How attackers hide backdoor in software used by companies

DUBAI: Kaspersky Lab experts have discovered a backdoor planted in a server management software product used by hundreds of large businesses around the world. When activated, the backdoor allows attackers to download further malicious modules or steal data. Kaspersky Lab has alerted NetSarang, the vendor of the affected software, and it has promptly removed the malicious code and released an update for customers.

ShadowPad is one of the largest known supply-chain attacks. Had it not been detected and patched so quickly, it could potentially have targeted hundreds of organizations worldwide.

In July, 2017 Kaspersky Lab's Global Research and Analysis (GReAT) team was approached by one of its partners - a financial institution. The organization's security specialists were worried about suspicious DNS (domain name server) requests originating on a system involved in the processing of financial transactions. Further investigation showed that the source of these requests was server management software produced by a legitimate company and used by hundreds of customers in industries like financial services, education, telecoms, manufacturing, energy and transportation. The most worrying finding was the fact that the vendor did not mean for the software to make these requests.

Further Kaspersky Lab analysis showed that the suspicious requests were actually the result of the activity of a malicious module hidden inside a recent version of the legitimate software. Following the installation of an infected software update, the malicious module would start sending DNS-queries to specific domains (its command and control server) at a frequency of once every eight hours. The request would contain basic information about the victim system (user name, domain name, host name). If the attackers considered the system to be "interesting", the command server would reply and activate a fully-fledged backdoor platform that would silently deploy itself inside the attacked computer. After that, on command from the attackers, the backdoor platform would be able to download and execute further malicious code.

Following the discovery, Kaspersky Lab researchers immediately contacted NetSarang. The company reacted fast and released an updated version of the software without the malicious code.

So far, according to Kaspersky Lab research, the malicious module has been activated in Hong Kong, but it could be lying dormant on many other systems worldwide, especially if the users have not installed the updated version of the affected software.

While analyzing the techniques used by the attackers, Kaspersky Lab researchers came to the conclusion that some of them are very similar to ones used previously by the PlugX and Winnti groups, which are known to be Chinese-speaking cyber espionage groups. This information, however, is not enough to establish a precise connection to these actors.

"ShadowPad is an example of how dangerous and wide-scale a successful supply-chain attack can be. Given the opportunities for reach and data collection it gives to the attackers, most likely it will be reproduced again and again with some other widely used software component. Luckily NetSarang was fast to react to our notification and released a clean software update, most likely preventing hundreds of data stealing attacks against its clients. However, this case shows that large companies should rely on advanced solutions capable of monitoring network activity and detecting anomalies. This is where you can spot malicious activity even if the attackers were sophisticated enough to hide their malware inside legitimate software," said Igor Soumenkov, security expert, Global Research and Analysis Team, Kaspersky Lab.

NetSarang Statement

"To combat the ever-changing landscape of cyber attacks NetSarang has incorporated various methods and measures to prevent our line of products from being compromised, infected, or utilized by cyber espionage groups. Regretfully, the Build release of our full line of products on July 18th, 2017 was unknowingly shipped with a backdoor which had the potential to be exploited by its creator.The security of our customers and user base is our highest priority and ultimately, our responsibility. The fact that malicious groups and entities are utilizing commercial and legitimate software for illicit gain is an ever-growing concern and one that NetSarang, as well as others in the computer software industry, is taking very seriously.

NetSarang is committed to its users' privacy and has incorporated a more robust system to ensure that never again will a compromised product be delivered to its users. NetSarang will continue to evaluate and improve our security not only to combat the efforts of cyber espionage groups around the world but also in order to regain the trust of its loyal userbase."

SMBs prioritize managing risk over winning customers

DUBAI: Running any business can be tough, but small and growing companies face particular challenges. Kaspersky Lab research shows that, in a world of rapidly evolving IT security threats and market volatility, companies with fewer than 100 employees are prioritising the management of risk ahead of innovation (39%), gaining new customers (37%) and becoming a digital business (35%).

Eugene Kaspersky

To help such businesses address their concerns, some of Kaspersky Lab's top managers, including the CEO, Eugene Kaspersky, have joined forces to share their personal thoughts on the key challenges facing smaller companies. The result, 'Take 10 minutes: Insight on big decisions for small businesses' is a collection of comments, quotes, advice, lists and more, illustrated with examples of Kaspersky Lab's own experience. Published to mark Kaspersky Lab's 20th birthday, the guide offers personal perspectives on leadership, finance, risk, recruitment, innovation, competition and IT - as well as favourite business quotes and top books.

