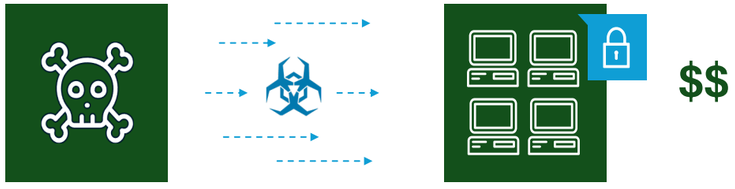
Incident Response Playbook – Ransomware

[Preparation]

Attack Description

A Ransomware attack consists of the compromise of systems, first encrypting or preventing access to their data and then requesting a ransom from the target enterprise for getting the data back.



The motivation of Ransomware attacks is financial gains based on ransoms. Threat actors in the ransomware business can generate profit in different ways, such as selling stolen data such as usernames, passwords, intellectual property, or selling access to your network.

The typical impact of a Ransomware attack is a temporary or permanent loss of data.

Incident Severity Matrix

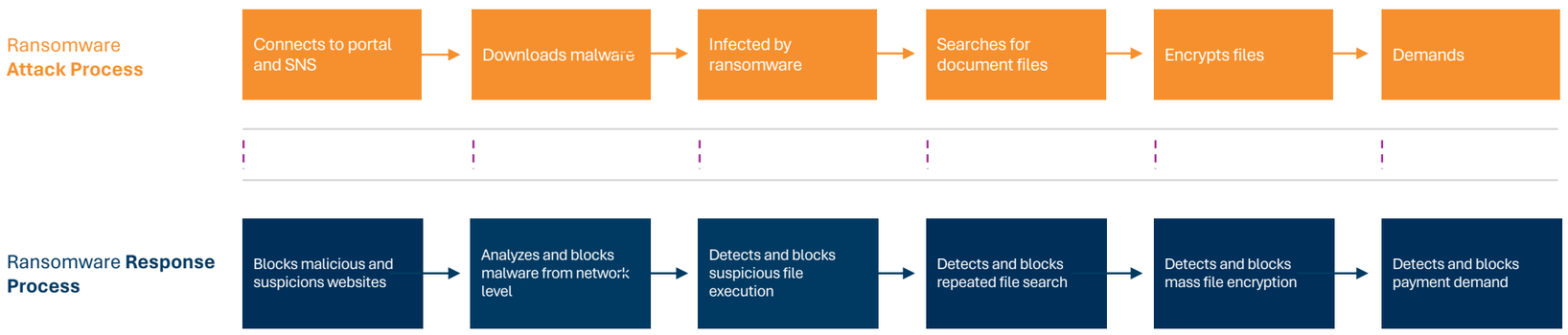
SEVERITY	CASE
Critical	Significant business disruption External visibility, media involved Police or government law enforcement involved (e.g. unavailability of data implying critical service interruption - manufacturing, health care)
High	Significant business impact External visibility without media involvement Risk of regulatory sanctions (e.g. loss of regulated data)
Medium	No significant business impact Internal impact without external visibility (e.g. single host affected, non-critical data affected)
Low	No business continuity issue Attack contained by normal security controls

Examples of well-known Ransomware attacks

BlackBasta: The ransomware was discovered in early 2022 and is known for its double extortion attack, the Russian-speaking group not only executes ransomware, but also exfiltrates sensitive data, operating a cybercrime marketplace to publicly release it. Initially at least 20 victims were posted to its leak site: Basta News. It targets large organizations in the construction, manufacturing industries, and other critical infrastructure, including the health and public health sector.

LockBit: In 2022, LockBit was the most deployed ransomware in the world. Attackers using LockBit have attacked organizations of varying sizes across various critical infrastructure sectors, making any organization a potential target. LockBit functions as a Ransomware-as-a-Service (RaaS) model, where attackers are recruited to conduct attacks using LockBit ransomware tools and infrastructure.

Typical Ransomware Attack and Response



Tips: preparing for a ransomware attack

- Following a ransomware attack, a breach assessment is needed to ensure the ransomware hasn't left any backdoors.
- When the ransomware cannot be reversed, consider using a professional negotiator to discuss with the threat actors, and use their expertise to reduce the ransom amount.
- The workload during ransomware attacks can be extremely high for IT operations. Plan for appropriate compensation and carefully distribute efforts. Restore only critical data first. Make available enough food, drinks and accommodation when needed.
- Be ready to switch off your fixed and VOIP servers and move to mobile communication.

Preparation

1. Implement critical data backup processes and solutions so that critical data is regularly backed-up and restore processes continually tested.
2. Define, maintain and test the following Standard Operating Procedures (SOPs):
   - Set network share in read only
   - Isolate a host from the network
   - Reconfigure at scale compromised hosts
   - Block accounts and reset active sessions
   - Block at both host and network levels a specific:
     - Domain
     - IP or range of IPs
     - Hash
     - URL pattern
   - Run script on hosts at scale
   - Forensics artefacts retrieval
   - Search and remove email on all mailboxes based on attachment name, file extensions, sender email, sender IP source or email subject
3. Have documents available both online on a separate site as well as hard-copies documentation :
   - Critical assets list
   - Network diagrams
   - Mobile phone contact list of key stakeholders including technical and DRP team
4. Integrate the ransomware attack scenario in the Business Continuity Plan of the Company:
   - Plan for a possible disruption of the entire infrastructure of the company
     - Emergency communication means planned
     - Emergency procedures stored in an alternative location
   - Plan for response when most critical applications are affected.

Incident Response Playbook – Ransomware
[Response Guide]

A Analysis

Confirm Ransomware Attack

1. Confirm detection of files with a suspicious extension (e.g. .locky, .ryk)
2. Identify ransom request and parameters (e.g. ransom amount, time to pay)

Identify the Scope of the Attack

Get a first sense of:

1. The number of hosts impacted (use Helpdesk calls, ransomware binary searches)
2. The amount and severity of the data encrypted (use file extension searches)
3. The speed in which the attack is spreading

Qualify Ransomware Attack

1. Use severity matrix to assign a severity level (see 'preparation')

Business Impact

1. What is the business impact? Is the business still vulnerable?
2. Was a vulnerability exploited? Which one? Consider the CVSS3 model for ranking its severity
3. Was potential sensitive data exposed to an unauthorized individual? All data or a single user's data?
4. Are we currently under attack? Are there signs of a previous attack? Is there continued unauthorized access?

B Containment

- Isolate the host - isolate the infected host from the network or disconnect the network cable, to avoid further spreading of the ransomware
- Hibernate the host - put the infected host in hibernation to avoid further encryption
- Protect Network Shares - put critical data in read-only mode if the ransomware is spreading to network shares
- Block accounts and reset sessions - limit ransomware propagation by blocking accounts of infected users. Block the affected accounts and reset the active sessions on VPN, o365 and AWS etc.
- Block and log threat actor's infrastructure, use IoCs and tools available

C Eradication and Recovery

Eradication

- ❑ Duplicate Hibernated hosts: before switching them back on, duplicate the hibernated hosts' hard disks (e.g. using the dd tool)
- ❑ Analyze infected hosts in an isolated environment to avoid further spreading (e.g. file system analysis, memory dump analysis), identify attack campaign based on binaries and encrypted files extensions
- ❑ Find Patient-0 (first infected host): look for ransomware binaries on all hosts
- ❑ Find infection vector: looking in the e-mails of the impacted users or on patient-0 (e.g. attachments, web links)
- ❑ Reconfigure systems enterprise-wide to break malware execution and propagation mechanism. Patch exploited vulnerabilities
- ❑ Clean-up infection vectors: remove all e-mails that have been used for host-infection (e.g. search for e-mails similar to infection vectors)
- ❑ Block all users that are not active during the cleanup step, so they are forced to contact IT for a secure login procedure. Users that login after the clean-up may cause a new infection, as antivirus signatures are usually updated with a delay
- ❑ Get attack context from related threat intelligence. Attribute ransomware to an existing campaign or technique

