Features | Internet AUTHOR: ONKAR SHARMA - NOVEMBER 26, 2015 Share Twitter

No comments

APTs can end the world

The recent terror attack on Paris has suddenly woken up the west to raise an offensive against the growing threat of terror. More so against the cybercrime and cyber terror which are potentially destroying critical infrastructure. The Paris attack is the first attack where the terrorists used cyber space equally to coordinat and execute their plans. The way it went undetected amazed the security experts.

To understand the collateral damage a Cyber attack can do, it is important that we revisit the Operation Olympic Games, which was nothing but a Stuxnet attack on Iran. It was launched by the United States. Th was aimed at disrupting Iran's nuclear bomb program. The attack literally damaged Iran's centrifuge and delayed its uranium enrichment efforts. The operation was successful. The US President Obam had then expressed concern about collateral damage in the U.S.-Israeli cyber attack on Iran's nucle program. Obama was aware of the excuses other nations might make while justifying their cyberattacks against others.

In Iran's case, the attacks were justified as Iran might trigger the nuclear war the world has not see since the World War 2. The Stuxnet worm raises key questions around the magnanimity of cyber weapons and indicates higher possibilities of the war which might see least use of the traditional weapons, bullets, warplanes, tanks and submarines but see nations fighting over the cyber space ar destroying or paralysing each other's critical infrastructure such as power grids, nuclear plants, banks, manufacturing units, and government networks, etc.

Cyber experts often share their concerns around the motivated cyber attacks aimed at organizatio and countries to cripple them financially, economically and physically. This is just an example of things that might go out-of-control in the near future risking the lives of millions of people at a fraction of the second.

Cyber Terror Groups

Future looks even hazier as we bring into picture the pernicious and destructive intentions of the terror groups which have in recent times targeted governments, groups and organizations. For terrorist groups, cyber space is becoming a tool of luring people into their network and launching cyber terror attacks on any individual, organization, group or state. "This is the time that global effo is made to achieve a common goal in the cyber space," called Indrajeet Banerjee, director, UNESCC at an event on Cybercrime, Cyberlaw and Cybersecurity in Delhi.

Data Center

Data center JANUARY 12, 2016

Huawei names William Zhao as chief operating officer of India R&D centre

Huawei today announced the appointment of William Zhao as the new Chief…

READ MORE Share

The CIO Takes Back Control with Hybrid IT

0 - DECEMBER 14, 2015

5 ways to improve your Data Center efficiency

0 - DECEMBER 1, 2015

How the next major meta trend in networking will reshape businesses

0 - NOVEMBER 18, 2015

How a cloud integrator can empower your company

0 - NOVEMBER 12, 2015

Gartner says data center infrastructure market in India to reach $2 billion in 2016

0 - NOVEMBER 5, 2015

Scared of the bigger and far more formidable cyber attacks, one of the security expert and practitioner, "Terror groups have become organized and have learned to exploit the web to damag the critical infrastructure of any country. In a world where we are inching closer to adopting IoT in bigger way, we recommend that we protect critical infra such as smart cities, power grids, government buildings and other things with utmost urgency."

Fears of a possible massive destruction often surface. Security experts and cyber law experts have warned governments from time to time to beef up their security shields for their networks. "Most the cyber attacks do not often surface as the governments and organizations prefer to maintain secrecy. Cyber terror is fast taking on the world. Terror groups have people who can exploit severa vulnerabilities in any network. They might trigger the next war. Or maybe the war is on and we do know it," said Sergey Novikov, Deputy Director, Global Research & Analysis Team, Kaspersky Lab.

From Cyberspace to War zone

The rise in advanced persistent threats (APTs) in the recent years suggest that things are getting out of control. While terrorists and cybercriminals are after your life, money and everything, governments are secretly running programs to attack networks of each other. Kaspersky Lab researcher reveals that ATPs a emerging on a daily basis. The problem is that their origin is sometimes not clear. When everyone is doing the shady things and cripple rival countries, the cyber war is indispensable.

The recent spate of cyber attacks on Sony Pictures and Ashley Madison, among others, are examples of th growing power in the hands of the cyber criminals. The topic resonated in higher volumes at the Cyber Crime Conference recently held in Delhi. "Economies are at risks as cyber criminals and hackers are becoming far more stronger day-by-day. In other words, Cyber space has become the hot spot where the stage has been set for the next war," warns Pavan Duggal, a Cyber Lawyer.

If the US can cause damage to the Iranian nuclear program using a Stuxnet, will nuclear bomb be not hack and exploded by terrorists or maybe governments in the future? Cyber experts do not deny the possibility formidable attacks of massive scale through the cyber space. They simply ask governments to focus on securing the critical infrastructure.

Dealing With Carbanak-like cybercrimes?

Defining legal limits for a country like India for crimes committed in the cyber space is becoming exceedingly difficult. The cyber attacks are in many cases borderless. It makes the job of law enforcement agencies even more difficult. The situation demands international coordination. It is easier said than done. But there are a few learnings that can be derived from the largest cyberheist to date, also known as Carban attack.

Carbanak, a major advanced persistent threat (APT) attack against financial institutions around the world, the largest cyberheist to date, in which hackers stole around $1 billion from banks around the world. The scope of the attack and the losses it caused make it a case for further learning. The surprise factor in this APT attack was the criminals' change in approach and careful planning. Unlike the usual cybercriminal method of stealing consumer credentials or compromising individual online banking sessions with malwar the Carbanak gang targeted banks' internal systems and operations. This resulted in a multichannel robber that averaged $8 million per bank. Such a large-scale APT operation took planning, skill and resources tha are not commonly seen from many organized cybercrime gangs. The banks from the US, Russia and Euro lost huge money.

Finally when the crime surfaced, the law enforcement agencies worked closely to nab the criminals. The governments have no choice to work closely with each other if they want that cybercriminals do not steal t money of their citizens from a place that does not fall in the jurisdiction. "Crossborder coordination betwe law enforcement agencies of various government can help minimize the crime. It is important that governments learn from attacks such as Carbanak," suggested Sergey Novikov, Deputy Director, Global Research & Analysis Team, Kaspersky Lab.

At this time, some of the organizations are still seeing related malicious activity taking place. They are working to spot its source, contain the threat and fully halt the attacks. It requires investment and resource which one organization may not have. Coordinated approach seems the best possible way.

Clearing the Haze

As the US took the liberty to launch a cyber attack against Iran, many other governments are doing the same. Similarly many believe Iran is responsible for a wave of denial of service attacks on U.S. banks, though it is unclear if that was retaliation for Stuxnet. The Paris attack is an alarm that shoul

awaken the entire world and address the cyber crime challenge through a coordinated approach. However, it is not easy. The hazy road lies ahead, demanding enormous effort by the global community.

Posted by: **Onkar Sharma**

View more posts

Tags: Carbanak, Cyber Law, cyber terror, Cybersecurity, Stuxnet

Facebook Twitter Google+ Linkedin Pinterest

‹ India's cheapest local calling service at 19 paise per min launched by Ringo

India Electronics & Semiconductor Association (IESA) announces "Outloc