the Availability Digest

www.availabilitydigest.com
@availabilitydig

Ponemon on Live Threat Intelligence

November 2013

Ponemon Institute conducts empirical studies on critical issues affecting the management and security of sensitive information about people and organizations. It has recently completed a study on the value of live cyberthreat intelligence for combating cyberattacks. Live cyberthreat intelligence refers to intelligence data about actual cyberattacks happening now. It is delivered with no delay, as compared to delays ranging from minutes to days and even weeks for many cyberthreat monitoring facilities.

The Ponemon study was based on a survey of 708 users. Thirty-five percent of the users were technical staff. Management staff (supervisors, managers, directors, vice presidents) represented 58% of the responses.

Over fourteen industry segments were included. The largest was financial services (19%), followed by health and pharmaceutical (12%), public sector (12%), and retail (9%).

The Ponemon study shows that the average cost to large organizations for defending cyberattacks is about USD $10 million per year. If these organizations had access to live threat information, they estimate that they could save 40% of this cost, or USD $4 million dollars per year.

We summarize the key findings of the report in this article.

Optimum Age of Actionable Intelligence

Companies that were successful in stopping cyberattacks as they were occurring said that the optimal age of threat intelligence was less than 4.6 minutes. Companies that had a history of not stopping cyberattacks felt that 12.1 minutes was satisfactory.

Companies say that, on average, they need at least ten minutes notice to stop an attack. However, 57% of companies say that their intelligence is too old to actually thwart an attack.

Key problems with dealing rapidly with threat intelligence are that it is difficult to share the intelligence with key stakeholders in a timely fashion and much of the intelligence is false positives.

Clearly, speed and accuracy are of the essence. The value of live threat intelligence ages very rapidly. False positives cost time and money and lead to complacency.

Success Rate of Cyberattack Defenses

Twenty-three percent of companies reported that they had successfully defended against all cyberattacks in the last two years. Sixty-two percent stated that they failed to prevent one or more security exploits in the last two years. Thirty-three percent of companies stated that they were successfully attacked nine times or more in the last two years.

The average number of successful attacks was six over the two year period.

The Most Serious Attacks

There are a wide range of cyberattacks that are carried out against companies. The most feared is advanced persistent threats (APT) that engage in a long-term pattern of sophisticated hacking attacks. In close order behind APTs are root kits (installing malware at the operating system level), and SQL and code injection.

The most lethal attackers are criminal syndicates, followed by malicious insiders and state sponsored attackers. Hactivists and lone-wolf hackers are at the bottom of the list.

The countries that currently represent the most active attackers are the United States followed by China and states in the Russian Federation. However, this demographic is expected to change. In the future, the primary attackers will be China, the Russian Federation, and then the United States.

Are Attacks Even Detected?

Sixty-five percent of companies believe that their organization has been a target of cyberattacks. Only 34% believe that it is unlikely that they have ever been attacked. Thirty-five percent of these companies say that their attack estimates are based on intuition. 23% of companies say that their organizations rely upon precise intelligence.

The lack of knowledge about whether their websites, networks, or other systems were compromised puts organizations at an elevated risk with respect to the effectiveness of cyberattacks against them. Thirty-seven percent of companies say that they would unlikely know of such an event. Only 10% of companies say that they would know with certainty when an attack had occurred. For those who felt that they can detect an attack, it would take an average of eleven days to determine that a cyberattack had occurred.

The Importance of Live Intelligence

It was felt by 63% of the companies that live intelligence is very important to achieving a strong cyberattack defense. However, they rate their ability to gather and to analyze live cyber intelligence very low – about 4 on a scale of 1 to 10 (10 being the highest).

The majority of respondents (59%) felt that big-data analytics was the solution to handling the mass of live intelligence data that can be generated.

The intelligence features that are considered to be most important to deal with cyberattacks include:

- Clear and concise reports so that quick action can be taken.
- Communication based on risk priority or level of compromise.
- Integrating intelligence information with enabling technologies such as SIEM (security information and event management) appliances.
- Expedited intelligence reports once a company knows that it has been targeted.
- Non-disruptive intelligence information reporting.
- Trend data such as the frequency of attacks included in the intelligence information.
- Distribution of intelligence reports to people based on their need to know.
- Capture of corroborating intelligence information from external sources.

IT Security Budget

The average IT budget of the respondents was USD $95 million, and USD $13 million of this budget was allocated to IT security. Of the security budget, about USD $3 million was spent on intelligence about cyberthreats.

Companies spent an average of USD $10 million per year to resolve the impact of cyberattacks. This includes out-of-pocket expenditures, productivity impact, legal costs, and reputational damage. Companies estimated that if they had actionable intelligence on an occurring cyberattack within 60 seconds of the compromise, they could save USD $4 million per year.

The Importance of Managing Threat Information

The success that a company has of stopping a cyberattack depends to a great deal on how effective is their threat intelligence and how effectively they manage it. Companies' success at thwarting cyberattacks depends upon how they handle their cyber intelligence, as shown in the following table.

	Comply with Function?	
	Yes	No
Function:	% Successful	% Successful
Organize intelligence based on perceived threats	49%	24%
Effective at gathering live intelligence	65%	36%
Effective use of technologies providing intelligence:		
Security exploits stopped	85%	69%
High level of certainty about targeted attacks	63%	30%
See intelligence-gathering activities as effective	97%	64%

Summary

The Ponemon study demonstrates the importance of having timely intelligence to stop a cyberattack. However, the majority of respondents agree that it is hard to stop an attack on enterprise systems because the threat intelligence is out of date. Furthermore, the high rate of false positives deters staff from pursuing the real threats and attacks.

The study shows that the effective use of enabling technologies such as SIEM appliances can lead to the prevention of security exploits and a greater understanding of the types of cyberattacks to which the company is being subjected.

This study was sponsored by Norse Corp. (www.norse-corp.com). Norse's synchronous global platform continuously collects and analyzes real-time, high risk Internet traffic to identify the sources of cyberattacks. Their system protects against today's most advanced cyber threats including zero-day and advanced persistent threats.