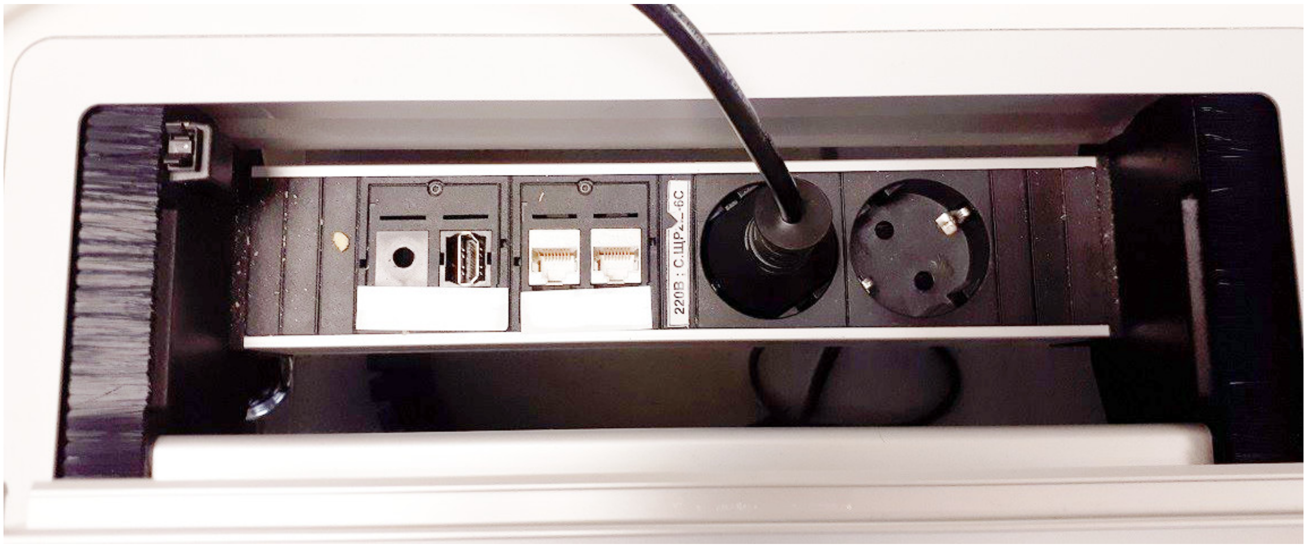
Netbooks, RPis, & Bash Bunny Gear - Attacking Banks from the Inside

bleepingcomputer.com/news/security/netbooks-rpis-and-bash-bunny-gear-attacking-banks-from-the-inside/

Ionut Ilascu

By
Ionut Ilascu

- December 7, 2018
- 02:36 AM
- 0



Multiple banks in Eastern Europe have been attacked from inside their network via various electronic devices connected directly to the company's own infrastructure, security researchers have discovered.

Where possible, the adversary made an effort to hide the entry point by planting the malicious devices in a way that did not attract attention. The losses created this way are estimated to tens of millions of dollars.

Direct access to the local network

Dubbed DarkVishnya, the attacks targeted at least eight banks using readily-available gear such as netbooks or inexpensive laptops, Raspberry Pi mini-computers, or a Bash Bunny - a USB-sized piece hardware for penetration testing purposes that can pose as a keyboard, flash storage, network adapter, or as any serial device.

They gained access to the local network from various places inside the victim's central or regional offices, and even from company branches in a different country.

Given their position, the devices could launch attacks that bypassed network defenses and could easily run reconnaissance routines, which are the first step of a cyber attack once on the target infrastructure.

Sergey Golovanov from Kaspersky Lab says that the researchers discovered this attack method between 2017 and 2018 while investigating cybertheft incidents.

"Inside the local network, the device appeared as an unknown computer, an external flash drive, or even a keyboard," he details.

To control the rogue gear remotely, the attackers used a built-in or USB-powered GPRS/3G/LTE wireless modules.

In the second stage of the attack, the intruders scanned the digital premises in search of open resources such as shared folders and web servers with public access.

The goal was to identify and collect valuable information like login credentials for systems used for making payments. To this end, the threat actor tried to brute-force their way in or intercept traffic to extract login data.

Evading firewall restrictions was possible through reverse TCP shells and the use of a different payload to create the communication tunnel. If all went well, the adversary would log into the target system and gain persistence.

Golovanov says that the threat actor launched on the compromised system malicious services created with the MSFvenom tool from the Metasploit Framework.

Fileless attacks are difficult to spot

The success of these operations is owed to the fact that they did not rely on specific malware to achieve their goals but relied on tools like PowerShell that could bypass whitelisting technologies and domain policies in most cases.

Although widely abused by cybercriminals to run malicious scripts, PowerShell is a legitimate component that is typically available on target machines.

Some system administrators block PowerShell on network machines to minimize the attack surface. If this was the case, the DarkVishnya attacks would use the Impacket Python library, winexesvc.exe or psexec.exe for remote execution of processes.

All three are legitimate tools used by admin to run commands on remote machines and redirect the output on the local system. PsExec has been used maliciously since at least 2004 and it was used by NotPetya ransomware for lateral movement.

Crims take a page from pentesters' book

This method of compromise is not new. It has been used in attacks against banks as early as 2013, when a gang stole over £1.3 million from Barclays Bank by connecting a keyboard video mouse (KVM) switch with a 3G router to a computer in the bank.

Penetration testers also use this method to breach defenses of a target with strong protections against outside access. Bash Bunny, for example, is specially built for this purpose as its form factor resembles a flash drive and once connected to a computer it can run scripts that give access to assets on the network.

Related Articles:

GitHub: Attackers stole login details of 100K npm user accounts

National bank hit by ransomware trolls hackers with dick pics

Heroku admits that customer credentials were stolen in cyberattack

A YouTuber is encouraging you to DDoS Russia—how risky is this?

Austin Peay State University resumes after ransomware cyber attack

- Bank
- Breach
- Cyber Attack

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: