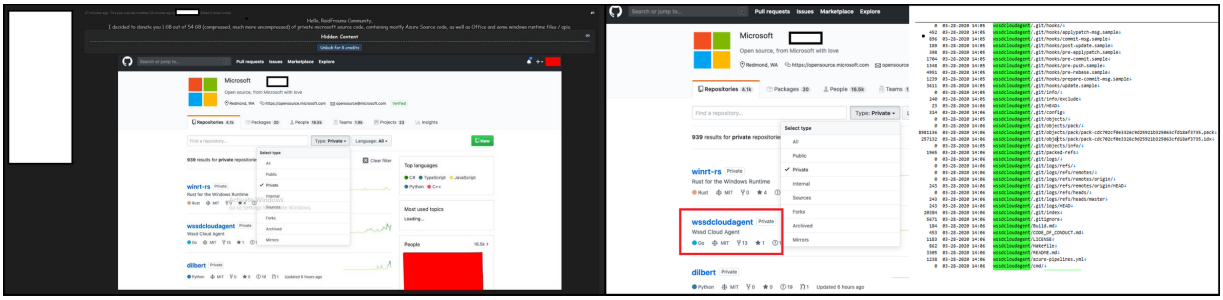
In the spotlight this week:

- ***We Chat, They Watch*** @jsrailton said: Everyone knows that Chinese chat apps do blocking, and sometimes monitoring. But the discovery that the rest of the world is being surveilled in order to train and refine censorship in China shows just how far private companies go to comply with Beijing's self-censorship demands. This is the reason why I use 2 phones and always turn off my China Mobile SIM when I left office. *(update: ZDnet has confirmed with multiple Micorsoft employees at least a small portion are authentic)*
- An alarming rumour was found from twitter on May 7. I said it is alarming because the twit mentioned a possible incident that Microsoft's Azure cloud platform source code may be leaked on private github. I remember another AWS incident. On Nov 2019, threatpost reported that Imperva's data breach[1] was actually caused by a misconfiguration on AWS cloud. In APAC, more and more entities are planning to move part of their data centres to the cloud but they seldom check the share responsibility SLAs on cybersecurity protection and just believe the myth CSP will protect them well… ;)
- There are two major ransomware incidents identified. TrendMicro reported: Targeted ransomware (***EDA2***[2] ***– educational ransomware***) attack hits Taiwanese Organizations. KrebsonSecurity reader also disclosed the Europe's largest private hospital operator was hit by ***Snake ransomware***. Kreb refers to his previous posting about ransomware gangs now outing victim business that don't pay by publishing[3] stolen data from victims.

[1] https://threatpost.com/imperva-data-breach-cloud-misconfiguration/149127/
[2] https://github.com/m0n0ph1/malware-1/tree/master/Eda2
[3] ***https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html***

(cisp-id:7992) May 8, 2020
How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus
Documents and images transmitted entirely among non-China-registered accounts undergo content surveillance wherein these files are analyzed for content that is politically sensitive in China. Upon analysis, files deemed politically sensitive are used to invisibly train and build up WeChat's Chinese political censorship system. From public information, it is unclear how Tencent uses non-Chinese-registered users' data to enable content blocking or which policy rationale permits the sharing of data used for blocking between international and China regions of WeChat.
https://citizenlab.ca/2020/05/we-chat-they-watch/

(cisp-id:7901) May 7, 2020
@underthebreach post this twit on 7/5/2020. HUGE: The person behind the recent Tokopedia hack claiming he has 500GB (uncompressed) worth of private Microsoft source code, containing mostly Azure Source code, as well as Office and some windows runtime files / APIs. Appears to be stolen from private Github repositories. After some research and because the actor dumped the entire dirlist of the private repositories, it appears this is real. I doubt there is anything too private in these repositories, but companies do sometime leave keys/passwords on Github by mistake.
https://twitter.com/underthebreach/status/1258153076554375168



(screenshots from @underthebreach's post)

(cisp-id:7909) May 6, 2020

On Tuesday, a KrebsOnSecurity reader who asked to remain anonymous said a relative working for Fresenius Kabi's U.S. operations reported that computers in his company's building had been roped off, and that a cyber-attack had affected every part of the company's operations around the globe. The reader said the apparent culprit was the Snake ransomware, a relatively new strain first detailed earlier this year that is being used to shake down large businesses, holding their IT systems and data hostage in exchange for payment in a digital currency such as bitcoin. Some or all of this data is then published on victim-shaming sites set up by the ransomware gangs as a way to pressure victim companies into paying up.

https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/

https://krebsonsecurity.com/2019/12/ransomware-gangs-now-outing-victim-businesses-that-dont-pay-up/

(cisp-id:7908) May 6, 2020

How hackers are updating the EVILNUM malware to target the global financial sector. Hackers behind a series of targeted financial attacks have been updating their malware to better evade detection over the last year, according to new Prevailion research slated to be published Wednesday. Since at least February 2019, the hackers, who have begun impersonating CEOs and banks in their lure documents, have introduced at least seven updates to the malicious software known as EVILNUM, which enables attackers to upload and download files, harvest tracking cookies, and run arbitrary commands.

