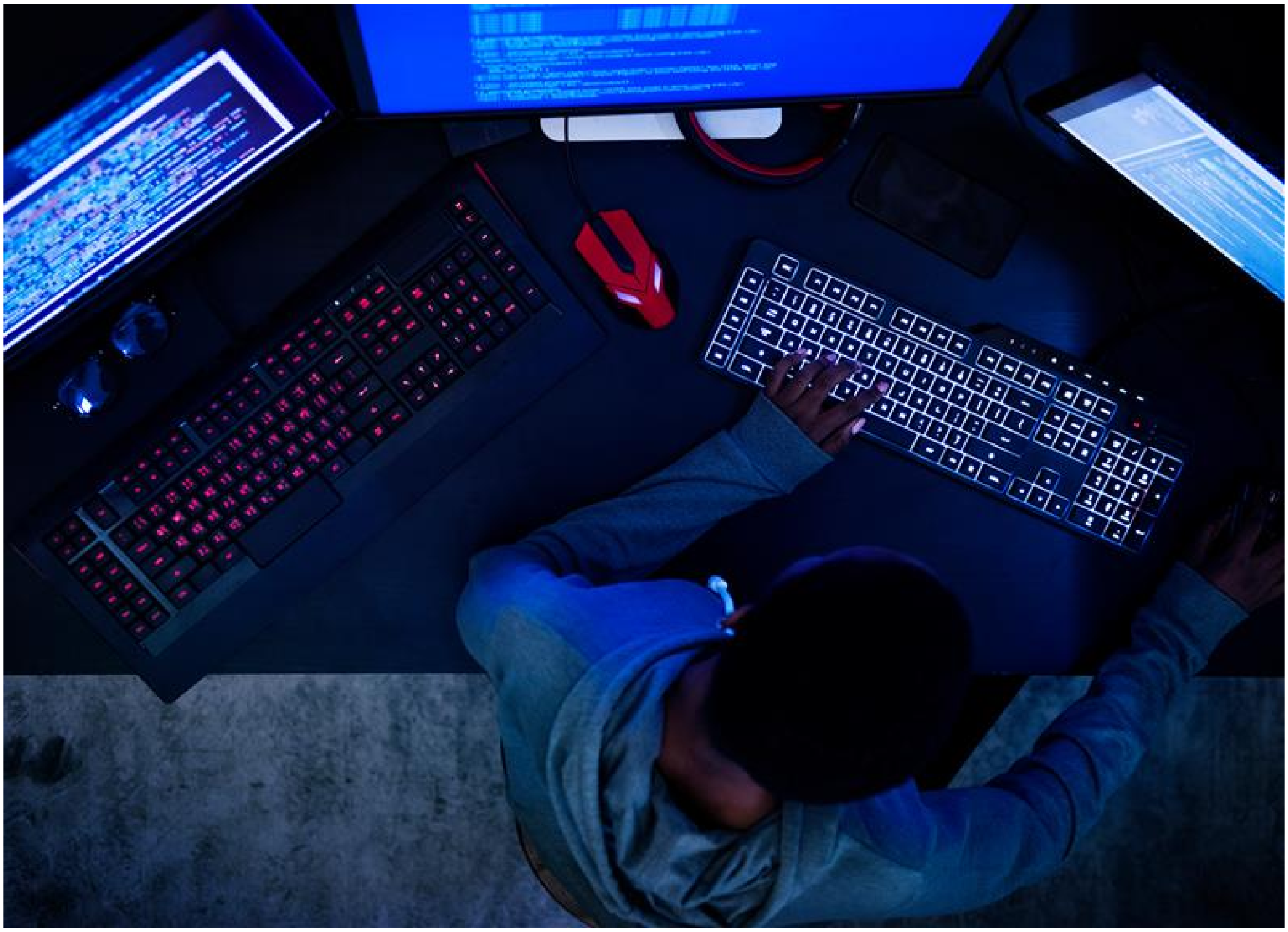
Operation DRBControl: Uncovering a Cyberespionage Campaign Targeting Gambling Companies in Southeast Asia

trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-drbcontrol-uncovering-a-cyberespionage-campaign-targeting-gambling-companies-in-southeast-asia



Uncovering DRBControl

Inside the Cyberespionage Campaign Targeting Gambling Operations

Kenney Lu, Daniel Lunghi, Cedric Pernet, and Jamz Yaneza

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 discovered 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 PlugX and the HyperBro 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.

