AREA 1

Security Bulletin

Equifax Data Breach

Summary

Overview

On September 7th, 2017 Equifax disclosed the occurrence of data breach that occurred between May 2017 and July 2017. Equifax discovered the breach in July 2017.

Initial estimates suggest that up to 143 million people could be affected. Credit card information of approximately 209,000 cardholders and personally identifiable information of 182,000 consumers was also compromised. Given past history with similar such breaches, additional impact is likely to be uncovered over time.

Area 1 Security Guidance

Aside from the actual usage of compromised credit card data, personal information is one of the highest value data for attackers since it allows them to leverage it for future credential access into any system.

End users (be it in their corporate or personal life) tend to cluster their credentials using similar information that is associated with an individual’s personal data and attackers take advantage of that very basic human trait.

Area 1 recommends taking the following steps in order to ensure your corporate systems are protected:

- Ensure that you have a robust multi-factor Authentication system in place that neutralizes or minimizes the use of personal credentials within corporate systems.
- Ensure that any known unpatched vulnerabilities, especially high severity ones, are patched and addressed.
- Isolate any unpatchable at risk systems; and limit access to these systems via appropriate network ACL rules.
- Ensure that you have deployed comprehensive Phishing protection across your entire organization. Attackers are already exploiting this breach to send end users look-alike Phishing messages and/or standing up credential harvesting sites purporting to be from Equifax. In order to contain lateral and future damage, please consider appropriate and robust Phishing controls wherever your organization’s digital presence is.

Area 1 Security Protections

Area 1 Security has had protections against associated Equifax phishing campaigns that could leverage Email messages or Web pages. Our systems have uncovered pages and messages related to Equifax based phishing attacks, with rapid escalation in both raw volume and sophistication of these attacks. Customers using Area 1 Horizon™ are automatically protected against these campaigns.

These protections are based on the following detection methodologies:

Proactive Web Crawling: Area 1 has activated several patterns related to Equifax specific credential harvesting pages. These look for evidence of pages similar to Equifax that are luring end users to share their usernames, passwords and other personal identifying information. These pages have no malicious payloads but instead force the end user to share data that can be used to breach corporate systems in future attacks.

Live Analytics using Computer Vision: Additionally, Area 1 systems are proactively looking for evidence of the Equifax brand being used by attackers as part of their phishing campaigns. Using advanced computer vision algorithms, the system programmatically discerns the presence of an Equifax logo (as it would appear for an end user) within phishing Web pages and phishing emails, stopping users from getting through to them.

About Area 1 Security

Targeted phishing attacks remain the primary cybersecurity threat to organizations large and small. These attacks come from all directions—email, web and network. Existing defenses struggle with these highly focused and sophisticated campaigns. Users consistently get lured into taking phishing baits, leading to significant financial damage or data loss.

The speed, variety, and maliciousness of these attacks demonstrate the urgent need for a new and advanced platform to address them. Area 1 Security stops phishing by preemptively identifying and neutralizing campaigns in the earliest stages of an attack; across all traffic vectors.

Learn more at https://area1.com and get in touch with us for a complimentary preview:
INFO@AREA1SECURITY.COM