A TrendLabs Cloud Security Primer

MALICIOUS NETWORK COMMUNICATIONS:

WHAT ARE YOU OVERLOOKING?

LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

According to a Trend Micro-sponsored Enterprise Strategy Group (ESG) study, nearly 40% of large organizations invested in new security defenses to respond to APTs.[1] However, enterprise efforts in curbing these high-priority threats are still insufficient as security researchers continue to find successful APT campaigns inside corporate networks.

The following are existing business realities that weaken enterprises' security posture against APTs:

- **Security is rarely a top priority in the corporate budget.**

  Enterprises allocate minimal budget for security.[2] As a result, organizations tend to address APTs in increments with marginal changes to existing layers of defense to save on IT expenses. This practice can leave holes in their network security.

- **Discrepancy between how enterprises perceive targeted attacks and how these campaigns unfold in real-world scenarios**

  Most organizations still deploy traditional anti-malware detection and prevention to protect against these kinds of attacks. Traditional solutions typically lead to investing in inadequate security solutions.[3]

- **APT defense as a bolt-on to pre-existing security architecture and practices**

  APT requires a reexamination of the current security strategy. However, in the same survey cited above, 67% of infosec professionals disclosed that APT awareness trainings have not increased and 82% revealed that vendor agreements regarding information exchange have not changed as well.

1 http://www.trendmicro.es/media/wp/esg-apts-deep-discovery-whitepaper-en.pdf
2 http://reports.informationweek.com/abstract/21/9736/Security/strategy-cybersecurity-on-the-offense.html
3 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx

The Role of C&C Communications in an APT Campaign

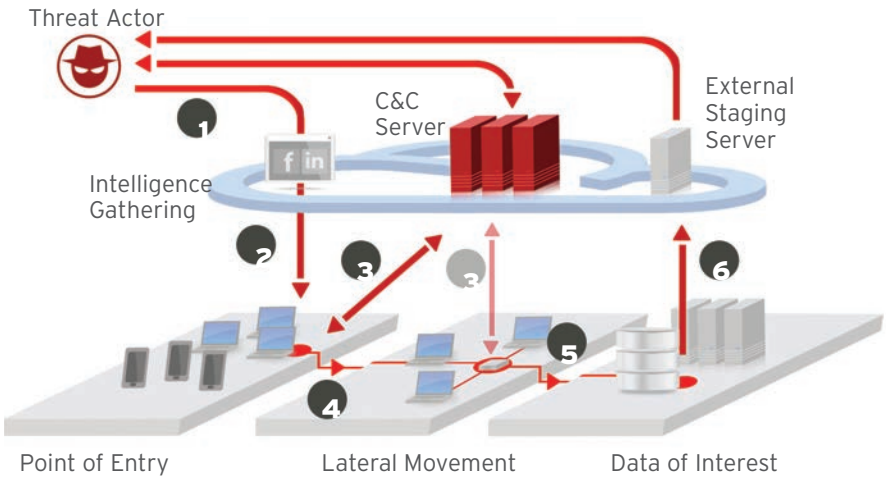

Figure 1. The Six Stages of an APT Campaign

An APT campaign/targeted attack can be segmented into six stages:

- **Intelligence gathering**: Threat actors prepare a customized attack design based on comprehensive research on the target organization. It uses public sources and other prior social engineering attacks such as LinkedIn, Facebook, or the company website.
- **Point of entry:** Threat actors launch a successful attempt to penetrate the target network by delivering malware via social engineering or watering hole technique.[4]
- **Command-and-control (C&C) communications:** After a backdoor opens the target network to infiltration, attackers use C&C channels to lead the compromised machines to the attack's subsequent phases.
- **Lateral movement and persistence:** Once inside the network, attackers compromise additional machines to gather credentials, escalate privilege levels, and maintain persistent control over the compromised network.
- **Asset/Data discovery:** Perpetrator employs several techniques to identify valuable servers and services that contain targeted information.
- **Data exfiltration:** Once the data is gathered, intruders send the stolen data to an internal staging server where it is chunked, compressed, and often encrypted for transmission to external locations.

4 http://blog.trendmicro.com/trendlabs-security-intelligence/watering-holes-and-zero-day-attacks/

"... The most high-profile targeted attacks in the past could have been discovered if security defenders kept their eyes on malicious network communications."

—Nart Villeneuve

Source: Detecting APT Activity with Network Traffic

APTs are a category of threat that refers to computer intrusions by threat actors that aggressively pursue and compromise specific targets. Threat actors use social engineering and malware to enter a network, after which they move laterally throughout the network to extract sensitive information. In an APT campaign, keeping the communication channel between the compromised machine and the threat actor's C&C server open is crucial for the success of targeted attacks.[5] These conduits allow threat actors to:

- Confirm system breach
- Obtain information about the targeted network
- Send commands to the malware within the compromised network
- Instruct the compromised PC to download "second stage" malware and the tools used for lateral movement

C&C Traffic in Uncovered APT Campaigns

Given the pivotal role of C&C communications in a targeted attack, Trend Micro research suggests that proactively detecting malicious C&C traffic is an important element in exposing APTs. Our research further shows that high-profile APTs in the past could have been discovered if security groups monitored malicious network communications.[6] In this same study, we identified network traffic indicators that reveal the presence of known APT campaigns in a network:

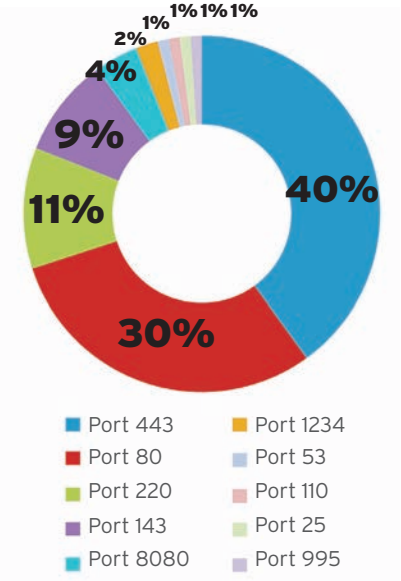

Figure 2. Regularly used ports by PoisonIvy samples found in Japan from 2008 to 2012

- **Consistent URL paths**

  The initial malware dropped by the GhOstNet campaign uses specific and consistent URL parameters.

- Detectable packet headers

  Network traffic of campaigns using GhOst RAT have packet headers that always contain five bytes, such as "GhOst" or "LURKO," followed 8 bytes later by a zlib compression header.

- Identifiable network communications

  PoisonIvy, a RAT used in the Nitro attack, uses the same 256-byte outbound packet containing mostly non-ASCII data, using varying ports. This is a challenge request. After the challenge response is received, it sends a consistent 4-byte value.

  Several versions of the Enfal malware exist; but the communication between its compromised host and a C&C server remains consistent.[7]

  The Taidoor campaign, likewise, constantly follows the same format for initial C&C server requests.

5 http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apt-primer.pdf
6 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
7 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_dissecting-lurid-apt.pdf

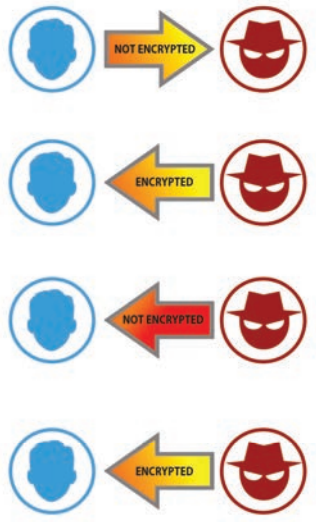

Figure 3. Initial communication between a PoisonIvy server and client

- Unusual ports and protocols

  GhOst RAT uses non-HTTP protocols on port 80, which usually only contains HTTP traffic.

- Secure sockets layer (SSL) certificates

  Even if Sykipot uses HTTPS to evade network detection, this campaign used consistent elements within its SSL certificates.

These consistent network traffic indicators provide an opportunity for enterprises to check if ongoing campaigns exist in the network. While changes to a certain campaign's network communications are not unheard of, the campaign's C&C network traffic patterns are relatively more difficult to modify than the servers, domains, or even the malware a threat actor uses.

Custom Defense against APTs

Targeted attacks constantly take advantage of unknown malware. The ability to identify anomalous network traffic indicative of these kinds of attacks constitutes a crucial part of any sound APT defense. Given the highly targeted and persistent nature of APT campaigns, an APT defense framework must enable the network to identify and assess threats in real time leveraging the following components:

- **Network content inspection technology:** An in-depth network monitoring technology that identifies and analyzes dubious C&C traffic can help security groups spot possible targeted attacks. An effective solution should have a deep packet inspection capability that performs port-agnostic protocol detection, decoding, decompression, and file extraction across hundreds of protocols.
- **Advanced threat detection technology:** On top of traditional antivirus file scanning and aggressive heuristic analysis, enterprises should leverage reputation-based detection that checks and correlates suspicious attack components (file, email and URLs) to discover both known and unknown malware and exploits.
- **Sandbox technology:** A virtualized threat sandbox analysis system that uses network-specific configurations to detect and analyze APTs further strengthens protection against these threats.
- **Threat intelligence:** You need to build threat intelligence using both external resources and your network's threat history. While the network indicators discussed in the earlier section can identify documented APT campaigns, an effective APT defense that leverages threat intelligence can enable security groups to develop their own indicators for ongoing campaigns.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO™

Securing Your Journey to the Cloud

TRENDLABS℠

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

TrendLabs
Global Technical Support & R&D Center of TREND MICRO