

Operation DRBControl: Uncovering a Cyberespionage Campaign Targeting Gambling Companies in Southeast Asia

Archived: 2026-04-02 11:38:14 UTC



[open on a new tab](#) Download Uncovering

DRBControl: Inside the Cyberespionage Campaign Targeting Gambling Operations

In 2019, Talent-Jump Technologies, Inc. reached out to Trend Micro about a backdoor they [discoveredopen on a new tab](#) during an incident response operation. We provided further intelligence and analysis on the backdoor, which we learned was being used by an advanced persistent threat (APT) actor that we dubbed "DRBControl." The threat actor is currently targeting users in Southeast Asia, particularly gambling and betting companies. Europe and the Middle East were also reported to us as being targeted, but we could not confirm this at the time of writing. Exfiltrated data was mostly comprised of databases and source codes, which led us to believe that the group's main purpose is cyberespionage.

The campaign uses two previously unidentified backdoors. Known malware families such as [PlugXopen on a new tab](#) and the [HyperBroopen on a new tab](#) backdoor, as well as custom post-exploitation tools were also found in the attacker's arsenal. Interestingly, one of the backdoors used file hosting service Dropbox as its command-and-control (C&C) channel. We disclosed our findings to Dropbox, which expired the tokens used in the campaign in August 2019 and has since been working with Trend Micro on the issues.

A newly identified threat actor behind a cyberespionage campaign targets gambling and betting entities by using publicly available and custom tools to elevate privileges and perform lateral movements. One of the deployed malware uses Dropbox as a way to communicate and exfiltrate data from targets.

Targets

DRBControl targets gambling and betting operations in Southeast Asia.

The threat actors behind the campaign use a variety of post-exploitation tools, such as a clipboard stealer, network traffic tunnel, brute-force tool, and password dumpers.

Operations

The first-stage intrusion uses spear-phishing .DOCX files. DRBControl distributes three versions of the infecting documents.

- The campaign primarily takes advantage of two backdoors, both of which use DLL side-loading through the Microsoft-signed MSMPeng.exe file.
- The type 1 backdoor already has nine versions, all developed between May to October 2019. All versions use the file hosting service Dropbox as their C&C channel.
- The type 2 backdoor uses a configuration file that has the C&C domain and connection port, as well as the directory and filename where the malware is copied. The file also sets its persistence mechanism.
- In most cases, IP addresses could be resolved only for subdomains hardcoded in malware samples; no IP address was linked to the domain names themselves.
- Known malware families (e.g., PlugX RAT, Trochilus RAT, and HyperBro backdoor) and software Cobalt Strike were also utilized in the campaign.

Network Activities

Connections with Other APT Campaigns

Different malware identified with [Winntiopen on a new tab](#) and [Emissary Pandaopen on a new tab](#) campaigns. Links to the Winnti group range from mutexes to domain names and issued commands. The HyperBro backdoor, which appears to be exclusive to Emissary Panda, was also used in this campaign.

Key Findings:

-
-
-

The DRBControl campaign attacks its targets using a variety of malware and techniques that coincide with those used in other known cyberespionage campaigns. The threat actors maintain a diverse infrastructure and take advantage of post-exploitation tools to further their operations.

The campaign not only uses file hosting service Dropbox as its C&C channel, but also for the delivery of different payloads. Dropbox repositories were also found to store information such as commands and post-exploitation tools, target user's workstation information, and stolen files.



EarthWorm network traffic tunnel



Public IP address retriever



Elevation of privilege vulnerability tool



Elevation of privilege vulnerability tool

Post-exploitation tools used by DRBControl

Conclusion

Unlike largely indiscriminate attacks that focus on typical forms of cybercrime, targeted attacks differ in terms of how threat actors actively pursue and compromise specific targets (i.e., through spear phishing) for lateral movement in the network and sensitive information extraction. Understanding attack tools, techniques, and infrastructure, as well as the links to similar attack campaigns, provides the context necessary to assess potential impact and adopt defensive measures. Trend Micro users can thwart advanced persistent threats with security that provide actionable threat intelligence, network-wide visibility, and timely threat protection.

Read our detailed findings in our research paper, "[Uncovering DRBControl: Inside the Cyberespionage Campaign Targeting Gambling Operations](#)," [open on a new tab](#) which looks into the malware that DRBControl uses, its relations to known APT groups, other noteworthy points of their activities, and indicators of compromise.

MITRE ATT&CK Matrix



[open on a new tab](#)

Download Uncovering DRBControl:
Inside the Cyberespionage Campaign Targeting Gambling Operations

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-
- - [The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructure](#)news article
 - [Complexity and Visibility Gaps in Power Automatenews article](#)
- - [Azure Control Plane Threat Detection With TrendAI Vision One™](#)news article
 - [AI Security Starts Here: The Essentials for Every Organization](#)news article
- - [The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026](#)predictions
 - [Ransomware Spotlight: DragonForcenews article](#)
- - [Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article](#)
 - [The Road to Agentic AI: Navigating Architecture, Threats, and Solutions](#)news article

Source: <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbccontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia>