

Weekly Intelligence Trends/Advisory

10 June 2022

TABLE OF CONTENTS

1. CYFIRMA's Weekly Insights [NEW]	2
1.1 Weekly Attack Type and Trends	2
1.2 Threat Actor in Focus	2
1.3 Major Geopolitical Developments in Cybersecurity	4
1.4 Rise in Malware/Ransomware and Phishing	4
1.5 Latest Cyber-Attacks, Incidents, and Breaches	5
1.6 Vulnerabilities and Exploits	6
1.7 Data Leak	7
2. Recommendations [NEW]	9

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, Remote Code Execution (RCE), Authentication Bypass, Privilege Escalation, Remote Injection, XML Routing Detour Attack, Reflected Cross-site Scripting (XSS)
- **Objective:** Data Theft, Data Encryption, Financial Gains, Unauthorized Access, Elevation of Privilege
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage, Operational Disruption
- **Ransomware – Hive | Malware – Clipminer and SMSFactory**
 - **Hive** – One of the ransomware groups.

Please refer to the trending malware advisory for details on the following:

- Malware – **Clipminer and SMSFactory**

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

State-sponsored Chinese Threat Actor Target Network Providers and Devices

Suspected Threat Actors: Unknown

- **Attack Type:** Vulnerabilities & Exploits, Remote Code Execution, Authentication Bypass, Privilege Escalation, Remote Injection, XML Routing Detour Attack
- **Objective:** Unauthorized Access, Data Theft, Elevation of Privilege
- **Target Technology:** Network Devices
- **Target Industry:** Telecommunication, Network Service Providers
- **Target Geography:** Global
- **Business Impact:** Data Loss, Financial Loss

Summary: A recent joint advisory by the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) describes how Chinese state-sponsored threat actors continue to exploit publicly known vulnerabilities to build a broad infrastructure of compromised systems. These threat actors attack a wide variety of targets including public and private sector organizations worldwide. The advisory detailed vulnerabilities associated with network devices routinely exploited by the attackers since at least 2020. The below figure illustrates these publicly known vulnerabilities:

Table 1: Top network device CVEs exploited by PRC state-sponsored cyber actors

Vendor	CVE	Vulnerability Type
Cisco	CVE-2018-0171	Remote Code Execution (RCE)
	CVE-2019-15271	RCE
	CVE-2019-1652	RCE
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	Authentication Bypass
MikroTik	CVE-2018-14847	Authentication Bypass
Netgear	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	Authentication Bypass
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	Privilege Elevation
	CVE-2019-7193	Remote Inject
	CVE-2019-7194	XML Routing Detour Attack
	CVE-2019-7195	XML Routing Detour Attack
Zyxel	CVE-2020-29583	Authentication Bypass

Source: Surface Web

The Chinese state-sponsored threat actors frequently take the help of open-source exploitation frameworks and tools such as RouterSploit and RouterScan for reconnaissance and vulnerability scanning. This type of activity allows them to identify make, model, as well as known vulnerabilities for further exploitation. In one such incident after gaining initial access into the network of a telecommunications organization/ network service provider, the threat actors identified critical users and infrastructure, in this case, they identified a critical Remote Authentication Dial-In User Service (RADIUS) server and later went onto compromise and dump credential from the underlying Structured Query Language (SQL) database which contained both cleartext and hashed passwords for user and administrative accounts.

Insights:

- The agencies highlight that these attackers are also consistent in evolving and adapting tactics to bypass defenses. They observed the state-sponsored actors monitored “accounts and actions” of network defenders, and then went on to modify their ongoing campaign accordingly to remain under the radar. They modified their infrastructure and toolsets as soon as information related to their ongoing campaigns become public. The Chinese state-sponsored threat actors were often found mixing their customized toolset with tools available publicly to obscure their activity in noise or normal activity of a network.

1.3 Major Geopolitical Developments in Cybersecurity

Crypto Exchanges Sanctions Are Helping in Fight Against Ransomware

According to a witness's testimony before the Senate Homeland Security and Governmental Affairs Committee, the "desired effect" has been achieved by the historic sanctions imposed on Russia-based cryptocurrency exchanges. However, calls for robust enforcement of money laundering-related laws internationally to thwart ransomware.

The head of a threat intel firm states they "have observed a winnowing down of the cash out destinations for illicit actors, including ransomware actors, mainly to offshore exchanges with little to no regulation and enforcement, which underscores our recommendation for enhanced US assistance in implementing AML — anti-money laundering — laws to cut off that illicit cash out destinations,"

Notably, a virtual currency exchange known as SUEX which operates out of Federation Tower in Moscow was put on a list of entities that are banned to be associated with US citizens by the Biden administration. More cryptocurrency exchanges have since then been added to the list.

As a result of this, especially in the case of SUEX "deposits dropped nearly to zero" and cybercriminals were forced to resort to offshore exchanges and "mixing" services where tracing the identity of the ultimate party receiving the funds is quite challenging. Increased utilization of mixing services was observed obfuscating the destination and going after "paths of least resistance", however, were narrowed to a handful of services.

