Weekly Intelligence Summary

Jul 17, 2020 (TLP: WHITE)

In the spotlight this week: ***#APT & #State-sponsored***

- Twitter Support said: we believe to be a coordinated social engineering attack by people who successfully targeted ***#some*** of our employees with access to internal systems and tools. We know they used this access to take control of many highly-visible accounts …. So ***#morethan1***, not ***#InsiderThreat***? Can they read ***#DM***?
- Phone of top Catalan politician 'targeted by government-grade spyware' ~= ***#State-sponsored*** spyware? Any chance ***NSO Group's #Pegasus*** has been deployed in HK?
- Secret Trump order gives CIA more powers to launch cyberattacks --> in APAC? If yes, who will be targeted?
- Checkpoint said: ***#SIGRed*** (CVE-2020-1350) is a ***#wormable***, critical vulnerability (CVSS base score of 10.0) in the Windows DNS server that affects Windows Server
- OK, I am going to buy Trola's new book: Hunting Cyber Criminal ***#DataViper***
- The UK's NCSC* and Canada's CSE assess that APT29 is a cyber espionage group, almost certainly part of the Russian intelligence services. The US's NSA agrees with this attribution and the details provided in a report on APT29 (Using ***#WellMess*** and ***#WellMail***, targets COVID-19 vaccine development.

*https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

(cisp-id:8293) Jul 16, 2020
Hackers Convinced ***Twitter Employee*** to Help Them Hijack Accounts.
A Twitter insider was responsible for a wave of high-profile account takeovers. On Wednesday, a spike of high-profile accounts including those of Joe Biden, Elon Musk, Bill Gates, Barack Obama, Uber, and Apple tweeted cryptocurrency scams in an apparent hack. "We used a rep that literally done all the work for us," one of the sources told Motherboard. The second source added they paid the Twitter insider. Vice granted the sources anonymity to speak candidly about a security incident. The accounts were taken overusing an internal tool at Twitter, according to the sources, as well as screenshots of the tool obtained by Motherboard. One of the screenshots shows the panel and the account of Binance.
https://www.vice.com/en_us/article/jgxd3d/twitter-insider-access-panel-account-hacks-biden-uber-bezos
https://krebsonsecurity.com/2020/07/whos-behind-wednesdays-epic-twitter-hack/

(cisp-id:8300) Jul 15, 2020
Phone of top Catalan politician 'targeted by ***government-grade spyware'***.
Sergi Miquel was in Belgium when targeted. The targeting of a telephone with NSO's spyware in Belgium, another EU country clearly indicates the need for an urgent European Union examination of the circumstances of these cases. Cases that was confirmed thus far were all used same technique, leveraging missed video calls from @whatsapp in April-May 2019. WhatsApp blocked the targeting shortly after it was discovered by CitizenLab.
https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware
https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

(cisp-id:8299) Jul 15, 2020
CIA most likely behind APT34 and FSB hacks and data dumps.

Secret Trump order gives CIA more powers to launch cyberattacks. Unlike previous presidential findings that have focused on a specific foreign policy objective or outcome — such as preventing Iran from becoming a nuclear power — this directive, driven by the National Security Council and crafted by the CIA, focuses more broadly on a capability covert action in cyberspace. Yahoo News reporters believe the CIA's new powers and modus operandi link it to a series of hack-and-dump incidents that took place primarily in 2019, such as: (a) Publishing hacking tools (malware) from ***APT34 on Telegram***, (b) Doxing IRGC intelligence agents on Telegram, (c) Dumping details about 15 million payment cards from three Iranian banks linked to Iran's IRGC, (d) Hacking two contractors that provide cyber-weapons and surveillance solutions for Russia's FSB intelligence agency.
https://www.zdnet.com/article/report-cia-most-likely-behind-apt34-and-fsb-hacks-and-data-dumps/
https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

