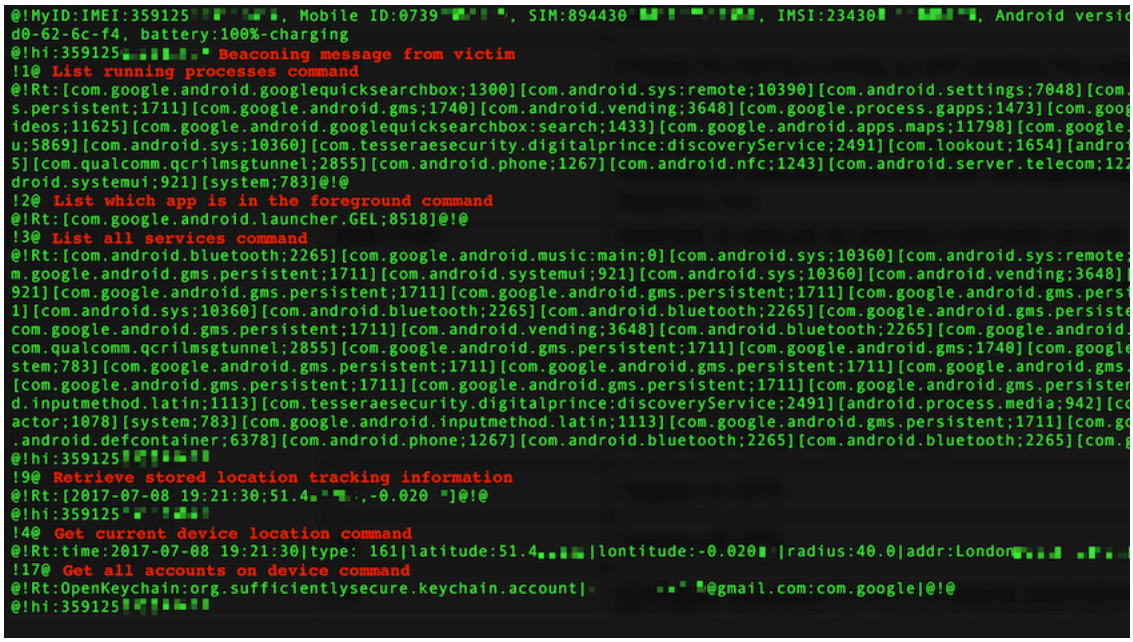
JadeRAT mobile surveillanceware spikes in espionage activity

blog.lookout.com/mobile-threat-jaderat



Lookout researchers are monitoring the evolution of an Android surveillanceware family known as JadeRAT, we believe may be connected to a government sponsored APT group.

