Arctic Wolf® Incident Response Timeline:

Ransomware Encryption Event

Time is of the essence when experiencing the fallout from a malicious attack or system intrusion.

2:14 AM

Encryption Event

- At 2:14am an organization receives a ransom note that states critical data has been stolen, web applications are no longer functioning, and their SQL servers are encrypted
- The organization immediately contacts Arctic Wolf Incident Response (IR) via the "Experienced a breach" button that is easily accessible from the arcticwolf.com homepage or inside of the Incident Response JumpStart Retainer (IRJS)

2:22 AM

Arctic Wolf 1-hour response time guarantee

- The IR team receives the incident notification and calls the organization 8 minutes later for a scoping call
- Guidance is provided to implement containment actions during the scoping call and a Statement of Work (SOW) is sent to the customer for sign-off
- Based on the scoping call, a team of digital forensics examiners, restoration and remediation specialists, threat actor negotiators, and cyber defense experts is assembled

Arctic Wolf IR JumpStart Retainer provides a 1-hour response time service level agreement (SLA).

2:50 AM-3:50 AM

Containment

- SOW is complete
- The IR team discovers that 3 SQL servers are impacted, and all other servers are operating normally
- Immediate containment actions are taken including:
  - Segmenting backups (taking backups off the network)
  - Limiting inbound and outbound network traffic
  - Disabling specific VPN accounts

The timeline shown is an example scenario based on optimal factors and should be used for informational purposes only and not for professional advice or guidance.

3:10AM

Monitoring and Active Defense

- The IR team starts monitoring the environment. This includes:
  - Endpoint monitoring
  - Network monitoring
  - Cloud monitoring
    - More specifically, the IR team monitors O365 and MS Entra ID (Azure Active directory)
- The IR team also actively defends the environment and remove any malware that is discovered via monitoring

> ***Monitoring and active defense will occur throughout the duration of the engagement.***

7:25 AM

Root Cause Analysis

- The IR team learns that 3 SQL servers were encrypted by the attacker using remote desktop protocol (RDP) from the primary domain controller
- The digital forensics team identifies the root cause
  - A user on a workstation inside of the shipping department accidentally clicked on a malicious email attachment that used Gootloader – a malicious JavaScript downloader –and gave the attackers access to the workstation.

8:05 AM

Restoration and Remediation

- The IR restoration team begins rebuilding the compromised domain controller, and safely restores SQL server backups
- Through monitoring and active defense, the IR team remediates the attacker's persistence mechanisms on the network and confirms that systems are clean

9:00 AM

Threat Actor Planning

- Based on restoration progress, the IR team determines that there are backups for all encrypted data and no decryption program is needed from the attacker
- The IR team recommends that the customer engage with a data privacy attorney and conduct the threat actor options under privilege
  - The IR team will share the pros and cons of reaching out to the threat actor over the stolen data
  - The IR team engages with the threat actor once a strategy has been selected by the customer's leadership team and legal counsel

11:37 AM

Restoration Complete

- SQL servers are up-and-running and critical business systems are operating at a pre-incident state

2 DAYS LATER

Digital Forensics Analysis

- The digital forensics team finds that the attack was able to compress 250 GB of sensitive SQL server data
- The complete list of stolen data is provided to the customer and the customer's legal counsel for review

2 DAYS AND 2 HOURS LATER

Threat Actor Negotiations

- The IR team reaches out to the threat actor and receives sample data to corroborate digital forensics findings
- Although the data is sensitive, the customer and their legal counsel decide not to pay the ransom

7 DAYS LATER

Executive Summary

- The IR team provides a summary to the customer's leadership team and legal counsel
  - The summary outlines how the incident occurred, what data was compromised, and what systems were impacted
  - The IR team also advises on how to harden systems and prevent a similar ransom attack in the future

Incident Response

Respond Faster. Emerge Stronger.

The Arctic Wolf Incident Response team knows that finding an active threat actor inside your network is one of the worst times that your business could experience and we're here to help. Expect to hear from a trusted IR teammate within **1 hour*** in response to a new or active incident.

Are you experiencing a ransomware attack?

Contact us for immediate assistance: **arcticwolf.com/emergency-incident-response**

*Response time is available with the Arctic Wolf IR JumpStart Retainer

Top Ten Tips To Mitigate an Active Ransomware Attack:

Don't Panic

Try your best to remain calm and rely on your preparations and team to best proceed.

Refer to Your Incident Response Plan

The plan holds valuable information you and your IT team need if you are experiencing a security incident. Be sure the IR plan is updated frequently and printed out on paper.

Reach Out to Your Trusted Advisors

Insurance Brokers, Insurance Claims Team, Legal Counsel, etc.

Isolate Your Backups

Ensure your backups are offline or physically offsite to isolate and prevent access from attackers.

Disconnect Servers and Critical Devices From the Internet and Each Other

If an attacker is taking data from your network in real-time, cutting off the internet will kill this action.

Do Not Engage the Threat Actor

Do not attempt to negotiate with threat actors or decrypt ransomed data on your own. Contact Arctic Wolf to save time, money, and your data.

Document What You Can (Screenshots, Photos, Etc.)

- Ransom Notes / File extensions
- Reviewed Logs
- Software conveying the state of the environment

Preserve All Evidence

- Do not turn off devices
- Do not wipe/re-image/restore from backup without consultation
- Failure to preserve all evidence will result in an incomplete investigation

Change Your Passwords

- Administrator accounts / all cloud accounts
- VPN / Remote connectivity software
- Firewall
- Email

Identify Where Sensitive Information Is Stored

Know the host name of this device, review your backups for this information. Consult with your legal team before you inform employees, clients, etc., of the attack.

About Arctic Wolf Incident Response

When cyber attacks result in a breach or cyber incident, organizations need a proven partner.

Arctic Wolf Incident Response is a trusted leader in incident response (IR), providing rapid remediation to any cyber emergency. Valued for our breadth of IR capabilities, technical depth of incident investigators, and exceptional service provided throughout IR engagements, Arctic Wolf Incident Response is a preferred partner of cyber insurance carriers.

ARCTIC WOLF