internet.watch.impress.co.jp

Pension mechanism tip of the iceberg, at least 300 places in the invasion already, also cloud operators to news agencies

June 4, 2015 • 1 min read • original

Ltd. Kaspersky is the 4th, we held a press briefing for the "Blue Termite (Blue ter Might)" APT, which is named (Advanced Persistent Threat) attack.

Blue Termite

Blue Termite is an APT attack the Japan 100% targeted, while the cyber attacks on Japanese pension mechanism also that it part of such efforts, the target is emphasized that it is "Japan as a whole" rather than by the same mechanism. It is assumed only attack is discovered in the same mechanism by chance thanks to information has been leaked, including the government agencies and news organizations, defense-related, energy-related, aerospace, financial, chemical,

manufacturing, research and academic institutions, further Until cloud servers of information and communication business, it revealed that at least 300 sites have been invaded by malware Blue Termite.

Rintaro Mr. Kawai Inc. Kaspersky President

Jie Mr. Ishimaru Inc. Kaspersky information security lab security researcher

Blue Termite is one of the attacks that the attacker group called "CloudyOmega (Claudio mega)" is deployed. The targeted attacks-mail and malware have been last fall, reported by Symantec and Trend Micro.

For example, in an e-mail that the source is "health insurance union secretariat", the file is attached that was disguised as a Word document file "Notice of health insurance", actually a self-extracting executable

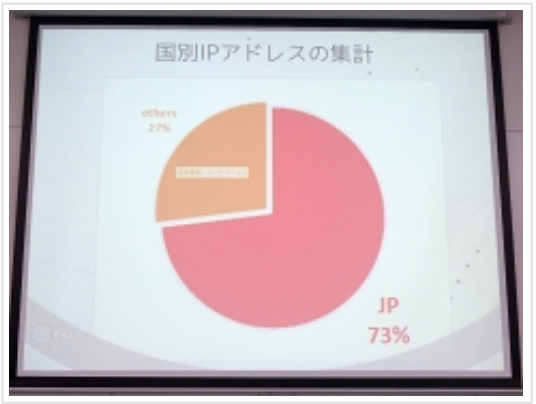
file (.exe) at is, when will open this, infection with malware of the body is executed in the back that Word document of the dummy is displayed. And it initiates communication with the attacker's command server (C & C servers) to perform activities such as information theft.

According to Kaspersky Lab's observation, communication to the C & C server is generated from last year September 18, 10, but in December there was also time to more than 100 cases per day, then, calm down. But later this year in April, it becomes active again, that came out some days there are more 140 when many.

In addition, where it was classified communication source of the IP address, but of which 27% were anti-virus vendors and virtual environment for automatic analysis, such as that carried out the malware analysis, that 73% is occupied by the Japanese organization have you found. It says that it only has to analyze about half of the observed data in the Kaspersky Lab, still the

organization more than 300 locations in Japan, you have to be the thing that has been invaded by this malware.

Note that this figure are those based on the number of unique IP addresses, it is going to be considered when using multiple IP addresses at the same organization. Also, its not always have evolved into activities such as information theft at all say (do not know), but, at least, malware is successful in the invasion, C & C number organization of considerable communication with the server has occurred I would that there.



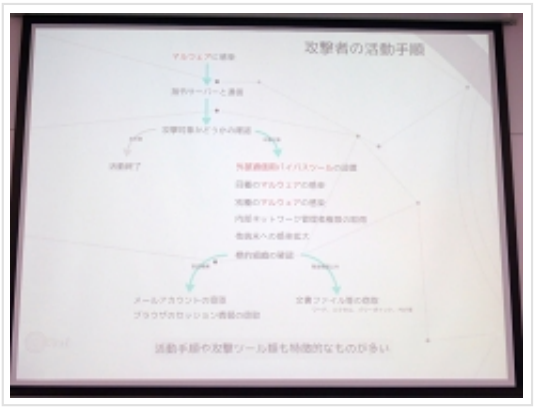
After the malware infection, it called for confirmation of whether the environment is or attack. Directories and files in the PC, and to reference the operation to that

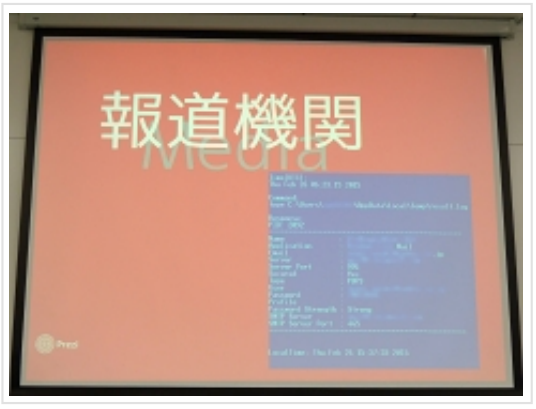
process, and ends the activity if it is determined not to be attacked. This corresponds the environment, such as the above-mentioned anti-virus vendor.

On the other hand, if it is determined that it is attacked, dropping hacking tools or similar, another type of malware, the acquisition of internal network management authority, in addition to performing activities such as spread to other terminals, the type of compromised tissue is also discriminated . Stealing your mail account and browser session information if it is determined that the news media, to try to steal sensitive information such as a document file if it is determined that that he except news agency.

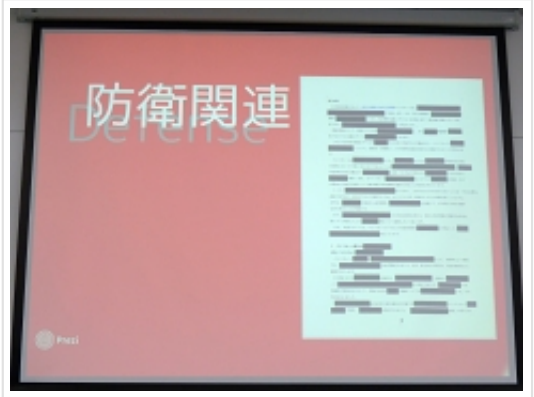
Kaspersky at a press briefing, introduction and content of the theft has been e-mail account information from news organizations, energy-related, defense-related, the case of sensitive information, such as manufacturing. As a case that is likely to further the most damage is large, it was introduced that there was a case that had been access to the Windows system directory in the information communication business.

And that in a business that provides cloud services, believed to have been stolen until the administrator authority of the mission-critical server body.

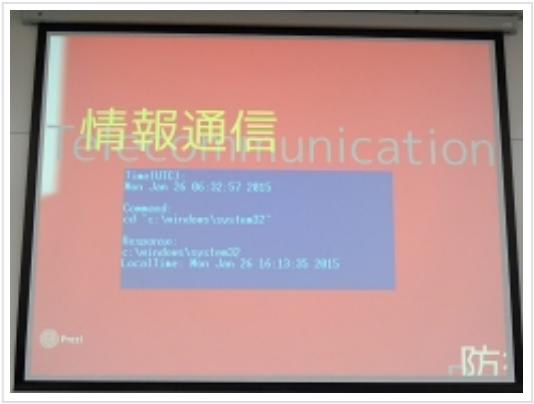




In fact, the



customer web site that is operating on its cloud service, Blue Termite C & C server is installed a large number, it is found that Kaspersky Lab has 80 reviews alone was able to parse domain has been abused It is other,



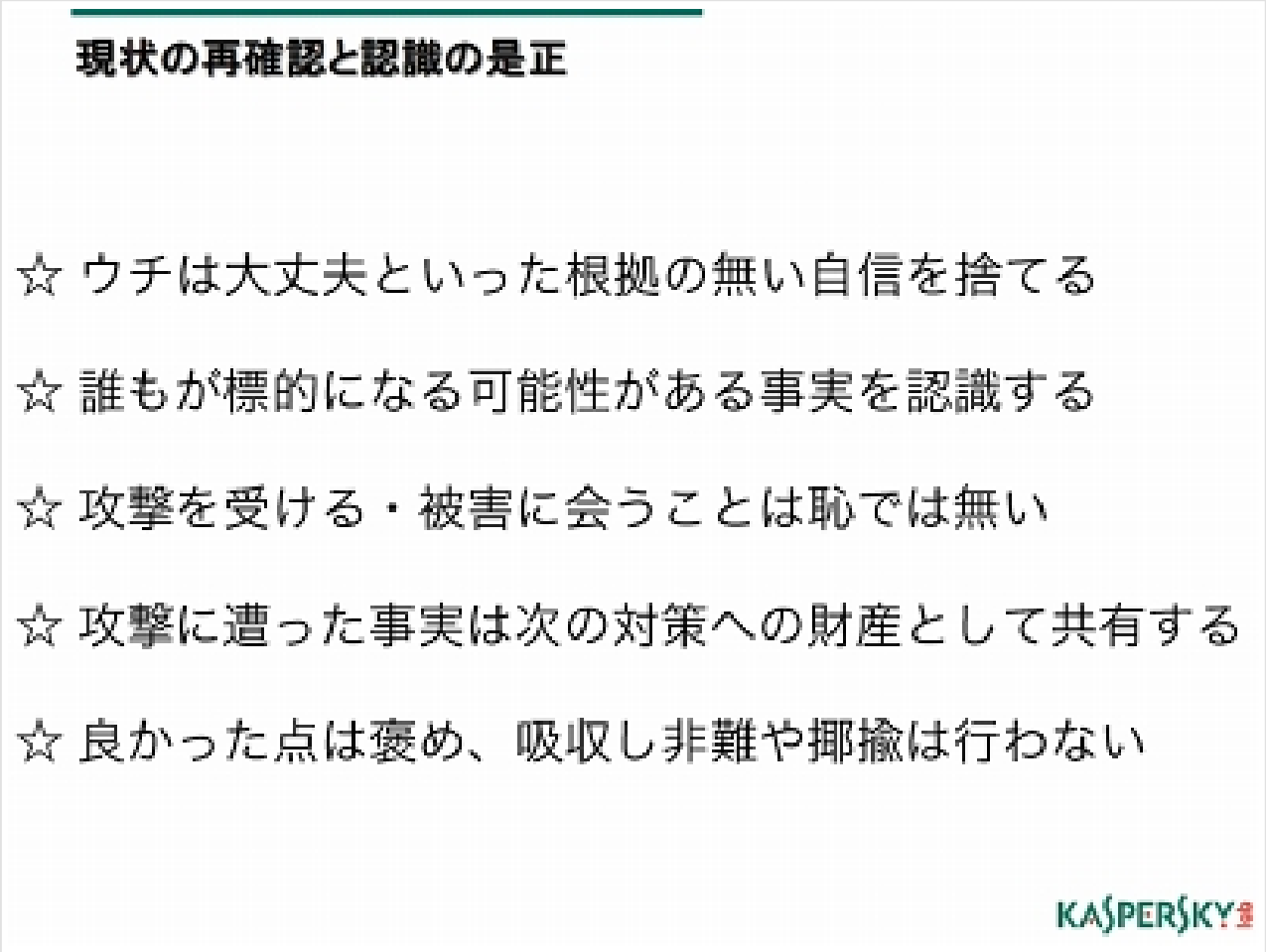
domestic several thousand domain in May point in time you have to be in the hands of the attacker.

C & C servers but were often placed abroad far, Blue those domestic C & C servers in Termite is used, the ratio is up to 93%. The communication of malware that had penetrated into the tissue, and that is difficult to judgment and cut off by the standard of overseas server.

The Blue Termite information of cloud services business who are under attack of, already it is assumed has to offer from Kaspersky Lab to the police, that should know at least the operators. However, at present business who announced that its I have not even one company.

In Kaspersky Lab, behavior after infection of these malware, back doors and hacking tools are using, from the commonality of the C & C server, cyber attacks on this time discovered the Japan pension mechanism, a series of Blue Termite that has continued from last fall

Description and was determined to be a part of the attack. "Our will discard the confidence unfounded such as okay, everyone recognizes the fact that there is likely to be a target," it can be appealed the need.

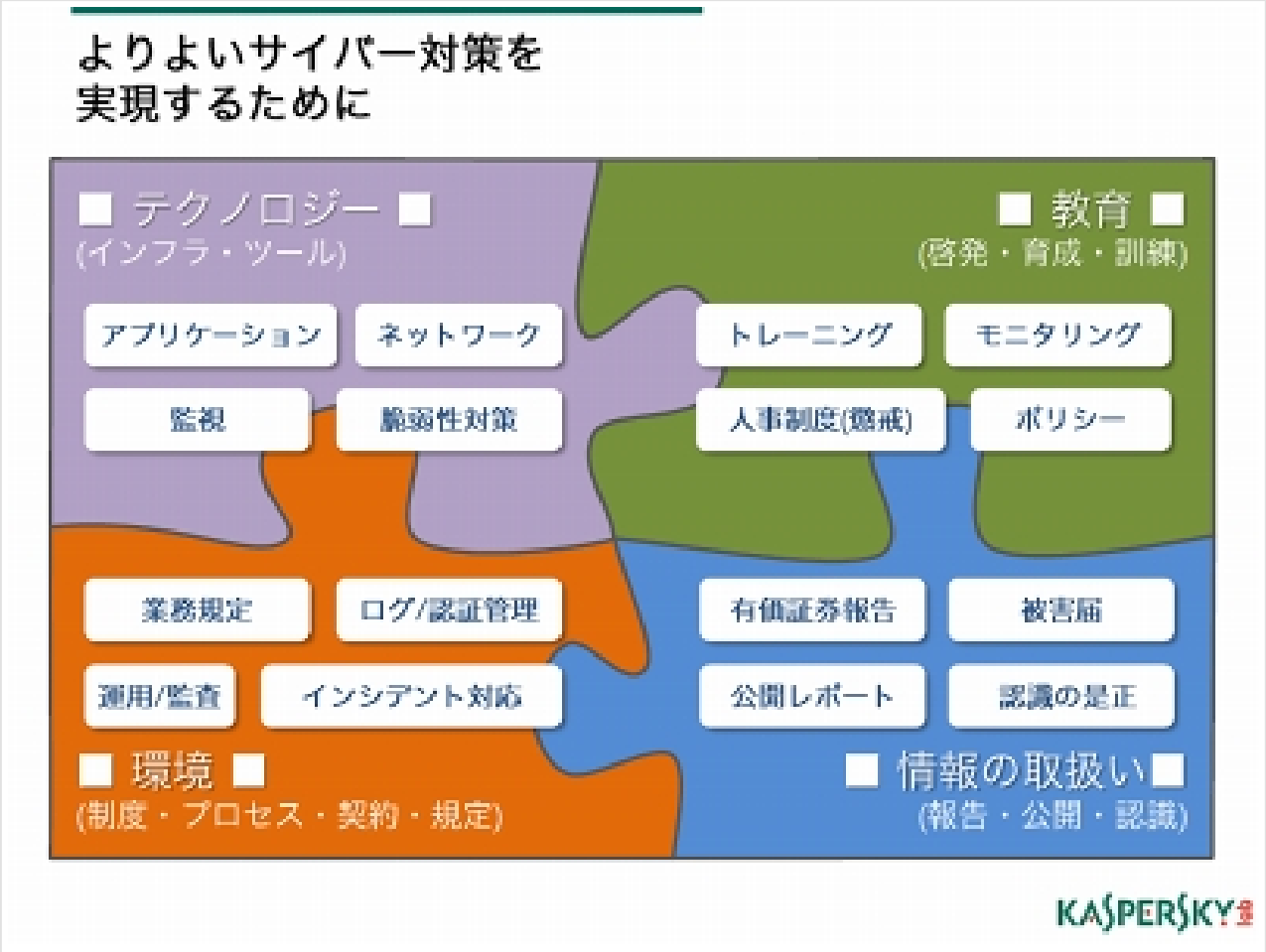


テクノロジーの観点からの対策

- 最後の砦であるエンドポイント対策を見直す
- 脆弱性対策を導入する
- メールの設定を見直す
  (.exeはデフォルトで削除ないし隔離)
- セキュリティコンサルティングを実施し、
  現状の設計/環境/運用の確認と評価

1件のインシデントで発生するコストは
中小企業の平均で $56,000、
大企業では $649,000

KASPERSKY



It is to be noted that it is assumed to be suspect infection If impersonation files and malware names, such as the following, the tool is found in the PC.

because in some cases the same name of the file exists, but is not that these are found PC is sure to infection, that it is better to suspected infection

In addition, the malware used in the Blue Termite is, in the Kaspersky Lab product to detect the name, such as the following.

Detection name in the Kaspersky Lab products

Original URL:
http://internet.watch.impress.co.jp/docs/news/20150604_705541.html