EC-COUNCIL

WANNACRYPT / wannacry: UPDATED BRIEFING

FROM THE DESK OF EC-COUNCIL GROUP CISO

CONTENTS

WHAT IS WANNACRYPT?
(WannaCry / Wcry)

A new ransomware attack, perhaps the largest so far, was designed to work only against unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems.

200K machines have been infected in just a few days.

INFECTION PROCESS

- Arrives via phishing email (pdf) and spreads like a worm using covert channels and exploiting the Windows SMB vulnerability (aka EternalBlue), which was fixed by Microsoft in March (MS17-010)
- Payload delivered via exploit running as a service
- It performs encryption in the background, with key-built in (no contact to C2 necessary)
- Uses tor to stay anonymous
- Drops ransom notes in 25+ languages
- Encrypts shared and local files (176 types of files)

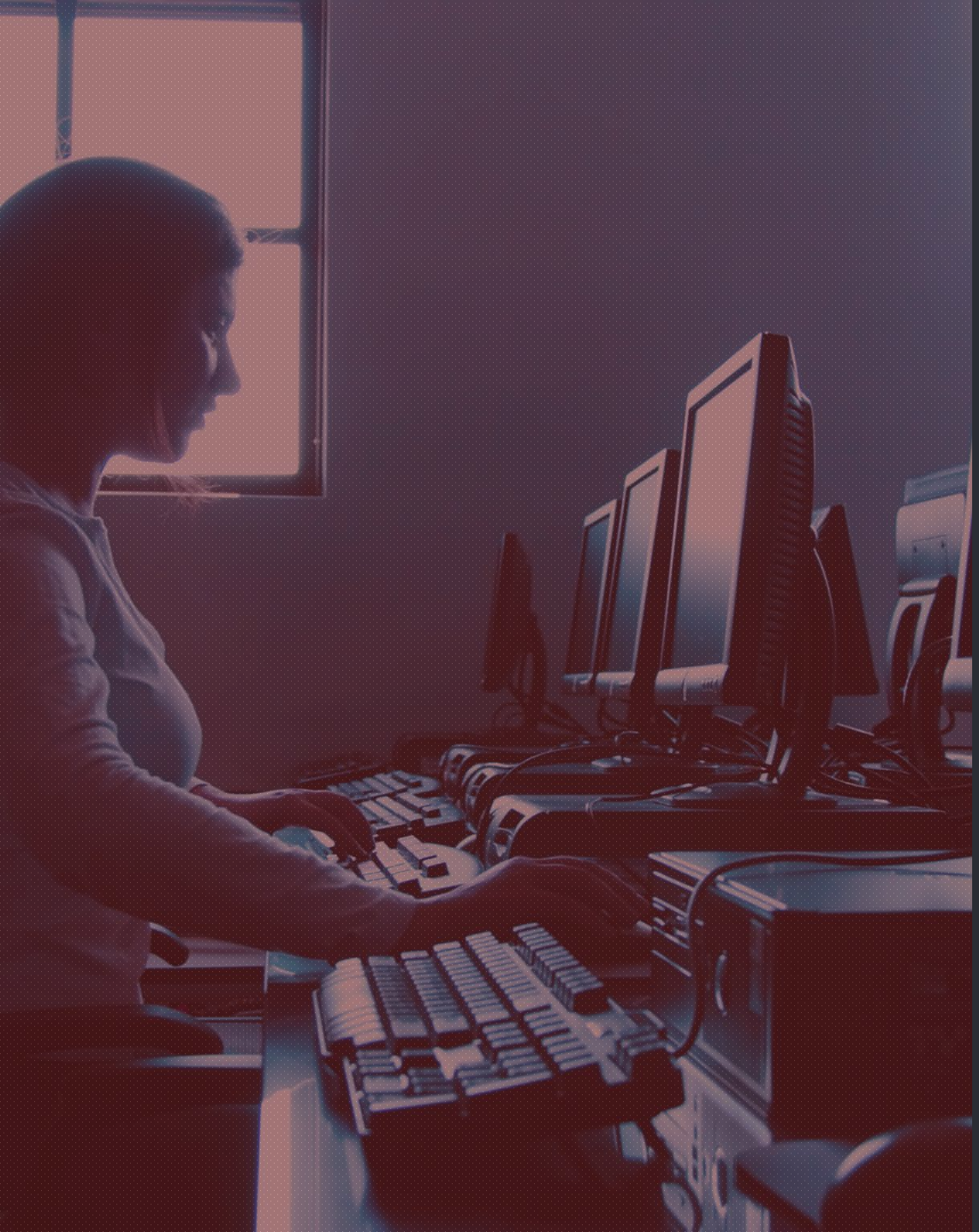
Ransom note demands $300 within 3 days or $600 within 6 days or lose files.

