DarkVishnya: Banks attacked through direct connection to local network

By Sergey Golovanov

Published: 2018-12-06 · Archived: 2026-04-06 02:00:41 UTC

06 Dec 2018

2 minute read

- Expert Sergey Golovanov

While novice attackers, imitating the protagonists of the U.S. drama *Mr. Robot*, leave USB flash drives lying around parking lots in the hope that an employee from the target company picks one up and plugs it in at the workplace, more experienced cybercriminals prefer not to rely on chance. In 2017-2018, Kaspersky Lab specialists were invited to research a series of cybertheft incidents. Each attack had a common springboard: an unknown device directly connected to the company's local network. In some cases, it was the central office, in others a regional office, sometimes located in another country. At least eight banks in Eastern Europe were the targets of the attacks (collectively nicknamed DarkVishnya), which caused damage estimated in the tens of millions of dollars.

Each attack can be divided into several identical stages. At the first stage, a cybercriminal entered the organization's building under the guise of a courier, job seeker, etc., and connected a device to the local network, for example, in one of the meeting rooms. Where possible, the device was hidden or blended into the surroundings, so as not to arouse suspicion.

High-tech tables with sockets are great for planting hidden devices

The devices used in the DarkVishnya attacks varied in accordance with the cybercriminals' abilities and personal preferences. In the cases we researched, it was one of three tools:

- netbook or inexpensive laptop
- Raspberry Pi computer
- Bash Bunny, a special tool for carrying out USB attacks

Inside the local network, the device appeared as an unknown computer, an external flash drive, or even a keyboard. Combined with the fact that Bash Bunny is comparable in size to a USB flash drive, this seriously complicated the search for the entry point. Remote access to the planted device was via a built-in or USB-connected GPRS/3G/LTE modem.

At the second stage, the attackers remotely connected to the device and scanned the local network seeking to gain access to public shared folders, web servers, and any other open resources. The aim was to harvest information about the network, above all, servers and workstations used for making payments. At the same time, the attackers tried to brute-force or sniff login data for such machines. To overcome the firewall restrictions, they planted shellcodes with local TCP servers. If the firewall blocked access from one segment of the network to another, but allowed a reverse connection, the attackers used a different payload to build tunnels.

Having succeeded, the cybercriminals proceeded to stage three. Here they logged into the target system and used remote access software to retain access. Next, malicious services created using msfvenom were started on the compromised computer. Because the hackers used fileless attacks and PowerShell, they were able to avoid allowlisting technologies and domain policies. If they encountered a allowlisting that could not be bypassed, or

PowerShell was blocked on the target computer, the cybercriminals used impacket, and winexesvc.exe or psexec.exe to run executable files remotely.

Verdicts

not-a-virus.RemoteAdmin.Win32.DameWare
MEM:Trojan.Win32.Cometer
MEM:Trojan.Win32.Metasploit
Trojan.Multi.GenAutorunReg
HEUR:Trojan.Multi.Powecod
HEUR:Trojan.Win32.Betabanker.gen
not-a-virus:RemoteAdmin.Win64.WinExe
Trojan.Win32.Powershell
PDM:Trojan.Win32.CmdServ
Trojan.Win32.Agent.smbe
HEUR:Trojan.Multi.Powesta.b
HEUR:Trojan.Multi.Runner.j
not-a-virus.RemoteAdmin.Win32.PsExec

Shellcode listeners

tcp://0.0.0.0:5190
tcp://0.0.0.0:7900

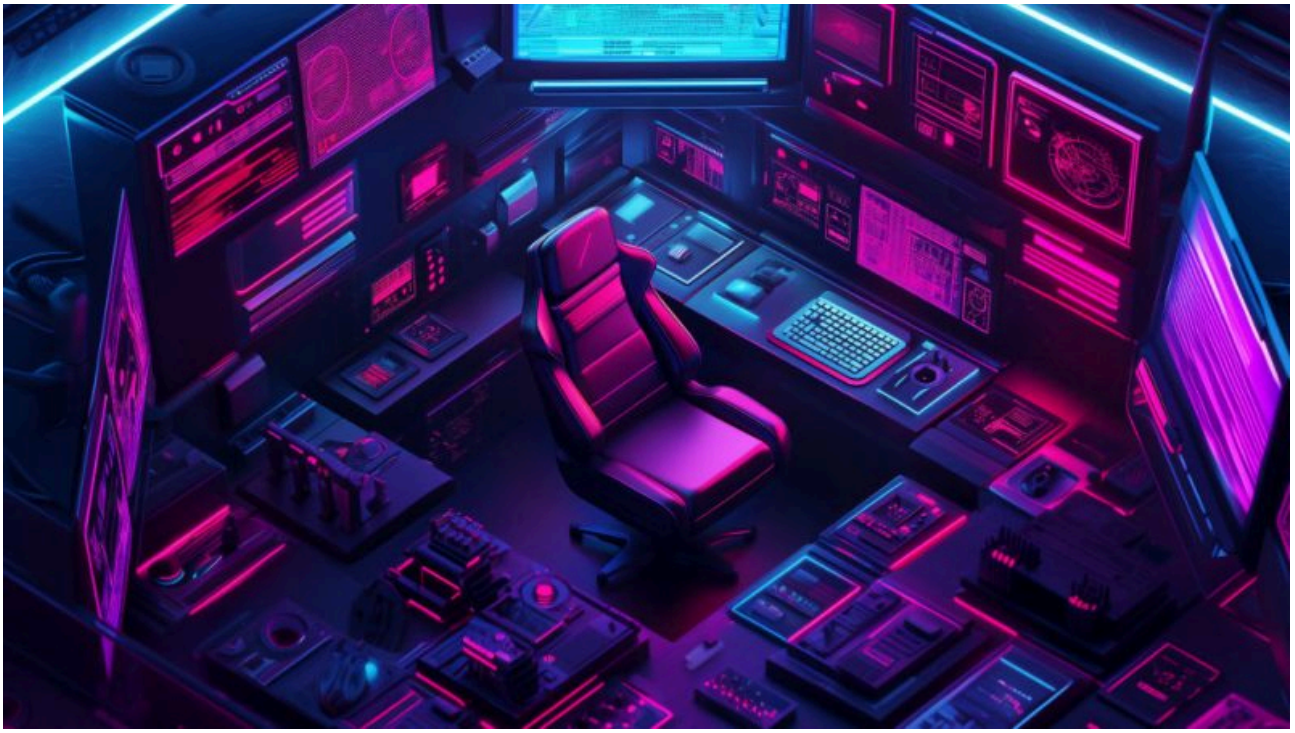
Shellcode connects

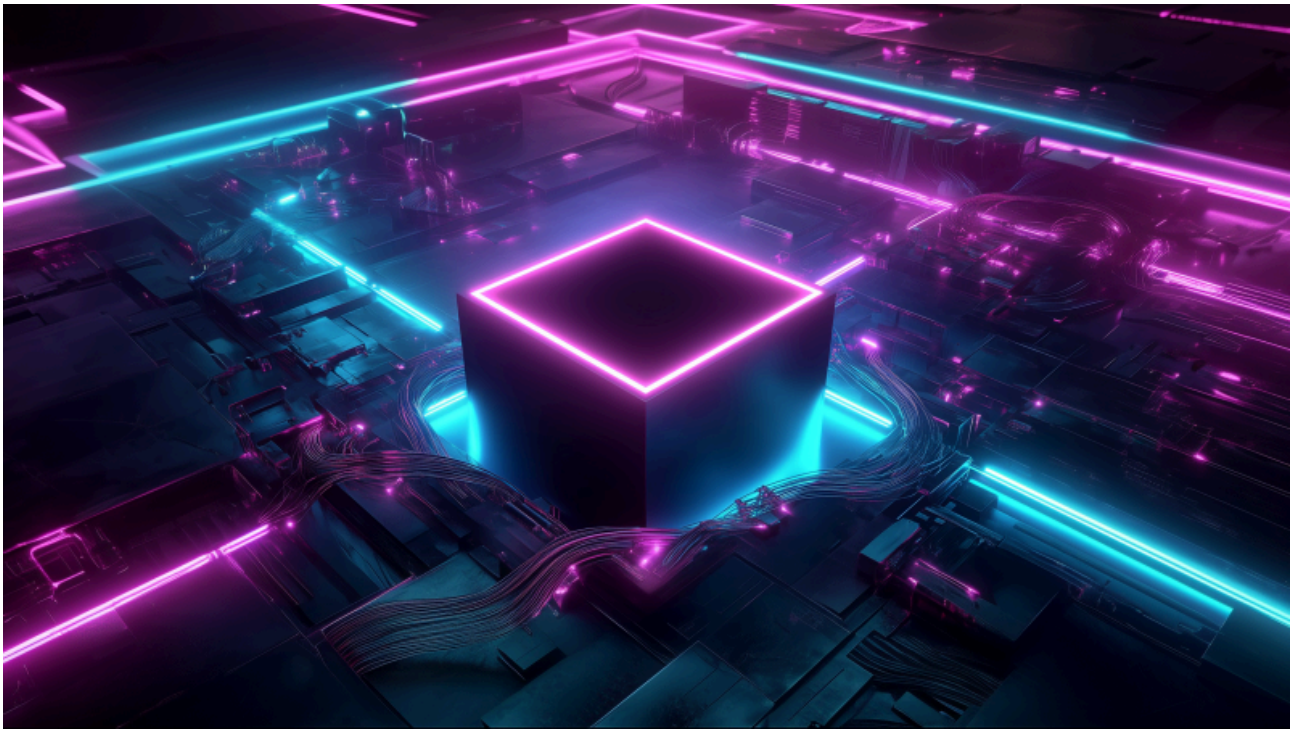
tcp://10.**.*.***:4444
tcp://10.**.*.**:4445
tcp://10.**.*.**:31337

Shellcode pipes

\\.\xport
\\.\s-pipe

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
