The Daily Star
DHAKA, MONDAY, FEBRUARY 23, 2015
e-mail: bytes@thedailystar.net

INFORMATION | GADGETS | TECHNOLOGY

BYTES

HANDS ON REVIEW

SYMPHONY EXPLORER ZV
Budget premium

SPECS

Display: 5 inches, IPS OGS 294PPi
Camera: 13 MP, 4128x3096 pixels, 5MP secondary
OS: Android OS 4.4.2
CPU0: Octa Core 1.4 GHz
GPU: Mali 450 Mp4
Sensors: Accelerometer, proximity, G-Sensor
ROM: 16GB, RAM: 2GB
Battery: 2000 mAh

PRICE: TK. 14,990/-

WORDS AND PHOTOS
EHSANUR RAZA RONNY

Symphony makes affordable phones. And affordable usually means cutting a few options out of the list. And now they have gone and built a range topping device tagged with a sub 15k price tag that is bound to make this a favorite. WE find out whether this is just good enough or something even better.

BUILD: its glass front and back is encased in a unibody structure giving it the right amount of weight and solidity. The up/down toggle switch and the power button is conveniently placed on the right with SIM and memory card trays on either side. It's a sharp edged device that provides good 'holdability' meaning I haven't dropped it yet.

DISPLAY: 5 inches is now the acceptable standard for reading, viewing, playing and showing off. The HD display with 294ppi provides sharp and clean fonts. The screen is super bright even in strong sunlight. The only gripe i have about it is that at its lowest brightness, it is still too bright for reading in the dark.

HARDWARE: An ARM Cortex A7 1.4GHz Octa-core processor means there's plenty of power for all your computing needs. This is backed up by a solid 2GB of RAM. I've been running plenty of games on this machine. SIM City and Real Racing 3 guzzle quite a significant amount of processing power. Both games have plenty of stuff going on at all times. The device so far performed without any hiccups seamlessly stitching from one app to the next. There's 16GB of onboard storage space with 32GB of expandable memory.

SOFTWARE: I hate bloatware and this device comes with a few. But Symphony has avoided the previous odd looking skins kept bloatware to a minimum. The interface works smoothly almost like a stock android. The 4.4.2 comes out of the box and an upgrade is due soon.

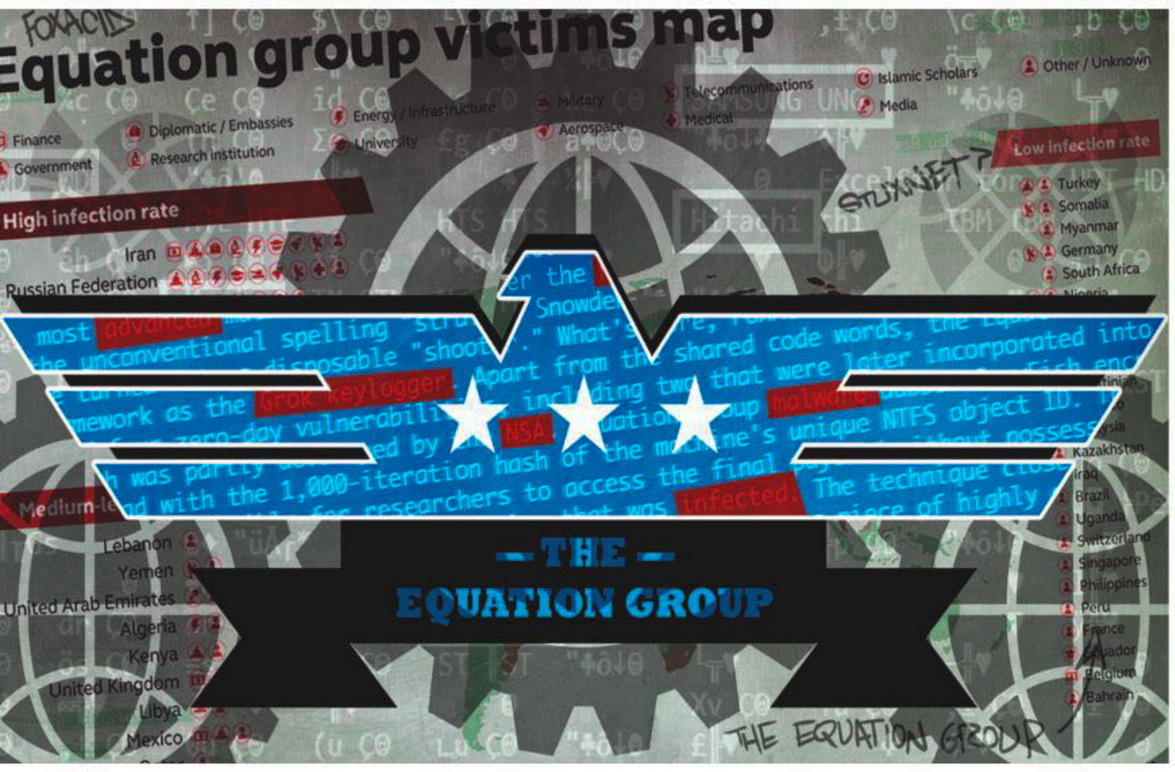
CAMERA: Yet another improvement over the cameras from Symphony I've used before. This has a 13MP primary unit and a 2MP moderately selfie friendly front unit. The camera responds quickly and takes the picture i want. Gone is the older units annoying shutter lag. There are plenty of options to play around with. The HDR takes its time but does produce brighter shots in lower lighting.

