Brace168

September 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

"Many things in life can be safely ignored but ignoring Cybersecurity Safe Practices is an open invitation for disaster"

- JC Hunter

Brace168 News!

Diversity Lunch!!

Brace168 staff were treated by Opeyemi Ajibola and his family to a very, very tasty Nigerian cuisine this month.

Gizdodo, also known as gizzard and dodo, is a happy marriage of fried plantain, fried gizzard and peppered stew, and is a staple in most Nigerian households. It can be served as a course meal or as a side. Ope's family likes to add fried rice to the traditional dish, a delicious combination loved by Brace168 team.

Thank you very much to Opeyemi Ajibola and his family, and we look forward to the next lunch!

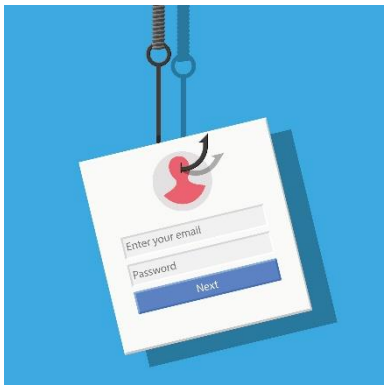
Brace168's thoughts on Industry News!

Ransomware-as-a-Service is on the rise!

Ransomware-as-a-Service (RaaS) has simultaneously grown more powerful and easier to use over the last couple of years, a disastrous combination for organisations with poor security posture. It has become so easy to use that just about anyone can launch successful and damaging ransomware attacks on organizations. Inexperienced attackers with little or no knowledge of coding only need to sign up with a RaaS provider for a "service", which includes everything a would-be hacker needs to launch a financially-motivated attack.

Brace168 first learned of the Dharma RaaS, one of the most profitable ransomware families, through customers using Sophos products. The vast majority of targets for the Dharma RaaS attacks are small to medium sized businesses; with 85 percent of the attacks seen in 2020 targeting exposed access tools such as Remote Desktop Protocol (RDP) servers.

To counteract RaaS attacks, companies need to make sure all their appliances are inspected, and all email attachments and links are analysed. It is also recommended that companies should utilise a SIEM / SOAR service integrated with analytical tools in order to derive attack patterns from the log data. Brace168 is both ISO27001 and CREST certified to provide SIEM and SOAR to the highest quality of security service in the cyber security industry, and our on-premise SOC utilises these next generation technologies to enhance our real-time incident and response service. Contact us via (02) 9136 6066 or info@brace168.com for more information about these services.



SANS Institute, a cybersecurity firm, victim to a phishing attack

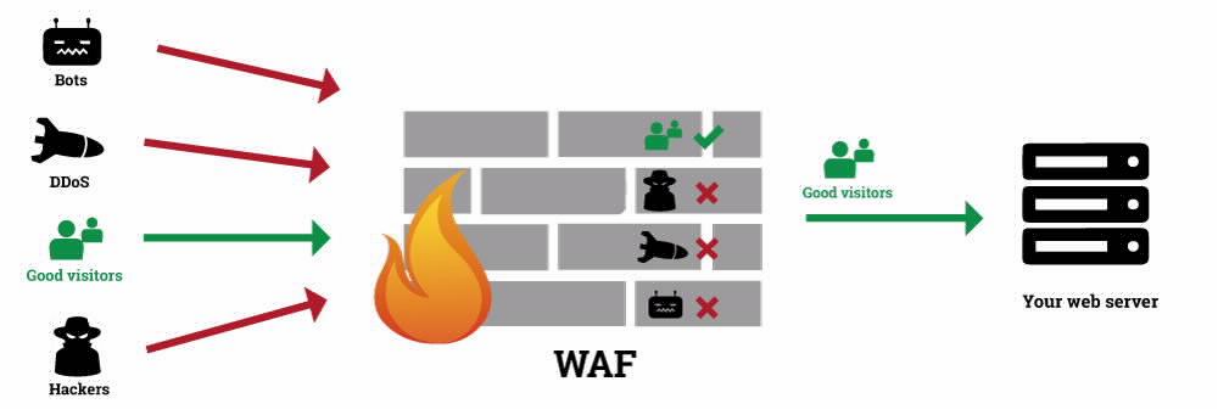
The SANS Institute, an information security training firm, has fallen victim to a phishing attack that exposed roughly 28,000 records containing personally identifiable information. The threat actor managed to get an employee to install a malicious MS Office365 add-on and grant it permissions to allow access to the sensitive data. SANS commented that the phish ""was a carefully crafted email that looks like a file share from SharePoint via O365." The fact that a trusted source of cyber expertise fell victim to the scheme demonstrates that no organization is immune to cyber attacks – as it takes just one uninformed, distracted or negligent employee to trigger an incident.

