TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: July 16, 2024

TATA COMMUNICATIONS

TATA

THREAT INTELLIGENCE ADVISORY REPORT

Cyber threats are on the rise as the digital world keeps evolving. Businesses globally are working hard to protect their data and improve their core security systems. Organisations need to stay informed about the latest cyberattack trends and actively implement security updates to safeguard their resources from potential attacks.

Tata Communications' weekly threat intelligence advisory helps you stay ahead of the game. By providing insights into the newest cyber risks, this report allows you to take proactive steps to strengthen your defences against potential cyber vulnerabilities.

Malware attack targets Israeli entities

Cybersecurity researchers have warned about a malware attack campaign, "Supposed Grasshopper," actively targeting various Israeli organisations across different sectors. The attack reportedly uses publicly available tools like Donut and Sliver frameworks in a well-coordinated effort.

The attackers employ tailored WordPress sites to deliver malicious payloads. They also use multi-stage processes that involve Excel files and cloud storage to maintain persistence. The attackers impersonated Israeli government entities and private companies to trick victims into giving up sensitive information or clicking on malicious links. The motives behind the attacks remain unclear. However, some experts speculate that it could be a part of a legitimate penetration test.

ATTACK TYPE	Malware	**SECTOR**	Information technology, healthcare, financial services, construction, government, oil and gas, energy, defence, BFSI, aviation, telecommunications
REGION	Israel	**APPLICATION**	Windows

Source - https://harfanglab.io/en/insidethelab/supposed-grasshopper-operators-impersonate-israeli-gov-private-companies-deploy-open-source-malware/

TATA COMMUNICATIONS

Critical GeoServer vulnerability demands urgent action

A critical vulnerability, CVE-2024-36401, that exposes systems to potential remote code execution attacks has been identified in GeoServer open-source software platform. This vulnerability is rated 9.8 on the CVSS scale, indicating a critical risk. The severe flaw stems from the GeoTools library and impacts all GeoServer versions. Users are urged to take immediate action.

Experts recommend two ways to mitigate the risk of CVE-2024-36401. The first option is a permanent fix by updating to GeoServer versions 2.24.4, 2.25.2 or 2.23.6. This ensures the system is patched against the vulnerability. The second option is a temporary workaround that removes the gt-complex-x.y.jar file from GeoServer installation. While this will eliminate the vulnerable code, it is important to note that it may also disrupt certain functionalities that depend on the gt-complex module.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://securityonline.info/cve-2024-36401-cvss-9-8-urgent-patch-needed-for-geoserver-rce-vulnerability/

Networks protected by Juniper SRX firewalls at risk

A new vulnerability (CVE-2024-21586) exposes Juniper SRX firewalls to remote attacks. This critical flaw allows attackers to crash the device's Packet Forwarding Engine (PFE), causing a denial-of-service (DoS) condition. The CVE-2024-21586 vulnerability impacts Junos OS versions running on the SRX Series firewall. Although Juniper has not identified active exploitation, there have been reports of incidents in production environments.

To address this security risk, Juniper Networks strongly recommends all users immediately upgrade their Junos OS to the latest patched versions to protect against potential attacks.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Juniper Junos

Source - https://securityonline.info/cve-2024-21586-juniper-srx-vulnerability-leaves-networks-open-to-attack/

RADNET64 issues threat to law enforcement agencies

In a move escalating tensions, hacktivist group RADNET64 has set its sights on Indian law enforcement agencies. Following their recent cyberattacks on Indian banks, the group announced via Telegram that the Indian police will be the primary target of their next operation. Indian authorities have responded to the threat and are preparing for potential distributed denial-of-service (DDoS) attacks. The motives behind these attacks remain unclear.

RADNET64 employs hacktivism and DDoS attacks to disrupt operations and expose perceived injustices. The group's activities highlight the growing threat of politically motivated cyberattacks in India.

ATTACK TYPE	Hacktivism, DDoS	**SECTOR**	Government, military, law
REGION	India	**APPLICATION**	Generic

Source - https://www.thehackerwire.com/hacker-group-radnet64-breaches-multiple-indian-government-websites/

Volcano Demon ransomware threat targets companies

Security experts have warned about a new ransomware group, Volcano Demon, actively targeting organisations. The group has been linked to several attacks over the past two weeks, primarily targeting manufacturing and logistics companies globally. Volcano Demon executes on both Windows workstations and servers by leveraging common administrative credentials. Once gaining access to victim networks, the ransomware deploys LukaLocker to encrypt files and extract data employing a double extortion tactic.

This group operates differently from many ransomware gangs by using phone calls to leadership and IT executives to demand ransom payments. Security researchers urge organisations to remain vigilant and implement strong cybersecurity measures to protect against this evolving threat.

