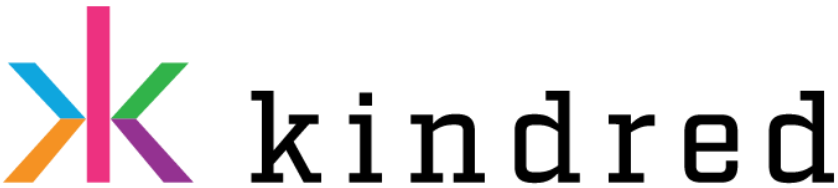
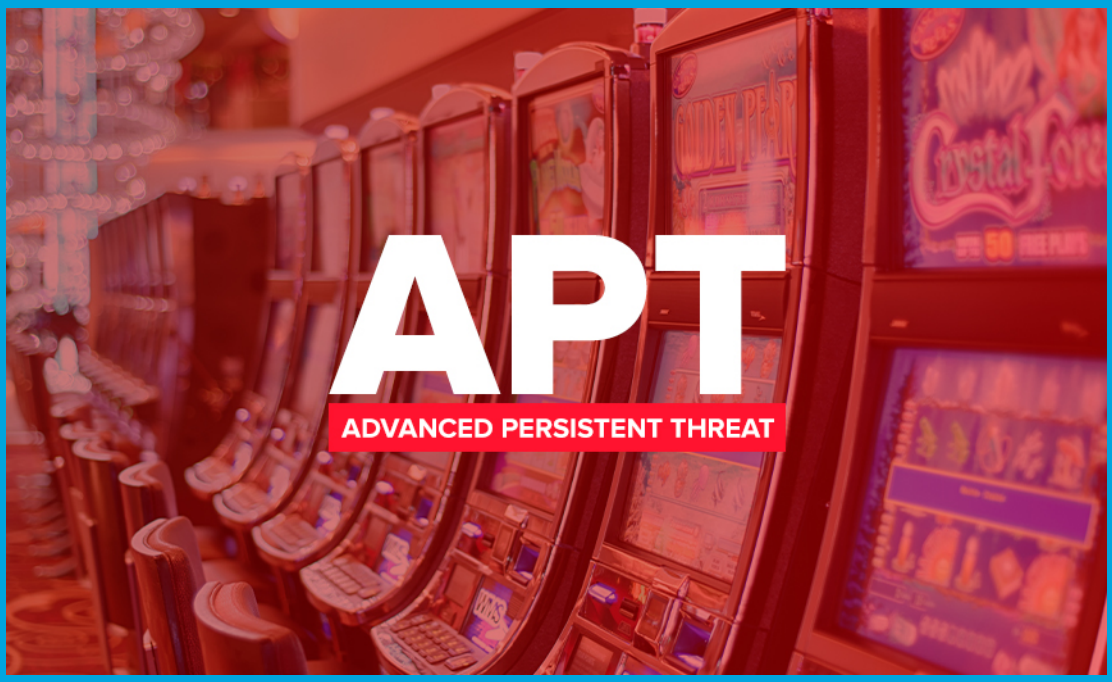


Security Newsletter

24 February 2020

Subscribe to this newsletter

New Hacking Group Targets Gambling Firms



A newly identified hacking group has been targeting gambling companies in Asia, the Middle East and Europe, using backdoors to steal source code and other data, according to new research from security firm Trend Micro. They call this newly discovered advanced persistent threat group "DRBControl."

The exfiltrated data was mostly composed of databases and source codes, which leads us to believe that the campaign is used for cyberespionage or gaining competitive intelligence. The attacks associated with DRBControl start with a spear-phishing email that targets individuals or departments within a company, according to the report. In several cases, it appears the hacking group targeted companies' customer support team. The phishing emails that Trend Micro examined came with attached Microsoft Word documents that also contained screenshots meant to show a problem to customer support. Once the attachments were opened, executable files began installing malicious software in the background, the report notes.The Trend Micro researchers also noticed that there were different versions of this backdoor, including one that used Dropbox, a cloud-based file and hosting service, to connect to the command-and-control server. The DRBControl hackers also used Dropbox files to store any stolen data as well as information about the devices targeted in the attack, the report finds.

