Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022

XVigil data indicates that the number of attacks targeting the government sector has increased by 95% in the second half of 2022, as compared to the same period in 2021. About 40% of the attacks targeted government entities in India, USA, Indonesia, and China.

Authors: Hansika Saxena and Aastha Mittal

Table of Contents

Table of Contents 1

Scope of Cyber Threat Landscape in the Government Sector 2

History of Cybercrime in the Government Sector 3

What Drives the Threat Actors? 4

Prominent Threat Actors 5

- KelvinSecurity 5
- AgainstTheWest 5

Most Targeted Regions 6

- China Emerges as the Most Targeted Country in 2021 7
- Attacks Against India Increase More than Double 7
- Sudden Spike in Attacks on Russia 7

The Era of Cyber Warfare 8

- Russia-Ukraine War 8

Using Hacktivism to Take a Stand 9

Significant Attacks on Government Entities 10

- Costa Rican Ransomware Attack 10
- Cyber Attacks on Ukraine 10
- US Federal Network Log4j Vulnerability 11

Impact 11

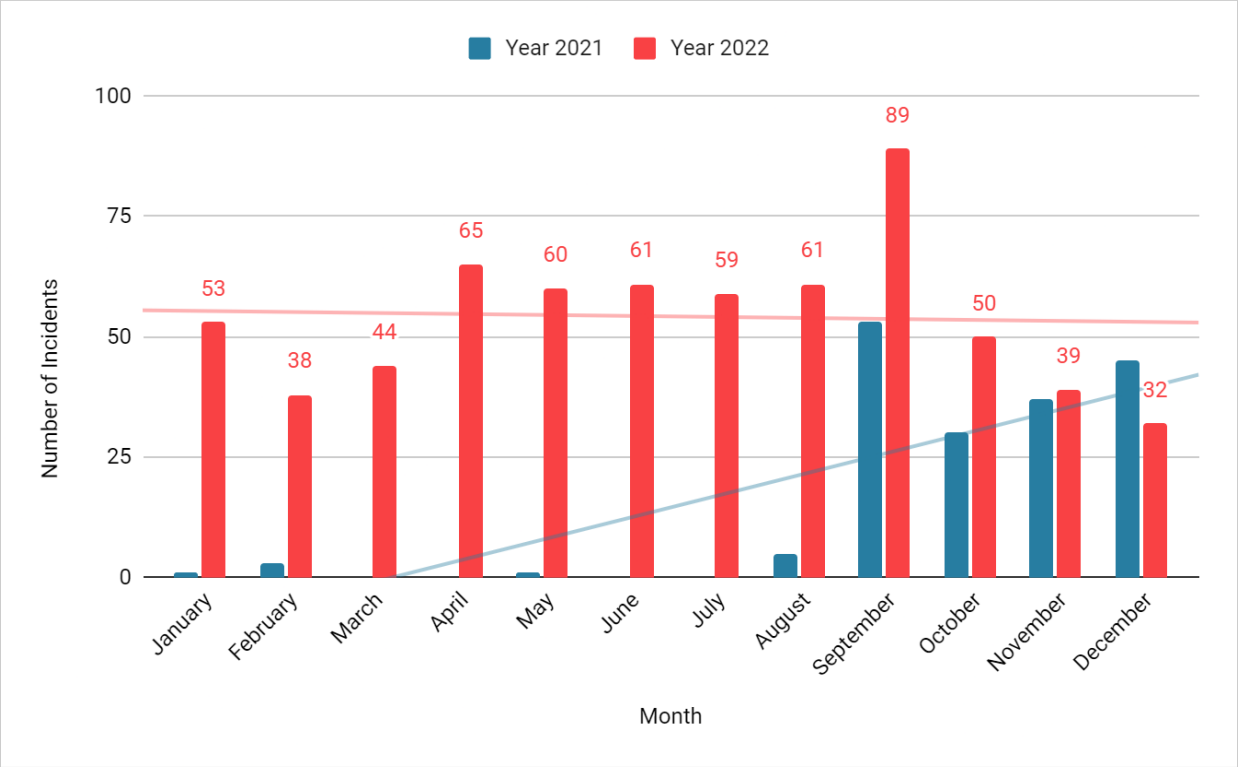
The Way Forward 12

References 13

About CloudSEK 13

Scope of Cyber Threat Landscape in the Government Sector

The government sector has emerged as a prime target for cybercriminals in 2022. Data gathered by XVigil suggests that the number of attacks targeting this sector has **increased by 95%* in the second half of 2022**, as compared to the same period in 2021. COVID-19 driven rapid digitization in this sector has not only increased the attack surface for threat actors but has also allowed governments to use cyber warfare as a tool to target other countries.



