Operation C-Major: Information Theft Campaign Targets Military Personnel in India

TrendLabs Security Intelligence Blog

David Sancho and Feike Hacquebord
Forward-Looking Threat Research (FTR) Team
March 2016

Contents

Introduction

The Trend Micro Forward-Looking Threat Research team recently uncovered an information theft campaign in India that has stolen passport scans, photo IDs, and tax information of high-ranking Indian military officers, non-Indian military attaché based in the said country, among others. We came across this operation while monitoring other targeted attack campaigns,[1,2] and what caught our interest, apart from its highly targeted nature, is the lack of sophistication in the tools and tactics it used.

Apart from using email and social engineering as entry point, this operation exploits a relatively old vulnerability, uses a malware that can easily be decompiled for a researcher to map out its network infrastructure, and has command-and-control (C&C) servers with open directories where exfiltrated data can be accessed and analyzed. Compared to its contemporaries, in terms of technique this targeted attack campaign is amateur at best, sloppy at worst. Despite this, it was able to get at least 16 gigabytes' worth of data from 160 targets.

Our analysis also leads us to believe that the attackers are located in Pakistan, although there is no evidence to suggest this attack is tied to the Pakistani government. We also have reason to believe that this operation also goes for information found in mobile devices of its targets.

This technical brief provides a detailed look into the operation: its targets, its tools and its tactics.

The attack

Like most targeted attacks, the actors behind this campaign use email as their point of entry. As in most targeted attacks, the attackers have a very good idea what the individual targets are interested in, what subjects they are most likely to click on, and use this to their advantage. Below is a sample email from this group, which was sent to the military attaché of a foreign country who was assigned to India:

---

[1] Proofpoint, Inc. (2016). *Threat Insight Blog.* "Operation Transparent Tribe - APT Targeting Indian Diplomatic and Military Interests." Last accessed March 23, 2016. https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe
[2] Cloudsek (2015). "Crimeware / APT Malware Masquerade as Santa Claus and Christmas Apps." Last accessed March 23, 2016 https://www.cloudsek.com/announcements/blog/apt-malware-masquerade-as-christmas-apps-and-santa-claus/
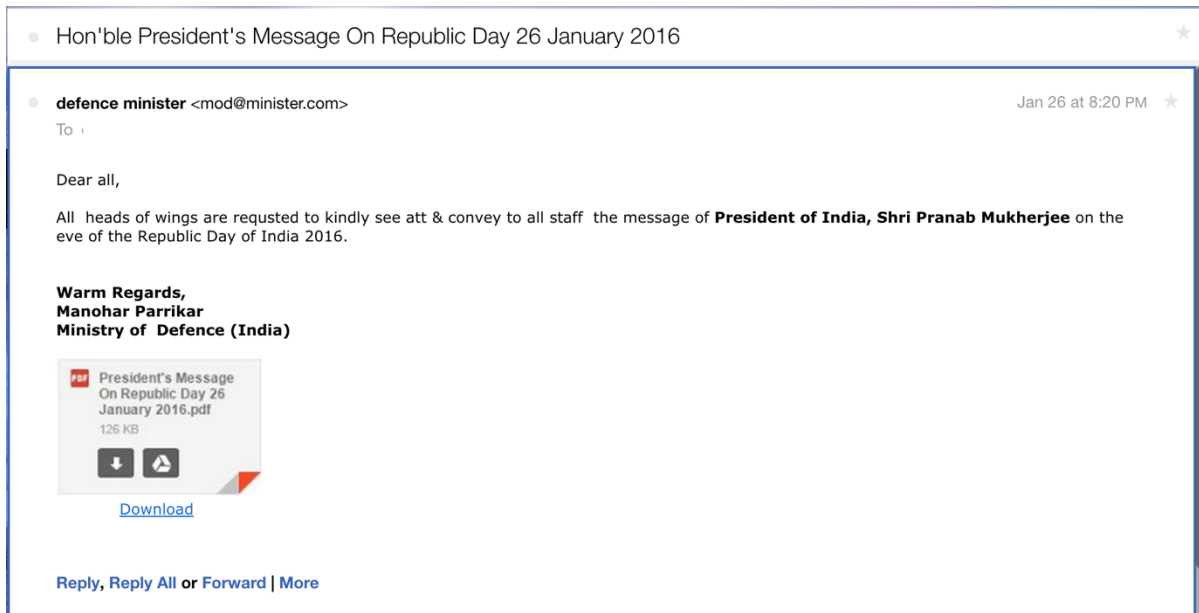
Once the PDF files are opened using Adobe Acrobat Reader, an exploit is triggered which drops a malicious Windows executable file—a Trojan—which then connects to and communicates with the C&C server. The main features of this Trojan are keylogging and password theft; however, the attackers, upon their request, can also make it record audio, steal any amount of files, or take screenshots. Invariably, after a few minutes, the server instructs the infected client to upload the keystroke log.

We assume that the attackers would use these logs to determine if the affected system is interesting enough that they need to perform more actions against it. More technical information about the binary and the C&C communication protocol can be found in the appendix below.

The malware is also compiled into a Microsoft Intermediate Language (MSIL) binary using Visual Studio. This means that: 1) the original source code was probably VB# (Visual Basic .NET) or C# (.NET version of C++), and; 2) the developers don't know (or didn't care) that these programs can be easily decompiled. This shows an unusual case of targeted information theft where the attackers are providing the source code for free. This implies that the threat actors responsible for it are not very sophisticated, not knowledgeable, or both.

The threat actors' command-and-control (C&C) servers have open directories, and from there we were also able to identify Microsoft Office files related to several other campaigns against other Indian targets:
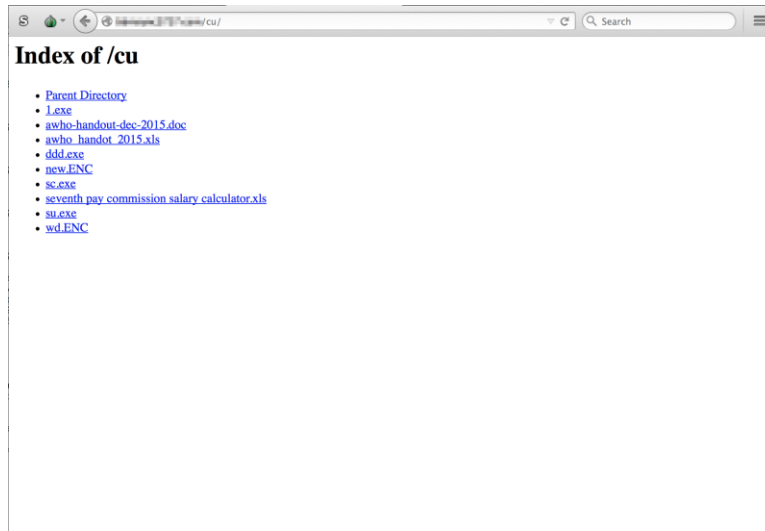
The targets

We found three open directories on the C&C servers associated with this operation.
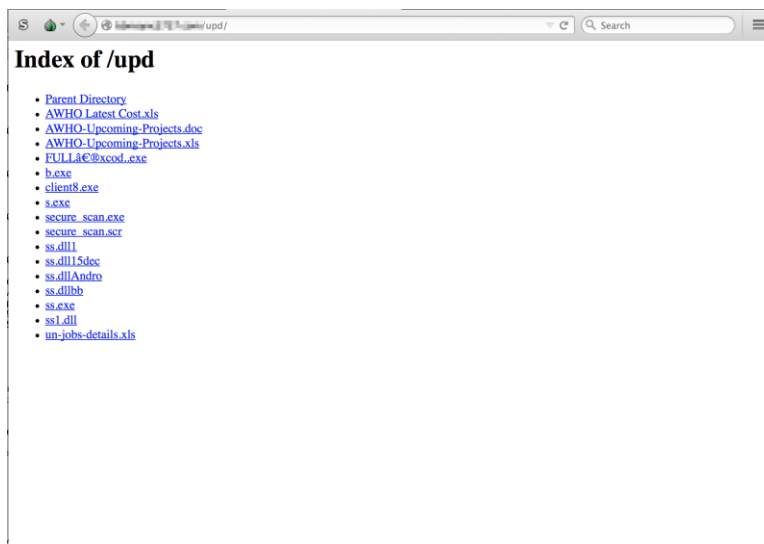
These directories contained more than 16 gigabytes' worth of the targets' data, and a careful analysis of the 160 records found in these directories gave us a good idea of the kind of people the attackers were after. The majority of them belonged to officers of the Indian army, although we identified some as IT consultants and/or resellers. The data that were exfiltrated from these people included:

> Passport scans and other photo IDs
> Salary and taxation data (Indian army PDF payslips)
> Army strategic and tactical documents
> Army training documentation
> Personal photos

LALGARH:

Lalgarh is a village in the Sujangarh tehsil of the Churu district in Rajasthan, India. It is situated at a distance of 57 km from Sujangarh in the southwest direction near the border of Nagaur and Bikaner districts. The lat 27.5138 and long 73.90611 u had sent, nothing noticeable and markable in that area.its showing plain desert area far away from rural area and houses.

I discovered only 1 thing which is located in east the area covered 336.23 yards with lat 27.515942

And long 73.916517.constructed in year 2013.it seems some vegetation occur and

Shadow indicates the area is high above as compare to its surface.In past few years

The area was plain till 2012.

in 2015

ARMY CYBER
SECURITY POLICY

RESTRICTED

CONTENTS

The personal data of the targets identified them as brigadiers, colonels, lieutenant colonels, majors, and lieutenants.

Command-and-control (C&C) servers

The malware connects to a single C&C server hardcoded into the malicious binary. Different campaigns use different C&C servers and ports. Here are some of the servers in use:

- 178.238.235.143:9999
- 213.136.79.50:80
- 80.240.134.51:80
- 82.196.13.94:80

- 93.104.213.217:1337
- 95.85.43.35:9999

Using reverse DNS, we were able to find associated domain names for the above IP addresses, as follows:

- 93.104.213.217 – vmi22485.contabo.host – *Contabo is the ISP hosting this server.*
- 95.85.43.35 – bbmsync2727.com
- 213.136.79.50 – bluesync2121.com
- 82.196.13.94 – pradahandbagsshoes.com
- 178.238.235.143 – vdjunky.org – *also m1343.contabo.host*
- 80.240.134.51 – ordering-checks.com

Older C&C servers give us the following information, too:

- bhai1.ddns.net:3050 (182.185.110.142) – *This IP is hosted in Pakistan*.

Especially interesting for us is the domain *vdjunky.org*. It was registered with the email address *akml614@yahoo.com*. This address was also used to register other malicious domains, as follows:

- Idnnews.net (91.194.91.202)
- Mpjunkie.com (193.164.131.225)
- Pbxmobiflex.com (178.238.230.88)

In addition, we found five more domains with a familiar pattern, the same as some of the C&C servers listed above. In fact, all of them are, or have been, C&C servers.

- Applemedia1218.com (213.136.79.50)
- Avssync3357.com (213.136.79.50)
- Bluesync2121.com (213.136.79.50)
- Eastmedia2112.com (75.98.175.79 and 213.136.79.50)
- Mvssync8767.com (213.136.79.50)

If we look at the first three domain names along with our original *vdjunky.org*, we see more interesting things too: *pbxmobiflex.com* was used as the C&C server of an Android spying app. This mobile malware can read the affected user's SMS and listen to phone conversations. We

suspect that malicious apps running on iOS and Blackberry may also connect to this same server, presumably used in similar spying campaigns.

While it is possible that the Windows and mobile malware are owned by different actors who are only sharing a hosted server, at least one news article[3] from Indian media reports that this very server was used to spy on Android users from the Indian army. Chances are that the same actors are behind both operations.

