Defeating Ransomware with Isla Web Malware Isolation

The Isla Web Malware Isolation System

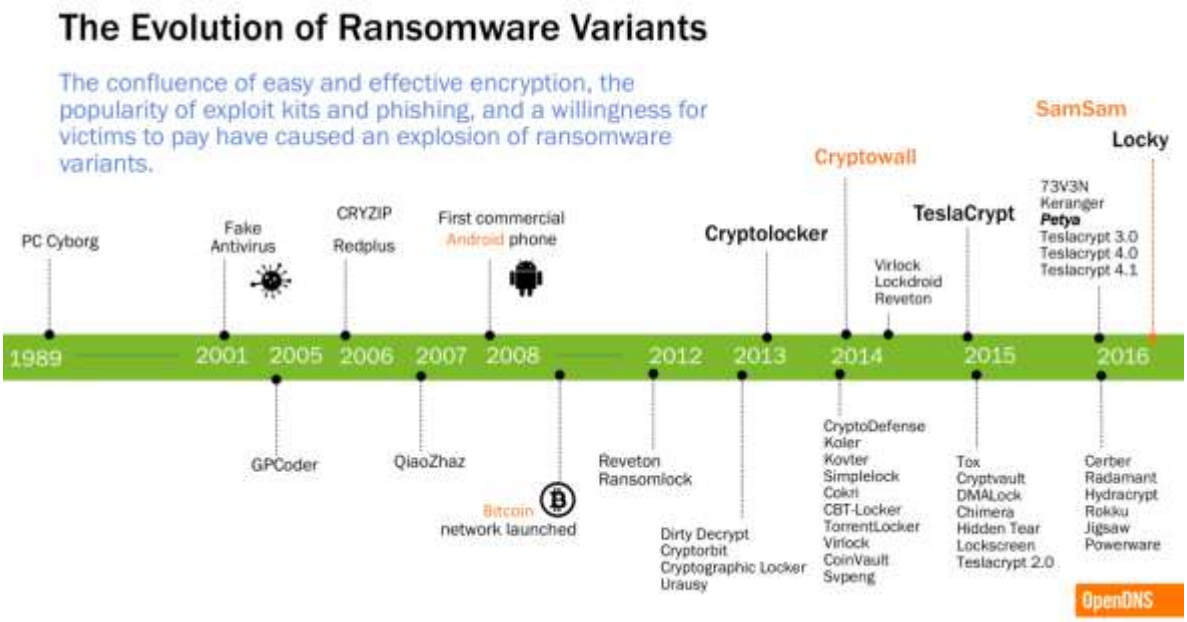
To effectively guard against Ransomware and the other advanced cyber-threats plaguing their businesses, security teams need to implement a solution that offers an isolation-based approach. Introducing Isla— a solution specifically engineered to combat web-based malware, including ransomware by isolating and protecting networks and endpoints.

This approach represents an innovative, fundamentally differentiated alternative to other security technologies, such as secure web gateways, firewalls, and intrusion detection systems. Unlike these other offerings, Isla doesn't rely on detection methodologies at all.

Instead, Isla is built based on the assumption that all web content is malicious. The solution isolates all original web content outside the network, away from endpoint devices, then transforms that content into benign, malware-free formats before delivering it to end users. Through this approach, Isla can stop all web-borne malware, including malicious code that exploits zero-day vulnerabilities to initiate the attack.

Ransomware – Putting data, and your business at risk

Ransomware continues to evolve and proliferate based on the proven success attackers have achieved. Experts estimate that Ransomware criminals took in almost $1b in 2016. Early Ransomware campaigns were targeted at consumers and focused on encrypting photos and other common consumer files that victims would be willing to pay a modest sum to recover. The focus quickly shifted to more lucrative targets and the range of businesses and organizations targeted has rapidly expanded.



This is certainly a strong incentive for them to continue development to counter industry efforts to detect and block Ransomware as illustrated by the global Ransomware Worm "WannaCry" in May of 2017. WannaCry blends traditional ransomware code with a recently discovered Windows SMB vulnerability released after the compromise of the NSA hacking tool kit to enable it to spread like wildfire around the globe.

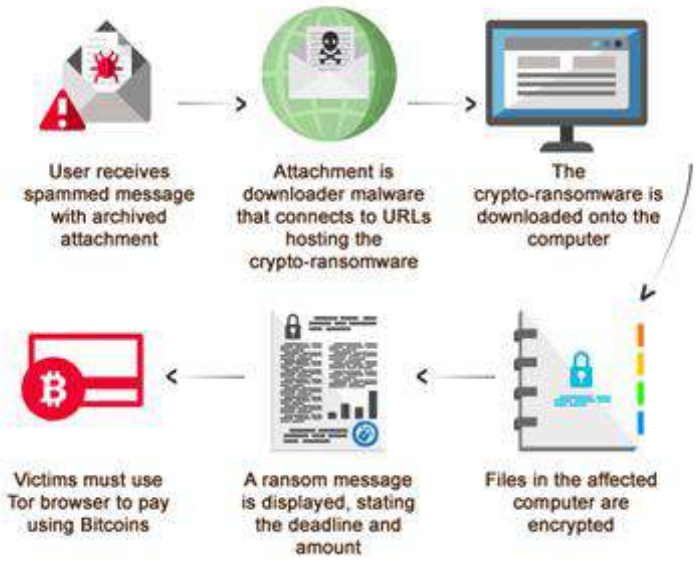
The industry has attempted to respond to Ransomware, as well as a range of other advanced attacks in different ways. Some of these efforts have had a short-term impact, but attackers are adapting and finding new ways to avoid the latest detection technologies as they have in the past.

According to Symantec "Ransomware is predominantly found on suspicious websites, and arrives either via a "drive-by download", stealth download or through a user clicking on an infected advert. Some distribution via email has also been seen."

How Ransomware Attacks Work

Following is a high-level overview of how a ransomware attack works:

- A user visits a malicious site or receives an e-mail with a malicious link or document.
- The system is redirected to a site containing an exploit kit.
- Exploit kits target vulnerabilities in browsers, Adobe Flash®, JavaScript™, or other software to gain access to a user's system.



- Compromised system is redirected to a server used to install the ransomware code onto the endpoint.
- The Ransomware encrypts all the files the system has access to, including cloud based or network share based copies in many instances.

- A “Ransom Note” is displayed with instructions on how to pay the attacker to decrypt the files.

Why Combatting Ransomware is so Difficult

Ransomware campaigns are proving very difficult to combat. First, like other malware approaches, ransomware authors are employing a range of sophisticated tactics that make their campaigns difficult to discover, classify, and counter. Advanced forms of ransomware evade detection by employing a range of tactics, including encrypting code and communications, using randomly generated file names and URLs, and injecting and running code in different programs and at different times.

Many attacks begin with a complex series of redirects. And, by using SSL encryption, these redirects make it difficult for security analysts to locate the origin of malware. Further, these cyber criminals are continuously updating and mutating their exploit kits and malware code to avoid whatever new security measures may be put in place.

Ransomware: One of Many Browser-based Threats

Ransomware is in it’s own right, the troubling reality is that it’s only one of many approaches at cyber criminals’ disposal.

For years, browsers have represented the most commonly exploited vector for cyber-attacks, and that doesn’t appear to be changing any time soon. Meanwhile, the breaches—and costs—continue to mount. A recent Ponemon report revealed the following statistics:

- Organizations experience an average of 51 browser-born security breaches a year.
- To respond to and remediate each breach, these organizations spend $62,000.
- All told, browser-based breaches are costing businesses $3.1M a year.

The Solution: Isolate Rather than Relying on Detection

As the stats above clearly articulate, browser-based attacks continue to result in breaches, and those breaches are costing businesses dearly. Ransomware generally, and sophisticated campaigns like Fobber in particular, provide a vivid illustration of why gaining complete protection against browser-based malware simply isn't possible with traditional security technologies and approaches. Quite simply, detection-based approaches aren't working. These tools aren't equipped to contend with the complex, dynamic, and evasive tactics being employed in today's malware campaigns. It is therefore vital for enterprise security teams to find new approaches that offer effective protections against browser-based threats.

Isla offers a number of critical advantages:

- Effective security. Through its unique isolation and transformation capabilities, Isla is extremely effective at keeping web-based malware off endpoints and outside of corporate networks. With this solution, users can fully leverage the web, without fear of malware.
- Flexible, scalable performance. Isla can effectively and efficiently scale to accommodate any number of enterprise users. With this solution, users don't see any compromise in performance relative to traditional browsing approaches.
- Easy to deploy and maintain. Compared to many security technologies, Isla is far simpler to implement and operate.

The Benefits of Isla

By harnessing Isla, organizations can realize the following benefits:

- Improve security. By offering capabilities for browser isolation and content transformation, Isla helps eliminate exposure to ransomware and other browser-based attacks.
- Reduce cost of remediating after web-based attacks. As outlined earlier, organizations spend $3.1M annually on average to clean up web-based malware attacks. Because Isla is highly effective at stopping browser-based malware, costs associated with forensics, remediation, and business disruption can be significantly reduced.
- Eliminate the patching "Window of Vulnerability".

Organizations must wait for vendors to develop patches to newly identified vulnerabilities and then test and schedule the roll out of software patches to reduce the chance of a patch disrupting the systems in their environments. The time required for this process can be quite lengthy and is referred to as the Window of Vulnerability during which their systems can be compromised. Isla eliminates this windows by isolating any potential attacks from ever reaching the vulnerable system. Organizations can now fully test and schedule patches saving time and money.

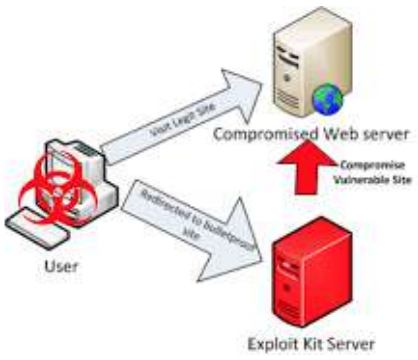
E-Mail based attacks- Email based attacks overwhelmingly come in the shape of phishing or spear-phishing. Phishing attacks generally the form of an e-mail which is designed in such a way as to lure a wide range of users into opening the e-mail and then clicking on a link or opening a file attachment. Spear-phishing uses the same technique although the attacker will generally be targeting a specific individual or organization in an attempt to make the e-mail seem more legitimate.

In either form when the user opens a malicious file attachment the file executes software which subsequently downloads a file containing the malware itself. The malware package downloaded can range from ransomware which will encrypt or destroy all the files on the system or a Remote Trojan program which allows the attacker to remotely control the system, steal credentials and data, or launch attacks deeper into the network.

Isla isolates all web code requested by an internal endpoint outside of the organization in the Isla appliance. This effectively "breaks the kill chain" and defeats an attack before it can succeed.

If a phishing mail contains a link to a malicious web site Isla will isolate the malicious code and will destroy it when the user completes their browsing session. Isla utilizes advanced virtualization technology within the appliance to provide a pristine "gold image" each time the user launches a new browsing session. This ensures that malware cannot persist between sessions and provides another layer of protection for the organizations.

Web Based Attacks- Web based attacks come in many forms and have been the top form of attack for the last several years. Web attacks exploit vulnerabilities within all of today's web browsers and their plugins like Flash or Acrobat to take control of the end users system and download additional malware.

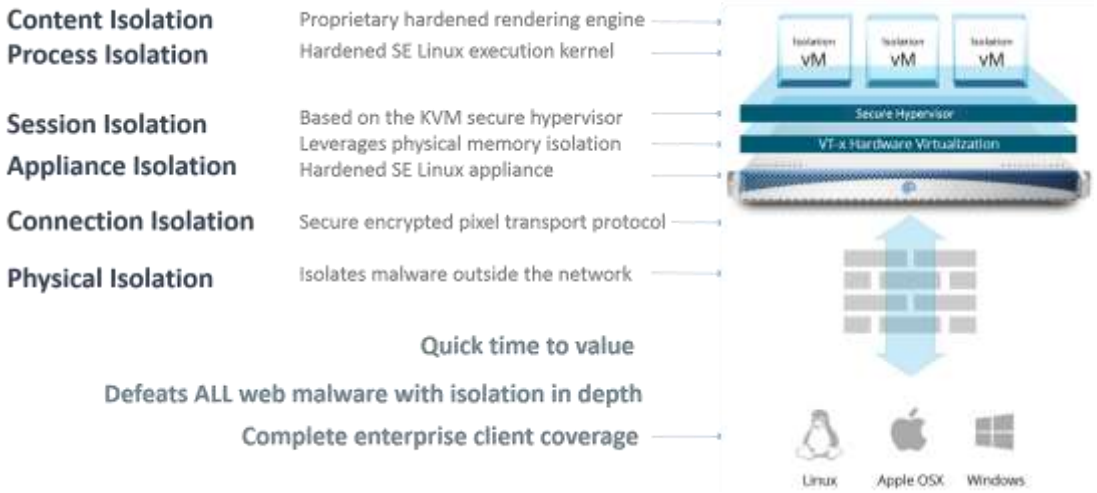


Web attacks target the web browser and are particularly dangerous as they generally do not require to "click" on anything to initiate the attack. These types of "drive by downloads" have grown in sophistication and even appear on legitimate, main stream web sites via paid advertising links, a technique known as Malvertising.

Web based attacks are extremely difficult to detect in advance as they are “file-less” attacks. Malicious software code is introduced directly into the memory of the web browser which eliminates most security technologies ability to scan or inspect it before it achieves its goal, to take control of the system the browser is running on.

The Isla Malware Isolation solution intercepts all web code sent from every web server a users accesses and executes within a specialized isolation environment on the Isla Appliance. Web code is processed in specialized form of web broswer within Isla and the resuling image is security transported back to the users system for display. The result is a completely secure web browsing experience that never allows any web software to be sent to the end user system.

Isolation in depth:



Isla is the only solution to offer six degrees of isolation between the user and an attack.

- **Content Isolation-** Isla isolates all web content in a hardened rendering engine with no access to the endpoint or other processes executing within the **R**emote **A**pplication **C**ontainer or RAC.
- **Process Isolation-** The Isla RAC uses a hardened SE Linux system kernel which applies mandatory access controls to isolate each running process from each other.
- **Session Isolation-** Each Isla session is contained within its own RAC which is isolated from all other sessions using Intels’ VT-X technology. This delivers hardware based separation of the execution environment of each RAC ensuring that attackers have no access to other sessions.
- **Appliance Isolation-** The Isla appliance uses a hardened SE Linux kernel with mandatory access controls to ensure the appliance is isolated from external attack.
- **Connection Isolation-** Isla utilizes a secure, proprietary transport protocol between the user and the appliance ensuring complete isolation of each connection.

- **Physical Isolation-** Deploying Isla outside the perimeter of the protected network ensures that no malware can attack the endpoint or be used for covert surveillance of the network.

Conclusion

With the Isla solution, your organization can address one of its most critical and frequently targeted vulnerabilities—the Web browser. Isla offers an innovative, highly differentiated approach that is effective at stopping all Web-based malware, making it an optimal complement to an organization's existing sandboxing investments.

About Cyberinc

Cyberinc delivers high-performance security solutions that enable businesses to leverage the power of the Web and benefit by complete protection against browser-borne malware. The company's initial anti-malware offering is Isla, a powerful and innovative solution that isolates all known and unknown Web-based malware. For more visit www.cyberinc.com