BATTERY PERFORMANCE: The 2000mAh battery sounds like a recipe for disaster. In case of a zombie outbreak, at the most crucial moment, you fear you will run out of power. Fear not. I have managed to get a full day worth of heavy usage out of the phone. And that shows how well the 4.4.2 manages to keep all that hardware running smoothly.

VERDICT

At just under Tk 15000, this is terrific value for money. Symphony played safe with the styling; going with a square design that has stood the test of time so far. You will like holding it because it feels premium. And you will like using it because it has plenty of juice for not much cash. And when the zombies do come running, you can kill one or two by hitting them with it. It feels that durable. It has been my daily driver for most of a month now and I am yet to find a serious flaw with it. It's the best smartphone I have used in this price category, period.

Equation Group: God of Cyber Espionage Detected
BANGLADESH TARGETED TOO!



Last week Kaspersky Lab unveiled the predecessor of Stuxnet and Flame – a potent threat actor called Equation Group. The malware used in their operations, dubbed EquationDrug and GrayFish, is found to be capable of reprogramming hard disk drive firmware. This 'outstandingly professional' group has been in play for more than a decade- experts say. Though Kaspersky Lab wasn't able to pinpoint the origin but security experts have pointed their fingers toward an American Intelligence Agency with prior history. Nearly 30+ countries were attacked or infected by this group including Bangladesh. We got in touch with Igor Soumenkov Principal Security Researcher; Global Research & Analysis Team, Kaspersky Lab Moscow. Igor, a virus analyst and malware expert, shares his concern with The Daily Star.

How did you first discover the malwares and how did Bangladesh come under your radar? And also how long has this been going on, particularly in Bangladesh (BD).
We discovered one of the first EQUATIONDRUG modules during our research into the Regin nation-state APT operation. Somewhere in the Middle East, there is a computer we are calling the "The Magnet of Threats" because in addition to Regin, it was also infected by Turla, ItaDuke, Animal Farm and Careto/Mask. When we tried to analyze the Regin infection on this computer, we identified another module which did not appear to be part of the Regin infection, nor any of the other APTs.

Further investigation into this module led us to the discovery of the EQUATIONDRUG platform.

Unfortunately, we don't have such level of details re-information on Bangladesh victims.

How can the general people check if their computers have been infected?
Our products have detection for the malware used in the attacks - the user may scan his computer to check it. Also we have publicly provided indicators of compromise which also should help detect the threat.

Are the infections limited to computers only or other smart devices- phones, tabs etc.
All the malware we collected so far is designed to work on Microsoft's Windows operating system. However, there are signs that non-Windows malware does. For instance, one of the sinkholed command-and-control domains is currently receiving connections from a large pool of victims in China that appear to be Mac OS X computers (based on the user-agent).

The malware callbacks are consistent with the DOUBLEFANTASY schema, which normally injects into the system browser (for instance, Internet Explorer on Windows). This leads us to believe that a Mac OS X version of DOUBLEFANTASY also exists.

