Living with Ransomware

The New Normal in Cyber Security

Vishal Thakur (Ankura, Australia)
John Lopes (Ankura, Australia)
Introduction: Presenters

Vishal Thakur
Senior Director – DFIR, Ankura
@vishUwell

John Lopes
Senior Director – DFIR, Ankura
Agenda

- Current Ransomware Threat Landscape
- Ransomware Groups: Motivation and Operation
- Managing Ransomware Attacks
- Interesting Real-world Cases
- Detection
- Forensics Best Practices
- Cyber Insurance Policies
- Communication Strategies
- Resources and further reading
Current Ransomware Threat Landscape

• Many Groups Operating Currently

• Targets:
  • Individuals, Small Businesses and Large Enterprises
  • Healthcare, Supply Chain, Government, Education

• Main Players:
  • REvil
  • Conti
  • Babuk
  • Darkside

• Ransomware Payments
Ransomware Groups: Motivation and Operation

• Motivation:
  • $$$
  • Disruption
  • Testing/Experimentation

• Operation
  • RaaS
  • In-house development
  • Buy finished product

Ransomware attack 'not designed to make money', researchers claim
Managing Ransomware Attacks

BEFORE
- DR Plan
- IRP
- TableTop Exercises
- Design Backup Systems
- Test Backup Systems
- Threat Hunting

DURING
- Coordination
- Communication
- Containment
- Response
- Technical Analysis
- Threat Hunting

AFTER
- Restoration
- Back to BAU
- Root Cause Analysis
- Lessons Learnt
- Update DR plans
- Update IRP
- All the points in ‘Before’
Real-world Cases 2022

• Freight Company
  • Threat Actors exploited the network back in 2020 (RDP)
  • The network was left exposed for a long time
  • Threat Actors installed MegaSync and exfiltrated data
  • Threat Actors used Ransomware in the end to encrypt servers

• Law Firm
  • Threat Actors used ProxyLogon
  • Ransomware was executed
  • Cron jobs were scheduled to spread the infection
  • TAs kept lowering the ransom demand
Detection

- In-house detection teams
- Threat-intel feeds
- Research publications

```
bcedit.exe /set {default} recoveryenabled No
bcedit.exe /set {default} bootstatuspolicy ignoreallfailures
```

Dec 23, 2021

**DefendAgainst: Ransomware ‘STOP’/DJVU**

```
esxcli --formatter=csv --format-param=fields="WorldID,DisplayName" vm process list | awk -F "\",\"" '{system("esxcli vm process kill --type=force --world-id=" $1")}'
```
Forensics Best Practices

• Virtual Machine snapshots – both current and before infection
• Available logs - cloud based and internal systems
• Active Monitoring - Endpoint detection and Response / Threat Hunting
• Engage specialist Incident Response and Forensics early
Cyber Insurance Policies

• Often the first port of call for victim organisations

• Facilitation of response management, legal counsel, engage forensics specialists, regulatory notifications, ransom payment negotiations, etc.

• Cost of Cyber insurance is skyrocketing and appropriate coverage is becoming a challenge.
Communication Strategies

• Critical component of the response - can affect the company brand.
• Many Stakeholders
  • Regulatory notifications and enquiries
  • Media
  • Customers
  • Internal staff
• Single point of contact for external communication.
• Consistent and timely based on available information.
• “Need to know basis” approach, prepare for possible scenarios.
• Legal and PR Approval.
Resources and further reading

https://ransomwhe.re - track ransomware payments
https://ransomwaretracker.abuse.ch/blocklist/ - Blocklist
Ransomware: Understand, Prevent, Recover - Allan Liska
Follow VX Underground on Twitter
Q&A
Thanks!

Contact details:

Vishal Thakur - @vishUwell

John Lopes - john@hack.sydney