ATTACK TYPE	Ransomware	**SECTOR**	Manufacturing, logistics, shipping
REGION	Global	**APPLICATION**	Windows

Source - https://www.halcyon.ai/blog/halcyon-identifies-new-ransomware-operator-volcano-demon-serving-up-lukalocker

Golang botnet Zergeca can unleash DDoS attacks

A new Golang-based botnet called Zergeca poses a serious threat. Cybersecurity analysts report that this sophisticated botnet can conduct distributed denial-of-service (DDoS) attacks, making it a powerful tool for cybercriminals. Its modular design allows it to establish persistence on infected devices, function as a proxy server, eliminate competing malware, and control infected devices (zombies) for malicious purposes. This versatility makes it a significant threat to a wide range of sectors.

Zergeca uses DNS-over-HTTPS (DoH) and a lesser-known library called Smux for communication. These features allow Zergeca to evade detection. Experts indicate that more sophisticated and dangerous versions of Zergeca can evolve. Organisations must update their software and implement strong security measures to detect and block malicious traffic.

ATTACK TYPE	Malware, DDOS	**SECTOR**	Information technology, healthcare, manufacturing, construction, government, oil and gas, energy, BFSI, aviation, telecommunications
REGION	Canada, Germany, United States	**APPLICATION**	Windows

Source - https://thehackernews.com/2024/07/new-golang-based-zergeca-botnet-capable.html

OpenStack patches critical flaw exposing cloud data

The OpenStack Foundation has released a security advisory regarding a critical vulnerability CVE-2024-32498 (CVSS 8.8). This flaw allows attackers who already have access to the system to steal sensitive data from OpenStack deployments across all sectors globally. This vulnerability affects multiple core components of OpenStack cloud infrastructure, such as Cinder, Nova, and Glance services.

OpenStack Foundation has released patches to address this security vulnerability. Users are urged to immediately fortify their deployments with the latest patched versions of Cinder, Nova, and Glance to mitigate the risk of data breaches.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://securityonline.info/cve-2024-32498-critical-openstack-flaw-exposes-cloud-data-to-attackers/

Apache fixes critical source code disclosure vulnerability

The Apache Software Foundation has issued a special security advisory about a critical code disclosure vulnerability (CVE-2024-39884) in its widely used Apache HTTP Server. This flaw stemmed from a regression in handling legacy content-type configurations, potentially exposing source code on affected servers. Attackers could exploit this flaw to execute DoS attacks, steal sensitive information, or gain unauthorised access.

The Apache Software Foundation has issued patches for various vulnerabilities in the Apache HTTP Server. Users of the Apache HTTP Server are urged to immediately upgrade to version 2.4.61 to mitigate the risk of these vulnerabilities.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Apache Software Foundation Apache HTTP Server

Source - https://securityaffairs.com/165422/security/apache-source-code-disclosure-flaw-apache-http-server.html

TATA COMMUNICATIONS

Microsoft SmartScreen flaw exploited in malware attacks

Cybercriminals are actively exploiting a vulnerability in Microsoft SmartScreen (CVE-2024-21412) to deploy malware. This vulnerability allows attackers to bypass SmartScreen's security checks, putting users at risk of downloading malware onto their devices. The criminals employ tactics such as sending deceptive emails with lures like healthcare, transportation, or tax notices to trick users into clicking malicious links.

The campaign leverages advanced malware such as Lumma and Meduza Stealer, indicating how the attackers have evolved in their tactics. Users are urged to be vigilant of suspicious emails and to strictly avoid clicking on any links or downloading attachments from such emails.

ATTACK TYPE	Malware, vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Windows

Source - https://cybersecuritynews.com/hackers-exploit-microsoft-smartscreen-stealer-malware/

Unpatched Gogs flaws leave code exposed to attackers

Gogs, a popular open-source Git service, is at risk due to critical unpatched vulnerabilities. The vulnerabilities, according to cybersecurity researchers, are CVE-2024-39930 (CVSS score: 9.9), CVE-2024-39931 (CVSS score: 9.9), CVE-2024-39932 (CVSS score: 9.9), and CVE-2024-39933 (CVSS score: 7.7). Among these four vulnerabilities, three are considered highly severe that could allow attackers to infiltrate vulnerable systems. Exploiting these vulnerabilities, attackers could steal or delete source code and even install malicious backdoors.

Experts state that Gogs instances running on Debian and Ubuntu are at high risk, while those running on Windows are safe. Users of Gogs are advised to exercise caution until a patch is released.

ATTACK TYPE	Vulnerability	**SECTOR**	All
REGION	Global	**APPLICATION**	Generic

Source - https://thehackernews.com/2024/07/critical-vulnerabilities-disclosed-in.html

TATA COMMUNICATIONS

TATA

Visit one of our **Cyber Security Response Centres** to learn how we can help your enterprise navigate the complexities of today's cyber threat landscape.

Book your visit