TATA COMMUNICATIONS

YOUR WEEKLY THREAT INTELLIGENCE ADVISORY

DATE: MAY 7, 2024

THREAT INTELLIGENCE ADVISORY REPORT

The digital revolution has made robust IT infrastructure a necessity for organisational security. Businesses, individuals, and governments are increasingly investing in cybersecurity to safeguard their assets and data from hackers. Think of cybersecurity as a digital armour. Effective policies and infrastructure work together to shield computer systems and networks from unauthorised access or attacks.

Subscribe to Tata Communications' weekly threat intelligence report to keep pace with cyber threats. Access actionable insights into emerging cyber risks and fortify your defences effectively.

INTRODUCTION | CORALRAIDER DISTRIBUTES MALWARE | HACKERS SPREAD GUPTIMINER MALWARE | HELLOKITTY REBRANDS TO HELLOGOOKIE | PIKABOT MALWARE SURGES | FROZEN#SHADOW TARGETS ENTERPRISES | ARCANEDOOR ATTACKS GOVERNMENT NETWORKS | GAMBLING ADS SPREAD MALWARE | TROJAN BROKEWELL THREATENS BFSI | FAKE JOB ADS DEPLOY RAT | PAKISTANI APTS ATTACK INDIAN GOVERNMENT ENTITIES

Suspected CoralRaider campaign distributes malware

Experts have discovered a sophisticated malware distribution campaign operated by the Vietnamese threat actor CoralRaider. Since February 2024, the campaign has targeted global businesses by deploying three types of malware—CryptBot, LummaC2, and Rhadamanthys—via CDN cache domains to evade security measures. Researchers have also found a new PowerShell command-line parameter within the LNK file, designed to evade antivirus software and facilitate the download of the final payload onto victims' systems. The campaign aims to infiltrate systems across various sectors, including call centres and civil defence organisations, by employing advanced techniques like booby-trapped ZIP archives and Windows Shortcut files.

Analysts express moderate confidence in CoralRaider’s involvement, citing similarities in tactics, techniques, and procedures (TTPs) with their past Rotbot campaign. This includes shared elements like using Windows Shortcut files for initial access, intermediate PowerShell decryption processes and payload download scripts, and the FoDHelper method to bypass User Access Controls (UAC). Organisations can use solutions such as Secure Endpoint, Secure Web Appliance, and Secure Email to mitigate this threat. Open-source Snort Subscriber Rule Set and ClamAV detections can also be leveraged for added security.

ATTACK TYPE	Malware	SECTOR	All
REGION	Japan, UK, Ecuador, Egypt, Germany, Nigeria, Norway, Pakistan, Philippines, Poland, Syria, Turkey, United States	APPLICATION	Windows

Source - https://blog.talosintelligence.com/suspected-coralraider-continues-to-expand-victimology-using-three-information-stealers/

INTRODUCTION | CORALRAIDER DISTRIBUTES MALWARE | HACKERS SPREAD GUPTIMINER MALWARE | HELLOKITTY REBRANDS TO HELLOGOOKIE | PIKABOT MALWARE SURGES | FROZEN#SHADOW TARGETS ENTERPRISES | ARCANEDOOR ATTACKS GOVERNMENT NETWORKS | GAMBLING ADS SPREAD MALWARE | TROJAN BROKEWELL THREATENS BFSI | FAKE JOB ADS DEPLOY RAT | PAKISTANI APTS ATTACK INDIAN GOVERNMENT ENTITIES

Hackers hijack antivirus updates to spread GuptiMiner malware

The "GuptiMiner" malware campaign has emerged as a highly sophisticated threat, exploiting vulnerabilities in the eScan antivirus update process to infiltrate corporate networks. This complex attack, potentially linked to the North Korean APT group, Kimsuky, deploys backdoors and the XMRig cryptocurrency miner on infected devices. GuptiMiner's advanced tactics include performing DNS requests to attacker-controlled servers and extracting payloads from harmless images. The malware distributes two variants of backdoors, facilitating lateral movement within networks and targeting stored private keys and crypto wallets. The final payload includes XMRig, enhancing the operation's stealth and impact.

