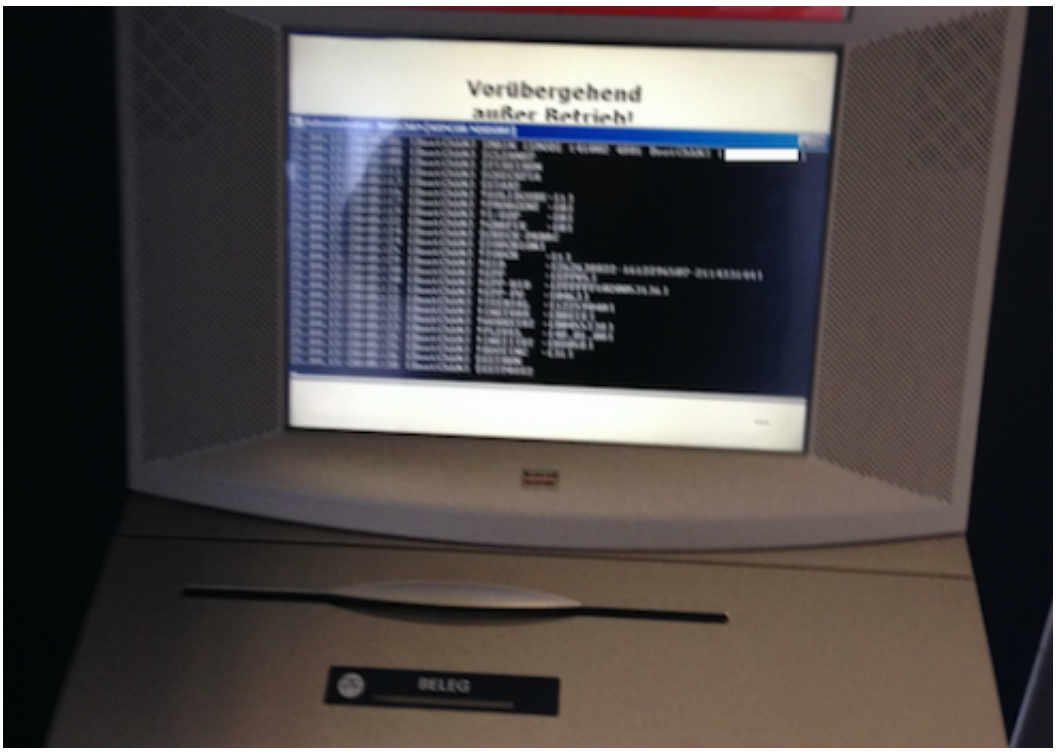
MUST READ Cracka hackers who doxed CIA Chief, now hit the FBI Deputy Director



Flaws in ATMs of a German Bank open the doors to cyber attacks

November 2, 2015 By Pierluigi Paganini

A security researcher at the Vulnerability Lab discovered that ATMs at the German savings bank Sparkasse can leak sensitive info during software updates.