The insight includes:

- How to convince financial backers you're worth investing in, and what to spend your money on.
- Why you should approach success with caution, especially in the early days.
- Why you should always listen to customers but not become over-dependent on them.
- Why some employees will not be ready to grow with the business.
- How to overcome the fear of failure.
- How to recognise when competitors are allies.
- Why you should never recruit someone who's perfect at the job and more.

Eugene Kaspersky, chairman and CEO of Kaspersky Lab, said: "When you run a business, every day brings new challenges and opportunities - and they all have something of value to teach you. Over 20 years, we've learned so much! And now we'd like to share some of that insight and experience with you. The journey from startup to global enterprise is a tough one -but also an exhilarating and rewarding one."

Copies of Take 10 minutes: insight on big decisions for small businesses can be downloaded from link.

Uber settles complaint over data protection for riders, drivers

WASHINGTON: Uber agreed to implement new data protection measures to settle complaints that it failed to prevent improper snooping on driver and customer information, officials said Tuesday.

The ridesharing giant had faced complaints that it allowed some employees to use the "God view" to monitor customer movements that could allow Uber managers to keep tabs on journalists investigating the ridesharing giant.

A separate complaint said that Uber had also failed to prevent a data breach that allowed hackers to gain access to personal information on some 100,000 drivers.

The Federal Trade Commission announced a settlement on an investigation into allegations that Uber failed to live up to data protection claims. It requires Uber to submit to independent privacy audits every two years for the next 20 years.

"Uber failed consumers in two key ways: First by misrepresenting the extent to which it monitored its employees' access to personal information about users and drivers, and second by misrepresenting that it took reasonable steps to secure that data," said FTC acting chairman Maureen Ohlhausen in a statement.

"This case shows that, even if you're a fast growing company, you can't leave consumers behind: you must honor your privacy and security promises."

Ohlhausen said the agency began its investigation in response to a "consumer uproar" over reports that Uber executives used "God view," indicating the whereabouts of riders, for parties and other purposes.

"We've always treated geolocation as sensitive information," Ohlhausen told a conference call.

The settlement contains no financial penalty, but Uber agreed to implement "a comprehensive privacy program" that will include independent audits, the FTC said. If it fails to live up to the agreement it could face fines.

The agency which enforces consumer and privacy protection said Uber had announced in November 2014 — but failed to enforce-a "strict policy" prohibiting employees from accessing rider and driver data except for legitimate business purposes.

The FTC added in a statement that Uber "did not take reasonable, low-cost measures" that could have prevented a breach by using better practices to protect data in the internet cloud. — AFP

Chinese teen internet addict dies after rehab

BEIJING: A Chinese teen has died after spending less than 48 hours at a centre that treats internet addicts, shining a spotlight on the controversial facilities that seek to unlatch people from their screens.

The first country to declare internet addiction a clinical disorder, China is estimated to be home to millions of primarily young men who spend hours online.

The parents of Li Ao, 18, had tried everything they could think of to cure his internet addiction: showing him the ropes of the family business, encouraging him to join the military and taking him on trips around the country.

But after none of these methods produced results, they decided to pay 22,800 yuan ($3,414) for 180 days of "closed, isolated special education" at the rehab centre.

The school had promised to use a combination of psychological treatment methods and military training, Li's parents told state channel CCTV on Sunday.

While the cause of Li's death remains unknown, his father Li Tao and mother Liu Dongmei told CCTV that the school called them just a day and a half after they had dropped off their son to say that the younger Li was in the emergency room.

By the time they arrived at the hospital, Li had already been moved to the morgue, where his parents found his body covered with scars.

"The teachers at the centre told us that their teaching style was very nurturing. They said they never beat kids or used corporal punishment," Liu Dongmei recalled to CCTV.

"But when I saw my son's body there were bruises all over his arms and legs."

According to CCTV, the school, located near the provincial capital of Hefei, was unlicensed and had already been directed several times by the local government to halt its operations.

"Now I just want the authorities to investigate and expose the truth of my son's death," said Li Tao. — AFP

BERLIN: People watch German chancellor Angela Merkel during a live interview with four of the most famous German Youtubers, yesterday in Berlin. — AFP

Merkel reaches out to young voters on YouTube

BERLIN: German Chancellor Angela Merkel, campaigning yesterday for the youth vote on YouTube ahead of September 24 elections, said her favourite emoticon was the "smiley" and dismissed fears about a potential World War III.

The 63-year-old leader, in power for nearly 12 years, also said she hoped to appoint equal numbers of male and female ministers from her conservative party if she wins a fourth term, though she could not speak for possible coalition partners.

In interviews with four young German YouTube personalities, including beauty, technology and politics video-bloggers, she spoke about issues ranging from refugees to climate and the importance of casting one's ballot.

She said her government would push on with the promotion of environmentally friendly electric cars, revealing that her main media spokesman drives one but that she could not because no automaker had yet manufactured an armoured model.

She confided that her favourite emoticon was the smiley, sometimes with a heart attached. Asked about the more serious issue of whether North Korea tensions and other international conflicts threatened to escalate into "World War III", she responded with a firm "no", adding that "we can avert such catastrophes". Speaking about North Korea and the role of US President Donald Trump, Merkel said "we must be very careful with language, generally.

"Language can be the precursor to an escalation that, somewhere down the road, could lead to violence." — AFP

From Isaac Asimov to Aimee Mann, 'robophobia' plagues humans

CINCINNATI: Robots are secretly plotting to kill us. Or enslave us. Or, at best, they will take our jobs, one by one. From science fiction written by Isaac Asimov eight decades ago to "Dilbert" cartoons today, the relationship between robots and humans has long fascinated - and worried - people.

There's even a term, "robophobia," for an irrational anxiety about robots and other advanced automation machines. And there are concerns beyond the ones stoked by watching too much "Terminator ." Apple computer pioneer Steve Wozniak once suggested that robots would turn us into their pets . Physicist Stephen Hawking and tech entrepreneur Elon Musk have also warned about the dangers of going too far, too quickly, in developing "thinking robots" with programmed intelligence that might keep evolving self-awareness, similar to the humanoids in the HBO series "Westworld ."

Hawking told the BBC in 2014 that "development of full artificial intelligence could spell the end of the human race." So there's that. Researchers vary in projections on how long from now, if ever, such a threat could exist. For now, deaths by robot are very rare among industrial accidents. However, in July 2015, a 57-year-old technician was killed by a robotic machine in an Ionia, Michigan, plant that makes auto bumpers, trailer hitches and chrome-plated plastics. Her husband filed a federal lawsuit, being contested by the defendants, alleging a malfunctioning robot took her "by surprise," crushing her head.

As chief technology officer for a private-public effort to facilitate robotic solutions in US manufacturing, professor Howie Choset of Carnegie Mellon University in Pittsburgh sees the fear of robots taking jobs making his mission tougher.

"You have to start this discussion with the baseline that automation and innovation creates jobs," he said, by leading to new products and processes and the new jobs to make and operate them.

"Then you have to ask yourself, why would robots be different? And people are very quick to say, 'Well, robots are intelligent, they do what humans can do,' and there's this fear that was sort of instilled by science fiction."

Comparing fear of robots to 19th-century worries about the impact of steam engines, Choset said: "Robots are just the next generation of tools." Singer Aimee Mann, with help from actress Laura Linney, humorously depicted the danger of letting robots help you too much in this music video. And Choset was amused by a recent "Dilbert " strip about the boss' inability to stop a robot worker who decided to quit.

Chris Boggess, 18, found the 2004 movie "I, Robot ," about a rogue killer robot drawn from Asimov stories, frightening, but he has come to understand and appreciate their potential through the Butler Tech robotics program at Colerain High School near Cincinnati.

"The first day I walked in, I fell in love. I knew this was where I needed to be," Boggess said. "I like robots, anything about technology." And if some day thinking robots acquired the ability to threaten humans, he said, "I would probably try to make friends with them." — AP

CAMBRIDGE: In this Oct 24, 2014 file photo, researchers Randall Briggs, left, and Will Bosworth monitor a robotic cheetah during a test run on an athletic field at the Massachusetts Institute of Technology in Cambridge, Mass. MIT scientists said the robot, modeled after the fastest land animal, may have real-world applications, including development for prosthetic legs. — AP