Cyberinc

Solution Brief

Isla Protection for threats used by Ransomware

Phishing Threats

Malicious links in phishing emails are frequently the initial attack vector used to distribute ransomware. Isla secures malicious links and weaponized documents in spoofed and phishing emails by isolating them from your endpoint. Your users remain safe with fetch, execute and render functions all performed safely away from your endpoint regardless of what links they click.

Web Threats

The initial attack vector used to distribute ransomware is often drive-by downloads on hacked websites. No exploits are used, visitors are told they must install a phony update or unknowingly download the ransomware by simply clicking on the site. Browser isolation stops ransomware attacks because all external code is intercepted and transformed into harmless pixels before it has a chance to touch the endpoint.

Weaponized Documents

Attackers hide ransomware by weaponizing documents, yet users may need to download documents to their endpoint to do their work. Isla gives administrators the ability to set policies that allow their users to safely upload and download documents. When enabled, Isla renders documents in a safe read-only mode that prevents weaponized documents from delivering ransomware to the endpoint.

Ransomware Protection

The first ransomware was created in 1989 and three decades later, we still read about devastating ransomware attacks that succeed. Today, attackers rely on phishing tactics to entice an organization's users to click an errant link, allowing ransomware to slip on to their endpoint. No matter how much we train end users, some will always click on links inside a phishing email opening your organization up to a breach.

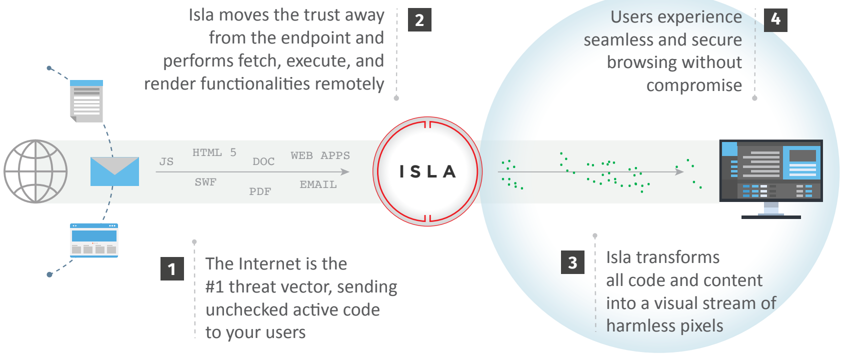
In the first quarter of 2019, ransomware attacks grew by 118%, while growing 41% for the full year.[1] Several new ransomware families are still being detected, such as Anatova, that is a modular architecture to facilitate newer ransomware development. Downtime costs from ransomware are up 200% Year-Over-Year. 205,280 enterprises lost access to their files due to such attacks.[2] Chasing the ransomware is clearly not working. Attackers are always evolving their approach.

With the Isla isolation platform, your users are safe from ransomware and related threats including credential theft, phishing and weaponized documents. While user safety training is important to modify user behavior, it doesn't take care of highly targeted attacks or compulsive clickers.

Security professionals know ransomware is insidious, relentlessly using social engineering attacks until one user is tricked into clicking a phishing link or opening a file attachment. Since it only takes one click to succeed, attackers know it's only a matter of time before they will succeed, with minimal chance of arrest because cryptocurrency transactions cannot be traced.

Once a ransomware attack succeeds, security professionals and business executives are faced with conflicting options. Paying the ransom encourages future attacks. Yet the recovery could be far more costly than the original demand. The city of Atlanta spent $2.6 million on emergency efforts when faced with a $50,000 ransom.[3] Have we reached the point where only three things are certain in life: death, taxes and ransomware?

RANSOMWARE SECURITY WITH ISLA



1 The Internet is the #1 threat vector, sending unchecked active code to your users

2 Isla moves the trust away from the endpoint and performs fetch, execute, and render functionalities remotely

3 Isla transforms all code and content into a visual stream of harmless pixels

4 Users experience seamless and secure browsing without compromise

With most cyber-attacks coming from your browser, there is a time proven technique for preventing infections in the physical world that can also prevent ransomware: isolation. Using a Zero Trust model, Isla isolates all code, media, and scripts coming through your web browser or links in email and neutralizes threats without the need for detection or compromising productivity. Your users can do everything they did before but now ransomware can't touch their endpoint, and your attack surface is dramatically reduced.

Ransomware Threats

Ransomware continues to evolve and to succeed. In April 2020, one of the largest tech and consulting companies in the Fortune 500[4] confirmed they were victims of ransomware. The previous month, a leading cybersecurity insurance provider[5] was a victim. New forms of ransomware steal user credentials and exfiltrate the data to the attackers' servers where it is held for ransom. If a ransom isn't paid, the attackers publish the files online. Isla doesn't look to detect new variants, but instead uses a proactive remote execution model to isolate ransomware before they ever reach your endpoint. Isla, using a Zero Trust model, continues to protect your data from evolving ransomware threats.

Ransomware Threat	Key Takeaway	Isla Protection
Initial attack vectors	Drive-by downloads on hacked websites or phishing links in email are used most often to distribute ransomware.	Isla blocks these methods because Isla fetches, executes, and renders all web content, including any links your users might click within their email, away from the endpoint.
Propagation through partner organizations	Attackers hide ransomware by weaponizing documents, and partners may unknowingly upload/download these documents into shared repositories like SharePoint and Google Drive.	With Isla, administrators set policies that allow their users to safely upload and download documents. When enabled, Isla renders documents in a safe read-only mode that prevents weaponized documents from delivering ransomware to the endpoint.
Evolving Ransomware	Attackers use stolen credentials to exfiltrate the data to the attackers' servers where it is held for ransom. If a ransom isn't paid, the attackers publish the files online.	Isla Safe Surf renders suspicious sites in a read-only mode to stop end users from unintentionally compromising their login credentials or risk losing other valuable information during phishing attacks that could be used for ransomware attacks.

[1] McAfee Labs Threats Report 2019 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf
[2] Hashed Out Feb 27, 2020 https://www.thesslstore.com/blog/ransomware-statistics/
[3] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-
[4] https://techcrunch.com/2020/04/18/cognizant-maze-ransomware/
[5] https://techcrunch.com/2020/03/26/chubb-insurance-breach-ransomware/

About Cyberinc

Cyberinc helps you experience a safer Internet by proactively stopping web, email, and document-based threats. Cyberinc's Isla platform uses cutting-edge isolation technology to neutralize threats and prevent them before they have a chance to act, simplifying the security strategy and delivering immediate protection. Cyberinc is trusted by businesses of all sizes and governments around the world.

Contact us

☎ +1 925-242-0777

✉ info@cyberinc.com