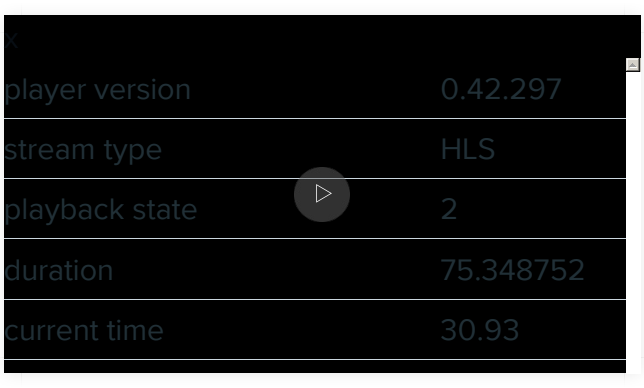
MUST READ: Intel is teaching a computer chip to smell

North Korean hackers infiltrate Chile's ATM network after Skype job interview

Redbanc employee applied for a LinkedIn job and got a call from the world's most active hacker crews.

By Catalin Cimpanu for Zero Day | January 16, 2019 -- 02:08 GMT (02:08 GMT) | Topic: Security



A Skype call and a gullible employee was all it took for North Korean hackers to infiltrate the computer network of Redbanc, the company that interconnects the ATM infrastructure of all Chilean banks.

Prime suspects behind the hack are a hacker group known as Lazarus Group (or Hidden Cobra), known to have associations to the Pyongyang regime, is one of the most active and dangerous hacking groups around, and known to have targeted banks, financial institutions, and cryptocurrency exchanges in the past years.

Lazarus' most recent attack took place at the end of December last year but only came to the public's attention after Chilean Senator Felipe Harboe called out Redbanc on Twitter last week for not disclosing its security breach.

The company, which has direct lines into the networks of all Chilean banks, formally admitted to the hack a day later in a message posted on its website, but that announcement didn't include any details about the intrusion.

However, a day after Redbanc's admission, an investigation conducted by Chilean tech news site *trendTIC* revealed that the financial firm was the victim of a serious cyber-attack, and not something that could be easily dismissed.

According to reporters, the source of the hack was identified as a LinkedIn ad for a developer position at another company to which one of the Redbanc employees applied.

The hiring company, believed to be a front for the Lazarus Group operators who realized they baited a big fish, approached the Redbanc employee for an interview, which they conducted in Spanish via a Skype call.

trendTIC reports that during this interview, the Redbanc employee was asked to download, install, and run a file named ApplicationPDF.exe, a program that would help with the recruitment process and generate a standard application form.

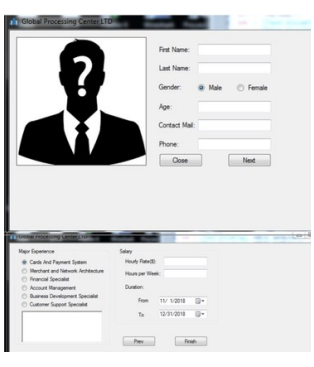


Image: Flashpoint

But according to an analysis of this executable by Vitali Kremez, Director of Research at Flashpoint, the file downloaded and installed PowerRatankba, a malware strain previously linked to Lazarus Group hacks, according to a Proofpoint report published in December 2017.

The malware, Kremez said, collected information about the Redbanc employee's work PC and sent it back to a remote server. Collected information included the PC's username, hardware and OS details, proxy settings, a list of current processes, if the infected host had RPC and SMB open file shares, and the status of its RDP connection.

The collected information would have been able to tell the hackers what computer they infected, and later decide if they'd want to deliver a second stage payload in the form of a more intrusive PowerShell script.

The Redbanc incident is yet another example of how one worker clicking on the wrong link or running the wrong file can result in a major security breach, and how one hacked PC or laptop can lead to an entire network getting compromised.

Previously, according to an indictment by US authorities, Lazarus Group hackers have been accused of attempting to steal money from Banco de Chile, a local Chilean bank.

Cybercrime and malware, 2019 predictions — SEE FULL GALLERY
1 - 5 of 15 — NEXT ›

MORE CYBERSECURITY NEWS:
- Anonymous hacker gets 10 years in prison for DDoS attacks on children's hospitals
- G Suite update warns you when someone is exporting your company's data
- US charges Ukrainian for SEC 2016 hack, others for insider trading
- A security conference will let you hack a Tesla car and earn cash prizes
- Liberian ISP sues rival for hiring hacker to attack its network
- Hacker 'BestBuy' sentenced to prison for operating Mirai DDoS botnet
- Google now lets you donate to charity through the Play Store CNET
- Phishing and spearphishing: A cheat sheet for business professionals TechRepublic

RELATED TOPICS: SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

By Catalin Cimpanu for Zero Day | January 16, 2019 -- 02:08 GMT (02:08 GMT) | Topic: Security

Recommended For You — Sponsored Links by Taboola
La fattoria di cui non potrai più fare a meno nel 2020. Gioco senza installazione — Taonga: la fattoria tropicale
Sylvester Stallone's Daughter Is Probably The Prettiest Woman To Ever... — MedicareGranny
Ora puoi illuminare ingresso, cortile e balconi... — SmartLed
Pocket Wi-Fi: Smart Device Lets Get Internenet Connection Wherever You... — Muama Ryoko
Confronta 120 offerte luce e gas di 40 gestori italiani | Comparasemplice.it — ComparaSemplice
Il costo dell'assicurazione auto a San Bonifacio potrebbe sorprenderti — Assicurazione auto | Ricerca annunci
Richest Countries in the World, Ranked — Work + Money
28 foto incredibili scattate in metropolitana — Graduatez

SHOW COMMENTS

MORE FROM CATALIN CIMPANU
Security — France warns of new ransomware gang targeting local governments
Security — Firefox to remove support for the FTP protocol
Security — COVID-19: With everyone working from home, VPN security has now become paramount
Google — Google pauses Chrome and Chrome OS releases due to coronavirus outbreak

NEWSLETTERS
ZDNet Security
Your weekly update on security around the globe, featuring research, threats, and more.
Your email address — SUBSCRIBE
SEE ALL

MORE RESOURCES
IT security and privacy: Concerns, initiatives, and predictions (TechRepublic Premium) — Research from TechRepublic Premium — READ NOW
IT Security: Concerns, budgets, trends and plans (TechRepublic Premium) — Research from TechRepublic Premium — READ NOW
Secure Browser Usage Policy — Tools & Templates from TechRepublic Premium — READ NOW

RELATED STORIES 1 of 3
Coronavirus and climate change reveal systemic risk for third parties — 94% of the Fortune 1000 are seeing supply chain disruptions.
Cisco tackles root privilege vulnerability in SD-WAN software — Three vulnerabilities have been patched in SD-WAN, two of which can lead to root privilege escalation.
This cryptocurrency miner uses unique, stealthy tactics to hide from prying eyes — A combination of botnet and cryptominer has been utilizing new obfuscation techniques never before made public.

France warns of new ransomware gang targeting local governments — PLUS: How destructive ransomware attacks could represent the future of cyberwarfare
Facebook's new project: To fix time itself
How European and British airlines are responding to the COVID-19 outbreak
Intel is teaching a computer chip to smell

JUST IN
New iPad Pro: It's an expensive package — 44 minutes ago
Apple's iPad Pro gets a big update, including official trackpad support — 1 hour ago
Coronavirus: They want to use your location data to fight pandemic. That's a big privacy issue — 1 hour ago
Free tools and services for businesses during the COVID-19 crisis — 2 hours ago
Oracle: Programming language Java 14 is out with these 16 major feature improvements — 2 hours ago
How Accenture is navigating COVID-19 pandemic — 3 hours ago
European Union to Netflix: Help stop the internet from breaking — 3 hours ago
Microsoft adds a new Microsoft 365 firstline worker plan to its line-up — 3 hours ago

NEWSLETTERS
ZDNet Announce UK
ZDNet's Announcements newsletter offers a mix of stories, special offers and members-only benefits.
Your email address — SUBSCRIBE
SEE ALL

TODAY ON ZDNET
ZDNet SPECIAL FEATURE: Cybersecurity: Let's get tactical
Collection: Coronavirus: Business and technology in a pandemic

