Weekly Intelligence Summary

May 28, 2020 (TLP: WHITE)

In the spotlight this week:

- Fortune 500 company NTT discloses security breach. NTT says hackers gained access to its internal network and stole information on 621 customers from NTT Communications. The attack is believed to have originated from an NTT base in Singapore. #NTT-Singapore 😨
- Based on a survey Sophos disclosed their insight into threat actor of #Netwalker ransomware and tools. #Do-the-IR-Investigation-with-Recovery
- Christian Beek disclosed in his findings - This short 'tipper' will discuss Kazuar and a universal love for Mark Russinovich's SysInternal Tools. #SysInTURLA #Sysinternaltools 😨
- Kaspersky's SecureList disclosed the zero-day exploits of Operation WizardOpium. #GoogleChromeremotecodeexecution

(cisp-id:8043) May 28, 2020

The hack took place on May 7, and NTT says it became of the intrusion four days later, on May 11. NTT says hackers gained access to its internal network and stole information on 621 customers from its communications subsidiary, NTT Communications, the largest telecommunications company in Japan, and one of the biggest worldwide. The company says hackers breached several layers of its IT infrastructure and reached an internal Active Directory (AD in the graph below) to steal and upload data to a remote serve. The attack is believed to have originated from an NTT base in Singapore, the company said today.
https://www.zdnet.com/article/fortune-500-company-ntt-discloses-security-breach/

(cisp-id:8044) May 28, 2020

The Netwalker threat actor has struck a diverse set of targets based in the US, Australia, and western Europe, and recent reports indicate the attackers have decided to concentrate their efforts targeting large organizations, rather than individuals. The tooling we uncovered supports this hypothesis, as it includes programs intended to capture Domain Administrator credentials from an enterprise network, combined with orchestration tools that employ software distribution served from a Domain Controller, common in enterprise networks but rare among home users. Some of the scripts and exploit tools were copied directly from Github repositories. Several of the tools are freely-available Windows utilities, such as Amplia Security's Windows Credential Editor. Hints they take advantage of well-known, heavily publicized vulnerabilities in widely used, outdated server software (such as Tomcat or Weblogic) or weak RDP passwords.
https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/

(cisp-id:8045) May 27, 2020

Today's threat actor of choice is one of my favorites, Turla (namesake of this blog). This prolific threat actor relies on a variety of toolkits (including Skipper, IcedCoffee, KopiLuwak among others). In the past two weeks alone, two distinct clusters of their activities piqued the interest of multiple research groups (see: Leonardo's 'Penquin_x64' and ESET's COMrat

v4 reports), but their bag of tricks is hardly exhausted. This short 'tipper' will discuss Kazuar and a universal love for Mark Russinovich's SysInternal Tools. #SysInTURLA
https://www.epicturla.com/blog/sysinturla

