A **TrendLabs** Security in Context Paper

TREND MICRO

Data Exfiltration: How Do Threat Actors Steal Your Data?

When attackers have reached this stage, it is not a big issue for them to transfer data out.

– Spencer Hsieh
Trend Micro threat researcher

Drawing data out of the network

Advanced persistent threats (APTs) refer to a category of high-risk threats that pertain to computer intrusions by threat actors that aggressively pursue and compromise chosen target institutions or enterprises. Data exfiltration is the main goal of advanced persistent threats (APTs).

APTs strive to remain undetected in the network in order to gain access to the company's crown jewels or valuable data. These valuable data include intellectual property, trade secrets, and customer information. In addition, threat actors may also seek other sensitive data such as top-secret documents from government or military institutions.

APTs typically use social engineering techniques by crafting email content that would be contextually relevant in order to deliver exploits. These exploits are later on used to download more malware.

Once threat actors penetrate the network and establish persistent control, they can easily transfer the gathered company data. At this stage, it becomes an arduous task for system administrators to detect any malicious activity in the network.

In the asset/data discovery stage, threat actors have access to "territories" that contain valuable information and noteworthy assets. These data are then identified and transferred through tools like remote access Trojans (RATs), and customized and legitimate tools.

Threat actors identify their target information using various data monitoring and collecting tools before the actual data exfiltration. Once attackers acquire the stolen information, the impact to any organization or institution may include sabotage, data theft, and damage to brand image and reputation.

Tools of the Trade

Attackers use a mix of legitimate and malicious tools and techniques in order to extract specific data from the target's perimeter. Here are some tools and techniques we have seen used in actual APT campaigns.

- **Backdoors** have built-in upload and download functions and are commonly installed in target systems. This is a capability also observed in RATs.

  Backdoors can upload collected files and use ports like 80 and 443 (for HTTP or HTTPS) and port 53 (for DNS) to hide their traffic. These attackers can bypass the connection restriction whenever they use HTTP to transmit data and to bypass detection. Based on our investigation, there are instances when attackers manually download the .ZIP file containing all collected data.

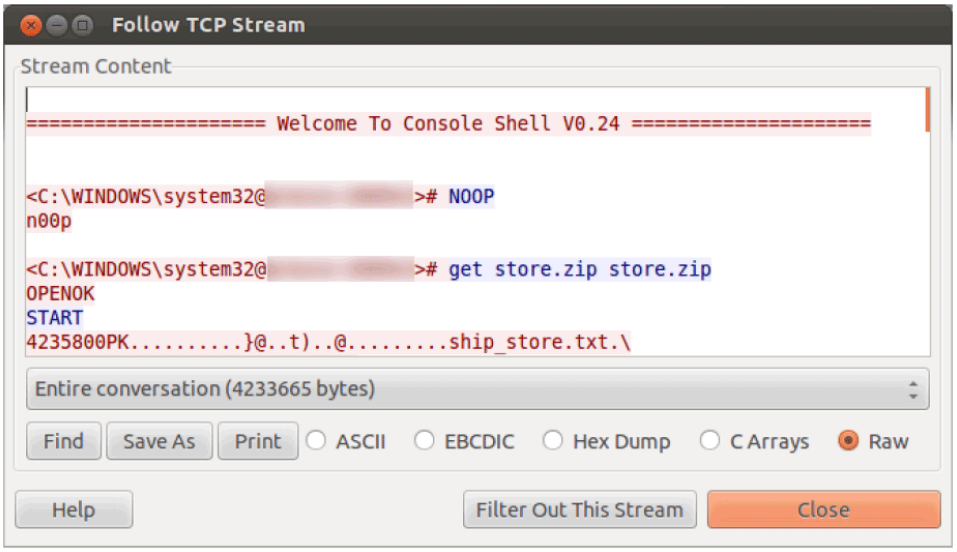

Figure 1. Screenshot of a backdoor traffic in data exfiltration

- **File transfer protocol (FTP)** is a standard network protocol used to transfer files may also be used to conduct data exfiltration.