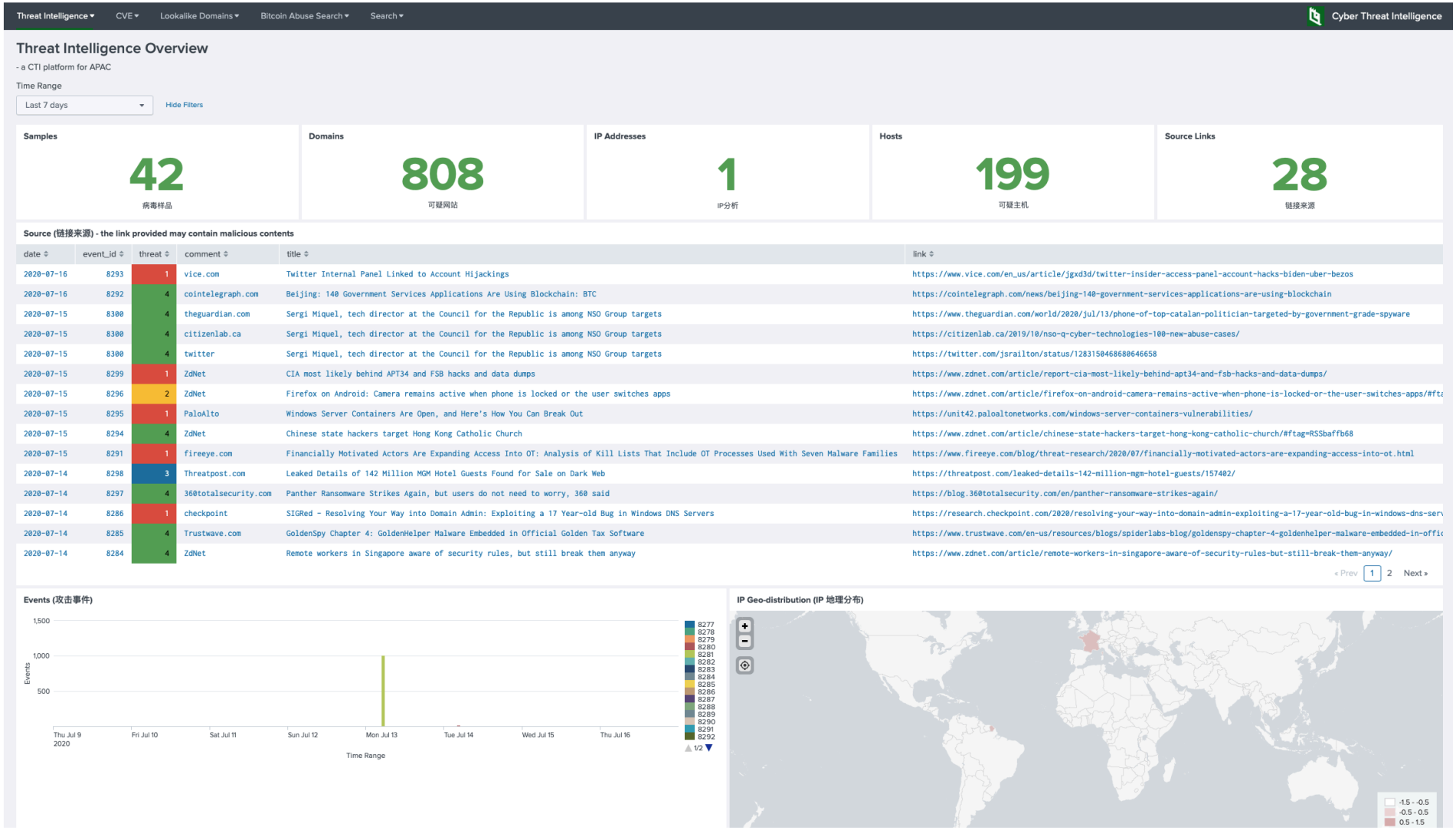
(cisp-id:8296) Jul 15, 2020
Firefox on Android: Camera remains active when phone is locked or the user switches apps.
The bug was first spotted and reported to Mozilla a year ago, in July 2019, by an employee of video delivery platform Appear TV. The bug manifests when users chose to video stream from a website loaded in Firefox instead of a native app. "This bug [fix] aims to address this by defaulting to audio-only when the screen is locked," Mozilla said. "[The fix] is scheduled for release at the platform-level this ***October***, and for consumers shortly after."
https://www.zdnet.com/article/firefox-on-android-camera-remains-active-when-phone-is-locked-or-the-user-switches-apps/#ftag=RSSbaffb68

(cisp-id:8286) Jul 14, 2020
SIGRed –Exploiting a 17 Year-old Bug in Windows DNS Servers.
SIGRed (CVE-2020-1350) is a ***#wormable,*** critical vulnerability (CVSS base score of 10.0) in the Windows DNS server that affects Windows Server versions 2003 to 2019 and can be triggered by a malicious DNS response. As the service is running in elevated privileges (SYSTEM), if exploited successfully, an attacker is granted Domain Administrator rights, effectively compromising the entire corporate infrastructure.
https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/cisa-releases-emergency-directive-critical-microsoft-vulnerability

(cisp-id:8290) Jul 14, 2020
Hacker breaches security firm in act of revenge.
A hacker claims to have breached the backend servers belonging to a US cyber-security firm and stolen information from the company's "data leak detection" service. The databases have been collected inside ***#DataViper***, a data leak monitoring service managed by Vinny Troia, the security researcher behind Night Lion Security, a US-based cyber-security firm.
https://www.zdnet.com/article/hacker-breaches-security-firm-in-act-of-revenge/#ftag=RSSbaffb68

(cisp-id:8289) Jul 13, 2020
蛇从暗黑中袭来——响尾蛇(SideWinder) APT 组织 2020 年上半年活动总结报告.
响尾蛇(又称***#SideWinder***，T-APT-04)是一个背景可能来源于***印度的 APT 组织***，该组织此前已对巴基斯坦和东南亚各国发起过多次攻击， 该组织以窃取政府， 能源， 军事， 矿产等领域的机密信息为主要目的。在今年年初的时候，Gcow 安全团队的追影小组发布了关于 SiderWinder APT 组织的报告——《游荡于中巴两国的魅影——响尾蛇(SideWinder) APT 组织针对巴基斯坦最近的活动以及 2019 年该组织的活动总结》。本小组也一直对该小组的活动加以跟踪。在 2020 上半年的活动中该组织的主要目标依然是巴基斯坦，中国，孟加拉国以及其他的东南亚国家，其主要是集中在政府，军事领域。
https://www.anquanke.com/post/id/210404

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



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