APT C&C Communication

Superior Detection with Trend Micro Custom Defense

Knowing your Adversary

Advanced Persistent Threats (APTs) continue to evade organizations' standard defenses, as recently witnessed with attacks on the New York Times, Wall Street Journal, and US Federal Reserve.

But, the real question is, why are they so hard to detect? The short answer – because they are carefully customized to your organization with:

- In-depth knowledge of your employees
- Malware engineered and tested to evade your standard security defenses
- Methods crafted to take advantage of your apps and environment
- Human interaction that guides the attack as it moves within your network
- A target specifically aimed at your data and intellectual property

Did You Know?

- **21%** of IT professionals reported that their enterprise has already been victimized by an APT
- **63%** of IT professionals think it is only a matter of time before their enterprise is targeted
- **98%** of data breaches stemmed from external agents with **58%** attributed to activist groups
- **85%** of breaches took weeks or more to discover
- **92%** of data breach incidents were discovered by a third party*

APT C&C Detection Challenges

Once inside the target organization, APTs are typically remotely orchestrated via "command and control" (C&C) communications between the infiltrated systems and the attackers themselves. Throughout the attack, the perpetrators will also use this channel to open and manipulate backdoor network access to discover and exfiltrate their targeted data.

Your organization's ability to effectively defend against APTs is directly dependent on the ability to quickly detect the attack's C&C communication; however, this poses a significant challenge across several fronts:

Difficult Detection

- Unlike botnets that have high volume traffic to thousands of zombie PCs, APT C&C traffic is intermittent with low volume making them harder to spot.
- Extensive attacker evasive methods, such as continual change of addresses or traffic redirection via proxy servers, are commonplace.
- C&C communications that blend in with normal web traffic, use or spoof legitimate apps or sites, or use attacker-created, internal C&C servers cannot be detected without advanced, local network monitoring.

Security Vendor Limited Capabilities

- Most security vendors lack the expertise, scale, technology, and resources to reliably identify APT C&C resulting in threat detection lists that are spotty, incomplete, and unreliable.
- Vendors predominantly approach the C&C problem at the global level only and don't provide local detection, making it impossible to uncover most C&C evasive techniques.

No Alerting or Policy Control

- Most vendor security products don't have clear APT C&C detection indicators. When a detection is found, it's likely to simply be blocked or logged without an alert or warning of the potential risk.
- Most products also do not give the customer the option to control whether the C&C should be blocked or monitored.

C&C Detection & Early Warning Requirements

Organizations clearly need a better detection and alerting system that provides the ability to reliably answer these critical questions:

1. Is there C&C activity on my network?
2. Is it a simple botnet or a possible targeted attack?
3. How risky is it? Where and whom is it from?
4. Should I immediately block and remediate or monitor it further?

Trend Micro Custom Defense against APTs

Only the Trend Micro Custom Defense solution can answer these questions with the C&C detection, protection, and intelligence needed to stop a targeted attack before the damage is done.

Our research shows that most high-profile targeted attacks in the past could have been discovered if security defenders kept their eyes on malicious network communications. This is based on consistent network traffic indicators and patterns that can give away the presence of an APT in the works.

The Trend Micro Custom Defense solution provides in-depth network monitoring that identifies and analyzes malicious content, dubious C&C traffic, and attacker behavior so your organization can get ahead of an APT attack that's currently in progress.

How the Custom Defense Works

Global Identification and Tracking

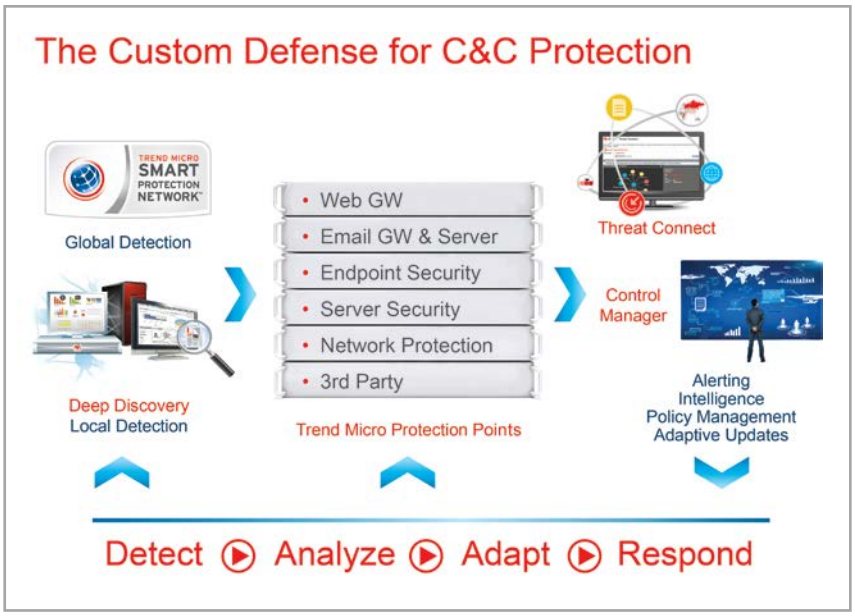
The Trend Micro Smart Protection Network automatically identifies active C&C sites worldwide based on daily processing of 12 billion IP/URL enquires and the correlation of over 6 Terabytes of data. Its correlation engines keep up with the changing nature of C&C addresses, and it employs the latest innovations from Trend Micro's 1200 Threat Researchers to continually detect evasive measures taken by attackers.

Network-Based Detection and Learning

Trend Micro Deep Discovery uses custom threat detection to discover advanced malware, communications, and attacker activities at the network level. Unique "fingerprint" detection of cloaked C&C traffic can identify attackers' use of legitimate applications and websites as well as other advanced techniques, such as the use of internal C&C servers. Deep Discovery custom sandbox analysis can also discover new C&C destinations of zero-day malware attacks and update the Smart Protection Network and all customer security protection points.

Integrated Protection Across Products

The latest global and local C&C detection information powers Trend Micro enterprise security products at the endpoint, server, network, gateway, and messaging protection points to identify and control C&C activity across your environment.



Response and Control

C&C detection at any point is clearly identified on a centralized console, immediately alerting your security team. C&C risk assessment, containment, and remediation are aided by the solution's unique Threat Connect that provides intelligence on the severity, activity, origins, and related addresses of the C&C site – helping you to quickly determine how containment and remediation should proceed, such as a high risk that should be immediately blocked.

Fighting Back Against Your Attackers with the Custom Defense

The Trend Micro Custom Defense empowers and unites your security infrastructure to discover and block APTs and targeted attacks before real damage occurs. Its unique, integrated, custom detection and intelligence deliver the best attack protection, enabling your organization to deploy a complete Detect – Analyze – Adapt – Respond lifecycle to fight back against your attackers.

Learn more at trendmicro.com/apt

*Sources: ISACA 2012 Advanced Persistent Threat Awareness Study, Verizon 2012 Data Breach Investigation

©2013 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, 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. [SB01_C&C_130219US