

## Contents

### 01 Patches Notes

---

### 02 Cyber Attack

---

### 03 Malware and Vulnerabilities

---

### 04 Cyber-Tech

---

“

THE HEALTH SECTOR  
CONTINUOUSLY GET'S  
PUMMELED BY MALICIOUS  
ACTORS AND HACKERS BECAUSE  
THEIR CYBER-KINETIC SECURITY  
IS BEING MANAGED BY  
“PARTICIPATION TROPHY”  
WINNING WIMPS!



# Patches Notes

---

## VMWARE PATCHES HIGH-SEVERITY VULNERABILITIES IN VREALIZE OPERATIONS


---

- VMware updates patches for a series of vulnerabilities in vRealize Operations, including four considered high severity.
- An unauthenticated attacker who has network access to the vRealize Operations Manager API could exploit the vulnerability to add new nodes to an existing vROps cluster.




## THE OPENSLL PROJECT PATCHED A HIGH-SEVERITY VULNERABILITY

---

- The OpenSSL Project released the OpenSSL 1.1.1l version that addresses a high-severity buffer overflow flaw, tracked as CVE-2021-3711.
- Which can allow an attacker to change an application's behaviour or cause the app to crash. 

## CISCO ISSUES CRITICAL FIXES FOR HIGH-END NEXUS GEAR

---

- Cisco Systems released six security patches tied to its high-end 9000 series networking gear ranging in importance from critical, high and medium severity.
- Bugs patched by Cisco (rated 9.1 out of 10) could allow a remote and unauthenticated adversary to read or write arbitrary files. 



## AT&T DENIES DATA BREACH AFTER HACKER AUCTIONS 70 MILLION USER DATABASE


- AT&T says that they did not suffer a data breach after a well-known threat actor claimed to be selling a database containing the personal information of 70 million customers.
- The threat actor, known as ShinyHunters, began selling this database yesterday on a hacking forum with a starting price of \$200,000 and incremental offers of \$30,000. The hacker states that they are willing to sell it immediately for \$1 million.

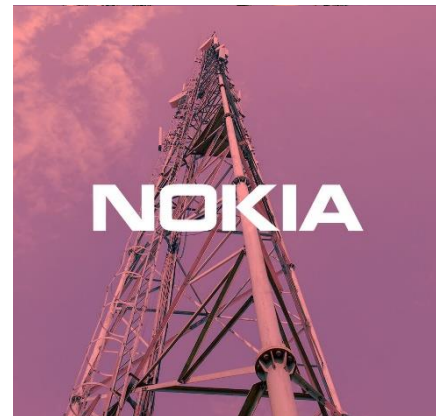


# CYBER ATTACKS




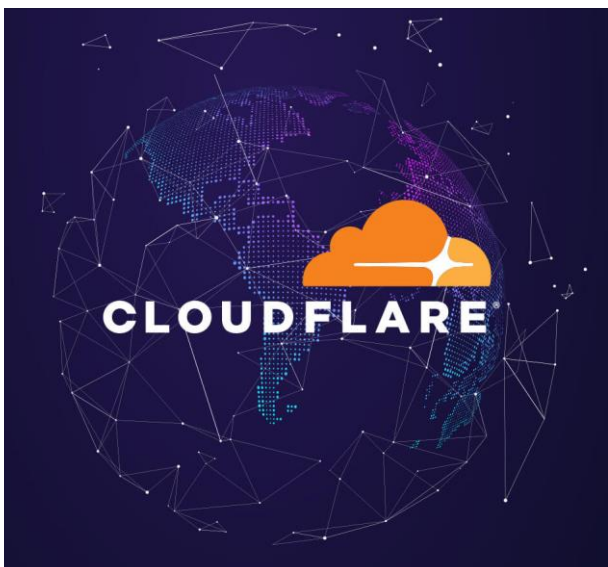
## NOKIA SUBSIDIARY DISCLOSES DATA BREACH AFTER CONTI RANSOMWARE ATTACK

- SAC Wireless, a US-based Nokia subsidiary, has disclosed a data breach following a ransomware attack where Conti operators were able to successfully breach its network, steal data, and encrypt systems.
- The wholly-owned and independently-operating Nokia company, headquartered in Chicago, IL, works with telecom carriers, major tower owners, and original equipment manufacturers (OEMs) across the US. 



## CLLOUDFLARE SAYS IT MITIGATED A RECORD-BREAKING 17.2M RPS DDOS ATTACK

- Web infrastructure and website security company Cloudflare on Thursday disclosed that it mitigated the largest ever volumetric distributed denial of service (DDoS) attack recorded to date.
- That's originate from a network of malware-infected systems — consisting of computers, servers, and IoT devices — enabling threat actors to seize control and co-opt the machines into a botnet capable of generating an influx of junk traffic directed against the victim. 



# Malware and Vulnerabilities



## NEW ZERO-CLICK IPHONE EXPLOIT USED TO DEPLOY NSO SPYWARE

- Digital threat researchers at Citizen Lab have uncovered a new zero-click iMessage exploit used to deploy NSO Group's Pegasus spyware on devices belonging to Bahraini activists.
- NSO Group attacks using the new iMessage zero-click (which circumvents the iOS BlastDoor feature designed to block such exploits) were first spotted in February 2021. [↗](#)



## NEW SIDEWALK BACKDOOR TARGETS U.S.-BASED COMPUTER RETAIL BUSINESS

- A computer retail company based in the U.S. was the target of a previously undiscovered implant called SideWalk as part of a recent campaign undertaken by a Chinese advanced persistent threat group primarily known for singling out entities in East and Southeast Asia. [↗](#)

## THE 'JOKER' VIRUS HAS RETURNED TO ANDROID

- The 'Joker' virus hides in several apps on the Google Play Store and the user does not realize it until their bank accounts are emptied. See how this malware operates and what are the dangerous applications.
- This malware is capable of subscribing the user to payment services without their authorization and emptying their bank accounts without them noticing. [↗](#)

## RAZER BUG LETS YOU BECOME A WINDOWS 10 ADMIN BY PLUGGING IN A MOUSE

- A Razer Synapse zero-day vulnerability has been disclosed on Twitter, allowing you to gain Windows admin privileges simply by plugging in a Razer mouse or keyboard.
- Razer is a very popular computer peripherals manufacturer known for its gaming mice and keyboards. [↗](#)

# CYBER TECH




## MICROSOFT SHARES GUIDANCE ON SECURING WINDOWS 365 CLOUD PCS


- Microsoft has shared guidance on securing Windows 365 Cloud PCs and more info on their built-in security capabilities.
- The guidance is broken down into actions customers can take to secure Cloud PCs enrolled in Windows 365 Business and Windows 365 Enterprise subscription plans.



## MICROSOFT WILL ADD SECURE PREVIEW FOR OFFICE 365 QUARANTINED EMAILS

- Microsoft is updating Defender for Office 365 to protect customers from embedded email threats while previewing quarantined emails.
- Microsoft Defender for Office 365 (previously Office 365 Advanced Threat Protection) provides Office 365 enterprise email accounts with protection from multiple threats, including business email compromise and credential phishing, as well as automated attack remediation. 

## ELASTIC ACQUIRES BUILD.SECURITY FOR SECURITY POLICY DEFINITION AND ENFORCEMENT

- Less than a year after raising its \$6 million seed funding round, Tel Aviv and Sunnyvale-based startup build.security is being acquired by Elastic.
- Build.security is focused on security policy management for applications. A core element of the company's technology approach is the Open Policy Agent (OPA) open-source project, which is part of the Cloud Native Computing Foundation (CNCF), which is also home to Kubernetes. 



## ABOUT INFOPERCEPT


Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

## MOVING TARGET DEFENCE



Due to the static nature of modern day computing systems, they are quite defenseless against the hackers. Hackers make use of the time to tap into the vulnerabilities or gaps in the system and initiate an attack. This is unacceptable as it provides a skewed advantage to the hackers.

This is where Moving Target Defense (MTD) comes into play. It has revolutionized the way defense technology works. Due to the dynamic nature of change that occurs across multiple systems, there is a certain level of uncertainty which hampers the progress of the attackers. It narrows down the window of opportunity for the cyber criminals which leads them to try harder and invest more time and resources but in vain. It further defuncts their surveillance on the system. 



SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117

[sos@infopercept.com](mailto:sos@infopercept.com)

[www.infopercept.com](http://www.infopercept.com)

