**What it is**

Rombertik is a form of spyware designed to steal confidential information from targets using IE, Firefox, or Chrome running on windows OS. If by any chance that Rombertik is detected by anti-malware software, it will attempt to destroy the Operating System.

**How it works.**

* **Phishing**
  1. Rombertik has been identified to propagate itself through spam and phishing emails. The message on the screen is one of the examples discovered by Cisco Talos Security and Intelligence Group.
  2. The program is disguised as a PDF document, but really it’s a .SCR (Screensaver executable) extension file.
  3. Once launched, Rombertik will begin to compromise the system.
* **Anti-analysis**
  1. One method it has to avoid discovery, is that 97% of it is garbage code that includes over 8000 functions that are never used. This is all just to overwhelm analysts by making it impossible to look at every function.
* **Sandbox evasion**
  1. To avoid discovery, Rombertik uses a similar method to sleeping, which forces the sandbox to time out. But instead of sleeping, it writes a byte of data to memory 960 million times. This is designed to consume time like sleeping but instead overwhelms tracing tools. Application tracing tools cannot trace all of the data because it would take about 100 gigabytes of memory and about 25 minutes to write it to a typical hard drive.
  2. After stalling the analysis environment, Rombertik check to see if analysis tools have modified code in the Windows API ZwGetWriteWatch routine. It calls the function with false parameters and waits for a specific error. If the routine doesn’t return with that specific error then Rombertik terminates. It terminates because sandboxes will suppress specific errors and return a generic one.
  3. Once it passes the ZwGetWriteWatch, then Rombertik calls the OutputDebugString function 335,000 times as an anti-debugging mechanism.
  4. Then finally, an anti-analysis function within the packer is called to check the username and file extension of the executing process for strings like “malwar”, “sampl”, “viru”, and “sandb”. If it detects any of them, it will stop unpacking and terminate. At this point the anti-analysis checks are done.
  5. Once the packer is done with the anti-analysis checks, it then checks to see if it’s executing from the right location(%AppData%\rsr\yfoye.exe). If not then it will proceed to install itself in order to ensure persistence across system reboots before it starts to execute its payload.
     + To install itself, Rombertik creates a VBS script named “fgf.vbs”, which is used to kick off Rombertik every time the user logs in, and places the script in the users Startup folder.
  6. Rombertik then creates %AppData%\rsr\yfoye.bat and moves the packed version of itself into %AppData%\rsr\yfoye.exe.
  7. If Rombertik detects it is already executing from %AppData%\rsr\yfoye.exe.
     + The malware will then begin decrypting and executing the main unpacking code in memory.
     + Yfoye.exe is launched a second time to create another process of the malware.
     + Once the unpacking is complete, Rombertik will overwrite the memory of the new process with the unpacked executable code.
     + The unpacking code is monstrous and has many times the complexity of the anti-analysis code.
     + The code contains dozens of functions overlapping with each other and unnecessary jumps added to increase complexity.

**What it does.**

* **Blastware**
  1. Once the unpacked version of Rombertik starts executing, it runs one last anti-analysis check. This anti-analysis is pretty nasty when discovered because it will terminate your operating system. The way it does this is by overwriting your MBR (Master Boot Record) which will render the OS inoperable.
  2. If it does not have the required permissions to overwrite the MBR, then it will destroy all of the users files in the home folder (C:\Documents and Settings\Administrator\) by encrypting every file with a random RC4 key. After the MBR is overwritten or the home folder is encrypted, then the computer will restart.
* **MBR Overwrite**
  1. The MBR contains code that is executed before it starts. Rombertik overwrites the code with a message and puts it in to an infinite loop that prevents the OS from starting.
  2. The MBR also contains information about the disk partitions. The altered MBR overwrites the bytes for these partitions with Null bytes, making it even more difficult to recover data from the sabotaged hard drive.
* **Spyware**
  1. Rombertik scans currently running browsers. If IE, Firefox, or Chrome is detected, it will then inject itself in to the process and hook API functions that handle plain text data. Then Rombertik captures any data the user types that is sent over HTTPS. This allows the malware to collect data such as usernames and passwords.
  2. Collected data is then Base64 encoded and forwarded to [www.centozos.org.lin/don1/gate.php](http://www.centozos.org.lin/don1/gate.php) through HTTP with no encryption.

**Who does it affect?**

* Anyone with an email account and a computer is in danger of getting infected by Rombertik.

**Cost**

**Monetary value**

* Depends on how big the company is or what type of information the program will copy.4

**Human expense**

* Depends on what you had on the computer

**Privacy Implications & Concerns.**

* The worst case scenario here is that your bank accounts may be compromised or identity may be stolen.
* Best case scenario is that it destroys your OS before any of your private information is stolen.

**Technical issues**

* Technical issues could be re-installing the OS or having to recover sensitive data from the hard drives.

**What Rombertik really is.**

* Rombertik is actually a modified version of the crimeware kit carbon FormGrabber. It was created by a commercial criminal enterprise for cybercriminals who don’t have the skill to create it themselves. The destructive mechanism was originally created for anti-piracy methods. The creators of FormGrabber didn’t want people using their software without the proper permissions. Who would have thought? The FormGrabber was developed specific to each client’s Command and Control server and no other. This is where novice hackers would think that they can just identify the C&C address in the binary code and just modify it. Well they thought wrong, this is where the anti-piracy kicks in and does its destructive business. A bit cut throat I would say.