ATHENIAN TECH

Chinese Threats to Indian National Critical Infrastructures

2023

www.atheniantech.com

TABLE OF CONTENTS

TABLE OF CONTENTS

The ladakh power grid attack

Powergrids are a critical part of any developing countries infrastructure and play a vital role in keeping other important infrastructures up and running. An important indian powergrid stationed in the Ladakh province recently went through an attempted cyber attack claimed to be by chinese state sponsored hacktivists.

This attack was targeted towards SLDC systems, the Chinese hackers targeted load State Load Dispatch Centers (SLDCs) or electricity distribution units in the Northern Indian states using a cluster of malware called ShadowPad threatening the supply of electric power. These attacks were preceded by cyber attacks against Regional Load Dispatch Centers (RLDCs) in Delhi, Karnataka, and Telangana as well as two ports: Mumbai Port and Tuticorin VOC port.

The attackers used an ‘unusual; method of attack through ‘compromised internet of things devices’ such as DVR/Cameras.
The devices used to launch the intrusions were based in Taiwan, with some in South Korea as well.

What does it imply? -

- This is clearly something that is linked to China’s geopolitical interests.
- It is established clearly that the People's Republic of China appears to be adopting and promoting the use of cyber offensive technologies and espionage in a pretty active manner.

The attackers, sometimes identified as Threat Activity Group 38 (TAG-38), are believed to have infiltrated the system via third-party devices like IP cameras that may have been left vulnerable when their default credentials were kept in place.

"The group likely compromised and co-opted internet-facing DVR/IP camera devices for command and control (C2) of ShadowPad malware infections, as well as the use of the open source tool FastReverseProxy (FRP).

it was most likely a mission to gather information about critical infrastructure, rather than seeking immediate-term benefit. Such information could later be used to gain access across a system to take (presumably disruptive) action.

Years of Espionage

Governments worldwide are fighting for digital supremacy in a new, mainly invisible theatre of operations known as cyberspace. Cyber-attacks, once limited to opportunistic criminals, are now becoming a significant weapon for governments defending national sovereignty and projecting national authority.

A cyber-attack is better understood as a potentially powerful method to achieve a wide range of political, military, and economic objectives rather than as an end in itself.

Chinese and Indian forces clashed in the remote Galwan Valley early last summer in a surprise border altercation, clubbing each other to death with rocks and clubs. The Galwan valley clash in 2020 heightened tensions between India and China. Following a severe skirmish in the Pangong Tso Lake area, an eastern Ladakh border stalemate between Indian and Chinese soldiers erupted on May 5, 2020.

Following the incident, both sides gradually enhanced their deployment by rushing in tens of thousands of soldiers as well as heavy weaponry, resulting in increased tensions at the friction points.

Four months later, more than 1500 miles away in Mumbai - India, trains stopped running and the stock exchange shuttered as the city's 20 million residents lost power. During one of India's deadliest coronavirus outbreaks, hospitals had to turn to emergency generators to keep ventilators working. The 2022 Mumbai power outage, which was described as the worst in decades, may have been linked to India-China border tensions. According to the allegation, the massive Mumbai power outage could be the consequence of a Chinese cyber-attack intended to warn India not to push too aggressively. At the same time, Indian and Chinese forces were fighting at the border, malware was being inserted into the control systems that oversee India's electricity supply.

Now, a new research backs up the theory that the two incidents were linked — as part of a larger Chinese cyber assault against India's power grid, timed to send a message that if India pressed its claims too hard, the country's lights may go out.

Chinese malware was streaming into the control systems that manage electricity supplies across India, as well as a high-voltage transmission substation and a coal-fired power plant, according to the report, as conflicts raged in the Himalayas, killing at least two dozen people.

Chinese Cyber Tactics

The People’s Republic of China is home to 1.35 billion people. As a result, China has the power to overwhelm cyber defences by focusing on quantity rather than quality, just as it did during the Korean War and could do in any other fight. Chinese malware isn't the most sophisticated or inventive. However, it has proven to be equally effective in a variety of situations. China uses brute-force attacks because they are frequently the cheapest method to achieve its goals. The attacks are successful because of the sheer volume of attempts, the presence and persistence of vulnerabilities in modern networks, and the cybercriminals' apparent indifference to being caught.

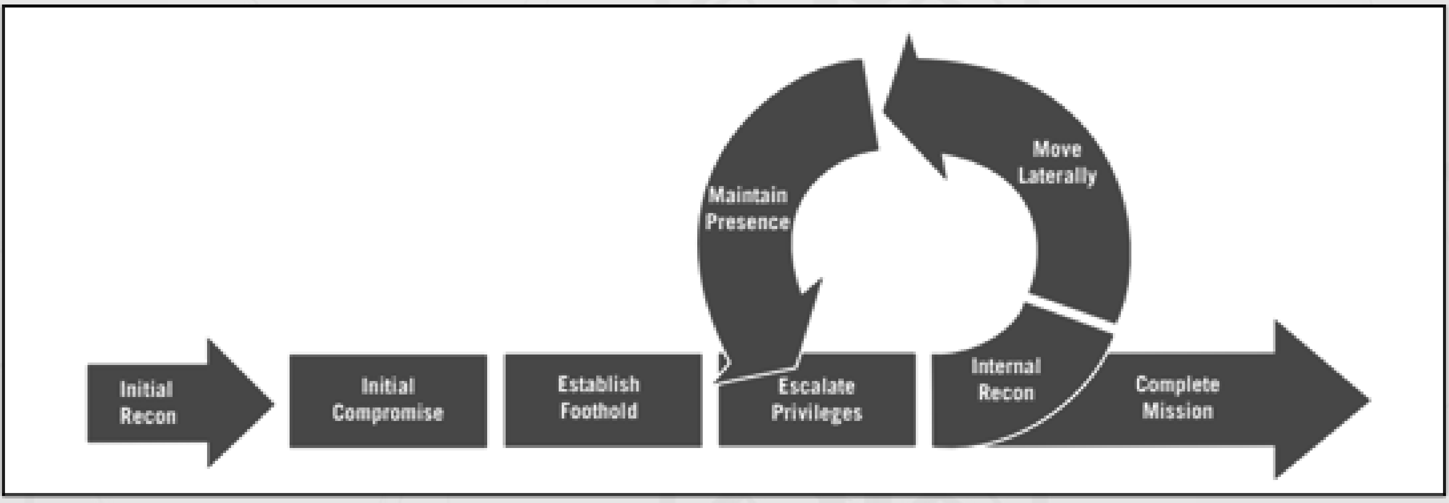


Fig: Chines attack threat lifecycle

Target Areas of Chinese Information Operation

The Chinese leadership is convinced that a joint offensive IW will be a key factor in achieving operational success. The Chinese Information Warfare is primarily focused on

