COMODO
ENTERPRISE

WHITE PAPER

Endpoint Security and the Case For Automated Sandboxing

A World of Constant Threat

We live in a world of constant threat. Hackers around the globe work every hour of everyday to attack companies, both large and small, across every industry. They write malicious codes and exploit company networks and websites.

Viruses, worms, spyware, rootkits, Trojans and other malicious software gain access to proprietary data and information. Every device connected to the network – desktop, laptop, tablet and mobile phone— is a vulnerable endpoint for these threats that disrupt the company's operations.

"Every computer, laptop, tablet and mobile phone connected to your network represents a vulnerable endpoint that needs to be protected."

Despite the constant threat, the majority of business owners are unaware of their websites' security. A 2013 survey by The Small Business Authority revealed that 60 percent of business owners are not concerned about vulnerabilities. Barry Sloane, President and CEO of The Small Business Authority, commented, "There is an air of complacency with business owners who think cyberattacks will not happen or affect them. Organizations or entrepreneurs that have experienced a cyberattack run the risk of decimation and elimination. "

In 2014, the data breach at JPMorgan Chase compromised personal information of more than 83 million households and businesses. The highly-publicized Sony Pictures breach released over 100 terabytes of internal files (e.g., executive emails, user names and passwords, personal information about employees, and films). Global Payments, a leading payments processing firm, reported a data breach that compromised 1.5 million accounts; the expenses associated with this data breach was $84.4 million.

According to a report by Ponemon Institute, the average global cost for computer security breach to a company was $3.5 million in 2014, which is 15 percent more than 2013(1). In addition to the high cost, data breach leads brand damage and loss of trust with customers, prospects and business partners. It is clear that endpoint security is no longer an option but a front-line priority.

Mobile Security and the Rise of BYOD

Bring Your Own Device (BYOD) trend is is on the rise; more employees are using their own smartphones and tablets to connect to corporate networks – most of these connections are unmanaged and unsecured. Many of those phones are used by employees to connect to corporate networks. Most of those connections are unmanaged and unsecure. The phenomenon of using your personal smartphone for business purposes is known as Bring Your Own Device or more popularly, BYOD.

"The average mobile security incident costs over $100,000 with many running in excess of $500,000"

With the rise of BYOD, it's no surprise that the majority of businesses had a mobile security incident in the past year. A report by Dimensional Research reveals that the average mobile security incident costs over $100,000 with many running in excess of $500,000.

The rising rate of incidents is due to the fact that mobile security continues to remain unmanaged. 67% of firms surveyed allow personal mobile devices to connect to their networks. 88% of those devices are used to access corporate email. And 53% of those devices have customer data stored on them.

Most companies estimate they have more than five times as many personal mobile devices connecting to their corporate networks than they had two years ago. Nearly all report securing corporate information as their greatest challenge when it comes to implementing BYOD policies.

Zero-Day Attacks and the Vulnerability Window

A zero-day attack targets an unknown vulnerability in a computer application. The vulnerability is exploited before the developers become aware of the attack and can address the problem.

Malware writers are able to exploit unknown vulnerabilities through several different attack vectors. Web browsers are often the primary target because of their widespread distribution and usage. Hackers can also send email attachments which exploit vulnerabilities in the application upon opening the attachment.

Vulnerabilities discovered by hackers will be kept secret for as long as possible and will circulate only through the ranks of hackers until the software or security companies become aware of them.

"Given the nature of zero-day attacks, it's impossible for a blacklist to be up-to-date 100% of the time for 100% of the threats."

Antivirus systems use a program called blacklist to prevent attacks by determining which files are safe to run. The problem with a blacklist is that it prevents only the files that have been identified as threats, and it needs to be updated often. Given the nature of zero-day attacks, it is impossible for a blacklist to be 100% up to date to prevent 100% of the threats.

What this means is that no protection is complete unless it addresses the files that are not yet on a blacklist.

The Case for Sandboxing

A sandbox enables you to run suspicious files safely in a virtual environment. When a suspicious file is sandboxed, it is prevented from making any permanent changes to your files or system. If the file turns out to be malicious, no harm is done.

Sandboxing copes with zero-day attacks that take advantage of unknown security holes or vulnerabilities in web software such as Adobe Flash, Internet Explorer and Java. Running suspicious files in a sandbox provides the protection from zero-day attacks that a blacklist cannot provide.

Not All Sandboxes Are Created Equal

Sandboxes can be divided into two categories: standalone and integrated. A standalone sandbox requires the user to select the files to run in the sandbox. This type of solution is popular with companies that want to segregate high risk software such as Internet browsers. But it does not address the problem of unknown threats.

A sandbox integrated with a security system provides an additional layer of protection by incorporating antivirus scanning to identify potential threats. Antivirus scanners deal with unknown files by leveraging heuristics, a process that analyzes a program's behavior as well as similarities with known viruses. If a file is considered a threat, it is segregated and ran safely in the sandbox.

Heuristics work well but it cannot guarantee 100% protection. Like a blacklist, they must first identify a threat in order to deal with it – and there will always be some threats that cannot be identified by antivirus scanners.

Why Default Deny is the Only Guaranteed Solution

Comodo's Detection+ is the only antivirus solution that guarantees protection against viruses. Detection+ is a Host-Based Intrusion Protection Solution (HIPS) that incorporates a Default Deny strategy to restrict the access of all unknown applications to important files, folders, settings and the Windows Registry.

Default Deny refuses all files permission to install or execute outside of its sandbox except when specifically allowed by the user or when the file appears on Comodo's whitelist, which identifies binaries that are known to be safe.

The benefit of Default Deny is that it closes the hole that other antivirus systems leave open – it eliminates the risk of unknown threats.

Where other antivirus solutions are limited to protecting against known threats, Comodo's Default Deny is the only strategy that protects against any files. Default Deny authenticates every executable and process running on your computer and prevents them from taking actions that could compromise or harm your files.

Equally important, Default Deny enables you to access and work with the files as they execute within the sandbox. The result is total guaranteed protection without the loss of time, money or productivity.

For Additional Information: Visit our **website**

Schedule a **demo**

About Comodo

Comodo is a leading global provider of internet and cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep 16-year history in SSL certificates, antivirus and endpoint security leadership, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information. With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for more than 600,000 businesses, and with more than 75 million desktop security software installations, Comodo is Creating Trust Online®. Headquartered in the United States, Comodo has offices and innovation labs in China, India, Romania, Turkey and the United Kingdom. For more information about Comodo visit http://www.enterprise.comodo.com.

Comodo Security Solutions, Inc.
1255 Broad Street Clifton,
NJ 07013
United States

Comodo CA Limited
3rd Floor, 26 Office Village
Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ
United Kingdom

Comodo Turkey
Büyükdere Caddesi Yapı Kredi
Plaza C Blok No:40
41 Kat 17 Levent, Istanbul
Turkey

COMODO
ENTERPRISE™

1-888-256-2608 enterprisesolutions@comodo.com