

**Contacts:** Lars Voedisch

PRecious Communications *for McAfee*

+65 9170 2470

[lars@preciouscomms.com](mailto:lars@preciouscomms.com)

Serene Chow

PRecious Communications *for McAfee*

+65 9836 4873

[serene@preciouscomms.com](mailto:serene@preciouscomms.com)

**intel® security REPORT details critical factors in preventing data breaches**

*Real-Time Response, Integrated Intelligence, and Eight Indicators of Attack Key to Proactive Threat Prevention*

**SANTA CLARA, CALIFORNIA/ SINGAPORE — November 19, 2014 —**McAfee, now part of Intel® Security, today issued a new report, [*When Minutes Count*](http://www.mcafee.com/us/resources/reports/rp-when-minutes-count.pdf)*,* that assesses organizations’ abilities to detect and deflect targeted attacks, reveals the top eight most critical indicators of attack, and examines best practices for proactive incident response. The report illustrates how much more effective enterprises are when they perform real-time, multi-variable analyses of subtle attack activity and factor time and threat intelligence in to risk scoring and incident response priorities.

A survey commissioned by Intel Security and conducted by Evalueserve, in conjunction with the report, suggests that a majority of companies lack confidence in their ability to detect targeted attacks in a timely manner. Even companies best prepared to handle targeted attacks are taking the time to investigate high volumes of events, contributing to a sense of urgency and organizational focus on creative approaches to earlier detection and more effective mitigation.

Key findings include:

* 74% of respondents indicated that targeted attacks are a primary concern for their organizations
* 58%of organizations investigated 10 or more attacks last year
* Only 24% of companies are confident in their ability to detect an attack within minutes, and just under half said it would take days, weeks, or even months before they noticed suspicious behavior
* 78% of those able to detect attacks in minutes had a proactive, real-time Security Information and Event Management (SIEM) system
* Half of the companies surveyed indicated that they have adequate tools and technologies to deliver faster incident response, but often critical indicators are not isolated from the mass of alerts generated, placing a burden on IT teams to sift through threat data

“You only gain the upper-hand versus attackers when you address the time-to-discovery challenge,” said Ryan Allphin, Senior Vice President and General Manager, Security Management at Intel Security. “Simplify the frantic work of filtering an ocean of alerts and indicators with real-time intelligence and analysis, and you can quickly gain a deeper understanding of relevant events and take action to contain and deflect attacks faster.”

Given the importance of identifying critical indicators, the Intel Security report revealed the top eight most common attack activities that successful organizations track to detect and deflect targeted attacks. Of these, five reflected tracking events across elapsed time, showing the importance of contextual correlation:

1. Internal hosts communicating with known bad destinations or to a foreign country in which an organization does not conduct business.
2. Internal hosts communicating to external hosts using non-standard ports or protocol/port mismatches, such as sending command shells (SSH) rather than HTTP traffic over port 80, the default web port.
3. Publically accessible or demilitarized zone (DMZ) hosts communicating to internal hosts. This allows leapfrogging from the outside to the inside and back, permitting data exfiltration and remote access to assets. It neutralizes the value of the DMZ.
4. Off-hour malware detection. Alerts that occur outside standard business operating hours (at night or on weekends) could signal a compromised host.
5. Network scans by internal hosts communicating with multiple hosts in a short time frame, which could reveal an attacker moving laterally within the network. Perimeter network defenses, such as firewall and IPS, are seldom configured to monitor traffic on the internal network (but could be).
6. Multiple alarm events from a single host or duplicate events across multiple machines in the same subnet over a 24-hour period, such as repeated authentication failures.
7. After being cleaned, a system is re-infected with malware within five minutes—repeated reinfections signal the presence of a rootkit or persistent compromise.
8. A user account trying to login to multiple resources within a few minutes from/to different regions—a sign that the user’s credentials have been stolen or that a user is up to mischief.

“We noticed a workstation making odd authentication requests to the domain controller at two o’clock in the morning. That could be normal activity, but it could also be a sign of something malicious,” said Lance Wright, Senior Manager of Information Security and Compliance at Volusion, a commerce solutions provider contributing to the report. “After that incident we set up a rule to alert us if any workstation has more than five authentication requests during non-business hours to help us identify the attack early, before any data is compromised.”

“Real-time, intelligence-aware, SIEM technologies minimize time to detection to help proactively prevent breaches based on contextualization of indicators during analysis and automated policy-driven responses,” said Allphin. “With the power to accelerate their ability to detect, respond to, and learn from events, organizations can dramatically shift their security posture from that of the hunted, to the hunter.”

To view the full Intel Security *When Minutes Count* report, please visit: [www.mcafee.com/SIEM](http://www.mcafee.com/SIEM)

**About Intel Security**

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security’s mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

*Note: McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries. Other names and brands may be claimed as the property of others.*

###