TELEGRID

3 Attacks from “Non-Critical” Apps

TELEGRID

The use of Single-Factor Authentication (i.e., usernames and passwords) does not provide adequate protection for network devices and applications. For this reason many organizations have been moving to Two-Factor Authentication (2FA) including Smartcards, RSA SecurID, Biometrics, etc.

However, due to software upgrade or network redesign costs, administrators have been forced to make difficult decisions about which devices and applications should be secured with 2FA. Administrators typically 2FA-enable only the most important applications including those that handle Personally Identifiable Information (PII) (e.g., names, social security numbers, medical records, payment information, etc.). Indeed governance and compliance often demand that these applications be 2FA-enabled which is why they are selected.

Too often we view cybersecurity through the lens of auditors. What are the requirements for PII protection under HIPAA or PCI DSS? This attitude causes us to ignore so-called non-critical devices and applications. However, it is often the non-critical devices and applications that are the easiest to compromise and offer the most potential for attacks. This paper describes three such attacks and the risks they present to the organization. It concludes with an introduction to the SMRTe™, a cybersecurity tool that provides 2FA to all network devices and applications.

Three Ways to Hack an Organization using Non-Critical Applications

- Phishing
- Password Mining
- Ransomware

PHISHING

Phishing encourages users to log onto a seemingly trustworthy site in order to steal PII or download malware. Companies' employees are trained not to click on external web addresses and spam filters are configured to prevent these types of emails from entering an organization.

The difficulty lies in the situation where a hacker compromises a "non-critical" username and password based website that lies within an organization's own domain. These emails will easily pass through a spam filter and an employee could click on the web address, believing that it is a legitimate corporate email.

Another potential phishing target is a usename and password based website that is customer facing. This type of attack could also damage the vendor's reputation. If a customer downloads malware from a vendor site it could call into question the vendor's security measures regarding PII.

Verizon's 2016 Data Breach Investigations Report (DBIR) refers to this as the Secondary Motivation of web application attacks. According to the Report, out of 100,000 incidents recorded in 2015, there were "20,000 incidents of websites that were used to either host malware, participate in distributed denial-of-service (DDoS) attacks or repurposed as a phishing site."

PASSWORD MINING

Password reuse is a common issue with roughly 59% of people reusing passwords. Indeed hackers use bots to scour weak websites in order to find passwords that can be reused at more high value websites (e.g., banking).

This issue is magnified for application developers who reuse administrator passwords and even private keys across multiple applications. The private key is used by developers to create a Certificate Signing Request (CSR) which is provided to the application user to prove the authenticity of the server. Application developers have been known to reuse private keys, and even CSRs, in order to simplify development amongst developers operating in multiple locations and time zones. While far from best practice this is a reality and is something every organization should ask when hiring third party developers.

If a weak application is compromised and the administrator password or private key is found in source control, it can be used to access more secure applications. Indeed if the private key is found it can be used to mimic the secure application, causing users to unwittingly provide PII.

TELEGRID

RANSOMWARE

Ransomware is the act of locking a user's personal computer and demanding a payment in order to unlock it. In the past few years we have started to see more brazen attacks on organizations' web applications. These attacks include locking databases with operational information or even entire websites and demanding money to have them unlocked.

While they do not contain PII, standard business applications are the lifeblood of an organization and even a minor hiccup in operations can result in millions of dollars of losses. How would your organization fair if it could not access its inventory database or a client relationship management system?

SMRTe

Verizon's DBIR states, "We are realists here, we know that implementation of multi-factor authentication is not easy." **TELEGRID disagrees!**

TELEGRID's SMRTe sits seamlessly between a 2FA provider (e.g., RSA SecurID) and a network device or application. TELEGRID's SMRTe allows 2FA without software redesigns by focusing on existing authentication and authorization protocols that have been widely used for over 20 years.

TELEGRID's patent pending technology provides secure authentication without the use of a firewall or reverse proxy. After a user is authenticated by the SMRTe, they can access the network device or application directly thereby removing any bottlenecks or latency. Even though devices do not "sit behind" the SMRTe, its revolutionary design ensures that hackers cannot perform a brute force password attack thereby eliminating the need for password vaults.

TELEGRID Technologies Inc.
23 Vreeland Road
Florham Park, NJ 07039
973-994-4440
sales@telegrid.com
www.telegrid.com