


INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS [Subscribe](#) | [2019 CISO Forum, Presented by Intel](#) | [ICS Cyber Security Conference](#) | [Contact](#)

[Malware & Threats](#)
[Cybercrime](#)
[Mobile & Wireless](#)
[Risk & Compliance](#)
[Security Architecture](#)
[Security Strategy](#)
[SCADA / ICS](#)
[IoT Security](#)

Home » Cybercrime



## RANCOR Cyber Espionage Group Uncovered

By Ionut Arghire on June 26, 2018

[Share](#)
[Tweet](#)
[Recommend 0](#)
[RSS](#)

A cyber espionage group that has remained undetected until recently, has been targeting South East Asia with two previously unknown malware families, according to Palo Alto Networks.

The group, referred to as RANCOR, has been targeting political entities in Singapore, Cambodia, and Thailand, but might have hit targets in other countries as well. The group mainly uses two malware families, DDKONG and PLAINTREE, the latter apparently being a new addition to its arsenal.

According to Palo Alto Networks researchers, the attacks likely begin with spear phishing emails and use decoy documents containing details taken from public news articles on political news and events. These documents are hosted on legitimate websites, including a website belonging to the Cambodia Government, and Facebook.

The newly discovered campaign appears related to [the KHRAT Trojan](#), a backdoor associated with the China-linked cyber espionage group known as [DragonOK](#).

One of the IPs the KHRAT associated domains started resolving to in February 2018 led the researchers to websites mimicking popular technology companies, including one named [facebook-apps\[.\]com](#). The researchers connected two malware samples to the domain, namely a loader and PLAINTREE.

Only six samples of the malware were found, and the researchers managed [to link](#) them to two infrastructure clusters that do not appear to overlap. Both clusters, however, were involved in attacks targeting organizations in South East Asia, and the malware was observed using the same file paths in each cluster.

At least one of the attacks used a Microsoft Office Excel document with an embedded macro to launch the payload. The main malicious code was embedded in an EXIF metadata property of the document. In another attack, an HTML Application file (.hta) was used, while other attacks used DLL loaders.

One of the DLLs downloaded a decoy from a government website that was previously used in a KHRAT attack and two DLLs (out of three) were found hosted on this same compromised website (the domain was likely hacked again in early 2018).

First observed in February 2017, the DDKONG malware might be used by multiple threat actors.

First observed in October 2017, PLAINTREE appears to be exclusively used by the RANCOR attackers. The malware uses a custom UDP protocol for its network communications, can add persistence on the victim machine, ensures only a single instance is running, and then starts collecting general system information.

The malware also beacons to the command and control (C&C) server and attempts to decode a configuration blob. After the server responds, the malware spawns several new threads to load and execute a new plugin that is to be received from the C&C in the form of a DLL with an export function of either 'shell' or 'file'.


The researchers believe the attackers were sending commands to the malware manually, due to a long period of delay between these commands (automated commands are performed quicker).

"The RANCOR campaign represents a continued trend of targeted attacks against entities within the South East Asia region. In a number of instances, politically motivated lures were used to entice victims into opening and subsequently loading previously undocumented malware families. These families made use of custom network communication to load and execute various plugins hosted by the attackers," Palo Alto Networks concludes.

**Related:** [China-linked KHRAT Operators Adopt New Delivery Techniques](#)

**Related:** [Hackers Linked to Luminosity RAT Targeted by Law Enforcement](#)

[Share](#)
[Tweet](#)
[Recommend 0](#)
[RSS](#)



Ionut Arghire is an international correspondent for SecurityWeek.

**Previous Columns by Ionut Arghire:**

- » [Tech Companies Partner to Securely Connect IoT to Cloud](#)
- » [Two Dozen Arrested for Laundering Funds From BEC, Other Scams](#)
- » [Rare Android Stalkerware Can Steal Data, Control Devices](#)
- » [Organizations Slow to Patch Targeted Microsoft Exchange Vulnerability](#)
- » [ProtonMail, ProtonVPN Will Use Alternative Routing to Bypass Censorship](#)

» [2020 ICS Cyber Security Conference | USA \[Oct. 19-22\]](#)

» [2020 Singapore ICS Cyber Security Conference | June 16-18 2020](#)





» [2019 CISO Forum, Presented by Intel \(Ritz-Carlton, Half Moon Bay CA\)](#)

**Tags:** [NEWS & INDUSTRY](#) [Cybercrime](#)


**SUBSCRIBE TO THE DAILY BRIEFING**

**BRIEFING**

Business Email Address

Most Recent	Most Read
» <a href="#">The Other Virus Threat: Surge in COVID-Themed Cyberattacks</a>	
» <a href="#">Sarr: FBI Probing If Foreign Gov't Behind HHS Cyber Incident</a>	
» <a href="#">Trend Micro Patches Two Vulnerabilities Exploited in the Wild</a>	
» <a href="#">Financial Services Firms Exposed 500,000 Sensitive Documents</a>	
» <a href="#">Tech Companies Partner to Securely Connect IoT to Cloud</a>	
» <a href="#">Private Application Access Firm Axis Security Emerges From Stealth</a>	
» <a href="#">Two Dozen Arrested for Laundering Funds From BEC, Other Scams</a>	
» <a href="#">Users Complain About Windows Update That Patches SMBGhost Vulnerability</a>	
» <a href="#">Senate Votes to Renew Surveillance Powers, Delaying Changes</a>	
» <a href="#">Rare Android Stalkerware Can Steal Data, Control Devices</a>	



June 16-18, 2020

<p><b>Popular Topics</b></p> <ul style="list-style-type: none"> <li>» Information Security News</li> <li>» IT Security News</li> <li>» Risk Management</li> <li>» Cybercrime</li> <li>» Cloud Security</li> <li>» Application Security</li> <li>» Smart Device Security</li> </ul>	<p><b>Security Community</b></p> <ul style="list-style-type: none"> <li>» IT Security Newsletters</li> <li>» ICS Cyber Security Conference</li> <li>» CISO Forum, Presented by Intel</li> <li>» InfosecIsland.Com</li> </ul>	<p><b>Stay Intouch</b></p> <ul style="list-style-type: none"> <li>» Twitter</li> <li>» Facebook</li> <li>» LinkedIn Group</li> <li>» Cyber Weapon Discussion Group</li> <li>» RSS Feed</li> <li>» Submit Tip</li> <li>» Security Intelligence Group</li> </ul>	<p><b>About SecurityWeek</b></p> <ul style="list-style-type: none"> <li>» Team</li> <li>» Advertising</li> <li>» Events</li> <li>» Writing Opportunities</li> <li>» Feedback</li> <li>» Contact Us</li> </ul>
--	--	--	---

Wired Business Media

Copyright © 2020 Wired Business Media. All Rights Reserved. [Privacy Policy](#)