TASK 1

Investigative approach on Ransomware attack

By Kowshik Kumar Aitha

GCPCSSI 2021 INTERN

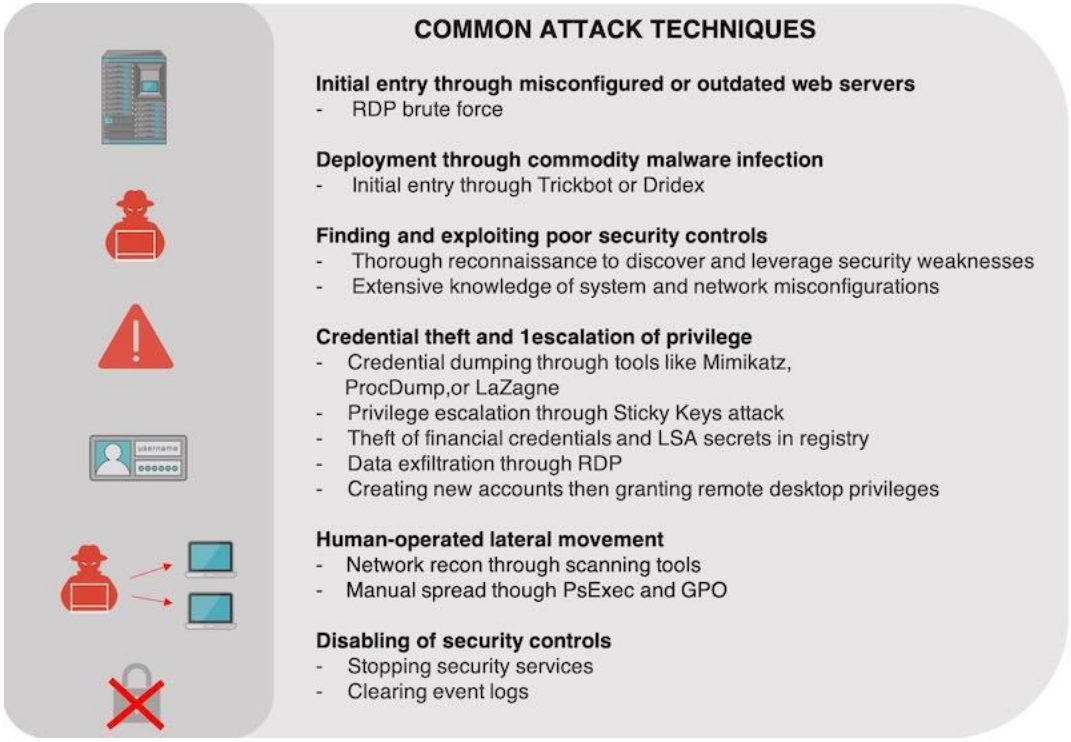
The tools used against ransomware attack -

- Bitdefender Antivirus Plus. The best **ransomware** protection. ...
- AVG Antivirus. Another good defense **against ransomware**. ...
- Avast Antivirus. Solid protection **against ransomware**. ...
- Webroot Antivirus. ...
- ESET NOD32 Antivirus. ...
- Malwarebytes Anti-Malware. ...
- Avast Free **Ransomware** Decryption **Tools**. ...
- Kaspersky Anti-**Ransomware Tool**.

The most common method used for ransomware attack - phishing emails

Techniques used to investigate ransomware attack –

- **Threat hunting** is a proven methodology for identifying ransomware.



What You Should Do When Ransomware Attacks

- Step 1: Understand Your Situation. You've been infected by malware. ...
- Step 2: Lock It Down. At this time, all we know is that you're infected. ...
- Step 3: Shut Down Patient Zero. ...
- Step 4: Identify the Infection. ...
- Step 5: Verify Your Backups. ...
- Step 6: Paying the Ransom. ...
- Step 7: Decrypting.

Ransomware Protection Tips –

1. Don’t click links in emails
2. Scan emails for malware
3. Firewalls and endpoint protection
4. Notify users of out-of-network emails
5. Backup your files
6. Protect your information
7. Keep your computer patched and up to date

Case Studies –

200 accounts ‘locked’: In Delhi’s first WannaCry attack, publishing firm hit

After the WannaCry ransomware cyber-attack spread like wildfire and paralyzed computer systems across the world, isolated incidents were reported from Andhra Pradesh, Gujarat, Kerala and West Bengal. Now, the capital has seen its first ransomware cyber-attack, with employees of Rachna Sagar Private Limited “locked” out of more than 200 computers.

The cyber-attack was reported on August 9 when staff at the publishing company found that they could not log into their user accounts, and could only use the “demo” account. The WannaCry malware attack exploits potential vulnerabilities of computer systems as hackers encrypt all files and demand ransom in exchange for unlocking them.

SamSam 2018 attack -

SamSam ransomware was identified a few years ago, more precisely in late 2015. But it was in 2018 that it gained much more prominence after infecting the city of Atlanta, the Colorado Department of Transportation and the Port of San Diego, in the U.S., abruptly stopping services.

In the same year, two Iranian hackers were accused of using SamSam against more than 200 organizations and companies in the U.S. and Canada, including hospitals, municipalities and public institutions. A loss of USD 30 million is estimated as a result of the attacks.

Investigative approach on Ransomware attacks can be done with AI – ML

Processes and Tools of Ransomware Detection

1. Cuckoo Sandbox
2. WEKA (Waikato Environment for Knowledge Analysis)
3. Ransomware detection taxonomy
4. Ransomware infection vectors
5. Using Regularized Logistic Regression
    - Pr (R = 1 x, T w, b) = sgm (w x +b).
6. Gradient Tree Boosting
    - $F(x, \beta, \alpha) = \sum \beta ih (z, \alpha i)$.
7. Ransomware Detection using Random Forest Technique
    - The random forest prediction is based on the majority voting for the result of the combination predictions of multiple decision trees. The decision tree is first constructed and based on the best combination of variables then the dataset will be spilled in to subtrees.

Submitted by

Kowshik Kumar Aitha

GCPCSSI 2021 INTERN