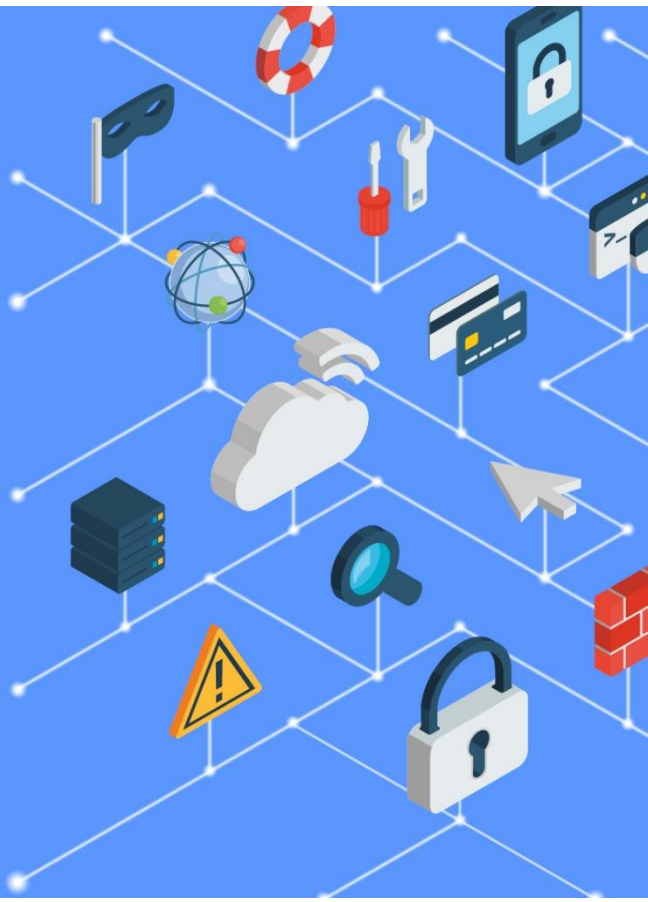
Cyber Scotland Bulletin



Threat Intelligence

ISSUE: 05.01.21

CyberScotland Bulletin

The CyberScotland Threat Intelligence Bulletin is designed to provide you with information about emerging or escalating cyber threats. We hope that you benefit from this resource and we ask that you circulate this information to your networks, adapting where you see fit.

This bulletin is provided in conjunction with SBRC's Cyber Incident Response. If there are any cyber terms you do not understand, you can look them up in the NCSC Glossary.

We would like to wish you a merry and safe Christmas and a happy New Year! The CyberScotland Threat Intelligence Bulletin will return in January 2021. Please remember to update the software and firmware of any new devices that you receive and the secure them with passwords in line with NCSC guidelines.

Jump To

Technical Threats

Microsoft Source Code Exposed

Microsoft confirmed last week that attackers were able to view some of its source code, which it found during an ongoing investigation of the SolarWinds breach. While its threat-modelling approach mitigates the risk of viewing code, many questions remain that could determine the severity of this attack.

While attackers were only able to view the source code, and not edit or change it, this level of access could prove helpful with some things — for example, writing rootkits. Microsoft, which did not provide

additional detail for this story beyond its blog post, has not confirmed which source code was accessed and how that particular source code could prove helpful to an attacker.

Source: DARK Reading

Zend Framework remote code execution vulnerability revealed

An untrusted deserialization vulnerability disclosed this week in how Zend Framework can be exploited by attackers to achieve remote code execution on PHP sites.

This vulnerability tracked as CVE-2021-3007 may also impact some instances of Laminas Project, Zend's successor.

Zend Framework consists of PHP packages installed over 570 million times. The framework is used by developers to build object-oriented web applications.

PHP powers about 80% of the internet sites in some capacity, and given the historic popularity of Zend Framework, developers are advised to thoroughly check their web applications for cases of untrusted object deserialization.

A similar gadget chain has been found in Yii Framework this week which the attackers can use to target vulnerable applications.

