Weekly Intelligence Trends/Advisory

3 June 2022

TABLE OF CONTENTS

1. CYFIRMA's Weekly Insights **[NEW]**

1.1 Weekly Attack Type and Trends

Key Intelligence Signals:

- **Attack Type:** Malware Implant, Ransomware, Vulnerabilities & Exploits, Ransomware-as-a-Service (RaaS), Data Leak, Distributed Denial-of-Service (DDoS), Credential Abuse, Spear-Phishing, Account Compromise, Privilege Escalation
- **Objective:** Data Theft, Payload Delivery, Data Encryption, Financial Gains, Unauthorized Access, Resource Exhaustion
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage, Operational Disruption
- **Ransomware – Hive | Malware – ERMAC**
  - **Hive –** One of the ransomware groups.

  Please refer to the trending malware advisory for details on the following:
  - Malware – **ERMAC**

  Behavior - Most of these malware use phishing and social engineering techniques as their initial attack vector. Apart from these techniques, exploitation of vulnerabilities, defence evasion, and persistence tactics are being observed.

1.2 Threat Actor in Focus

Gamaredon Conducts DDoS with Open-source Trojan

Suspected Threat Actors: Gamaredon

- **Attack Type:** DDoS
- **Objective**: Resource Exhaustion
- **Target Technology**: Internet-facing Assets
- **Target Industry**: Unknown
- **Target Geography**: Global
- **Business Impact**: Operational Disruption, Data Loss, Financial Loss

Summary: Researchers suspect that the Russian APT Gamaredon threat actor group could fuel a new wave of DDoS attacks. They found that this group has open-sourced the code of a DDoS Trojan program called "LOIC " to carry out DDoS attacks. During monitoring Gamaredon's activity researchers also found multiple attack chains including – phishing emails, remote template injection, malicious scripts with self-extracting programs, Wiper payloads, and registry modification for scheduled tasks among others. The malicious code distributed by the APT group includes hardcoded IP addresses and ports for the targets.

Insights:

- The malware samples observed by researchers seem to have been compiled in early March this year – shortly after the Russian invasion of Ukraine had taken place. After the military conflict, a new trend of disruptive attacks is gaining momentum including wiper attacks and DDoS. Ukraine is already facing the brunt of these DDoS attacks; however,

they are not the only one. Recently, the Italian Computer Security Incident Response Team also alerted about the potential risk of DDoS attacks against its national entities.

Indicators of Compromise
Kindly refer to the IOCs Section to exercise controls on your security systems.

1.3 Major Geopolitical Developments in Cybersecurity

The Quad to Strengthening Cybersecurity in Software, Supply Chains

The Quad nations Australia, the United States, India, and Japan have committed to several initiatives in cybersecurity concerning software, supply chain, and user data during the recent meeting in Tokyo.

The countries' leaders including US President – Joe Biden, Australian Prime Minister – Anthony Albanese, Indian Prime Minister – Narendra Modi, and Japanese Prime Minister – Fumio Kishida stated in a joint statement, "their renewed commitment to deepening cooperation in addressing some pressing challenges currently facing the Indo-Pacific region." This includes issues such as the ongoing COVID-19 pandemic, climate change, infrastructure, peace and stability (due to the Ukraine invasion), and cybersecurity.

The White House said, "In an increasingly digital world with sophisticated cyber threats we recognize an urgent need to take a collective approach to enhance cybersecurity. To achieve the Quad Leaders' vision of a free and open Indo-Pacific, they committed to bolstering defences of critical infrastructure by sharing threat information, identifying and evaluating risks in digital supply chains, and among other cybersecurity initiatives that will have benefits to all users.

The Quad also aims to form a Quad Cybersecurity Partnership. The group will also initiate "capacity building programs" for the region and launch a Quad Cybersecurity Day to "help individual internet users across our nations, the Indo-Pacific region, and beyond to better protect themselves from cyber threats."

1.4 Rise in Malware/Ransomware and Phishing

Travira Air Impacted by Hive Ransomware

- **Attack Type**: Ransomware, Data Exfiltration
- **Target Industry:** Aviation
- **Target Geography:** Indonesia
- **Ransomware**: Hive
- **Objective**: Data Theft, Data Encryption, Financial Gains

- **Business Impact**: Data Loss, Financial Loss, Reputational Damage

Summary: CTI observed **Travira Air** – a charter airline server operator based out of Jakarta, Indonesia – being impacted by HiveLeaks ransomware. The ransomware group claimed the airline provider as one of their victims by disclosing the update on their dedicated leak site HiveLeaks on 28 May. The update also claims the encryption of the company's data was carried out on 12 May. At the time of CTI's observation, no sample evidence or any links to exfiltrated have been published by the ransomware group. It appears that the ransomware group is awaiting ransom negotiation and in case of non-compliance to their ransom demand, the group will likely publish all exfiltrated data on their dedicated leak site for anyone to download.

The following screenshot was observed published on the dark web:

Source: Dark Web

Insights:

- The Hive ransomware was first observed in June 2021 and suspected of running as affiliate-based ransomware similar to the majority of the ransomware groups at current times. The ransomware group employs a wide array of tactics, techniques, and procedures (TTPs) in their attacks. They leverage multiple methods to compromise an organization's networks, which include phishing emails with malicious attachments to foothold into the network and exploiting Remote Desktop Protocol (RDP) for lateral movement.
- It uses a double-extortion strategy for attacks. The attackers threaten to publish the exfiltrated data (victim data) if victims are not ready to pay the ransom.
- The ransomware operators implemented a new IPfuscation (obfuscation) technique to conceal the Cobalt strike beacon payload. The payload was disguised as an array of ASCII IPv4 addresses in the malware executable binary. Code obfuscation is a technique that helps threat actors hide the malicious code from security analysts or security software to evade detection.
- The Hive ransomware operators changed its VMware ESXi Linux encryptor to the Rust programming language to make it more difficult for security researchers to eavesdrop on

victims' ransom conversations. This feature is implemented from the BlackCat ransomware operation.

1.5 Latest Cyber-Attacks, Incidents, and Breaches

Agency Warns of Widespread Credential Leak on Russian Hacker Forums

- **Attack Type**: Credential Abuse, Unauthorized Access, Spear-Phishing, Ransomware
- **Target Technology:** VPN, Network Devices
- **Target Industry:** Education
- **Target Geography:** United States
- **Business Impact:** Data Loss

Summary: According to a new alert from the FBI, the Russian hacker forums are full of network credentials and virtual private network access of employees from US educational institutions. The agency said these credentials are being advertised widely across hacker forums. Just in May 2021, the FBI found approximately 36,000 email and password combinations for accounts related to domains ending with .edu in public instant messaging platforms used by cybercriminals. The agency suggests most of these credentials are likely acquired by the prevalent attacks on US colleges and universities over the past few years including spear-phishing, ransomware, and other types of cyberattacks. As of January 2022, network credentials for sale or public access have been offered in Russian hacker forums for various US-based educational institutions. The prices of these listings range from anywhere between a few to multiple thousand US dollars.

Insights:

- There have been numerous ransomware incidents reported this year alone where multiple education institutes have been targeted. Often the educational institutions are not entirely transparent about ransomware attacks or data exfiltration, neither they are in a position to fulfill the ransom demand when attacked. The majority of education institutions are still recovering from the COVID-19 pandemic and a ransomware attack during this time may turn out to be a final blow. CTI has already observed, one such incident where a 157-year-old Lincoln College in Illinois had to permanently close down after suffering a ransomware attack.

1.6 Vulnerabilities and Exploits

Two Bugs In Strapi Allow Data Exposure

- **Attack Type:** Vulnerabilities & Exploits, Account Compromise, Potential Privilege Escalations
- **Target Technology:** Strapi
- **Vulnerability:** CVE-2022-30617 (CVSS score: 8.8), CVE-2022-30618 (CVSS score: 7.5)
- **Vulnerability Type:** Improper Removal of Sensitive Information Before Storage or Transfer

Summary: In a recent patch update the popular open-source content management system (CMS) Strapi fixed two vulnerabilities that could allow attackers to access sensitive data such as email and password reset tokens. While not as well-known as its competitors which include the

likes of WordPress or Joomla, Strapi is known for its "headless" capability meaning its front end and back end software run separately and it is being used by the some of the major organizations including IBM, NASA, and Walmart.

According to researchers, the vulnerability details access to sensitive information enables a user to compromise other users' accounts by successfully invoking the password reset workflow. In a worst-case scenario, a low-privileged user could get access to a "super admin" account with full control over the Strapi instance and could read and modify any data as well as block access to both the admin panel and API by revoking privileges for all other users.

Insights:

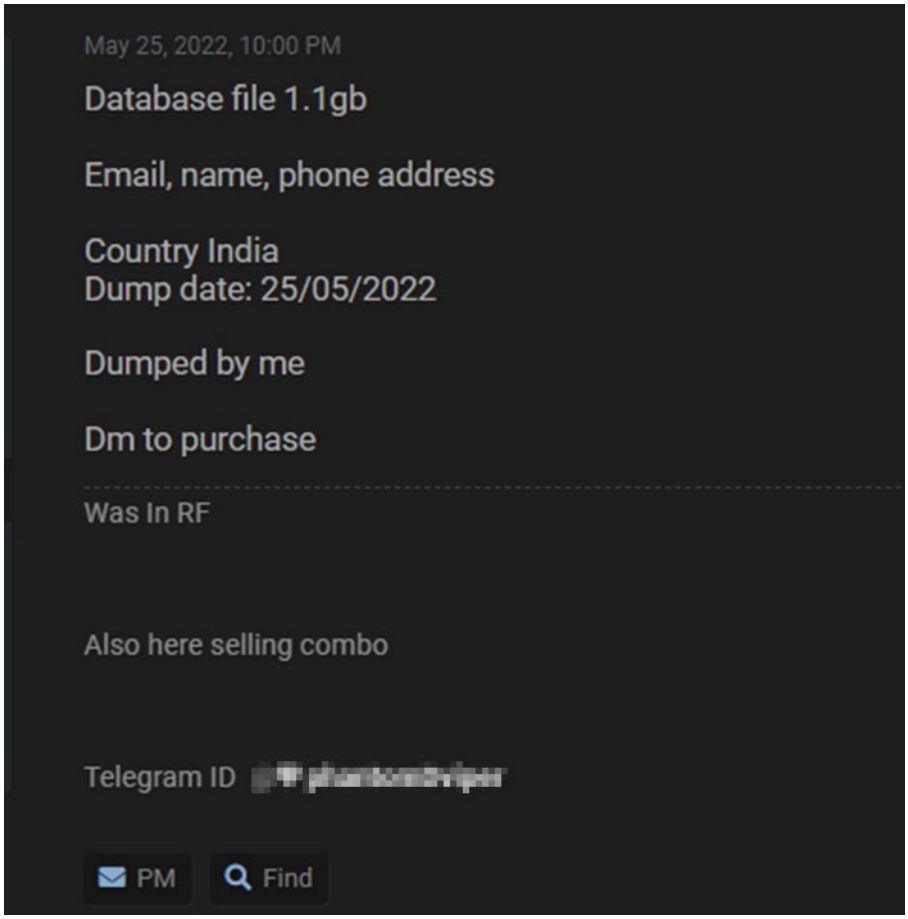
- The latest release of Strapi CMS accounts for approximately 40,000 weekly downloads on NPM and around 25,000 weekly downloads for its older version. Researchers have found the vulnerabilities in the admin panel and state that an account compromise is fairly easy to perform.
- While it is unclear how many instances are currently vulnerable but given the patch was made available in recent weeks, researchers presume it is reasonable that not everyone has upgraded yet.

1.7 Data Leak

Tax Filings APP Data Advertised for Sale

- **Attack Type:** Data Leak
- **Target Industry:** Finance
- **Target Geography:** India
- **Objective:** Data Theft, Financial Gains
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage

Summary: As part of routine threat hunting efforts, CTI has observed potential data of **Tax Filings APP (https://www.taxfilingsapp.com/)** – an online business services platform that allows filling of income tax returns – leaked by an unknown threat actor in one of the underground forums. As per the advertisement, the threat actor claims the stolen database of approximately 1.1 gigabytes has around 475 records that include user details such as the name, email address, and phone number of users. At the time of CTI's observation, no sample evidence was advertised.



Source: Underground Forums

Insights:

- Opportunistic cybercriminals motivated by financial gains are always on the lookout for exposed and vulnerable systems and applications**.** The majority of these attackers operate in underground forums engaging in related conversations and buying/selling stolen digital goods. Unlike other financially motivated attackers such as ransomware groups or extortion groups who often publicize their attacks, these attackers like to operate under the hood. By taking advantage of an unpatched system or exploiting a vulnerability in an application or system – they gain access and steal valuable data. The stolen data is then advertised for sale in underground forums, resold, and repurposed by other attackers in their attacks.

2. Recommendations **[NEW]**

STRATEGIC RECOMMENDATIONS

Attack Surface Management should be adopted by organizations, ensuring that a continuous closed-loop process is created between attack surface monitoring and security testing.

Deploy a **unified threat management** strategy – including malware detection, deep learning neural networks, and anti-exploit technology – combined with vulnerability and risk mitigation processes.

Incorporate **Digital Risk Protection (DRP)** in the overall security posture that acts as a proactive defence against external threats targeting unsuspecting customers.

Implement a **holistic security strategy** that includes controls for attack surface reduction, effective patch management, active network monitoring, through next generation security solutions and ready to go incident response plan.

Create **risk-based vulnerability management** with deep knowledge about each asset. Assign a triaged risk score based on the type of vulnerability and criticality of the asset to help ensure that the most severe and dangerous vulnerabilities are dealt with first.

MANAGEMENT RECOMMENDATIONS

Take advantage of global **Cyber Intelligence** providing valuable insights on threat actor activity, detection, and mitigation techniques.

Proactively monitor **effectiveness of risk-based information security strategy**, the **security controls** applied and the proper implementation of **security technologies**, followed by corrective actions remediations and lessons learned.

Move beyond traditional model of security awareness towards **improved simulation and training** exercises that mimic real attack scenarios, account for behaviours that lead to a compromised and, are measured

Consider implementing **Network Traffic Analysis (NTA)** and **Network Detection and Response (NDR)** security system to compensate the shortcoming of EDR and SIEM solutions.

Detection processes are tested to ensure awareness of anomalous events. Timely communication of anomalies and continuously evolved to keep up with refined ransomware threats.

TACTICAL RECOMMENDATIONS

Patch software/applications as soon as updates are available. Where feasible, automated remediation should be deployed since vulnerabilities are one of the top attack vectors.

Consider using **security automation** to speed up threat detection, improved incident response, increased visibility of security metrics and rapid execution of security checklists.

Build and undertake safeguarding measures by monitoring/ blocking the IOCs and strengthen defences based on tactical intelligence provided

Deploy **detection technologies** that are behavioural anomaly-based to detect ransomware attacks and help to take appropriate measures.

Implement combination of security control such as **reCAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), Device fingerprinting, IP backlisting, Rate-limiting, and Account lockout** to thwart automated brute-force attacks.

Ensure **email and web content filtering** uses **real-time blocklists, reputation services** and other similar mechanism to avoid accepting content from known and potentially malicious sources.