Introduction

Cyber security is a crisis scenario that is extremely top of mind these days – and rightfully so. Over the last few years, countless brands watched mass destruction due to cyber security incidents. The truth is that a cyber-security incident is a crisis scenario that every organization is vulnerable to, which makes it one of the most important types of high-risk scenarios to include within crisis preparedness program of any organization. A cyber security crisis management plan looks at security from another angle.

Cyber Security related threats have not only become numerous and diverse but also caused serious damages and disruptive impact. Effective cyber security crisis management involves a combination of preventive, detective and reactive processes to deal with security crises. The ability to respond to cyber crises and invoke proper procedure in time is vital t minimize the impact of cyber crises.

Effective Cyber crisis management plan extends beyond preparing for any specific event to development of broad, flexible capabilities that enable response to a wide range of events along various dimensions. From the standpoint of cyber security—the main deterrent to cyber incidents— the goal is to develop a secure, vigilant, and resilient organization.

Purpose of Cyber Crisis Management Plan

The purpose of this plan is to establish the strategic framework and actions to prepare for, respond to and begin to coordinate from a cyber-incident. The plan discusses type of cyber crises, policies, actions and responsibilities for a coordinate, multi-disciplinary, broad-based approach to prepare for rapid identification, information exchange, respond and remedial to mitigate and recover from malicious cyber related incidents.

Cyber Crisis management plan document provide guidelines for organization on planning and preparation for incident handling, team structure, steps need to be taken during first hour and in first 24 hours for incident response.

The field of cyber security is technology intensive and new vulnerabilities emerge with progress in technology giving rise to new types of incidents. Hence, the plan to respond to cyber security incidents need to be updated on regular basis, preferably once in a year.

The approach and methodology of Cyber Crisis Management Plan of CyberSecure Systems Ltd. has been prepared in line with the same of CERT-In.

The technologies used in cyber-attacks are being continuously improved for making greater impact. Therefore, it is essential to review cyber-attack methodologies for modification of CCMP document.

Nature of Cyber Crisis and Contingencies

This section identifies the different types of threats and crisis that affect specific targets. The impact of such a crisis on respective targets and critical business functions and services of various departments are identified to determine suitable response and mitigation action.

While preparing the CCMP the following actions are kept in mind:

- Functions and services of the organization
- Inventory of critical assets
- Risk Assessment and Risk Management
- Business Impact Analysis
- Contingency Plan for IT systems
- Cyber Security Event, Incident and Crisis

Event

An event is any observable occurrence in a system or a network like a user connecting to a network file share or browsing a webpage, or even sending an email. Adverse events are those that have a negative consequence that can lead to a disruption of service and has a negative impact to business. Examples of such events are system crashes, slow response on system/network, network flooding, high network utilization etc.

Cyber Security Incidents

A security incident is defined as an adverse event in an information system and/or network that pose a threat to computer or network security. In other words, an incident is any event

that causes, or may cause a breach of information security in respect of availability, integrity and confidentiality. Examples of such incidents could be unauthorized access to Information system, disruption of data, denial of services/availability, misuse of system resources, computer viruses etc. any vioslations of organization's information security policy would also classify as a security incident. Examples of such incidents could include activity such as:

Attempts (either failed or successful) to gain unauthorized access to a system or its data

Unwanted disruption or denial of service

The unauthorized use of a system for the processing or storage of data

Changes to system hardware, firmware, or software characteristics without the owner's

knowledge, instruction, or consent

Incidents caused by employees, contractors, or others with privileged access who misuse their privileges for malicious purposes such as data theft and sabotage.

Unauthorized access to secure areas of the organization's premises leading to theft,

tampering and damage to IT assets.

Cyber Security Crisis

A situation wherein security characters of information are compromised as a result of failure of an IT system or network of IT systems, due to technical reasons, intentional acts or negligence, leading to consequences that may threaten lives, economy, national security and public confidence. Al

cyber security crises are cyber security incidents; however, all cyber security incidents are not cyber security crises but may lead to crisis situations if not attended to in a timely manner.

Cyber Security Threat Landscape – Changing Scenario

The landscape includes an overview with current and emerging threat agents and trends.

Covert threats to enterprises- Advance Persistent Threats and Targeted Attacks

Attack Modalities

Sophisticated attacks use the wealth of public information to develop a complete picture of the target organization. This picture enables them to identify particular individual who may have access to the kind of information that they seek. The attacker's initial goal is to gain control of the victim's workstation. From that point, all the victim's work and communications become an open book. These attacks often involve malformed documents or web pages that target zero-day vulnerabilities with obfuscated exploits. The attack might come as an e-mail, addressed from a business partner of colleague, with a malicious attachment that sounds directly relevant to the victim's job function. The attack might also come as a link to a juicy document or perhaps an USB token with an interesting presentation. Recent trends indicate exploitation vulnerabilities in client-side applications through websites that are of interest to targeted organizations. Such attacks are being termed as "Watering hole" attacks. The custom malware that is installed by the exploit uses covert channels over the network without being noticed. Once the attackers have their malware running on one victim's machine, they often tried to spread their control to other systems in the targeted network. These are cases of sophisticated spear phishing attacks on Govt. executives and executives in key institutions that have access to sensitive and strategic information. Essentially these advanced targeted attacks include reconnaissance, social engineering, exploitation of vulnerabilities in client- side applications such as MS office, Adobe Applications (PDF reader, Acrobat), Browsers and Browser Plugins (JAVA, FLASH) specially crafted malware and Remote Administration Tools (RATs) and resilient Command & Control channels.

Client-Side Targeted Attacks

These attacks leverage the weakness/vulnerabilities in the client-side applications which in turn interact with an attacker controlled remote server.

The major client-side application targets generally are:

Microsoft Office applications (MS Word, MS Excel, MS PowerPoint, etc.)

Adobe PDF applications (Acrobat Reader, etc.)

JAVA/JRE

Browsers/Browser Plugins

APT campaigns reported in recent past, capitalized the weakness in the client-side software's and the weakest link in the security chain, the human. Carefully crafted spear phishing mails with catchy subjects with spurious attachments were delivered to the unsuspecting victims.

Microsoft Office Applications

A series of exploit attempts against MS office applications were on the rise the way in which office parser treats various file formats (RTF, DOCX, XLSX, PPTX etc.) coming as attachments. Once successful, attackers will be able to take complete control of the infected machine.

Alternatively, web as an attack vector, an attacker hosts a website containing webpages that contains specially crafted files that is used to attempt to exploit these vulnerabilities.

Adobe PDF

PDF exploitation has become a popular mode of attack as compare to browser based and ActiveX based attacks. First, the plug-ins like PDF and flash are ubiquitous to virtually all browsers. Second, complexity of vulnerabilities involved in browser specific exploits may be relegating them through targeting attacks. Third, compared to ActiveX bugs, there is no evidence that PDF vulnerabilities are easier to find. Fourth, another advantage of PDF exploitation over browser specific attacks is that the document specification for PDF is complex and attackers can easily stuff data away elsewhere in PDF document that can be later retrieved programmatically and put through a decoder algorithm to return malicious script. Fifth as of now zero-day PDF attacks enjoy a lead-time before patches are available, creating enhanced value for PDF attacks.

- Protection against PDF based attacks
- Update to the recent reader versions
- Enable Enhanced Security/ Protected View
- Disable JavaScript
- Enable privileged Locations
- Java / JRE

Fishy websites that host crafted jar files or java Network launching Protocol (JNLP) files and tricking users to the sites. Successfully exploits allowing the execution of arbitrary code on vulnerable systems without user interaction and subsequently infecting them and possibly Remote access Tool (RAT) variants.

Protection against Java based attacks

Stay updated

Uninstall / selectively disabled JAVA/JRE

Use No Script (a browser extension for Mozilla Firefox browsers) that can proactively prevent Java applets.

Browsers / Browser Plug-ins

Malicious code may target ActiveX, JAVASCRIPT, JAVA, or other related Web technologies to execute run arbitrary code on browsers address space and several vulnerabilities were reported leveraging them.

Alternatively, Web-based attacks can originate from malicious websites as well as from legitimate websites that have been compromised to serve malicious content. Some content, such as media files, documents, or presentation formats, are often presented in browsers via browser plug-in technologies. While browser functionality is often extended by the inclusion of various plug-ins, the addition of plug- in component also results in a wider potential attack surface for client-side attacks.

Mitigation of Browser based threats

Keep the browser software/ plugins updated

Disable / remove the unnecessary plug-ins

Check Browser Plugins periodically

Securing Browser Best Practices securing_ browser/

Notable trends in APT campaigns

Operation Clandestine Fox:

Zero-day vulnerability in Internet Explorer (1E) enabled owners of malicious websites to gain complete access to the site visitor's computer if the visitor used IE version 6 and up.

The Sunshop Campaign:

Zero-day IE vulnerability (CVE-2013-1347) combined with patched Java exploits CVE-2013-2423 and CVE-2013-1493 were involved in the attack campaign by compromising strategic websites and hosting exploits on the same.

Operation Deputy Dog:

Zero-day vulnerability in Internet Explorer (IE) - CVE-2013-3893- would allow owners of malicious websites to gain complete access to the site visitor's computer if the visitor used IE version 6 and up.

Operation Ephemeral Hydra:

Strategic websites are compromised and loaded with IE zero-day vulnerability exploit. The payload known to make analysis of infected system difficult, by keeping the sample on the memory.

Siesta Campaign:

The attacker serves the archive under a URL path named after the target organization's name (http://{malicious domain}/{organization name}/{legitimate archive name}.zip, and the downloaded file contains an executable masquerading as a PDF document. This malicious component is a backdoor Trojan that connects to (short-lived) C&C servers at previously defined intervals, and to download additional malicious files from a specified URL.

A user-after free vulnerability in IE-CVE-2014-0322-leading attackers to

Operation Greedy Wonk:

A zero-day Adobe Flash exploit (CVE-2014-0502) hosted on major websites of international interest was redirected to an exploit server hosting this Flash zero-day through a hidden iframe. Successful exploitation leads PLUGX RAT being pushed onto the victim machine.

Operation Snowman:

A user-after free vulnerability in IE-CVE-2014-0322-leading attackers to perform drive-by-download attack by injecting malicious scripts onto major known website

Operation Ke3chang:

Spear-phishing emails with malware attachment or a link to a malicious download. Exploits include Java zero-day vulnerability (CVE-2012-4681), Microsoft Word (CVE-2010-3333) and Adobe PDF Reader (CVE-2010-2883). also sent Windows screensaver files (.scr) and executable files (.exe) using the Unicode Right-To-Left-Override (RTLO) technique to cloak the original filename extension from the targeted user.

TravNet:

This campaign made use of a malware family identified as NetTraveler based on the strings found in the malware code.

Protection against Advance Persistent Threats (APT)

Of-the-shelf security solutions can provide some tools that help but cannot wish the problem way. Since APTs defeat the signature-based systems (such as Antivirus), layered defence controls need to be deployed. Important controls include

Adequately training the users to be on guard Wider use of physical network segmentation Real time event collection and correlation at host and network level

Monitoring hosts for signs of suspicious entries in files, processes, registry, DNS requests, web connections etc.

Monitoring of network traffic and detecting connections to suspicious hosts/ sites

Universal e-mail signing

Application white listing at the level of software program

Updating applications such as Adobe Reader, Flash, Microsoft Office, Browsers regularly and follow the advisories and alerts issued by CERT-In/CSIRTs and Vendors

Reporting suspicious emails/attachments to local administrator's, CSIRTs and CERT-In

Enhancing user awareness about social engineering

Botnets

Scope of the problem

Botnets are described as networks of compromised computers that are remotely and surreptitiously controlled by one or more individuals called bot-herders. Computers in a botnet called nodes or zombies, are often ordinary computers in homes and offices around the world. Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and perform tasks, such as sending spam, hosting or distributing malware or other illegal files or attacking other computers. Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Additionally, Downloader Trojans, Exploit Kits, spam mails, p2p file sharing service, Fake media files are generally identified as the distribution mechanisms.

Users are often unaware that their computer has been used for malicious purposes. The botnet word is divided between bot families that are closely controlled by individual groups of attackers and bot families that are produced by malware kits. These kits are collection of tools, sold and shared within the malware underground, that enable aspiring bot-herders to assemble their own botnets by creating and spreading customized malware variants. Some kits are freely available, while others are sold like commercial software products.

Fighting botnets

The methods for detecting bots are generally divided into two categories - one involving static analysis against the list of known threats and the other involving behaviour analysis monitoring communications in a network for behaviours that are known to be exhibited by botnets. Effective botnet detection strategies involve both statistical and behaviour analysis. In order to collect malware infections and analyse the bot activities, often honey pots are deployed to act as deliberate targets for malware infections. In addition to monitor the incoming traffic, a dark-net (a sub-net of unused IP addresses) is used to detect a malware as it scans the net while crossing over the dark- net. The data can be used to identify network

configuration issues. Dark-nets are used to host flow collectors, DDoS, back scatter detectors and intrusion detection systems as well as redirect traffic to honey-pots.

In the year 2013, some popular Botnets such as Zero Access, Carberp, Dorkbot, Festi, Bamital Waldec, Rustock and Kelhios were tracked and mitigated with effective coordination between Governments, CERTs, software product & security vendors and Service Providers.

Threats to watch

NTP based Distributed Reflected Denial of Service (DrDoS) Attacks

A large-scale Network Time Protocol (NTP) based Distributed Reflection Denial of Service (DrDoS) attacks were reported onto reputed ecommerce, banking and public/ private sector websites all over the world. Network Time Protocol (NTP) is a networking protocol used for clock

synchronization, server administration, maintenance, and monitoring. Certain NTP implementations that use default unrestricted query configuration are susceptible to a reflected denial-of-service (DrDoS) attack. In a reflected denial-of-service attack, the attacker spoofs the source address of attack traffic, replacing the source address with the target's address. These attacks were being carried out by exploiting vulnerability in the "monlist" feature of NIP which allows unauthenticated remote attackers to misuse the vulnerable NTP servers to carryout large scale reflected denial of service (DrDoS) attacks. NTP servers that respond to MONLIST Mode 7 command requests will generate responses that are more than 5000 times bigger in size than the requests. With the help of IP address spoofing this attack allows the attacker to send a huge number of requests toward a number of known public NTP servers and solicit a huge response toward the spoofed address of the (source) victim.

Hactivist attacks

The cyber-attacks carried out by hactivist groups such as Anonymous, ranged from defacement to large scale DDoS. Some of the hacker groups posted documents claimed to be stolen on public websites. The attackers distributed tools and used activists distributed across various countries to simultaneously run the tools capable of generating flood of requests to target website and networks to cause disruption of services. While these attacks may not be very complex, but remediation requires coordinated and timely efforts from various stakeholders including Governments, Industry and Internet Service Providers.

Exploit kits

An exploit kit/ exploit pack, is a toolkit that facilitates the automation of client-side vulnerability exploitation. The modus operandi normally revolves around targeting browsers and programs that a website can invoke through the browser.

The exploit kits typically conceal client-side software vulnerabilities in Adobe Reader, JRE, Adobe Flash Player, Media Players, browsers, etc.

Some of the notabe noted exploit packs are Nuclear,GonDA, Fiesta, NeoSploit, DotkaChef, Angler, FlashPack, SafePack, WhiteLotus, InCognito, Magnitude/Death Touch, Sakura, Whitehole, Blackhole, Phoenix, Redkit, Elenore etc.

Fake Antivirus Software

One of the most persistent threats is fake antivirus, also commonly known as 'scareware' or 'rogueware'. In this widespread practice, software is injected into victim's computer system, closely resembling and in some cases directly impersonating genuine security solutions. In many cases, the users actually end up installing a malware on to their system that allows cyber criminals to carry out malicious activities. As of now, over half-a-million fake anti-virus software variants have been encountered. A good step to combat the fake anti-virus threat is user education. However, even informed attempts to fight back are hindered by unwise activities of legitimate service providers.