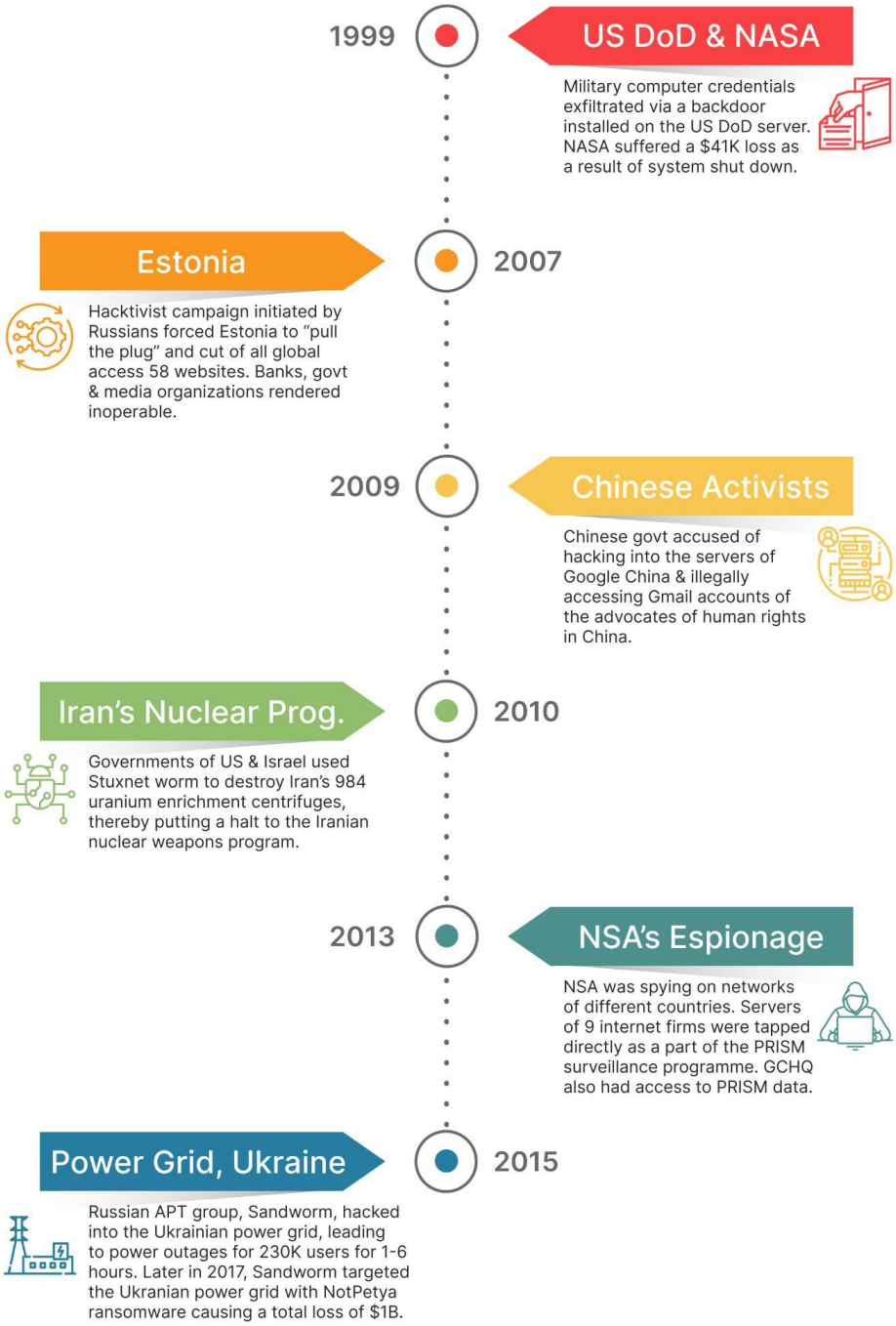
Number of cyber incidents targeting the government sector recorded in the past two years

