Centre for Air Power Studies

ZERO DAY VULNERABILITY EXPLOITATION: CYBER WEAPON OF CHOICE

Wg Cdr ***Ashish Gupta***
Research Fellow, CAPS

The tentacles of Cyber espionage are expanding their reach entwining almost every facet of life. The vulnerability quotient due to activities in cyber space has gone many notches up. A direct ramification of this is a burgeoning market offering services, tools and technologies facilitating credible and potent espionage activities. The spirit of entrepreneurship has caught up with computer geeks, who having proven prowess in exploiting cyber vulnerabilities, have no qualms in offering their services to the highest bidder. Unlike traditional espionage, which requires humans operating in the physical world, operatives in cyber space leverage and obfuscate cyber techniques for stealing information and proprietary data in the cyber realm.

Countries, governments, critical information infrastructures and companies manufacturing high-tech products are vulnerable to espionage activities. These activities may threaten economy, national security and well being of people. Companies offering innovative solutions with an **international clientele** in the worldwide marketplace are in great peril of experiencing impediments in conducting business and protecting intellectual property due to potential exploitation of cyber vulnerabilities by criminals and competitors. The adversaries have equal motivation to gain access to state secrets and intellectual property. The defenders as well as the attackers have compelling motivation to understand the vulnerabilities associated with cyber operations, either for protection or for exploitation.

The Net, with all its glossy outward appearances, has a murky, hostile and turbulent under belly where criminals, inimical actors, military and intelligence agencies, terrorists and law enforcement agencies are engaged in constant low-level cyber warfare. In effect, cyber space is a warzone with various warring actors engaged in securing both their benevolent and ulterior motives. For being victorious, they require weapons and equipment. This has given rise to a niche market where bugs are sold as arms by a number of unscrupulous or conscientious dealers.

The mother of all malicious programs and bugs is the "zero day exploit". In a zero day exploit, the creation of exploit is concomitant with the knowledge of vulnerability before, or on the same day. By creating a virus or bug that takes advantage of a vulnerability not known to the vendor and without a security patch, the attacker can inflict debilitating damage to unsuspecting victims. On an average, zero-day vulnerability remains unknown to the affected software vendor and its users for an average of 312 days. [1]

In the recent past, software vendors and security researchers have been caught up in animated debate on the issue of ethicality, legality and desirability of disclosing vulnerability information. The dichotomous dilemma of making the information public on the one hand may allow all affected parties to carry out risk assessment, while on the other hand, the information also be available for exploitation. The dependence of society on information technology has transformed the knowledge about security vulnerabilities, a highly prized and valuable asset. An ethical security researcher may seek monetary compensation for time spent uncovering vulnerabilities. However, reporting vulnerabilities for seeking compensation might be viewed akin to extortion by the vendor. On the other hand, cyber criminals, with no ethical considerations, are willing to pay substantial amount for suitable vulnerability information. The market for sale and purchase of vulnerabilities has evolved from its nascent stage, operating from dark and isolated alleys under the shroud of anonymity, to commercial service offerings with legitimacy.

Vulnerability Purchase Programs (VPPs)

Traditionally, the primary players in the commercial vulnerability market have been iDefense, which started its Vulnerability Contributor Program (VCP)[2] in 2002 and

TippingPoint, which started its Zero Day initiative (ZDI)[3] in 2005. In a bid to show their ethical intents, both vendors publicly disclosed their vulnerability handling services and policies. The VCP and ZDI programs typically purchase vulnerability information to protect customers before a vulnerability becomes public knowledge, subsequently informing the vendor of the affected software. The VCP and ZDI programs entreat security researchers to accept lower compensation with the assurance that the information would not be used with malicious intent. Upon acquiring vulnerability, both programs provide detailed technical information on the vulnerability and on the timeline from its initial purchase through publication. Under VCP and ZDI programs, both the companies together have purchased 2,392 vulnerabilities til September 23, 2013.

Bug Bounty Programs

In order to bring in resilience to their product, a number of software vendors have embarked on 'Bug Bounty Programs'. Under this program, a finder can directly report a vulnerability to the software vendor and is monetarily compensated by the vendor. This incentive may discourage a finder going public with the vulnerability information or selling it to an unscrupulous person. It was first introduced by Mozilla Foundation and since then Google, Facebook, PayPal and others have followed suit. Microsoft, which vehemently opposed such a system, finally succumbed to commercial and security imperatives and introduced its bug bounty program.

- Under bug bounty program, Google on 12 Aug 13 announced that it had paid more than USD $ 2 million to security researchers. Since the launch of the program three years ago, the company rewarded researchers for reporting more than 2,000 security bugs in Chromium and its web apps. [4]

- Mozilla, in the last three years has paid approximately USD $ 57,000 for the knowledge of 190 vulnerabilities which were discovered in Firefox browser.

Facebook has paid out a whopping USD $ 2 million since it introduced its bug bounty program in 2011, with USD $ 1.5 million of that being spread between 330 researchers in 2013 alone.[5]

- Microsoft has paid to the tune of USD $ 100,000 from June 2013 onwards,

when it decided to became part of Bug Bounty program. On 8 Oct 2013, it awarded USD $ 100,000 to James Forshaw (head of vulnerability research at Context Information Security) for discovering a new type of mitigation bypass technique that could potentially threaten the security and integrity of its latest version of Windows operating system.[6]

The cost benefit accrued by bug bounty program is much higher than the cost of hiring full-time security researchers to locate bugs internally. Bug bounty programs help software vendors to plug in the security loopholes which otherwise have the potential to be exploited offensively. It also hastens up the action towards remedy of vulnerabilities reported through a bug bounty program.

State Actors

Most nation-states are leveraging cyber warfare technique either with hostile intent or for protection of their Critical Information Infrastructure (CII). In the recent past, the budget outlays and spending to acquire capabilities for waging cyber war have increased manifold. While unethical hackers and even criminal organizations have limited resources and have to operate within the confines of shoe-string budgets, a nation-state's cyber warfare assets have plenteous resources and immunity from prosecution. In order to keep a step ahead of potential adversaries, it is not uncommon for nation-states to purchase vulnerabilities for exploitation. Recently, it was revealed that the National Security Agency (NSA) plans to spend USD $25 million on exploit purchases this year.[7] This would enable it to acquire more than 100 exploits based on the present going rate. Other countries are also big spenders when it comes to acquiring exploits.

The year 2009 was a defining year which marked the arrival of the first true cyber weapon, "Stuxnet'. A complex computer worm was developed with specific objective to decommission uranium enrichment facilities in Natanz in Iran. It was introduced into the facility's computer system with a USB drive. It affected the computers responsible for controlling the centrifuges for enriching uranium and destroyed about 20% of these. It is believed that the perpetrators used four zero-day security vulnerabilities to spread around Microsoft's Windows operating system. After detailed study, Microsoft admitted that the attackers initially exploited the old MS08-067 vulnerability which was a remote code

execution vulnerability. Successful exploitation of this vulnerability enables the attacker to take complete control of an affected system remotely[8]. A new LNK (Windows Shortcut) flaw was used to launch exploit code on vulnerable Windows systems and a zero-day bug to exploit the Print Spooler vulnerability (this vulnerability was leveraged to propagate and affect systems connected to the affected machine's network).

Presently, a number of new entrants are offering services ranging from vulnerability feed, penetration testing to vulnerability and security assessment. Few among them are Exodus Intelligence and Netragard in the U.S., Vupen in France, Revuln in Malta and Telus in Canada. In fact, Vupen publically offers sales of 'exclusive and extremely sophisticated zero-days for offensive security'. It also advertises that it offers government-grade zero-day exploits which could be used by law enforcement agencies and the intelligence community in furtherance of their offensive cyber missions and operations. These companies are hunting with the hounds and running with the hare with an aim to make money by leveraging the fear factor emanating from concerns among companies and organisations about the security of their systems as well as by selling the zero-day exploits to the highest bidder.

ARTICLES BY SAME AUTHOR

ROADMAP FOR UNITED STATES CYBER COMMAND AND ITS APPLICABILITY FROM INDIAN PERSPECTIVE

INDICTMENT OF CHINESE NATIONALS BY US ON CHARGES OF CYBER-ESPIONAGE: ITS IMMEDIATE IMPLICATIONS AND LONG TERM RAMIFICATIONS

On any given day, a number of vulnerabilities are privately known. Out of these, it can be safely assumed that a substantial number are exploitable. These vulnerabilities and exploits are being purchased with equal gusto by cyber criminals as well as by government agencies. Big software vendors will leave no stone unturned to plug these vulnerabilities either by internal evaluation or by purchasing out rightly from vendors under Bug Bounty program. This has added a new dimension to an already complex issue of cyber security and warfare. This calls for using the weapon of 'vulnerability exploitation' both for

offensive and defensive role. In defensive role, the objective would be to secure cyber space against a determined enemy by plugging in the vulnerabilities. However, successful attainment of this objective is cost and effort intensive. The costs of these vulnerabilities are exorbitantly high and are being offered to the highest bidder. Even with possession of a specific vulnerability, the depth in defence so acquired will be ephemeral and will require the repetitive process of repurchasing the newly discovered vulnerability being offered for purchase to attain the same depth in defence. On the other hand, in an offensive role, the exploitation of vulnerability will accrue better results as the adversary may not have credible defence against such vulnerability. However, the window of opportunity for exploitation of such vulnerability would be short due to the likelihood of this being identified and plugged in by the adversary.

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

End Notes

[1] "How Many Zero-Days Hit You Today? ",at http://krebsonsecurity.com/2013/12/how-many-zero-days-hit-you-today/ , Dec 13, accessed on 01 Aug 14.

[2] "VeriSign iDefense Threat Intelligence Services Overview, at https:// www. verisign.com /static / 031415.pdf, accessed on 01 Aug 14.

[3] "Why Did We Create the Zero Day Initiative?", at http://www.zerodayinitiative.com/about/ accessed on 01 Aug 14.

[4] "Goggles-bug-bounty-program" , at http://techcrunch.com/2013/08/12/googles-bug-bounty-program, accessed on 01 Aug 14.

[5] "Facebook bug bounty program paid out $1.5m in 2013' at http:// nakedsecurity. sophos. com / 2014/04/04, accessed on 01 Aug 14

[6] " Microsoft-pay-out-first-100000-bug-bounty", at http://nakedsecurity.sophos.com/2013/10/09, accessed on 01 Aug 14.

[7] Stefan Frei, "The Known Unknowns: Empirical Analysis Of Publicly Unknown Security Vulnerabilities", NSS Labs, p.14.

[8] "Vulnerability in Server service could allow remote code execution , at http://support.microsoft.com /kb/958644 MS08-067, accessed on 01 Aug 14.