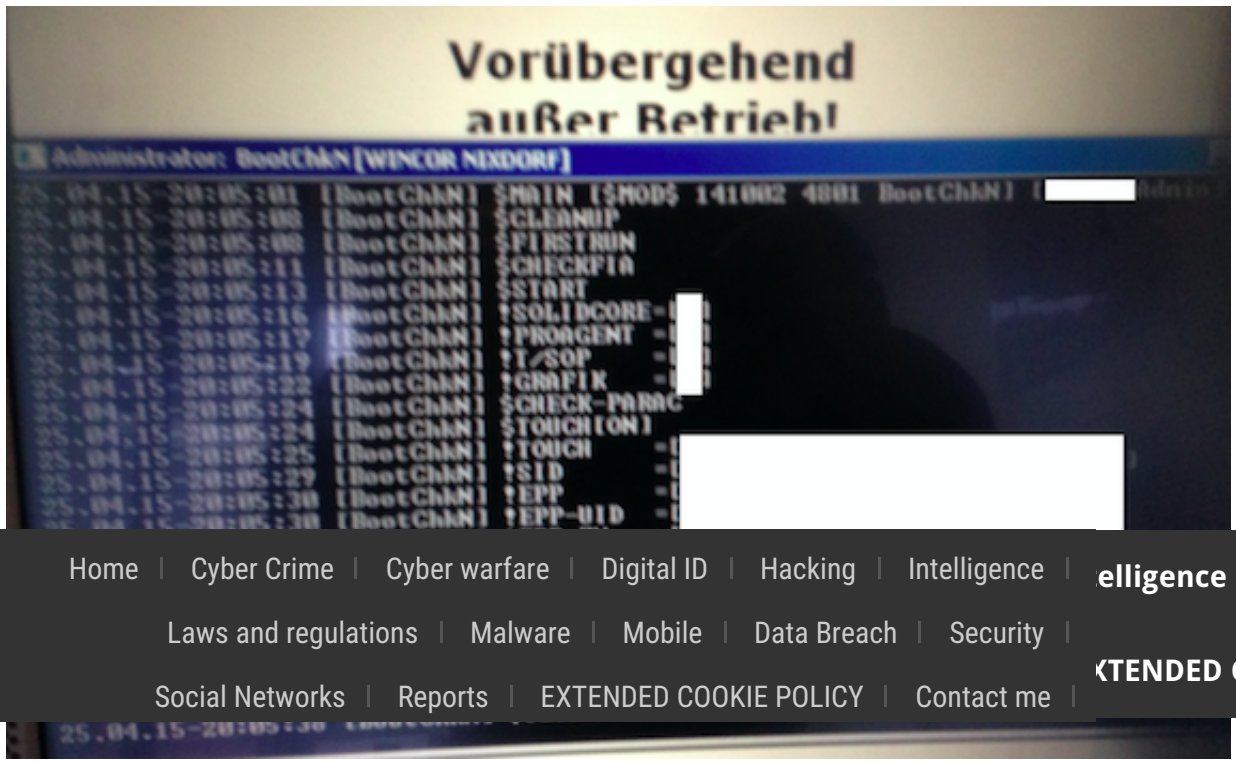
The security researcher Benjamin Kunz-Mejri, CEO of the Vulnerability Lab, discovered that ATMs at

the German savings bank Sparkasse can leak sensitive data during software updates.

The discovery of the anomaly was casual, Benjamin Kunz-Mejri was was using the ATM when it ejected his card and resulted “temporarily not available.” The expert tried to interact with the ATM and observed a Windows command prompt showing on ongoing update process, he took a video of the information displayed on the terminal.

The change of the status was caused by a software update, and the researcher used the term “timing attack” to describe his interaction with the ATM.

He was surprised that the ATM keyboard was not disabled, allowing an attacker to execute system commands via the command prompt. He also noticed that the card reader remained usable during the update process.



Video recording has allowed the expert to analyze the information displayed on the screen, he noticed that many sensitive data was revealed, including the bank’s main system branch usernames, serial numbers, network and firewall configurations, device IDs, ATM settings, and two system passwords.

The ATM machines analyzed by the researcher are manufactured by Wincor Nixdorf, one of the most important company of the retail and banking industry. The flawed terminals are running Windows 7 and Windows XP operating systems. It is likely that other banks which are using the Wincor Nixdorf ATMs might be affected as well.

The experts warn about a large scale attack coordinated by a criminal ring in conjunction with a planned update, they described the following possible attack scenarios:

- The attacker could use the information disclosed during the update process to run a man-in-the-middle (MitM) attack on the targeted bank's local network. This attacker needs a physical access to bank network.
- The attacker could push a bogus update to reconfigure the ATMs, also in this case he needs physical access to bank network.
- The Attacker could conduct fraudulent transactions by forcing the ATM crash and corrupt th logging or debugging mechanism.

The Vulnerability Lab reported the security issue to Sparkasse's Security and Data Protection tea May, the flaw was confirmed after the vulnerability report was received by the internal Finance Security Center.

The Sparkasse bank has already pushed out updates that fix the issue to a limited number of A in the city of Kassel. The purpose is to run further tests before issuing the update to all the ATM used by the organization.

It is the first time that a German bank admits the security vulnerability in an ATM and reward th researchers.

Pierluigi Paganini

(Security Affairs – ATMs , banking)

Breaking News Hacking

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief

at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Third suspect arrested in connection with the TalkTalk breach

NEXT ARTICLE
CISA Passes Senate, criticism about privacy and security