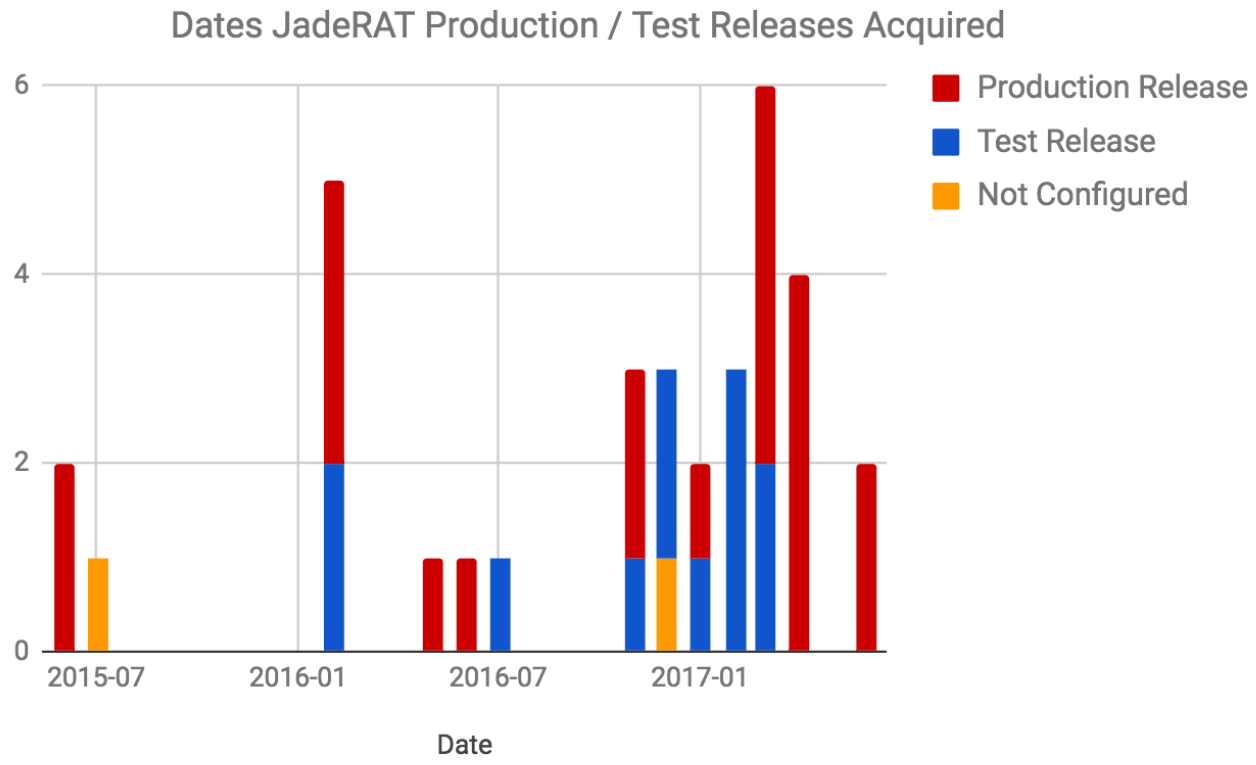
Emerging in 2015 and becoming increasingly active, JadeRAT provides its operators with a significant degree of control over a compromised device and supports over 60 commands that are focused on retrieving sensitive information and profiling victims.
All Lookout customers are protected from this threat.

JadeRAT is just one example of numerous mobile surveillanceware families we've seen in recent months, indicating that actors are continuing to incorporate mobile tools in their attack chains. Some of these active families have included FrozenCell, an attack against government officials in Palestine; xRAT, associated with a family targeting Hong Kong protestors; and ViperRAT, an attack targeting members of the Israeli Defense Force. Research into those families suggests they are highly targeted however we've also seen more wide-reaching spyware such as SonicSpy that was discovered in thousands of malicious apps, some of which made their way into the Google Play Store.

Potential attribution

Based on the apps we've seen JadeRAT trojanize, it appears the actors behind it are primarily targeting groups and individuals in China. While our analysis has identified several possible leads that could tie this surveillanceware family to the Naikon APT, Scarlet Mimic, or one of several other groups operating in the region, at this point in time we do not have conclusive evidence to confirm this. Our findings do support the theory that the actor behind JadeRAT is operating around a similar set of objectives to those followed by other Chinese government sponsored groups. We're hoping that by sharing this information it will increase awareness about the rise in targeted surveillance attacks against mobile devices and provide further leads to the research community investigating actors operating in this region.

