Menlo Security

BRIEF

Menlo Security Protects Organizations from Iranian Retaliation in New Front as Middle East Tensions Increase

As warfare extends to cyberspace, U.S.-based organizations can use email and web isolation to protect users from common tactics used by Iranian-backed threat actors.

Benefits:

- 100% malware-free email and web browsing—guaranteed
- Protection against phishing, drive-bys, and credential theft
- Suspicious web forms rendered in read-only mode

The U.S. Department of Homeland Security (DHS) issued an alert for U.S.-based companies and government agencies that they may be targets of Iranian retaliation as a result of escalating tensions in the Middle East. The advisory from DHS's Cybersecurity and Infrastructure Security Agency (CISA) gives examples of past cyberattack attempts, lists potential technical systems and technologies that could be targeted, and provides guidance on how to counter those tactics. Many of these attacks could begin with a phishing attack or malware that is downloaded onto a user's machine.

According to DHS, Iranian cyberthreat actors have improved their offensive cyber capabilities and engage in activities ranging from website defacement and distributed denial-of-service attacks to theft of personal identifiable information. The Iranian state-sponsored attacks are carried out by the Islamic Revolutionary Guard Corps (IRGC) or contractors in the Iranian private sector. Iran's cyber capabilities make it very likely that they may escalate their conflict with the United States beyond traditional battlefields to cyberspace—with new cyberwarriors waging highly technical dogfights in a new type of Cold War. Caught in the crossfire are businesses, nonprofits, utilities, and civilian government agencies—organizations that when breached can cripple the domestic economy and disrupt mission-critical operations.

Traditional Cybersecurity Solutions Fall Short

Phishing remains a favorite delivery method of Iranian-sponsored threat actors. Using fake emails and web forms to steal credentials is a relatively easy and inexpensive way to gain access to critical business systems. And the method has proven to work. According to Verizon's 2018 Data Breach Investigations Report, 12

percent of users will open a malicious email, and 4 percent will always click a link in a malicious email. The only thing that threat actors have to do is continue to send legitimate-looking emails to targeted individuals until eventually someone clicks on a link that sends them to a fake login page or a compromised website.

The problem is that most organizations continue to rely on cybersecurity solutions grounded in outdated detect-and-respond tactics. Detection simply doesn't work when the emails themselves don't carry malware, or when the highly targeted nature of today's attacks results in little or no reputational information available to reference.

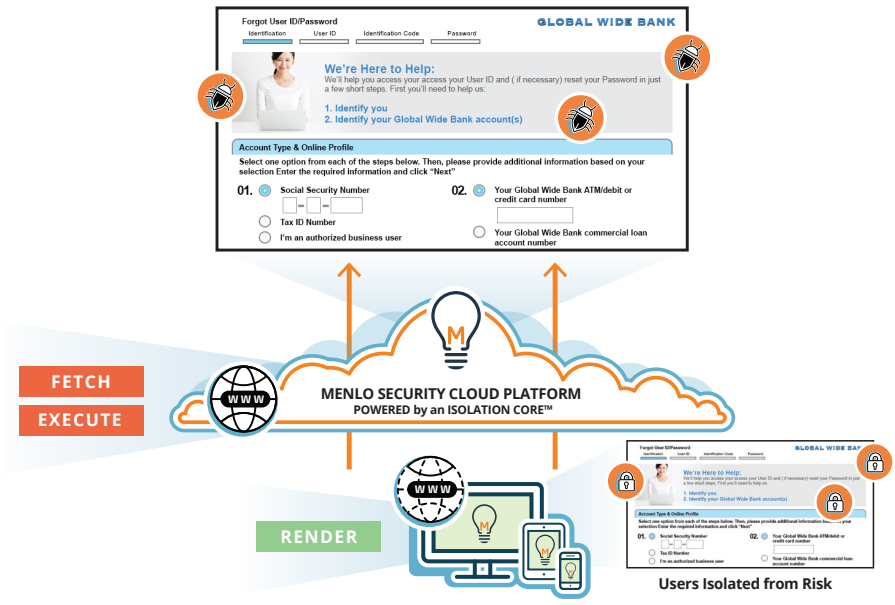
Isolation Provides 100 Percent Protection

Email and web isolation can level the playing field by inserting a secure, logically air-gapped execution environment in the cloud between the user and potential sources of attacks. By executing sessions away from the endpoint and delivering only safely rendered information to devices, users are protected from malware and malicious activity. A cloud proxy platform built on an Isolation Core™ is the only cybersecurity approach that can guarantee 100 percent protection.

The result is that malware cannot infect a device it cannot reach. Isolation eliminates the possibility of malware reaching user devices via compromised or malicious websites, email, or documents. This approach is not detection or classification; rather, the user's web session and all active content (JavaScript,

A cloud proxy platform built on an Isolation Core™ is the only cybersecurity approach that can guarantee 100 percent protection.

Zero Trust Internet Architecture



Flash, etc.)—whether it's good or bad—is fully executed and contained in a remote web browser in the cloud. Only safe, malware-free information is mirrored to the user's endpoint device. No active content—including any potential malware—is able to escape the environment, because it has no path to reach an endpoint.

Secure Internet

Secure Internet solution is the only cloud proxy platform built on an Isolation Core™ and is the ideal solution to protect users, business systems, and data from Iranian-backed threat actors. The Department of Defense (DOD) recently awarded Menlo Security a contract to build Cloud-Based Internet Isolation (CBII) prototype capability for the Defense Information Systems Agency (DISA). Managed by By Light Professional IT Services, the Menlo Cloud Proxy platform built on an Isolation Core™ will protect DOD employees from the type of attacks favored by Iranian-sponsored threat actors. Menlo Security has also helped hundreds of Global 2000 companies and major government agencies use isolation to prevent phishing, drive-by exploits, and other web- and email-based attacks.

To find out how Menlo Security can provide your company with protection against cyberattacks, visit menlosecurity.com or contact us at ask@menlosecurity.com.

In today's threat landscape, perfect prevention of breaches is not possible, and isolation and containment of an attacker's ability to do damage is becomingly increasingly important.

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents, and email. Menlo Security has helped hundreds of Global 2000 companies and major government agencies achieve Secure Cloud Transformation. The Menlo Security Cloud Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. The company was named a Visionary in the Gartner Magic Quadrant for the Secure Web Gateway.

Contact us
menlosecurity.com
(650) 614-1705
ask@menlosecurity.com