ALVAKA

Navigating the Storm
A Guide to Ransomware Recovery

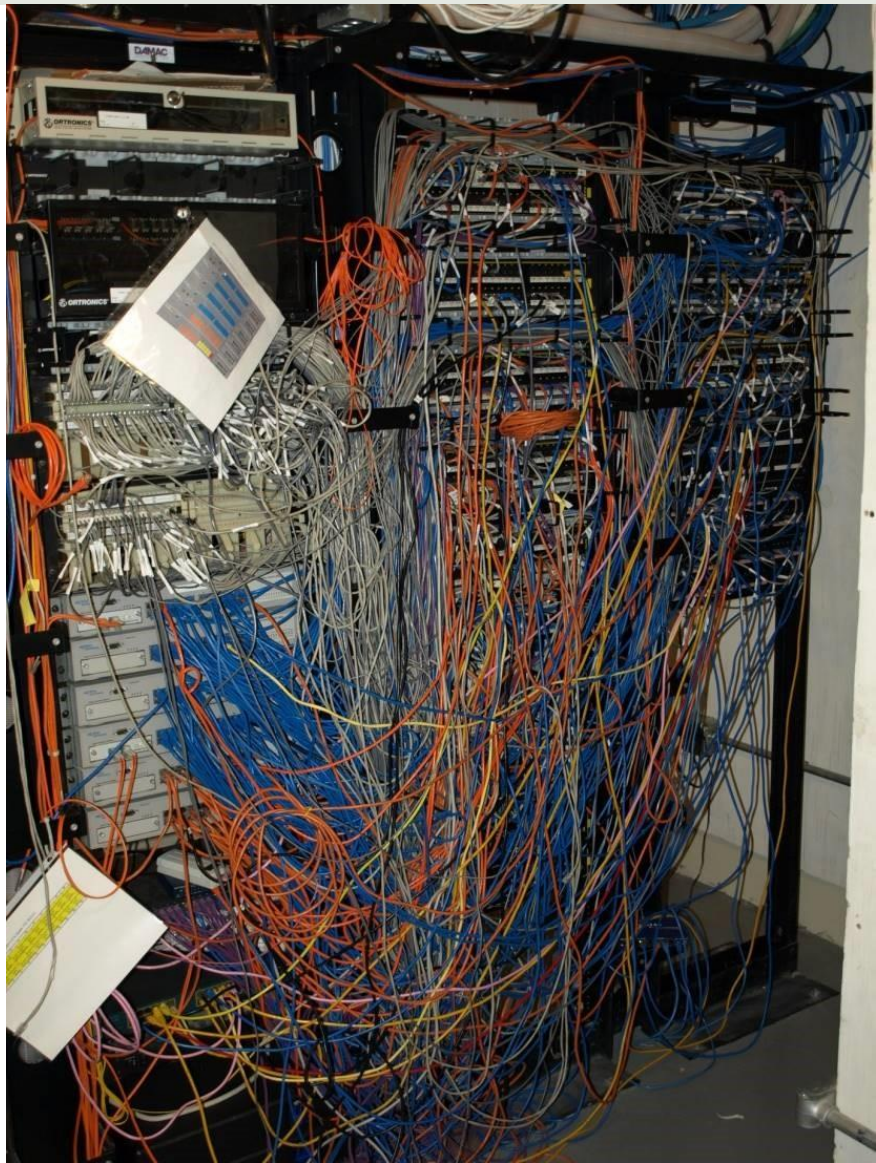
Ransomware Recovery Experience

Containment & Restoration

- 24x7 NOC
- Dedicated Ransomware Recovery teams
- Engaged by
  - Breach counsel
  - Forensics firms
  - Insurance carriers
- Experience – 300+ Cases
  - Largest case 40,000 compromised hosts, 28 offices, 12 countries
  - Manufacturer incurring $2M per day in contract performance penalties
  - 21 school districts, 7 universities
  - Unregulated Industries - Manufacturers, Distributers, Pro Services
  - Advised dozens of MSPs who have been attacked or had Clients attacked
- Proprietary methods – scripts, compute, storage
- **Accelerate recovery by 5 days**

What are we getting into?