JadeRAT samples

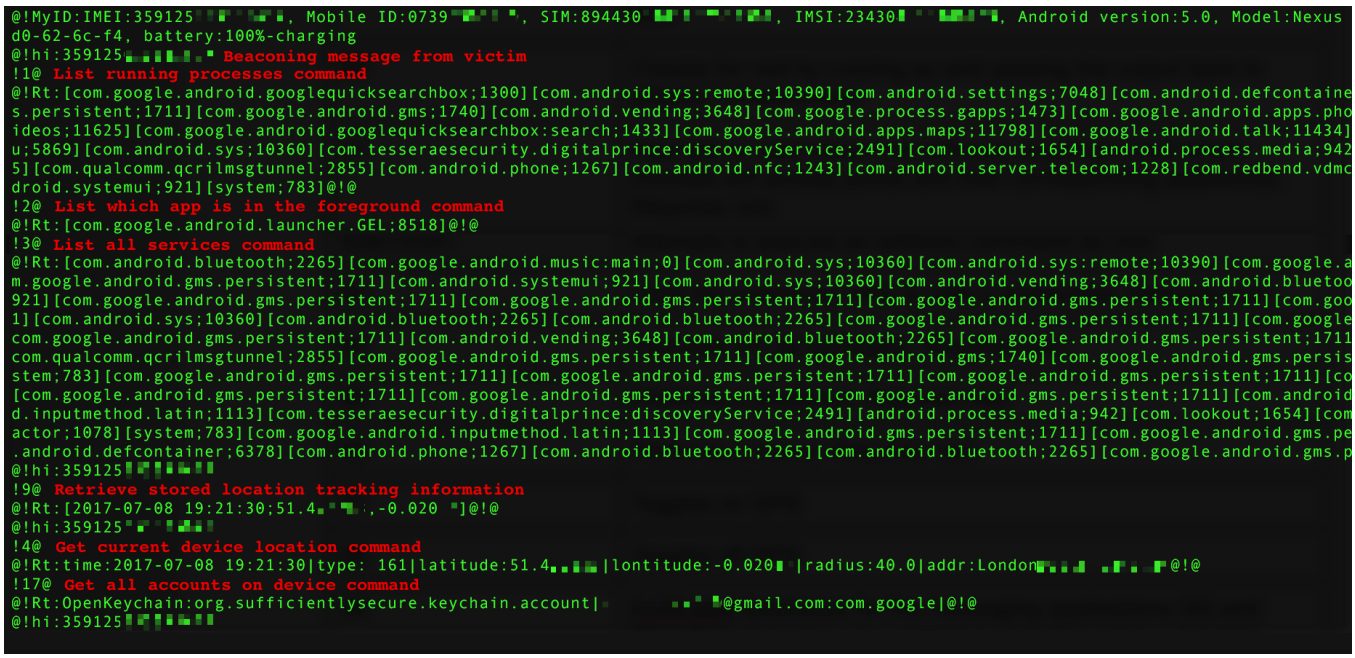


There is a strong indication that the actor behind this family is becoming increasingly active in the mobile space. As of June 2017, we have acquired 34 JadeRAT samples, 50 percent of which were acquired just this year. Looking at hard coded configuration details, we were able to determine which samples are likely production releases and which are used for internal testing. This shows that the majority of production samples were released this year.

JadeRAT sample names have remained fairly consistent. The apps SIM卡管理 (SIM Card Management), 手机管家 (Phone Guardian), and Google Searcher are the most popular observed titles. Others have included Uyghur, 170602, Telegram, and Voxer, indicating the actor is impersonating communication apps and may be running some campaigns targeting ethnic minorities in China, given the Uyghur reference.

JadeRAT supports over 60 commands that can be issued in the format !<command_id>&<optional_cmd_params>@. Many of these offer standard information gathering functionality seen in typical mobile surveillanceware, however JadeRAT supports several less common capabilities. These include notifying an operator via SMS when a device has booted and silently dropping calls and texts to attacker specified numbers. The following are JadeRAT's core capabilities:

Get a list of running processesConfigure call recording to occur if a call is made to a specified numberGet the name of the foreground taskAlert a 'secure phone' that a victim's device is now onlineGet active servicesRecord audio at a specific time for a set durationRetrieve device locationStart / stop audio recording / set to record based on calls to certain numbersRetrieve contacts, accounts, call logs, text messagesAttempt to call an attacker specified numberKill a specific processSilently drop calls and SMSes to specific numbersRetrieve location data that has been periodically collectedEnable / disable Wi-FiList the contents of a specific directoryEnable / disable mobile dataDownload / upload / delete a specified file Enable / disable GPSRecursively search a directory on a victim's device for a specific filenameDelete all SMSes, call logs, contacts, and content on the SDCardUse ZipUtils to compress a specific file, placing the compressed output in /sdcard/.tempExecute arbitrary commands if rootExfiltrate MicroMsg and QQ media files and chat databasesTake a screenshotCheck for root accessShutdown / reboot deviceRetrieve Wi-Fi access points and their corresponding passwords



As JadeRAT simply opens up a socket to a specified address and uses quite a basic instruction format without any authentication its capabilities can be tested out by redirecting traffic from a compromised device to an analysis machine running netcat.

