



CYBER SECURITY

และแนวทางการป้องกัน

Information Technology

CYBER SECURITY คืออะไร ทำไมทุกองค์กรถึงให้ความสำคัญ

Cyber Security คือเทคโนโลยี, กระบวนการและวิธีปฏิบัติที่ถูกออกแบบมาเพื่อปกป้องเครือข่าย, อุปกรณ์, โปรแกรมและข้อมูลจากการโจมตี, ความเสียหายหรือการเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต สรุปสั้น ๆ **Cyber Security** อาจเรียกว่าความมั่นคงปลอดภัยทางไซเบอร์



ความสำคัญของ **Cyber Security**

การรักษาความมั่นคงปลอดภัยไซเบอร์ มีความสำคัญอย่างยิ่ง เนื่องจากองค์กร ไม่ว่าจะเป็นภาครัฐหรือเอกชนต่างรวบรวม, ประมวลผลและจัดเก็บข้อมูลจำนวนมากบนคอมพิวเตอร์และอุปกรณ์อื่น ๆ ซึ่งข้อมูลเหล่านั้นอาจเป็นข้อมูลที่ค่อนข้างละเอียดอ่อนไม่ว่าจะเป็นทรัพย์สินทางปัญญา, ข้อมูลทางการเงินข้อมูลส่วนบุคคลหรือข้อมูลประเทศอื่น ๆ ที่บุคคลอื่นสามารถเข้าถึงหรือเปิดเผยได้โดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อด้านลบกับองค์กรได้ เพราะองค์กรมักส่งข้อมูลที่มีความสำคัญข้ามเครือข่ายและอุปกรณ์ในการทำธุรกิจ ข้อมูลเหล่านั้นจึงควรได้รับการปกป้องโดยเฉพาะในยุคที่การโจมตีทางไซเบอร์นั้นมีความซับซ้อนมากขึ้น การโจมตีทางไซเบอร์และการสอดแนมทางดิจิทัลเป็นภัยคุกคามที่สำคัญที่สุดต่อการทำธุรกิจ

ดังนั้นเพื่อความปลอดภัยบนโลกไซเบอร์ที่มีประสิทธิภาพองค์กรจำเป็นต้องมี **Cyber Security** เพราะมันเป็นสิ่งที่ครอบคลุมสิ่งต่อไปนี้

- **Network security** : เป็นกระบวนการปกป้องเครือข่าย หรือเน็ตเวิร์คจากผู้ใช้ที่ต้องการการโจมตีและการบุกรุก
- **Application security** : แอปพลิเคชันต้องการการอัปเดตและการทดสอบอย่างต่อเนื่องเพื่อให้แน่ใจว่าโปรแกรมเหล่านี้ปลอดภัยจากการโจมตีของบุคคลที่สาม
- **Data security** : สิ่งที่อยู่ภายในเครือข่ายและแอปพลิเคชันคือข้อมูล การปกป้องข้อมูล บริษัท และลูกค้าเป็นความปลอดภัยอีกชั้นหนึ่ง
- **Cloud security** : ในปัจจุบันไฟล์จำนวนมากอยู่ในสภาพแวดล้อมแบบดิจิทัลหรือ“ คลาวด์” การปกป้องข้อมูลในสภาพแวดล้อมที่เป็นออนไลน์ถือเป็นความท้าทายอย่างหนึ่ง ที่

```
charset="<?php bloginfo( 'charset' ); ?>"  
<?php wp_title( '|', true, 'right' ); ?>"  
rel="profile" href="http://gmpg.org/xfn/11" />  
rel="pingback" href="<?php bloginfo( 'pingback_url' ); ?>"  
fruitful_get_favicon(); ?>  
wp_head(); ?>  
<?php body_class();?>  
<div id="page-header" class="hfeed site">  
$theme_options = fruitful_get_theme_options();  
$logo_pos = $menu_pos = '';  
if (isset($theme_options['logo_position']))  
$logo_pos = esc_attr($theme_options['logo_position']);  
if (isset($theme_options['menu_position']))  
$menu_pos = esc_attr($theme_options['menu_position']);  
$logo_pos_class = fruitful_get_class($logo_pos);  
$menu_pos_class = fruitful_get_class($menu_pos);  
$responsive_menu_type = fruitful_get_class($responsive_menu_type);
```