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 losses in 2020.

Brace168 Service Spotlight:

Web Application Firewall



A web application firewall (WAF) is a firewall that monitors, filters and blocks data packets as they travel to and from a website or web application. A WAF can be either network-based, host-based or cloud-based and is often deployed through a reverse proxy and placed in front of one or more websites or applications.

A WAF analyses Hypertext Transfer Protocol (HTTP) requests and applies a set of rules that define what parts of that conversation are malicious. The main parts of HTTP conversations that a WAF analyses are GET and POST requests. GET requests are used to retrieve data from the server, and POST requests are used to send data to a server to change its state.

Methods of filtering via WAF:

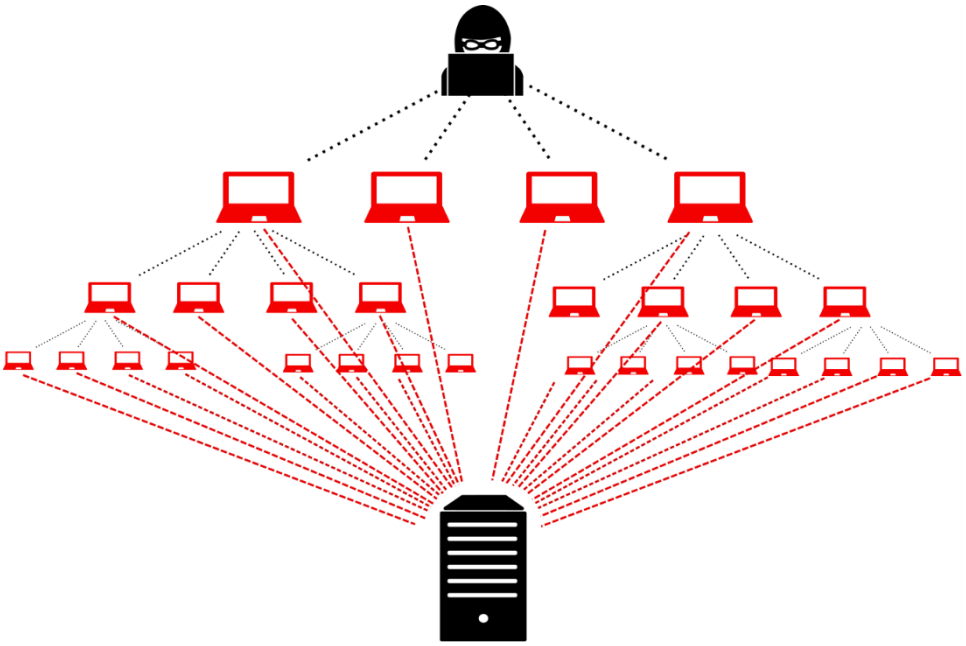
- **Whitelisting**: A kind of WAF where you allow only trusted entities like provided IP address that are known to be safe. Though it is less time consuming than Blacklisting, it needs to run over frequently to update the safe known IP Address.
- **Blacklisting**: A extensive kind a WAF which is more appropriate for public websites and web applications because they receive a larger amount of traffic from unfamiliar IP addresses that are not familiar or malicious. Blacklisting approach requires more information to filter packets, based on specific characteristics, rather than just accepting trusted IP addresses.
- **Hybrid:** It uses both the Whitelist and Blacklist method of rules which are customised to specific environment. Its more intensive method of filtering the packets by analysing them and allow only the trusted packets to move over

Types of web application firewalls:

- **Network-based WAFs**: Enable replication of rules and settings across multiple appliances, thereby making large-scale deployment, configuration, and management possible.
- **Host-based WAFs:** May be fully integrated into the application code itself. Host-based WAFs require application libraries and depend upon local server resources to run effectively which intern require developers, system analysts and DevOps/DevSecOps, to monitor.
- **Cloud-hosted WAF's:** These third parties have the latest threat intelligence and can help identify and block the latest application security threats.

