Weekly Intelligence Summary

Jun 19, 2020 (TLP: WHITE)

In the spotlight this week:

- Lines between Advance Persistent Threat (**APT**) and cyber-crime gangs are becoming even more blurred. After robbing banks and cryptocurrency exchanges, state-sponsored hackers have been recently spotted trying **BEC** scams. ESET researchers found a new actor called #OpeartionInterception #HKcryptoExNetflowToC2
- SameOperation: ESET researchers uncover #cyberattacks against #aerospace and #military companies, with hints suggesting the #Lazarus #APT group may be behind the #attacks. Read about ***Operation In(ter)ception*** on WeLiveSecurity. #infosec #malware #espionage
- #MAZE and #Netwalker ransomware gangs still active publishing leaks from compromised networks. The leaks of 1 HK company was removed from #Netwalker Blog, but another HK company, currently undergoing a General Offer, their leaks are still be found from #MAZE blog in the dark web. ***#1PaidRansom?***
- In my first Weekly Summary (published on April 9), I said: "*the term Cyber Threat Intelligence means different to different people*". PewPew map is usually loved by top management and Hong Kong regulators since 2016. They are still love it, but the "i" seems changed to "information" instead of "intelligence" ;)

(cisp-id:8127) Jun 17, 2020

Aerospace and military companies in the crosshairs of cyberspies.

To compromise their targets, the attackers, the same "**Operation In(ter)ception**" used social engineering via **LinkedIn**, hiding behind the ruse of attractive, but bogus, job offers. Having established an initial foothold, the attackers deployed their custom, multistage malware, along with modified open-source tools. Besides malware, the adversaries made use of living off the land tactics, abusing legitimate tools and OS functions. Several techniques were used to avoid detection, including code signing, regular malware recompilation and impersonating legitimate software and companies. According to our investigation, the primary goal of the operation was espionage. While we did not find strong evidence connecting the attacks to a known threat actor, we discovered several hints suggesting a possible link to the Lazarus group, including similarities in targeting, development environment, and anti-analysis techniques used.

https://www.welivesecurity.com/wp-content/uploads/2020/06/ESET_Operation_Interception.pdf
https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

(cisp-id:8126) Jun 17, 2020

North Korea's state hackers caught engaging in BEC scams.

ESET researchers said they spotted North Korean state-sponsored hackers attempting to steal money from targets they initially breached for cyber-espionage purposes. Codenamed "**Operation In(ter)ception**," this campaign targeted victims for both cyber-espionage and financial theft. ESET security researcher Jean-Ian Boutin said the attacks have been carried out by members of the Lazarus Group -- codename given by security firms to North Korea's biggest hacking unit, part of the country's intelligence service. Boutin described how Lazarus