Cyberattacks have often been used to target governments during wartime. The first instance where technology was used to win wars was the use of the Turing machine to unravel the secret messages encrypted using the German Enigma. Over the years, threat actors have developed more tools and acquired a more sophisticated skillset to target governments (military and otherwise). In this article, we delve into the various aspects of cybersecurity concerning the government sector.

***Note: The insights and distribution of threats by region are contingent on the presence of our clients in those regions.**

History of Cybercrime in the Government Sector

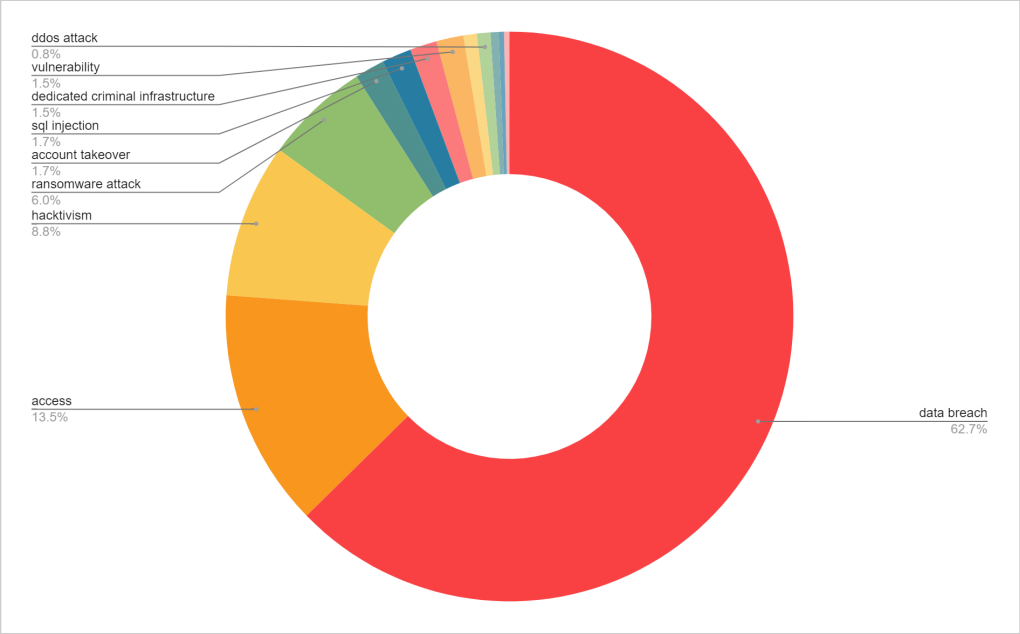
Cyber attacks on government entities is not a new phenomenon. Over the years, financially motivated threat actors, hacktivists, and state-sponsored groups have leveraged vulnerabilities in government infrastructure, along with social engineering, to wreak havoc. Here are some significant incidents that have paved the way for the current increase in attacks on government entities.



What Drives the Threat Actors?

Over the years threat actors have evolved immensely in the way they operate. Although the primary motive of most of the threat actors is exfiltrating data and selling it for monetary benefit, it is not the only reason they target government entities. This change is clearly evident from the emergence of various APT groups and hacktivist campaigns over the last decade. The year 2022 saw a significant increase in **hacktivist activity, which accounted for about 9% of the recorded incidents** reported in the government sector. Ransomware groups were also very active in this industry accounting for 6% of the total incidents reported, with LockBIT as the most prominent ransomware operator.

These statistics are suggestive of the fact that cyberattacks in this particular industry are no longer limited to financial gains; rather, they are now used as a means to express support or opposition for certain political, religious, or even economic events and policies.