A WAF has an advantage over traditional firewalls because it offers greater visibility into application data that is communicated using the HTTP application layer. It can prevent application layer attacks that normally bypass traditional network firewalls, including the following:

- **Cross-site scripting (XSS) attacks** enable attackers to inject and execute malicious scripts in another user's browser.
- **SQL injection** attacks can affect any application that uses an SQL database and enables attackers to access and potentially change sensitive data.
- **Web session hacking** enables attackers to hijack a session ID and take over as an authorized user. A session ID is normally stored within a cookie or Uniform Resource Locator (URL).
- **Distributed denial-of-service (DDoS)** attacks overwhelm a network by flooding it with traffic until it is unable to serve its users. Both network firewalls and WAFs can handle this attack type but approach it from different layers.



Another advantage of a WAF is that it can defend web-based applications without necessarily having access to the source code of the application. As the number of applications created increases, the longer amount of time needs to be taken to perform SAST Code review, which may delay the go live and require monetary value. As a consequence, companies will often use the WAF as an alternative to secure their application from upcoming threats.

At Brace168, we would work with you and understand your requirements to implement the most appropriate WAF to your unique security posture, safeguarding your application from threats.

Common Vulnerabilities & Exposure for September

1. A remote code execution vulnerability and a denial of service vulnerability has been found in Apache Struts 2 versions 2.0.0-2.5.20. Apache Struts 2 is a widely used open source web application framework for developing Java web applications. Approximately 65% of Fortune 100 firms use web applications built with this framework. The infamous 2017 Equifax data breach was achieved through exploiting a previous vulnerability in Apache Struts 2.
    - CVE-2019-0230
    - CVE-2019-0233

Score: NO OFFICIAL SCORE - Critical

Likelihood: Medium – This vulnerability has active exploits being shared on GitHub making attempts at exploitation very likely. However, since every Struts application is unique, the actual payload needed to exploit it will be different from application to application.

Recommendation: Brace168 recommends keeping track of what frameworks your web applications are built off because it can be easily ignored, leaving a blind spot for threat actors to attack (which is exactly what happened to Equifax). Please patch to Apache Struts version 2.5.22.

2. Millions of Internet of Things (IoT) devices are exposed to a critical vulnerability found in their processors. Thales, a manufacturer of processors, has found that 9 of their computer chips are vulnerable to a remote code execution exploit that could be used to steal credentials and potentially gain control over the device or gain access to the central network to conduct widespread attacks. Attacks against IoT devices has increased by 2000% since 2018 and represent the largest opportunity for threat actors to breach your environment due to the prevalence of IoT devices such as any "smart" device (smart speaker, smart doorbell, etc…).
    - CVE-2020-15858

Score: 8.8 High

Likelihood: High – It is near impossible to keep track of what IoT devices are connected to your network and its even harder to know what processor they use. As such, they represent an easy opportunity for threat actors to gain access to your network. Given the critical nature of many of these devices, a targeted cyberattack could be significant. For example smart meters could be compromised to deliver falsified readings to increase or reduce an electricity bill.

Recommendation: Do you know what IoT devices are connected to your network? Do you know what information is stored on these devices? Do you monitor the activity on these devices? Have you performed a penetration test on the IoT devices connected to your network? If you answered no to any or all of these questions, get into contact with Brace168.

3. Adobe Acrobat Reader DC has had several vulnerabilities, the most critical of which is a remote code execution which could be used to infect users' computers with Malware. Since Adobe Acrobat Reader DC is commonly used in organizations to access PDF's, there is a high risk of being exposed to this vulnerability.
    - CVE-2020-9693
    - CVE-2020-9694

Score: 9.3 High

Likelihood: Medium – The prevalence of Adobe Acrobat Reader DC makes an exploit likely, however a good antivirus tool can prevent exploits.

Recommendation: Update Adobe Acrobat Reader DC and ensure you are protected by a good Antivirus software. Brace168 recommends Checkpoint Sandblast as the Antivirus tool of choice.