OPERATION DRBCONTROL

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.

GAMBLING

BETTING

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 Winnti and Emissary Panda 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.

Clipboard stealer

EarthWorm network traffic tunnel

Public IP address retriever

NBTScan tool

Brute-force tool

Elevation of privilege vulnerability tool

Password dumpers

UAC bypass tools

Elevation of privilege vulnerability tool

Password dumpers

UAC bypass tools

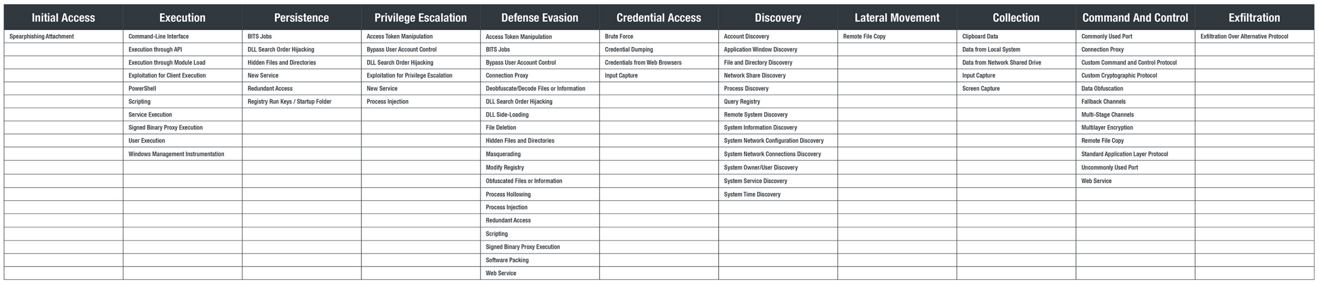
Code loaders
Post-exploitation tools used by DRBControl

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," 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



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration
Spearphishing Attachment	Command-Line Interface	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Account Discovery	Remote File Copy	Clipboard Data	Commonly Used Port	Exfiltration Over Alternative Protocol
	Execution through API	DLL Search Order Hijacking	Bypass User Account Control	BITS Jobs	Credential Dumping	Application Window Discovery		Data from Local System	Connection Proxy	
	Execution through Module Load	Hidden Files and Directories	DLL Search Order Hijacking	Bypass User Account Control	Credentials from Web Browsers	File and Directory Discovery		Data from Network Shared Drive	Custom Command and Control Protocol	
	Exploitation for Client Execution	New Service	Exploitation for Privilege Escalation	Connection Proxy	Input Capture	Network Share Discovery		Input Capture	Custom Cryptographic Protocol	
	PowerShell	Redundant Access	New Service	Deobfuscate/Decode Files or Information		Process Discovery		Screen Capture	Data Obfuscation	
	Scripting	Registry Run Keys / Startup Folder	Process Injection	DLL Search Order Hijacking		Query Registry			Fallback Channels	
	Service Execution			DLL Side-Loading		Remote System Discovery			Multi-Stage Channels	
	Signed Binary Proxy Execution			File Deletion		System Information Discovery			Multilayer Encryption	
	User Execution			Hidden Files and Directories		System Network Configuration Discovery			Remote File Copy	
	Windows Management Instrumentation			Masquerading		System Network Connections Discovery			Standard Application Layer Protocol	
				Modify Registry		System Owner/User Discovery			Uncommonly Used Port	
				Obfuscated Files or Information		System Service Discovery			Web Service	
				Process Hollowing		System Time Discovery				
				Process Injection						
				Redundant Access						
				Scripting						
				Signed Binary Proxy Execution						
				Software Packing						
				Web Service						

Uncovering DRBControl

Inside the Cyberespionage Campaign Targeting Gambling Operations

Kenney Lu, Daniel Lunghi, Cedric Pernet, and Jamz Yaneza

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.

Posted in Cyber Attacks, Research, Targeted Attacks, Cybercrime