Radware Cybersecurity Alert
Australian Cyberattacks
June 22, 2020

On June 19, 2020, Australia's Prime Minister Scott Morrison warned Australian businesses and governments about a sustained cyberattack. Morrison said the Australian organizations were currently being targeted by a sophisticated foreign "state-based" attacker and emphasized the attacks "hadn't just started" but were ongoing and constant threats to Australia. The accumulation of attacks required a firm warning to the government and private sectors to take affirmative action to protect their valuable business and personal data.

> *"This activity is targeting Australian organizations across a range of sectors, including all levels of government, industry, political organizations, education, health, essential service providers and operators of other critical infrastructure," Morrison said. "We know it is a sophisticated state-based cyber actor because of the scale and nature of the targeting and the tradecraft used."*

The government's Australian Cyber Security Centre (ACSC) published an advisory note[1] on June 18 with details of the tactics, techniques, and procedures (TTPs) identified during their investigation of the cyber campaign targeting Australian networks. Morrison said the government would not take formal steps of publicly naming a state behind the attacks, despite blaming a "sophisticated state actor."

> *The announcement and the increase of malicious activity comes at a time when relations between Australia and China have grown tense and significantly worsened after Australia echoed the US in calling for an inquiry into the origins of the coronavirus. China has since imposed tariffs on Australian barley, stopped beef imparts and warned Chinese citizens and students about the risks of travelling to Australia for tourism or education because of racist incidents. Morrison recently said he would not give in to "coercion" from Beijing. Australia's leadership has chosen a moment when its relationship with its powerful trading partner is at an all-time low to announce publicly that it is under cyberattack from a powerful state.*
> *-- Shaimaa Khalil, BBC News Australia correspondent* [2]

Attack Methods

The attacks identified by the ACSC are based on existing and known exploits, leveraging publicly accessible proof of concept code, web shells and other open source tools. The top vulnerabilities referenced by the ACSC are threats that have been alerted on in the past few months by US and UK agencies:

- Telerik UI vulnerability
- Microsoft Internet Information Server deserialization vulnerability
- 2019 SharePoint vulnerability
- 2019 Citrix vulnerability

[1] ACSC Advisory 2020-008 (https://www.cyber.gov.au/threats/advisory-2020-008-copy-paste-compromises-tactics-techniques-and-procedures-used-target-multiple-australian-networks)
[2] BBC - Australia cyberattacks: PM Morrison warns of 'sophisticated' state hack (https://www.bbc.com/news/world-australia-46096768)

The actor or actors have the capability to quickly leverage new proof-of-concepts and to target networks of interest looking for vulnerable services. The actor or actors are potentially maintaining a list of public-facing services and targets to quickly conduct reconnaissance and exploitation.

The ACSC identified several spear phishing techniques which have taken the form of:

- Links to fake websites for credential harvesting
- Email with malware attachments are links to download malware infected documents
- Links to grant Office 365 OAuth tokens to the malicious actors
- Leverage email tracking services to lure clickthrough events

Once the actor has established access to the victim's network, the actor will use different open source tools to establish persistence and to interact with the network. One of the persistence tactics is the migration to legitimate remote access by leveraging stolen credentials. This means that once compromised, even when all malicious files are cleaned from the network and vulnerabilities in the victim's infrastructure are fixed, the actor still has persistence unless the victim resets all user accounts.

The actor is making use of compromised legitimate Australian websites as command and control servers to evade geo-based detection and blocking while rendering reputation services ineffective in blocking domains or IP addresses.

At the time of publication, there is no indication of attempts to cause disruption within the victim's network which corresponds to a tactic of intelligence gathering and stealing of sensitive data and intellectual property.

Targeted Attacks

Radware is aligned with the ACSC's observation that the actor or actors are potentially maintaining a list of public-facing services and targets. The Radware Threat Research Center maintains several honeypots in Australia, and except for a mild spike between June 7 and 8, there is no immediate indicator of increased random malicious activity in the last weeks and months (Figure 1).

Honeypots are able to register global and random activity for regions such as scans for internet facing and vulnerable services. During these 'spray-and-pray' attacks, malicious actors are opportunistically scanning the entire regional range, without exception, while trying to exploit as many targets, independent of the nature of the target.

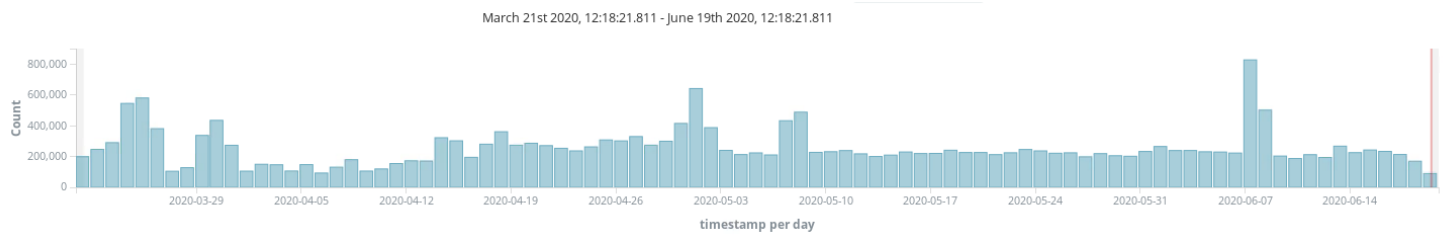

Figure 1: Total events per day in Australian sensors for last 90 days

The absence of a specific increase in activity in our Australian honeypots does not follow the increased activity reported by the ACSC which would correspond with their observation of the actors targeting a specific list or victims.

The general activity recorded by the Australian sensors (Figure 2) is not much different than the activity Radware is witnessing in other regions and is concentrated on SSH (22), RDP (3389), VNC (5900), and some of the more popular IoT device ports (8080, 8088).

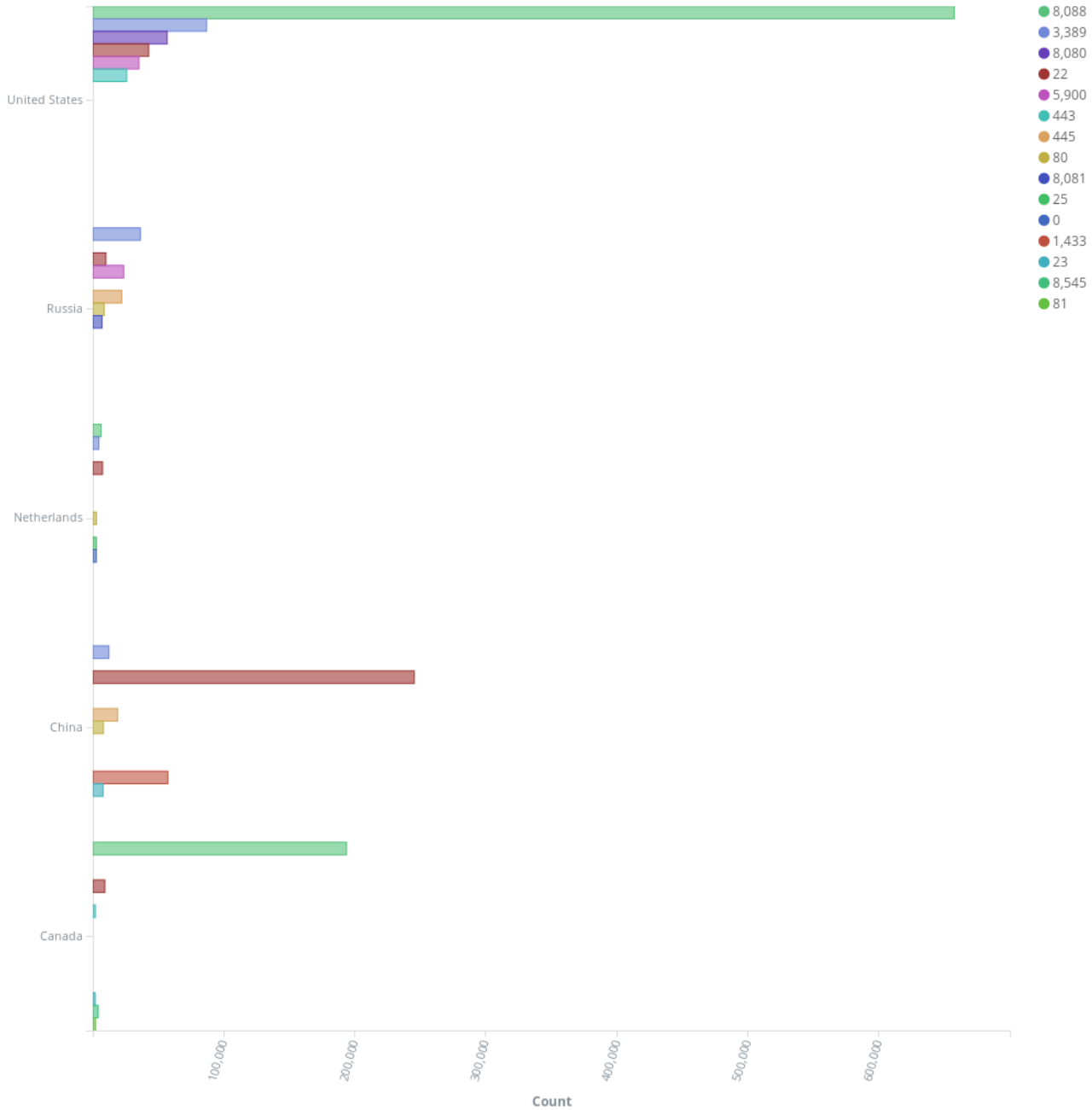

Figure 2: Top port activity for top five countries - last 30 days, Australian sensors

The top originating countries are US, Russia and China, respectively. However, an originating country does not mean the actor is operating from that country. Most actors are leveraging resources and cloud servers in other countries, a common evasion tactic that makes geo-blocking and attribution harder.