There is no guarantee of recovery of files.

The CISO Guide to WannaCry malware

- Patch and update immediately
- User Awareness (Phishing, Attachments, Respond and Report)
- Block SMB
- Improve Detection by implementing IoCs in SoC, where available
- Perform backup and DB integrity checks
- Updated AV/Anit-Malware systems

- **Patch, Patch, And Patch**
  - Windows machines and servers (MS released patches for legacy versions) URL
  - EternalBlue exploit (MS17-010) URL
- **Prevent Phishing Mails And Suspicious Attachments**
- **Prepare Users (User Awareness Script)**
  - Remind them how to recognize phishing mails
  - Tell them not to click suspicious attachments
  - Tell them what to do if they think they are infected - disconnect from the network and report to Infosec team / IT team, for example.
- **Avoid Smb (Port 445) And Rdp On Servers [Guidance]**
- **Backup & Db - Check Integrity Periodically**
- **Implement Iocs Into Soc And Timely Incident Response**
- **Ensure Antivirus And Antimalware Is Up To Date And Have Latest Definitions To Prevent Infection**
- **If infected**
  - Report to Law enforcement agencies and ISAC (where applicable)
  - Activate your incident response plan



User Awareness Script

- Phishing
- Attachments
- Respond and Report

Dear Colleagues,

As you may have heard, in last few days a massive cyber attack has infected machines around the world. The attack, called "WannaCry", locks users out of their own systems and demands a ransom payment to release files. WannaCry has so far has impacted over 120 countries (and counting) and a large number of computers.

In this heightened situation, we request you to stay vigilant while using your computers. While dealing with any emails from any unknown email address, do not click any link or open any unknown attachments.
We request you to follow the best practices outlined below while performing your daily operations:

- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list.
- Do not click on any URLs contained in an unsolicited e-mail.
- Report any suspicious emails or attachments to the IT/IS team.
- Follow the Computer Usage policy. <link to corporate policy>
- Do not download software, videos, MP3s, etc.
- Check that your antivirus is updated and running in any machine you are using.
- Backup your critical data periodically.

If you believe your computer has been infected, immediately disconnect your machine from the network by pulling the LAN cable out of the port in your computer and call the information security team. Do not try to restore any data on your own.

<CISO Signature Block>

REFERENCES

Prepared by Subrahmanya Gupta BODA, Group CISO, EC-Council, C|CISO,
gupta.boda@eccouncil.org

- Overview
  - https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
  - https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/
  - https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis (Technical Analysis)
- Spread / impact
  - https://intel.malwaretech.com
- Advisories
  - https://www.us-cert.gov/ncas/alerts/TA17-132A
  - https://www.gov.uk/government/news/ransomware-guidance-from-the-national-cyber-security-centre
  - https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance
- Prevention Scripts
  - http://www.hackatrick.com/2017/05/wannasmile-simple-tool-to-protect-from-wannacry-ransomware.html
  - https://www.ccn-cert.cni.es/en/updated-security/ccn-cert-statements/4485-nomorecry-tool-ccn-cert-s-tool-to-prevent-the-execution-of-the-ransomware-wannacry.html
- Decryption related
  - http://sensorstechforum.com/wncry-wannacry-virus-how-to-restore-encrypted-files-may-2017/

DISCLAIMER

This briefing is for informational purposes only and should not be utilized as a solution to the WannaCry attack. If you believe you have been affected or have questions on how to remediate, reach out to a security consulting company.