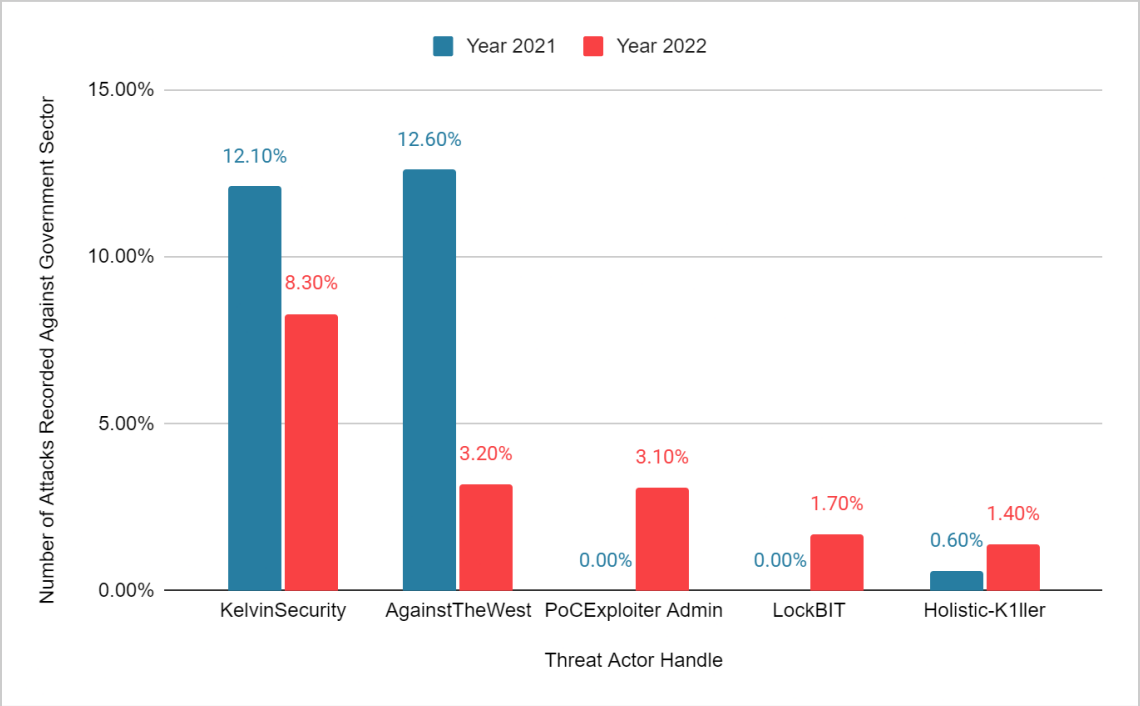


Attack vectors targeting the government sector in 2022

While the majority of attacks were related to compromised data and access, there were also a few attacks conducted to help highlight the various flaws in the country's security posture and help improve it. A series of such attacks were observed against government entities in Indonesia. The number of government-sponsored attacks has also multiplied. However, there is no exact figure for this increase since these attacks are difficult to trace. This growth can primarily be attributed to the advent of offerings such as initial access brokers (IABs) and ransomware-as-a-service (RaaS). Threat actors have started developing and advertising services of dedicated criminal infrastructure which can be bought by governments (or individuals) and used for various nefarious purposes.

Prominent Threat Actors

Given the various ups and downs faced by this sector, it is notable that the top two threat actors targeting this industry have remained the same in 2021 and 2022.



Top 5 threat actors targeting the government sector in 2022

KelvinSecurity

- Mostly seen operating under the handle **Kristina,** this group is in top two actors in 2021 and 2022.
- The group uses targeted fuzzing and exploits common vulnerabilities to target victims. Being highly skilled in the use of tools and having a wide knowledge of various exploits, they share their list of tools and payloads for free.
- They typically target victims with common underlying technologies or infrastructure at any given time.
- The group doesn't shy away from attention and publicly shares information such as new exploits, targets, and databases on cybercrime forums and communication channels such as Telegram.
- They also have a data leak website where other threat actors can share databases.

