INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -3 Jan 2021

Contents

Patches Notes

APPLE FIXES MACOS SECURITY FLAW BEHIND GATEKEEPER BYPASS

- Apple has addressed a macOS vulnerability that unsigned and unnotarized script-based apps could exploit to bypass all macOS security protection mechanisms even on fully patched systems.
- If they circumvent automated notarization security checks (which scans for malicious components and code-signing issues), the applications are allowed to launch by Gatekeeper, a macOS security feature designed to verify if downloaded apps are notarized and developer-signed.

APACHE'S NEW SECURITY UPDATE FOR HTTP SERVER FIXES TWO FLAWS

- There's a fix for a critical flaw in Apache HTTP Server, the world's second most widely used web server. The Apache Software Foundation has released an update to address a critical flaw in its hugely popular web server that allows remote attackers to take control of a vulnerable system.
- The foundation has released version 2.4.52 of the Apache HTTP Server (web server) that addresses two flaws tracked as CVE-2021-44790 and CVE-2021-44224, which have respective CVSS severity scores of 9.8 (critical) and 8.2 (high) out of a possible 10.

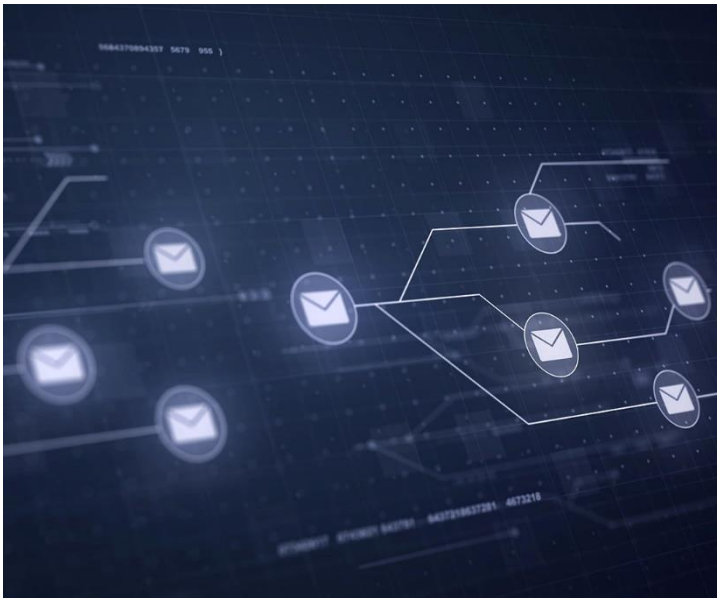
CYBER ATTACKS

New BLISTER Malware Using Code Signing Certificates to Evade Detection

- Cybersecurity researchers have disclosed details of an evasive malware campaign that makes use of valid code signing certificates to sneak past security defenses and stay under the radar with the goal of deploying Cobalt Strike and BitRAT payloads on compromised systems.
- The binary, a loader, has been dubbed "Blister" by researchers from Elastic Security, with the malware samples having negligible to zero detections on VirusTotal.

CYBER-ATTACK ON BELGIUM'S MILITARY

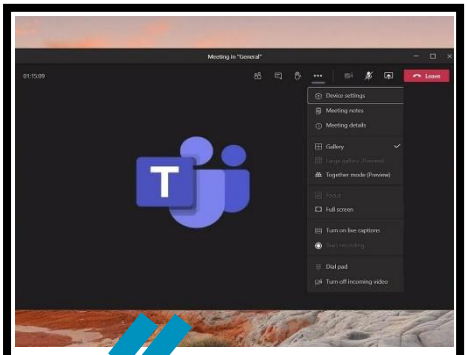
- Threat actors have exploited a vulnerability in Log4j software to wage a cyber-attack on Belgium's Defense Ministry.
- The attack began on December 16 and was confirmed by Belgium's Ministry of Defense on Monday. Log4j is a Java-based logging library that tracks system processes.