The researchers at Trend Micro note that some of the malicious tools used by DRBControl are the same as those deployed by other advanced persistent threat groups that have been linked to China's government. But they acknowledge that there's not enough evidence to establish a definitive link between these groups.

Read More on BankInfoSecrity

Even More on TrendMicro

Apple drops a bomb on long-life HTTPS certificates: Safari to snub new security certs valid for more than 13 months

Safari will, on September 1st this year, no longer accept new HTTPS certificates that expire more than 13 months from their creation date. That means websites using long-life SSL/TLS certs issued after the cut-off point will throw up privacy errors in Apple's browser. Older certs, issued prior to the deadline, are unaffected by this rule.

By implementing the policy in Safari, Apple will, by extension, enforce it on all iOS and macOS devices. This will put pressure on website admins and developers to make sure their certs meet Apple's requirements – or risk breaking pages on a billion-plus devices and computers. The aim of the move is to improve website security by making sure devs use certs with the latest cryptographic standards, and to reduce the number of old, neglected certificates that could potentially be stolen and re-used for phishing and drive-by malware attacks. If boffins or miscreants are able to break the cryptography in a SSL/TLS standard, short-lived certificates will ensure people migrate to more secure certs within roughly a year.

Companies need to look to automation to assist with certificate deployment, renewal, and lifecycle management to reduce human overhead and the risk of error as the frequency of certificate replacement increase. Let's Encrypt issues free HTTPS certificates that expire after 90 days, and provides tools to automate renewals.

Read More on TheRegister

More #News

- Ring makes 2FA mandatory to keep hackers out of your doorbell account
- Credit Card Skimmer Found on Nine Sites, Researchers Ignored
- New Actors Attack Industrial Control Systems, Old Ones Mature

- WhatsApp Phishing URLs Skyrocket With Over 13,000% Surge
- Microsoft Defender ATP for Linux Now In Public Preview
- Tesla Pays $10K for Microsoft SQL Server Reporting Services Bug
- Hackers Were Inside Citrix for Five Months
- Canadian Government Breaches Exposed Citizens' Data
- Encoding Stolen Credit Card Data on Barcodes
- US Govt Warns of Ransomware Attacks on Pipeline Operations
- Microsoft has a subdomain hijacking problem
- Pay Up, Or We'll Make Google Ban Your Ads
- Israeli soldiers tricked into installing malware by Hamas agents posing as women
- IRS Urges Taxpayers to Enable Multi-Factor Authentication
- Unpatched VPN Servers Hit by Apparent Iranian APT Groups
- These Guys Figured Out a Way to Get Endless Free McDonald's
- Windows, Linux Devices at Risk Due to Unsigned Peripheral Firmware
- Nedbank says 1.7 million customers impacted by breach at third-party provider
- DNSSEC Keysigning Ceremony Postponed Because of Locked Safe
- Malware and HTTPS – a growing love affair
- Suspect who refused to decrypt hard drives released after four years
- Details of 10.6 million MGM hotel guests posted on a hacking forum

#Patch Time!

- Adobe releases out-of-band patch for critical code execution vulnerabilities
- Serious Vulnerabilities Expose SonicWall SMA Appliances to Remote Attacks
- Over 400 ICS Vulnerabilities Disclosed in 2019
- Over 20,000 WordPress Sites Run Trojanized Premium Themes
- Over 22,000 Vulnerabilities Disclosed in 2019

#Tech and #Tools

- Exploiting Jira for Host Discovery
- Bypass Windows 10 User Group Policy (and more) with this One Weird Trick
- OpenSSH now supports FIDO U2F security keys for 2-factor authentication
- Logging Made Easy Through Graylog Part 1
- Modern Routing For Red Team Infrastructure - using Traefik, Metasploit, Covenant and Docker
- GadgetProbe: Probe endpoints consuming Java serialized objects
- Top 10 web hacking techniques of 2019
- VirusTotal API script
- Content Security Policy (CSP) Bypasses
- Shodan Pentesting Guide
- CLAMBLING - A New Backdoor Base On Dropbox
- ViperSoftX - New JavaScript Threat
- IIS Raid – Backdooring IIS Using Native Modules
- Testing your RedTeam Infrastructure
- Privilege escalation and post exploitation tactics in GCP environments

Kindred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us