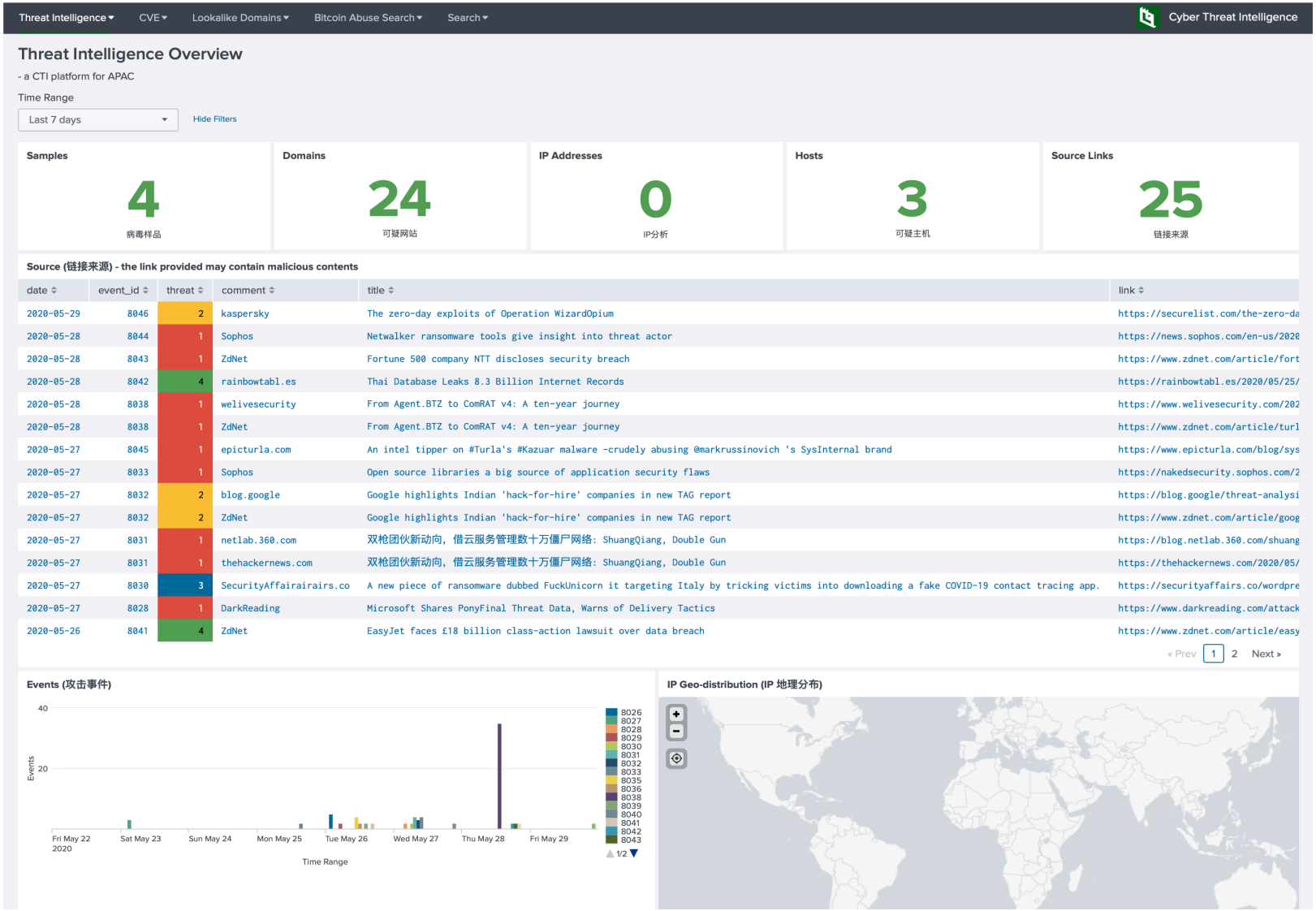
(cisp-id:8046) May 28, 2020
The zero-day exploits of Operation WizardOpium
Back in October 2019 we detected a classic watering-hole attack on a North Korea-related news site that exploited a chain of Google Chrome and Microsoft Windows zero-days. While we've already published blog posts briefly describing this operation (available here and here), in this blog post we'd like to take a deep technical dive into the exploits and vulnerabilities used in this attack.
https://securelist.com/the-zero-day-exploits-of-operation-wizardopium/97086/

(cisp-id:8038) May 26, 2020
From Agent.BTZ to ComRAT v4: A ten-year journey: ESET researchers have found a new version of one of the oldest malware families run by the Turla group, ComRAT. Turla, also known as Snake, is an infamous espionage group that has been active for more than ten years. We have previously described many campaigns attributed to this group. ComRAT, also known as Agent.BTZ and to its developers as Chinch, is a Remote Access Trojan (RAT) that became infamous after its use in a breach of the US military in 2008. The first version of this malware, likely released in 2007, exhibited worm capabilities by spreading through removable drives. From 2007 to 2012, two new major versions of the RAT were released. Interestingly, both employed the well-known Turla XOR key.
https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/

(cisp-id:8032) May 27, 2020
Chinese Researchers Disrupt Malware Attack That Infected Thousands of PCs
Chinese security firm Qihoo 360 Netlab said it partnered with tech giant Baidu to disrupt a malware botnet infecting over hundreds of thousands of systems.
The botnet was traced back to a group it calls ShuangQiang (also called Double Gun), which has been behind several attacks since 2017 aimed at compromising Windows computers with MBR and VBR bootkits and installing malicious drivers for financial gain and hijack web traffic to e-commerce sites.
https://blog.netlab.360.com/shuang-qiang-zui-xin-huo-dong-fen-xi-bao-gao-nei-bu-bao-gao-ban/

(cisp-id:8037) May 13, 2020
Nigeria's anti-corruption agency, the Economic and Financial Crimes Commission (EFCC), has arrested two Chinese nationals for allegedly offering a $250,000 (£203,000) bribe in local currency to one of its senior officials. The alleged bribe was said to be an attempt to scuttle an investigation into multi-million-dollar corruption allegations involving a Chinese construction company in Nigeria where the two suspects work The EFCC said it was investigating alleged corruption involving about $130m (£105m) in contracts for roads and water projects. The contracts were awarded by Nigeria's Zamfara state government to China Zhonghoa Nigeria Limited between 2012 and 2019.
https://www.businessghana.com/site/news/Politics/212855/Chinese-nationals-arrested-with-$250,000-bribe

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



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