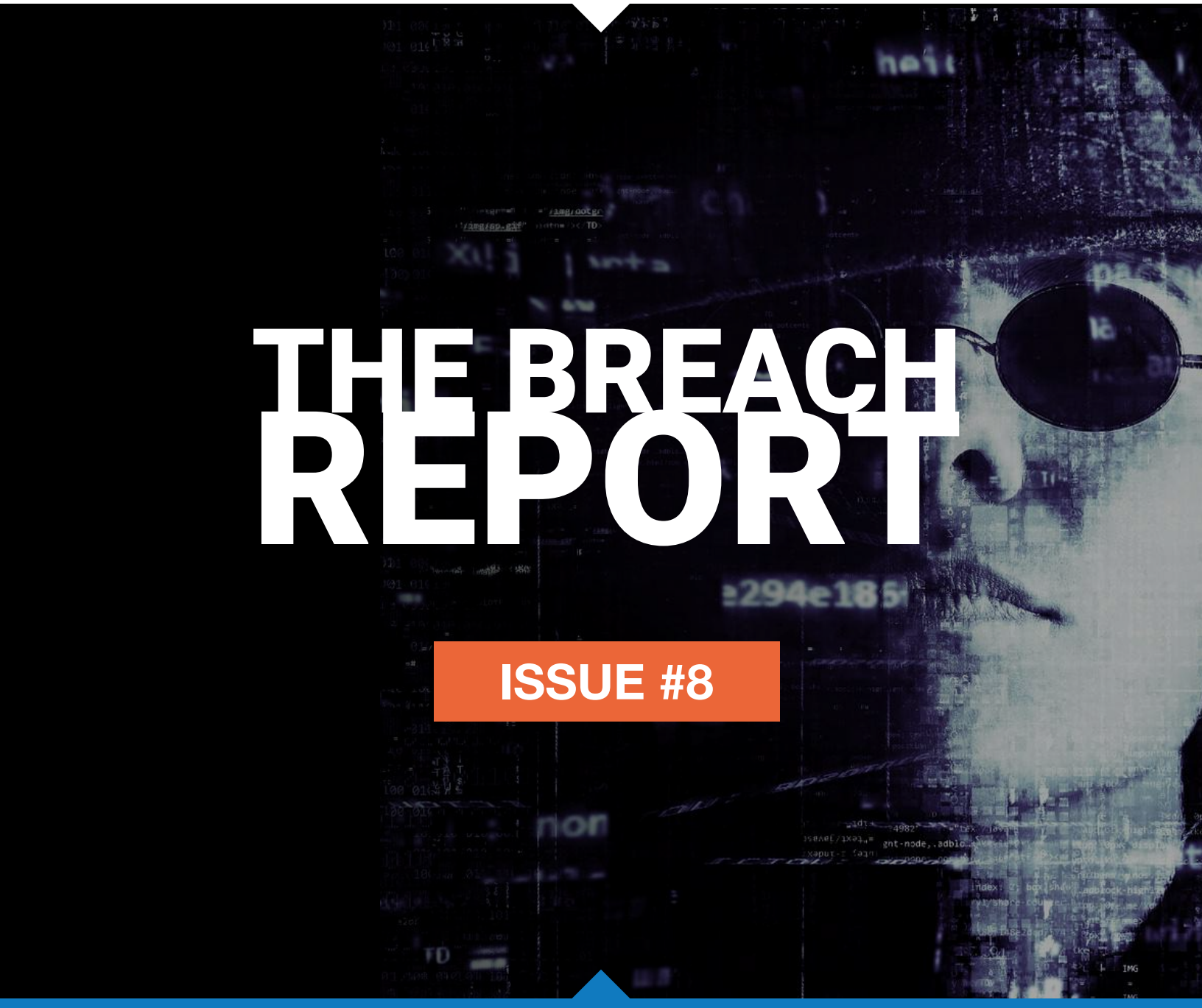
CALIAN®



THE BREACH REPORT

ISSUE #8

www.calian.com
1.877.225.4264 | 770 Palladium Drive, Ottawa, ON, K2V 1C8

The Background

In today's digital business environment, enhanced and holistic cyber security is essential. However, many companies continue to struggle with resilience, often experiencing breaches that lead to everything from compliance issues, to lost and stolen data and, ultimately, to brand damage and revenue loss. And though it is easy to read about these breaches, the causes and potential solutions are rarely identified.

It is for these reasons that Calian has created the Breach Report. Each month, we spotlight a particular type of company, the breach it has experienced, and what it could have done to mitigate risk against the specific type of cyber attack—all to create better insight for the general public and to educate people on proper cyber security best practices.

In this month's report, we spotlight a scandalous hacking operation: It is alleged that to enable COMAC, a Chinese state-owned aerospace manufacturer, build a C919 airplane, the Ministry of State Security (MSS) tasked the Jiangsu Bureau (MSS JSSD) to acquire the needed intellectual property to manufacture all of the C919's components inside China.

The Company Profile

Commercial Aircraft Corporation of China, Ltd. (COMAC) functions as the main vehicle in implementing large passenger aircraft programs in China. It is also mandated with the overall planning of developing trunk liner and regional jet programs and realizing the industrialization of civil aircraft in China. COMAC is engaged in the research, manufacture and flight tests of civil aircraft and related products, as well as marketing, servicing, leasing and operations of civil aircraft.

The C919 aircraft is a large civil jet aircraft independently developed by China in accordance with international civil aviation regulations, and owns independent intellectual property rights (COMAC website).

The Environment

In its report, CrowdStrike, a cybersecurity technology company, exposed one of China's most scandalous hacking operations that involved Ministry of State Security officers, the country's underground hacking scene, legitimate security researchers, and insiders at companies all over the world. The aim? To acquire intellectual property so COMAC could build the C919 airplane, enabling it to compete with Airbus and Boeing. The hacking operation was a coordinated multi-year campaign that systematically went after those foreign companies that supplied components for the C919—they wanted to manufacture all of the plane's components inside China (as cited in Cimpanu, 2019).

Without the hacking operation, known as Turbine Panda, it would have been impossible for COMAC to adhere to the development principles of "Chinese design, system integration, global tendering, and gradual promotion of domestication," and to follow the technical route of "independent development, international cooperation, and international standard" (as stated in its company description). Between 2010 and 2015, the hacking team successfully breached C919 suppliers like GE, Safran, Ametek, Honeywell, Capstone Turbine, and others. To find proprietary information and exfiltrate it to remote servers, Turbine Panda deployed malware such as Sakula, PlugX, and Winnti, (as cited in Cimpanu, 2019).

The Outcome

As the C919 relies heavily on components from a long supply chain of foreign suppliers, the cyber-enabled espionage launched by Turbine Panda focused on compromising CFM International's supply chain—targeting several aerospace companies using multiple hacking techniques spread over five years. Basically, Turbine Panda attacked the weaker links in the supply chain; therefore, when large corporations were too well defended, they attacked the smaller component suppliers (Scroxton, 2019).

The MSS JSSD's hackers eventually made a mistake. They went after too big a target—healthcare provider Anthem and the US Office of Personnel Management (OPM)—and caught the attention of the US government. Foreign company insiders were the first to go, then the hacker Yu was arrested when he attended a security conference in Los Angeles and charged for his involvement in the Anthem and OPM hacks. This triggered the Chinese government to prohibit Chinese researchers from participating in foreign security conferences.

Finally, a high-ranking Chinese intelligence officer was arrested—he was the MSS JSSD officer in charge of recruiting insiders at foreign companies.

The Potential Risk

The attacks on aviation companies will probably continue as COMAC's C919 hasn't been successful and a fully Chinese manufactured airliner is still many years away. Since Turbine Panda appears to have disappeared from the scene, other Chinese cyber espionage groups have appeared: Emissary Panda, Nightshade Panda, Sneaky Panda, Gothic Panda, Anchor Panda, and many more.

For years, it's been reported that China has built its economical might on the backs of other countries and foreign competitors. So the risk of further attacks is almost a given, especially considering that "Chinese hackers often helped with 'forced technology transfer,' breaching business partners and stealing their intellectual property, allowing the Chinese state-owned companies to put out high-end competing products in record time and at very low prices" (as cited in Cimpanu, 2019).

The Solution

Protect both your intellectual property (IP) and your supply ecosystem against data breaches with Data Loss Prevention (DLP).

Follow your data across networks and devices—both at rest and in use. Create and enforce policies that provision the access and movement of data to prevent data breaches and to help ensure compliance with DLP.

- Data Fingerprinting – Follow data with automatic application of controls even when user devices are not on the network.
- Predefined Policy Library – Get started quickly with an extensive Policy Library that addresses common regulatory and IP protection use cases, including General Data Protection Regulation (GDPR).
- Optical Character Recognition – Enables textual data, including PII and PHI, to be detected and extracted from images such as source codes, engineering drawings, M&A documents and trade secrets.
- Automated Classification & Labeling – Simplify data classification with automated validation and application of labels for sensitive files with Boldon James Classifier and Azure Information Protection.
- Advanced Incident Workflow – Secure workflow notifications for data owners, providing users role-based access and data privacy on their mobile devices with DLP.
- Single Console Control – Set DLP policies across your network and endpoints once from a single console for your environment.
- Gain Visibility into Microsoft Rights Management – Enable Microsoft Protection RMS to securely share information with partners. Automatically encrypt and decrypt using Microsoft Azure Information Protection.
- Achieve Risk-adaptive Protection – Leverage DLP within the Dynamic Data Protection solution to achieve automatic policy enforcement in a matter of seconds.
- Educate Data Owners to Protect Data – Dynamic in-action coaching to educate end-users on appropriate data use while using Forcepoint's DLP tool.
- Data Leakage Prevention – Detect and protect against low and slow data exfiltration and data leakage via print, email, cloud applications, and removable media.

Contact us for a **free consultation or to receive a free cloud security audit** to assess the effectiveness of your current cyber security initiatives.

1.877.225.4264

www.calian.com

CALIAN®

References

Cimpanu, Catalin (2019, October 14). *Building China's Comac C919 airplane involved a lot of hacking, report says*. Retrieved from https://www.zdnet.com/article/building-chinas-comac-c919-airplane-involved-a-lot-of-hacking-report-says/

Scroxton, Alex (2019, October 14). *Researchers reveal the cyber campaign that built China's new airliner*. Retrieved from https://www.computerweekly.com/news/252472244/Researchers-reveal-the-cyber-campaign-that-built-Chinas-new-airliner

THE BREACH REPORT

ISSUE #8

CALIAN®