A STUDY ON RECENT SOPHISTICATED MALWARES AND ADVANCED THREATS ON CYBERSPACE

Vaishali S Raj[1], Dr. R. Manicka Chezhian[2]

Research Scholar, Dr. Mahalingam Centre for Research and Development (CS), NGM College, Tamilnadu, India[1]

Associate Professor, Dr. Mahalingam Centre for Research and Development (CS), NGM College, Tamilnadu, India[2]

Abstract: Malware is a term that has come to encompass a range of threats including Viruses, Worms, Spywares, Trojans, Bots and other malicious programs. They have evolved into a highly complex, polymorphic and sophisticated platform and have become the launch pad for almost all kinds of cyber attacks. The recent threat patterns of these advanced malwares and the intentions for which they have been written is an absolute technical dexterity and are not just a mere cyber attacks. During the recent times, high percentage of Corporate and Government agencies are besieged by these kinds of superior malwares and threats, which are extremely successful in compromising their victims and perform Data Breaches of high complexity. Initially, the targets of any cyber attack were specific Organization or Software or an IT Infrastructure, but these sophisticated malwares have instigated themselves into the echelon of sabotaging a Nation's Infrastructures and Defence sectors. Moreover advanced threats that has aroused on the cyber space are becoming a big part of Cyber espionage network, which are capable of broadening the Cyber risks.

Keywords: Stuxnet, Flame, Duqu, Cyber threats, Cyber Espionage

I. INTRODUCTION

Malware is a single trend that has experienced a tremendous intensification in such short period and has become more popular and notorious in recent times. Malwares are gaining more sophistication and agility with time and their attacks are becoming particularly complicated that, it is becoming highly unrecognisable to any complex security analysis. In case of considering the Android malware platform: the trend for 2013 is one of exponential growth of malicious code for android – is that in 2012 the amount of unique detections grew 17 times globally compared to 2011 and the malware growth for android will rise much more rapidly in 2013[1]. The authors of these advanced malwares have promoted themselves into innovative industry models and software paradigms to build dangerous, polymorphic and sustained attacks with the capability of remaining undetected for very long time. The Cyber threats, on the other hand have emerged into highly Targeted, Stealthy, Persistent and Dynamic. Traditional defences like Firewalls, Intrusion Prevention (or Detection) Systems, antivirus, anti malwares & spywares, gateways lack techniques to tackle with these kinds of threats. With an increased dependency on cyber space in almost all parts of society, the myriad dangers and risks are also increasing in high scale. Initially, the purpose of malicious codes like viruses or worms or Trojans was to spread; as much as possible and cause disruptions. But in the recent years, the situation has changed and rose to technically advanced Cybercrimes and Espionage activities.

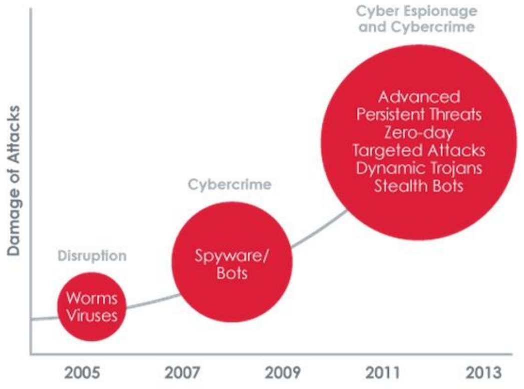

Fig. 1 Graph showing the evolution of Cyber Threats and Malwares and the attack Damages

II. STUXNET MALWARE

Stuxnet is a large and way more complex piece of malware, which was found lurking in the Databanks of Power plants, Traffic control systems and Factories across the world. Stux is 20 times more complex and polymorphic than any malicious code written and apart from the malware payload; the sophisticated Stux has used 4 Zero Day vulnerabilities, which is an absolute technical intensity. Stux was designed to attack and sabotage Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems by infiltrating and degrading the softwares and other important factors that control the ICS's, which are critical parts of any National Infrastructures. Stux has been designed to carry an array of capabilities and among them are the ability to switch off oil pipelines, turn off the pressure inside the Nuclear reactors and even after all the disruptions; this malware can make everything look normal. Deep within the stuxnet code is a 'specific target', and it remains dormant until it reaches the specific target. Stuxnet was first discovered at 'Natanz Uranium Enrichment Facility' at Iran in the year 2010, which was targeted to attack and cause damage to the centrifuges that spin nuclear materials by varying the speed of the motors in that centrifuge. As of September 25, 2010 – Iran had identified 'the IP Addresses of 30,000 Industrial Computer systems' that had been infected by stuxnet, According to Mahmoud Liaii, Director of Information Technology Council of Iran's Industries and Mines Ministry [2]. One of the puzzling parts of Stuxnet is the 'MYRTUS' – found to be a Hebrew reference. The "Myrtus" is the name of specific stuxnet file, serves as a solitary and linguistically intricate hint [3]. Myrtus is found to be an allusion to the Hebrew word 'Myrtle' which refers a character named Esther. It has been found that there had been earlier versions of stuxnet called Stuxnet 0.5 which was alive around the year 2005 to 2009. The 0.5 version of the code finally deactivated in 2009, six months before Stuxnet 1.0 was released [4]. Stuxnet is a weapon first ever to be made entirely out of sophisticated codes. Stuxnet will likely inspire, accelerate and serve as a building block for the development of new cyber weapons that target (ICS) devices. Stuxnet could be a forbearer of the way nation – states use cyber warfare, offering militaries a weapon that may be morally superior to a kinetic one, such as bomb, when it incurs less harm and risk than the kinetic weapon while achieving the same objective. The impact of stuxnet has spread across counties like India, Indonesia, Pakistan, Russia and some other countries, which shows an outline that the Stux infection has spread way further than their initial targets. As of September 29, 2010, the data has shown that there are approximately 100,000 infected hosts. The following graph shows the percentage of infected hosts by countries [6].

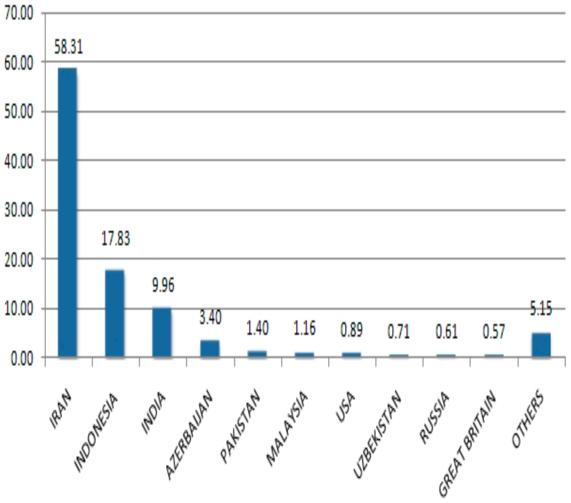

Fig.2 The percentage of Stuxnet infected hosts by Countries

III. THE FLAME (AKA SKYWIPER)

Flame also known as sky wiper or Flamer is highly sophisticated malicious malware that is actively used as a Cyber weapon and used designed for the Espionage purposes. Discovered by Kaspersky lab's experts – during an investigation that was prompted by the International Telecommunication Union (ITU) – Flame is designed to carry out cyber espionage. Flame infects computers by using sophisticated techniques that were previously used by only one cyber weapon: Stuxnet [7]. Whereas the conventional malware is designed to be small and hidden, the utter size of Flame allowed itself to remain undetectable even for years, and untraceable for any of malicious detectors. The astuteness is in such a way that, flame is not designed to deactivate automatically, but supports a 'kill' function that makes it eliminate all traces of its files and operation [8] from its target system thereby leaving no hint of any existence of the malware. This currently active attack is multifaceted and in many ways sets a new precedent for recon and data exfiltration within its attack genre [9]. Flame has proved to be a highly clever info stealer which is capable of, but not limited to espionage functions like Stealing specific or all information, detecting the presence of more than 100 security products (Antivirus, Antispyware, Firewalls etc) [9], scanning Network resources [9], and gather intelligence in multiple ways including Logging keystrokes, capturing screenshots, eavesdropping on conversations and recording them by turning on the microphone (and also web camera if available) and many. This espionage toolkit if found to have been infecting target systems in Iran, Lebanon, Syria, Sudan, the Israeli occupied territories and other counties in the Middle East and North Africa [10].

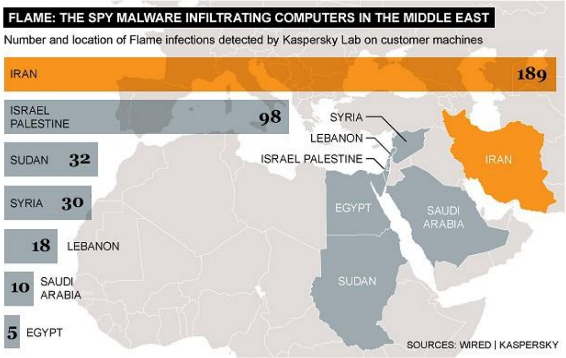

Fig.3 Number and Location of Flame Infections (Source: Kaspersky)

Information security companies say they are convinced Flame was the work of National Government, inter alias because of the sophistication. Moreover, Kaspersky noted, most cyber attacks by ordinary criminals are aimed at either stealing money or, in the case of activist hackers, bringing down the websites [11].

IV. THE DUQU MALWARE

The Duqu was discovered around September 2011 and was found to be a Remote Access Trojan (RAT). Duqu's purpose is to gather Intelligence Data and Assets from entities such as Industrial Infrastructure and System Manufacturers, among others not in industrial sector, in order to more easily conduct a future attack against third party [12]. It appears that the creators of duqu were highly influenced with the stuxnet and once the malware is able to get a grip onto an organization, the attackers can command it to spread to other systems. A common characteristic of stuxnet, duqu, flame is that they have all been active for an extended period before they were actually discovered. This Stealthiness is achieved by carefully avoiding the generation of visible anomalies [13]. At the time of writing, duqu infections have been confirmed in six possible organizations in eight countries. The confirmed six possible organizations and their countries of presence include: Organization A – France, Netherlands, Switzerland, Ukraine; Organization B – India; Organization C – Iran; Organization D – Iran; Organization E – Sudan; Organization F – Vietnam [14].

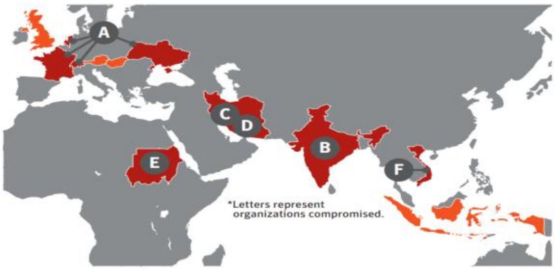

Fig.4 Countries with reported Duqu infections: Red represents confirmed infections; orange represents unconfirmed reports [14]

A. MiniDuke

Another advanced piece of malware discovered recently is the MiniDuke, which has used Adobe Reader 0-day exploit. The MiniDuke attackers are found to be still active at this time and have created malwares as recently as February 20, 2013. According to Kaspersky Lab's analysis, a number of high profile targets have already been compromised by the MiniDuke attacks [15].

V. ADVANCED CYBER THREATS

The recent graph of cyber threats and attacks has drastically grown into active cyber crimes and highly stealthy and complicated espionage attacks. This cyber espionage threat mainly involves the act of obtaining secrets and information (can be of personal, sensitive, proprietary or of classified type) without any authorization and consent and are increasing in recent times.

A.Net Traveler

The Net Traveler (aka 'Travnet' or 'Netfile') threat is found to be a part of global cyber espionage network discovered by Kaspersky labs and been found to have compromised more than 350 high profile companies across 40 countries. The largest number of samples (of 'Net Traveler') observed by Kaspersky was created between 2010 and 2013. This 'Net Traveler' tool used by the attackers is an automatic data exfiltration tool, designed to extract large amounts of private information from victim's system over long period of time [16]. The main targets of this threat network were government institutions, embassies, oil & gas industries, military contractors; and has extended up to space explorations, nano technology, energy and nuclear powers.

B. Red October

Another similar high level cyber espionage threat network is 'Operation Red October' discovered by Kaspersky on October 2012. Red October, in short 'Rocra'(a malware payload) is still active as of January 2013, and has been a sustained campaign dating back as far as 2007 and the attackers have been focusing on diplomatic and governmental agencies of various countries across the world, in addition to research institutions, energy & nuclear groups, and trade and aerospace targets. The main purpose of this espionage threat appears to be gathering of classified information and geopolitical intelligence [17].

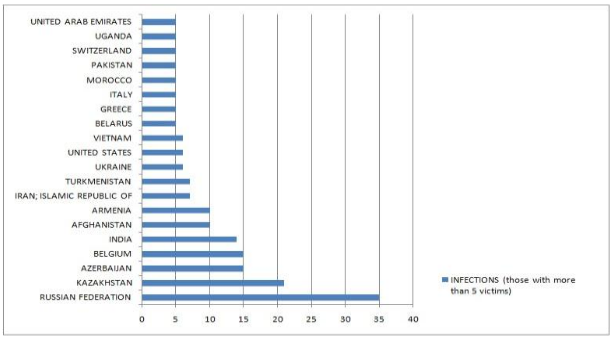

Fig.5 Graph showing the list on countries with most infections (Data source: Kaspersky)

C. Operation Aurora

The Operation Aurora is found to be an ultra sophisticated cyber hack attack against Google, while high profile companies like Yahoo, Symantec, Dow chemical's, Adobe systems, Morgan Stanley, Northrop Grumman were also targeted by this attack. Operation aurora is probably the smartest combination of stealth programming, strong encryption and exploration of a rather unknown vulnerability seen till date [18]. According to McAfee, the primary goal of the attack was to gain access and potentially modify source code repositories at these high tech, security and defense contract companies.

VI. THE IMPACT

With the emergence of cyber weapons like stuxnet, the cyber threats and attacks have posed a great hazard on a Nation's Infrastructures. Critical infrastructures include power grids, energy sources, communication networks, trade & commerce, transportations, health care services, defence sectors, emergency response teams and the like. Disruption of one infrastructure (for example, a communication network) harms the effort to fix other infrastructures that have been damaged by another entity (emergency services, commerce). A cyber attack could directly cause this type of failure. The cyber threat to critical infrastructure is perhaps the most significant issue in the realm of cyber security [19]. A threat moving through the cyberspace puts a stress on how bad the effect could be when compared with when or why the attack has been made. With the rise of advanced malwares like Duqu and Flame; superior cyber threats like Red October, Net Traveler and state of art cyber hack like Operation Aurora, the act of cyber espionage and theft of intellectual property and Nation – State's secrets are on the rise. These attack level have the ability to breach into any kind of defense systems on their way leaving no traces of their existence. With these kinds of targeted threats and stealthy attacks, the cyber landscape requires not just traditional defense systems, but requires high level handiness in countering the threats; close investigation of intrusion cases; providing timely cyber threat information to defend; new breed of intrusion prevention and detection systems; and mainly step forward into strengthening own cyber security environment against internal and external threats of any kinds.

VII. CONCLUSION

This study elucidated an insight into some of the potential malwares and advanced threats that are being encountered lately on the cyberspace and their impact. The recent cyber attacks are not just financial frauds, identity theft, web violations or copyright infringements but are developing a platform to execute stern threats against privacy, confidentiality and security. This rampant growth of cyber assaults; complexity available to develop advanced malwares and initiate a cyber attack against a critical infrastructure will undeniably contribute to the urgency of cyber defense and counter intelligence to tackle with these kinds of attacks.

REFERENCES

[1] 'Trends for 2013 Astounding Growth of Mobile Malware', ESET Latin American Lab.

[2] Paul K. Kerr, John Rollins, Catherine A. Theohary, "The Stuxnet computer worm: Harbinger of an emerging warfare capability", Congressional Research Service, December 2010.

[3] Warren Riddle, "Mysterious 'Myrtus' Biblical Reference Spotted in Stuxnet Code ", October 1, 2010. http://www.switched.com/2010/10/01/mysterious-myrtus-biblical-reference-spotted-in-stuxnet-code

[4] Iain Thomson, "Very different code caused gas attack on nuclear program", February 26, 2013. http://www.theregister.co.uk/2013/02/26/early_stuxnet_code_found/

[5] Dorothy E. Denning, "Stuxnet: what has changed?" Future Internet 2012,Volume 4 issue 3, 672-687.

[6] Nicolas Falliere, Liam O Murchu, and Eric Chien, Symantec, "W32.Stuxnet Dossier", Version 1.4, February 2011.

[7] What is Flame? www.kaspersky.com/flame

[8] Flame (malware), http:// http://en.wikipedia.org/wiki/Flame_(malware)#cite_note-Lee-5

[9] Jim Walter, "Flame Attacks": Briefing and Indicators of Compromise", McAfee Labs, May 2012.

[10] Kim Zetter, "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers", May 28, 2012. http://www.wired.com/threatlevel/2012/05/flame/

[11] Oded Yaron, "Flame virus had massive impact on Iran, says Israeli security firm", May 30, 2012. http://www.haaretz.com/print-edition/news/flame-virus-had-massive-impact-on-iran-says-israeli-security-firm-1.433222

[12] Symantec, "W32.Duqu The precursor to the next Stuxnet", Version 1.4, November 23, 2012.

[13] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán and Márk Félegyházi, "The Cousins of Stuxnet: Duqu, Flame, and Gauss", Future Internet 2012, volume 4 issue 4, 971 – 1003.

[14] Vikram Thakur, "Duqu: Status Updates Including Installer with Zero-Day Exploit Found", Symantec, November 2011.

[15] Global Research & Analysis Team (GReAT), "The MiniDuke Mystery: PDF 0-day Government Spy Assembler 0x29A Micro Backdoor", Kaspersky Lab, February 2013.

[16] Global Research & Analysis Team (GReAT), "THE NETTRAVELER (AKA 'TRAVNET') ", Kaspersky Lab.

[17] Secure List, "The Red October Campaign", January 2013. http://www.securelist.com/en/blog/785/

[18] Ruk cooray, "Operation Aurora – Beginning Of the Age of Ultra-Sophisticated Hack Attacks", January 18,2010. http://www.sporkings.com/2010/01/operation-aurora-beginning-of-the-age-of-ultra-sophisticated-hack-attacks/

[19] Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats', Military and Strategic Affairs, Volume 3 No 2, November 2011.