Cisco tackles root privilege vulnerability in SD-WAN software — Three vulnerabilities have been patched in SD-WAN, two of which can lead to root privilege escalation. — 3 hours ago by Charlie Osborne in Security
Tesla's Elon Musk: We'll make ventilators if coronavirus causes a hospital shortage — Elon Musk says Tesla will produce ventilators if there is a shortage due to the new coronavirus outbreak. — 3 hours ago by Liam Tung in Tech Industry
Neuromorphic computing: Intel is teaching a computer to smell hazards — The company says it has built an algorithm that mimics the brain's activity to detect and identify different smells. — 3 hours ago by ZDNet Editors in Innovation
AI: A Guide For Thinking Humans — Tonya Hall sits down with Dr. Melanie Mitchell, Davis professor at the Santa Fe Institute, to discuss Mitchell's book about whether smart machines can actually think or understand, and what might make AI more reliable and trustworthy. — 3 hours ago by Tonya Hall in Artificial Intelligence
Microsoft Teams usage up by 12 million in the past week, hitting 44 million daily active users, due largely to COVID-19 — Microsoft says Teams usage is spiking because of remote working due to the COVID-19 coronavirus. Meanwhile, it's readying more new Teams features for delivery later this year. — 3 hours ago by Mary Jo Foley in Collaboration

Apple's iPad Pro gets a big update, including official trackpad support
Neuromorphic computing: Intel is teaching a computer to smell hazards
AI: A Guide For Thinking Humans
Apple cracks down on coronavirus apps
Australian universities tout development of quantum error correction codes
Deep learning changes scientific research, finds antibiotic for multi-resistant bacteria
Article: Top cloud providers 2019: AWS, Microsoft Azure, Google Cloud; IBM makes hybrid move

VIDEO: Coronavirus: How hackers are exploiting the epidemic to steal your information
Amid growing employee activism, Google agrees to set up a worker council in Europe — The search giant has agreed to set up a council in Europe – but it is not clear how much power it will really have. — 4 hours ago by Daphne Leprince-Ringuet in Google
Safeguarding customer information policy — Data breaches can cost companies tens of thousands of dollars or more and can pose a significant risk to company operations and reputation. Customer information is usually one of the favorite targets... — from TechRepublic Premium
New SpaceX launch: Starlink now has 360 internet-beaming satellites, as US service nears — SpaceX's Starlink gets closer to minor coverage of North America. — 4 hours ago by Liam Tung in Networking
Apple finally decides the iPad Pro is a computer (and isn't) — In two new ads, Apple slyly refers to promises it made before. — 4 hours ago by Chris Matyszczyk in Apple
2gether unveils how women are spending digital currencies — As digital crypto currencies continue to gain momentum, and used more widely, how are women using these currencies? — 5 hours ago by Eileen Brown in Blockchain
This cryptocurrency miner uses unique, stealthy tactics to hide from prying eyes — A combination of botnet and cryptominer has been utilizing new obfuscation techniques never before made public. — 6 hours ago by Charlie Osborne in Security

Wyndham Hotels & Resorts tackled technical debt, cloud, hybrid cloud in a hurry [Cloud TV]
HSBC charts out its move to the cloud [Cloud TV]
How Brinker International thinks through cloud, data, Apple iPads [Cloud TV]
Why security is the top barrier in enterprise cloud adoption [Hybrid Cloud TV]
How New Belgium Brewing evaluated managed vs. private cloud [Hybrid Cloud TV]
With Red Hat, IBM to become the leading hybrid cloud provider

GALLERY: Coronavirus: How to clean and disinfect your tech gadgets
LOAD MORE

Recommended For You — Sponsored Links by Taboola
Se hai più di 40 anni, questo gioco è un must! — Vikings: Gioco online gratuito
Il gioco di strategia più coinvolgente del 2020 — Total Battle: Gioco di Strategia Online
Come assumere un investigatore privato in Italia? Quanto costano? — Investigatori privati | Ricerca annunci
How To Get Unrestricted Internet Access Worldwide With One Simple Tool — ExpressVPN

MORE RESOURCES
Lunch and learn: Dealing with the risks of identity theft — Downloads from TechRepublic Premium — DOWNLOAD NOW
IT leader's guide to the threat of cyberwarfare — eBooks from TechRepublic Premium — READ NOW
Quick Guide: Lock Down the IT Department — eBooks from TechRepublic Premium — READ NOW
Quick Guide: Securing Windows Server 2003 — eBooks from TechRepublic Premium — READ NOW

© 2020 CBS Interactive. All rights reserved. Privacy Policy | Cookies | Ad Choice | Advertise | Terms of Use | Mobile User Agreement
Visit other CBS Interactive sites: Select Site
Manage Cookies