2013 Survey of Information Security Professionals

Defending Against State-Sponsored Attacks and Other Advanced Persistent Threats

Published: September 4, 2013
Executive Summary

In 2013 Lieberman Software surveyed nearly 200 IT security professionals at Black Hat USA 2013 in Las Vegas, NV. The survey measured attendees’ insights into state-sponsored cyber attacks and other advanced persistent threats. It also gauged their opinions on the likelihood of these attacks to be identified and mitigated in today’s corporate and government IT environments.

Black Hat USA was selected as the venue for the survey due to the demographics of its attendees. According to the event’s web site, this show “brings together thought leaders from all facets of the infosec world - from the corporate and government sectors to academic and even underground researchers. The environment is strictly vendor-neutral and focused on the sharing of practical insights and timely, actionable knowledge.”

The following sections summarize the survey results. Highlights include:

- More than 74% of respondents are not confident that their network has never been breached by a foreign state sponsored attack or an advanced persistent threat.
- Nearly 58% of those surveyed think that the US is losing the battle against state-sponsored attacks.
- Nearly 63% of respondents think a state-sponsored attacker will attempt to breach their organization in the next six months.
- 52% are not confident that their IT staff could detect the presence of an attacker who attempts to breach their network or extract private data – even though the overwhelming majority of respondents work in organizations that have taken at least some additional security precautions.
1. Likelihood of Being Breached by State-Sponsored Attack

Among IT security professionals surveyed, 74.3% of respondents are not confident that their network has never been breached by a foreign state-sponsored attack or an advanced persistent threat. 22.9% were confident that this had never occurred, while 2.8% either did not know or did not answer.

Commenting on these findings, Martyn Croft, CIO of The Salvation Army UK said, “since I would assume that state-sponsored attacks are a covert operation, it sort of begs the question whether anyone can know the full extent. I guess a certain amount of inference from the known attacks, e.g. Stuxnet, would lead one to believe that it's become a commonplace occurrence.”
2. Who is Winning the Battle?

The US is not doing well in the ongoing cyber war, according to BlackHat USA 2013 attendees. Of those we surveyed, 57.7% think that the US is losing the battle against state-sponsored attacks, compared to 30.3% who say otherwise. The remaining 12% either do not know or chose not to answer this question.

"I would have imagined this figure to be higher than 58% because the truth is that most organizations will lose the battle if they end up on the target list of a state-sponsored attacker," said Amar Singh, ISACA Security Advisory Group Chair.
3. Likelihood of Being Targeted

62.9% of respondents think their organizations will be a target of a state-sponsored attack some time in the next six months.
4. Confidence in IT Security Measures

Not only do the majority of survey respondents think that their organizations will be targeted for state-sponsored cyber attacks, most (52%) also do not think that their IT staff are able to detect such an attack. 40% are confident that they could at least detect an attack.

![Pie chart showing confidence in IT staff detecting attacks](chart.png)
5. Additional Security Precautions

Respondents were asked which additional security precautions their organizations’ had taken: user training, security appliances, end point testing and pen testing. 69.7% replied that they use all of these security measures, while only 1.1% stated that they do not use any of them. Individual breakdowns are below.
6. Handling New and Emerging Threats

Perhaps the extra security measures our respondents have employed (see number five above) have given them confidence. 57.1% think that their security products and processes can keep up with new and emerging threats. 36% do not.

![Pie chart showing response to question]

**Do you think that your organization’s security products and processes can keep up with new and emerging security threats?**

- Yes: 57%
- No: 36%
- Other: 7%
7. Will Hacking Get Worse?

When directly asked whether or not the hacking landscape will get worse, an overwhelming 95.9% of polled IT security professionals said yes, it will. Only 2.9% of respondents think that the problem has reached the bottomed.

“The hacking landscape will be getting much worse over time,” said Amar Singh, ISACA Security Advisory Group Chair. “The icing on the cake, from the malicious hackers’ perspective will be when the world fully embraces IPV6, the next generation internet protocol that will allow every single human being on this planet to own at least 2000 fixed and permanent cyberspace addressees. Think about the attack surface when your TV, your watch, your wristband, your car’s engine, your car’s brake systems have a unique cyber space address and these devices will be always connected to cyberspace!”
Survey Methodology

The 2013 Survey of IT Security Professionals was conducted among nearly 200 attendees of Black Hat USA 2013 in Las Vegas, NV. All responses were anonymous. Respondents were all registered attendees of the show and were polled one on one, on site at the venue. Only fully completed surveys were measured for this report. Any incomplete or indecipherable responses were discarded by the tabulators.

Limitations

The number of surveys was dependent on time constraints. Lieberman Software conducted as many surveys as possible during the allotted time while attendees were present on the show floor. Surveys were continually conducted one on one, in person, until the exhibit hours ended.

In an attempt to maximize survey response, the number of questions was purposefully limited. Therefore, demographic questions such as industry and size of organization were eliminated. Ideally we would have correlated and measured these factors.

About Lieberman Software

Lieberman Software provides privileged identity management and security management products to more than 1000 customers worldwide, including nearly half of the Fortune 50. By automatically discovering and managing privileged accounts throughout the network, Lieberman Software helps secure access to sensitive data, thereby reducing internal and external security vulnerabilities, improving IT productivity and helping ensure regulatory compliance. The company developed the first solution for the privileged account management space, and its products continue to lead the market. Lieberman Software is headquartered in Los Angeles, CA with an office in Austin, TX and channel partners throughout the world. For more information, visit www.liebsoft.com.