INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -22 November 2021

Contents

Patches Notes

ADOBE PATCHES CRITICAL ROBOHELP SERVER SECURITY FLAW

- Adobe announced updates on Tuesday to address at least four known security flaws that expose users to dangerous hacker attacks.
- CVE-2021-43015 and CVE-2021-43016 are two vulnerabilities that can be used to conduct arbitrary code execution and application denial-of-service attacks.

ZOOM FIXES HIGH-RISK CONNECTOR AND CLIENT FLAWS

- Zoom, a video messaging platform company, has released patches for high-severity vulnerabilities that can lead to remote code execution and command injection attacks for enterprise users.
- If a malicious user used the Key base client's public folder sharing feature to exploit this flaw, remote code execution may occur.

MICROSOFT EMERGENCY UPDATES FIX WINDOWS SERVER AUTH ISSUES

- CVE-2021-43015 and CVE-2021-43016 are two vulnerabilities that can be used to conduct arbitrary code execution and application denial-of-service attacks.
- End-users on impacted systems cannot use Single Sign-On (SSO) in Active Directory on-premises or hybrid Azure Active Directory deployments to sign into services or applications.

CYBER ATTACKS

FBI system hacked to email 'urgent' warning about fake cyberattacks

- The FBI's email systems were hacked, and spam emails imitating FBI alerts that the recipients' networks had been infiltrated and data stolen were sent out.
- At least 100,000 people received the bogus emails. However, the figure is a cautious estimate, since the researchers feel "the campaign may have been much, much greater."

7 MILLION ROBINHOOD USER EMAIL ADDRESSES FOR SALE ON HACKER FORUM

- After one of its workers was compromised, the threat actor utilised their account to gain access to the information of around 7 million customers through customer care systems, Robinhood announced a data breach.
- The attacker was selling the stolen information of 7 million Robinhood clients for at least five figures, which is $10,000 or more.

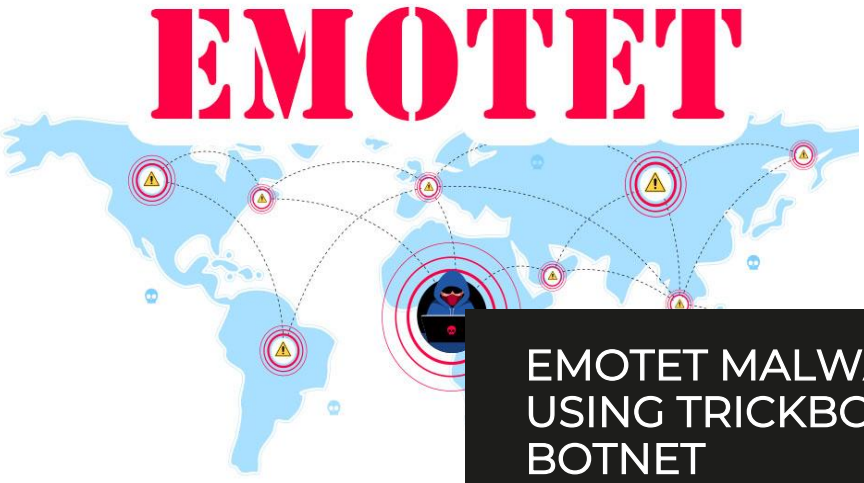
CLOUDFLARE MITIGATED 2 TBPS DDOS ATTACK, THE LARGEST ATTACK IT HAS SEEN TO DATE

- Cloudflare said that it had mitigated a distributed denial-of-service (DDoS) attack with a peak of just under 2 terabytes per second (Tbps), the company's greatest attack to date.
- A Mirai botnet variant with 15,000 bots started the attack, which included DNS amplification and UDP floods. Internet of Things (IoT) devices and GitLab instances were among the botnet's targets.

Malware and Vulnerabilities

BOTENAGO MALWARE ENDANGERS MILLIONS OF ROUTERS AND IOT DEVICES

- BotenaGo, written in Google's Golang programming language, can exploit more than 30 different vulnerabilities.
- Newly surfaced malware that is difficult to detect and written in Google's open-source programming language has the potential to exploit millions of routers and IoT devices. BotenaGo



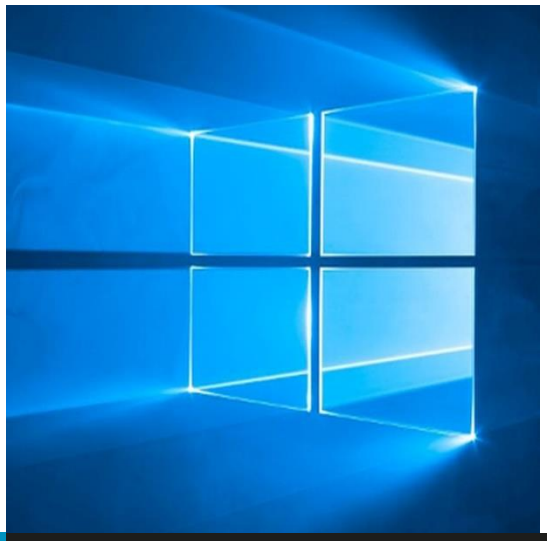
EMOTET MALWARE IS BACK AND USING TRICKBOT TO REBUILD ITS BOTNET

- Emotet would then utilise infected devices to carry out additional spam campaigns and install other payloads like the QakBot (Qbot) and Trickbot malware. These payloads would subsequently be utilised to give threat actors, such as Ryuk, Conti, ProLock, Egregor, and others, early access to deploy ransomware.
- This absence of spam activity is most likely due to the Emotet infrastructure being rebuilt from the ground up, as well as new reply-chain emails being stolen from victims in future spam campaigns.

NUMEROUS INTEL CHIPS ARE AFFECTED BY SEVERE BIOS ISSUES.

- Intel has publicly disclosed two high-severity vulnerabilities that affect a wide variety of Intel chip families and allow threat actors and malware to gain elevated privileges on the system.
- Unfortunately, adding a BIOS password will not fully prevent you from this attack, as the weaknesses can be exploited remotely if the attacker has gained access to the system.

CYBER TECH



GOOGLE DEBUTS CLUSTERFUZZLITE SECURITY TOOL FOR CI, CD WORKFLOWS

- Fuzzing is an automated testing technique that involves introducing faulty and random data into programmes to detect faults and unexpected behaviour. This can reveal vulnerabilities or mistakes that might otherwise go undetected by manual analysis.
- ClusterFuzzLite can be integrated into current workflows to fuzz pull requests, increasing the likelihood of vulnerabilities being discovered earlier in the development process and prior to committal.

WINDOWS 10 21H2 IS RELEASED

- Windows 10 21H2, also known as the November 2021 upgrade, is now available as an optional update in Windows Update for customers using Windows 10 2004 or later.
- This feature update is being given out as an enabling package for Windows 10 2004, Windows 10 20H2, and Windows 10 21H1, allowing these versions to update to the new feature update more quickly.

MICROSOFT DEFENDER NOW INCLUDES AI-DRIVEN RANSOMWARE PROTECTION

- Microsoft Defender for Endpoint clients now have access to an AI-driven ransomware attack detection solution that complements existing cloud protection by analysing risks and stopping attackers at the perimeter.
- In a consumer scenario, the AI-driven adaptive protection function was very effective in preventing people from gaining access to the network by blocking the binary that would allow them to do so.

Infopercept

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.

DISASTER RECOVERY AUTOMATION

In today's day and age a company's online presence and operational consistency are the central components contributing to its marketing, branding, revenue generation, information, lead generation, sales and overall business. There is little doubt then, that most companies who want to succeed in this competitive market have to invest wisely and proactively into the stability and continuation of its business's critical-function apps.

Given the importance and benefit of digital business operations for the success of a business you would ideally want it to continue unabated so that you can perform your daily business operations conveniently. Due to this, the demand for DR automation is growing as businesses are looking for ways to reduce their operational downtime. A disaster recovery plan helps you achieve this very important task, by allowing you to continue or quickly resume and kickstart important business operations and functions in the event of a disaster happening.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN
+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense