A TrendLabs Security in Context Paper

Defending Against Backdoor Techniques Used in Targeted Attacks

Although the motivation behind targeted attack campaigns may vary, threat actors continue to go after the 'crown jewels' or confidential company data of enterprises. Based on a Harvard Business Review study,[1] there are four types of data commonly stolen in targeted attacks: personally identifiable information (PII) (28%), authentication credentials (21%), intellectual property (20%), and other sensitive corporate/organizational data (16%).

Before getting to the crown jewels, though, attackers need to gather a whole lot of other information about their target in order to infiltrate the network without being detected. This may involve gathering publicly available information about the target, as well as information about the target's network infrastructure. The latter is often done with the use of malware, such as remote access tools or backdoors.

The Crucial Role of Backdoors in Targeted Attacks

Backdoors play a critical role in targeted attacks. Besides being the primary tool for stealing data, it is also through backdoors that attackers are able to go deeper into the target network without being detected. For this reason, threat actors often employ a wide-array of backdoor techniques to evade detection.

For instance, attackers will launch a first-line backdoor to execute commands and establish command-and-control (C&C) communications. This will download the second-line backdoor that will steal information from compromised systems that attackers can use to be able to go deeper into their target networks. In the data exfiltration stage, backdoors are used for uploading files and employing certain ports to hide attackers' malicious tracks.

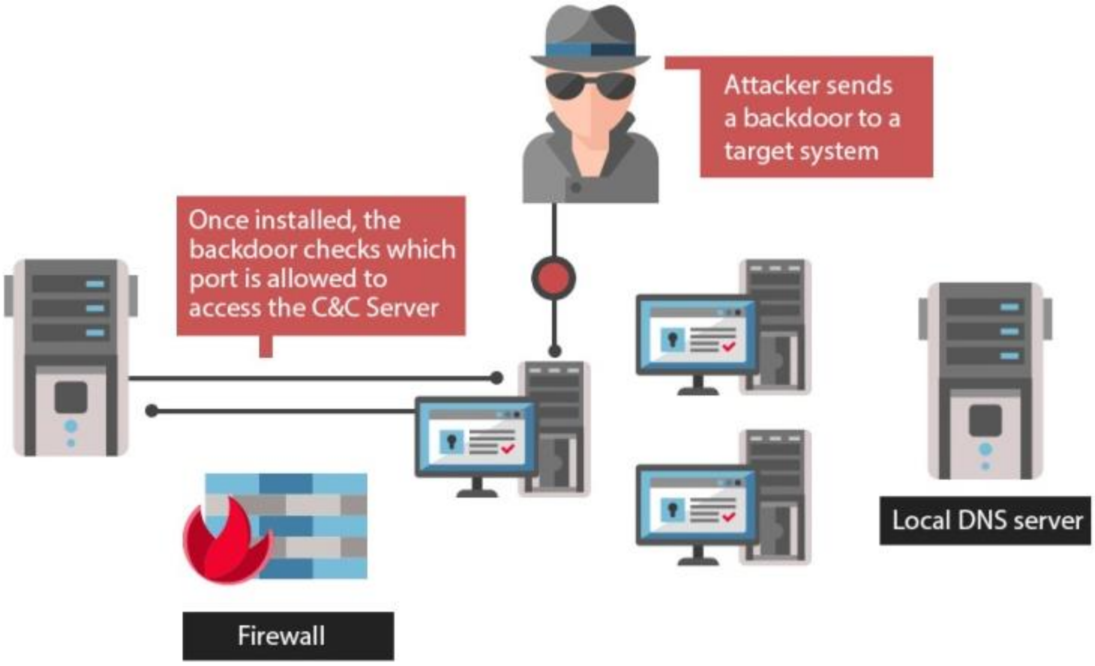
Attacker sends a backdoor to a target system
Once installed, the backdoor checks which port is allowed to access the C&C Server
Local DNS server
Firewall

Figure 1. Backdoor techniques in targeted attacks

[1] Scott Shackelford. (April 16, 2014). "Aggressive and Persistent: Using Frameworks to Defend Against Cyber Attacks." Last accessed November 20, 2014, http://www.slideshare.net/trendmicro/hbr-apt-framework

Recommendations for Combatting Backdoors

Backdoors are applications typically used for remote access and to bypass intrusion detection systems (IDSs). Despite its capabilities, IT administrators can armor their network against backdoor techniques[2] used in targeted attacks with these recommended practices and solution technologies.

- Use Firewall

  Firewall serves to block/allow any network traffic and creates a 'wall' between client and network to secure the network from threats. This can be used to block connections from a backdoor, which usually communicates or 'binds' with specific server ports and protocols to launch commands from an attacker, and consequently, establish control over their target servers.

  IT administrators can configure its firewall settings to control network traffic. They can modify their firewall to ensure that open ports connect only to the right/designated protocols. This can prevent a backdoor from connecting to a specified C&C servers and protocols to use.

  Apart from connecting to ports and protocols, attackers customize DNS lookup where the real traffic to C&C server address is diverted via a customized lookup query to Web services. A firewall can block the IP addresses the customized domain names lead to. However, IT administrators need to identify those first.

- Use Solutions That Monitor Network Packets

  Threat actors check their connection to their C&C servers to ensure that the final payload is executed via Netcat or Ping. This technique is dubbed as connection availability abuse. There are cases when attackers incorporated Netcat-like capability/utility into their malware to bypass IDS. To be able to detect this, IT administrators need to employ a solution that detects malicious network patterns. However, some backdoors have the capability of appearing like a normal HTTP protocol.

  Legitimate platforms are also abused to go undetected in the network so that it can pass off as normal network traffic that is commonly accessed. One targeted attack campaign abused blog sites to store its C&C server information. PlugX RAT (remote access tool) abused file hosting/storage platform[3] Dropbox to download its C&C settings. While it is difficult to detect this, it can be done via network patterns but the occurrence of false positives is likely. We recommend IT administrators to decrypt the cipher text and get the domains it leads to so as to block it immediately.

[2] Dove Chiu, Shih-Hao Weng, and Joseph Chiu. (2014). "Backdoor Use in Targeted Attacks." Last accessed November 20, 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-backdoor-use-in-targeted-attacks.pdf

[3] Maersk Menrige. (June 25, 2014). *TrendLabs Security Intelligence Blog*. "PlugX RAT With "Time Bomb" Abuses Dropbox for Command-and-Control Settings." Last accessed November 20, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/

- Install Anti-malware Solutions

  Anti-malware solutions can protect systems from malicious files, such as backdoors, by detecting it on infected systems and blocking malicious URLs where users download the malicious files from. Anti-malware solutions that have Web reputation services can block access to C&C servers and other malicious URLs. It stops threats from proliferating at the endpoint level.

  There are instances when attackers also leverage instant messaging applications and free email services as part of evasion tactics. Similarly, anti-malware software can identify malicious links coming from instant messages, emails, social networking sites, and websites, thus preventing users from having access to it. Email reputation services in anti-malware solutions can also detect spammed messages that may contain malicious file attachments.

  Only anti-malware solutions with file reputation services, together with network IDSs and intrusion prevention systems (IPSs), can aid in the detection of port reuse, a common backdoor technique that refers to listening to any open port and reuses it.

Enterprises Fight Back: Mitigations and Countermeasures

Targeted attacks often employ consistent network indicators. With this, IT administrators are recommended to monitor the network traffic[4] that can help identify command-and-control communications. However, as discussed here, attackers use a wide array of backdoor techniques that may include the use of legitimate or normal protocols like HTTP, making it difficult for IT administrators to detect targeted attacks. The best practice is still to assume compromise.

Apart from the suggested recommendations above, enterprises can secure their network through simple network defense.[5] For instance, they can tag services with protocols that don't have ports as suspicious. Note that applications and services use protocols and definite ports. As such, IT administrators should look for unknown protocols and close unused ports in the network to prevent abuse.

Attackers often use social engineering tactics to lure users into opening and executing email file attachments that could lead to network infiltration. A basic step like checking file attributes—too many spaces in the file name, more than two file extensions, and mismatched file types and names, among others—should rouse suspicion. Check also if there is any presence of Tor in the network. Threat actors use this to remain anonymous and hide their tracks.

In the data exfiltration stage, threat actors employ HTTP packets to send in information. As such, it is highly recommended to check if these contain information.

[4] Nart Villeneuve. (October 25, 2014). *TrendLabs Security Intelligence Blog*. "How to Detect APT Activity with Network Traffic Analysis." Last accessed November 20, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/how-to-detect-apt-activity-with-network-traffic-analysis/

[5] Bryant Tan. (September 14, 2014). *TrendLabs Security Intelligence Blog*. "The Easy-to-Miss Basics of Network Defense." Last accessed November 20, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/the-easy-to-miss-basics-of-network-defense/

Another recommendation[6] is to regularly patch and update systems and applications because attackers often leverage tried-and-tested vulnerabilities in order to infiltrate the network. Case in point, Windows common controls (addressed in MS12-027) remains to be the favored target vulnerability of threat actors. PLEAD is one of the many campaigns that used this vulnerability to infiltrate attackers' target networks. IT administrators should also regularly check/monitor their network as well as control ghost machines or devices brought by employees and are connected to the network. It is recommended that enterprises have security solutions with virtual patching capabilities that can protect servers[7] and endpoints[8] from any attacks leveraging vulnerabilities.

Enterprises also need a Custom Defense solution[9] that has advanced threat protection that can perform network-wide monitoring to detect zero-day malware, malicious communications, and attacker behaviors. This robust security technology should use shared indicator of compromise (IoC) intelligence to detect, analyze, adapt, and respond to attacks that are invisible to standard security defenses.

[6] Ziv Chang. (September 04, 2014). *TrendLabs Security Intelligence Blog*. "Network Vulnerabilities IT Admins Can Use to Protect Their Network." Last accessed November 20, 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/network-vulnerabilities-it-admins-can-use-to-protect-their-network/

[7] Trend Micro Incorporated. (2014). *Trend Micro*. *"*Deep Security Platform." Last accessed November 20, 2014, http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/

[8] Trend Micro Incorporated. (2014). *Trend Micro.* "OfficeScan—Endpoint Protection." Last accessed November 20, 2014, http://www.trendmicro.com/us/enterprise/product-security/officescan/

[9] Trend Micro Incorporated. (2014). *Trend Micro*. "Custom Defense Solution." Last accessed November 20, 2014, http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/#why-a-custom-defense

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud