TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MARCH 12TH, 2024

TATA COMMUNICATIONS

THREAT INTELLIGENCE ADVISORY REPORT

As technology advances, the strategies of cybercriminals and malicious entities also evolve. These adversaries tirelessly exploit vulnerabilities using advanced hacking methods and deceptive social engineering tactics. A single breach, no matter where it occurs, can have extensive global repercussions. Thus, it is crucial to remain vigilant and proactive in combating these threats.

Improve your organisation's cybersecurity readiness with Tata Communications' weekly threat intelligence advisory report. By accessing up-to-date insights on emerging security threats, you can take informed, proactive measures to strengthen your defences and minimise potential risks.

US and allies warn of the rising threats from Russian cloud-based cyberattacks

The Five Eyes (FVEY) intelligence-sharing alliance, composed of Australia, Canada, New Zealand, the United Kingdom, and the United States, has issued alerts regarding the activities of advanced persistent threat-29 (APT29), also known as Midnight Blizzard, the Dukes, or Cozy Bear. This threat group, associated with Russia's Foreign Intelligence Service or Sluzhba Vneshney Razvedki (SVR), employs sophisticated tactics to compromise security, particularly targeting cloud services like Microsoft 365 and Exchange Online through methods such as brute force attacks and password spraying. These pose significant risks to cloud-based infrastructures.

In response, FVEY recommends stringent security measures, including multi-factor authentication (MFA), strong passwords, deactivation of dormant accounts, and strict device registration policies. Additionally, deploying canary accounts is advised to enhance the early detection of suspicious activities and fortify defence mechanisms against APT29's intricate cyber strategies.

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

Source - https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

BlackCat ransomware threatens US healthcare, FBI and CISA warn

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) have jointly issued an alert, urging U.S. healthcare organisations to maintain vigilance against the actions of the ALPHV/Blackcat ransomware group. Stemming from the DarkSide and BlackMatter lineage, BlackCat has aggressively targeted the healthcare sector since November 2021, resulting in over 60 breaches and extracting more than $300 million in ransoms.

Moreover, a recent attack on UnitedHealth Group's Optum subsidiary impacted Change Healthcare, a vital payment exchange in the U.S. healthcare system. This attack reportedly exploited a vulnerability in a remote access tool, known as ScreenConnect. Though the FBI, CISA, and HHS have not directly linked this incident to their broader warning, they strongly advise healthcare entities to fortify defences against the advancing threat of ransomware and data extortion.

ATTACK TYPE	Ransomware	**SECTOR**	All
REGION	USA	**APPLICATION**	Windows/Linux

Source - https://www.bleepingcomputer.com/news/security/fbi-cisa-warn-us-hospitals-of-targeted-blackcat-ransomware-attacks/

TATA COMMUNICATIONS

Black Basta and Bl00dy ransomware groups are exploiting an unpatched ScreenConnect vulnerability

The Black Basta and Bl00dy ransomware groups, along with other cybercriminals, exploit two recently patched vulnerabilities in ConnectWise ScreenConnect, a widely-used remote desktop access software. These common vulnerabilities and exposures (CVE), identified as CVE-2024-1709 and CVE-2024-1708, entail a critical authentication bypass and a path traversal bug. Exploiting these, attackers impersonate administrators and seize control of compromised systems.

Following the release of a proof-of-concept exploit named SlashAndGrab, exploitation of these vulnerabilities surged, resulting in malicious activities like malware deployment and network breaches. Black Basta conducts reconnaissance to identify valuable targets, escalating privileges for higher access levels. They deploy Cobalt Strike beacons for a stealthy presence. Moreover, the threat actors are leveraging these gaps to install the XWorm malware, facilitating remote access and data exfiltration. ConnectWise urges users to upgrade to ScreenConnect version 23.9.8 promptly to shield against evolving ransomware threats.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/black-basta-bl00dy-ransomware-gangs-join-screenconnect-attacks/

TATA COMMUNICATIONS

Phobos ransomware targets US infrastructure, CACTUS launches a coordinated attack

Recent U.S. cybersecurity alerts reveal a notable surge in Phobos ransomware attacks across critical sectors such as government, emergency services, and healthcare since 2019. This ransomware, alongside variants like Eking and Eight, typically breaches networks through phishing campaigns or exploiting vulnerabilities in the remote desktop protocol (RDP). Once inside, attackers deploy various tools and alter system registries to maintain control.

