The Hacker News™
Security in a serious way

Report: German Bank ATMs vulnerable to Hackers

Monday, November 02, 2015 Swati Khandelwal

Avoiding Credit Card Fraud is simply easy as long as you use cash. But, what if you even get hacked while withdrawing cash from an ATM?

If you are living in Germany or traveling there, then think twice before using your payment cards in the ATMs.

Here’s why:

A Security researcher in Germany has managed to hack ATM and self-service terminal from Sparkasse Bank that allowed him to reveal the sensitive details from the payment card inserted into the machine.

Benjamin Kunz-Mejri, CEO of Germany-based security firm *Vulnerability Lab*, discovered a vulnerability while using a Sparkasse terminal that suddenly ejected his card, and changed status to "*temporarily not available*."

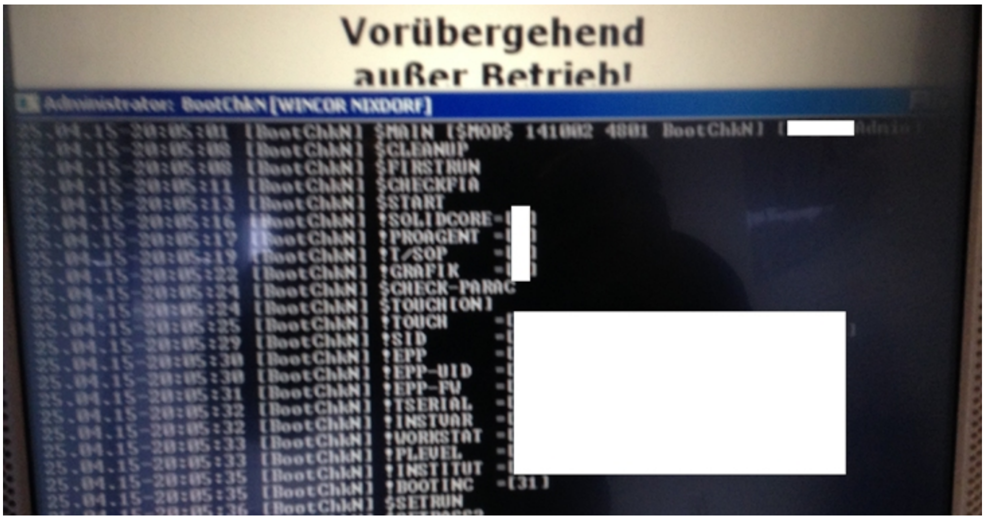
Meanwhile, the machine automatically started performing software update process in the background. However, Benjamin used a special keyboard combination to trick the ATM into another mode.

Benjamin’s trick forced ATM system to put update process *console (cmd)* in the foreground of the warning message.

> "*At that moment the researcher realized that there is a gap and used his iPhone to capture the bootChkN console output (Wincor Nixdorf) of the branch administrator,*" a blog post on Vulnerability-Lab stated.

After saving the data and reviewing the recording, Benjamin was able to reveal a lot of sensitive information, including the bank’s main branch office:

- Usernames
- Serial numbers
- Firewall settings
- Network information
- Computer name
- Device IDs
- ATM settings



```
Vorübergehend
außer Betrieb!
Administrator: BootChkN [WINCOR NIXDORF]
25.04.15 20:05:01 [BootChkN] $MAIN [$MOD$ 141002 4801 BootChkN] [[redacted] Admin
25.04.15 20:05:08 [BootChkN] $CLEANUP
25.04.15 20:05:08 [BootChkN] $FIRSTRUN
25.04.15 20:05:11 [BootChkN] $CHECKFIA
25.04.15 20:05:13 [BootChkN] $START
25.04.15 20:05:16 [BootChkN] ?SOLIDCORE=[[redacted]]
25.04.15 20:05:17 [BootChkN] ?PROAGENT =[ ]
25.04.15 20:05:19 [BootChkN] ?T/SOP    =[ ]
25.04.15 20:05:22 [BootChkN] ?GRAFIK   =[ ]
25.04.15 20:05:24 [BootChkN] $CHECK-PARAC
25.04.15 20:05:24 [BootChkN] $TOUCH[ON]
25.04.15 20:05:25 [BootChkN] ?TOUCH    =[[redacted]
25.04.15 20:05:29 [BootChkN] ?SID      =[
25.04.15 20:05:30 [BootChkN] ?EPP      =[
25.04.15 20:05:30 [BootChkN] ?EPP-UID  =[
25.04.15 20:05:31 [BootChkN] ?EPP-FW   =[
25.04.15 20:05:32 [BootChkN] ?TSERIAL  =[
25.04.15 20:05:32 [BootChkN] ?INSTVAR  =[
25.04.15 20:05:33 [BootChkN] ?WORKSTAT =[
25.04.15 20:05:33 [BootChkN] ?PLEVEL   =[
25.04.15 20:05:35 [BootChkN] ?INSTITUT =[
25.04.15 20:05:35 [BootChkN] ?BOOTINC  =[31]
25.04.15 20:05:36 [BootChkN] $SETRUN
```

- Two system passwords
- Other hardware related information

> "*Benjamin reported the critical issue to the Sparkasse Bank, which acknowledged the issue and has now started patching its ATMs and self-service terminals in a pilot program to prevent attacks.*" Sparkasse Bank said in a statement.

The ATM (Automated Teller Machine) analyzed by Benjamin is manufactured by Wincor Nixdorf, one of the most famous company in the retail and banking industry.

Therefore, the chances are high that other banks that are using the Wincor Nixdorf ATMs and self-service terminals are also affected, along with Sparkasse Bank.

Benjamin reported the critical issue to the Sparkasse Bank, which acknowledged the issue and has now started patching its ATMs and self-service terminals to prevent attacks.

ATM Hacking, Bank Hacking, Debit Card Hacking, Hacking Atm Machine, Hacking News, Secure Online Banking, Sparkasse Bank

Join us on Facebook: ✓ Like You, Elven Liu and 797,754 others like this.

ABOUT THE AUTHOR

Swati Khandelwal

Swati Khandelwal is Senior Technical Writer and Cyber Security Analyst at The Hacker News. She is a Technology enthusiast with a keen eye on the Cyberspace and other tech related developments. She is lover of digital culture, gadgets, creative media, technology, and general interest reporting.

SUBSCRIBE TO UPDATE

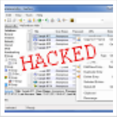
Want more Interesting Articles to your Inbox every Morning?.

What's your email?

Sign Me Up

LATEST STORIES

Fourth, a 16-year-old Hacker, Arrested over TalkTalk Hack

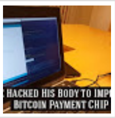


Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password Manager

Backdoor in Baidu Android SDK Puts 100 Million Devices at Risk

Anonymous Hackers to Leak 1000 of KKK Members Details on Million Mask March (Nov 5, 2015)

Kim Dotcom's Decentralized Internet — For You, Powered By You



Meet The World's First Person Who Hacked His Body to Implant a Bitcoin Payment CHIP

Hackers WIN $1 Million Bounty for Remotely Hacking latest iOS 9 iPhone

Report: German Bank ATMs vulnerable to Hackers

COMMENTS

5 Comments The Hackers News Исследовательс... ▾

Recommend Share Sort by Newest ▾

Join the discussion…

Lucy Howard • a day ago

2Ton9, bank hacker

^ | ˅ • Reply • Share ›

johnny Doe • a day ago

This entry is actually misleading. He can't dump cards off existing processes on this embedded XP install. He needs to get a process on the machine and to execute since batch files can neither scrape using API or dump via API since it's unlikely there is a single function somewhere that can be called with rundll32 or a CLI DB output of CC data. PowerShell isn't even on the machine either, and the CMD assembler where he'd hand type low level code isn't realistic. VBS might work if the runtime is installed since it has poor domain design and can use API. This all rides on the assumption you don't need a privilege escalation not blocked by policies and domains as well..

The machine is on leased line not routed to the public internet so no exploiting or downloading. You'd need code that could poll ToolTip API for process dumps to regex or something that could use the existing driver or API or hook and MITM the card reader process where it extracts data to go to processing center via socket call in the custom protocol handler..

ATM networks have weird protocol wrapping that weird ISO they use. I remember one was some encrypted TCP/IP protocol called BlueStream or something. In the early two-thousands someone actually got malware to spread and mine on one of these networks(it was BankOfAmerica I think); it was most likely someone with inside knowledge. If you can actually get on the subnet it's not that hard if you work faster than sysops looking at IDS and FW logs which especially these days are likely all over their infrastructure and I'm assuming they have weak signatures.

This is actually why crime syndicates don't just try to get in on the leased line networks and infect and mine everything with an embedded OS and reader hardware.. Instead using skimmers and internet botnets that MITB, and poll ToolTip on POS servers.

^ | ˅ • Reply • Share ›

Jens • 3 days ago

Yes, that cmd screen is commonly being displayed by the Wincor Nixdorf Machines during updates. Seen that a couple of times before. I did not record it but was able to memorize some of the network configs and user names involved. Told the clerks in reach, that this could be a serious risk, but no one seemed interested enough to escalate the issue to the apropriate department.

^ | ˅ • Reply • Share ›

Maximilian Kretschmer DSK • 3 days ago

I can tell you everything about Volksbank, most ATMs in Germany reboots on 00:30 AM, just use some boot device as before and you are happy. Their ATM software is some java software running on XP machines.

^ | ˅ • Reply • Share ›

Carina → Maximilian Kretschmer DSK • 2 days ago

Truth

^ | ˅ • Reply • Share ›

ALSO ON **THE HACKERS NEWS** WHAT'S THIS?

Hacking Team Offering Encryption Cracking Tools to Law Enforcement Agencies

5 comments • 5 days ago

droopyar — HackingTeam is a kids company. I still dont know how a goverment will use this kids companies that adds backdoors in ALL their …

Google is Merging its Chrome OS with Android

7 comments • 6 days ago

Jason Shin — It seems like Java is coming to its end as soon as Android drops Java and base itself on JS and HTML5

Hackers WIN $1 Million Bounty for Remotely Hacking latest iOS 9 iPhone

4 comments • 2 days ago

buck rogers — i heard the pangu team did it first anyway for free?

CryptoWall Ransomware raised $325 Million in Revenue for Its Developer

7 comments • 6 days ago

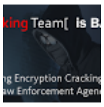
michaelrivero — The NSA says they cannot cannot find these guys. The official FBI recommendation is to pay up. Is ransomware …

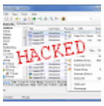
Subscribe Add Disqus to your site Privacy DISQUS

Popular Stories

Hackers WIN $1 Million Bounty for Remotely Hacking latest iOS 9 iPhone

Tor Releases Anonymous Instant Messenger. Here's How to Use It

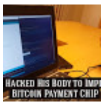

Hacking Team Offering Encryption Cracking Tools to Law Enforcement Agencies


Researcher releases Free Hacking Tool that Can Steal all Your Secrets from Password Manager

Free Ransomware Decryption Tool — CoinVault and Bitcryptor

Kim Dotcom's Decentralized Internet — For You, Powered By You

Meet The World's First Person Who Hacked His Body to Implant a Bitcoin



Payment CHIP

Biggest Free Hosting Company Hacked; 13.5 Million Plaintext Passwords Leaked

Report: German Bank ATMs vulnerable to Hackers

MIT Scientists: Now You Can See Through Walls with Wi-Fi

About | THN Magazine | The Hackers Conference | Sitemap | Advertise on THN | Submit News | Privacy Policy | Contact