CYBER SECURITY OUTLOOK FOR PAKISTAN

FAROOQ NAIYER*

The Global Threat Landscape in 2019

Back ground

Year 2019 has been an interesting year in terms of state and non-state actors in the cyberspace. There has been significant growth in cyber-crime. It is quite evident that several countries paid lip-service to curbing cyber space activities, but behind the scenes, they expanded their cyber espionage operations, besides making further forays into destructive attacks and financially motivated fraud. Non-state actors engaged in cybercrime demonstrated new-found flexibility, forming and breaking alliances and quickly changing tactics mid-campaign to achieve their objectives. The shifting currents of the underground economy — including the availability of new resources (cyber mercenaries for hire) and the fluctuating value of crypto currencies — were all contributing factors. The world also saw a significant rise in "Big game hunting" where cyber-crime actors combine targeted intrusions with ransomware to extract big payoffs from large public and private sector organizations, with the local governments and municipalities bearing the brunt of it.

The world is in a veritable "arms race" for cyber superiority. However, there are some important differences between an arms race in the cyber sphere versus the physical world: In cyberspace, any player can potentially become a superpower. The capital costs are alarmingly low, compared to funding a physical war machine. Even some of the world's most impoverished regions proved their ability to make a global impact through cyber campaigns in 2019.

Pakistan's Cyberattack Readiness

In the summer of 2019 a leading VPN provider aggregated threat-report data from Secure list including Global Cybersecurity Index (GCI) scores for cyberattack readiness. Developed by the International Telecommunication Union (ITU), GCI scores countries' cybersecurity readiness on a scale of 0.0-1.0 based on a composite of five key factors:

- **Legal**: Legal institutions and frameworks for dealing with cybersecurity and cybercrime.
- **Technical**: Technical institutions and frameworks dealing with cybersecurity.
- **Organizational**: Policy coordination institutions and strategies for cybersecurity development at the national level.
- **Capacity Building**: Research and development, education, and training programs; certified professionals, and public sector agencies dedicated to cybersecurity.
- **Cooperation**: Partnerships, cooperative frameworks, and information sharing networks.

Pakistan was ranked at number two amongst the worst prepared countries for cyber-crime with a rating of (0.447), behind Ecuador, which took the top spot. The countries that scored highest were those with more developed infrastructure and technical capabilities. In the top 10, Singapore scored highest at 0.925, followed by the US at 0.919 and Malaysia at 0.893. France and Canada

round out the top five at 0.819 and 0.818, respectively

Tensions in South Asia

Advanced Persistent Threat (APT) activity in India and Pakistan witnessed a sharp increase over the first six months in 2019: Based on the analysis of leading Cyber Security Incident Response Teams (CERTS), the escalation was due to rising tensions between the two countries in the early part of the year. The sheer number of individual campaigns and associated malware samples spiked dramatically during most part of the year. Increasing tensions in the region have contributed to both countries prioritizing intelligence-gathering activities against one another. This has had a domino effect, since neighboring countries gather intelligence on both in order to keep tabs on the situation.

India has one of the world's largest militaries, which is used, among other things, to assert the territorial boundaries it shares with six neighboring countries — an ostensible motivation in India's APT targeting. Pakistani APT targeting is heavily focused on India, but also gathers intelligence on other neighbors and keeps tabs on internal dissent.

The cyber component of this hostile relationship dates to the early 1990s. APT motives include traditional intelligence-gathering operations and credential theft for follow-on operations. The specific campaigns the two countries launch against each other are nearly always in sync with the geo political situation, current events and government priorities. With a right-wing fascist regime firmly in power in India, with more than two thirds of majority in its second term in India, such campaigns have increased and are more likely

Both countries typically combine freely available malware with custom code. Often, malware that is used in one campaign will be later modified by the victim country and reused against the originator, making malware-based attribution fraught with error. The two countries utilize Android malware, a good investment since both countries appear on the Top 50 Countries/Markets for Smartphone Users and Penetration list. While both countries' early iterations were an amalgamation of free malware with custom code, later versions, such as Pakistan's Stealth Mango/Tangelo malware, were identified as an entirely new malware family. Most of the time, however, both India and Pakistan successfully conduct operations with simple, freely available malware that relies heavily on a phishing-based campaign. Their operating style serves as a reminder that most APT groups are defined by being nation-state sponsored, not by having sophisticated technique and pioneering technological prowess.

Other Targets

The adversaries targeting Pakistan have been specifically going after government officials, businessmen, and diplomats residing in or visiting other countries. Embassy targeting remains popular. Businesses in Europe and the United States, especially defense contractors involved in missile technology, aeronautics and aviation, have also been targeted. In those cases, the attackers are interested in their businesses' operations in South Asia. Theft of missile technology data has happened more than once.

The financial sector of Pakistan saw a rise in APT activities in the latter part of 2018, which led to a potential financial loss of about $6 million for one of the banks and compromise of a significant number of credit and debit cards, which surfaced

on the dark web. In the latter part of 2019 particularly early December 2019 at least 5 leading banks were defaced over a period of few hours followed by several fraudulent fund transfers, which were then tracked by the payment switch in a timely manner.

In December 2019 it was also revealed that mobile phones of at least two dozen Pakistani government officials were allegedly targeted earlier this year with technology owned by the Israeli spyware company NSO Group.