Concurrently, the CACTUS e-crime group orchestrates coordinated ransomware attacks, targeting the virtualisation infrastructure of companies. This includes systems like Hyper-V and VMware ESXi hosts, crucial for managing multiple virtual machines on a single physical server. The parallel operations of Phobos and CACTUS highlight a concerning trend in cybercrime, as they aim at intricate and critical virtualisation environments beyond traditional Windows systems.

ATTACK TYPE	Ransomware	**SECTOR**	Government, hospitals and healthcare
REGION	Global	**APPLICATION**	VMWare ESXi, Windows

Source - https://www.bitdefender.com/blog/businessinsights/cactus-analyzing-a-coordinated-ransomware-attack-on-corporate-networks/
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060

Iranian hackers attack Middle Eastern aerospace and defence firms

The Iranian Revolutionary Guard Corps (IRGC)-linked group UNC1549 is conducting targeted cyberattacks on the aerospace and defence sectors in Israel, the United Arab Emirates, and other Middle Eastern countries. Employing spear phishing and watering-hole strategies, they introduce backdoor programmes, particularly MINIBIKE and MINIBUS, to infiltrate and monitor systems. Mandiant, a premier cybersecurity agency within Google Cloud, has detected this sophisticated campaign, revealing the assailants' substantial resources and advanced techniques, posing significant challenges in detection and accurate identification.

Furthermore, Mandiant's comprehensive investigation unveils UNC1549's in-depth reconnaissance, including tailored phishing emails and counterfeit job advertisements to target defence and aerospace industry personnel. This strategic approach aims to gather critical data, potentially impacting national security. Mandiant attributes these activities to UNC1549 with medium confidence, suggesting a likely but intricate web of cyber espionage activities.

ATTACK TYPE	Malware, cyberespionage	**SECTOR**	Defence industry, aviation, defence and space manufacturing
REGION	Middle East, India, Albania, Israel, Turkey, United Arab Emirates	**APPLICATION**	Windows

Source - https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east

Chinese cyber actors infiltrate Ivanti VPNs with new malware

Chinese cyber espionage groups UNC5325 and UNC3886 are exploiting vulnerabilities in Ivanti Connect Secure Virtual Private Network (VPN), notably CVE-2024-21893, deploying malware such as LITTLELAMB.WOOLTEA and PITSTOP, along with VIRTUALPITA and VIRTUALPIE. While UNC5325 focuses on exploiting the VPN's vulnerabilities to gain network persistence, UNC3886 targets the defence and technology sectors, demonstrating a coordinated effort to penetrate and maintain presence within key network infrastructures.

Following the patching of initial vulnerabilities by Ivanti, these groups quickly adapted their modus operandi, using new exploits and malware to maintain access and circumvent detection. They employ web shells like BushWalk and modify open-source tools to exploit vulnerabilities in Ivanti's systems, overcoming challenges such as encryption key mismatches. Meanwhile, the Volt Typhoon, potentially China-sponsored, is targeting critical US infrastructure with discreet tactics for extended espionage.

ATTACK TYPE	Vulnerability, malware	**SECTOR**	Information technology, defence industry, telecommunications
REGION	Asia, United States	**APPLICATION**	Ivanti

Source - https://www.mandiant.com/resources/blog/investigating-ivanti-exploitation-persistence

Backdoor threat targets Europeans connected to Indian diplomatic events

SPIKEDWINE, a new threat actor, actively targets European officials linked to Indian diplomatic missions using a backdoor called WINELOADER. This campaign employs a deceptive hypertext markup language (HTML) application within a portable document format (PDF), posing as an invitation from the Indian Ambassador for a wine-tasting event to distribute malware.

Discovered in Latvia, this deceptive PDF has been part of the threat landscape since at least July 2023, indicating a sustained espionage operation. The PDF contains a deceptive link, disguised as a questionnaire. Clicking this link activates an HTML application, using obfuscated JavaScript to download WINELOADER. This backdoor executes commands from the command and control (C2) server, self-injects into other processes, and adjusts beaconing intervals to avoid detection. Additionally, threat actors are utilising compromised websites for the C2 framework and payload hosting to enhance the campaign's stealthiness.

ATTACK TYPE	Malware	**SECTOR**	Government
REGION	Europe	**APPLICATION**	Windows

Source - https://www.zscaler.com/blogs/security-research/european-diplomats-targeted-spikedwine-wineloader

LockBit resurfaces with fresh encryptors and servers

The LockBit ransomware gang swiftly resumed operations after 'Operation Cronos' was disrupted by the National Crime Agency (NCA), FBI, and Europol. This resulted in the seizure of their infrastructure and decryptors. They promptly launched a new data leak site, accompanied by a detailed note sent to the FBI. In the note, they claimed that a hypertext preprocessor (PHP) bug enabled law enforcement to infiltrate servers, suggesting a possible connection to a known vulnerability like CVE-2023-3824 or even a zero-day exploit.

Following the disruption, LockBit upgraded encryptors and infrastructure, indicating a determined comeback. While they previously boasted around 180 affiliates conducting attacks, the precise number engaged post-disruption remains uncertain. Nevertheless, LockBit actively seeks experienced penetration testers to enhance their operations and potentially amplify the frequency and scale of their ransomware attacks.

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

Source - https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-to-attacks-with-new-encryptors-servers/

New Bifrost malware poses sneaky threats to Linux users

The BIFROSE remote access trojan (RAT), also known as Bifrost, has introduced a new Linux variant. Since 2004, BlackTech, a hacking group linked to China, has used it to target entities in Japan, Taiwan, and the USA. BlackTech has enhanced BIFROSE by adding backdoors like KIVARS and XBOW for cyber-espionage.

Bifrost spreads through email attachments or malicious websites, extracting critical data like hostnames and IP addresses. The updated version communicates with a C2 server via a domain resembling VMware, using typosquatting to avoid detection. Moreover, recent research has found a surge in Bifrost's activity, with 104 new samples showing improvements such as a Taiwan-based domain name system (DNS) resolver and support for advanced RISC Machine (ARM) architecture. These advances indicate an expansion in Bifrost's operational reach and improved concealment methods.

ATTACK TYPE	Malware	**SECTOR**	All
REGION	Global	**APPLICATION**	Linux

Source - https://unit42.paloaltonetworks.com/new-linux-variant-bifrost-malware/

#OpIndiaV4: Cyber threats are targeting the Indian infrastructure

Tata Communications' Cyber Threat Intelligence Team has uncovered a series of attacks by multiple hacktivist groups operating under the banner of Operation India Version 4 (#OpIndiaV4), targeting India's digital framework. These threat actors focus on governmental and educational websites, employing specific cyberattack methods to exploit vulnerabilities. Their modus operandi includes structured query language (SQL) injection and distributed denial of service (DDoS) attacks.

To counteract these threats, India's cybersecurity teams need to collaborate and implement robust defence mechanisms. Understanding and mitigating SQL injection requires securing database inputs while defending against DDoS attacks involves monitoring traffic and implementing filters or barriers. By proactively strengthening their cybersecurity posture, Indian institutions can better protect against these targeted threats, ensuring the security and resilience of the nation's digital infrastructure.

ATTACK TYPE	Hacktivism, DDOS	**SECTOR**	All
REGION	India	**APPLICATION**	Generic

Source - N/A

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