Weekly Intelligence Summary

May 12, 2020 (TLP: WHITE)

In the spotlight this week:

- Winnti Group is brought to our attention again by Welivesecurity. Trojanize game executables was found on gaming platforms. Case found led to a supply-chain-attack.
- SecureWorks CTU Researchers Publish Threat Group. APT41→Bronze Atlas, APT4→ Bronze Edison, APT30→Bronze Geneva, APT34→Cobalt Edgewater, CrimsonRAT→CopperFieldStone
- Hundreds of thousands of QNAP devices vulnerable to remote takeover attacks. In a Medium blog post on May 19, Huang published in-depth technical details about three of four vulnerabilities he found in the QNAP devices. Three impact the Photo Station app, while a fourth impacts the QTS file manager app. #Only3AreDisclosed.
- FBI warns (May 6) about attacks on #Magento online stores via old plugin vulnerability. IOCs associated with e-skimming threat #Magecart or #FIN7. It is a three-year-old (CVE-2017-7391) vulnerability are still being used by hackers. 360.com[1] has a network-wide DNS malicious domain analysis system with the 10%+ total-DNS traffic coverage in China. #total-dns-in-CHINA.

[1] https://blog.netlab.360.com/ongoing-credit-card-data-leak-continues/

(cisp-id:8005) May 20, 2020

No “Game over” for the Winnti Group.

In February 2020, we discovered a new, modular backdoor, which we named PipeMon. Persisting as a Print Processor, it was used by the Winnti Group against several video gaming companies that are based in South Korea and Taiwan and develop MMO (Massively Multiplayer Online) games. Video games developed by these companies are available on popular gaming platforms and have thousands of simultaneous players. In at least one case, the malware operators compromised a victim’s build system, which could have led to a supply-chain attack, allowing the attackers to trojanize game executables. In another case, the game servers were compromised, which could have allowed the attackers to, for example, manipulate in-game currencies for financial gain.

https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/

(cisp-id:8002) May 20, 2020

Counter Threat Unit Researchers Publish Threat Group Definitions.

SecureWorks publish these records, given that they are not full actor profiles and there are no infrastructure indicators? You might be asking yourself if this is just a marketing exercise. I assure you that it isn’t. Yes, we want to make the names available to those who care. But the decision was driven by a desire to help establish a shared language for discussing these groups. We often receive requests for a unified “Rosetta Stone” that relates our Threat Groups to others. Others in the industry have done great work in that area, but we wanted to complement their work and also provide a dynamic feed of our mappings. As aficionados of “master data management” know, documents are problematic. Documents from a single data source are stale as soon as they are created. To address this issue, the website will continuously synchronise with our Threat Intelligence Management System to convey the most current information

https://www.secureworks.com/research/threat-profiles

(cisp-id:7999) May 19, 2020

QNAP Pre-Auth Root RCE Affecting ~450K Devices on the Internet.

In 2019, I discovered multiple vulnerabilities in QNAP PhotoStation and CGI programs. These vulnerabilities can be chained into a pre-auth root RCE. All QNAP NAS models are vulnerable, and there are ~312K vulnerable QNAS NAS instances on the Internet (statistical prediction). These vulnerabilities have been responsibly reported, fixed and assigned CVE-2019–7192 (CVSS 9.8), CVE-2019–7193 (CVSS 9.8), CVE-2019–7194 (CVSS 9.8), CVE-2019–7195 (CVSS 9.8). This article is the first public disclosure, but only 3 of the vulnerabilities are disclosed, because they're enough to achieve pre-auth root RCE.
https://medium.com/bugbountywriteup/qnap-pre-auth-root-rce-affecting-450k-devices-on-the-internet-d55488d28a05

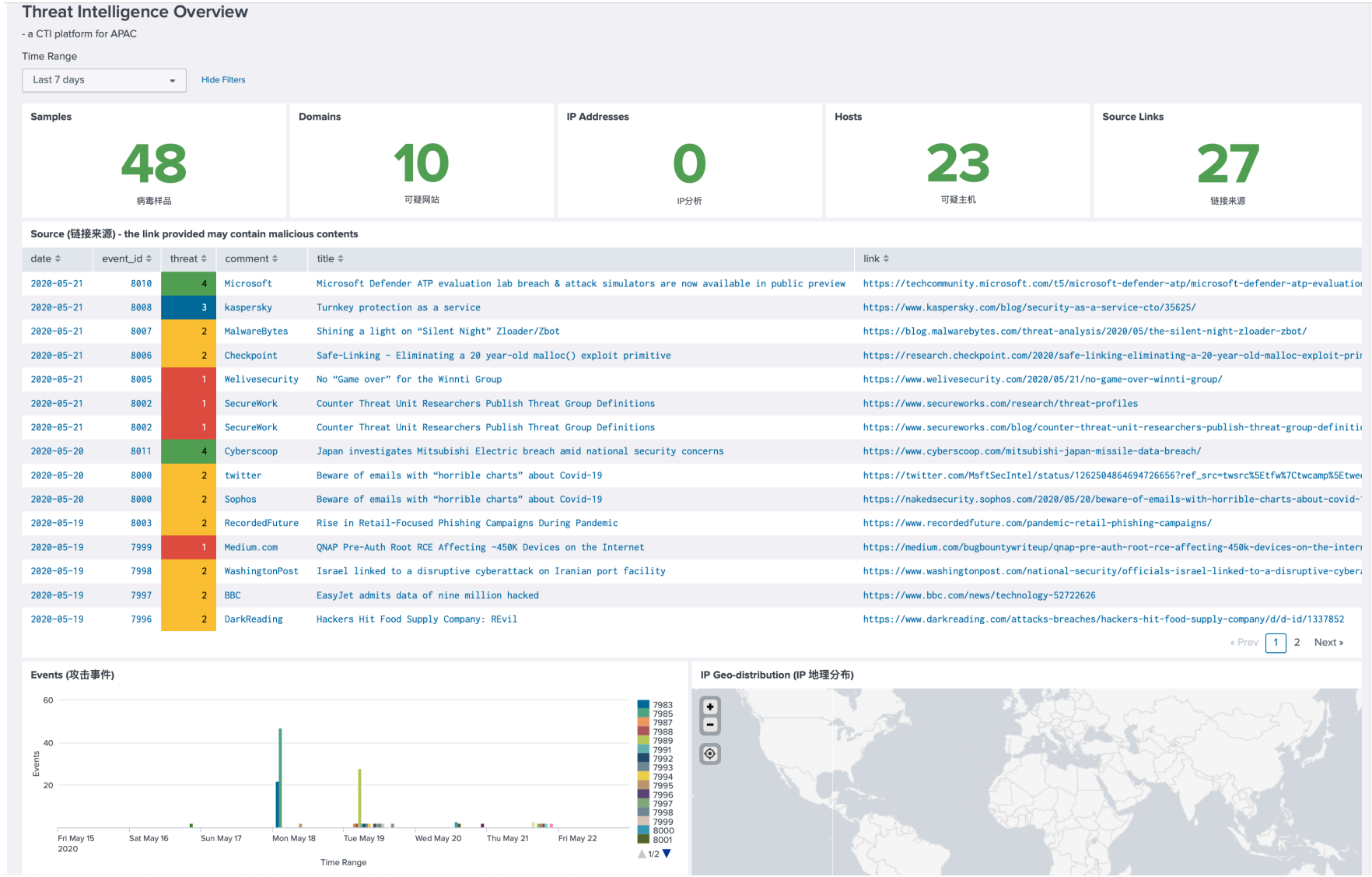
(cisp-id:7997) May 19, 2020
EasyJet admits data of nine million hacked.
EasyJet has admitted that a "highly sophisticated cyber-attack" has affected approximately nine million customers. It said email addresses and travel details had been stolen and that 2,208 customers had also had their credit card details "accessed".
The firm has informed the UK's Information Commissioner's Office while it investigates the breach. EasyJet first became aware of the attack in January. #GDPR
https://www.bbc.com/news/technology-52722626

(cisp-id:7994) May 19, 2020
FBI warns about attacks on Magento online stores via old plugin vulnerability.
The FBI says hackers are exploiting a three-year-old (CVE-2017-7391) vulnerability in a #Magento plugin to take over online stores and plant a malicious script that records and steals buyers' payment card data. The vulnerability is a cross-site scripting (XSS) bug that allows the attacker to plant malicious code inside an online store's HTML code.
blog.netlab.360.com reports of this server being used in web skimmer attacks goes back as far as May 2019. #DNSMon identified one malicious site magento-analytics[.]com stealing credit card info from online shopping users by injecting JS on E-commerce sites, soon after our blog, the original site went offline.
https://www.zdnet.com/article/fbi-warns-about-attacks-on-magento-online-stores-via-old-plugin-vulnerability/
https://www.documentcloud.org/documents/6893935-FBI-Flash-Alert-MU-000127-MW.html

(cisp-id:7998) May 19, 2020
Israel linked to a disruptive cyberattack on Iranian port facility.
On May 9, shipping traffic at Iran's bustling Shahid Rajaee port terminal came to an abrupt and inexplicable halt. Computers that regulate the flow of vessels, trucks and goods all crashed at once, -creating massive backups on waterways and roads leading to the facility. After waiting a day, Iranian officials acknowledged that an unknown foreign hacker had briefly knocked the port's computers off-line.
https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

(cisp-id:7987) May 19, 2020
REvil to Auction Stolen Madonna Data: ransomware. A threat group that claims to have stolen nearly a terabyte of data from a prominent entertainment law firm has said it will put sensitive information relating to Madonna up for auction. REvil allegedly made off with 756GB of data from New York lawyers Grubman Shire Meiselas & Sack in a ransomware attack earlier this month.
https://www.infosecurity-magazine.com/news/revil-to-auction-stolen-madonna/

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



Threat Intelligence Overview

- a CTI platform for APAC

Time Range

Last 7 days Hide Filters

Samples	Domains	IP Addresses	Hosts	Source Links
48	10	0	23	27
病毒样品	可疑网站	IP分析	可疑主机	链接来源

Source (链接来源) - the link provided may contain malicious contents

date	event_id	threat	comment	title	link
2020-05-21	8010	4	Microsoft	Microsoft Defender ATP evaluation lab breach & attack simulators are now available in public preview	https://techcommunity.microsoft.com/t5/microsoft-defender-atp/microsoft-defender-atp-evaluatio
2020-05-21	8008	3	kaspersky	Turnkey protection as a service	https://www.kaspersky.com/blog/security-as-a-service-cto/35625/
2020-05-21	8007	2	MalwareBytes	Shining a light on “Silent Night” Zloader/Zbot	https://blog.malwarebytes.com/threat-analysis/2020/05/the-silent-night-zloader-zbot/
2020-05-21	8006	2	Checkpoint	Safe-Linking - Eliminating a 20 year-old malloc() exploit primitive	https://research.checkpoint.com/2020/safe-linking-eliminating-a-20-year-old-malloc-exploit-pri
2020-05-21	8005	1	Welivesecurity	No “Game over” for the Winnti Group	https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/
2020-05-21	8002	1	SecureWork	Counter Threat Unit Researchers Publish Threat Group Definitions	https://www.secureworks.com/research/threat-profiles
2020-05-21	8002	1	SecureWork	Counter Threat Unit Researchers Publish Threat Group Definitions	https://www.secureworks.com/blog/counter-threat-unit-researchers-publish-threat-group-definiti
2020-05-20	8011	4	Cyberscoop	Japan investigates Mitsubishi Electric breach amid national security concerns	https://www.cyberscoop.com/mitsubishi-japan-missile-data-breach/
2020-05-20	8000	2	twitter	Beware of emails with “horrible charts” about Covid-19	https://twitter.com/MsftSecIntel/status/1262504864694726656?ref_src=twsrc%5Etfw%7Ctwcamp%5Etwe
2020-05-20	8000	2	Sophos	Beware of emails with “horrible charts” about Covid-19	https://nakedsecurity.sophos.com/2020/05/20/beware-of-emails-with-horrible-charts-about-covid-
2020-05-19	8003	2	RecordedFuture	Rise in Retail-Focused Phishing Campaigns During Pandemic	https://www.recordedfuture.com/pandemic-retail-phishing-campaigns/
2020-05-19	7999	1	Medium.com	QNAP Pre-Auth Root RCE Affecting ~450K Devices on the Internet	https://medium.com/bugbountywriteup/qnap-pre-auth-root-rce-affecting-450k-devices-on-the-inter
2020-05-19	7998	2	WashingtonPost	Israel linked to a disruptive cyberattack on Iranian port facility	https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyber
2020-05-19	7997	2	BBC	EasyJet admits data of nine million hacked	https://www.bbc.com/news/technology-52722626
2020-05-19	7996	2	DarkReading	Hackers Hit Food Supply Company: REvil	https://www.darkreading.com/attacks-breaches/hackers-hit-food-supply-company/d/d-id/1337852

« Prev 1 2 Next »

Events (攻击事件)

IP Geo-distribution (IP 地理分布)

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