- **Critical Information Storage Systems,**
- **Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance & logistical systems**
- **Navigation and guidance systems of platforms**
- **Decision support and fire control systems**
- **Social media platforms**
- **Public web domains**
- **Internet of Things of the adversaries**

Cyber Attack on India

The People’s Republic of China is home to 1.35 billion people. As a result, China has the power to overwhelm cyber defences by focusing on quantity rather than quality, just as it did during the Korean War and could do in any other fight. Chinese malware isn't the most sophisticated or inventive. However, it has proven to be equally effective in a variety of situations. China uses brute-force attacks because they are frequently the cheapest method to achieve its goals. The attacks are successful because of the sheer volume of attempts, the presence and persistence of vulnerabilities in modern networks, and the cybercriminals' apparent indifference to being caught.

This report contains the cyber activity that China is involved in India. Athenian Tech has observed a significant surge in suspected targeted intrusion activities by Chinese state-sponsored organizations against Indian organizations.

The use of infrastructure monitored as AXIOMATICASYMPTOTE, which includes ShadowPad command and control (C2) servers, to target a massive swath of India's power sector increased dramatically from mid-2020 onwards, according to Recorded Future's halfway collection. In a coordinated assault targeting India's essential infrastructure, ten unique Indian power sector companies have been designated targets, including four of the five Regional Load Despatch Centres (RLDCs) responsible for power grid operation by balancing electricity supply and demand. Two Indian seaports are also recognized as potential targets.

"INDIAN OFFICIALS WORRY THAT CHINA COULD DISRUPT THEIR COMPUTER NETWORKS DURING A CONFLICT. ONE EXPERT CONFIDED THAT AN EXCLUSIVE RELIANCE ON CHINESE HARDWARE MIGHT GIVE CHINA A “PERMANENT” DENIAL-OF-SERVICE CAPABILITY. ONE SOPHISTICATED ATTACK ON AN INDIAN NAVY HEADQUARTERS ALLEGEDLY USED A USB VECTOR TO BRIDGE THE “ AIR-GAP” BETWEEN A COMPARTMENTALIZED, STANDALONE NETWORK AND THE INTERNET."

Source: Pubby, M. (01 Jul 2012) "China hackers enter Navy computers, plant bug to extract sensitive data" The Indian Express.

Furthermore, after any major events in India, the number of cyberattacks tends to rise. For example, 80,000 cyber-attacks were recorded after the demonetisation of currency, and more than 40,300 attacks were reported in Indian cyberspace after the Galwan incident.

In the month following the Galwan Clash, there was a 200 percent increase in Chinese cyberattacks, mostly aimed at stealing sensitive information.

The government of the People's Republic of China (PRC) is a decade into a sweeping military modernisation programme that has fundamentally transformed its ability to fight high tech wars. China's modernisation plans for its armed forces include the development of a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum. The PLA Science and Engineering University serves as a centre for defence related scientific, technological, and military equipment research. The university also provides advanced information warfare and networking training.

Chinese Cyber Espionage and Warfare Globally

India is not China's only cyber target. All traditional, geopolitical conflicts have moved into cyberspace, and Chinese compromises encompass the entire globe. But many contests have been one-sided affairs, with all publicly known attacks emanating from China.

Europe: In 2006, Chinese cybercriminals targeted the UK House of Commons;9 in 2007, German Chancellor Angela Merkel raised the problem of nation-state hacking with China's President; in 2010, British MI5 warned that undercover Chinese intelligence officers had given UK business executives malware-laden digital cameras and memory sticks.

South Korea: The South Korean government has complained for years of Chinese activity on its official computers, including a 2010 compromise of the personal computers and PDAs belonging to much of South Korea's government power structure and a 2011 assault on an Internet portal that held personal information for 35 million Koreans.

QUICK FACTS

- To target the power sector, the attacker uses the AXIOMATICASYMPTOTE infrastructure consisting of ShadowPad C2 servers.
- Ten power-related firms were targeted, including four Regional Load Despatch Centres (RDPL).
- Seaports in Kochi and Mumbai were the other two.
- The ten power sector companies are responsible for over 80% of India's geography in terms of energy coverage.
- These were in Himachal Pradesh, Rajasthan, Uttar Pradesh, Uttarakhand, and Delhi.

Japan: Here, the target list includes government, military, and high-tech networks. Chinese cybercriminals have even stolen classified documents.

Australia: China allegedly stole the blueprints of the Australian Security Intelligence Organization's new $631 million building.

Worldwide: In 2009, Canadian researchers discovered that China controlled a worldwide cyber espionage network in over 100 countries. In 2010, a Chinese telecommunications firm transmitted erroneous routing information for 37,000 computer networks, which misrouted some Internet traffic through China for 20 minutes. The attack exposed data from 8,000 U.S. networks, 1,100 Australian networks, and 230 French networks.