Recovery

1. Lift containment measures
2. Identify if a ransomware decryption exists
3. Recover Data
   - If decryption exists, attempt to decrypt data on the duplicated hard disk
   - If backups available, restore encrypted data
   - Otherwise, and if critical data is impacted, contact your Emergency IR partner or law enforcement to support you with ransom negotiation
4. Monitor for new infection - monitor for Indicators of Compromise (IoC's) identified during the analysis phase (e.g. specific domains, IP addresses, hashes, registry keys) to ensure that another attempt of infection would be immediately detected
5. Clean-up: re-image infected systems

D Post-Incident Review

1. Assess security controls against ransomware risks and update security program and detection mechanisms
2. Review Incident Response process to identify improvement points with the involved internal and external teams
3. Review security awareness process to limit risk of infection

Detection and Containment Technologies

Incident detection capability matrix

Detection	Domain	Hash	Executable	IP	Email	File	Forensics	URL	Vuln.
Network-Based Detection									
Edge Firewall (Cisco ASA)	?	?	?	X				?	
Edge Secure Internet Gateway (Cisco Umbrella)	X	P	X	X		?		X	
Edge IDS (Cisco Firepower)	P	?	?	X		?		P	P
Host Based Detection									
CrowdStrike	P	X	X	P		X	?		?
Cisco AMP	X	X	X	X		X			
Email Based Detection									
Cisco Email Security Appliance (ESA)	P	P	P	P	X		P	X	
Correlative Detections									
LogRhythm	X	X	X	X	X	X	P	X	

X = Capability Exists P = Partial Capability Exists O = Capability Does Not Exist

Example	Description	Benefits
Cisco Umbrella	Next Generation Firewall Secure Internet Gateway	DNS/IP layer Security. Data loss prevention, Intrusion Prevention, cloud malware detection, Remote browser isolation
LogRhythm	SIEM tool – collects logs and correlates threat data and alerts	Rapid threat detection. Enables creating and activating new detection rules
Cisco AMP	Next-Gen AV protection, EPP, EDR, XDR.	Enables advanced malware detection and prevention of unauthorized applications and suspicious behavior
Cisco Stealthwatch	Network traffic analysis (NTA) / Network detection and response (NDR)	Enabled detection of malware, insider threats like data exfiltration, policy violations. Analyze encrypted traffic for threats and compliance, without decryption
Cisco FirePower	Network traffic analyzer, includes: IDS, IPS, URL Filtering, Malware, Analysis, DNS monitoring	Rapid detection and prevention blocking network connections based on IoC's and specific network patterns
Office 365	Email solution, license E1, E3, E5	Enables detection and removal of malicious email as well as data exfiltration when using the corporate email systems
CrowdStrike	Next-Gen AV protection, behavioral detection, provides correlation of threat data and alerts	Enables detection of unauthorized applications and suspicious behavior
Cisco ESA	Email Security Appliance	Defends against spam, advanced malware, phishing, and data loss
ServiceNow	Incident Management Platform	Centralizes incident data and enables rapid handling

Containment capability matrix

Detection	Domain	Hash	Executable	IP	Email	File Protect	URL	Malicious Behavior
Network-Based Detection								
Router				X				
Edge Firewall (ASA)	P			X				
Edge Secure Internet Gateway (Cisco Umbrella)	X	P	X	X				P
Edge IDS (Cisco Firepower)	X			X				P
Host Based Detection								
EDR	X	X	X	X		P		X
AV		X	X					P
NextGen AV (EDR)		X	X					X
	X	P	X	X		P		P
Email Based Detection								
Cisco Email Security Appliance	P		P		X		P	

X = Capability Exists P = Partial Capability Exists O = Capability Does Not Exist