Android Backdoor GhostCtrl Records Your Audio, Video

blog.trendmicro.com/trendlabs-security-intelligence/android-backdoor-ghostctrl-can-silently-record-your-audio-video-and-more/

July 17, 2017

Updated as of August 6, 2017, 7:45 PM PDT to clarify GhostCtrl's attack vectors.

The information-stealing RETADUP worm that affected Israeli hospitals is actually just part of an attack that turned out to be bigger than we first thought—at least in terms of impact. It was accompanied by an even more dangerous threat: an Android malware that can take over the device.

Detected by Trend Micro as ANDROIDOS_GHOSTCTRL.OPS / ANDROIDOS_GHOSTCTRL.OPSA, we've named this Android backdoor GhostCtrl as it can stealthily control many of the infected device's functionalities.

GhostCtrl was hosted in RETADUP's C&C infrastructure, and the samples we analyzed masqueraded as a legitimate or popular app that uses the names App, MMS, whatsapp, and even Pokemon GO. Socially engineered phishing emails were also attack vectors; they had malicious URLs that led would-be victims to download these apps.

There are three versions of GhostCtrl. The first stole information and controlled some of the device's functionalities without obfuscation, while the second added more device features to hijack. The third iteration combines the best of the earlier versions' features—and then some. Based on the techniques each employed, we can only expect it to further evolve.

GhostCtrl is literally a ghost of itself

GhostCtrl is also actually a variant (or at least based on) of the commercially sold, multiplatform OmniRAT that made headlines in November 2015. It touts that it can remotely take control of Windows, Linux, and Mac systems at the touch of an Android device's button—and vice versa. A lifetime license for an OmniRAT package costs between US $25 and $75. Predictably OmniRAT cracking tutorials abound in various underground forums, and some its members even provide patchers for it.

There's actually a red flag that shows how the malicious APK is an OmniRAT spinoff. Given that it's a RAT as a service, this can be modified (or removed) during compilation.

Figure 1: Snapshot of GhostCtrl version 3's resources.arsc file indicating it's an OmniRAT variant (highlighted)

GhostCtrl is hauntingly persistent

When the app is launched, it base64-decodes a string from the resource file and writes it down, which is actually the malicious Android Application Package (APK).

The malicious APK, after dynamically clicked by a wrapper APK, will ask the user to install it. Avoiding it is very tricky: even if the user cancels the "ask for install page" prompt, the message will still pop up immediately. The malicious APK doesn't have an icon. Once installed, a wrapper APK will launch a service that would let the main, malicious APK run in the background:

Figure 2: How the wrapper APK leads to the main APK

The main APK has backdoor functions usually named *com.android.engine* to mislead the user into thinking it's a legitimate system application. The malicious APK will then connect to the C&C server to retrieve commands via the socket (an endpoint for communication between machines), *new Socket("hef--klife[.]ddns.net", 3176).*

GhostCtrl can possess the infected device to do its bidding

The commands from the C&C server are encrypted and locally decrypted by the APK upon receipt. Interestingly, we also found that the backdoor connects to a domain rather than directly connecting to the C&C server's IP address. This can be an attempt to obscure their traffic. We also found several Dynamic Name Servers (DNS), which at some point led to the same C&C IP address:

- hef--klife[.]ddns[.]net
- f--klife[.]ddns[.]net

- php[.]no-ip[.]biz
- ayalove[.]no-ip[.]biz

A notable command contains action code and Object DATA, which enables attackers to specify the target and content, making this a very flexible malware for cybercriminals. This is the command that allows attackers to manipulate the device's functionalities without the owner's consent or knowledge.

Here's a list of some of the action codes and what each does to the device:

- ACTION CODE =10, 11: Control the Wi-Fi state
- ACTION CODE= 34: Monitor the phone sensors' data in real time
- ACTION CODE= 37: Set phone's UiMode, like night mode/car mode
- ACTION CODE= 41: Control the vibrate function, including the pattern and when it will vibrate
- ACTION CODE= 46: Download pictures as wallpaper
- ACTION CODE= 48: List the file information in the current directory and upload it to the C&C server
- ACTION CODE= 49: Delete a file in the indicated directory
- ACTION CODE= 50: Rename a file in the indicated directory
- ACTION CODE= 51: Upload a desired file to the C&C server
- ACTION CODE= 52: Create an indicated directory
- ACTION CODE= 60: Use the text to speech feature (translate text to voice/audio)
- ACTION CODE= 62: Send SMS/MMS to a number specified by the attacker; the content can also be customized
- ACTION CODE= 68: Delete browser history
- ACTION CODE= 70: Delete SMS
- ACTION CODE= 74: Download file
- ACTION CODE= 75: Call a phone number indicated by the attacker
- ACTION CODE= 77: Open activity view-related apps; the Uniform Resource Identifier (URI) can also be specified by the attacker (open browser, map, dial view, etc.)
- ACTION CODE= 78: Control the system infrared transmitter
- ACTION CODE= 79: Run a shell command specified by the attacker and upload the output result

Another unique C&C command is an integer-type command, which is responsible for stealing the device's data. Different kinds of sensitive—and to cybercriminals, valuable—information will be collected and uploaded, including call logs, SMS records, contacts, phone numbers, SIM serial number, location, and browser bookmarks.

The data GhostCtrl steals is extensive, compared to other Android info-stealers. Besides the aforementioned information types, GhostCtrl can also pilfer information like Android OS version, username, Wi-Fi, battery, Bluetooth, and audio states, UiMode, sensor, data from camera, browser, and searches, service processes, activity information, and wallpaper.

It can also intercept text messages from phone numbers specified by the attacker. Its most daunting capability is how it can surreptitiously record voice or audio, then upload it to the C&C server at a certain time. All the stolen content will be encrypted before they're uploaded to the C&C server.

Figure 3: Code snapshot showing how some information will be deleted after upload

Figure 4: Most of the related function codes for stealing information are in the "transfer" package.

The other C&C commands are self-defined, such as "account", "audioManager", and "clipboard". These commands will trigger malicious routines. It's worth noting that these aren't commonly seen in Android RATs:

- Clearing/resetting the password of an account specified by the attacker
- Getting the phone to play different sound effects
- Specify the content in the Clipboard
- Customize the notification and shortcut link, including the style and content
- Control the Bluetooth to search and connect to another device
- Set the accessibility to TRUE and terminate an ongoing phone call

How do GhostCtrl's versions stack up to each other?

GhostCtrl's first version has a framework that enables it to gain admin-level privilege. While it had no function codes at the time, the second version did. The features to be hijacked also incrementally increased as the malware evolved into its second and third iterations.

Figure 5: Framework of GhostCtrl's first version for gaining admin-level privilege

Figure 6: Comparison of backdoor function of the first (left) and second (right) versions

Figure 7: Code snapshot of GhostCtrl's second version applying device admin privileges

GhostCtrl's second version can also be a mobile ransomware. It can lock the device's screen and reset its password, and also root the infected device. It can also hijack the camera, create a scheduled task of taking pictures or recording video, then surreptitiously upload them to the C&C server as mp4 files.

Figure 8: Code snapshot showing GhostCtrl's ransomware-like capability

Figure 9: Code snapshot showing how GhostCtrl roots the infected device

The third version of GhostCtrl incorporates obfuscation techniques to hide its malicious routines, as shown below:

Figure 10: The attack chain of GhostCtrl's third version

In GhostCtrl's third version, the wrapper APK first drops a packed APK. The latter unpacks the main APK, a Dalvik executable (DEX), and an Executable and Linkable Format file (ELF). The DEX and ELF files decrypt strings and Application Programming Interface (API) calls in the main malicious APK in runtime. This longwinded attack chain helps make detection more challenging, exacerbated by the fact that the wrapper APK hides the packed APK as well as DEX and ELF files in the assets directory.

Mitigation

GhostCtrl's combination with an information-stealing worm, while potent, is also telling. The attackers tried to cover their bases, and made sure that they didn't just infect endpoints. And with the ubiquity of mobile devices among corporate and everyday end users, GhostCtrl's capabilities can indeed deliver the scares.

But more than its impact, GhostCtrl underscores the importance of defense in depth. Multilayered security mechanisms should be deployed so that the risks to data are better managed. Some of the best practices that information security professionals and IT/system administrators can adopt to secure bring-your-own devices (BYOD) include:

- Keep the device updated; Android patching is fragmented and organizations may have custom requirements or configurations needed to keep the device updated, so enterprises need to balance productivity and security
- Apply the principle of least privilege—restrict user permissions for BYOD devices to prevent unauthorized access and installation of dubious apps
- Implement an app reputation system that can detect and block malicious and suspicious apps
- Deploy firewalls, intrusion detection, and prevention systems at both the endpoint and mobile device levels to preempt the malware's malicious network activities
- Enforce and strengthen your mobile device management policies to further reduce potential security risks
- Employ encryption, network segmentation and data segregation to limit further exposure or damage to data
- Regularly back up data in case of device loss, theft, or malicious encryption

Trend Micro Solutions

End users and enterprises can also benefit from multilayered mobile security solutions such as Trend Micro™ Mobile Security for Android™ which is also available on Google Play.

Trend Micro™ Mobile Security for Enterprise provides device, compliance and application management, data protection, and configuration provisioning, as well as protects devices from attacks that leverage vulnerabilities, preventing unauthorized access to apps, as well as detecting and blocking malware and fraudulent websites.

A list of all the hashes (SHA-256) detected as ANDROIDOS_GHOSTCTRL.OPS/ANDROIDOS_GHOSTCTRL.OPSA is in this **appendix**.