Asia in the crosshairs of APT attackers: FireEye CTO

By Gabey Goh

Published: 2015-07-26 · Archived: 2026-04-05 21:07:17 UTC

IT is going to be a 'fun' upcoming decade for cybersecurity practitioners in Asia, as the rising wave of attacks and the awareness of them in the region reflect what happened in the United States 10 years ago.

"Asian organisations are right in the crosshairs of today's APT (advance persistent threat) attackers," FireEye chief technology officer Grady Summers said at the RSA Conference Asia Pacific & Japan (RSAC APJ) 2015 in Singapore last week, citing research conducted by his security software firm.

About 37% of FireEye's customers in Asia Pacific detected advanced cyber-attacks in the second half of 2014, and are 33% more likely to be targeted than the global average of 27%.

Speaking to Digital News Asia (DNA) on the sidelines of the conference, Summers said that in terms of IT maturity, Europe was about five to six years behind the United States while Asia was about 10 years behind.

"Ten years ago in American IT, it was all about cost-cutting. Outsource all your IT to India, and we were getting 10-20% cost cuts year on year, but after a while you ran up against a brick wall in terms of security – and that forced a lot of change.

"There are a lot of factors at play and IT is now being seen as a driver of business, so we are seeing budgets creeping up again.

"Asia as a region can be averse to spending money on IT and security, but the trend has to reverse in the next few years because you can't solve this problem with cost cutting," he said.

Summers said that FireEye recently closed a deal with a government agency in Indonesia.

"We're seeing countries like Indonesia, Vietnam and Malaysia picking up our technology, and I feel that that's a sign that companies in Asia are getting it. You always expect countries like Hong Kong or Singapore to be leaders, but many second-tier markets are investing as well," he said.

When pointed out that FireEye's solutions are priced at a premium compared with other similar vendors in the market, Summers agreed, but said that the company's products reflect the money paid for them.

"We're very cognisant of the security poverty line out there, where not all companies will spend the investment, but to stay on top of these attackers takes a huge R&D (research and development) budget.

"If you look at our financials, you'll see that we spend triple the amount versus our competitors, and it shows in our detection rates – we are regarded as one of the best," he claimed.

In addition, the talent shortage of qualified security professional globally and in the region has seen the rise of service models being the preferred approach for many companies.

"Our 'FireEye as a service' model has really gained a lot of traction, especially in Asia, with many companies realising they might not be able to hire eight security resources, but they can hire us," said Summers.

"While the price tag may be big, when compared with hiring an entire team internally, the cost becomes quite competitive," he added.

The China APT party

In April, FireEye released a report on APT30 (Advanced Persistent Threat No 30), which detailed the work of a highly organised, efficient and well-funded team of attackers whose work spanned a decade.

"APT30 deployed customised malware for use in specific campaigns targeting Asean (Association of South-East Asian Nations) members or nations with close ties or interests aligned with Asean states, in January 2013 and April 2013.

"APT30 appears to focus not on stealing businesses' valuable intellectual property or cutting-edge technologies, but on acquiring sensitive data about the immediate South-East Asia region, where they pursue targets that pose a potential threat to the influence and legitimacy of the Chinese Communist Party," FireEye said in the report.

Summers ***(pic)*** said the company was confident in publicly suggesting that the Chinese Government was funding these efforts, given that the timing, issues, targets and types of data phished reflect the interests of the state, in addition to indicators present in the malware itself.

FireEye had also discovered other APT campaigns recently active in the region, according to Summers.

A group dubbed APT4 is suspected to be behind a breach of an Asian airline company discovered in the second quarter of this year. Its attack style uses well-written and researched 'spear-phishes' with industry themes. The attacks were aimed at public key infrastructure targets.

Spear-phishing is an attack geared at acquiring confidential information from a specific individual or organisation.

Another group, APT10, active in the last few months, is believed to be behind the compromise of an East Asian manufacturer and two Japanese public policy organisations.

A common attack style used by the group leverages videogame-themed phishing emails, primarily *Angry Birds* and *Block*, which install a trojanised videogame onto victim's devices.

"We often get asked why think-tanks get targeted and it's important to remember that cyber activity mirrors what you see in real-world tensions," Summers said at the RSA Conference.

"If you see right now the tensions going on between China and Japan with maritime disputes, there's a lot that China can gain by getting inside access into who is influencing legislation and what might Japan's public policy stance be on this, in order to anticipate and head off any strategy deployed," he added.

According to Summers, the phishing emails are poorly worded and minimally researched, while other malware used is commonly self-signed and suffers from high detection rates by commercial antivirus software.

"This group is sloppier than other APT groups we're been studying but it's still very effective as it only takes one successful spear-phishing attack to gain access," he said.

In April, there was an attack against a South Asian defence contractor and the APT5 group managed to steal e-mails, procurement bids and proposals, documents on UAVs (unmanned aerial vehicles), and proprietary product specifications.

Summers said this particular group was highly capable. It had initially gathered reconnaissance information from compromised hosts, and had been focusing on signals intelligence technologies by targeting telecommunications, information technology, and defence companies.

APT17, a group which Summers described as "clever," targeted a popular Japanese software company in March.

It first stole the company's product source code, along with the code-signing certificate, and then compromised the company's website. The group wrote in its malware into the source code, signed the modified software, and posted it for customers to download.

That attack leveraged Blackcoffee malware, which supports a range of a command-and-control functions including creating a reverse shell, uploading and downloading files, and enumerating files and processes.

The work of APT17 prompted a more comprehensive report by FireEye, highlighting how threat actors have found a new way to dodge security professionals using popular websites' legitimate functionalities to hide their hacking operations.

FireEye Threat Intelligence and the Microsoft Threat Intelligence Centre investigated a command-and-control (C+C) obfuscation tactic used on Microsoft's TechNet, a web portal for IT professionals.

The report found that TechNet's security was not compromised by this tactic, which is likely possible on other message boards and forums.

APT17 was embedding the encoded C+C IP address for the Blackcoffee malware in legitimate Microsoft TechNet profiles pages and forum threads, a method some in the information security community call a "dead drop resolver."

Encoding the IP (Internet Protocol) address makes it more difficult for network security professionals to identify the true C+C address.

"We have already observed threat actors adopting similar techniques and moving some C+C activity to legitimate websites that they do not need to compromise," FireEye said in its report.

"In the same vein, some threat actors have already begun using social media sites such as Twitter and Facebook for malware distribution and C+C.

"FireEye expects that threat groups are already using this technique, with their own unique variations, and others will adopt similar measures to hide in plain sight," the report added.

Not just China anymore

Summers told DNA that all case studies presented during his talk at the RSA Conference were believed to be efforts sponsored by the Chinese Government.

"We're often accused [of saying] 'Oh it's always China,' but my response is, we're tech guys and we just report what we find.

"The fact is, is that we don't even do that much business with the US Government, so it's not like we have an agenda with this," he said.

Asked about the potential rationale for a nation such as China to devote so much monetary resources to such efforts, Summers said, "The fact is, a little bit goes a long way in cyberspace."

"Back when I was working at General Electric, management asked me once what it would take to build a world-class intrusion team that could knock over any Fortune 500 company, and what would it take to defend against it.

"The asymmetry is incredible – for a million bucks I could assemble a team that could take down any major corporation, but to defend against it? Two million doesn't even scratch the surface. I could spend 100 million, and it still won't be fool-proof.

"The point I'm trying to make is that this is a stated strategic goal of China's, so to put a few billion dollars behind it, I can guarantee that the payoff is many times over in terms of the intellectual property and information stolen," he argued.

Summers also reported that in the past 12 months, the APT space had got more diverse, with groups emerging from different geographies.

"Now we're seeing countries like Iran, North Korea and Syria getting in the game," he said.

"There's an increasing diversity in the threat actors that are coming up, so it's not just about groups from China anymore, though they remain the most prolific and brazen," he added.

Next Up: Plugging the gaps

Related Stories:
