IS YOUR BSA/AML COMPLIANCE TEAM PRODUCTIVE AND PROTECTED ON THE WEB?

DANGEROUS EXPOSURE OF INFRASTRUCTURE

Watering Hole Attacks on BSA/AML Compliance Professionals

The websites of state and federal regulators are among the online destinations most frequently accessed by compliance managers and AML/Anti-fraud analysts and researchers. While improving productivity, such government online resources often also suffer from significant IT security weaknesses.

This can lead to dangerous exposure of the bank's IT infrastructure, because many AML teams lack adequate protection against web-borne exploits when they access the internet. When they use a local browser, adversaries can easily identify the originating organization and launch pinpointed malware and spyware attacks against financial institutions.

Does your organization provide its BSA/AML team with sufficient protection against such threats? Consider this recent case:

TARGETED INSTITUTIONS

Malware campaign hits banks using a regulatory website

In 2016/17, financial institutions in more than 30 countries were targeted by attackers who compromised websites known to be frequently accessed by compliance managers in the financial services sector.

In this "watering hole" campaign, they infected those website visitors with previously unknown malware. A bank in Poland discovered it on its network and informed other institutions, who also confirmed infiltration by the same malware strain.

Investigators later identified the likely source of the attack. It was the website of the Polish Financial Supervision Authority KNF, Poland's financial regulator. Users of this website, including many AML/Anti-fraud specialists from other countries obtaining regulatory updates, had been redirected to an exploit kit that was programmed to install malware on selected targets in the financial sector.

MAIN FACTORS OF SUCCESS

How can financial institutions prevent such attacks?

Incidents like this can be prevented by disconnecting from the "bad parts" of the web - with a cloud browser that isolates and processes all content remotely. Why is this important? Mainly two factors allowed the watering hole attack to succeed. Both were the result of using a regular browser:

- First, when bank employees access the web with a local browser, their IP address is disclosed. On infected sites, this can trigger a targeted attack by a data-driven automated malware dropper.
- Second, exploit kits can take hold in the victims' IT infrastructure because regular browsers indiscriminately download and process web content, including malicious code, on the local computer.

Research confirms that traditional AV software provides little or no protection against sophisticated attacks like this. More likely, it will exacerbate this problem. The only way to completely protect your compliance team against such web-borne threats is to effectively disconnect them from the web's risk zone.

This can be accomplished by deploying a cloud browser. Silo, the cloud browser provided as a service on Authentic8 servers, is built fresh from a clean image at the start of each web session. Because only

Authentic8's IP addresses are used, attribution to a specific organization and browser fingerprinting become impossible.

All web content is isolated and rendered in a secure container in the cloud. Only visual display information (pixels) is transmitted back to the user. No code from the web can touch (and infect) the endpoint (and spread from there through the network).

TRY SILO YOURSELF!

www.authentic8.com/AML

COMPANY HISTORY

Authentic8 is a company with history rooted in another. Postini was founded in 1999 by the Authentic8 co-founder, and the core business and technology team were key Postini personnel. Postini pioneered the idea that a cloud-based service could solve security and compliance problems with email, and back in 1999 this was heresy. But the model won out.

Authentic8 was founded in 2010 around a different idea, but the parallels with Postini are many. The company addresses a real problem with an innovative approach. The thesis is simple: as business apps move to the cloud, the browser becomes more important than ever. Yet it's an unmanageable resource. Silo was conceived to change that.

We have headquarters and Federal Operations in California, Washington DC and Berlin Germany. For further content use web, email or phone (US, International).