OR



ALVAKA

Subject: pic of computer room attached!!

ALVAKA

Subject: pic of IT war room attached

Average Restoration Times

50% - CANNOT Recover from Backups – Pay Ransom – 19 Days

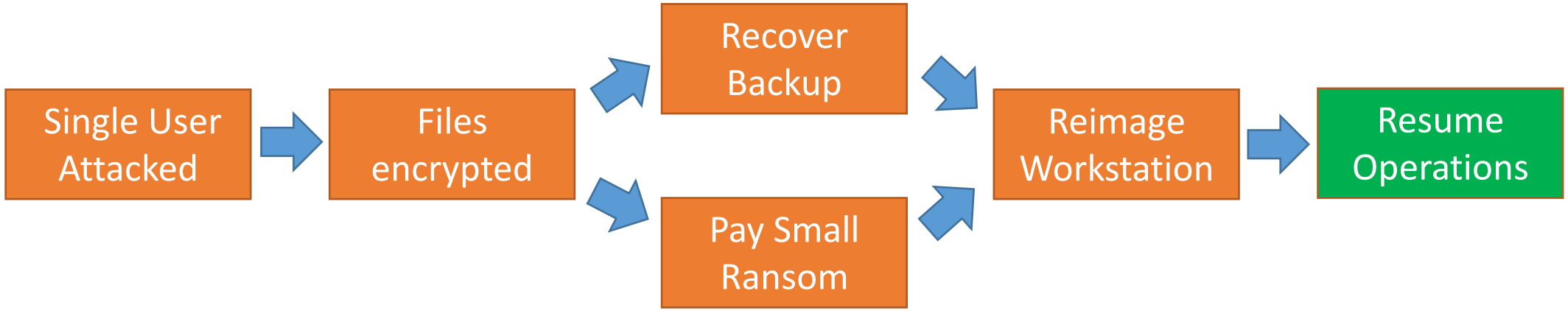
50% - CAN Recover from Backups – 12 Days

Recover from attack that didn’t happen – 0 Days

Projections for 2025

- The Attacks will continue until morale improves
- Attacks will continue to be more sophisticated
- Re-attacks will continue to proliferate
- If you experience a Ransomware Attack, you will be conscripted into the Recovery Team

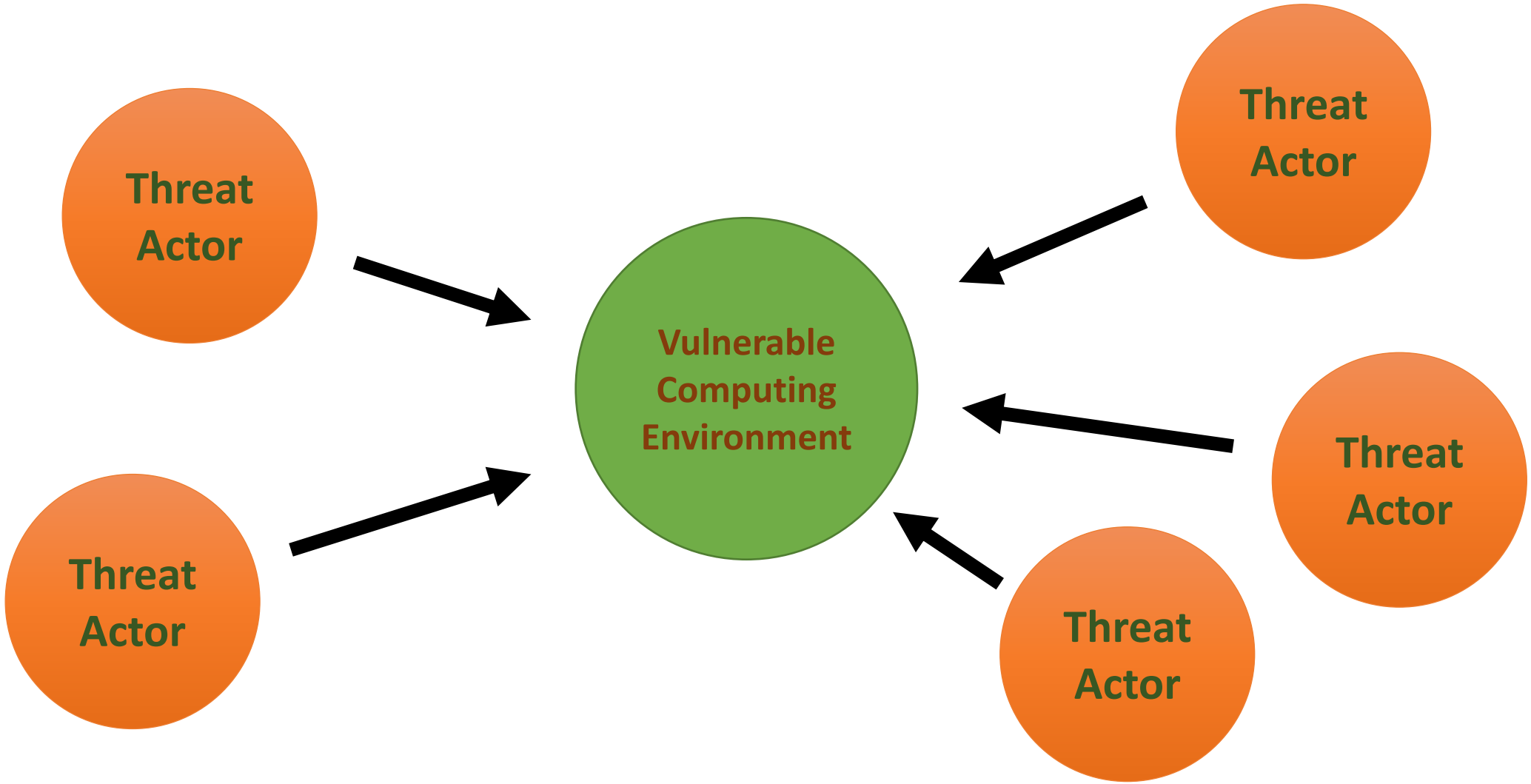
Ransomware Attack circa 2019



- Technical Problem
- Minimal Disruption
- Low incidence of re-attack
- Minimal Cost

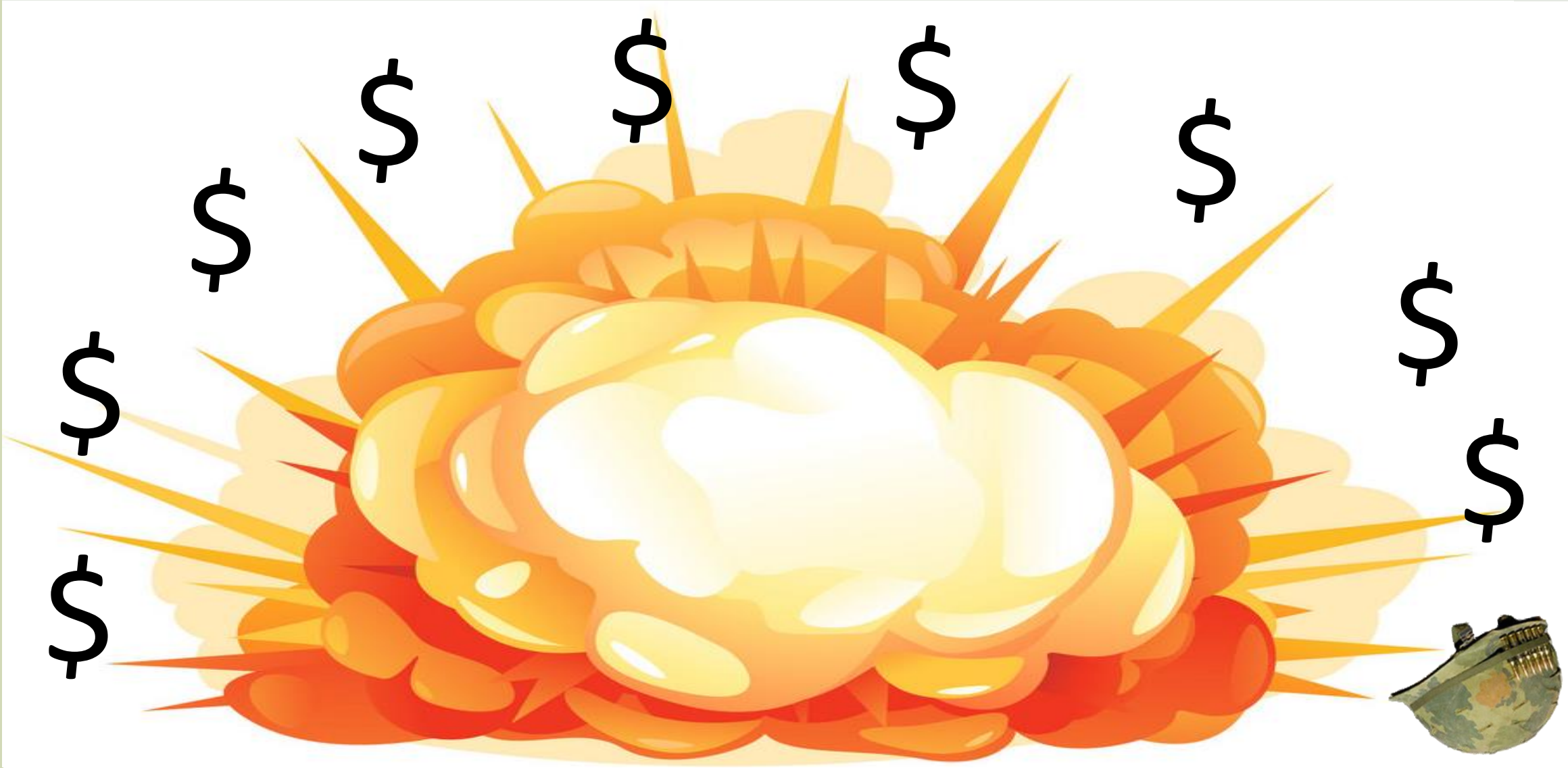
ALVAKA

Confluence of Unfortunate Events



Non-Technical Executive Version

Confluence of Unfortunate Events



ALVAKA

Costs & Potential Damages

DIRECT RECOVERY COSTS

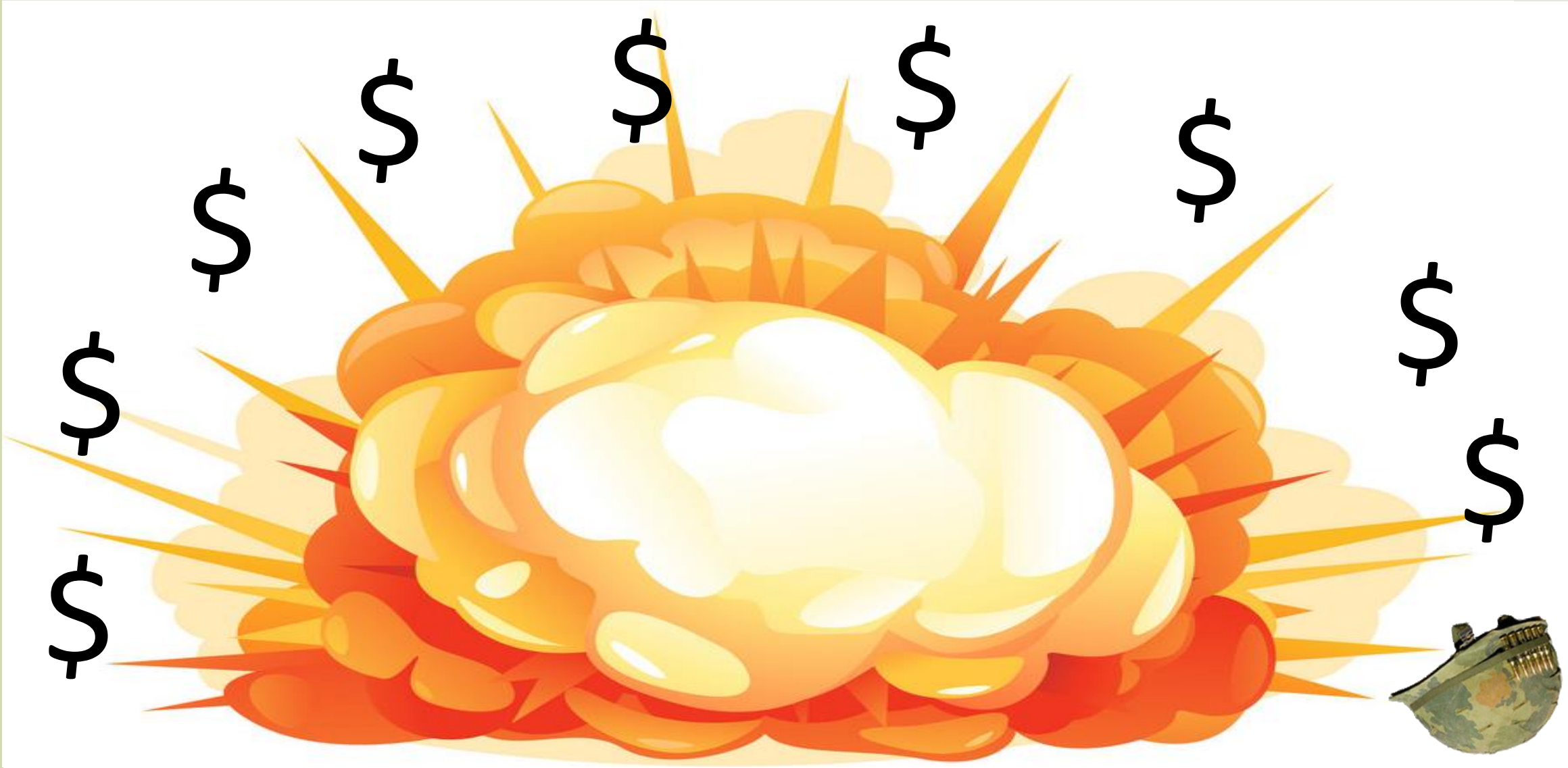
- Ransom
- Breach Counsel
- Forensics & Data Mining
- Threat Actor Negotiation
- Data & System Recovery
- PR & Crisis Communications
- Notifications
- Credit Monitoring

CONSEQUENTIAL DAMAGES

- Lost Revenue
- Performance Penalties
- Opportunity Costs
- Brand & Reputational Damage
- Reduced Valuation
- Fines
- Litigation
- Denial of Coverage

What About Cyber Liability Insurance?

Confluence of Unfortunate Events



Insurance is Not a Panacea

Benefits

- Financial Resources
- Case Experience
- Structured Recovery Plan

Caveats

- Claims Experience Varies
- Limitations of Coverage
  - Restoration
  - “Betterment”
- “Panel” Vendors
- Conflict of Interest

Moral: Know your Carrier and Policy

ALVAKA

Goals for Recovery

1. Recover operations as quickly as possible
2. Avoid the reattack
3. Minimize cost and risk to the business

ALVAKA

Roles – Ransomware Recovery

- Breach Counsel - Minimize legal exposure, PR & Crisis Communications
- Forensics Investigator - Determine cause, extent of damage, stolen data, successful ejection of criminals
- Negotiator - Communicate with criminal threat actor
- Containment - Eject the criminals, secure the network
- Restoration - Restore data & systems
- Data Mining – Define notification scope
- Notification Services – Communications to affected parties

ALVAKA

NEW for 2024/2025 (actual cases)

- Double Extortion is now standard
- EDR is being defeated
  - XDR essential, also consider ASM
- Veeam backups are being destroyed
  - Implement Immutability & Test
- SOC providers are **D**etecting, not **R**esponding
  - Evaluate IR policy, enable Response
- TA creativity / aggressiveness is increasing

Immediate Actions

DO

- Disconnect Internet
- Power off network switches
- Disconnect backup systems
- Write-protect backup media
- Collect ransom note
- Contact Alvaka 24x7

DO **NOT**

- Power off systems
  - Exception: Critical servers / SANs that have not been encrypted
- Attempt to “clean” malware
- Contact Threat Actor

Next Actions

DO

- Engage outside Breach Counsel
- Engage forensics
- Open case with insurance carrier
- Setup “burner” e-mail accounts for recovery team
- Change banking credentials and setup MFA

DO **NOT**

- Render legal advice
- Assume there is no insurance coverage
- Disclose there has been a ransomware attack
- Recover backups until threat has been contained
- Reimage systems
- Engage questionable decryption firms

Next Actions – First 24 Hours

DO

- Establish recovery plan
- Deploy EDR software to ALL hosts, infected or not
- Assess viability of backups
- Prioritize applications for recovery
- Establish recovery environment
- Preserve firewall logs

DO **NOT**

- Reimage systems
- Prioritize recovery over containment

Questionable Decryption Firms

"Recovery" Firm: *"**Don't Pay the Ransom**. Paying criminals a ransom doesn't guarantee you'll get your data back. **Paying-up is a risk you don't want to take**. Let our experts handle the situation for you."*

PROPUBLICA

"As ransomware attacks crippled businesses and law enforcement agencies, two U.S. data recovery firms claimed to offer an ethical way out. Instead, they typically paid the ransom and charged victims extra."

ALVAKA

Blunder Management

- **Assuming backups are viable, deleting encrypted data, only to find backups are NOT viable.**
- **Assuming backups are NOT viable, paying a Ran$om, only to find backups ARE viable.**
- **Restoring without Containment, only to be reattacked.**

“How do we NOT do that again?”

Implement the most effective measures FIRST:

- **PREVENT** - MFA for ALL Admin and Remote access
- **DETECT & RESPOND** - XDR in addition to EDR, monitored by SOC empowered to **R**espond
- **RECOVER** - Immutable Air-Gapped backups that are impossible for a TA to compromise

