Menlo Security

RANSOMWARE SOLUTION BRIEF

The Problem

Cybercriminals are increasingly utilizing ransomware to extort funds from individuals and organizations. Ransomware is a particularly insidious type of malware that restricts access to device or network data, primarily via encryption, until a ransom is paid to remove the restriction. Victims of these attacks are left little choice but to pay the cybercriminals in the hope that they will receive an unlock code or an encryption key that will free their information.

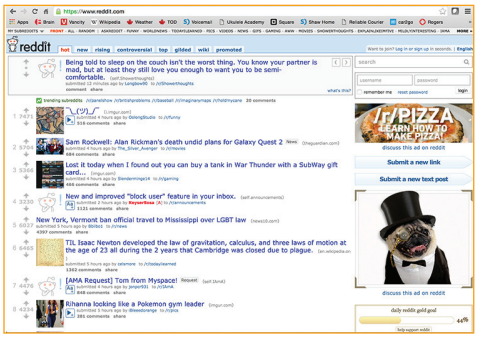
Users contract ransomware in the same way they contract other types of malware, primarily via the web and email.

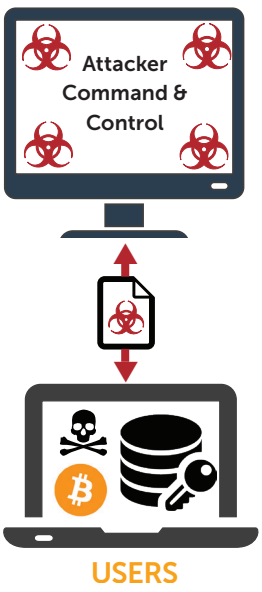
Their devices can be infected by simply navigating to a compromised web site or by inadvertently downloading a weaponized document. Any web site can potentially serve ransomware, even those considered safe, such as respected news and popular entertainment sites.

A typical scenario involves a user visiting a trusted website which unknowingly delivers malicious Flash by way of a third-party advertisement. The Flash then contacts the cybercriminal's command and control via an anonymous proxy and requests a dropper file. The dropper file contains an executable that locks or encrypts the device content. From there, the dropper is free to start encrypting files across the network, holding the information hostage until a ransom is paid. Even if the ransom is paid, there is no guarantee the data will be freed.

Defending against ransomware has been difficult to date. Conventional threat prevention products attempt to distinguish between good and bad content, and then implement policies intended to allow the good content and block the bad. This approach to threat prevention has failed because in today's threat landscape, all content is potentially harmful. A new solution is required.

1. Trusted website inadvertently serves up malicious Flash to user device





2. Flash compromises user device and makes request for malware dropper file from attacker command and control via anonymous proxy

3. Dropper file encrypts all device data which is now held hostage for bitcoin ransom

About Menlo Security

Menlo Security is making it safe to click with isolation, protecting organizations from cyber attack by eliminating the threat of malware from web and email.

Menlo Security is trusted by some of the world's largest enterprises, including Fortune 500 companies and financial services institutions. The company was founded by security industry veterans, in collaboration with acclaimed researchers from the University of California, Berkeley. Backed by General Catalyst, Sutter Hill Ventures and Osage University Partners, Menlo Security is headquartered in Menlo Park, California.

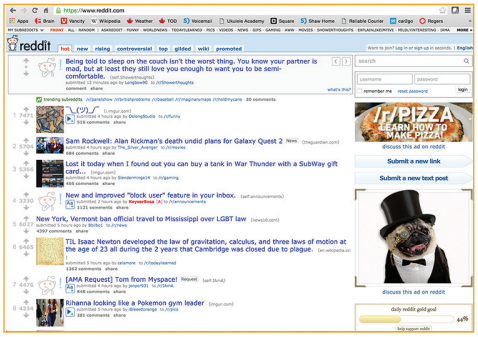
The Solution: Isolation

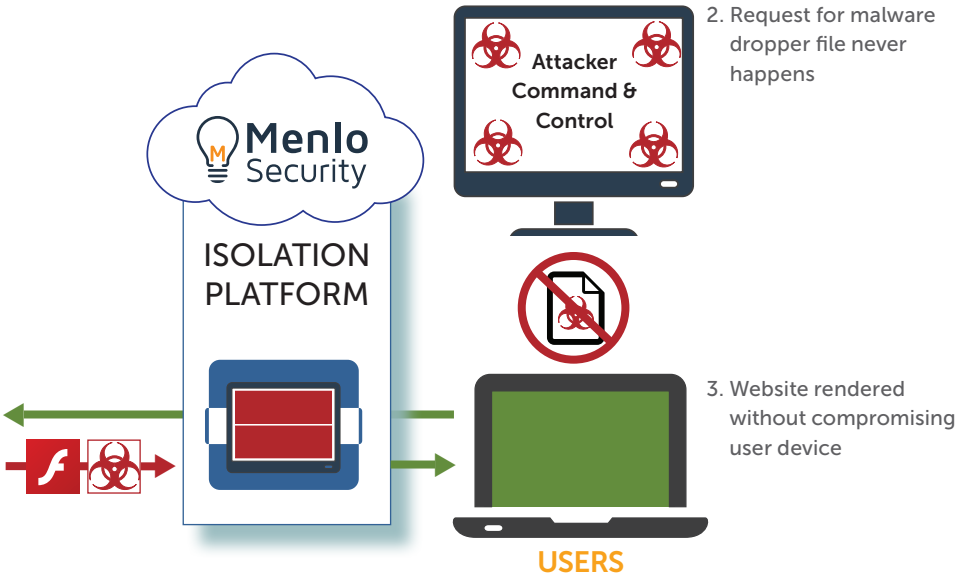
A new model for security based on isolation technology avoids trying to distinguish between legitimate content and malware. Isolation inserts a secure, trusted execution environment, or isolation platform, between the user and potential sources of attacks. By executing user sessions away from the endpoint and delivering only safe rendering information to devices, users are protected by eliminating the possibility of infection by malicious Flash, weaponized documents, and infected sites.

If isolation were deployed in the scenario described above, when the user accesses the compromised site, the malicious Flash would be safely transcoded and rendered on the endpoint. Thus, the Flash request for the dropper file would never happen and ransomware would never reach the device—no data would be held hostage.

Menlo Security delivers isolation with the Menlo Security Isolation Platform (MSIP). The MSIP is a cloud-based solution that sits between a user's device (e.g. desktop, laptop, tablet or smartphone) and the Internet. Web requests are proxied via the MSIP, which accesses the Web on the user's behalf, and executes the session completely. Only safe, malware-free rendering information is sent to the endpoint, eliminating the possibility of malware reaching it. MSIP delivers isolation security without compromising the user experience or placing a significant burden on IT staff. By leveraging patent-pending virtualization and Adaptive Clientless Rendering™ (ACR) technologies, MSIP enables enterprise-wide deployment of isolation security without the need to deploy or manage endpoint software or appliances, dramatically reducing ransomware risks.

1. Trusted website is still compromised but MSIP safely re-writes Flash without the user seeing any difference





For more information, visit menlosecurity.com or sales@menlosecurity.com.

Menlo Security

934 Santa Cruz Avenue
Menlo Park, CA 94025
Tel: 650 614 1795
info@menlosecurity.com