Weekly Intelligence Summary

Aug 14, 2020 (TLP: WHITE)

In the spotlight this week:

- NSA and FBI Expose T=the Russian General Staff Main Intelligence Directorate (***GRU***) 85th Main Special Service Center (GTsSS) military unit 26165, whose activity is sometimes identified by the private sector as ***Fancy Bear***, Strontium, or ***APT 28***, is deploying malware called ***Drovorub***, designed for Linux systems as part of its cyber espionage operations.According to @DAlperovitch, @NSACyber translates the malware name “Drovorub” as “woodcutter” wrong because “Drova” is slang in Russian for “drivers”, as in kernel drivers. So the name likely was chosen to ***mean “(security) driver slayer"***
- Google Project Zero researcher who discovered the elevation of privilege flaw (***CVE-2020-1509***) in the Windows Local Security Authority Subsystem Service (***LSASS***) warn that Microsoft did not properly address it.
- Microsoft August 2020 ***Patch Tuesday*** fixes 120 vulnerabilities, two zero-days. Among the 120 vulnerabilities fixed this month, 17 bugs have received the highest severity rating of "Critical," and there are also two zero-days — vulnerabilities that have been exploited by hackers before Microsoft was able to provide today's patches. Perhaps the most “elite” vulnerability addressed this month earned the distinction of being named ***CVE-2020-1337***, and refers to a security hole in the Windows Print Spooler service that could allow an attacker or malware to escalate their privileges on a system if they were already logged on as a regular (non-administrator) user. (source: https://krebsonsecurity.com)
- 安天 CERT 发现一批针对我国政府多封邮件的发件 IP 位于中国台湾地区，邮件字体的格式为台湾地区特有的“新細明體”，这些痕迹意味这批活动背后的攻击者可能来自中国台湾。

(cisp-id:8501) Aug 13, 2020

NSA and FBI Expose Russian Previously Undisclosed Malware “Drovorub” in Cybersecurity Advisory. The National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) released a new Cybersecurity Advisory about previously undisclosed Russian malware. The Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165, whose activity is sometimes identified by the private sector as Fancy Bear, Strontium, or APT 28, is deploying malware called Drovorub, designed for Linux systems as part of its cyber espionage operations.

https://www.nsa.gov/news-features/press-room/Article/2311407/nsa-and-fbi-expose-russian-previously-undisclosed-malware-drovorub-in-cybersecu/

(cisp-id:8498) Aug 13, 2020

Microsoft did not properly address an elevation of privilege flaw (CVE-2020-1509) in the Windows Local Security Authority Subsystem Service (LSASS).

Google Project Zero researcher who discovered the elevation of privilege flaw (CVE-2020-1509) in the Windows Local Security Authority Subsystem Service (LSASS) warn that Microsoft did not properly address it. “An elevation of privilege vulnerability exists in the Local Security Authority Subsystem Service (LSASS) when an authenticated attacker sends a specially crafted authentication request. A remote attacker who successfully exploited this vulnerability could cause an elevation of privilege on the target system’s LSASS service.” reads the Microsoft’s advisory. “The security update addresses the vulnerability by changing the way that LSASS handles specially crafted authentication requests.”

https://securityaffairs.co/wordpress/107102/hacking/cve-2020-1509-lsass-flaw.html

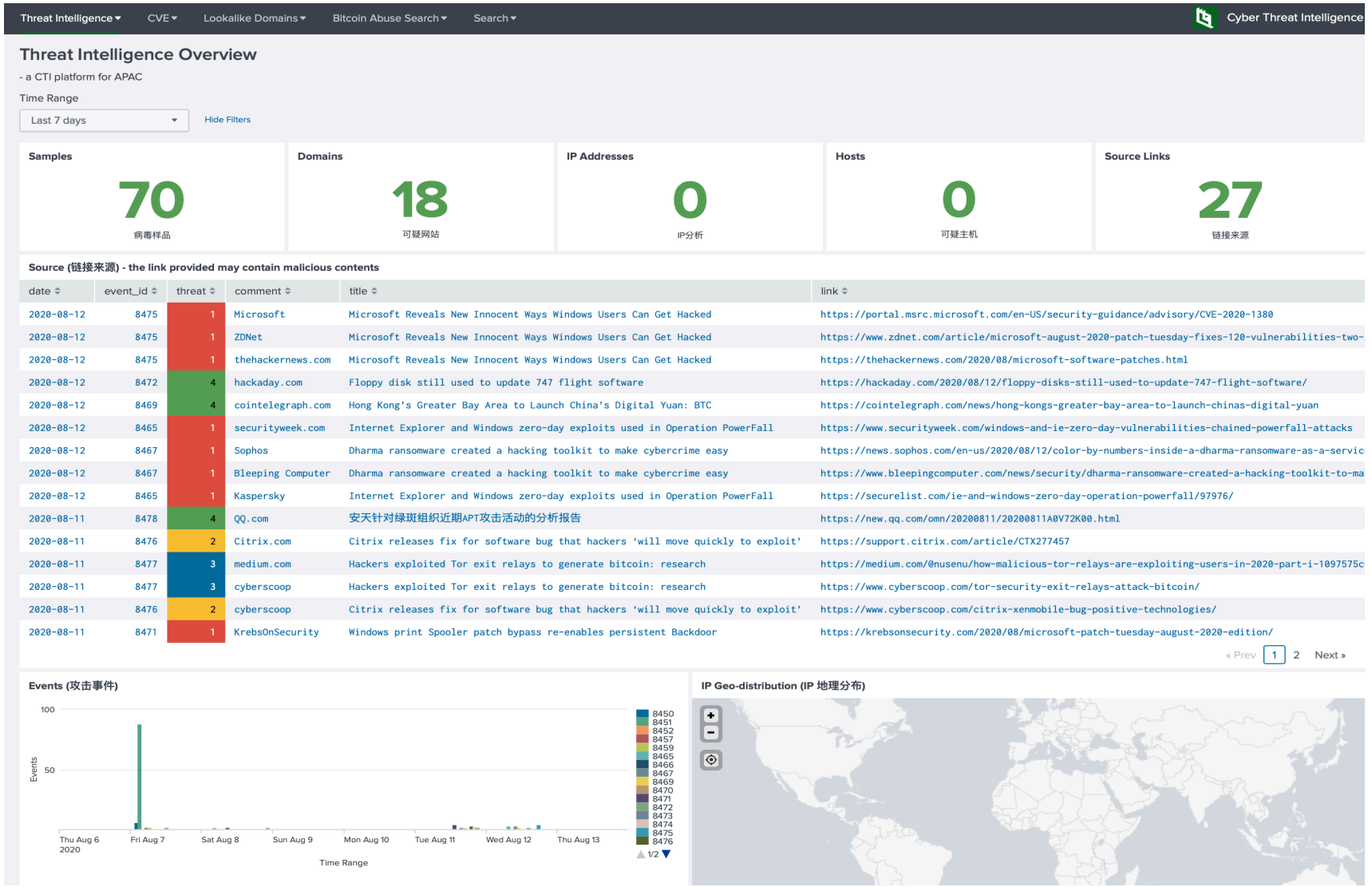
(cisp-id:8492) Aug 13, 2020
An advanced group specializing in corporate espionage is on a hacking spree.
A Russian-speaking hacking group specializing in corporate espionage has carried out 26 campaigns since 2018 in attempts to steal vast amounts of data from the private sector, according to new findings. The hacking group, dubbed RedCurl, stole confidential corporate documents including contracts, financial documents, employee records and legal records, according to research published Thursday by the security firm Group-IB, which has offices in Moscow in Singapore. Victims spanned a range of industries — including construction, finance, retail and law — with headquarters in Russia, Ukraine, the U.K., Canada, Germany and Norway. Group-IB did not speculate on where RedCurl is based. That the group speaks in Russian, as researchers noted, does not indicate RedCurl is a Russian-based hacking group.
https://www.cyberscoop.com/redcurl-groupib-russian-hacking-espionage/
https://www.group-ib.com/resources/threat-research/red-curl.html

(cisp-id:8465) Aug 12, 2020
Internet Explorer zero-day exploits (CVE-2020-1380) used in Operation PowerFall.
In May 2020, Kaspersky technologies prevented an attack on a South Korean company, their analysis revealed that the attack used a previously unknown full chain that consisted of two zero-day exploits: a remote code execution exploit for Internet Explorer and an elevation of privilege exploit for Windows. They tested the full chain attack (used in Operation WizardOpium) on system with Internet Explorer 11 and Windows 10 build 18363 x64). They are calling this and related attacks 'Operation PowerFall'. Currently, we are unable to establish a definitive link with any known threat actors, but due to similarities with previously discovered exploits, we believe that DarkHotel may be behind this attack. Kaspersky products detect Operation PowerFall attacks with verdict PDM:Exploit.Win32.Generic.
https://securelist.com/ie-and-windows-zero-day-operation-powerfall/97976/
https://www.securityweek.com/windows-and-ie-zero-day-vulnerabilities-chained-powerfall-attacks

(cisp-id:8478) Aug 11, 2020
安天针对绿斑组织近期 APT 攻击活动的分析报告.
近期，安天 CERT 在梳理安全事件时，发现一批针对我国政府、科研等机构的鱼叉邮件攻击活动。经分析，这批攻击活动的手法和代码与 2019 年的绿斑组织活动基本一致。鱼叉邮件中多数为钓鱼链接，目的是钓取目标邮箱账户和密码信息，钓取成功后转向一个下载页面，下载到的均为看似来自官方的正常文件。另有少数邮件带有压缩包附件，里面包含的恶意文件负责释放后续的窃密程序。我们基于已掌握的数据进行汇总、梳理、分析并形成本篇报告。 通过溯源分析发现，存在部分邮件、文档的正文和钓鱼网页的源码包含有繁体中文字，多封邮件的发件 IP 位于中国台湾地区，邮件字体的格式为台湾地区特有的"新細明體"，这些痕迹意味这批活动背后的攻击者可能来自中国台湾。
https://new.qq.com/omn/20200811/20200811A0V72K00.html

(cisp-id:8476) Aug 11, 2020
Citrix releases fix for software bug that hackers 'will move quickly to exploit'.
A newly revealed set of vulnerabilities in popular software made by Citrix, whose clients include Fortune 500 companies, could let hackers who exploit the bugs gain control of a mobile server and steal sensitive data. Citrix's CISO Fermin wrote in a blog: "While there are no known exploits as of this writing, we do anticipate malicious actors will move quickly to exploit," The bugs are in a software product known as Citrix Endpoint Management or XenMobile, which allows clients to remotely connect to corporate networks with their mobile devices.
https://www.cyberscoop.com/citrix-xenmobile-bug-positive-technologies/
https://support.citrix.com/article/CTX277457

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



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