- **Web applications:** Attackers open their own browsers and can directly access information. IT administrators won't suspect any malicious activity since connecting

to web pages outside the network isn't out of the ordinary.

- **Windows Management Instrumentation (WMI)** may be used to check the files opened by the targeted employees or users. As such, cybercriminals can easily determine and gather these files for transferring data.
- The forwarding rule in **Microsoft® Outlook®** enables attackers to receive copies of the emails that their target users receive.
- Attackers may use legitimate tools for gathering a list of file types and documents files. They may also put a timestamp to prevent duplicating the transferred data.
- Peripheral devices such as microphones and webcams may be used to record audio and video in order to monitor the targeted users' activities.

Attackers need to leverage the abovementioned legitimate tools and activities in order to hide their tracks and remain undetected in the targeted network. They also make use of built-in or HTTP file transfers. In addition, the *Tor anonymity* network masks one's location and traffic.

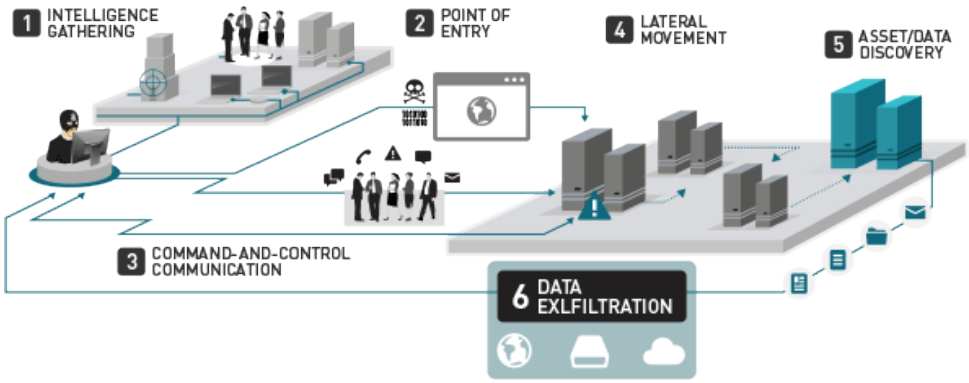

Figure 2. Stages of an APT

No Silver Bullet for APTs

Attributing attacks is often very difficult to do. Accurately ascertaining who attacked your device is a daunting task and will only provide you a small subset of possible motivations. Determining motivations is also very difficult to do, as attackers would nearly never reveal their real intentions.

Kyle Wilhoit
– Trend Micro senior threat researcher

As threat actors move deeper into a target's network, it is difficult for IT administrators to detect and mitigate APTs. Early detection then is crucial in order to prevent attackers from exfiltrating or transmitting data.

Once the IT administrator suspects any malicious activity in the network, he/she should assume compromise and trigger an investigation. This is why it is essential for enterprises to develop threat intelligence to help determine any indicators of activities that may be related to APTs.

Since email is the most common form of office communication, securing email remains a trusted solution against attackers who use it as an entry point. However, enterprises should ensure that their email security solutions are complemented by a robust security technology with real-time local and global intelligence. This can support the threat intelligence efforts of enterprises via its network-wide security event collection and analysis enabling IT administrators to carry remediation and containment plans.

It is also recommended that enterprises employ the Trend Micro™ Custom Defense Solution, an advanced threat protection platform that performs network-wide monitoring to detect zero-day malware, malicious communications, and attacker behavior that remains unseen to traditional security solutions. This security platform has sandbox simulation that enables enterprises to block spearphishing emails and exploits used by attackers during the early stages of an APT. As such, a Custom Defense strategy can prevent APTs from entering the network, moving laterally to 'territories' that house crucial company data, and subsequently, transferring these information to threat actors.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

TREND MICRO 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.

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