Endpoint Protection

community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument

Back to Library

Android RATs Branch out with Dendroid

1 Recommend

Mar 05, 2014 09:24 AM



Migration User

Darwinism is partly based on the ability for change that increases an individual's ability to compete and survive. Malware authors are not much different and need to adapt to survive in changing technological landscapes and marketplaces. In a previous <u>blog</u>, we highlighted a free Android remote administration tool (RAT) known as AndroRAT (<u>Android.Dandro</u>) and what was believed to be the first ever malware APK binder. Since then, we have seen imitations and evolutions of such threats in the threat landscape. One such threat that is making waves in underground forums is called Dendroid (<u>Android.Dendoroid</u>), which is also a word meaning something is tree-like or has a branching structure.



Figure 1. Dendroid advertisement banner

Dendroid is a HTTP RAT that is marketed as being transparent to the user and firmware interface, having a sophisticated PHP panel, and an application APK binder package. The APK binder used by Dendroid just so happens to share some links to the author of the original AndroRAT APK binder.

	up	Status	Last Updated	Cell Info	Location	Device	SDK	Version	Add	Selected: 1 Dese	Aust All Select
22	2	Online	2013-09-18 12:11:09			Nexus4	18	1		Ringer Up	Ringer Do
21		Offine	2013-09-14 18:10:54		1000	sdk	17	1	• •	Madia Up	Modia Do
										Sureen On	
										Intercept On	Intercept
										Block SMS On	Block SMS
										Time in MS	Record Au
										Time in MS	Record Vid
										Take Photo	Front
										Take Photo Record Calls On	Frank Record Cal
										Record Calls On	
His	story Of: All Bots	All Doris 🖌 A	uto Scrolt: On View Awa	iling Commands	UID	File			Options	Record Calls On	Record Cal
100	2010,00,10,10	08.95] -		alling Commands	UID		3_09_18	.12,04.jog	_	Record Calls On	Record Cal
Up	2013, 38, 18, 73 Piceding: Monapelemulated OrSyste (2013, 38, 48, 42 Piceding: Monapelemulated OrSyste	08.55) - n/Pctures/2913, 08.95) - n/Petures/2013,	18.10.12.03.pg	elling Commands	UID	201		.12,04.jpg	•	Record Calls On	Record Cal
Up Up	para, as, 16, 10 piceding, hitomps (emulated 0/5yste (2910, 08, 16, 10	06.55) - niPctures/2013, 06.953 - niP6tures/2013, 06.96] - niP6tures/2013,	08, 18, 12, 03, jpg 38, 18, 12, 23, jpg Conplete	eling Commands	UID	201	3_09_18		_	Record Calls On Uption	Record Cal

Figure 2. Dendroid control panel

According to postings on underground forums, the official seller of Dendroid is known as "Soccer." The seller markets Dendroid as offering many features that have never been seen before and comes with 24/7 support, all for a once off payment of \$300 to be paid through BTC, LTC, BTC-e, or other services. Some of the many features on offer include the following:

- Delete call logs
- Call a phone number
- Open Web pages
- Record calls and audio
- Intercept text messages
- Take and upload photos and videos
- Open an application
- Initiate a HTTP flood (DoS) for a period of time
- Change the command-and-control (C&C) server

Арк	Binder	_ ×
Binding APK Search Downloads		
SEARCH	Title	
Search	FileSize: Version:	
Results: Found 683 Applications!	Downloads:	
	Description	
	Screenshots	
Displaying Results 0-30 Of 683 NEXT 30>>	Download	

Figure 3. Dendroid APK binder

As previously mentioned, according to reports on underground forums, the author of the Dendroid APK binder included with this package had assistance writing this APK binder from the author of the original AndroRAT APK binder.

The evolution of remote access tools on the Android platform was inevitable. The creation of Dendroid and the positive feedback on underground forums for this type of threat shows that there is a strong cybercriminal marketplace for such tools. On the PC platform, other crimeware toolkits like Zeus (<u>Trojan.Zbot</u>) and SpyEye (<u>Trojan.Spyeye</u>) started off in a similar manner and grew quickly in popularity due to their ease of use and notoriety stemming from the high profile crimes perpetrated as a result of their usage. While this may be early days for Dendroid, Symantec will be keeping a close eye on this threat.

To stay protected, Symantec recommends installing a security app, such as <u>Norton Mobile</u> <u>Security</u>, which detects this threat as <u>Android.Dendoroid</u>. For general safety tips for smartphones and tablets, please visit our <u>Mobile Security</u> website.

Statistics

0 Favorited

0 Views

0 Files

0 Shares

0 Downloads

Tags and Keywords

Related Entries and Links

No Related Resource entered.