Implications for India

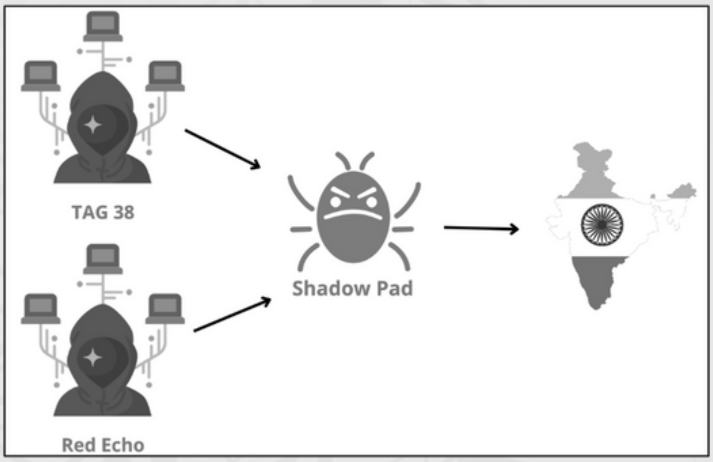
According to the Cert-In reports, there has been an array of critical cyber-attacks associated with Information Operations carried out by the Chinese on India, targeted on both government and public domain. The nation has been witnessing Chinese Cyber-attacks since the first recorded cyber-attack on India was on the computers of BARC (Bhabha Atomic Research Centre) in June 1998.

Some of the significant Chinese information operations and their implications are namely,

- In 2010, China used the Stuxnet worm to compromise Indian communication satellite, led to the loss of TV signals for many. The government created the National Critical Information Infrastructure Protection Centre (NCIIPC) as a measure, to predict and prevent information breaches in the future.
- In 2012, Chinese malware-infected computers in the campus of Indian Eastern Naval Command. The incident had a significant impact, as the command was responsible for the security of India's Eastern border and other strategic assets. In response to it, the Indian Navy issued an advisory to the officers regarding usage of, computers and other IoTs within the establishments.
- Likewise, in 2013, computers in the DRDO had been compromised by the Chinese and a large number of electronic files were stolen and diverted to a server located in Guangdong Province in China.
- Moreover, Information operations are carried out not only on targeting Defence & Security domains. Incidents were related to, Information operations also reported in Indian Space Research Organisation (ISRO), BSNL other Public sector undertakings. They also targeted other fields such as Banking & Finance, Public Healthcare, Industries, consumer domains.
- Disinformation and hate propaganda and other instruments of Psychological operations, such as media campaign, virtual deceptions were used by the Chinese, via posts in the Social media platforms such as Facebook, Instagram and Twitter.

Threat Analysis

Insikt Group tracks the network infrastructure used in ShadowPad infections as AXIOMATICASYMPTOTE. This technique fingerprints unique characteristics, including header responses and similar network components. We discovered that a subset of these AXIOMATICASYMPTOTE servers is being utilized by a China-linked activity group known as RedEcho to target a massive swath of India's power sector using a combination of proactive infrastructure detections, domain and network traffic analysis.



ShadowPad

First Known Sample: 2017

Discovery: 2017

Number Of Targets: Unknown

Current Status: Active

Type: Backdoor

Top Targeted Countries: Worldwide

The Way of Propagation: Trojanized software installers

Purpose/Functions: Remote control

Special Features

ShadowPad exemplifies the dangers that a successful supply-chain attack might bring. Given the potential for covert data collecting, attackers are likely to try this type of attack with more widely used software components in the future.

Targets

Construction, Electronics manufacturing, Financial institutions, Heavy industry manufacturers, Manufacturing, Media, Medical Industry, Software companies, Telecoms, Transportation, and Energy.

Artefacts/Attribution

Attribution is hard, and attackers were careful not to leave apparent traces. However, specific techniques were used in other malware like PlugX and Winnti, which Chinese-speaking actors allegedly developed.

Description

A supply chain attack in 2017 delivered a backdoor Trojan hidden in modified versions of software produced by NetSarang, a developer of network connectivity solutions. Once inside a system, the malware can upload files, create processes, and store information.

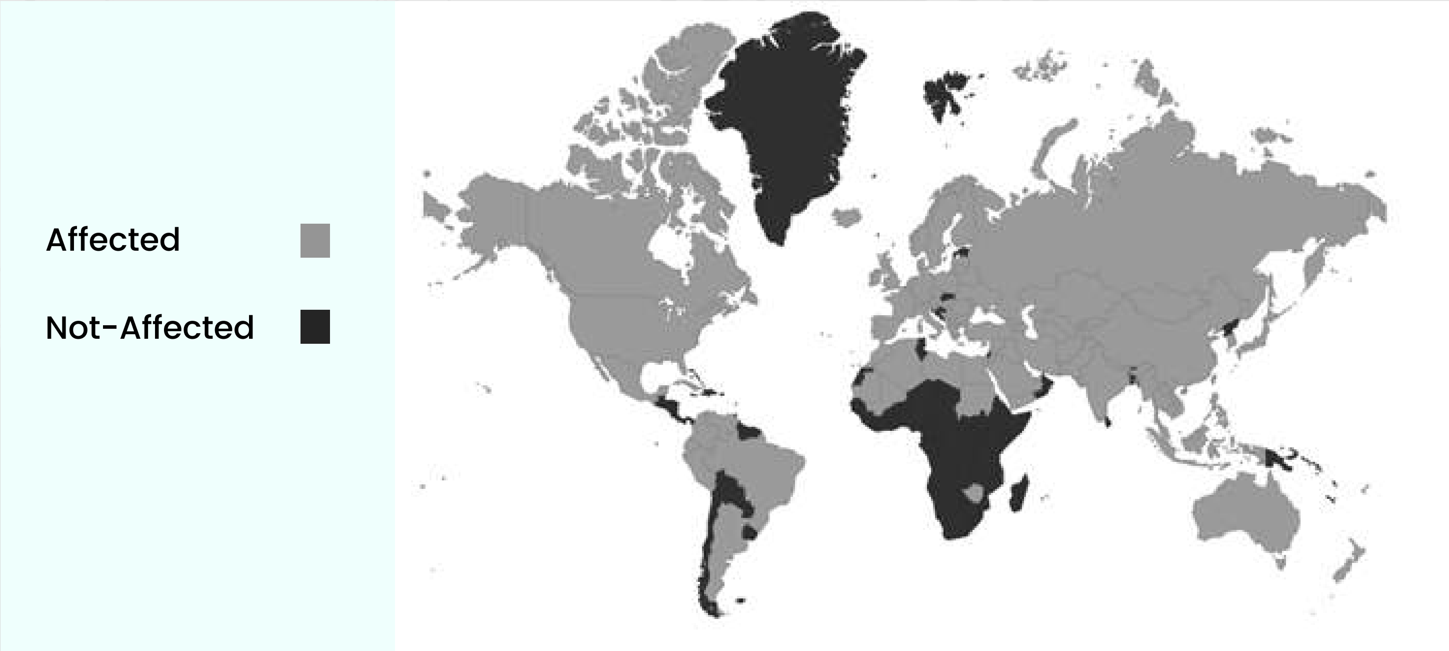


Fig: Worldwide affected area of ShadowPad

Five separate Chinese threat clusters have used ShadowPad, a known Windows backdoor that allows attackers to download more malicious modules or steal data. Since 2017, the Chinese government-sponsored BRONZE ATLAS threat organization has used the ShadowPad sophisticated modular remote access trojan(RAT).

Since 2019, many other Chinese threat groups have used it in assaults against corporations in various industries. ShadowPad samples analysed by SecureWorks Counter Threat Unit(CTU) identified activity clusters connected to threat groups affiliated with the Chinese Ministry of State Security(MSS) civilian intelligence agency and the People's Liberation Army.

- ShadowPad is a modular backdoor that allows attackers to harvest information about the victim machine, run commands, transfer files, interact with the file system and registry, and deploy additional modules to increase functionality (such as keylogging and screen recording)
- The American cybersecurity firm dubbed ShadowPad a "masterpiece of privately sold malware in Chinese espionage."
- The hacking group, dubbed TAG-38, has used a kind of malicious software called ShadowPad, which was previously associated with China's People's Liberation Army and the Ministry of State Security
- The devices used to launch the intrusions are based in South Korea and Taiwan.

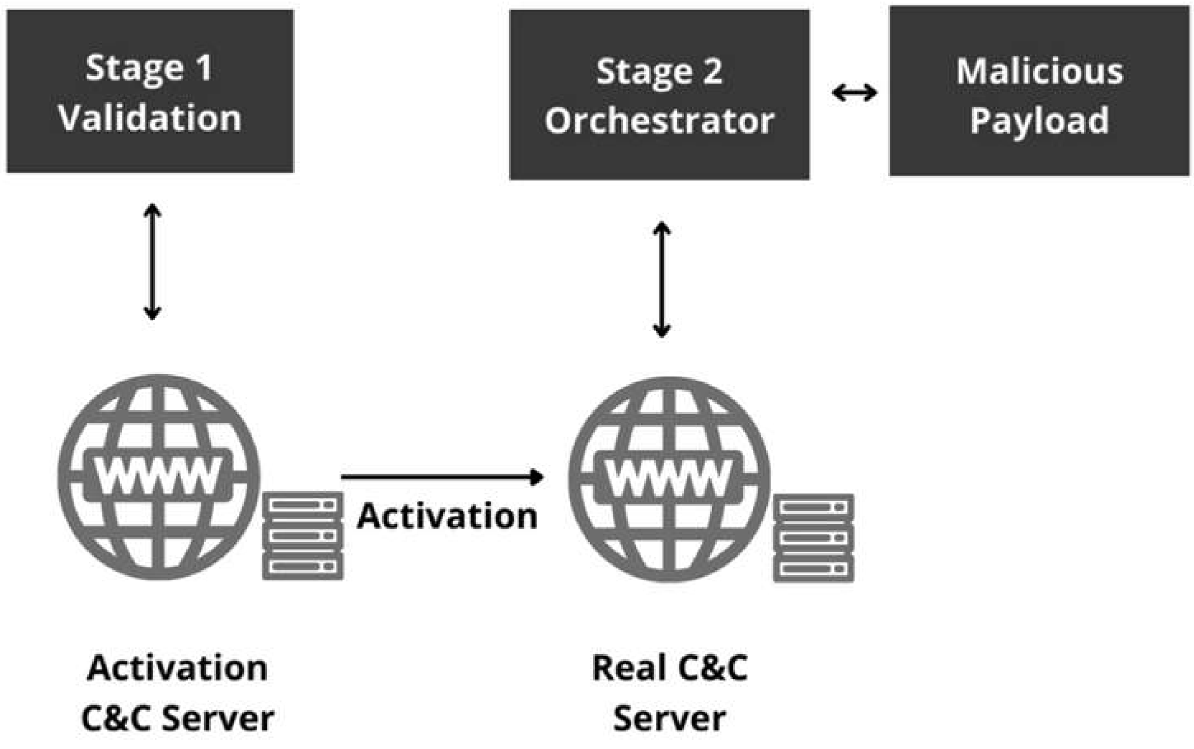
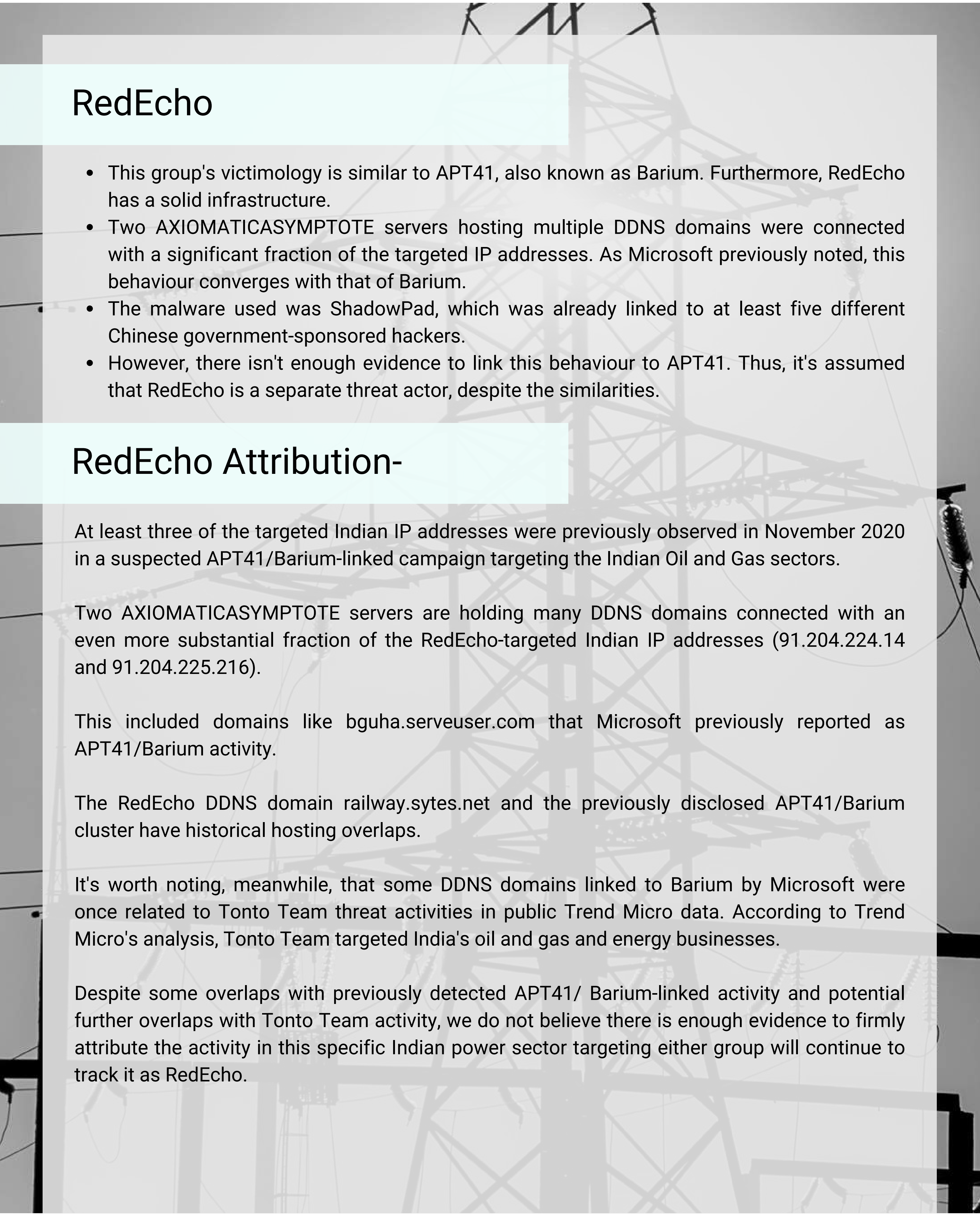


Fig: The architecture of ShadowPad backdoor



RedEcho

- This group's victimology is similar to APT41, also known as Barium. Furthermore, RedEcho has a solid infrastructure.
- Two AXIOMATICASYMPTOTE servers hosting multiple DDNS domains were connected with a significant fraction of the targeted IP addresses. As Microsoft previously noted, this behaviour converges with that of Barium.
- The malware used was ShadowPad, which was already linked to at least five different Chinese government-sponsored hackers.
- However, there isn't enough evidence to link this behaviour to APT41. Thus, it's assumed that RedEcho is a separate threat actor, despite the similarities.

RedEcho Attribution-

At least three of the targeted Indian IP addresses were previously observed in November 2020 in a suspected APT41/Barium-linked campaign targeting the Indian Oil and Gas sectors.

Two AXIOMATICASYMPTOTE servers are holding many DDNS domains connected with an even more substantial fraction of the RedEcho-targeted Indian IP addresses (91.204.224.14 and 91.204.225.216).

This included domains like bguha.serveuser.com that Microsoft previously reported as APT41/Barium activity.

The RedEcho DDNS domain railway.sytes.net and the previously disclosed APT41/Barium cluster have historical hosting overlaps.

It's worth noting, meanwhile, that some DDNS domains linked to Barium by Microsoft were once related to Tonto Team threat activities in public Trend Micro data. According to Trend Micro's analysis, Tonto Team targeted India's oil and gas and energy businesses.

Despite some overlaps with previously detected APT41/ Barium-linked activity and potential further overlaps with Tonto Team activity, we do not believe there is enough evidence to firmly attribute the activity in this specific Indian power sector targeting either group will continue to track it as RedEcho.

RedEcho Infrastructure TTPs -

A subset of RedEcho AXIOMATICASYMPTOTE servers was set up with domains that impersonate several Indian power generation and transmission companies. For example, the domain ntpc-co.com is most likely a misspelling of ntpc.co.in the website of NTPC Limited, an Indian power producing firm. According to the Recorded Future new domain registration stream, the domain was originally registered in July 2019.

According to the approach of viewing network indicators as composite objects, Insikt Group evaluated the detected RedEcho operational infrastructure and discovered a pattern of behaviour.

The following is a summary of RedEcho's operational infrastructure modus operandi in the identified intrusion campaign:

- Domains were registered using the registrar WEBCC, which used eznowdns[.]com as the authoritative name server.
- RedEcho's operational infrastructure is linked to cndns.com, a Chinese domain, and infrastructure reseller.
- Used the WhoisProtection - WHOIS privacy protection service.
- EHOSTICT and HKBN Enterprise Solutions HK Limited (AS9381) host AXIOMATICASYMPTOTE infrastructure (AS45382)
- Domains imitated (lexically similar) Indian entities or had strings mentioning India.
- A common top-level domain was used (.com)
- For operational infrastructure, dynamic DNS domains were used.

While none of these qualities are unique to RedEcho on their own, the combination of these holistically recognized distinct behaviours is likely indicative of RedEcho activity.

We discovered other domains that were likely associated based on these highlighted TTPs, which included overlaps with known AXIOMATICASYMPTOTE servers and previous hosting data for domains inside the highlighted infrastructure cluster.

Further pivots restricted to shared old hosting infrastructure discovered a new group of RedEcho dynamic DNS (DDNS) domains with the same Indian-themed domain naming pattern and AXIOMATICASYMPTOTE servers:

Domain used in attacks:

Domain	IP Address	Details
pandorarve.com	223.255.155.247 223.255.155.252	223.255.155.252 - Confirmed AXIOMATICASYMPTOTE server
Indrails.com	223.255.155.237	Matches infrastructure TTPs and Indian railway themed
astudycarsceu.net	27.255.94.21	Confirmed AXIOMATICASYMPTOTE server, matches infrastructure TTPs, and overlapping victimology
escanavupdate.club	218.255.77.60	Multiple hosting overlaps within the infrastructure cluster. Likely spoofing Indian antivirus provider eScan AV
indiasunsung.com	223.255.155.243 180.150.226.216	180.150.226.216 - Confirmed AXIOMATICASYMPTOTE server
ixrails.com	223.255.155.243 101.78.177.227	101.78.177.227 - Confirmed AXIOMATICASYMPTOTE server

Table- RedEcho domains matching infrastructure TTPs

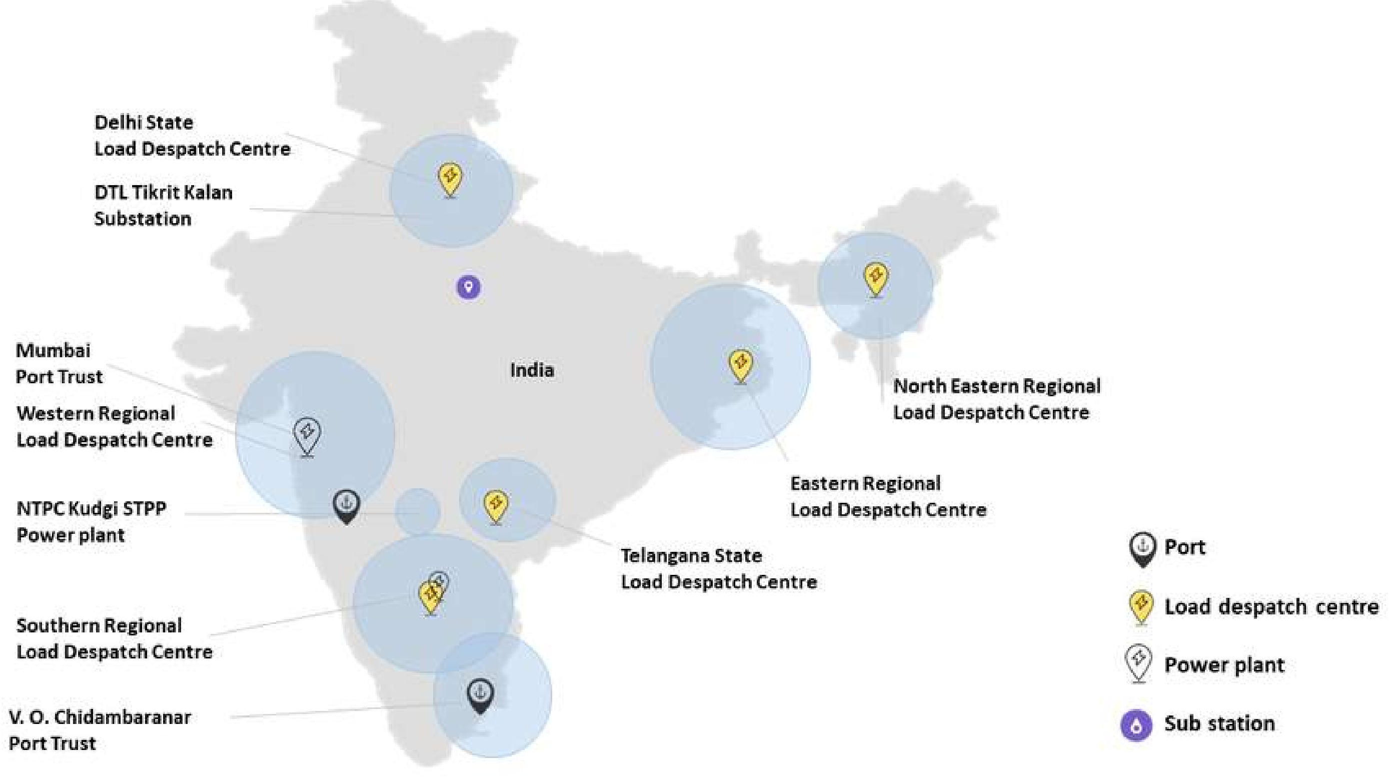

Delhi State Load Despatch Centre
DTL Tikrit Kalan Substation
Mumbai Port Trust
Western Regional Load Despatch Centre
NTPC Kudgi STPP Power plant
Southern Regional Load Despatch Centre
V. O. Chidambaranar Port Trust
India
North Eastern Regional Load Despatch Centre
Eastern Regional Load Despatch Centre
Telangana State Load Despatch Centre
Port
Load despatch centre
Power plant
Sub station

Fig: Suspected Indian power sector victims of RedEcho targeted intrusions (Source: Recorded Future, Map data ©2021 Google Map)

A total of 21 IP addresses resolving to 10 different Indian firms in the power production and transmission sector and two entities in the maritime sector were targeted. According to the Indian National Vital Information Infrastructure Protection Centre (NCIIPC) criteria, all 12 organizations are potentially critical infrastructures.

RedEcho performed alleged network breaches in India's electricity industry, targeting at least four of the country's five Regional Load Despatch Centres (RLDCs) and two State Load Despatch Centres (SLDCs). RLDCs and SLDCs are in charge of assuring India's power grid's real-time integrated functioning by balancing electricity supply and demand to maintain a steady grid frequency.

Additionally, local media reports attributed a power outage in Mumbai in October 2020 to discovering malware at a State Load Despatch Centre in Padgha. The supposed relationship between the blackout and the finding of an unnamed malware variant is now unproven. However, this information adds to the notion that Indian Load Despatch Centres were targeted in a coordinated manner.

TAG-38

TAG-38 is a China based hacking group. The hacking group, has used a kind of malicious software called ShadowPad, which was previously associated with China’s People’s Liberation Army.