https://twitter.com/underthebreach/status/1258153076554375168

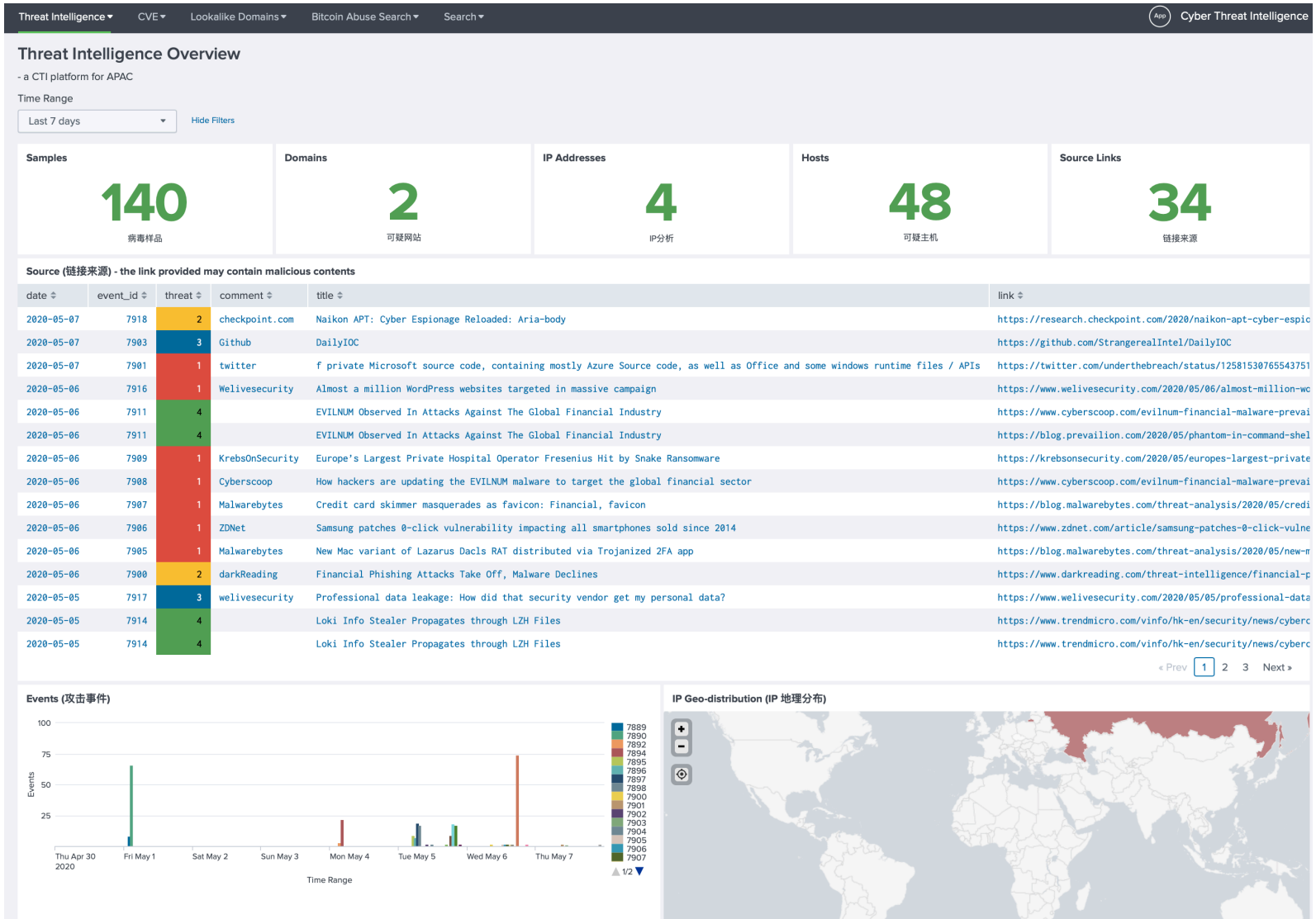
(cisp-id:7901) May 6, 2020

Credit card skimmer masquerades as favicon: Financial, favicon.

Malware authors are notorious for their deceptive attempts at staying one step ahead of defenders. As their schemes get exposed, they always need to go back to their bag of tricks to pull out a new one. When it comes to online credit card skimmers, we have already seen a number of evasion techniques, some fairly simple and others more elaborate. The goal remains to deceive online shoppers while staying under the radar from website administrators and security scanners. In this latest instance, we observed an old server-side trick combined with the clever use of an icon file to hide a web skimmer. Threat actors registered a new website purporting to offer thousands of images and icons for download, but which in reality has a single purpose: to act as a façade for a credit card skimming operation.

https://blog.malwarebytes.com/threat-analysis/2020/05/credit-card-skimmer-masquerades-as-favicon/

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



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