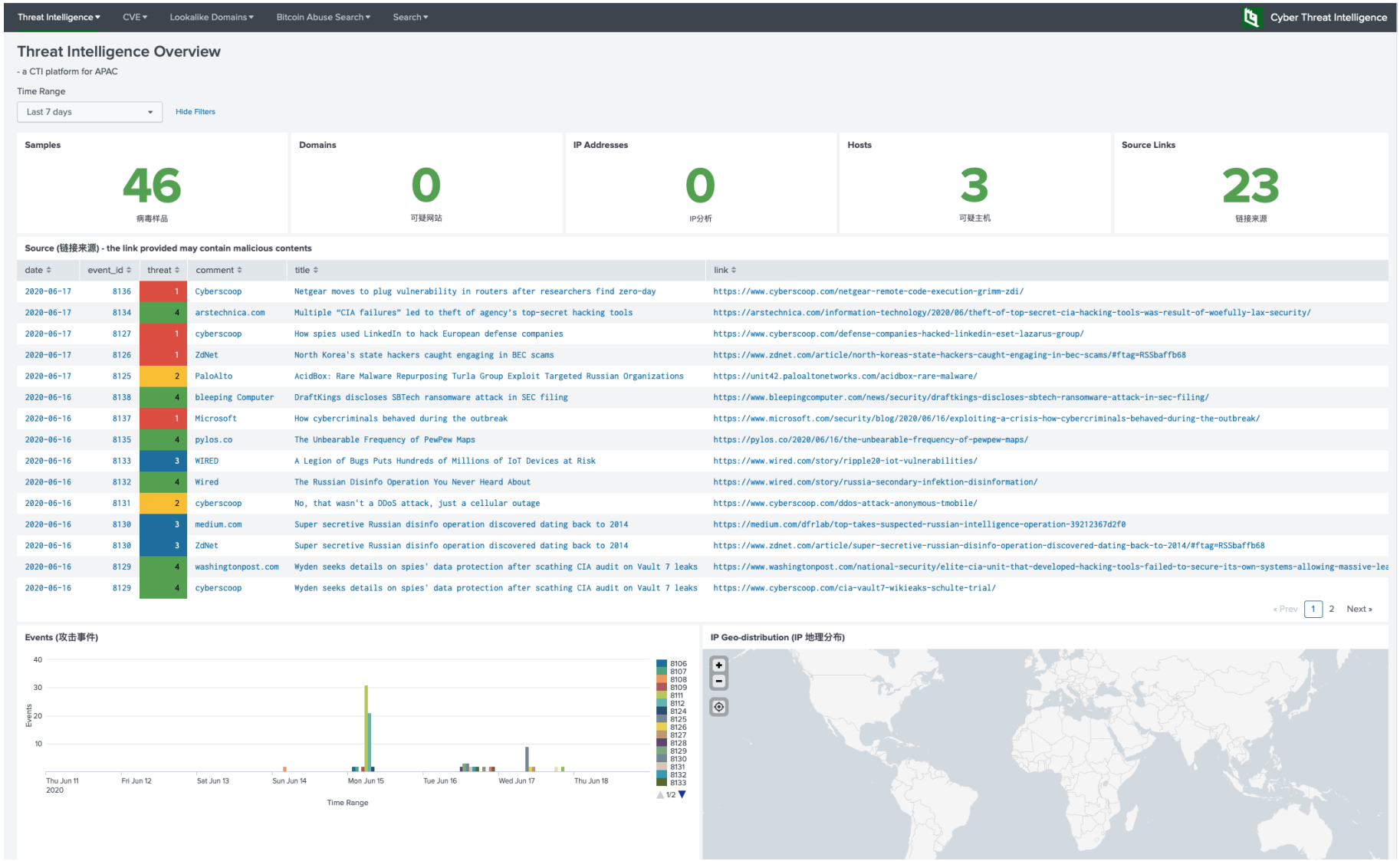
members used LinkedIn job recruiter profiles and private messages to approach their targets. On the guise of conducting a job interview, victims were given archives to open and view files stored inside that allegedly contained salary and other information about their future jobs.
https://www.zdnet.com/article/north-koreas-state-hackers-caught-engaging-in-bec-scams/#ftag=RSSbaffb68

(cisp-id:8125) Jun 17, 2020
AcidBox: Rare Malware Repurposing Turla Group Exploit Targeted Russian Organizations. When the news broke in 2014 about a new sophisticated threat actor dubbed the Turla Group, which the Estonian foreign intelligence service believes has Russian origins and operates on behalf of the FSB, its kernelmode malware also became the first publicly-described case that abused a third-party device driver to disable Driver Signature Enforcement (DSE). This security mechanism was introduced in Windows Vista to prevent unsigned drivers from loading into kernel space. Turla exploited the signed VirtualBox driver, VBoxDrv.sys v1.6.2, to deactivate DSE and load its unsigned payload drivers afterward. In February 2019, Unit 42 found that a yet-to-be-known threat actor — unbeknownst to the infosec community — discovered that the second unpatched vulnerability can not only exploit VirtualBox VBoxDrv.sys driver v1.6.2, but also all other versions up to v3.0.0.
https://unit42.paloaltonetworks.com/acidbox-rare-malware/

(cisp-id:8135) Jun 16, 2020
The Unbearable Frequency of **PewPew Maps**.
Joe - the blogger, recently made a joke online relative to a major – and very respected, if geopolitically controversial – security company advertising its revised “Cyberthreat Real-Time Map”. As many members of the security community are aware, “threat maps” – referred to derisively as “pewpew” maps – are heavy on eye-candy but very light on use or value. Yet pewpew maps – such as that featured by now-defunct security company Norse remain prominent in security operations centers (SOCs), watchfloors, and sales demos to this day. Oddly enough, roughly the same time as this discussion, a mini-controversy erupted over an alleged (and since debunked) distributed denial of service (DDoS) activity against US cellular providers – based on a pewpew map.
https://pylos.co/2020/06/16/the-unbearable-frequency-of-pewpew-maps/

Similar Pewpew map on Hong Kong TV a few years ago (Source: HK TVB)

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



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