In addition, we found that a server connected with this group, 93.104.213.217, is actually a live C&C for a Windows .EXE file called "*NATO soldier killed in firefight between US_ Afghan forces.exe*". This same server also acts as the C&C for an off-the-shelf Android malware called Sandrorat. We believe that there is a definite connection between the Android malware, these actors, and their spying campaigns against India.

The Pakistani connection

Although we cannot be 100% certain who is behind the operation and exactly where it is coming from, there are certain clues that point to it with a high probability. First, the Indian army is targeted by both the Android and Windows versions of this malware. The older C&C servers of this malware were located in Pakistan until they were moved to Internet service providers (ISPs) in Western countries. The new C&C servers seem to be administered by somebody located in Pakistan.

Another interesting fact is that malware samples from this group get a lot of rescans on VirusTotal by the same user ID from Pakistan. The picture this paints becomes clearer: threat actors (without much training or resources) located in Pakistan are responsible for attacks against targets predominantly tied to the Indian Army.

These actors send emails to high-ranking officers with relevant social engineering techniques, and are intent on stealing information. Additionally, there is evidence that these same attackers infect mobile phones of Indian army officers with spyware that steals communication data.

---

[3] IBN Khabar (2016). "सबसे बड़ा पर्दाफाश, 200 फौजियों की हर जानकारी पाकिस्तान के पास!" Last accessed, March 23, 2016. http://khabar.ibnlive.com/news/desh/more-than-200-army-personnels-under-pakistani-honey-trap-460616.html [article in Hindi]

Conclusion

When one thinks of targeted attacks, the first thought always goes to bigger countries with big budgets and very tight well-thought-out operations. As Operation C-Major shows, smaller players are in this game, too, and what they may lack in technical sophistication, they make up for through tenacity, persistence and clever social engineering.

For those in charge of defending a corporate or organization network, this attack reinforces the fact that any user, regardless of rank or position, is susceptible in becoming the organization's weakest security link. As such, while network defenders should be prepared to help prevent, or minimize the damage of attacks, people who use the said network should likewise be knowledgeable of threats that could possibly come. The need for proper user awareness training is clear.

In the same way that there are different levels of cybercriminals with varying levels of sophistication, the same thing applies to threat actors and info-stealing attacks. Methods of defense in the technological realm are, of course, recommended—one could say they are a must nowadays—but do not underestimate plain social engineering attacks on the basis that only cybercriminals lurk behind all malicious attachments.

The attackers don't need to be high-tech in order to conduct a successful targeted attack operation and in cases such as these, the same thing can be said of a successful defense.

Appendix

Technical Features

The malware used in the operation is an information-stealing Trojan. Its main purpose seems to be obtaining and exfiltrating information from the target Windows computer and uploading it to an external server. Although it is flexible in what it can do, by observing the ways it is being installed in its targets, we believe this to be a targeted operation.

Based on how this Trojan was programmed and compiled, it's highly doubtful that it came from a well-funded organization. Rather, it appears that a modest, low-profile developer team or even a single programmer created it.

The strings within the malware code are in English, although the amount of misspellings point to a non-native English speaker. The EXE seems to have been compiled in Visual Studio and programmed in VB#. Therefore, the final product is a .NET binary that has not been obfuscated, and the original function names and variables are kept as they were written. This makes analysis much easier.

Main program

The main program's internal name is *msdocuments* but the attackers rename it depending on the social engineering theme used against the target. We have observed names like *securescan.exe* and *wservices.exe*. The original internal version we analyzed was 1.0.0.0, which implements a primitive communication protocol with the C&C server that only supports updates. This communication happens through a high TCP port; ports 1337, 9990, 9999 and others have been observed. Once the client connects for the first time to the server, it stays quiet. Then the server responds with a string: "info=command", which the client does not immediately reply to. After a brief moment, the client starts sending the following command:

updatc=<user> | <machine> | WINDOWS <AV_installed>

In this command, the client is requesting an update for the infected computer. <user> refers to the logged in user name and <machine> to the hostname of the infected PC. "WINDOWS" is a

hardcoded string, although we have not seen other OS ports of this Trojan. <AV installed> is a key string that the client assigns based on an analysis of the process list. If no active antivirus program is found, this string is "Not.Found". Otherwise, there are a few strings, like "[Kaspersky]", "[Symantec]", "[Microsoft-Security-Essentials]" or a generic "[Anti-Malware]". Trend Micro is not on the list, although an Indian vendor's AV is: "[Quick-Heal]". Perhaps this is a reflection of the AV market share of the region the developer is from or where the expected target might be.

The reply to the update request coming from the server is the following:

> updatc=client=\wservices.exe<BINARY>

This binary is an updated version of the main program, which will replace the older version. The malware writes the new version to disk and starts it up.

The new malware sample has a version number 1.0.0.6 and the communication protocol is much more comprehensive. Whereas the old one had only three commands (*updatec*, *info*, and *upsecs*), this new one supports 40.

The downloader program seems to be the spearhead part of the attack, but the new version looks like the real client. Each of the EXEs in this attack group seem to have an internal name assigned to them. In this case, the downloader's is *DOSERS* and the main client program's is *FORYUO*". This string will later be used as a prefix of each command, perhaps to identify the version of the client.

Once the new client starts up, it establishes again a TCP connection with the same server and port and stays quiet. As usual, the server responds with an "info=command", which the client doesn't immediately respond to. The client then sends a full info command, telling the server more information. This is the command observed:

> FORYUOR-info=user <MAC>|<hostname>|<user>|<OS>|<version>|<AV_installed>|
> FORYUOR-uklog>
> FORYUOR-sndps>
> FORYUOR-secup>
> FORYUOR-audio>
> FORYUOR-usbdiv>
> FORYUOR-sapp=httpscan<\Scaner\>
> FORYUOR-kapp=svehost<\services\>
> FORYUOR-uapp=udriver<\Drivers\>
> FORYUOR-papp=servicescan<\services\>
> FORYUOR-mapp=httpservice<\Windows Data\>||c:\Documents and
> Settings\user\Application Data\Windows Data\

<MAC> refers to the MAC address of the network card used to connect. <version> refers to the client version. In our sample, this was "Microsoft-1.0.0.6". The rest of the fields point to the many modular components of the attack. "uklog" refers to the keylogger binary, "sndps" to the sound binary, "secup" to the backup client process, "audio" to the audio driver and "usbdi" to the filestealing module. On first call, this set of commands is empty, as shown above, although the directory paths assigned to them are already decided and set up by the client program. The path where each of them will reside, are sent in the last few lines (the commands "sapp" (the backup program), "kapp" (the keylogger), "uapp" (the file stealing module), "papp" (a password stealing module not requested although the path is already set up) and "mapp" (the main application).

The response to this message coming from the C&C server brings all the binaries that the client has requested (keylogger, sound module, audio driver, filestealing module and backup module):

```
uclntn=98
uklog=loger=\svshost.exe<BINARY>
secup=client=\servicescan.exe<BINARY>
audio=mcaudio=\Naudio.dll<BINARY>
update=usbdriver=\udriver.exe<BINARY>
```

The TCP connection is left open and the C&C server will be sending a ping command at specified intervals to keep it that way:

```
clping=Ping
```

Other commands supported by the 1.0.0.6 version of the clients shed more light on what the purpose of this threat really is. Here is a list of all the commands and a brief explanation of their functionality:

- afile: Functionality not identified
- audio: Updates the audio driver
- clping: Sets last communication time to current time
- clrklg: Stops and deletes the keylogger module
- cnls: Enables "Cnls" capability
- cscreen: Takes screenshot and uploads it to server
- delt: Deletes a file on disk

