White Paper

A Guide to Cyber Crime Security in 2010

A Web of Crime

Internet crime is easy to commit, highly lucrative and largely under-policed. Once started as innovative attempts at causing mayhem by technologically-savvy youth, modern cyber criminals are now highly sophisticated and the cyber crime economy is a vibrant, worldwide market, spreading at an alarmingly dangerous rate. Law Enforcement and Computer Crime Experts are overwhelmed as the threats to consumers, businesses and national security are increasing daily, resulting in stolen identity data, fraudulent online transactions and cyber espionage. This whitepaper will cover current and emerging trends behind internet vulnerabilities as well as the methods and solutions available today to help combat this pandemic.

> “Consider that, in 2009, 10 million USD were stolen worldwide in 24 hours using an elaborate scheme of ATM cards created with white plastic.”

Understanding Internet Vulnerabilities

Using traditional crime as an analogy, we see that vulnerabilities in computers and software are much like original bank structures with distinct physical defects. Vulnerabilities may be seen as the way the system processes information and can also be in the default configurations that most criminals know how to change and exploit to their advantage. Another vulnerability, social engineering, relies on the human faults to trust information intentionally left to deceive us and execute a carefully orchestrated plan which uses technology against us. When all of these elements are combined together into a master criminal plan, exploitation of tens of millions of dollars can occur in a short period of time. Consider that, in 2009, 10 million USD were stolen worldwide in 24 hours using an elaborate scheme of ATM cards created with “white plastic”. This act of cyber crime relied on the combination of vulnerability exploitation and social engineering across multiple countries by a well organized band of bank robbers to carry out their diabolical plans

Research remains the most effective way to understand a vulnerability. This starts with understanding how an exploit can take advantage of a specific vulnerability, allowing malicious software to operate on a device. Once it is has been absolutely determined how this occurs, known as an investigation, then a remediation can be created (generally a software patch) or a mitigation (a configuration change) can occur to eliminate the threat. In addition, detection of a vulnerability in a reliable and consistent manner provides detailed insights into which systems can be compromised. Unfortunately, just because key databases and servers may not be vulnerable, other systems that are interconnected and not deemed sensitive can be used as beach heads to leverage other devices to achieve their devious mission. One vulnerable device, such as a secretaries desktop, could be exploited and leveraged to gain access to other devices and their sensitive information. The compromised host acts as a proxy for funneling out valuable information and may be used to spread malicious code throughout the environment. Therefore, identification of the vulnerability before exploitation occurs is critical. But even if malicious software does find its way onto a host via email, website, or usb drive, proper identification of the malware is just as critical. This is where endpoint protection comes into play. Using signatures, heuristics, sandbox technology, rules, and analyzers , an endpoint solution can detect and prevent malicious activity regardless of the entry point; including social engineering.

The endpoint to vulnerability starts here.

eEye Digital Security®

Finding an Effective and Efficient Solution to Modern Cyber Crime

The initial step to managing these types of threats is to acknowledge your weaknesses. Start with known vulnerabilities that can be readily exploited to compromise a technology solution. Using a vulnerability solution to identify weaknesses, an organization can easily thwart a drive-by type of attack and data theft. Protecting your information technology infrastructure from malicious software that can be used to execute hostile plans also stops these attacks by looking for programs that have malicious intent to steal information. Consider that even the United States Government can lose large quantities of valuable information due to malicious software and social engineering. Many of these systems did not have up-to-date antivirus software and were out of government established best practices for security and configuration hardening lead to this unfortunate event.

As a business, being informed about vulnerabilities and protecting your assets from malicious programs by either loading or executing is imperative to stopping cyber criminals. For example, by not allowing a bank robber to know what alarm system you have, where the cameras are, or what model of safe you have is analogous to revealing what firewall and IDS/IPS vendors you use, or which servers, web servers, and databases are storing your sensitive and potentially financially valuable information. Information privacy becomes the foundation of information security best practices.

The ideal solution for an organization to meet these numerous challenges is a comprehensive vulnerability management program. One that stays up to date with the latest threats, vulnerabilities, attacks, exploits, malware and even zero day threats used by cyber criminals for financial gain. Having a solution that collects this information and allows proactive responses to newly identified weaknesses allows organizations to go on the offense for mitigating these risks verses always being reactive. In addition, having the security data assimilate into other business practices such as network management and call centers allows for vulnerable assets and suspicious attacks to be logically represented in the organization for the actual business function it serves verses just another IP address. Vulnerability management as a complete solution represents the best possible approach to managing cyber crime today within an environment.

> "The ideal solution for an organization to meet these numerous challenges is a comprehensive vulnerability management program."

Retina CS, Compliance and Security: Complete Vulnerability Management

Retina CS is designed to be the next generation vulnerability management solution for organizations. By defining vulnerability management as the proper identification of vulnerabilities and protection against exploitation, Retina CS provides a simple user interface for management of this data in a single, rich internet enabled application available through any browser that supports Adobe Flash Player.

To better understand why Retina CS can help manage our environment better, lets first look at the underlying security problems. First, any device connected to the network becomes a potential liability if it is misconfigured or has vulnerabilities. The assessment of these devices is critical for determining how a cybercriminal can leverage your systems. Second, assets that are being attacked, whether it be from malware or network exploits, need to have that information escalated to the appropriate individuals. This data indicates how cyber criminals are currently probing your network for exploitation using manual and automated techniques. Having both sources of information correlated by asset and time provide a business oriented approach to fighting cyber crimes compared to an event driven architecture present in other solutions. In addition, logical "smart groups" of these assets allow threats to be assessed by the business functions they serve rather than a device just associated with a potential for exploitation.

→ Retina CS provides a results-driven architecture to manage these sources of security data.

As a result-driven solution, many businesses decide what security questions they need answered and then how to implement them in technology and extract the appropriate report. Retina CS eliminates that problem by asking in advance, what type of report and business problem you are trying to solve and how you can be threatened.

In essence, ask yourself how many times these questions have surfaced:

- Do I need a PCI DSS report for my infrastructure to meet regulatory compliance?
- What ports are open on my firewalls and servers in my DMZ?
- What viruses have been detected on my laptops, desktops, and servers?
- Which assets are highest in risk from being compromised by a cyber criminal?
- Which assets are currently being attacked?

Retina CS provides the answers to these questions, and many more, by giving you report templates specifically designed for this purpose. Once a report is selected, and optionally customized to meet your unique needs, Retina CS inspects its database for relevant information and will recommend if additional scanning or data collection is needed to fulfill your request. Once all data is present, a report is generated and sent automatically for review. Your businesses questions correlate directly to reports with Retina CS and the solution is intelligent enough to gather the information it needs to build the report without any customization. Retina CS is designed for administrators and engineers alike. Administrators can gather these reports with no technical insight into scanning, audits, or job control while security engineers can dive deep into the advanced options to set scan threads, port groups, and other low level settings to meet any technical requirement. These steps are a single mouse click away, one layer down, from the result driven architecture for the more advanced users.

As many organizations grasp the concepts of vulnerability management and cyber threats, eEye Digital Security has simplified the approach to these problems with Retina CS. Retina CS can address your vulnerability management needs and ultimately how to fend off attacks for cyber criminals. We are all at risk.

About Retina CS, Compliance and Security

Retina CS is a fully integrated, complete web-based security solution for managing vulnerabilities, direct attacks, spyware and remediation and is available as software, appliance, or managed service. Retina CS simplifies the management of distributed, complex infrastructures while protecting your mission critical assets from evolving threats with one complete end-to-end vulnerability management system.

About eEye Digital Security

eEye Digital Security is the global leader in the next generation of security solutions: comprehensive vulnerability management and zero-day endpoint security protection. eEye enables secure computing through world-renowned research and innovative technology, supplying the world's largest businesses with integrated and research-driven vulnerability assessment, intrusion prevention, asset security and compliance solutions. Founded in 1998, eEye Digital Security is an award-winning CA internet security company headquartered in Orange County, California.

To learn more, please visit **www.eeye.com** or call 866.282.8276.

References

1. "FBI Probes Hacker's $10 Million Ransom Demand for Stolen Virginia Medical Records", May 7, 2009, http://www.foxnews.com/story/0,2933,519187,00.html
2. First iPhone Worm Spreads Rick Astley Wallpaper, November 8, 2009, http://www.pcworld.com/businesscenter/article/181697/first_iphone_worm_spreads_rick_astley_wallpaper.html
3. Life After the Conficker Worm-Why You Should be Worried, April 2, 2009, http://blog.novashield.com/
4. Common Configuration Enumeration, http://cce.mitre.org/
5. http://www.cbsnews.com/video/watch/?id=5578986n
6. 60 Minutes covers cybersecurity threats, federal data breach, November 9, 2009, http://itknowledgeexchange.techtarget.com/it-compliance/60-minutes-covers-cybersecurity-threats-federal-data-breach/
7. Security Readiness Review Evaluation Scripts, http://iase.disa.mil/stigs/SRR/index.html
8. Personally Identifiable Information, http://en.wikipedia.org/wiki/Personally_identifiable_information
9. Exploit, http://en.wikipedia.org/wiki/Exploit_(computer security)

   Vulnerability, http://en.wikipedia.org/wiki/Vulnerability_(computing)
10. Zero Day Threats, http://en.wikipedia.org/wiki/Zero_day_attack

The endpoint to vulnerability starts here.