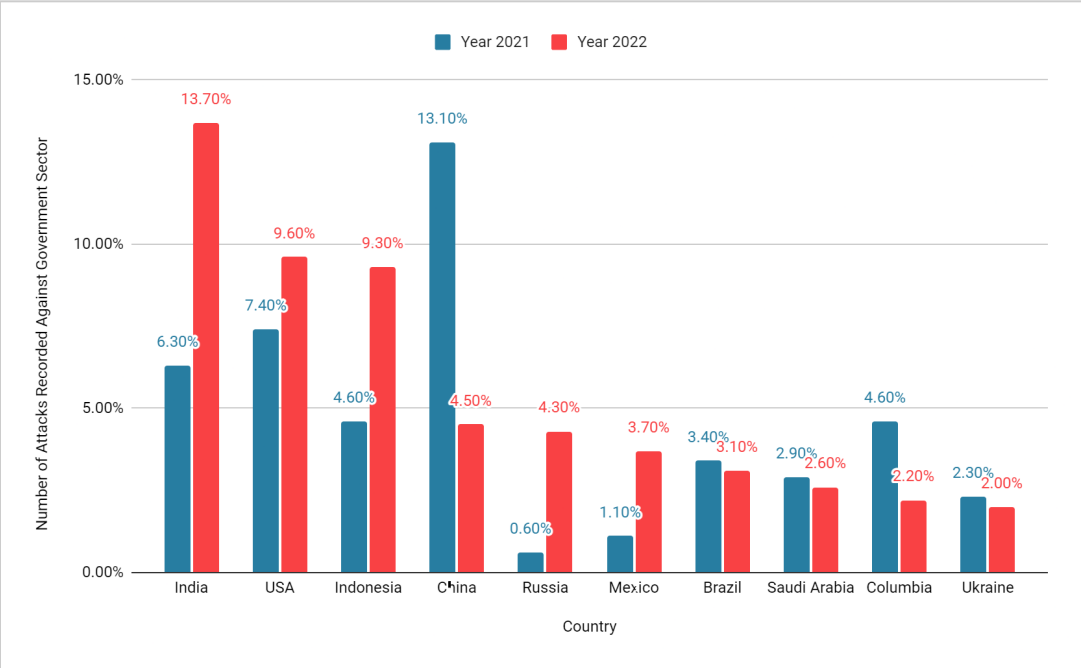
AgainstTheWest

- Having emerged in October 2021, this group identifies itself as an APT49 or, BlueHornet. They have been highly focused on exfiltrating region-specific data and selling it on the dark web.

- Based on their previous activity they appear sophisticated, skilled, and organized.
- The group has been targeting various countries under campaigns including **Operation Renminbi**, **Operation Ruble, Operation EUSec, etc**.
- Time and again they collaborate with different threat actors to target various nations.
- The group has been constantly exploiting a common set of vulnerabilities and exploits to target multiple countries.
- A confidential source in contact with the group ascertained that the group was exploiting **SonarQube zero-day and Swagger UI** vulnerabilities.
- They used to have an Onion website as an alternative store to purchase data compromised by them.

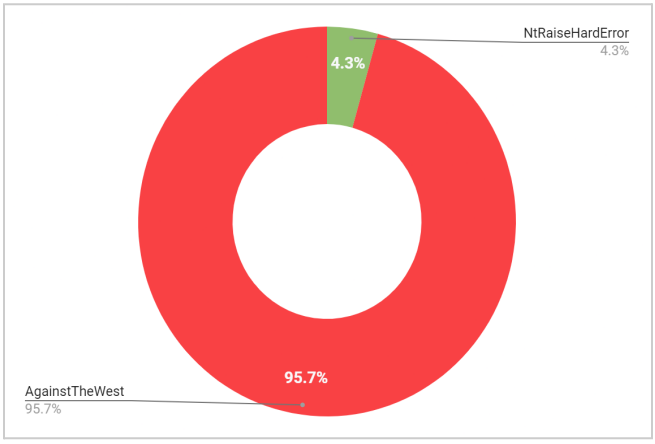
Most Targeted Regions

India, USA, Indonesia, and China continued to be the most targeted countries in the past two years. Together, these four countries accounted for ~40% of the total reported incidents in the government sector. There are three interesting findings observed in the variations in the number of attacks from 2021 to 2022.