- dirs: Lists drives in the system, then uploads results to server
- dowf: Downloads a file from the server
- dowr: Downloads a remote executable file and runs it
- endpo: It quits the main program
- file: Uploads a file to the server
- filsz: Provides filesize
- fldr: Lists folders on disk, then uploads it to server
- fles: Searches files on disk
- info: Sends pc info (MAC, user, hostname, AV, etc.)
- klgs: No functionality. Possibly a remnant of an older version.
- listf: Looks for files with certain extensions on any disk
- mesg: Send a message to the user. It displays a MessageBox
- passl: Runs password logger, then uploads results to server
- procl: Lists all windows processes and uploads the results to server
- runf: Runs an executable in a separate process
- rupth: Sends back the path where the main program is located
- savaf: Saves a remote file to the infected PC
- scren: Takes a screenshot
- scrsz: Sets screenshot size
- secup: Updates the backup module
- sndpl: Updates password logger, runs it and uploads results to server
- sndps: Updates password stealing module
- splitr: Splits a file in pieces. Possibly to steal bigger files more efficiently.
- stops: Disables screenshot capability
- stpre: Stops audio recording
- stsre: Starts audio recording
- sysky: Uploads keylogs to server
- thumb: Saves an image to disk (of the current application, possibly)
- uclntn: Sets a version number in the registry. It looks like a sequential number
- udlt: Downloads a "remove user" module and runs it
- uklog: Updates the keylogger module
- updatc: Updates main module
- updatu or usbwrm: Updates file stealing module

Indicators of Compromise (IoCs)

Malware hashes involved in the attacks

- 0007a5cbdfcda9175635bd1b30e5d3a8683bdcb6
- 0306d2ba75656cefc171edf4ab2495f7d79407c3
- 038f970e9292c921c2a97fe4f80a2213b7b624d7
- 03b10fd1a78b7bd1dc64042991f1ebaf38fee7f6
- 08a93ca86a8770f5d971e78d018628428052292a
- 08e25cc3674d9b5cead2c883132b7f8996f7bf10
- 0bebfcdb6f23b7bb749633068e176c35a72768cc
- 0cff5cc4c46e148d3d8c93d11c459f7ede3a854c
- 0edc71cc01ec8d16aeddf0c807bb696966c83266
- 0efbc946db0d865aa443eba0f00333efab20ba06
- 0f570eabe749b05d59cb2eca9dcef81ad9b044bc
- 12fef517621b28f94dadb7d45fc2a4731909aaab
- 13d59ec2aa935f80342b5bccc9d1bf447948feff
- 1421c353bfba53249fcbf0504b8580095cdd7e86
- 156a22ae48bf7b0e6ae604cec30eb793cf3a1e35
- 1ac9991fb65dd30d9a085046da27c04ce1cf6948
- 1bf850ec4dacd43323e75be040ee6bc7a3d05fe9
- 1c104d02048ad62224e0f725cee1becfb75d4976
- 1ff42d996489812602d65f9eb7433c8018b17acc
- 20bd67010fe69f56bdb00667100a0c1bc1e7c906
- 2114d6763cb93ac34d6bd773c2ab261e2510deba
- 23dcec87435af17e695c8612f1453d38950bc61d
- 2504320598b8e603f46936037491111718907e98
- 27385b5fdfab1fd83dcac32750879ff4c2f82797
- 281ebc259e96531d4512b5ee9c5d4dc646feda2c
- 2873f5215cd6e62b4b0a12861fce64685e557fdf
- 28f9a68807b06b1464d7663eb6164969142959c9
- 2d97f9f42aeafdae2cceb79d538e5036b8e5bbff
- 2f5c5627ae45f1244927aa02a3bf4a0b81d312de
- 313049a0594f50b0015a06b44703d903ad36bc68
- 32a0618dde949902a02cf39c59b609c31d976ffe
- 340a13547cef341ee99e5d2bc49a0e850310b6e3