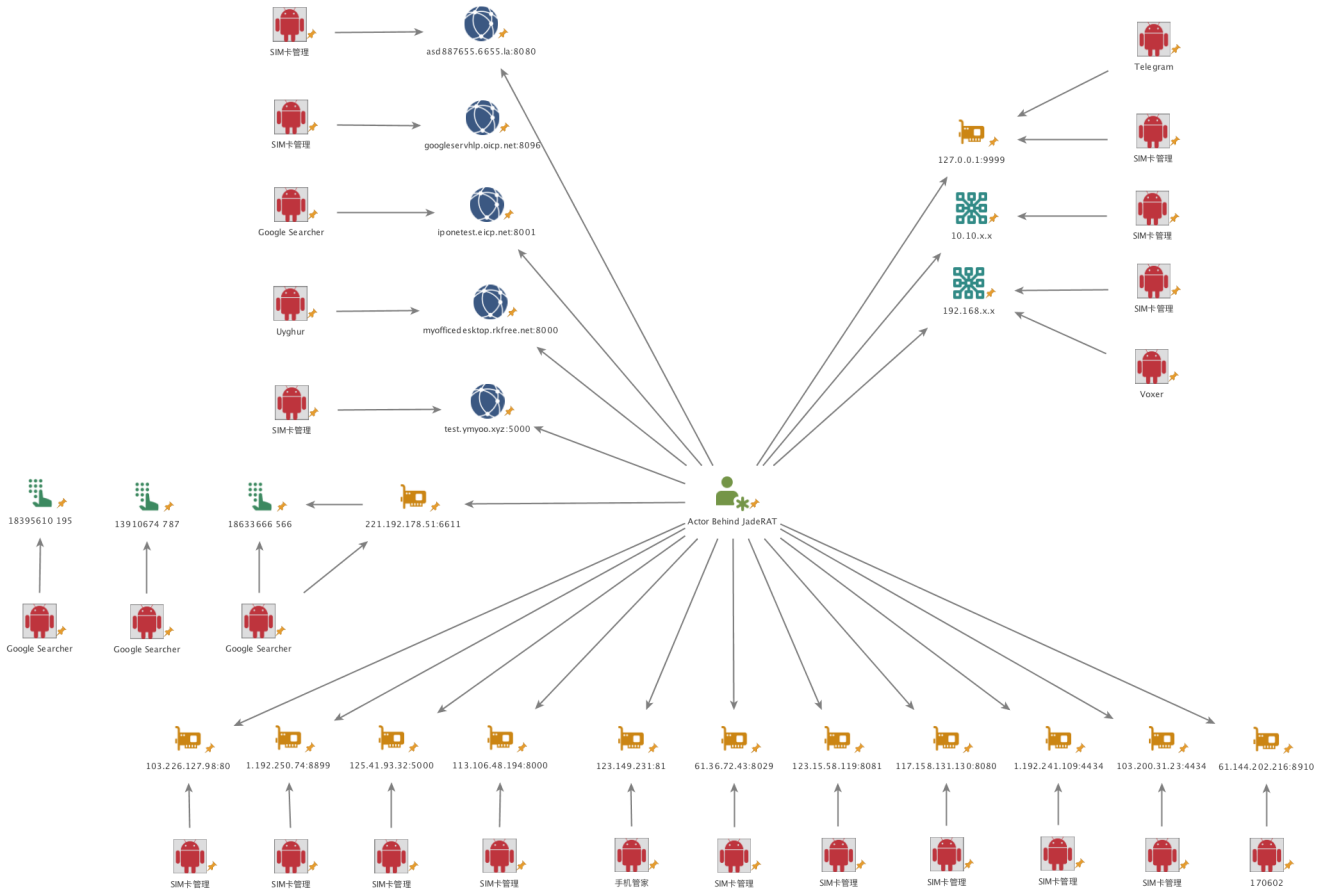
Infrastructure

JadeRAT's operators have consistently changed their infrastructure. Production releases rarely reuse domains or IP addresses, frequently use dynamic DNS, and communicate on various non-standard ports. JadeRAT is configured to send SMS messages to an attacker-specified phone number when the compromised device first comes online, however these have only been pre-configured in three of the most recently observed samples. We extracted the following phone numbers from samples acquired during April of 2017:

NumberRegionOperatorBrand18395610195Shijiazhuang City, Hebei ProvinceChina Mobile Communications CorporationGlobal pass, M-Zone, Shenzhou line, G318633666566Handan City, Hebei ProvinceChina United Network Communications Group Co., LtdUnknown13910674787BeijingChina Mobile Communications CorporationGlobal pass, M-Zone, Shenzhou line, G3

Though these phone numbers are only associated with a limited number of samples, all samples come configured with specific infrastructure to which they communicate. Below are observed domains and external IP addresses.

IP / DomainPortgoogleservhlp.oicp.net8096iponetest.eicp.net8001myofficedesktop.rkfree.net8000asd887655.6655.la8080103.226.127.9880125.41.9



Lookout is continuing to track JadeRAT and its associated infrastructure closely as we anticipate this family will only continue to grow.

Want to learn more about threats like JadeRAT and our Threat Advisory services? Contact Lookout today.

SHA-1sfea0bc1df035ea8eb683bc91cef4d925d8a260f3b86d8dc815f50377e444a297f5f33bba1b16cc8e674224a4fe7ec9badd5eefce303ec0867a4afcdf3

All these indicators have been added to AlienVault under the JadeRAT pulse.

Lookout researchers are monitoring the evolution of an Android surveillanceware family known as JadeRAT, we believe may be connected to a government sponsored APT group.

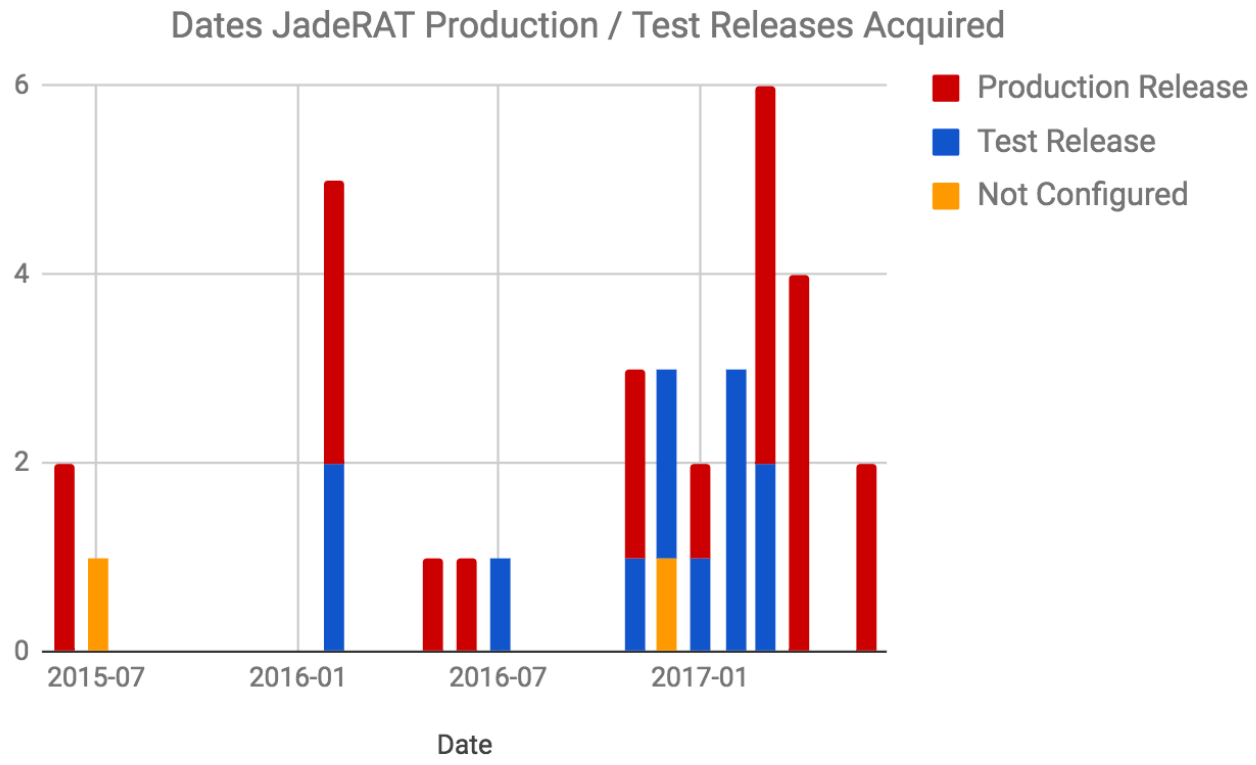
Emerging in 2015 and becoming increasingly active, JadeRAT provides its operators with a significant degree of control over a compromised device and supports over 60 commands that are focused on retrieving sensitive information and profiling victims.
All Lookout customers are protected from this threat.

JadeRAT is just one example of numerous mobile surveillanceware families we've seen in recent months, indicating that actors are continuing to incorporate mobile tools in their attack chains. Some of these active families have included FrozenCell, an attack against government officials in Palestine; xRAT, associated with a family targeting Hong Kong protestors; and ViperRAT, an attack targeting members of the Israeli Defense Force. Research into those families suggests they are highly targeted however we've also seen more wide-reaching spyware such as SonicSpy that was discovered in thousands of malicious apps, some of which made their way into the Google Play Store.

Potential attribution

Based on the apps we've seen JadeRAT trojanize, it appears the actors behind it are primarily targeting groups and individuals in China. While our analysis has identified several possible leads that could tie this surveillanceware family to the Naikon APT, Scarlet Mimic, or one of several other groups operating in the region, at this point in time we do not have conclusive evidence to confirm this. Our findings do support the theory that the actor behind JadeRAT is operating around a similar set of objectives to those followed by other Chinese government sponsored groups. We're hoping that by sharing this information it will increase awareness about the rise in targeted surveillance attacks against mobile devices and provide further leads to the research community investigating actors operating in this region.

JadeRAT samples

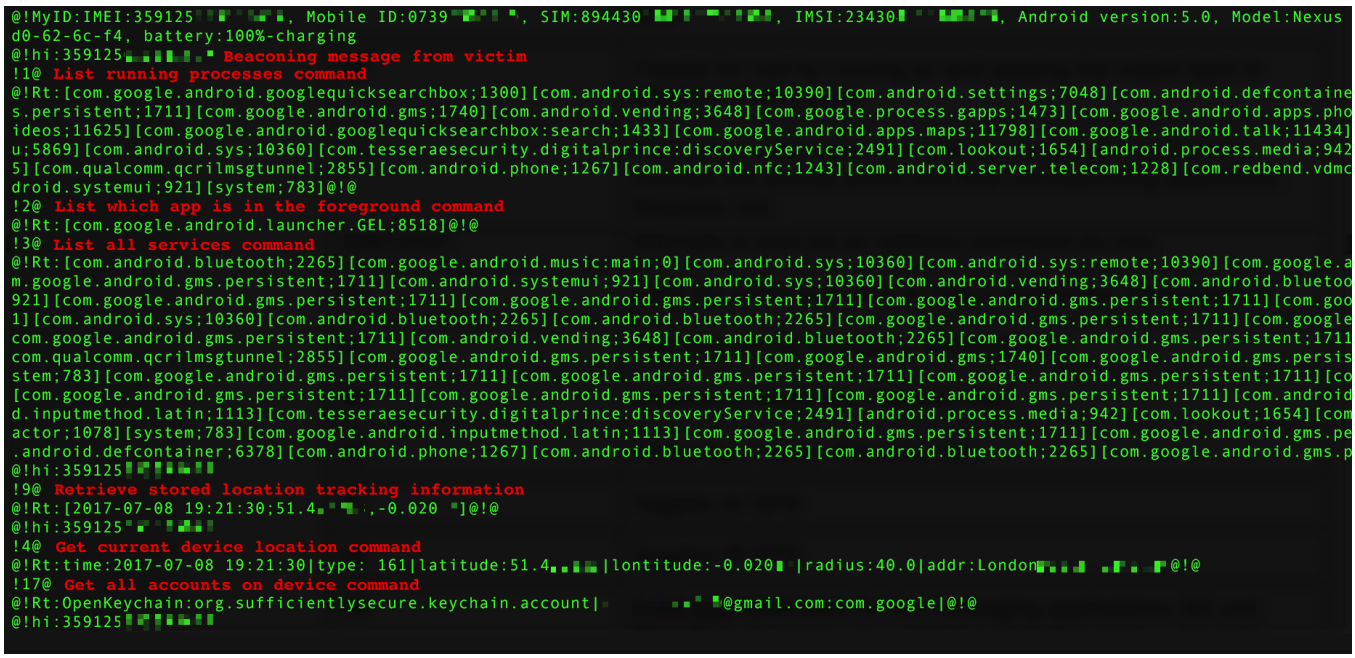


There is a strong indication that the actor behind this family is becoming increasingly active in the mobile space. As of June 2017, we have acquired 34 JadeRAT samples, 50 percent of which were acquired just this year. Looking at hard coded configuration details, we were able to determine which samples are likely production releases and which are used for internal testing. This shows that the majority of production samples were released this year.

JadeRAT sample names have remained fairly consistent. The apps SIM卡管理 (SIM Card Management), 手机管家 (Phone Guardian), and Google Searcher are the most popular observed titles. Others have included Uyghur, 170602, Telegram, and Voxer, indicating the actor is impersonating communication apps and may be running some campaigns targeting ethnic minorities in China, given the Uyghur reference.

JadeRAT supports over 60 commands that can be issued in the format !<command_id>&<optional_cmd_params>@. Many of these offer standard information gathering functionality seen in typical mobile surveillanceware, however JadeRAT supports several less common capabilities. These include notifying an operator via SMS when a device has booted and silently dropping calls and texts to attacker specified numbers. The following are JadeRAT's core capabilities:

Get a list of running processesConfigure call recording to occur if a call is made to a specified numberGet the name of the foreground taskAlert a 'secure phone' that a victim's device is now onlineGet active servicesRecord audio at a specific time for a set durationRetrieve device locationStart / stop audio recording / set to record based on calls to certain numbersRetrieve contacts, accounts, call logs, text messagesAttempt to call an attacker specified numberKill a specific processSilently drop calls and SMSes to specific numbersRetrieve location data that has been periodically collectedEnable / disable Wi-FiList the contents of a specific directoryEnable / disable mobile dataDownload / upload / delete a specified file Enable / disable GPSRecursively search a directory on a victim's device for a specific filenameDelete all SMSes, call logs, contacts, and content on the SDCardUse ZipUtils to compress a specific file, placing the compressed output in /sdcard/.tempExecute arbitrary commands if rootExfiltrate MicroMsg and QQ media files and chat databasesTake a screenshotCheck for root accessShutdown / reboot deviceRetrieve Wi-Fi access points and their corresponding passwords



As JadeRAT simply opens up a socket to a specified address and uses quite a basic instruction format without any authentication its capabilities can be tested out by redirecting traffic from a compromised device to an analysis machine running netcat.

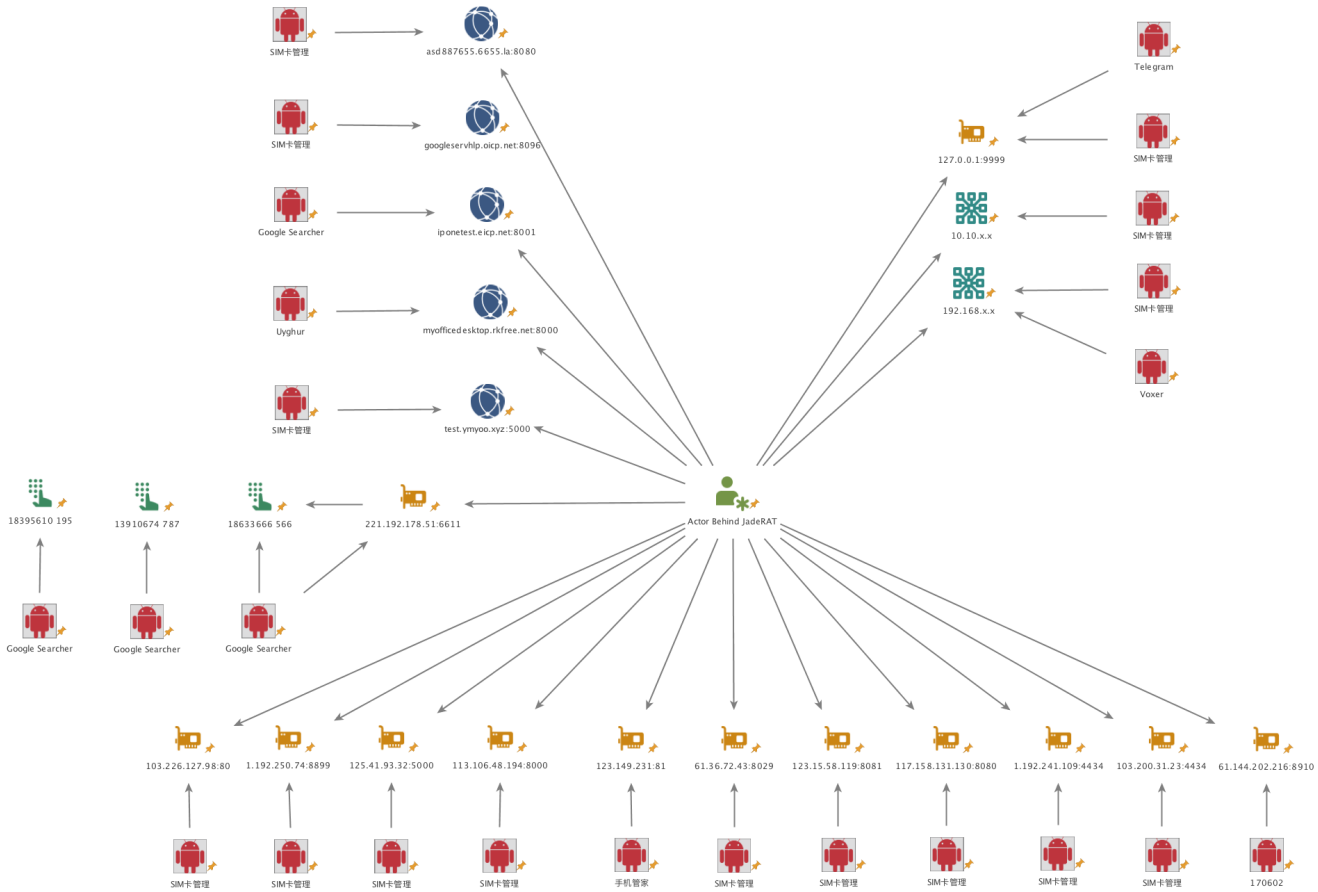
Infrastructure

JadeRAT's operators have consistently changed their infrastructure. Production releases rarely reuse domains or IP addresses, frequently use dynamic DNS, and communicate on various non-standard ports. JadeRAT is configured to send SMS messages to an attacker-specified phone number when the compromised device first comes online, however these have only been pre-configured in three of the most recently observed samples. We extracted the following phone numbers from samples acquired during April of 2017:

NumberRegionOperatorBrand18395610195Shijiazhuang City, Hebei ProvinceChina Mobile Communications CorporationGlobal pass, M-Zone, Shenzhou line, G318633666566Handan City, Hebei ProvinceChina United Network Communications Group Co., LtdUnknown13910674787BeijingChina Mobile Communications CorporationGlobal pass, M-Zone, Shenzhou line, G3

Though these phone numbers are only associated with a limited number of samples, all samples come configured with specific infrastructure to which they communicate. Below are observed domains and external IP addresses.

IP / DomainPortgoogleservhlp.oicp.net8096iponetest.eicp.net8001myofficedesktop.rkfree.net8000asd887655.6655.la8080103.226.127.9880125.41.9



Lookout is continuing to track JadeRAT and its associated infrastructure closely as we anticipate this family will only continue to grow.

Want to learn more about threats like JadeRAT and our Threat Advisory services? Contact Lookout today.

SHA-1sfea0bc1df035ea8eb683bc91cef4d925d8a260f3b86d8dc815f50377e444a297f5f33bba1b16cc8e674224a4fe7ec9badd5eefce303ec0867a4afcdf3

All these indicators have been added to AlienVault under the JadeRAT pulse.

October 20, 2017

Download Case Study
{{consumer="/components/cta/consumer"}}

TAGS:

|

Threat Intelligence
|

Surveillanceware