Given the example of the effectiveness of the Financial Action Task Force in the case of terrorism instances, a more consistent regulatory environment internationally is expected by the application of KYC, AML, and other regulatory measures to fight these cybercriminals.



1.4 Rise in Malware/Ransomware and Phishing

Caracol Television Impacted by Hive Ransomware

- **Attack Type:** Ransomware, Data Exfiltration
- **Target Industry:** Media
- **Target Geography:** Colombia
- **Ransomware:** Hive
- **Objective:** Financial Gains, Data Theft, Data Encryption
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage

Summary: CTI observed **Caracol Television (www.caracol.tv)** – a Colombian free-to-air television network owned by Caracol Medios – being impacted by Hive ransomware. The ransomware group claimed the television network provider as one of their victims by disclosing the update on their dedicated leak site HiveLeaks on 30 May. The update also claims the encryption of the company's data was carried out on 22 May. At the time of CTI's observation, the ransomware group has provided links to suspected exfiltrated data which they claim contains documents related to Finance, Budget, Projects, and Contracts. It appears that the ransom demand has not been met, as a result, the ransomware group has leaked the data for anyone to download.

The following screenshot was observed published on the dark web:

<h1>Caracol TV</h1> <p>Founded in 1954 and based out of Bogota, Columbia, Caracol Television operates as a media and entertainment company</p> <p>Website www.caracoltv.com</p> <p>Revenue \$1 000M</p> <p>Employees 1 950</p>	<p>Encrypted at</p> <p>22 May 2022</p> <p>10:18:30</p> <p>Disclosed at</p> <p>30 May 2022 • 21:55:30</p>	<p>Share</p> <p></p> <p></p>
<p>Disclosed Links ▾ 2 links</p>		

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

Stolen Social Security Numbers Marketplace Shutdown by Federal Agencies

- Objective: Financial Gains, Data Theft
- **Attack Type:** Credential Abuse, Unauthorized Access, Data Exfiltration
- **Target Technology:** Unknown
- **Target Industry:** Unknown
- **Target Geography:** United States

- **Business Impact:** Data Loss

Summary: In a joint action by The Justice Department, IRS, and FBI - the popular SSNDOB Marketplace used by cybercriminals to acquire stolen Social Security numbers and other sensitive personal information by sized and shut down alongside coordination with agencies in Cyprus and Latvia. . According to the DOJ the marketplace used to generate over USD19 million in sales revenue. The seizure orders were executed against several domains associated with SSNDOB which included ssndob.ws, ssndob.vip, ssndob.club, and blackjob.biz. The cybercriminals behind SSNDOB used to put advertisements for their services in other dark web forums known to be frequented by cybercriminals, offered support to their customers, used servers in various geographic locations, and required payment in cryptocurrencies like Bitcoin.

Insights:

- According to a firm specializing in blockchain analysis stated that in addition to Social Security numbers, the SSNDOB also dealt in email addresses, passwords, and credit card numbers. Further, they also found a link between one of the other popular stolen credential marketplaces including Joker's Stash, which was another large marketplace located on the dark web that offered stolen credit card information and other information before being shut down in January 2021.

1.6 Vulnerabilities and Exploits

XSS Vulnerability In Download Manager Plugin

- **Attack Type:** Vulnerabilities & Exploits, Reflected XSS
- **Target Technology:** Download Manager WordPress plugin
- **Vulnerability:** CVE-2022-1985 (CVSS score: 6.1)
- **Vulnerability Type:** Lack of Input Sanitization

Summary: On May 30, 2022, a Security Researcher reported a reflected XSS vulnerability in the Download Manager - a WordPress plugin that is installed on over 100,000 websites. The vulnerability has been assigned identifier CVE-2022-1985. One feature of the Download Manager plugin gives the ability to embed files and other assets in a page or post by using shortcode. This particular function was found by researchers vulnerable to reflected XSS. The vulnerability exists due to a lack of proper input sanitization and escaping the user-supplied inputs. Due to the vulnerability, JavaScript can be invoked to manipulate the page, hijack the forms, and disclose sensitive information by tricking the site administrator unknowingly.

Insights:

- Researchers state that the vulnerability may also lead to more specialized attacks where using the vulnerability attacker may acquire administrator access or install a backdoor and compromise the site entirely. When successful, this type of attack would allow the attacker to gain access to the same level of information as accessible to the administrator including user details and customer information.
- According to WordPress security analysts, users with Free, Premium, Care, and Response, are protected from exploitation of this vulnerability due to Wordfence Firewall's built-in Cross-Site Scripting protection. Regardless, of the protection, the vendor has recommended upgrading to the latest patched instance.

1.7 Data Leak

Agricultural Bank of China Data Advertised for Sale

- **Attack Type:** Data Leak
- **Target Industry:** Banking
- **Target Geography:** China
- **Objective:** Data Theft, Financial Gains
- **Business Impact:** Data Loss, Financial Loss, Reputational Damage, Regulatory Implications

Summary: As part of routine threat hunting efforts, CTI has observed potential data of **Agricultural Bank of China** – also known as **AgBank**, which is one of the "Big Four" banks in China – advertised for sale by an unknown threat actor in one of the underground forums. As per the advertisement, the threat actor claims the stolen database contains approximately 889310 records and includes user details such as the Name, sex, age, education, nationality, Province, Mobile, ID card No, Bank Card No, Bank Name, and Address. The threat actor has also provided a piece of sample evidence containing claimed stolen dataset.

June 1, 2022, 02:45 PM (This post was last modified: June 2, 2022, 10:19 AM by [redacted])

Total: 889310 records

Included: Name,sex,age,Education,nationality,Province,Mobile,IDcardNo,BankCardNo,BankName,Address,Address2

Sample: [Download](#)

Dm me via telegram: [redacted]

Source: Underground Forums

近	女	'48'	'大'	'汉'	'黑力	'4532 '231	'28480 '河北	'译'黑力	'市东五
张	女	'64'	'初'	'汉'	'上海	'2190 '310	'28480 '上海	'译'上海	'亭北路
徐	男	'33'	'高'	'汉'	'上海	'6268 '310	'28480 '上海	'译'上海	'亭北路
张	男	'65'	'初'	'汉'	'上海	'1706 '310	'28480 '上海	'译'上海	'亭北路
盛	男	'35'	'高'	'汉'	'上海	'8226 '310	'28480 '上海	'译'上海	'山镇余
赵	男	'46'	'专'	'汉'	'上海	'1765 '310	'28450 '上海	'译'上海	'每西路
李	男	'70'	'中'	'汉'	'上海	'2266 '310	'28480 '重庆	'译'重	'登路2
顾	男	'64'	'初'	'汉'	'上海	'1519 '320	'28480 '江苏	'译'江	'阳镇小
黄	女	'54'	'初'	'汉'	'上海	'0628 '310	'28480 '辽宁	'译'上海	'台镇港
俞	女	'64'	'高'	'汉'	'上海	'6182 '352	'28480 '上海	'译'上海	'洛880
沈	女	'46'	'初'	'汉'	'上海	'1707 '310	'28480 '上海	'译'上海	'工路1
金	男	'23'	'中'	'汉'	'上海	'1841 '310	'28480 '上海	'译'上海	'村路1
陶	男	'27'	'高'	'汉'	'上海	'1713 '310	'28480 '上海	'译'上海	'旧五村
杨	女	'53'	'高'	'回'	'上海	'1800 '310	'28480 '上海	'译'上海	'主北路
戴	女	'57'	'高'	'汉'	'上海	'0172 '310	'28480 '上海	'译'上海	'甬路2
王	女	'57'	'初'	'汉'	'上海	'6722 '310	'28480 '上海	'译'上海	'路221
张	女	'31'	'大'	'汉'	'上海	'2796 '310	'28480 '上海	'译'上海	'甬路3
李	女	'54'	'高'	'汉'	'上海	'0212 '310	'28480 '上海	'译'上海	'路555
刘	女	'78'	'小'	'汉'	'上海	'2174 '310	'28480 '上海	'译'上海	'主北路
刘	女	'64'	'初'	'汉'	'上海	'2417 '310	'59980 '上海	'译'上海	'夜路5
钱	女	'70'	'大'	'汉'	'上海	'7151 '310	'28480 '上海	'译'上海	'每花路
顾	女	'51'	'高'	'汉'	'上海	'1191 '310	'28480 '上海	'译'上海	'家镇江
范	女	'55'	'初'	'汉'	'上海	'6154 '310	'28480 '上海	'译'上海	'寅陈南
茅	女	'70'	'初'	'汉'	'上海	'1015 '310	'28480 '上海	'译'江	'宁区红
徐	女	'48'	'高'	'汉'	'上海	'1884 '310	'28480 '中国	'译'上海	'圣镇持
徐	男	'57'	'初'	'汉'	'上海	'1609 '310	'28480 '开	'译'祝	'5115号
健	男	'21'	'大'	'汉'	'中国	'3970 '310	'28480 '上海	'译'上海	'兑桥镇
孙	女	'58'	'高'	'汉'	'上海	'6719 '310	'28480 '上海	'译'上海	'川沙镇
陆	男	'74'	'初'	'汉'	'上海	'2229 '310	'28480 '上海	'译'上海	'川沙镇
薛	女	'55'	'初'	'汉'	'上海	'2776 '310	'28480 '上海	'译'上海	'曹路镇
陆	女	'59'	'高'	'汉'	'上海	'2167 '310	'28480 '上海	'译'上海	'川沙镇
张	男	'65'	'大'	'汉'	'上海	'0684 '330	'28480 '宁波	'译'现	'社区')
张入志	男	'65'	'初'	'汉'	'上海	'2189 '310	'28480 '上海	'译'上海	'合庆镇

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]



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.



STRATEGIC RECOMMENDATIONS

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.



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 against real attacks the organization receives.



MANAGEMENT RECOMMENDATIONS

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.



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



TACTICAL RECOMMENDATIONS

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.

