Brace168

May 2020
Newsletter

Author: Lachlan Rodwell – Security Analyst

Brace168 Pty Ltd,

157 Walker St, North Sydney

www.brace168.com

info@brace168.com

P: (02) 9136 6066

> “There are only two types of companies: those that have been hacked and those that will be”
>
> - Robert Mueller

RIGHTCROWD IQ: INSIDE OUT SECURITY

The question to the right is a simple question that can be difficult to answer and provide big security surprises. In any organization, new hires and role changes are constant. If unmanaged, they result in the accumulation of access privileges that create hidden security risks around breaches.

Who's got access to your critical applications and information?

That's where RightCrowd IQ focuses. The application analyses who has access to your systems and critical information. Users can instantly assess the health of access or remediation is required. The real benefit is quite simple – auditing access across different systems is disjointed and complex. RightCrowd IQ makes it easy.

RIGHTCROWD IQ

The other benefits of RightCrowd IQ included:

- Identify access issues – so that team leaders and IT could see who shouldn't have access proactively
- Reduce the cost of audit – automating user access reporting that reduces the direct overhead of compliance
- Improved security controls – by investigating underlying issues and processes
- Improved security posture – proactively managing your environment with preventative controls

Call us for a demonstration today!

Check Point®
SOFTWARE TECHNOLOGIES LTD

BRACE168 CHECK POINT PARTNERSHIP

Brace168 is also proud to be partnered with Check Point Software Technologies to offer Public Cloud Solutions to secure your cloud environments! Check Point is the worldwide leader in securing the Internet.

Security is the biggest barrier to wide-spread enterprise cloud adoption, but traditional security approaches don't fit the dynamic nature of the cloud, leaving businesses exposed. Check Point's CloudGuard services aim to provide advanced threat protection to keep your cloud network, data and application protected from the most sophisticated attacks. It ensures all of your assets are fully protected while supporting the elastic, dynamic and cost-effective nature of the cloud.

Brace168’s thoughts on Industry News!

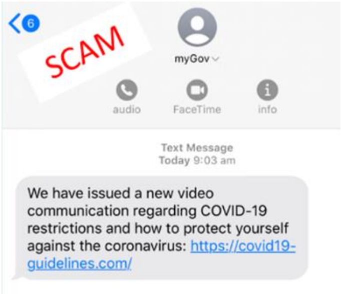
Brace168’s Comments on COVID-19 and ongoing Cyber Risk

Cybercrime actors are continuing to pivot their online criminal methods to take advantage of the COVID-19 pandemic.

COVID-19 themed websites are being used as a vehicle for distributing malicious software that has the capability to harvest personal information of unsuspecting users. Spoofed government health websites are being reported as curious individuals attempt to learn more about the pandemic. We have found that our anti-virus and anti-malware have been regularly blocking infected links inside these websites for our customers, however users should ensure they are accessing trusted sources like the .gov.au domain.

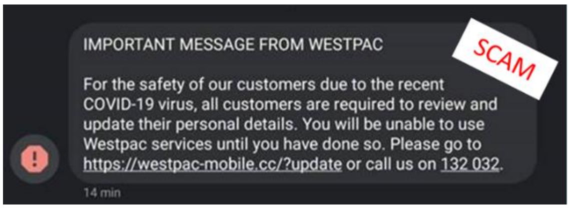
In addition to this, elaborate and sophisticated COVID-19 themed phishing campaigns are taking advantage of individuals seeking out health-related information. Email phishing continues to be one of the most successful threat vectors for criminals as it relies upon an unsuspecting and ill-informed end user. While O365 does a good job of detecting phishing emails, the learning engine is still evolving and is incapable of picking up all emails. Users should always confirm the authenticity of the source of the email prior to opening it and any associated links and/or attachments.

Targeted SMS campaigns claiming to offer health-related information continue to be reported as shown in the photo to the right. Furthermore, SMS campaigns that masquerade as the users’ bank are being proliferated to harvest banking credentials; an example of this is seen below.



Text Message
Today 9:03 am

We have issued a new video communication regarding COVID-19 restrictions and how to protect yourself against the coronavirus: https://covid19-guidelines.com/



IMPORTANT MESSAGE FROM WESTPAC

For the safety of our customers due to the recent COVID-19 virus, all customers are required to review and update their personal details. You will be unable to use Westpac services until you have done so. Please go to https://westpac-mobile.cc/?update or call us on 132 032.

14 min

All of these threats pose serious risk and regular communications should be made to ensure that individuals are aware of threat-trends across the mediums relevant to them, such as SMS, email, social media and web browsing.

We can manage your anti-virus and anti-malware solution and if your employees need stronger awareness of phishing attacks; we can train them and monitor their emails for suspicious activity so that your employees are secure!

Common Vulnerabilities and Exposure for May

1. A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
   - CVE-2020-1020
   - CVE-2020-0938
2. Two vulnerabilities for Google Chrome have been found, potentially affecting 2 billion devices. These vulnerabilities are yet to be publicly release due to their severity, so information is limited. We do know these vulnerabilities are use-after-free bugs which is where an attempt to access memory after it has been freed elsewhere so that arbitrary code can be executed.
   - CVE-2020-6461
   - CVE-2020-6462
3. Under certain conditions, vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Services Controller (PSC), does not correctly implement access controls. A malicious actor with network access to port 389 on an affected vmdir deployment1 may be able to extract highly sensitive information such as administrative account credentials which could be used to compromise vCenter Server or other services which are dependent upon vmdir for authentication.
   - CVE-2020-3952

Score: 8.1 High

Likelihood: High – This vulnerability is remotely exploitable and has been used in active attacks. There are multiple ways an attacker could exploit the vulnerability such as convincing a user to open an infected document.

Recommendation: This exploit can use two different vulnerabilities. The fist has been patched so update your respective version of windows with the latest security patch for that version. The other vulnerability has yet to be patched but has also yet to be used in active attacks. It is imperative that you are more vigilant to phishing attacks during this period, especially with remote work forces. If you need help detecting phishing attacks, please contact us!

Score: ???

Likelihood: Low – All we know is that these are very serious vulnerabilities by which a threat actor can run code on your computer remotely without warning. However, there is currently no evidence that it has been actively exploited and by Google not releasing the information of these vulnerabilities publicly, threat actors will have a more difficult time figuring out how to exploit it.

Recommendation: Due to the severity of this vulnerability, you need to update google chrome to the latest version before this vulnerability gets publicly released because the likelihood of it being exploiting increase drastically!

Score: 9.8 Critical

Likelihood: Medium –Active attacks are unknown and due to remote working conditions, virtual workstations are being used more than ever, increasing the likelihood for exploit.

Recommendation: Apply the patches using the following Response Matrix:

https://www.vmware.com/security/advisories/VMS