> Guardian reported: "Scores of Pakistani senior defence and intelligence officials were among those who could have been compromised, according to sources familiar with the matter who spoke on the condition of anonymity. The alleged targeting was discovered during an analysis of 1,400 people whose phones were the focus of hacking attempts in a two-week period earlier this year, according to the sources. All the suspected intrusions exploited a vulnerability in Whatsapp software that potentially allowed the users of the malware to access messages and data on the targets' phones. The discovery of the breach in May prompted WhatsApp, which is owned by Facebook, to file a lawsuit against NSO in October in which it accused the company of "unauthorised access and abuse" of its services. The lawsuit claimed intended targets included "attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials".

5th Generation Warfare

In November 2019 Researchers discovered a network of 265 fake local news sites — named after defunct newspapers and media outlets — across 65 countries that were being used to disseminate anti-Pakistan coverage and serve Indian governmental interests.

Uncovered by the EU DisinfoLab, an EU based NGOfocused on researching sophisticated disinformation campaigns, the operations were traced back to a group of Indian companies, NGOs, and think tanks.
The sites — such as 4newsagency.com, eptoday.com, and timesofgeneva.com — operated by serving syndicated news from Russia Today and Voice of America. But the researchers said they "unexpectedly" found many articles and op-eds related to minorities in Pakistan as well as other India-related topics.

"Times of Geneva publishes the same type of content as EP Today and produces videos covering events and demonstrations criticizing Pakistan's role in the Kashmir conflict," the EU DisinfoLab noted.

By piecing together the campaign to an online media company — interchangeably called as International Institute for Non-Aligned Studies (IINS), New Delhi Times, and the Srivastava Group — the EU DisinfoLab believes the goal was to influence public perceptions on Pakistan by multiplying the same negative anti-Pakistan press coverage across hundreds of sites.

More troublingly, a network of zombie companies was found lobbying the EU and the UN by repeatedly criticizing Pakistan — a move that culminated in a group of 27 EU parliamentarians, mostly from right-wing political parties, visiting

Occupied Kashmir Valley upon an invite from IINS.

"The idea seems to have been an effort to control the conversation around what is happening in the region," BBC reported on the EU delegate visit.

In the earlier part of 2019 hundreds of twitter accounts were identified by twitter and shut down for launching various disinformation campaigns.

Future outlook, threats to critical infrastructure and Strategic initiatives including CPEC

The geo-political situation has evolved a lot given the fact that China now has strategic interests in the region in the shape and form of CPEC and defence cooperation with Pakistan. This has led to adversaries planning to cause all kinds of hurdles and disruptions in the cyber space and beyond. The primary targets are the strategic assets including the nuclear program, nuclear power plants, missile development programs; telecommunications back bone; power grids and distribution companies; gas distribution system.

State Actors such as Israel and the US could launch a Stuxnet type of a malware attack on any supervisory control and data acquisition (SCADA) based systems in Pakistan i.e. not limited just to the nuclear program but can impact our power grids or other infrastructure in Pakistan that are supported by such systems. Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including centrifuges for separating nuclear material. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart.

Based on the trends in late 2018 and early 2019 which saw a rise in attacks on wired telecommunications carriers and telecommunications, Pakistan's telecommunication infrastructure can be a target by state and non-state actors in the region in near future.

Key Steps to be taken by the Government

Tactical

- User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques, such as 2018's massive Emotet outbreak.
- Asset management and software inventory are crucial to ensuring that organizations understand their own footprint and exposure.
- Deploy with Secure perimeters: Deploy all devices and services within secure perimeters (secure VLANs with firewalls controlling access).
- Block Access: Block access to all services except where absolutely required.
- Require Security Best Practices: Require that internet of things (IoT) and customer-premises equipment (CPE) vendors follow best security practices but also treat those devices as potential infection vectors.
- Vulnerability and patch management can verify that known vulnerabilities and insecure configurations are identified, prioritized and remediated.
- Multifactor authentication (MFA) should

be established for all users because today's attackers have proven to be adept at accessing and using valid credentials, leading quickly to deeper compromise. MFA makes it much more difficult for adversaries to gain privileged access. In addition to MFA, a robust privilege access management process will limit the damage adversaries can do if they get in. It would also reduce the likelihood of lateral movement.

- Implement password protection to prevent disabling or uninstalling endpoint protection that provides critical prevention and visibility for defenders. Disabling it is always a high-priority for attackers looking to deepen their foothold and hide their activities

Strategic

- Cyber Security Policy and Framework: The Federal Government needs to develop and implement an overarching cyber security policy in order to develop a strong cyber security posture.
- Cyber Security Incident Responses teams: Need of the hour is to have CERTS established at the national level and at all critical organisations of the country under the umbrella of the National and provincial Information Technology (IT) Boards.
- Data Protection Bill: Data protection bill is being worked on as we pen this article by several civil rights groups in Pakistan. The Ministry of IT should initiate consultation process with public and private stakeholders to draft a law in line with internal conventions and standards on data privacy and protection.

Farooq Naiyer

Mr Farooq Naiyer is the chief information security officer at ORION, which is the largest research and education network in Canada. He has vast experience in cybersecurity, privacy, technology compliance and assurance.