10 most targeted countries in the government sector in 2022

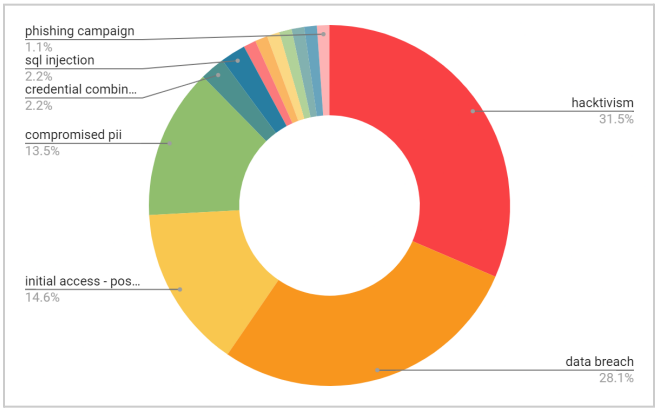
China Emerges as the Most Targeted Country in 2021



Threat actors responsible for attacks against China in 2021

The significant hike observed in the number of attacks targeting the Chinese government can be attributed to APT groups. Almost **96%** of attacks against China were initiated by AgainstTheWest, under their campaign **Operation Renminbi** which began as retaliation to China's activities against Taiwan and the Uyghur community. It is also speculated that conspiracy theories about China being responsible for the outbreak of COVID-19 may have contributed to the increase in attacks.

Attacks Against India Increase More than Double



Threat actors' favored attack vector against India in 2022

In 2022, attacks on the Indian government intensified to the point where it became the country that was most frequently targeted in this sector. This expansion is the result of the hacktivist group Dragon Force Malaysia's #OpIndia and #OpsPatuk campaigns. Numerous hacktivist groups joined and supported these campaigns, which laid the path for subsequent ones.

Government agencies in India have become popular targets of extensive phishing campaigns.

Sudden Spike in Attacks on Russia

Attacks on Russia went up by over 600% owing to the ongoing Russia-Ukraine war. Russia's invasion of Ukraine fueled saw concerted cyber attacks on government entities and critical infrastructure of both countries. State-sponsored actors and activists showed their support for Ukraine by targeting Russia, thus converting it into a widespread cyber war.

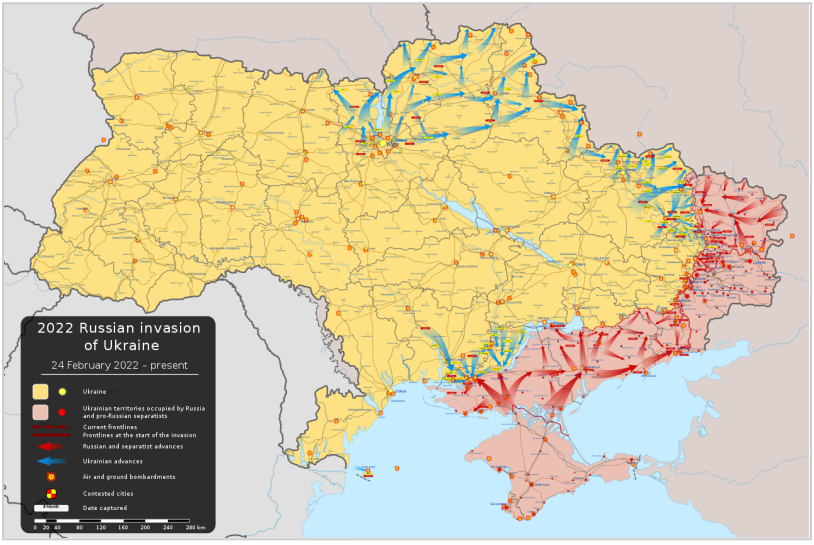
The Era of Cyber Warfare

Cyberwarfare is a cyberattack or series of cyberattacks launched against an enemy state. Cyber warfare involves weaponizing hacking to both initiate attacks and prevent cyber attacks. Cyberwarfare can cause comparable harm to actual warfare and civilian life. Although cyberwarfare generally refers to cyber attacks perpetrated by one nation-state on another, it also includes terrorist groups or cyber threat actor groups aimed at furthering the cause of a nation or a political agenda. Cyber warfare can sabotage the electric and physical assets of a nation, and cause physical-world disruptions, along with economic damage.