400,000 INDIVIDUALS AFFECTED BY EMAIL BREACH AT WEST VIRGINIA HEALTHCARE COMPANY

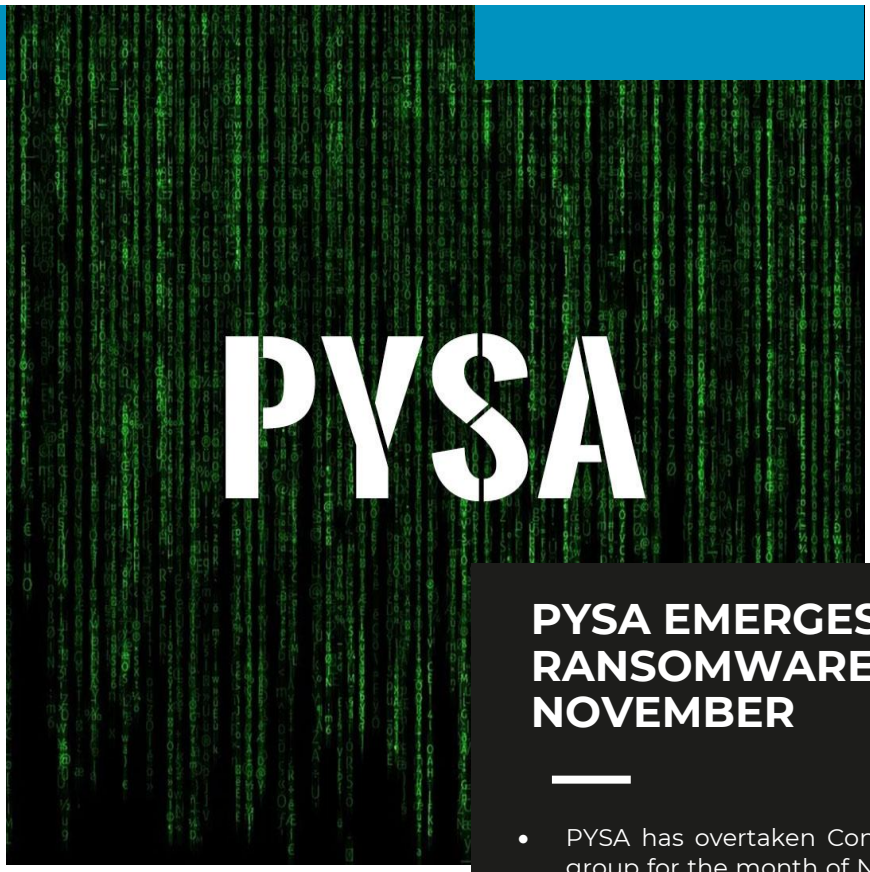
- Cybercriminals likely had access to the organization's email system between May 10 and August 15, 2021. A contractor's email account was used to send messages in an attempt to obtain funds through fraudulent wire transfers.
- The organization has since secured the affected email accounts and reset their passwords and says that its electronic health records systems were not compromised during the incident.

Malware and Vulnerabilities



FOUR BUGS IN MICROSOFT TEAMS LEFT PLATFORM VULNERABLE SINCE MARCH

- Vulnerabilities in Microsoft Teams allowed link spoofing of URLs and opened the door to DoS attacks against Android users, researchers said. So far, only one of the bugs appears to have been patched by Microsoft. Microsoft said the reported bugs do not pose an immediate threat to users.



PYSA EMERGES AS TOP RANSOMWARE ACTOR IN NOVEMBER

- PYSA has overtaken Conti as the top ransomware threat group for the month of November. It joined Lockbit, which has dominated the space since August.
- PYSA increased its market share with a 50 percent rise in the number of targeted organizations. In previous incidents, cyber-actors exfiltrated employment records that contained personally identifiable information (PII), payroll tax information and other data that could be used to extort victims to pay a ransom," the FBI warned.

TELEGRAM ABUSED TO STEAL CRYPTO-WALLET CREDENTIALS

- Attackers are targeting crypto-wallets of Telegram users with the Echelon infostealer. The malware is aimed at defrauding new or unsuspecting users of a cryptocurrency discussion channel.
- It was posted to a channel focused on cryptocurrency in October, researchers found. The campaign was a "spray and pray" effort, they said. The Echelon malware was delivered to users of the "Smokes Night" channel on the Telegram messaging app, researchers say.

CYBER TECH

THUNDERBIRD 91.4.1 EMAIL CLIENT RELEASED WITH SECURITY FIXES

- Thunderbird, the open source email client, has a new version available. Thunderbird 91.4.1 is a security update for the email client that also includes a slew of non-security fixes and enhancements.
- The new version of the email client fixes several attachment, account setup, and saving issues. Thunderbird would display save dialogues instead of opening certain types of attachments, such as ICS attachments.

HONEYPOT EXPERIMENT REVEALS WHAT HACKERS WANT FROM IOT DEVICES

- The honeypot ecosystem created by researchers consisted of three components: server farms, a vetting system, and data capture and analysis infrastructure. Cowrie, Dionaea, KFSensor, and HoneyCamera, which are off-the-shelf IoT honeypot emulators, are installed to create a diverse ecosystem.
- The experiment generated data from 22.6 million hits, the vast majority of which targeted the HoneyShell honeypot. The various actors used similar attack patterns, most likely because their goals and means of achieving them were similar.

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.

DECEPTION TECHNOLOGY

Deception Technology is a defense practice in cybersecurity which aims to deceive attackers. This is done by the distribution of a collection of traps and decoys across your organization's systems infrastructure, in order to replicate legitimate assets.

Deception technologies have to be designed in a way to entice the attackers so that they consider it to be a worthy asset and inject a malware. Upon injection of the malware into the decoy, automated static and dynamic analysis of the injected malware is conducted and reports are automatically generated and sent to the Information Security team of your organization.

What Type of Activities Do Deception Systems Detect?

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

INVINSENSE™
Attacktical Cybersecurity Sense