The targeting of SSH, RDP and VNC ports has been an ongoing activity, mostly indicating account takeover (either credential brute force or stuffing) attempts. The rest of the activity consists of probing for and exploiting any of the known vulnerabilities. This is a continuous level of malicious activity we have come to expect from the internet on an ongoing basis and which we typically refer to as "grey noise" due to the combination of white hat activity, scanning the internet to assess attack surfaces, and black hat activity scanning for and exploiting vulnerabilities to abuse devices.

Targets

The cyberattacks are targeting all levels of government, industry, political organizations, education, health, essential service providers and operators of other critical infrastructure

Reasons for Concern

Similar malicious activity targeting vulnerabilities in several VPN and remote access products has been reported by US and UK agencies last year and earlier this year, asking governments and organizations across the globe to keep software and appliances updated. In October 2019, the UK National Cyber Security Centre (NCSC) reported[3] investigating the exploitation, by advanced persistent threat (APT) actors, of known vulnerabilities affecting VPN products from vendors Pulse Secure, Fortinet, and Palo Alto. In January 2020, the US Cyber Security and Infrastructure Security Agency (CISA) alerted[4] unknown cyber network exploitation actors that successfully compromised numerous organizations that employed vulnerable Citrix devices.

The attack tactics reported by the ACSC will not manifest immediately through disruptions, extortion or demands. Intelligence gathering and exfiltration by nation and advanced persistent threat actors are covert operations, typically establishing persistence and expanding foothold inside the victim without raising alarms. Detecting such compromises is hard and requires full network and application visibility in all parts of the infrastructure (on-premise, private cloud, public cloud).

The lingering threat and extensive foothold, from a competing nation, inside a nation's cyber infrastructure can lead to weakened competitiveness of its economy and can be an effective weapon to orchestrate attacks on governments, critical infrastructure or businesses by causing disruption.

[3] NCSC – Vulnerabilities exploited in VPN products used worldwide (https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities)
[4] CISA Alert AA20-031A – Detecting Citrix CVE-2019-19781 (https://www.us-cert.gov/ncas/alerts/aa20-031a)

Recommendations

The ACSC has identified two key mitigations which, if implemented, will greatly reduce the risk of the identified attacks:

- Prompt patching of internet-facing software, operating systems and devices
- Use of multi-factor authentication across all remote access services, including but not limited to, web and cloud-based email and applications, collaboration platforms, VPN and remote desktop services

Given the nondisruptive nature of the threat and the volume of security events organizations must deal with, detection of malicious events that are spread over an extended period are difficult to detect without advanced algorithms and automation. When facing a sophisticated threat actor, automated detection tools will allow security teams to keep the upper hand. Automation and orchestration of an organization's security will help them to become more agile, react timelier and let them focus on what is important.

Radware web application security solutions can provide additional resilience against known and unknown vulnerabilities by securing public facing web applications and APIs with adequate positive security models. Radware's cloud workload protection for public cloud will reduce the attack surface of your cloud environments and through advanced automation and algorithms helps to detect malicious activity quickly and adequately.

There has been no reports and no indicators of an increased risk from disruptive DDoS attacks. However, customers owning Radware DefensePro solutions can leverage the anti-scanning feature to detect and block network level port scanning activity. The signature update subscription available on DefensePro allows organizations to protect against many of the known vulnerabilities and prevent compromise. Signatures can be an effective tool to virtually patch vulnerabilities, providing more time to plan and test critical updates before deploying them in production. Signatures should not be considered a replacement for the actual software fixes and updates, but it provides convenience and allows safely delaying updates to a schedule maintenance window.

IOC

The ACSC advisory, available here, does a great job at describing and documenting the indicators related to the Australia cyberattack. In addition, Radware advises to review vulnerability information to protect against multiple remote access and VPN threats as reported by the AU, US, and UK agencies:

- Citrix Application Delivery Controller (ADC) and Citrix SD-WAN WANOP appliance vulnerability CVE-2019-19781
- Palo Alto Network Security Advisory PAN-SA-2019-0020, in relation to CVE-2019-1579
- FortiGuard Security Advisories FG-IR-18-389, in relation to CVE-2018-13382; FG-IR-18-388 in relation to CVE-2018-13383; FG-IR-18-384, in relation to CVE-2018-13379;

- Pulse Secure Security Advisory SA44101, in relation to CVE-2019-11510, CVE-2019-11508, CVE-2019-11540, CVE-2019-11543, CVE-2019-11541, CVE-2019-11542, CVE-2019-11539, CVE-2019-11538, CVE-2019-11509, CVE-2019-11507

Radware Threat Intelligence

To learn about current and emerging threats and attack vectors, understand the business impact of cyberattacks, or get insights in the risks and the overall threat landscape, visit DDoSWarriors.com. Visit the new Threat Researchers Live site and join one of the upcoming live events where Radware's threat researchers discussed the latest new and threats, or watch previous editions on demand.

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and **cloud DDoS protection** for real-time **DDoS attack prevention** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cybersecurity Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed date for preemptive protection against currently active known attackers.

For further **network and application protection** measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based