Additionally, we observed one of the malicious forum injections, in the form of a PHP script, takes special precautions to show a different type of HTML code to Apple iPhone visitors. Unlike other cases, visitors from Jordan, which do not get targeted, iPhone visitors are simply redirected to the exploit server, suggesting the ability to infect iPhones as well.

What are the possible countermeasures?
We suggest individuals and companies to use modern Internet Security solution (many of attacks against our users were not successful due to Automatic Exploit Prevention technology which generically detects and blocks exploitation of unknown vulnerabilities) and to timely update their software not to get infected with help of the exploits for old zero-day vulnerabilities.

Since these are no more considered as zero day exploit, what could be the next move?
We don't know. And taking into account that we don't see any activity of the group starting from the end of 2013, they may have already found the way how to hide better and work stealthier. And this is scary.

Does Kaspersky think hardware companies cooperated with Equation Group to provide access to the source codes/firmware codes?
We don't know how the group got access to the firmware source code. But we doubt it was a case of cooperation.

You commented on several media that the only solution to the Equation Group threat is destroying the hard drive. Is there any other way to combat that?
First of all, the HDD firmware reprogramming module is extremely rare. It is probably only kept for the most valuable victims or for some very unusual circumstances. In case if a user has nothing to do with some extra-secret research or things like this, the chances that his HDD firmware is infected are close to zero. That was a good thing.

And the bad thing is that there is no way to understand whether a HDD is infected. Once the hard drive gets infected with this malicious payload, it's impossible to scan its firmware. To put it simply: for most hard drives there are functions to write into the hardware firmware area, but there are no functions to read it back. It means that we are practically blind, and cannot detect hard drives that have been infected by this malware.

So yes, if you think that your HDD firmware is infected, the only solution for now is to physically destroy the hard drive.

INTERVIEWED BY: SHAHRIAR RAHMAN

Come.....Contribute:
Enrich Bangla Online

Bangla is the 7th most widely spoken language in the world, and still Bangla was the 65th language to be added to Google translation service. Hence Google Developer Group Bangla (GDG Bangla) has undertaken an initiative to improve the Bangla translation of Google Translate. Google Translation-a-Thon- the name of the initiative to add Bangla words to Google Translate, will be going on throughout the month of February. This entire project is a result of initiatives from individuals and voluntary work. People from all across the world are enriching Google translate through their own efforts and with their own language. Anyone can help make Google Bangla translate an even better experience. GDG Bangla is looking for everyone's participation to reach the goal of adding 200,000 words to Google Translate within a month. With the slogan 'Shimana Chariye Bangla (Bangla Beyond Borders), GDG Bangla has started its project of spreading out Bangla throughout the internet.
To add Bangla words, you'll have to go

to http://translate.google.com/community. Once you've accessed the site, you'll have to select the language right at the start. Then, you can contribute to the translation services in two key ways: you can either add new words to the 'Translate' segment or you can go to the 'Validate' section and review the translations that are already there and can correct mistakes. To spread out word about the initiative, GDG Bangla is organizing workshops in various educational institutes. Those interested to participate in the project can visit http://goo.gl/WuXLKp to know more.

KASPERSKY SECURITY UPDATE

The greatest heist of the century
Hackers stole USD 1 Billion

In order to infiltrate the bank's intranet, the attackers used spear phishing emails, luring users to open them, infecting machines with malware. A backdoor was installed onto the victim's PC based on the Carberp malicious code, which, in turn gave the name to the campaign — Carbanak.

After obtaining control over the compromised machine, cybecriminals used it as an entry point; they probed the bank's intranet and infected other PCs to find out which of them could be used to access critical financial systems.

That done, the criminals studied the financial tools used by the banks, using keyloggers and stealth screenshot capabilities.

Then, to wrap up the scheme, the

hackers withdrew funds, defining the most convenient methods on a case-by-case basis, whether using a SWIFT transfer or creating faux bank accounts with cash withdrawn by 'mules' or via a remote command to an ATM.

On average, it took from two to four months to drain each victim bank, starting from the Day 1 of infection to cash withdrawal.

TECH BITS

Android Lollipop lets you tweak some settings using voice commands

Samsung teases that the 'Next Galaxy' is borderless and metal

Google's staring down the barrel of a Russian antitrust probe

BlackBerry's latest update brings Amazon Appstore to its phones

Microsoft will soon help you find friends with Windows phones