Source: Beeping Computer

Secret backdoor discovered in Zyxel firewalls and AP controllers

Over 100,000 Zyxel devices are potentially vulnerable to a secret backdoor caused by hardcoded credentials used to update firewall and AP controllers' firmware.

The account does not show in the Zyxel user interface and has a login name of 'zyfwp' and a static plain-text password. The account could be used to log into vulnerable devices over both SSH and the web interface. Since the SSL VPN interface operates on the same port as the web interface.

VPN device vulnerabilities are extremely dangerous as they can be used to create new VPN accounts to gain access to an internal network or create port forwarding rules to make internal services publicly accessible.

"Someone could for example change firewall settings to allow or block certain traffic. They could also intercept traffic or create VPN accounts to gain access to the network behind the device. Combined with a vulnerability like Zerologon this could be devastating to small and medium businesses."

Source: Bleeping Computer

Google Discloses Poorly-Patched, Now Unpatched, Windows 0-Day Bug

Google's Project Zero team has made public details of an improperly patched zero-day security vulnerability in Windows print spooler API that could be leveraged by a bad actor to execute arbitrary code.

Details of the unpatched flaw were revealed publicly after Microsoft failed to rectify it within 90 days of responsible disclosure on September 24.

Successful exploitation of this vulnerability could result in an attacker manipulating the memory of the "splwow64.exe" process to achieve execution of arbitrary code in kernel mode, ultimately using it to install malicious programs; view, change, or delete data; or create new accounts with full user rights.

Although Microsoft eventually addressed the shortcoming as part of its June Patch Tuesday update, new findings from Google's security team reveals that the flaw has not been fully remediated.

"The vulnerability still exists, just the exploitation method had to change," Google Project Zero researcher Maddie Stone said in a write-up.

Source: The Hacker News

Corporate/Individual Threat Landscape

Leading Game Publishers Hit Hard by Leaked-Credential Epidemic

Over 500,000 leaked credentials tied to the top two dozen leading gaming companies are for sale online.

Leading gaming companies, such as Ubisoft, have become big targets for cybercriminals that aim to turn a profit by selling leaked insider-credentials tied to the top game publishers. Over 500,000 stolen credentials tied to the top 25 gaming firms were found on caches of breached data online and up for sale at criminal marketplaces, according to researchers at Kela.

In a recent scan, they found 1 million compromised credentials associated with the larger gaming universe of “clients” and also employees – half of which were for sale online. More than 500,000 of the leaked credentials pertained to employees of leading game companies

Source: Threat Post

Malware uses WiFi BSSID for victim identification

Malware authors are using the WiFi AP MAC address (also known as the BSSID) as a way to geo-locate infected hosts.

Malware operators who want to know the location of the victims they infect usually rely on a simple technique where they grab the victim's IP address and check it against an IP-to-geo database like MaxMind's GeoIP to get a victim's approximate geographical location.

A security researcher with the SANS Internet Storm Center, said he discovered a new malware strain that is using a second technique on top of this. The technique relies on grabbing the infected user's BSSID.

The malware is collecting the BSSID and then checking it against a free BSSID-to-geo database. The database is a collection of known BSSIDs and the last geographical location they've been spotted.

Source: ZNET

Healthcare Industry Witnessed 45% Spike in Cyber Attacks Since Nov 2020

Cyberattacks targeting healthcare organizations have spiked by 45% since November 2020 as COVID-19 cases continue to increase globally.

The average number of weekly attacks in the healthcare sector reached 626 per organization in November as opposed to 430 the previous month, with attack vectors ranging from ransomware, botnets, remote code execution, and distributed denial-of-service (DDoS) attacks.

The usage of Ryuk [Ransomware] emphasizes the trend of having more targeted and tailored ransomware attacks rather than using a massive spam campaign, which allows the attackers to make sure they hit the most critical parts of the organization and have a higher chance of getting paid.

Central Europe topped the list of regions impacted by the increase in attacks against healthcare organizations with a 145% uptick in November, followed by East Asia (up 137%) and Latin America (up 112% increase). Europe and North America saw increases of 67% and 37% respectively.

Source: The Hacker News