Brace168

August 2020 Newsletter

IN THIS ISSUE:

Brace168 Pty Ltd

Level 2, 157 Walker St,
North Sydney

www.brace168.com

info@brace168.com

P: (02) 9136 6066

"A good programmer is someone who always looks both ways before crossing a one-way street."

- Doug Linder

Brace168 News!

New SOC Analyst!!

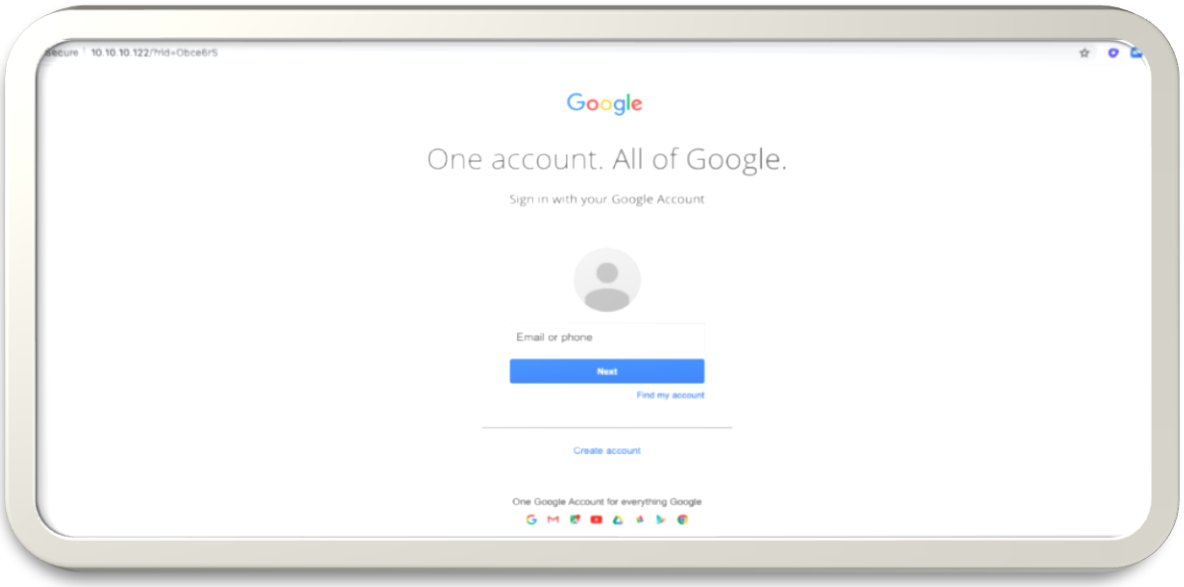
We are proud to announce that Gagan Kaur will be joining the Brace168 team! Gagan brings great experience to our Security Operations Centre (SOC) as a Security Analyst, enhancing our cyber security incident response process and threat monitoring services. Our SOC team adopts the Security Orchestration, Automation and Response (SOAR) process and next generation technologies to enhance our real-time incident and response service. Through utilising the SOAR process, Brace168 correlates different types of alerts, detects anomalies that would have otherwise been missed, and gives our SOC analysts a clear life cycle from the indicators of compromise all the way to the attack on the victim.

A little bit on Gagan:

"I am random, clumsy, compassionate, positive and passionate about cyber security. If I see someone without a smile, I never hesitate to give them one. I like food (not cooking), learning new things, deep conversations and anything comedy. My hobbies are sketching and dancing (when no one is watching!). An interesting fact about me is that I am enrolled in a part time Diploma for Mental Health with TAFE Digital cause that is another thing I am very passionate about."

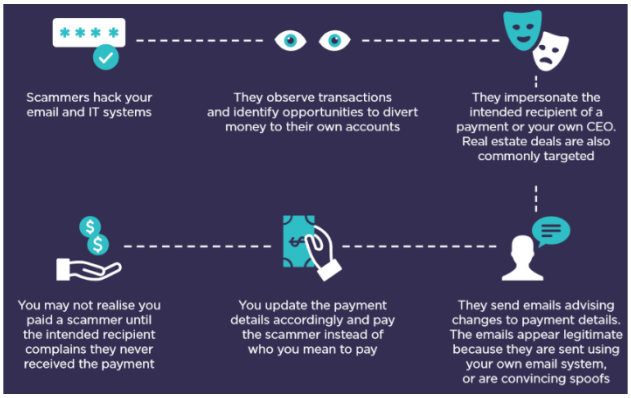
Welcome to the team Gagan!!