- 349f6ad58fdb5708abd97fd39a338ebbe0818a74
- 3abd37f20fa74462f4e49d24b38e33889da22a63
- 3b3866ab32843d6a717fee0be718fbfb7b5eff67
- 3cc931db58298134cbaec5dfd0c8030447b673d7
- 3d44cf9a814e57ded1590b008d1e9b28545f6bc3
- 40fd6d368bce6dcf6a933c6494d74f01a07587af
- 4336f402037d48321331c89c2848f971a6838ffb
- 4382d38acfd62bddd6858393b3d47cecde7e3d6e
- 43b836a3293c41bf45906fb1eefd09d8a1a9ed87
- 44ffd554b2a4ece3b0283bd5674434e09f8bfbbc
- 4796aa0b2415f127feef35bfe183c5297f291e50
- 4909a5c48c1d2684b830567e18bfcba8d05a267f
- 4aae973372d5eeaff5b1b1b9f53ed5cd2d3ea15e
- 4ad5ded6f7ebb033c8c854700e329eec5ccb0f0f
- 4af62f9021e86e30be1bc31c2113e0c1e019aa14
- 4fe5eb02299fbbca4157e6e8b414f8a575a465d0
- 58b7cdbf101fe762d34fa21a61b5896e6eb15b6f
- 591d8dcea6ec8c65f0c3140abec7ff63a90cdd11
- 5ab950210e46a2aa600844e2168b8acb9c1a1780
- 5b29e5e7ee100af6cdb4269fc4cc174550c7c869
- 61c1f54434e373df9be0426dce5cabae4d46612f
- 61ff8373337e21910291021301c36cf8216e13cb
- 63203e01d8d648f30d322ba8e7d85a694edb8241
- 637edcd549c8be0e2e8b7bc61c932ca0a58ca77d
- 66802d4bd6d405458dcf9ebf081e347a946f0f8b
- 6c286d171ecf588bc16efe4847e57711cd5e74bf
- 6d4e788a36fc95899e035d8a1871a135c56ba1b5
- 6e3e89e2f3d096ee09d4bf88410e80ef17536ab7
- 6e9f7890dbe523a5cadcb33e20a2e78a69936b01
- 702104c7b7b7ff2176d7a0718f19196ff392af34
- 71e51de9a64d3378165f8bc4bfb495daec21ed53
- 72adf01044e7ceeefc7b50977b329a903cbcb6cb
- 75dd19ec9719f82b94d1e207102fa1f0bca55c9f
- 75dec30eb62c03b917f62a091971c5640e556170
- 79bbacbbe55c1065fe2e6a07aac852ef5c0c86ba
- 7b930d3516d1396a4f374ee30339e2003714e51a
- 82488d289d724f0dfb6432062a227d8ad009335d
- 880fa1a65d8c529753e64e4ed22d0e3622b9b030
- 8a99a63a1f283be8056f872bacf458c0b764668c

- 8afaec7a8d1e17bbf18c3a00bd13a2af5901711f
- 8f645390ceff5e1eb93dd3a152aea57d6489e2ff
- 8f70d77577ccc3428dd0f33c5b83858b5c5f5cff
- 8fc1f5f09f918816b5f5ff2ceb133d5c0c336bdd
- 900b78ead56dfdfa7ec22fda8b1ad9b4e4dcaf6f
- 916bd8577a7454ac4ba4dc480ade4fe465eb4386
- 92acf54e2532aff41ad6d99e4c83c223088ab077
- 963d63b93f28f7077c77bdbdc2ec5dc39e909a3f
- 98414f9455d6a86d5abe444d983f337266bbd56b
- 98afd9d5cd9a651c346441e8ab01ec080b3d2bee
- 9b9599ee504272c90d01c93225d999cdc8431795
- a39ec00c5cc51db7fcdb28cdc04aa0cdf154f322
- a85238cb1bb67a8b7e6a9def967f13fd1bd0b731
- acf3761c0bf627be5dfa25c4bb89451ec8a2ff8f
- ad505ac717d8a76d926503d0d0c26ae72f2014be
- b0f9c9caa24bf105bc85a1ef959a8a662d187fa3
- b354767bde1b493570a8f56a8facefd195eb3842
- b38d2d37030b2b43555b6a184cfebca55f524f80
- b589dfe2d215d93b0c8d4ab4cb9ec2b407c53b84
- b9c59c248adaa8e50dc7d05f12d01bd134ca16a9
- b9fc15f37996096889ed889a422e56303e209a6f
- baf96699ad162d7c9d55108a7c083937b0290956
- bcca68cc9af142fefb70a3721a2e87973e0c988e
- bd92fc6363e38592893e7c87b327ff879dd4d5b5
- bdbec6894729e6d550d3000a00433b5fc23987ac
- bf18bc2e10a458bf1172b0abaad90d065dd2da69
- c1740206e858bc8526553c7eab8fdf3ec4cfb92c
- c38b85c1eac3beacd7cb7841202376b15ac90d8c
- c79ffb9fe8ad886f85ce6b070f3a98996fdfe250
- c7fc5c49edfab9b77b70e03047d57583f27d2f5c
- c91df56b7d387d7ae8f207ecf84ef3c0674f8927
- c9d3cd219021d0a64716c185ea38105d3f17e97e
- cacb10f08b6c3fa72a7cf03f163a4acde97f6eb0
- ce429271292095ca04f6231e1f403ad914db81b1
- d140c6cc6929db8666f4b6b2c8734c013755a514
- d4d68ec24deedbd526d8b153be9d5370aed02618
- dc9a686a37ad0275f65f267a0c6b1ab7d35b35b8
- df42097d95236bbad6d05839aa55a8bac68d26cd
- df8822b47f7bea4a8b21a0708dd48b1cbced8e90

