MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
03 December 2015

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 0312-28-2015

1. References:

   a. Command Guidance
   b. Cybersecurity Awareness
   c. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cyber Security Bulletin number 036 with topic regarding **ROMBERTIK- Self-destructing virus kills off PCs.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cyber Security Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC) PA AC OF S FOR CEIS, G6, PA	

Army Core Purpose: Serving the people. Securing the land.

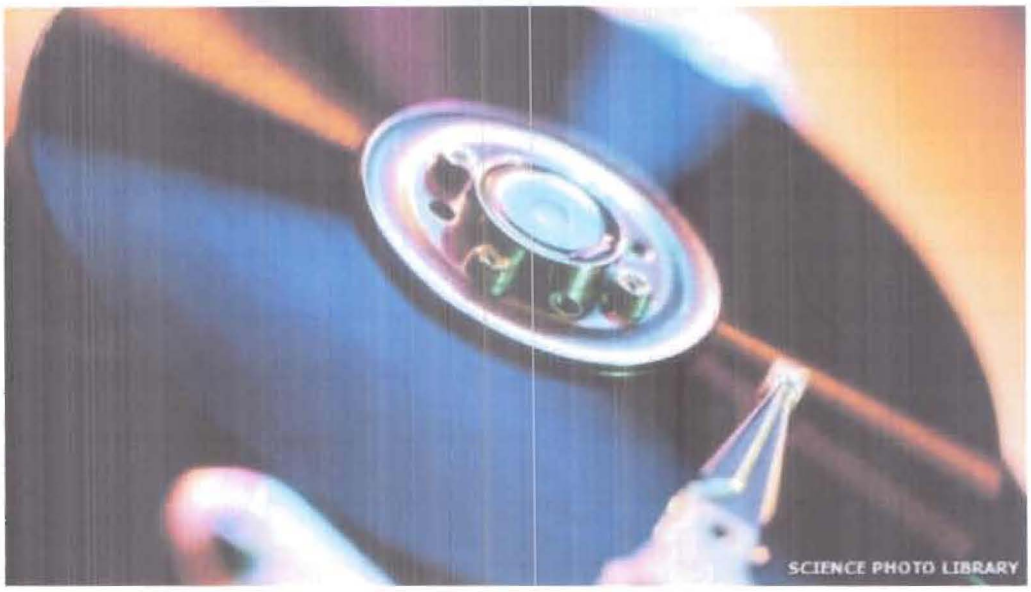
HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 03 December 2015

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #36

ROMBERTIK - Self-destructing virus kills off PCs



The Malware also tries to fool security tools by flooding hard drive with data

A computer virus that tries to avoid detection by making the machine it infects unusable has been found.

If Rombertik's evasion techniques are triggered, it deletes key files on a computer, making it constantly restart.

Analysts said Rombertik was "unique" among malware samples for resisting capture so aggressively.

On Windows machines where it goes unnoticed, the malware steals login data and other confidential information.

Endless loop

Rombertik typically infected a vulnerable machine after a booby-trapped attachment on a phishing message had been opened, security researchers Ben Baker and Alex Chiu, from Cisco, said in a blogpost.

Some of the messages Rombertik travels with pose as business enquiry letters from Microsoft.

The malware "indiscriminately" stole data entered by victims on any website, the researchers said. And it got even nastier when it spotted someone was trying to understand how it worked.

"Rombertik is unique in that it actively attempts to destroy the computer if it detects certain attributes associated with malware analysis," the researchers said.

The malware regularly carries out internal checks to see if it is under analysis.

If it believes it is, it will attempt to delete an essential Windows system file called the Master Boot Record (MBR).

It will then restart the machine which, because the MBR is missing, will go into an endless restart loop.

The code replacing the MBR makes the machine print out a message mocking attempts to analyse it. Restoring a PC with its MBR deleted involves reinstalling Windows, which could mean important data is lost.

Rombertik also uses other tricks to foil analysis.One involves writing a byte of data to memory 960 million times to overwhelm analysis tools that try to spot malware by logging system activity.

Security expert Graham Cluley said destructive viruses such as Rombertik were quite rare. "It's not the norm," he said. "That's because malware these days doesn't want to draw attention to itself, as that works against its typical goal - to lie in wait, stealing information for a long time."

SOLUTION

Ironically, getting hit right away by Rombertik's data-wiping payload is probably a safer outcome than being infected for days or weeks without noticing. Remember that the non-destructive part of the malware sets out, amongst other things, to snoop on your browsing and steal your data, perhaps even your identity.

Either way, as with any malware, your best bet is not to get infected in the first place:

- Keep your operating system and applications patched.
- Use an active anti-virus and keep it up-to-date.
- Avoid unexpected attachments.
- Try stricter filtering at your email gateway.
- And these precautions will shield you against all sorts of catastrophes, not just destructive malware:
- Only logon with Administrator privileges when you genuinely need to.

- Take regular backups, and keep one backup set off-site.
- Remove unnecessary or unwanted software so there is less to go wrong.

References:

- *www.securityweek.com › Virus & Malware*
- *https://nakedsecurity.sophos.com/2015/05/06/can-the-rombertik-malware-really-destroy-computers-no-no-three-times-no/*