Brace168's simulated Phishing Campaigns!



It's just a regular Monday morning, you're sipping on your coffee as you log into your Google account. Tony from sales is explaining his weekend camping trip away, how amazing his "off-road beast" handled the muddy terrain. And with a click of a button, you've been PHISHED. Bet you didn't notice that malicious IP address in the top left corner. Even if you did, statistics prove that one of your work colleagues won't.

Phishing attacks are increasing. The ACCC's Targeting Scams report has found that Business Email Compromise scams caused the highest losses across all types of scams in 2019, costing Australian businesses a total of $132 million, an 120% increase on the previous year.



While having data protection and advanced threat monitoring services tailored to your unique environment is essential to maintain a healthy security posture, your staff are the last and most important line of defence in protecting your business from cyber security threats.

Brace168 simulated phishing campaigns are a quick and easy diagnostic tool to determine the health of your last line of cyber defence. It will help protect your organization by exposing employees to convincing phishing emails and reporting back on those who click on included weblinks, or enter credentials. You can consider a Brace168 simulated phishing campaign like a fire drill, giving staff regular practice in correct cyber-secure behaviour. While we have all participated in numerous fire drills throughout our lives, let me ask you this, how many phishing campaigns have you engaged in??

Get in contact with Brace168 to see how you can diagnose your company's defence against phishing attacks, and implement the recommended steps to prevent your company from contributing to phishing attacks losses in 2020.

Brace168's

WFH Safeguards!

The line between our ONLINE and OFFLINE lives is shifting as technologies bring the internet into our workplaces, homes, and everywhere in between. As more and more employees begin to work from home on a permanent basis, Brace168 has developed 11 easy to follow, cyber defense best practices for securing your company's digital systems and data. Our customers received all 11 this month, and as a Brace168 newsletter subscriber, you have access to 6 of them. If you would like to unlock the other 5, feel free to contact us and we would happily provide them to you.

Common Vulnerabilities & Exposure for August

1. A CRITICAL remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests. Exploited through an attacker sending malicious requests to a Windows DNS server. The 17-year-old vulnerability, which has been given the name SigRed, is wormable, meaning it has the potential to spread via malware between vulnerable computers without user interaction. The vulnerability was first discovered by our very own partner Check Point, click here for a detailed write up.
    - CVE-2020-1350

Score: 10 Critical

Likelihood: Critical – Every organisation using Microsoft infrastructure is at major risk of a complete breach of the entire corporate network. The vulnerability is easy to exploit and is self-propagating. Since this vulnerability has been present for 17 years, it is likely that a threat actor has already found and exploited it.

Recommendation: Patch all versions of Windows Server used for DNS immediately, click here for the security update matrix. Brace168 can run vulnerability scans on your systems to ensure you are not vulnerable, and we can perform malware scans to ensure vulnerabilities are not being exploited.

2. SAP NetWeaver versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system. The vulnerability, known as RECON, can be exploited over HTTP without authentication, bypassing existing access controls and can lead to a full compromise of the system.
    - CVE-2020-6287

Score: 10 Critical

Likelihood: Critical – Every organisation using Microsoft infrastructure is at major risk of a complete breach of the entire corporate network. The vulnerability is easy to exploit and is self-propagating. Since this vulnerability has been present for 17 years, it is likely that a threat actor has already found and exploited it.

Recommendation: Patch all versions of Windows Server used for DNS immediately, click here for the security update matrix. Brace168 can run vulnerability scans on your systems to ensure you are not vulnerable, and we can perform malware scans to ensure vulnerabilities are not being exploited.

3. F5 BIG-IP devices have a remote code execution vulnerability that would allow an attacker to create or delete files, disable services, intercept information, run arbitrary system commands and Java code, completely compromise the system, and pursue further targets, such as the internal network. To exploit, an attacker needs to send a specifically crafted HTTP request to the server hosting the Traffic Management User Interface utility for BIG-IP configuration.
    - CVE-2020-5902

Score: 9.8 Critical

Likelihood: Medium – Active exploits are in the wild, but you are only at risk if your F5 BIG-IP web interface is exposed to the internet.

Recommendation: Patch using this matrix – click here. Brace168 can perform scan the internet to see if your devices are exposed to the internet without you knowing.