TAG-38 Infrastructure Clustering

We uncovered a cluster of C2 infrastructure engaged in this prolonged targeting of Indian critical infrastructure over several months using proactive infrastructure detection techniques and network traffic analysis. The analysis identified that the adversary infrastructure cluster consists entirely of likely compromised internet-facing, third-party DVR/ IP camera devices. The compromise of often poorly secured internet-of-things (IoT) devices such as IP cameras for use in follow-on intrusion activity has previously been seen for threats ranging from Mirai-based botnets to the Chinese state-sponsored threat activity group RedBravo (APT31/ZIRCONIUM). They have not determined how these devices were originally compromised, which may include the use of default credentials. Using a series of analytical techniques and heuristics, we were able to cluster a network of these C2 IPs together, all of which matched all or most of the following criteria:

Network Indicator	First Seen	Last Seen
14.43.108[.]22	27-08-2021	31-12-2021
59.10.140[.]47	13-01-2022	02-02-2022
59.127.10[.]132	12-02-2022	15-03-2022
61.74.255[.]16	25-02-2022	15-03-2022
122.116.165[.]62	23-02-2022	15-03-2022
112.171.218[.]39	12-01-2022	13-02-2022
114.34.10[.]80	17-02-2022	15-03-2022
114.35.16[.]182	01-03-2022	20-03-2022
114.35.191[.]224	12-01-2022	22-02-2022
119.200.211[.]197	08-02-2022	03-03-2022
121.128.198[.]233	17-02-2022	13-03-2022
121.151.212[.]101	18-10-2021	23-12-2021
122.116.234[.]73	23-12-2021	13-03-2022
124.216.159[.]70	23-02-2022	21-03-2022
175.200.146[.]227	29-12-2021	17-02-2021
175.208.234[.]194	18-02-2022	21-02-2022
175.214.193[.]170	12-02-2022	21-03-2022
182.220.237[.]217	17-02-2022	22-03-2022
210.123.140[.]200	15-09-2021	02-03-2022
211.184.160[.]108	28-02-2022	22-03-2022
220.132.106[.]193	17-02-2022	15-03-2022
220.133.141[.]117	17-02-2022	15-03-2022

- Victim infrastructure observed communicating to all of the identified C2 servers consisted solely of the same overlapping Indian power grid victims, logistics company, and Indian emergency response system.
- All C2 servers were likely compromised DVR/IP camera devices and were primarily geolocated in Taiwan or South Korea.
- They observed potentially compromised devices with the default open ports 80-554-9090 associated with the compromised machine and additional actor-controlled ports opened for malware C2 communications.
- A large proportion was confirmed as ShadowPad C2 servers using Recorded Future C2 detection methodologies, a technique previously used in historical Insikt Group reporting on RedEcho and other Chinese state-sponsored activity groups

- Many identified C2s had the open-source tool Fast Reverse Proxy (FRP) server component configured on port 8443. FRP can read specified configurations and expose local services hidden behind NAT or a firewall to the internet. This tool has been abused by numerous state-sponsored groups, including the Iran-linked group Phosphorus and several Chinese actors
- A large proportion of the identified C2s shared a unique SSL certificate spoofing Microsoft on port 443 (SHA1 fingerprint: 0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf). This certificate has multiple links to wider Chinese state sponsored cyber espionage activity

Connection With Other China Threat Activity

We discovered many ties to other suspected Chinese state-sponsored operations while researching the TAG-38 intrusion. It's worth noting that the targeting and usage of ShadowPad are consistent with earlier RedEcho activity, and this latest activity involves a repeat SLDC victim. However, the infrastructure TTPs employed in this newest campaign differed significantly. We have yet to find enough technical evidence to link these two activity groups apart beyond the common targeting sets and capability use.

The use of a shared SSL certificate (SHA1 fingerprint 0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf) exhibited on several TAG-38 servers was also notable. This SSL certificate was also identified historically on a few dozen other servers with links to Chinese cyber espionage activity. For example, one of the IP addresses exhibited this certificate, 185.243.41[.]240, concurrently hosted several domains attributed to the group we track as TAG-26 referenced earlier in this report (including supership.dynv6.net, supermarket.ownip.net, and a great song. soundcast.me). We believe that the usage of this certificate is unlikely to be limited to a particular activity group at this time.

This is based on the wider context, such as differing targeting patterns, infrastructure TTPs, and capability use linked to the historically sighted infrastructure exhibiting this certificate, which may indicate a shared capability.

Subject: CN=www.microsoft.com
Issuer: CN=www.microsoft.com
Decimal: -3057430298263606566302079470361224100
Hex: 0xfdb3290c46b41fb24a0fefd16e565c5c
Validity: 2021-06-07 14:29:51 to 2039-12-31 23:59:59
Names: www.microsoft.com
SHA-256: B63e14d24e0893f85e80b4b94ad0bd800d6e105
70dc93ec56bbe75cd665385b0
SHA-1: 0f6afc6e4e383883a6308fcf8d84b14a5bf4ccaf
MD5: d06cc3e6f5673b2e9bfdac55944109a5

Similar threats

- This isn't the only threat to the electricity industry. Similar instances have occurred recently, all of which were disastrous.
- Dragos showed that the Russian military intelligence agency Sandworm has been spying on the United States' energy grid for years.
- Customers of Austin Energy have been warned about unknown foes posing as business employees and threatening to turn off their electricity until they pay a fictitious outstanding bill.
- An intruder tried to raise the sodium hydroxide levels at a Florida water treatment plant from 100 to 11,100 parts per million.

NTPC Warehouse
NTPC Kudgi STPP
NTPC Parking
DTDC Courier Service

Fig: Location of suspected victim NTPC Kudgi STPP (Source: Google Map)

Insikt Group tracks the network infrastructure used in ShadowPad infections as AXIOMATICASYMPTOTE. This technique fingerprints unique characteristics, including header responses and similar network components. We discovered that a subset of these AXIOMATICASYMPTOTE servers is being utilized by a China-linked activity group known as RedEcho to target a massive swath of India's power sector using a combination of proactive infrastructure detections, domain analysis, and network traffic analysis.

Mitigations

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in the appendix.
- Multiple state-sponsored and financially motivated threat activity groups use DDNS domains in network intrusion activity. All TCP/UDP network traffic involving DDNS subdomains should be blocked and logged (using DNS RPZ or similar).
- All domains using eznowdns.com as an authoritative nameserver should be blocked and logged (using DNS RPZ or similar).
- Recorded Future Threat Intelligence, Third-Party Intelligence, and SecOps Intelligence module users can monitor real-time output from Network Traffic Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Monitor for domain abuse, such as typosquat domains spoofing your organization through the Recorded Future Brand Intelligence module.