Experts promptly notified both eScan antivirus and India CERT about the vulnerability, leading to its resolution on 31st July 2023. While eScan has patched the vulnerability, the true scope of GuptiMiner's operation may still be unfolding.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://decoded.avast.io/janrubin/guptiminer-hijacking-antivirus-updates-for-distributing-backdoors-and-casual-mining/

HelloKitty ransomware rebrands as HelloGookie

The ransomware operator behind HelloKitty has rebranded as "HelloGookie", releasing sensitive information, including passwords from CD Projekt's leaked source code, Cisco's network data, and decryption keys for previous campaigns. The move coincides with the launch of a new dark web portal for HelloGookie, featuring internal documents from a 2022 Cisco cyberattack. The leaked CD Projekt source code has been compiled by developers already, with Witcher 3 development builds surfacing online.

HelloKitty's history includes high-profile attacks on CD Projekt Red and the creation of a Linux-focused variant targeting VMware ESXi. Collaborative ties between HelloKitty's operator, Gookee/kapuchin0, and the Yanluowang ransomware group have also come to light. The return of HelloGookie raises concerns over potential operational success and notoriety levels reminiscent of HelloKitty's previous exploits.

ATTACK TYPE	Ransomware	SECTOR	All
REGION	Global	APPLICATION	Generic

Source - https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-rebrands-releases-cd-projekt-and-cisco-data/

Malware threat Pikabot on the rise

Sophisticated malware Pikabot which leverages a core module for executing cyberattacks has emerged as the latest cybersecurity threat. Employing advanced obfuscation, intricate techniques such as injecting code into legitimate processes, and diverse campaign methods, including HTML files and Excel documents, Pikabot executes malicious activities with stealth. Akin to QakBot trojan, it allows attackers to execute arbitrary commands and evade detection by security tools.

Distributed mainly via geolocalised spam emails containing links to malicious zip files, Pikabot has already found a place in the arsenals of ransomware gangs like BlackBasta. The gang uses the malware to establish encrypted communication channels with command and control (C&C) servers. Pikabot can also provide gangs with in-depth insights into compromised systems, helping them tailor their ransomware for maximum impact. To mitigate this multifaceted threat effectively, organisations must deploy Endpoint Detection and Response (EDR) platforms combined with proactive threat-hunting.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.malwarebytes.com/blog/business/2024/03/pikabot-malware-on-the-rise-what-organizations-need-to-know

INTRODUCTION | CORALRAIDER DISTRIBUTES MALWARE | HACKERS SPREAD GUPTIMINER MALWARE | HELLOKITTY REBRANDS TO HELLOGOOKIE | PIKABOT MALWARE SURGES | FROZEN#SHADOW TARGETS ENTERPRISES | ARCANEDOOR ATTACKS GOVERNMENT NETWORKS | GAMBLING ADS SPREAD MALWARE | TROJAN BROKEWELL THREATENS BFSI | FAKE JOB ADS DEPLOY RAT | PAKISTANI APTS ATTACK INDIAN GOVERNMENT ENTITIES

FROZEN#SHADOW attacks target domain takeover

Experts have discovered a complex cyberattack called FROZEN#SHADOW which uses SSLoad malware, ConnectWise ScreenConnect, and Cobalt Strike implants to allow attackers to pivot and gain control over the entire network domain. The SSLoad malware has been designed to infiltrate systems, collect sensitive data, pass on the findings to the operators, and introduce additional malware. Once inside the system, it sets up payloads and multiple backdoors to avoid detection. The campaign also uses the Cobalt Strike toolkit and ConnectWise ScreenConnect for remote access. This global assault targets organisations indiscriminately, using deceptive JavaScript files and macro-laden documents to compromise systems, posing a threat to organisational security and data integrity.

The attack, initiated through phishing emails containing a single redirect link, has affected victims across Asia, Europe, and the Americas. Subsequently, attackers established dominance within victim Windows domains, highlighting the importance of user awareness and robust security measures to mitigate such assaults effectively. Caution should be exercised with unsolicited emails, particularly those that arrive unexpectedly or create a sense of urgency.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Windows

Source - https://www.securonix.com/blog/securonix-threat-research-security-advisory-frozenshadow-attack-campaign/

ArcaneDoor campaign targets perimeter network devices

The ArcaneDoor malware campaign associated with the state-sponsored group UAT4356 (also known as Storm-1849) exploited two zero-day vulnerabilities in Cisco devices to deploy sophisticated backdoor Line Runner and Line Dancer. These tools manipulate network configurations and intercept data, potentially enabling lateral movements within targeted networks.

Prompted by a customer's security concerns regarding their Cisco Adaptive Security Appliances (ASA), the organisation launched an investigation uncovering vulnerabilities CVE-2024-20353 and CVE-2024-20359. This discovery led to urgent patching directives from the U.S. Cybersecurity and Infrastructure Security Agency (CISA). The use of customised tools indicates a focus on spying, while the deep understanding of the targeted devices highlights the involvement of a sophisticated state-sponsored actor targeting perimeter network devices. The timeline of the attack, stretching back to November 2023, suggests ongoing development and testing of capabilities. Defenders must patch vulnerabilities and monitor for signs of compromise, including unexpected reboots and gaps in logging data.

ATTACK TYPE	Vulnerability, Malware	SECTOR	Government
REGION	Global	APPLICATION	Cisco Adaptive Security Appliance (ASA), Cisco FirePOWER, Cisco ASA

Source - https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/

Malware attacks domestic servers through gambling ads

A recent cybersecurity investigation uncovered a sophisticated malware campaign aimed at local web servers to promote illegal gambling sites. Experts confirmed the distribution of the malware designed to induce connections to these prohibited gambling advertising sites, particularly targeting domestic web servers. The attackers initially breached poorly managed Windows Internet Information Services (IIS) servers, deploying a range of malicious tools including a meterpreter backdoor, port forwarding tool, and IIS module malware.

This malware, installed via improper server management, manipulated HTTP responses to redirect users to gambling sites based on specific search queries. It exploited server vulnerabilities, demonstrating the necessity for strict server management and continuous security updates. As attackers increasingly utilise search engines like Shodan and FOFA to identify vulnerable targets, proactive asset identification and ongoing security patch management are essential for corporate security personnel.

ATTACK TYPE	Malware	SECTOR	All
REGION	Global	APPLICATION	Microsoft Internet Information Services (IIS)

Source - https://asec.ahnlab.com/ko/64558/

Android trojan Brokewell threatens banking security

A recent cybersecurity analysis has uncovered a new Android banking trojan named "Brokewell", designed to target users primarily in Germany through advanced tactics such as overlay attacks and keylogging. This malware, attributed to Baron Samedit of the Brokewell Cyber Labs, is distributed via a deceptive website posing as a Chrome update page.

Once installed, Brokewell exploits Android's Accessibility Service to conduct malicious activities like screen recording and cookie theft, posing a significant threat to mobile banking security. The trojan's ongoing development, indicated by frequent updates and international code references, hints at potential expansion beyond its current focus. Brokewell is expected to be marketed as a rental service on underground platforms, drawing the attention of cybercriminals to instigate new attacks in various geographical areas. Multi-dimensional fraud detection strategies, incorporating factors like device characteristics, behavioural tendencies, and user-specific identity risks can identify and mitigate potential fraud stemming from emerging malware strains like Brokewell.

ATTACK TYPE	Malware	SECTOR	BFSI
REGION	Germany	APPLICATION	Android

Source - https://www.threatfabric.com/blogs/brokewell-do-not-go-broke-by-new-banking-malware https://cyble.com/blog/brokewell-a-new-android-banking-trojan-targeting-users-in-germany/

Lazarus Group deploys RAT through fake job ads

North Korea's Lazarus Group has been using fake job advertisements to deploy a new remote access trojan, Kaolin RAT, with features that go beyond traditional RAT operations. Dubbed "Operation Dream Job", this multi-stage attack modifies file timestamps, executes DLL files from its command server, and delivers the FudModule rootkit via a patched vulnerability (CVE-2024-21338) for kernel-level access. Investigation revealed a thorough attack chain from the infection vector to the deployment of the "FudModule 2.0" rootkit through a zero-day Admin -> Kernel exploit.

This 2023 discovery highlighted Lazarus' sophistication, targeting specific individuals with technical backgrounds in Asia. The attackers' resourcefulness is evident in their deployment of file-less malware and meticulous toolset preparation, indicating careful victim selection. The extensive attack chain emphasises Lazarus' continuous adaptation and substantial investment in complex attack methodologies.

ATTACK TYPE	Malware	SECTOR	All
REGION	Asia	APPLICATION	Windows

Source - https://decoded.avast.io/luiginocamastra/from-byovd-to-a-0-day-unveiling-advanced-exploits-in-cyber-recruiting-scams/

INTRODUCTION | CORALRAIDER DISTRIBUTES MALWARE | HACKERS SPREAD GUPTIMINER MALWARE | HELLOKITTY REBRANDS TO HELLOGOOKIE | PIKABOT MALWARE SURGES | FROZEN#SHADOW TARGETS ENTERPRISES | ARCANEDOOR ATTACKS GOVERNMENT NETWORKS | GAMBLING ADS SPREAD MALWARE | TROJAN BROKEWELL THREATENS BFSI | FAKE JOB ADS DEPLOY RAT | PAKISTANI APTS ATTACK INDIAN GOVERNMENT ENTITIES

Pakistani APTs intensify attacks on Indian government entities

Pakistan-linked APT groups like SideCopy and APT36 have intensified cyberattacks against Indian government entities, employing sophisticated malware such as AllaKore and Crimson RATs in multiple campaigns. These groups utilise tactics like spear-phishing and compromised domains, indicating a persistent cybersecurity threat. Additionally, there has been a surge in unauthorised access sales and high-profile ransomware attacks in India, increasing concerns about the cyber threat landscape.

SideCopy, known for targeting Indian defence and government entities since 2019, utilises a range of RATs, while its parent group Transparent Tribe (APT36) employs payloads like Crimson RAT. Recent campaigns have witnessed the deployment of custom AllaKore variants via compromised domains, showcasing evolving attack strategies. Moreover, new spear-phishing campaigns like Operation RusticWeb and FlightNight have emerged, further aggravating cybersecurity challenges in India.

ATTACK TYPE	Malware, Cyberespionage	SECTOR	Government
REGION	India	APPLICATION	Windows

Source - https://www.seqrite.com/blog/pakistani-apts-escalate-attacks-on-indian-gov-seqrite-labs-unveils-threats-and-connections/

INTRODUCTION | CORALRAIDER DISTRIBUTES MALWARE | HACKERS SPREAD GUPTIMINER MALWARE | HELLOKITTY REBRANDS TO HELLOGOOKIE | PIKABOT MALWARE SURGES | FROZEN#SHADOW TARGETS ENTERPRISES | ARCANEDOOR ATTACKS GOVERNMENT NETWORKS | GAMBLING ADS SPREAD MALWARE | TROJAN BROKEWELL THREATENS BFSI | FAKE JOB ADS DEPLOY RAT | PAKISTANI APTS ATTACK INDIAN GOVERNMENT ENTITIES

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

All content is provided AS IS and for information purposes only. Tata Communications does not make any representations or warranties of any kind, including completeness, adequacy or accuracy of such information and disclaims all liability in connection with the use of this information. The information contained herein should not be construed as a substitute for professional advice.