- dfff31642cddc28498df7e67682eef4a7647c61a
- e4b95a1f7d17b5a46a21d5a65290a87ace0077e5
- e654542942839c8441f79209e5a7c565af682667
- e861c257c257401a5bd4c5487a45696d7796135c
- ea342e170658732483329218a6bd76d127ba39bb
- eb5df6b6b4037a4117d203ce643371e68d13355c
- ec1df6ba0af285931bab81205e8c177e727cade5
- edb9006f9a1ee46000727f99e4049c4163675e2c
- f3683123c76b0806ebf7cf2951a9754cadb2c149
- f3f27b29c534d919a1261c2e6b7b9c2eaa404d41
- f83048f505a2dc298a130d8e4af66fc3eb44863f
- fa4b8715b344b12bc2387e1c1a9248b4780b265f
- fa930506d5ae47abe9c9a5b48f3bfc57e6a1b4e8
- fcc8ac89581e1625a05ef54cee9ce8d3a48a8144
- fd9622452d02c6d84532b51b3599f2015301371d

Android sample hashes

- 0441109fe1408d412e8cb61362c8169981156a29
- 9288811c9747d151eab4ec708b368fc6cc4e2cb5

C&C servers involved in attacks

Some of these might be compromised servers hosting some of the samples.

- bhai1.ddns.net:3050
- 176.10.136.96:4782
- 178.238.228.113:7861
- 178.238.228.113:9001
- 178.238.235.143:52399
- 178.238.235.143:52400
- 178.238.235.143:8688
- 178.238.235.143:9001
- 178.238.235.143:9999

- 191.101.23.190:5552
- 193.164.131.58:10000
- 193.37.152.28:9990
- 213.136.64.119:10101
- 213.136.87.122:10001
- 5.189.137.8:1453
- 5.189.143.225:11114
- 5.189.152.147:12200
- 5.189.167.23:7866
- 5.189.167.65:12010
- 80.241.221.109:10000
- afgcloud7.com
- Attachment.biz
- bhai1.ddns.net:10110
- bhai1.ddns.net:3050
- http://bbmsync2727.com/upd/ss1.dll
- http://ordering-checks.com/bbm/bbm.exe
- http://ordering-checks.com/bzu/ordc.exe
- http://ordering-checks.com/cum/orc.crm
- http://ordering-checks.com/cum/ordd.exe
- http://ordering-checks.com/ord/bb1j.exe
- http://ordering-checks.com/ord/dc1j.exe
- http://ordering-checks.com/patch2/perfect.exe
- http://ordering-checks.com/sms/bbms.exe
- http://ordering-checks.com/sms/ordapr.exe
- http://thefriendsmedia.com/est/controller.exe
- hussainibuilder.com
- knockknock-jokes.com
- ordering-checks.com/bzu/ordc.exe
- ordering-checks.com/bzu/ss.exe
- pradahandbagsshoes.com

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003