Russia-Ukraine War

Long-standing political tension between Russia and Ukraine has resulted in multiple cyber attacks being used as a component of confrontation between the countries. Some of the significant cyber attacks over the past years include:

- Ukraine power grid hacks in 2015 and 2016
- Attacks against Ukrainian websites using the Petya virus in 2017
- Hacking of corporate servers of Russian “Channel One” in 2016
- Compromise of emails and documents allegedly belonging to Russian political operative Vladislav Surkov in 2016



Zones of control in Ukraine as of 8 December 2022 (Source: Wikipedia)

The recent Russia-Ukraine war predictably increased the number of cyberattacks faced by the governments of both countries. Cyber attacks against the Russian government particularly increased, which was likely caused due to multiple hacktivists, along with various governments, supporting Ukraine against Russia. The government sector of Russia became the 5th most targeted in 2022.

Using Hacktivism to Take a Stand

In 2022 hacktivists made their presence felt by launching concerted campaigns and collaborating with each other to cause large-scale disruptions. They also employed social media to rally other threat actors and civilians, to collaborate with each other, and to publicize their attacks and motives.

Name of Campaign	Target	Initiator	Motivation
OpSaudi	Saudi Arabia	YourAnonRiots	Multiple government websites from Saudi targeted for various reasons
OpsBantaiKaw2	India	Khalifah Cyber Crew	Protest against "Muslim discrimination" by Indian government
OpAmerika	USA	Hacktivist of Garuda	Targeting American firms if any exploit it discovered
OpIndonesia	Indonesia	Indian Cyber Commandos	Retaliation to the attacks by hacktivists from Indonesia and Pakistan
OpIran	Iran	KromSec Group, GhostSec	Protest against the execution of Mahsa Amini
OpNicaragua	Nicaragua	GhostSec Group	Demanding resignation of Nicaraguan President
OpIndia/OpsPatuk	India	DragonForce	Protest against Indian politician's controversial comments on Prophet Muhammad
OpBangladesh	Bangladesh	Hacktivist of Garuda	News headline "At least 398 people were killed and 774 injured in 319 road accidents from July 3 to 17, the Bangladesh

			Passenger Welfare Association says”
OPBRICS	BRICS (Brazil, Russia, India, China, South Africa)	YDIO Group	Against the five major emerging economies Brazil, Russia, India, China and South Africa
OpIsrael	Isreal	Anonymous Hackers	Annual campaign to commemorate Holocaust Remembrance Day
OpCambodia	Cambodia	Desorden	Against human and organ trafficking
OpJane	USA	SiegedSec Group	Against the anti-abortion laws

Significant Attacks on Government Entities

Costa Rican Ransomware Attack

In May 2022, the Costa Rican government declared a state of emergency after facing multiple cyberattacks starting in April. A ransomware attack was launched against nearly 30 government institutions, including the Ministry of Finance, the Ministry of Science, Innovation, Technology and Telecommunications (MICITT), the National Meteorological Institute, and the state internet service provider RACSA.

The Conti group claimed responsibility for the first group of attacks and demanded a ransom of USD 10 million in exchange for not leaking the information stolen from the Ministry of Finance. As a result, the government had to shut down the computer systems used to declare taxes and for the control and management of imports and exports, causing a loss of USD 30 million per day to the productive sector. 50% of the stolen government data was published on Conti’s extortion website.

Cyber Attacks on Ukraine

During the 2022 Russian invasion of Ukraine, multiple cyberattacks against Ukraine were reported. On 14 January 2022, more than a dozen Ukrainian government websites were taken down. Around 70 government websites, including the Ministry of Foreign Affairs, the Cabinet of Ministers, and the Security and Defense Council, were targeted. Most of the websites were restored within a few hours. It is

suspected that a third-party company's administrative rights were used to carry out the attacks. In February multiple DDoS attacks were carried out, affecting the websites of the defense ministry, army, and various banks. In retaliation, the IT Army of Ukraine was established, with the primary target being cyberwarfare against Russia.