Vulnerable area of a power grid

Hardware Layer

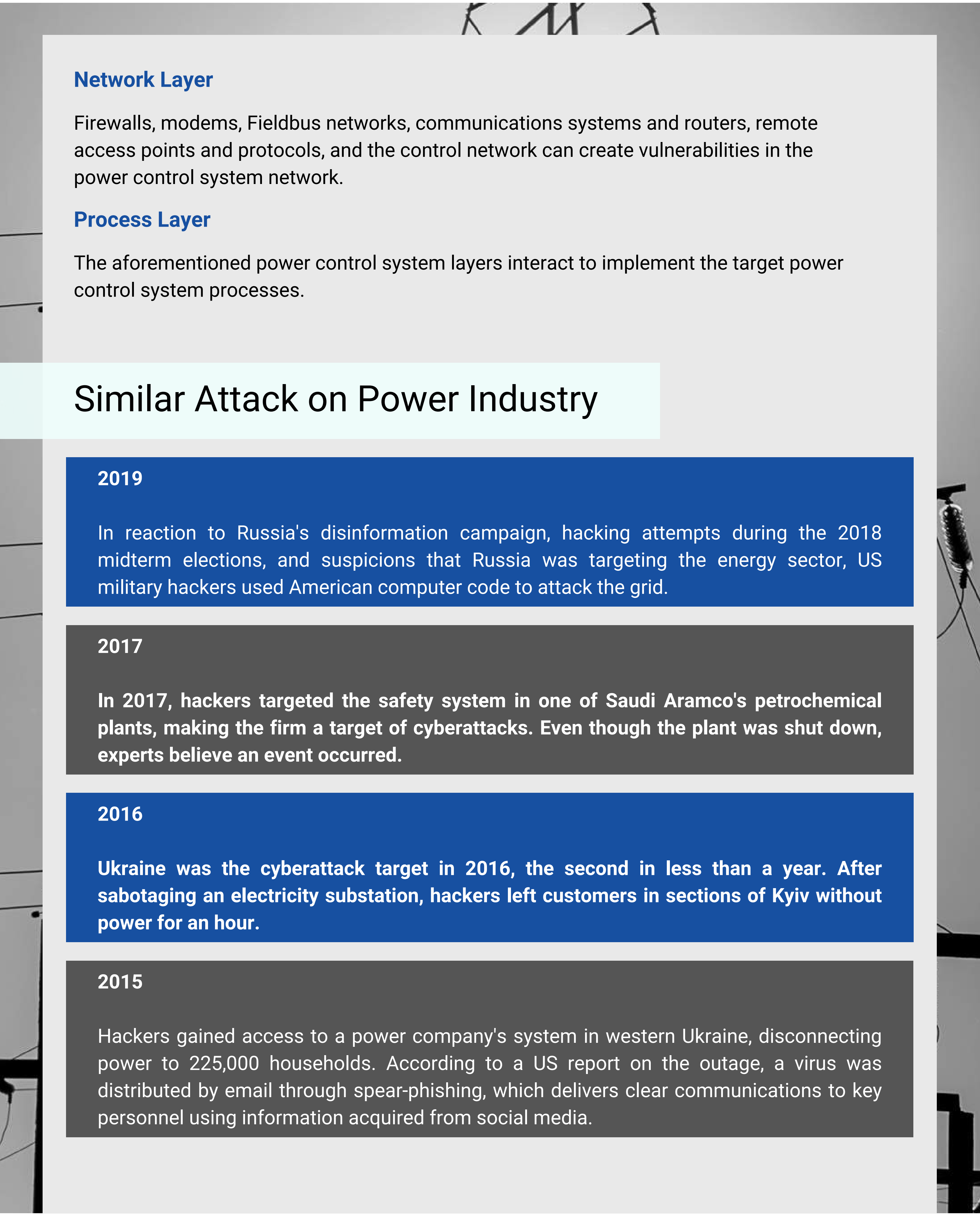
Embedded components, such as Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU), are hardware modules that run software to communicate and control information.

Firmware Layer

Between the hardware and the program is the firmware. It contains data and instructions that allow the hardware to be controlled.

Software Layer

Power Control Systems use several software platforms and applications, and software vulnerabilities can vary from minor coding flaws to improper access control implementation.



Network Layer

Firewalls, modems, Fieldbus networks, communications systems and routers, remote access points and protocols, and the control network can create vulnerabilities in the power control system network.

Process Layer

The aforementioned power control system layers interact to implement the target power control system processes.

Similar Attack on Power Industry

2019

In reaction to Russia's disinformation campaign, hacking attempts during the 2018 midterm elections, and suspicions that Russia was targeting the energy sector, US military hackers used American computer code to attack the grid.

2017

In 2017, hackers targeted the safety system in one of Saudi Aramco's petrochemical plants, making the firm a target of cyberattacks. Even though the plant was shut down, experts believe an event occurred.

2016

Ukraine was the cyberattack target in 2016, the second in less than a year. After sabotaging an electricity substation, hackers left customers in sections of Kyiv without power for an hour.

2015

Hackers gained access to a power company's system in western Ukraine, disconnecting power to 225,000 households. According to a US report on the outage, a virus was distributed by email through spear-phishing, which delivers clear communications to key personnel using information acquired from social media.

2014

Korea Hydro and Nuclear Power (KHNP), a South Korean nuclear and hydroelectric power business, was hacked in 2014. Hackers stole the designs and manuals for two nuclear reactors and the personal information of 10,000 personnel and uploaded them online.

References

https://www.power-technology.com/analysis/the-five-worst-cyberattacks-against-the-power-industry-since2014/

https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

https://www.recordedfuture.com/continued-targeting-of-indian-power-grid-assets/

https://wikipedia.org/wiki/Ukraine_power_grid_hack

https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

ATHENIAN TECH

Contact Us

arvind@atheniantech.com

www.atheniantech.com