Not All Hope Is Lost: Planning For An Effective Defense-in-Depth Against APTs

ChiBrrCon 2022
Chicago, IL

Dr. Pranshu Bajpai
@AmlRootYet
Security Architect
Agenda

● Introduction

● The State of the Cybercrime Underground

● Case Studies

● Cyber Defense Matrix and Threat Intelligence

● Questions and Answers
INTRODUCTION
Overall Threat Landscape - Industry and Threat Actors
STATE OF THE CYBERCRIME UNDERGROUND
THREAT ACTORS - BOTH EXTERNAL AND INTERNAL
A MODERN ATTACKER - ADVANCED, RESOURCES, AND MOTIVATED

EXTERNAL

Organized Crime
55%
Crime ring and gang activity

State Actors
11%
Nation-state actors or advanced persistent threat

Unaffiliated
4%
No specified or affiliated group

INTERNAL

System Admins
10%
Insiders in the form of system administrators

End Users
9%
Employees or end users of a system

Other
11%
Did not fall into any other category
RANSOMWARE TRENDS

Ransomware Attacks on Public Safety: Jan 2019 - March 2021

Total value received by ransomware addresses per year, 2013 - 2020

Image: Chainalysis
RANSOMWARE-AS-A-SERVICE
UNDERGROUND DARK MARKETS

[NEW][HOT][BITCOIN] Ransomware-as-a-Service

Hello!
We present you new Ransomware As A Service.

Features:
- Fully customizable.
- You will get 50% of decryption price.
- Instant withdraw.
- Support for all versions beginning with Windows XP.

More info:

- dot2 -------- onion.to
- dot2 -------- onion.nu
- dot2 -------- hiddenservice.net
- dot2 -------- onion.casa
- dot2 -------- onion

Price: $40

Following features:
- Small stub size
- Loader accept encryption Like botnets, Rats
- Bypass UAC
- Delete Shadow copy
- Encryption speed faster than ever
- Uses a hybrid combination of encryption algorithms (AES-256 and RSA 2048)
- Used asymmetric encryption It uses the public key in to encrypt the symmetric key
- Track the number of victims

New User

Price: $40

It is an attractive price. But it could rise in the future.

Telegram: [URL]
Email: [URL]
Demo Videos: https://youtu.be/YaRlbncC8w
THE MENACE OF RANSOMWARE
CAUSE AND EFFECT

- GandCrab shows *responsiveness* of ransomware developers
- Satan ransomware shows *diversity* and *refinement* in attack vectors
- *Targeted* and *manual* ransomware attacks are gaining traction
- Increasing ransom demands indicate successful business model

Example scenario

- Organization hit with a novel ransomware
  - Attack vector: EternalBlue exploit
  - Impact: Multiple systems
  - Demand: $100,000 - $5,000,000
MAPPING TACTICS, TECHNIQUES, PROCEDURES
UNDERSTANDING THE ATTACK STAGES

(ADAPTED) RANSOMWARE KILL CHAIN

PREPARATION
Weaponize modules

EXPLOITATION
Launch payload

PERSISTENCE
Maintain foothold

RECONNAISSANCE
Initial entry & execution

ENUMERATION
Discover valuable assets

Diligence
Remove backups

OBJECTIVE
Maximize revenue

Minutes to Months

Covert operations

Days to Weeks

Ransom extraction
CYBERSECURITY CHALLENGE
GAINING VISIBILITY AND UNDERSTANDING ENTRY POINTS

PUBLIC SAFETY CLOUD SERVICES

ENTERPRISE IT ENVIRONMENT
- Dispatch Workstations
- Mobile Dispatch
- Web Sites
- Email
- IP workstations
- Printers
- SaaS Applications
- Wireless Networks
- Legacy Devices

CUSTOMER ENTERPRISE NETWORK
- Cloud Services
- Networks
- IP Endpoints

LAND MOBILE RADIO

911 CALL HANDLING
- COMPUTER AIDED DISPATCH
- RECORDS & EVIDENCE
- VIDEO SECURITY
CYBER DEFENSE MATRIX
WHAT ARE WE DEFENDING AND HOW?
THREAT MODELLING - RECONNAISSANCE

ADVERSARY
Potential entry points
- Social engineering
- Remote desktop services
- Known vulnerabilities
- Compromised credentials
- Supply chain
- Misconfiguration

DEFENDER
Visibility and Risk Identification
- Inventory systems
- Identification of vulnerabilities (technical and nontechnical)
- Catalogue hardware and software
- Collect logs from all systems and establish baseline
- Gather threat intelligence from multiple sources
THREAT MODELLING - PREPARATION

ADVERSARY

Weaponize modules
- Connect to C2 server
- Plant backdoors
- Connect to APIs

DEFENDER

Risk reduction
- Security awareness training
- Incident response exercises and penetration tests
- Mitigate network and host vulnerabilities
- Compartmentalize access to resources
THREAT MODELLING - ENUMERATION

ADVERSARY

* Discover valuable assets
  * Silent exploration
  * Map systems, networks, services
  * Lateral movement

DEFENDER

Anomaly Detection

* Monitor network traffic for unusual connections, endpoints for suspicious processes, and analyze security tools 24/7
* File integrity monitoring on systems where possible
* Malware scanning in place
THREAT MODELLING - EXPLOITATION

ADVERSARY

Payload execution
- Data encryption
- Take resources offline

DEFENDER

Response Actions
- Incident handling procedure/team engaged
- Quarantine and isolate infected systems
- System is down, pen and paper is your new medium for taking calls
THREAT MODELLING - DILIGENCE & PERSISTENCE

ADVERSARY

Leave no alternatives

- Remove access to system and network backups

DEFENDER

Recovery

- System level backups - Keep an eye on deletion of shadow copies stored on windows systems
- Network backups - offline and usable (not on network and recent enough to provide value if restored and multiple versions)
THREAT MODELLING - OBJECTIVE
ADOPT A HOLISTIC SOLUTION FOR CYBERSECURITY
IDENTIFY A FRAMEWORK - NIST

1. KNOW YOUR NETWORK - Hardware, Software, Applications, Data Flows

2. KNOW YOUR ADVERSARY - Who is attacking you and how might they do it?

3. PATCH, PATCH, PATCH - This is not easy to execute operationally but it is essential

4. KNOW WHAT NORMAL LOOKS LIKE - The only way to detect abnormal

5. EDUCATE YOUR USERS - Cybersecurity is everyone's responsibility

6. KNOW HOW TO RESPOND TO A CYBER ATTACK - Train Hard, Fight Easy
Questions & Answers
THANK YOU