US Federal Network Log4j Vulnerability

In November 2022, one of the US federal networks was exploited by taking advantage of the Log4Shell vulnerability in an unpatched VMware Horizon server. XMRig crypto mining software was installed on the server to move laterally to the domain controller (DC), compromising credentials, and then Ngrok reverse proxies were implanted on several hosts to maintain persistence. Passwords of a local administrator account on several hosts as a fail-safe in case the rogue domain admin account was flagged and terminated. The attack affected several departments of the US government including the Department of the Treasury, the Department of Commerce, and the Department of Homeland Security. According to the FBI and CISA, Iranian state-sponsored cyber criminals were responsible for the attack.

Impact

Government entities collect and store huge amounts of data ranging from information about individual citizens that can be sold on the dark web, to issues of national security and military data that can be used by terrorist organizations. Government entities, due to the size and scale of their operations, often overlook standardized cybersecurity practices and vulnerable systems.

Cyber attacks on government entities could lead to the exposure of sensitive data, financial loss for the state, often in the form of ransom payments and recovery costs, and even widespread panic and misinformation. The leaked data can then be future leveraged to target citizens via social engineering campaigns. According to an IBM report, the average total cost of a breach in the public sector increased from USD 1.93 million to USD 2.07 million, indicating a 7.25% increase.

The Way Forward

Governments need to increase their cybersecurity capabilities and implement policies that ensure that data and critical infrastructure is not vulnerable to threat actors. This includes building strong capabilities for detection, response, reconnaissance, and recovery. They should have a clear understanding of which data and IT infrastructure they are working with, the sensitivity of the data, and provide limited access. Cybersecurity is more than an IT problem, and the management and general employees should similarly be trained in responsible cybersecurity practices.

The government's role should not be limited to securing the public networks, national cyber defense depends on the security of both public and private networks. Collaboration with the private sector means sharing information about vulnerabilities, threats, and remedies among a community of governments, companies, and security vendors. Combining threat intelligence from multiple entities creates a strong collective intelligence, which helps in assessing adversaries and predicting future threats.

The exponentially increasing number of cyberattacks means that governments don't just need to fend off cyber attacks, rather they need to shift to a zero-trust model, wherein it is preemptively assumed that the user identities or the network itself may already be compromised, proactively verifying the authenticity of user activity. According to IBM, "organizations with zero trust deployed saved nearly USD 1 million in average breach costs compared to organizations without zero trust deployed". Governments should continuously monitor the dark web and known threat actors to understand their latest TTPs and take measures to preempt attacks. They should also proactively monitor their infrastructure and networks for vulnerabilities and suspicious behavior. Aside from traditional pen testing, governments should also focus on bug bounty programs and vulnerability disclosure programs.

References

- Increased Cyber Attacks on the Government Sector in Indonesia - CloudSEK
- Hacktivist Group Summons Allies and Hackers to Unite Against Govt. of India - CloudSEK
- Profiling YDIO, the Blackhat Group Behind #OpBRICS - CloudSEK
- Multiple Indian Entities Targeted by the Khalifah Cyber Crew Under the #OpsBantaiKaw2 Campaign - CloudSEK
- Russo-Ukrainian War - Wikipedia
- OpIsrael - Wikipedia
- Hacktivism - Wikipedia
- 2022 Costa Rican ransomware attack - Wikipedia
- 2022 Ukraine cyberattacks - Wikipedia
- Cost of a data breach 2022 | IBM
- The Consequences Of Cyber Attacks And Their Impact On Cybersecurity
- Government's cyber challenge
- The Impact of a Cybersecurity Incident or Breach on Governments
- Cybersecurity and the government | Deloitte Insights
- Government's cyber challenge
- Iranian APT Uses Log4j Vulnerability To Hack US Federal Network | Security Insights By PurpleSec

About CloudSEK

CloudSEK is a contextual AI company that predicts Cyber Threats.

At CloudSEK, we combine the power of Cyber Intelligence, Brand Monitoring, Attack Surface Monitoring, Infrastructure Monitoring and Supply chain to give context to our customers' digital risks.

To learn more about CloudSEK, visit https://cloudsek.com/.