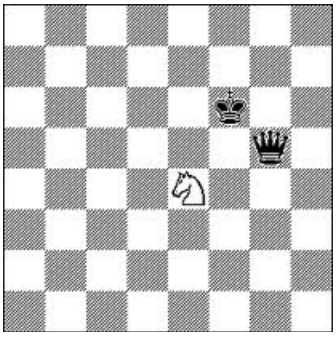
The Knight Fork: Defining Defense in 2013

A Trend Micro Opinion Piece
By Tom Kellermann, Vice President of Cyber Security, Trend Micro Inc.
November 2012



"People do not care to play chess on the edge of a precipice."

—Madame Suzanne Necker, Mother of Germain de Stael

A knight's fork is defined as: "an attack by one chess piece (as a knight) on two pieces simultaneously." (Merriam-Webster Dictionary)

When was the last time you played chess? If you are responsible for cyber security you are unwittingly playing it every day. We must appreciate the ancient sport of chess in order to reorganize our defense in 2013.

To begin, we must pay homage to strategies and tactics being employed by the elite hacker community. Spin the chess board: the elite hacker of 2012 has evolved their stages of cyberintrusion. This now includes a maintenance stage as it is their goal to maintain the colony they built within your ecosystem. These colonies are built to cover tracks via:

- Internal compromised systems used as C&C nodes
- Random connections to outside C&C servers
- Dynamic DNS services

The malware is innovative: RATs have all capabilities hard-coded internally; encrypted traffic, dynamic drop zones, complex command and control. The infrastructure is internal to the operation, or bulletproof hosts are carefully selected. In 2012 we have observed significant tactical trends. There is a high degree of modularization in more advanced malware; there is an increased sophistication via the use of Traffic Direction Systems (TDS); Man-in-the-Browser attacks are becoming mainstream as is exploitation via HTML5 and finally, mobile malware is flourishing as proximity attacks can now be realized.

To improve our defense in depth we must appreciate that APTs are consistent and part of ongoing campaigns; that targeted attacks do not always use zero-day exploits as they generally use older exploits and simpler malware; and finally that targeted campaigns are a series of failed and successful attempts over time to establish a covert presence which can be tracked in due course. Advanced detection techniques can be used to identify the adversary once we appreciate the challenges of maintaining a persistent presence within a network. We must spin the chess board and value the nuance of becoming overextended. From a hacker's perspective, changing C&C protocols requires considerable effort. Thus, network traffic can be

correlated with other indicators to provide proactive detection. Unknown threats may be detected by extrapolating methods and characteristics from known threat communication behaviors. If we can accomplish this then we can achieve advanced situational awareness in real time so as to manifest custom defense. Risk management in 2013 will be defined by the following set of defensive tactics:

- Does a log inspection program exist?
- Does file integrity monitoring exist?
- Can vulnerabilities be virtually patched?
- Do you utilize a DLP?
- Do you maintain multi-level rule-based event correlation?
- Is there custom sandbox analysis?

If you can answer yes to these risk management questions we can begin to customize defense. The goal of custom defense is to increase the level of discomfort of hackers to a point wherein they become resource constrained in order to maintain a clandestine persistent presence within our systems.

"People do not care to play chess on the edge of a precipice."

—Madame Suzanne Necker, Mother of Germaine de Stael

The "precipice" is a manifestation of greater situational awareness—situational awareness via multi-level, rule-based event correlation and custom sandbox analysis. Deep Discovery can endow you—the defender—with a cyber knight's fork.

Tom Kellermann
VP of Cyber Security,
Trend Micro

As Vice President of Cyber Security at Trend Micro, Mr. Kellermann is focused on acting as a trusted cyber security advisor and strategist within the federal, state and local government markets. He utilizes his experience as a security evangelist and government affairs expert to forge strategic partnerships both domestically and internationally, and increase Trend Micro's profile in emerging technologies and policy issues.

Tom Kellermann served as a Commissioner on The Commission on Cyber Security for the 44th Presidency and serves on the board of the International Cyber Security Protection Alliance (ICSPA). He sits on many boards including: the National Board of Information Security Examiners Panel for Penetration Testing, the Information Technology Sector Coordinating Council, and the Information Technology Information Sharing and Analysis Center (IT-ISAC) subcommittee on International Cyber security policy.

Mr. Kellermann is a Professor at American University's School of International Service and is a Certified Information Security Manager (CISM).

Formerly holding the position as Chief Technology Officer and Chief Cyber Strategist at AirPatrol Corporation, Tom Kellermann also spent five years as Vice President of Security Awareness for Core Security.

Previously, he was the Senior Data Risk Management Specialist for the World Bank Treasury Security Team, where he was responsible for internal cyber-intelligence and policy and for advising central banks around the world about their cyber-risk posture and layered security architectures. Along with Thomas Glaessner and Valerie McNevin, he co-authored the book "E-safety and Soundness: Securing Finance in a New Age."

Mr. Kellermann is also Trend Micro's representative on the The National Cyber Security Alliance (NCSA).

TREND MICRO™

Securing Your Journey to the Cloud

©2012 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, OfficeScan, and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.