Weekly Intelligence Summary

Aug 28, 2020 (TLP: WHITE)

In the spotlight this week:

- ***The Lazarus Group*** exposed Wednesday, which is also known as APT38, has also recently been sending fake job postings in spear-phishing attacks targeting the ***defense sector***. U.S. government have also exposed financially-motivated hacking campaign launched by North Korea's ***BeagleBoyz*** for the sophisticated cyber-enabled ATM cash-out campaigns identified publicly as "***FASTCash***". The BeagleBoyz often put ***destructive anti-forensic*** tools onto computer networks of victim institutions. In 2018, they deployed wiper malware against a bank in Chile that crashed computers and servers to distract from efforts to send fraudulent messages from the bank's ***compromised SWIFT terminal***.
- A company involved in ***billion-dollar real estate*** deals in New York, London, Australia, and Oman has recently become the target of a cyber-espionage campaign. The hackers infiltrated the victim firm by imitating a plugin for a popular 3D computer graphics software, ***AutoDesk 3ds Max***. The perpetrators are likely ***hackers-for-hire*** who split their time between running nation-state cyber-operations and conducting corporate espionage on behalf of private sector entities.
- DDoS extortionists target NZX, Moneygram, Braintree, and other financial services. One of the victims, the ***New Zealand stock exchange*** (NZX), has halted trading for the third day in a row following the attacks. The group uses names like ***Armada Collective*** and ***Fancy Bear*** — both borrowed from more famous hacker groups — to email companies and threaten DDoS attacks that can cripple operations and infer huge downtime and financial costs for the targets unless the victims pay a huge ransom demand in Bitcoin. DATC found the actors once threatened a ***Hong Kong Domestic Bank*** in last Oct.
- While some ransomware groups have heavily targeted ***Citrix and Pulse Secure VPNs*** to breach corporate networks in H1 2020, most ransomware attacks take place because of compromised RDP endpoints. The top three most popular intrusion methods include unsecured ***RDP endpoints***, ***email phishing***, and the exploitation of corporate ***VPN appliances***. Hong Kong Pwc Darklab blog also disclosed two HK companies were compromised because of the Pulse Secure VPN vulnerability.
- A new and interesting module in the modern ***QBot variant*** described by Check Point as an "***email collector module***" extracts all email threads contained within an Outlook client and uploads them to the attacker's command-and-control (C2) server.

(cisp-id:8567) Aug 27, 2020

An Old Bot's Nasty New Tricks: Exploring Qbot's Latest Attack Methods.

Towards the end of July, one of today's most serious cyber threats, the Emotet Trojan, returned to full activity and launched multiple malspam campaigns. One of Qbot's new tricks is particularly nasty, as once a machine is infected, it activates a special 'email collector module' which extracts all email threads from the victim's Outlook client and uploads it to a hardcoded remote server. These stolen emails are then utilized for future malspam campaigns, making it easier for users to be tricked into clicking on infected attachments because the spam email appears to continue an existing legitimate email conversation.

https://research.checkpoint.com/2020/exploring-qbots-latest-attack-methods/

(cisp-id:8570) Aug 26, 2020

Malicious Autodesk plugin at root of cyber-espionage campaign.

A company involved in billion-dollar real estate deals in New York, London, Australia, and Oman has recently become the target of a cyber-espionage campaign. The hackers waged the campaign

against the target, an international architectural and video production entity, in a likely effort to collect financial information or negotiation details of competing contracts for a customer, Bitdefender assessed. They infiltrated the victim firm by imitating a plugin for a popular 3D computer graphics software, AutoDesk 3ds Max, and then deploying a malicious file against the target.
https://www.bitdefender.com/files/News/CaseStudies/study/365/Bitdefender-PR-Whitepaper-APTHackers-creat4740-en-EN-GenericUse.pdf

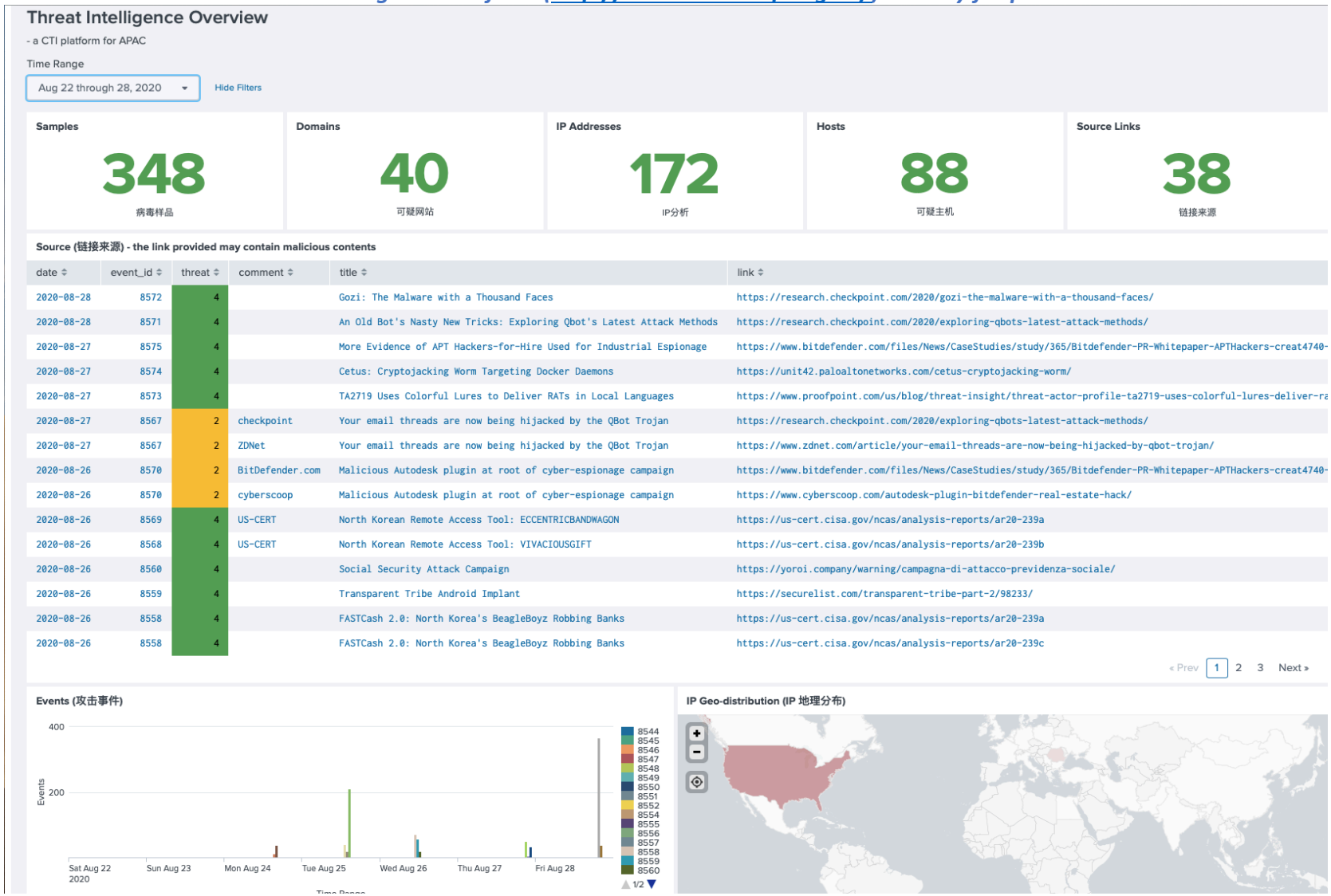
(cisp-id:8546) Aug 26, 2020
US government exposes North Korean government ATM cashout hacking campaign.
The joint announcement follows a steady stream of U.S. government efforts to publicly ferret out North Korean government-linked hacking. The hacking group exposed Wednesday, which is also known as APT38 or Lazarus Group, has also recently been sending fake job postings in spearphishing attacks targeting the defense sector. Previous announcements from the U.S. government have also exposed financially-motivated hacking campaigns. North Korea's BeagleBoyz are responsible for the sophisticated cyber-enabled ATM cash-out campaigns identified publicly as "FASTCash" in October 2018. The BeagleBoyz's bank robberies pose severe operational risk for individual firms beyond reputational harm and financial loss from theft and recovery costs. In 2018, a bank in Africa could not resume normal ATM or point of sale services for its customers for almost two months following an attempted FASTCash incident. The BeagleBoyz often put destructive anti-forensic tools onto computer networks of victim institutions. Additionally, in 2018, they deployed wiper malware against a bank in Chile that crashed thousands of computers and servers to distract from efforts to send fraudulent messages from the bank's compromised SWIFT terminal.
https://us-cert.cisa.gov/ncas/alerts/aa20-239a

(cisp-id:8547) Aug 25, 2020
Threat Intelligence Report: Lazarus Group Campaign Targeting the Cryptocurrency Vertical.
In 2019, F-Secure uncovered technical details on Lazarus Group's1 modus operandi during an investigation of an attack on an organization in the cryptocurrency vertical, hereafter referred to as "the target". Lazarus Group's interests reportedly align with those of the government of the Democratic People's Republic of Korea (DPRK). According to a 2019 UN report2 Lazarus Group has been targeting organizations in the cryptocurrency vertical since at least 2017.
https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf

(cisp-id:8555) Aug 24, 2020
Lifting the veil on DeathStalker, a mercenary triumvirate.
Kaspersky blog published State-sponsored threat actors and sophisticated attacks of DeathStalker: a unique threat group that appears to target law firms and companies in the financial sector (although we've occasionally seen them in other verticals as well). This actor isn't motivated by financial gain. They don't deploy ransomware, steal payment information to resell it, or engage in any type of activity commonly associated with the cybercrime underworld. DeathStalker first came to our attention through a PowerShell-based implant called Powersing. By unraveling this thread, we were able to identify activities dating back to 2018, and possibly even 2012.
https://securelist.com/deathstalker-mercenary-triumvirate/98177/

(cisp-id:8556) Aug 24, 2020
Top exploits used by ransomware gangs are VPN bugs, but RDP still reigns supreme.
While some ransomware groups have heavily targeted Citrix and Pulse Secure VPNs to breach corporate networks in H1 2020, most ransomware attacks take place because of compromised RDP endpoints. The top three most popular intrusion methods include unsecured RDP endpoints, email phishing, and the exploitation of corporate VPN appliances.
https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/#ftag=RSSbaffb68

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



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