Featured Articles 11.06.15

RATs Targeting Android – Crime, Surveillance, or Something Else?

BY EMILIO IASIELLO (http://darkmatters.norsecorp.com/author/eiasiello/)

()

Recent reporting (http://news.softpedia.com/news/iran-interested-in-rats-remote-access-trojans-targeting-android-devices-495471.shtml) indicates that Iranian hackers have demonstrated interest in remote access Trojans (RATs) designed to exploit Android mobile devices. A threat researcher (http://www.theregister.co.uk/2015/10/29/iranian_hackers_android/) monitoring prominent Iranian hacker boards noted that many of the discussions focused on those RATs that targeted Android operating systems. The two RATs cited – AndroRAT and DroidJack – drew comparisons to njRAT due to its availability for download/purchase, ease of use, and strong community response, according to the researcher. Both Trojans can be integrated into legitimate-looking mobile applications in order to entice users into installing them onto their phones.

Middle East

While there is intimation that the high penetration rate of Android devices in the Middle East may be the catalyst for this increased interest, Android dominated the smartphone market at 82.8 percent, according to 2015 2Q findings (http://www.idc.com/prodserv/smartphone-os-market-share.jsp) from International Data Corporation, the premier global provider of market intelligence. According to vendor statistics (https://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/), nearly 85% of the mobile device market was occupied by Android in Q2 2014. Given Android's undisputed leadership among mobile environments, coupled with easy to use malware readily available, such developments shouldn't come as a surprise.

Exploitation

The targeting of mobile phones has been liberally attributed to cybercriminals seeking to exploit user weakness as well as the notorious security reputation (http://www.stuff.co.nz/technology/gadgets/73031845/90-of-Android-phones-are-not-secure) of Android. However, given that mobile RATs, like their counterparts, gives an attacker complete control over the victimized device. Among the advanced spying features (http://news.softpedia.com/news/iran-interested-in-rats-remote-access-trojans-targeting-android-devices-495471.shtml) associated with the two Android RATs are the power to intercept SMS messages, view call logs, access contact lists, browser history, and even take control of the phone's microphone and camera.

Censorship and surveillance

The purposes of such a capability extend well beyond the criminal enterprise and can be used for law enforcement, intelligence surveillance, and collection capabilities. According to a 2014 Freedom House (https://freedomhouse.org/sites/default/files/Freedom%20in%20the%20World%202014%20Booklet.pdf) survey, globally, governments are increasing censorship and surveillance of the Internet, as overall online freedom declined for the fifth consecutive year. Notably, many of these governments are based in the Middle East, with Iran and Syria being highlighted as among the governments administering the most severe restrictions. Certainly, the use of such RATs in a region registering among the worst civil liberty scores is highly desirable when the Android penetration rate for the region is around 40 percent, according to one survey (https://www.infinitemonkeys.mobi/blog/smartphone-usage-in-the-middle-east-statistics-and-trends-infographic/).

But there's evidence to suggest that such RATs may not just be used with monitoring dissidents or groups that pose an ideological challenge to existing regimes. After the mysterious death (http://www.bbc.com/news/magazine-32887939) of Alberto Nisman, an Argentinian prosecutor

whose investigations into a 1994 bombing of a Jewish community center in Buenos Aires had reputedly collusion between the then-Argentine government and Iran, AlienSpy RAT malware (https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/)was found both on his phone and the phone of an investigative journalist covering the same story. The targeting of both individuals, coupled with the lack of any noticeable increased rate of mobile RAT malware targeting Argentinian public, bolsters suspicions that the deployed malware was used for surveillance, as opposed to committing financial crimes.

Threat landscape

As people increasingly rely on mobile technology for all of their computing needs, it makes such devices key targets for the diverse cyber threat actor landscape seeking entrance into the personal and financial lives of their targets. RATs are the tools of choice for novices, criminals, and espionage groups because they provide the necessary means with which to gain access, control, and maintain presence on these valuable assets. The fact that Iranian hackers are discussing specific RATs should not mislead assumptions that these tools may only be employed regionally; it should serve as notice that we can expect more activity directed against all portable devices. The playing field isn't reduced simply because the screen is smaller.

YOU MIGHT ALSO LIKE

THE UPSIDE OF ACCIDENTALLY HIRING A HACKER
(HTTP://DARKMATTERS.NORSECORP.COM/2014/09/26/THE-UPSIDE-OF-ACCIDENTALLY-HIRING-A-HACKER/)

REVEALING THE AWESOME TRUTH ABOUT HACKERS
(HTTP://DARKMATTERS.NORSECORP.COM/2014/09/18/REVEALING-THE-AWESOME-TRUTH-ABOUT-HACKERS/)

DARKWATCH UNCOVERS THOUSANDS OF PREVIOUSLY UNKNOWN THREATS (HTTP://DARKMATTERS.NORSECORP.COM/2014/07/31/DARKWATCH-UNCOVERS-THOUSANDS-OF-PREVIOUSLY-UNKNOWN-THREATS/)

THE NEW REALITY IN SECURITY: OFFENSE ALWAYS WINS AND DEFENSE ALWAYS LOSES (HTTP://DARKMATTERS.NORSECORP.COM/2014/11/10/THE-NEW-REALITY-IN-SECURITY-OFFENSE-ALWAYS-WINS-AND-DEFENSE-ALWAYS-LOSES/)

Emilio Iasiello

Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as a private sector company providing cyber intelligence to Fortune 100 clients. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in peer-reviewed journals.

▶ MORE POSTS (23) (http://darkmatters.norsecorp.com/author/eiasiello/)

TOPICS: ANDRORAT, CENSORSHIP, CYBERCRIMINALS, DROIDJACK, HACKER, HACKERS, INTELLIGENCE SURVEILLANCE, IRAN, IRANIAN HACKERS, LAW ENFORCEMENT, MARKET INTELLIGENCE, MIDDLE EAST, MOBILE, NJRAT, RATS, SURVEILLANCE, SYRIA, THREAT ACTOR, TROJANS,