ทำความรู้จักกับมัลแวร์
(MALWARE) และ
วิธีการป้องกันง่าย ๆ
ด้วยตัวคุณเอง



MALWARE

Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (**Malware**) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (**Virus**), หนอน (**Worm**), โทรจัน (**Trojan**), สบายแวร์ (**Spyware**) เป็นต้น ดังนั้น ผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในทุกรูปแบบ รวมถึงการป้องกันตัวเองจากมัลแวร์ง่าย ๆ ที่ใคร ๆ ก็สามารถทำได้



ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

- **Virus:** มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น
- **Worm:** สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์
- **Trojan:** หลอกล่อผู้ใช้งานว่าเป็นโปรแกรมที่ปลอดภัย แต่จริง ๆ แล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้งานหลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย
- **Backdoor:** เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว
- **Rootkit:** เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)
- **Spyware:** แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย
- **Ransomware:** ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

ข้อเสนอแนะในการป้องกันการติดมัลแวร์

1. อัปเดตคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
2. ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
3. ระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดรฟ์ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
4. ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ
5. ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่
6. หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

การใช้งานโปรแกรม Antivirus Apex One

The screenshot displays the Trend Micro Apex One Security Agent interface. At the top, a red header bar contains the logo and the text "Trend Micro | Apex One Security Agent". Below this, a large green checkmark icon is followed by the text "Protection Enabled" and "You are protected and your software is up to date".

The main content area is divided into several sections:

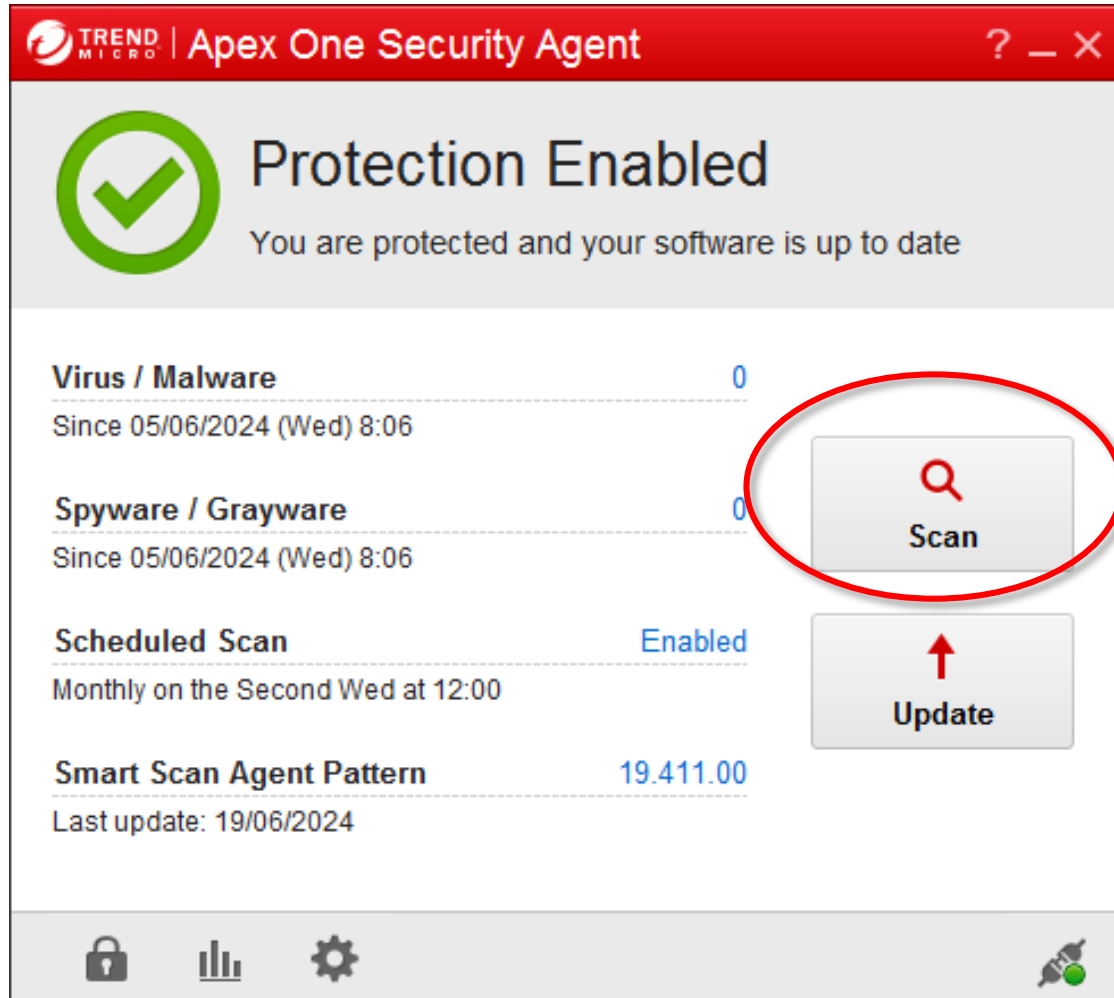
- Virus / Malware:** Shows a count of 0 and a last scan time of "Since 05/06/2024 (Wed) 8:06".
- Spyware / Grayware:** Shows a count of 0 and a last scan time of "Since 05/06/2024 (Wed) 8:06".
- Scheduled Scan:** Shows "Enabled" and "Monthly on the Second Wed at 12:00".
- Smart Scan Agent Pattern:** Shows a count of 19,411.00 and a last update of "19/06/2024".

On the right side, there are two buttons: "Scan" (with a magnifying glass icon) and "Update" (with an upward arrow icon).

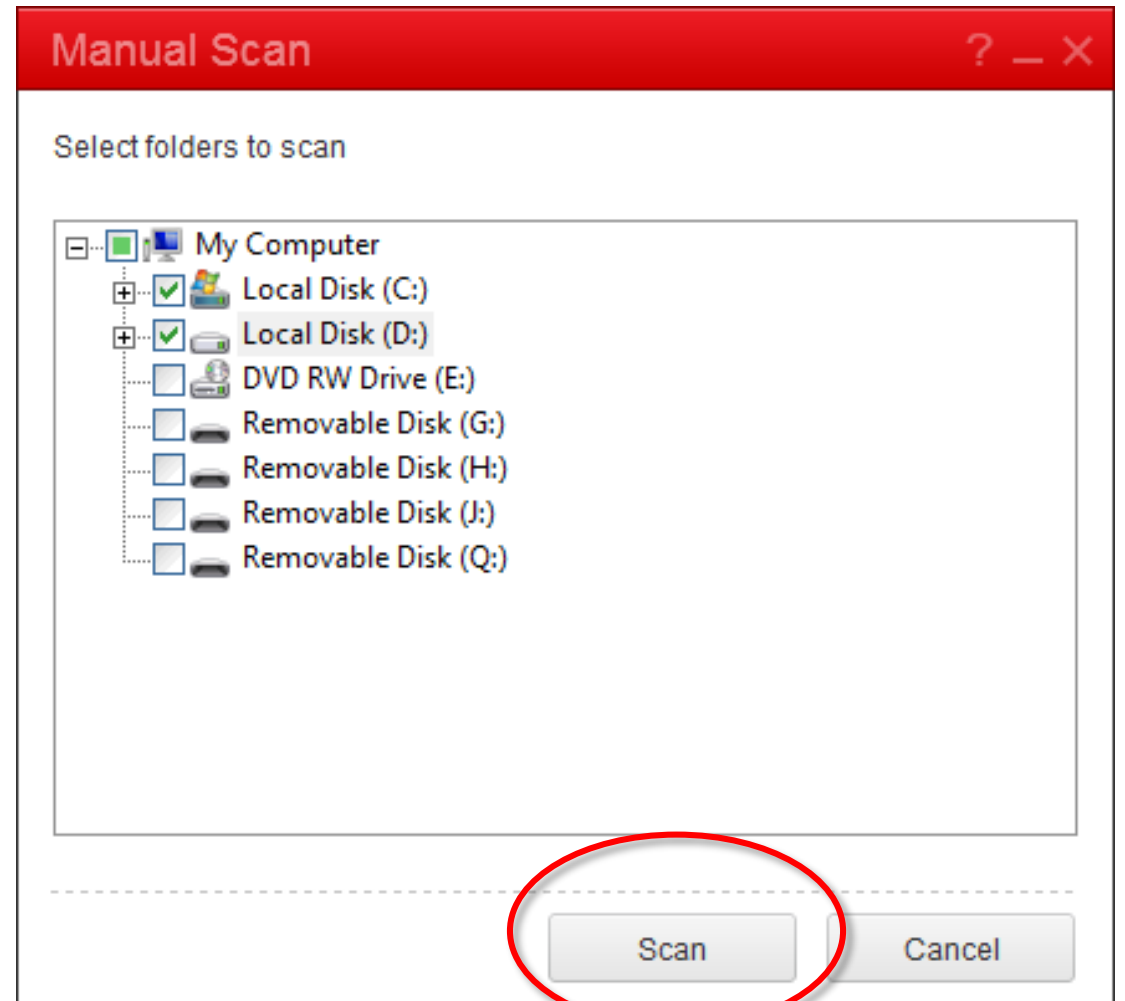
At the bottom of the interface, there is a navigation bar with icons for a lock, a bar chart, and a gear. A red arrow points from the gear icon to a system tray notification for "Trend Micro Security Agent (Online)", which lists "Real-time Scan (Enabled)" and "Smart Scan (Connected)".

The system tray at the bottom right shows the language set to "EN", the time as "8:34 AM", and the date as "20/06/2024".

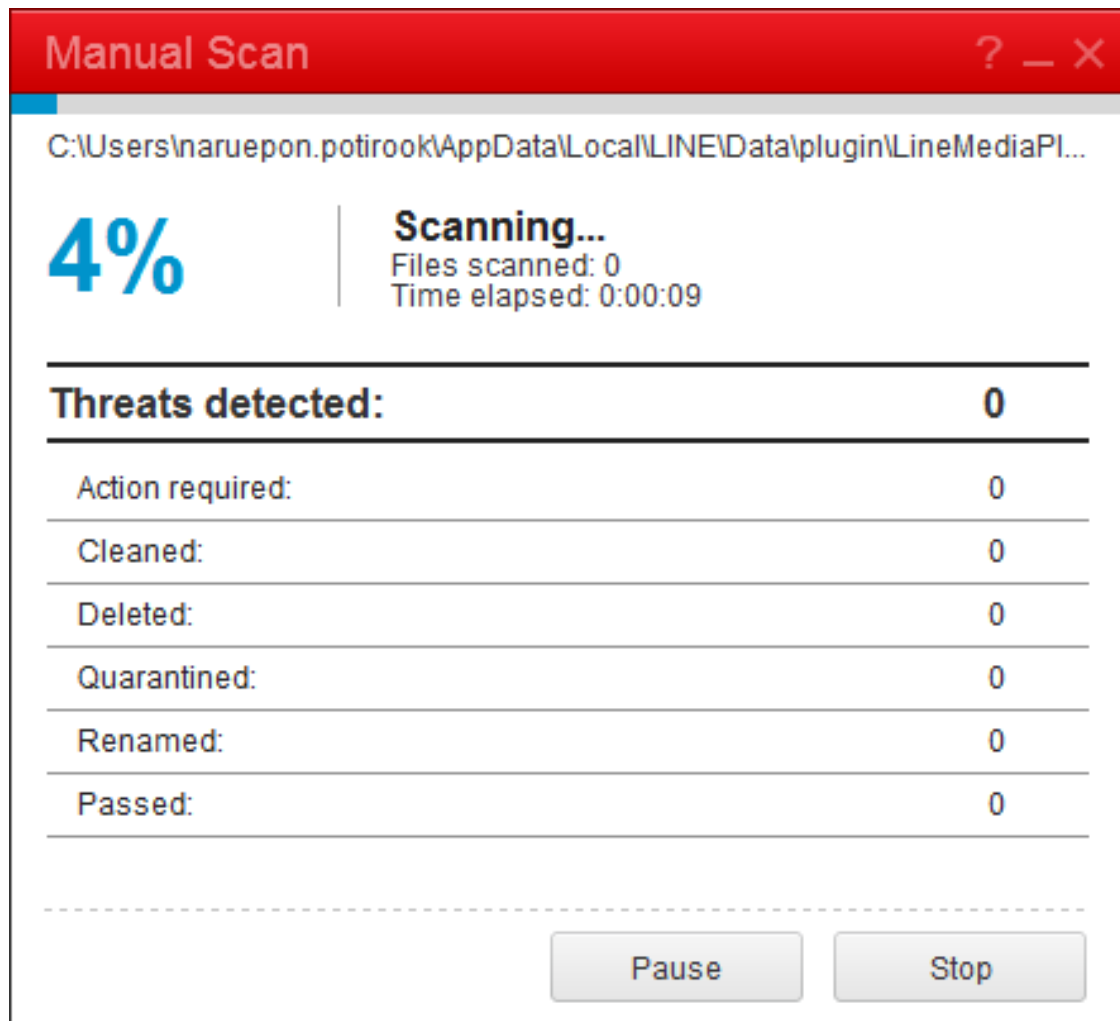
- Click Scan



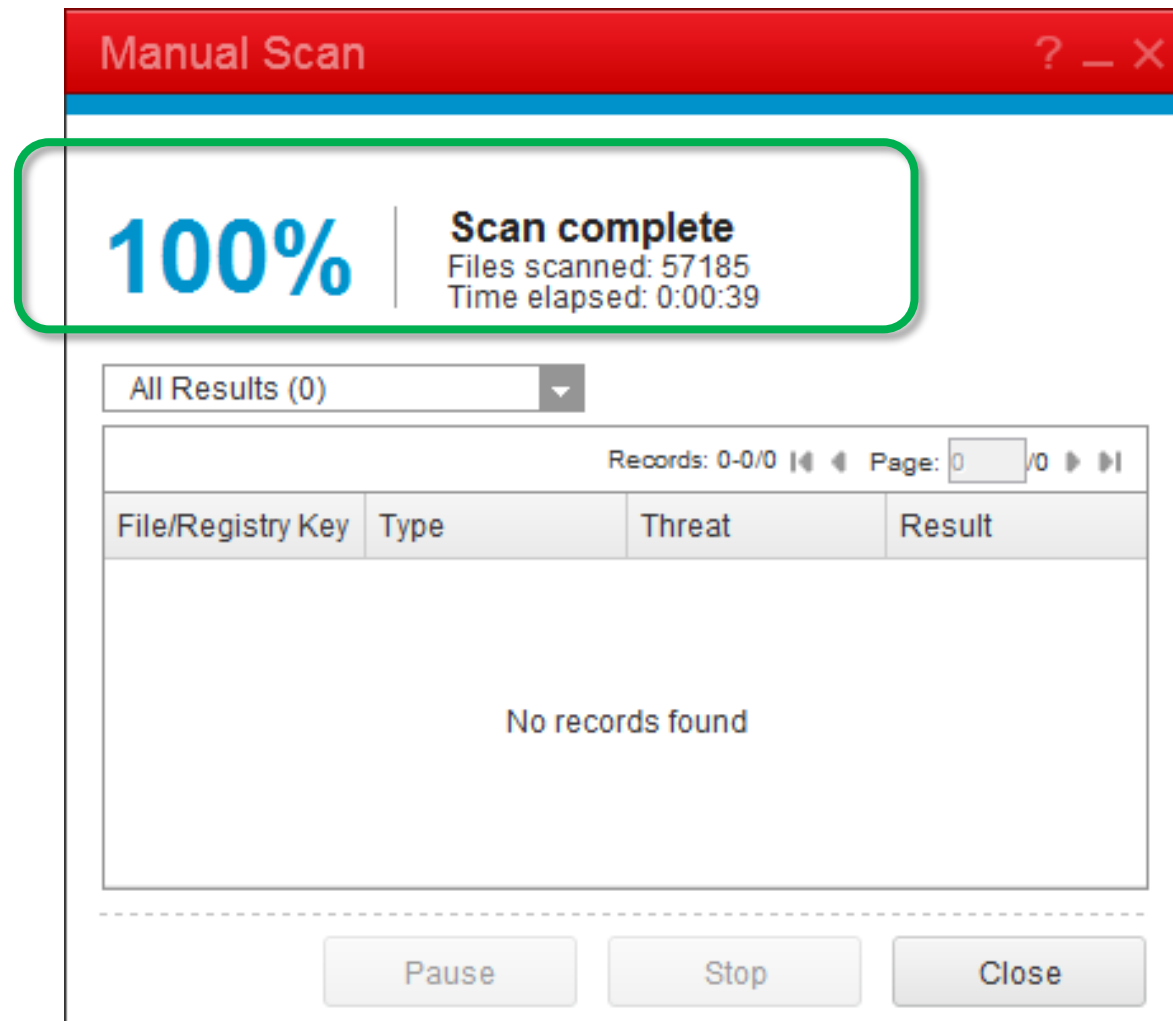
- เลือก Drive ที่ต้องการ Scan Virus กดปุ่ม Scan



- เครื่องจะเริ่ม **Scan Virus**
และ **Show %** การทำงาน



- หลังจาก **Scan** ครบ 100% จะโชว์
Report การตรวจ **Virus**





THANK YOU