Hackers Plundered Israeli Defense Firms that Built ‘Iron Dome’ Missile Defense System

Published: 2014-07-30 · Archived: 2026-04-02 10:42:01 UTC

Three Israeli defense contractors responsible for building the “Iron Dome” missile shield currently protecting Israel from a barrage of rocket attacks were compromised by hackers and robbed of huge quantities of sensitive documents pertaining to the shield technology, KrebsOnSecurity has learned.

The never-before publicized intrusions, which occurred between 2011 and 2012, illustrate the continued challenges that defense contractors and other companies face in deterring organized cyber adversaries and preventing the theft of proprietary information.

A component of the ‘Iron Dome’ anti-missile system in operation, 2011.

According to Columbia, Md.-based threat intelligence firm **Cyber Engineering Services Inc.** (CyberESI), between Oct. 10, 2011 and August 13, 2012, attackers thought to be operating out of China hacked into the corporate networks of three top Israeli defense technology companies, including **Elisra Group**, **Israel Aerospace Industries,** and **Rafael Advanced Defense Systems**.

By tapping into the secret communications infrastructure set up by the hackers, CyberESI determined that the attackers exfiltrated large amounts of data from the three companies. Most of the information was intellectual property pertaining to Arrow III missiles, Unmanned Aerial Vehicles (UAVs), ballistic rockets, and other technical documents in the same fields of study.

Joseph Drissel, CyberESI's founder and chief executive, said the nature of the exfiltrated data and the industry that these companies are involved in suggests that the Chinese hackers were looking for information related to Israel's all-weather air defense system called Iron Dome.

The Israeli government has credited Iron Dome with intercepting approximately one-fifth of the more than 2,000 rockets that Palestinian militants have fired at Israel during the current conflict. The U.S. Congress is currently wrangling over legislation that would send more than $350 million to Israel to further development and deployment of the missile shield technology. If approved, that funding boost would make nearly $1 billion from the United States over five years for Iron Dome production, according to The Washington Post.

Neither Elisra nor Rafael responded to requests for comment about the apparent security breaches. A spokesperson for Israel Aerospace Industries brushed off CyberESI's finding, calling it "old news." When pressed to provide links to any media coverage of such a breach, IAI was unable to locate or point to specific stories. The company declined to say whether it had alerted any of its U.S. industry partners about the breach, and it refused to answer any direct questions regarding the incident.

Arrow 3 launch in January 2014.

"At the time, the issue was treated as required by the applicable rules and procedures," IAI Spokeswoman **Eliana Fishler** wrote in an email to KrebsOnSecurity. "The information was reported to the appropriate authorities. IAI undertook corrective actions in order to prevent such incidents in the future."

Drissel said many of the documents that were stolen from the defense contractors are designated with markings indicating that their access and sharing is restricted by International Traffic in Arms Regulations (ITAR) — **U.S. State Department** controls that regulate the defense industry. For example, Drissel said, among the data that hackers stole from IAI is a 900-page document that provides detailed schematics and specifications for the Arrow 3 missile.

"Most of the technology in the Arrow 3 wasn't designed by Israel, but by **Boeing** and other U.S. defense contractors," Drissel said. "We transferred this technology to them, and they coughed it all up. In the process, they essentially gave up a bunch of stuff that's probably being used in our systems as well."

WHAT WAS STOLEN, AND BY WHOM?

According to CyberESI, IAI was initially breached on April 16, 2012 by a series of specially crafted email phishing attacks. Drissel said the attacks bore all of the hallmarks of the "Comment Crew," a prolific and state-sponsored hacking group associated with the Chinese People's Liberation Army (PLA) and credited with stealing terabytes of data from defense contractors and U.S. corporations.

Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.

From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges.

Image: FBI

The Comment Crew is the same hacking outfit profiled in a February 2013 report by Alexandria, Va. based incident response firm **Mandiant**, which referred to the group simply by it's official designation — "P.L.A. Unit 61398." In May 2014, the **U.S. Justice Department** charged five prominent military members of the Comment Crew with a raft of criminal hacking and espionage offenses against U.S. firms.

Once inside the IAI's network, Comment Crew members spent the next four months in 2012 using their access to install various tools and trojan horse programs on systems throughout company's network and expanding their access to sensitive files, CyberESI said. The actors compromised privileged credentials, dumped password hashes, and gathered system, file, and network information for several systems. The actors also successfully used tools to dump Active Directory data from domain controllers on at least two different domains on the IAI's network.

All told, CyberESI was able to identify and acquire more than 700 files — totaling 762 MB total size — that were exfiltrated from IAI's network during the compromise. The security firm said most of the data acquired was intellectual property and likely represented only a small portion of the entire data loss by IAI.

"The intellectual property was in the form of Word documents, PowerPoint presentations, spread sheets, email messages, files in portable document format (PDF), scripts, and binary executable files," CyberESI wrote in a lengthy report produced about the breaches.

"Once the actors established a foothold in the victim's network, they are usually able to compromise local and domain privileged accounts, which then allow them to move laterally on the network and infect additional systems," the report continues. "The actors acquire the credentials of the local administrator accounts by using hash dumping tools. They can also use common local administrator account credentials to infect other systems with Trojans. They may also run hash dumping tools on Domain Controllers, which compromises most if not all of the password hashes being used in the network. The actors can also deploy keystroke loggers on user systems, which captured passwords to other non-Windows devices on the network."

> the attackers infiltrated and copied the emails for many of Elisra's top executives, including the CEO, the chief technology officer (CTO) and multiple vice presidents within the company.

The attackers followed a similar modus operandi in targeting Elisra, a breach which CyberESI says began in October 2011 and persisted intermittently until July 2012. The security firm said the attackers infiltrated and copied the emails for many of Elisra's top executives, including the CEO, the chief technology officer (CTO) and multiple vice presidents within the company.

CyberESI notes it is likely that the attackers were going after persons of interest with access to sensitive information within Elisra, and/or were gathering would be targets for future spear-phishing campaigns.

Drissel said like many other such intellectual property breaches the company has detected over the years, neither the victim firms nor the U.S. government provided any response after CyberESI alerted them about the breaches at the time.

"The reason that nobody wants to talk about this is people don't want to re-victimze the victim," Drissel said. "But the real victims here are the people on the other end who are put in harm's way because of poor posture on security and the lack of urgency coming from a lot of folks on how to fix this problem. So many companies have become accustomed to low-budget IT costs. But the reality is that if you have certain sensitive information, you've got to spend a certain amount of money to secure it."

ANALYSIS

While some of the world's largest defense contractors have spent hundreds of millions of dollars and several years learning how to quickly detect and respond to such sophisticated cyber attacks, it's debatable whether this approach can or should scale for smaller firms.

Michael Assante, project lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security at the **SANS Institute**, said although there is a great deal of discussion in the security industry about increased information sharing as the answer to detecting these types of intrusions more quickly, this is only a small part of the overall solution.

> maybe a $100 million security program can do all these things well or make progress against these types of attacks, but that 80-person defense contractor? Not so much.

"We collectively talk about all of the things that we should be doing better — that we need to have better security policies, better information sharing, better detection, and we're laying down the tome and saying 'Do all of these

things',” Assante said. “And maybe a $100 million security program can do all these things well or make progress against these types of attacks, but that 80-person defense contractor? Not so much.”

Assante said most companies in the intelligence and defense industries *have* gotten better at sharing information and at the so-called “cyber counter-intelligence” aspect of these attacks: Namely, in identifying the threat actors, tactics and techniques of the various state-sponsored organizations responsible. But he noted that most organizations still struggle with the front end of problem: Identifying the original intrusion and preventing the initial compromise from blossoming into a much bigger problem.

“I don't think we've improved much in that regard, where the core challenges are customized malware, persistent activity, and a lot of noise,” Assante said. “Better and broader notification [by companies like CyberESI] would be great, but the problem is that typically these notifications come after sensitive data has already been exfiltrated from the victim organization. Based on the nature of advanced persistent threats, you can't beat that time cycle. Well, you might be able to, but the amount of investment needed to change that is tremendous.”

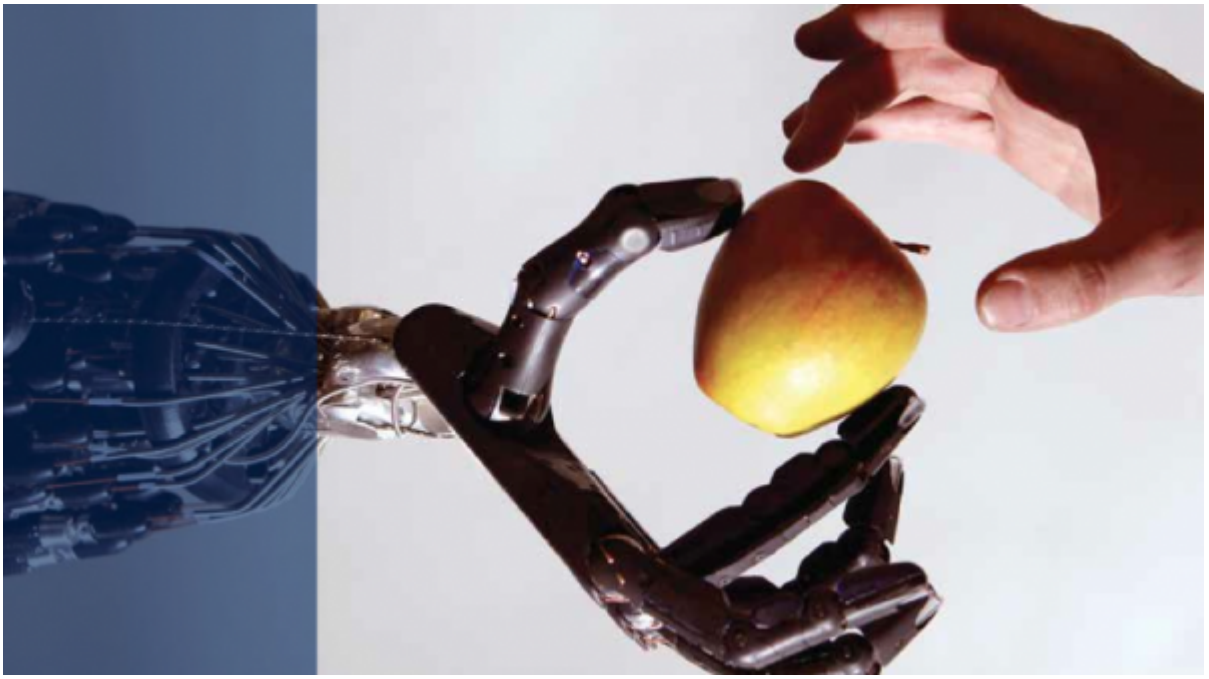
Ultimately, securing sensitive systems from advanced, nation-state level attacks may require a completely different approach. After all, as Einstein said, “We cannot solve our problems with the same thinking we used when we created them.”

Indeed, that appears to be the major thrust of a report released this month by **Richard J. Danzig**, a board member of the **Center for New American Security**. In “Surviving on a Diet of Poison Fruit,” (PDF) Danzig notes that defensive efforts in major mature systems have grown more sophisticated and effective.

“However, competition is continuous between attackers and defender,” he wrote. “Moreover, as new information technologies develop we are not making concomitant investments in their protection. As a result, cyber insecurities are generally growing, and are likely to continue to grow, faster than security measures.”

In his conclusion, Danzig offers a range of broad (and challenging) suggestions, including this gem, which emphasizes placing a premium on security over ease-of-use and convenience in mission-critical government systems:

“For critical U.S. government systems, presume cyber vulnerability and design organizations, operations and acquisitions to compensate for this vulnerability. Do this by a four-part strategy of abnegation, use of out-of-band architectures, diversification and graceful degradation. Pursue the first path by stripping the 'nice to have' away from the essential, limiting cyber capabilities in order to minimize cyber vulnerabilities. For the second, create non-cyber interventions in cyber systems. For the third, encourage different cyber dependencies in different systems so single vulnerabilities are less likely to result in widespread failure or compromise. And for the fourth, invest in discovery and recovery capabilities. To implement these approaches, train key personnel in both operations and security so as to facilitate self-conscious and well- informed tradeoffs between the security gains and the operational and economic costs from pursuing these strategies.”



Source: Center for New American Security