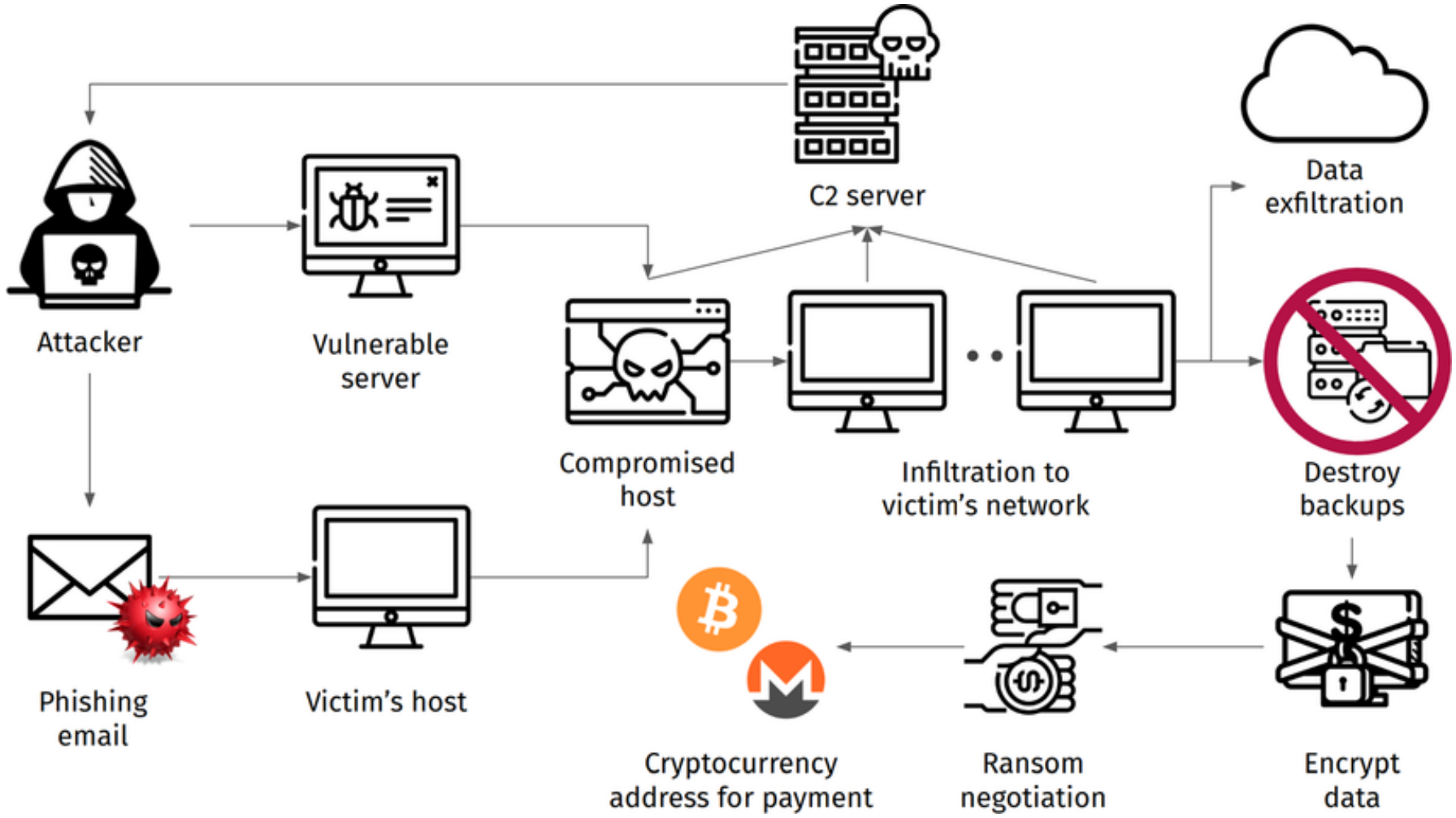
Dave White

M.A., COMPTIA A+/NET+/SECURITY+,
FBI CART/CICP, GCFE, GCIH, INFOSEC

- 35-YR HUSBAND
- 30-YR LAW ENFORCEMENT (RETIRED)
- 26-YR DAD
- 21-YR DFIR (DIGITAL FORENSICS IR)
- 12-YR ADJUNCT PROFESSOR
- 6-MO DOG DAD (#2)

Ransomware attack

1. RECONNAISSANCE
2. INITIAL ACCESS
3. PERSISTENCE
4. PRIV ESCALATION
5. DATA EXFILTRATION
6. ENCRYPTION
7. RANSOM NOTE
8. NEGOTIATION
9. PAYMENT
10. DOUBLE EXTORTION



Goals: Financial Gain / Disruption / Data Theft & Extortion / Brand Damage / Malware / Access or Control / Political / Fame

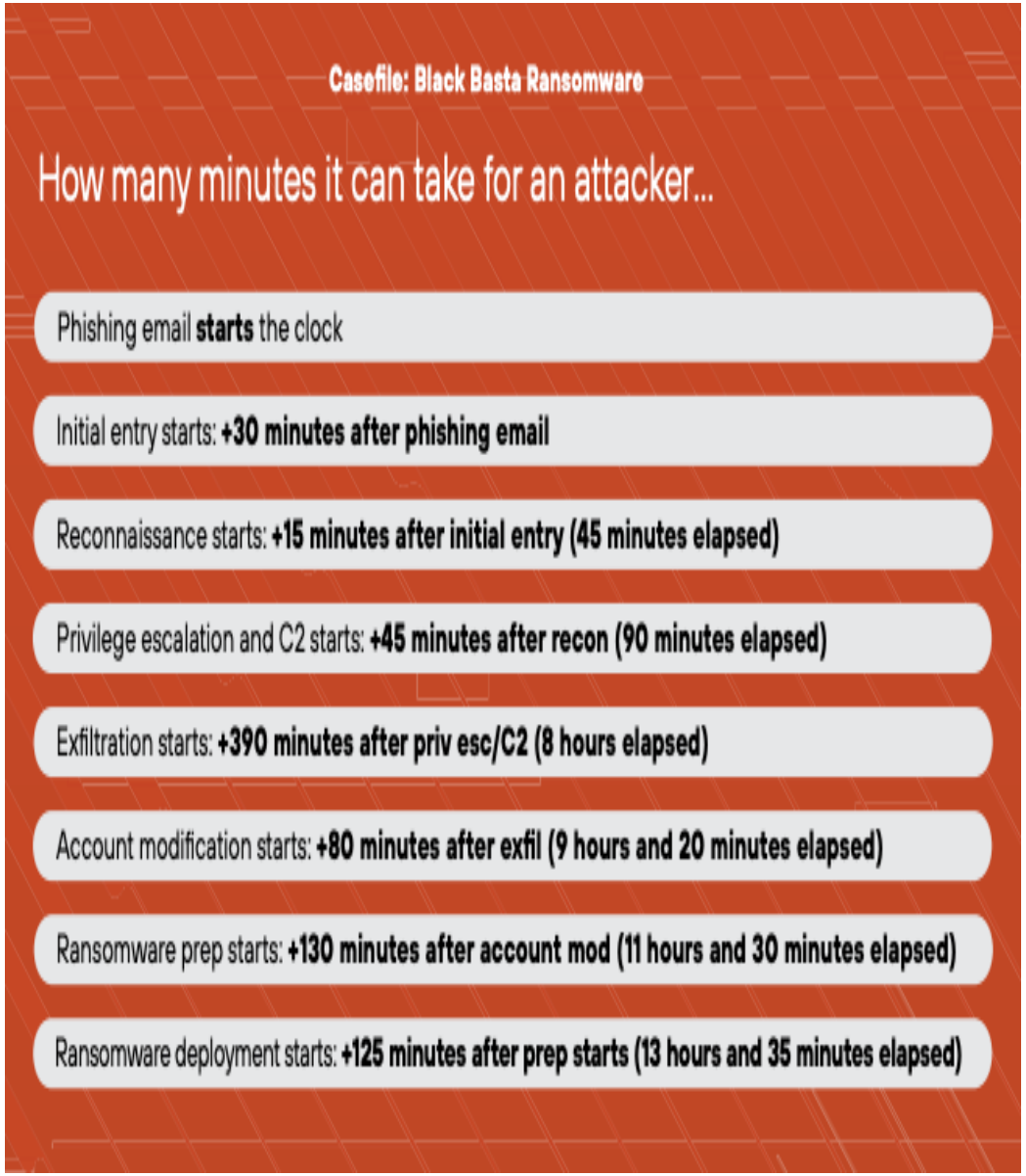
Case study

Black Basta Ransomware

"In less than 14 hours, attackers gained access to an organization, exfiltrated terabytes of data, and deployed ransomware to nearly 10,000 endpoints."

Source: 2024 Unit42 Incident Response Report

Black Basta | Emerged in 2022–possible Conti spin-off | Ransomware-as-a-Service (RaaS) | Double Extorsion | Data Leak Site | Attack methods: Phishing/zero-day vulns/RDP brute force/Mimikatz (credential theft & privilege escalation) Cobalt Strike & Metasploit (maintain persistence & evade detection) | Healthcare, Finance, Education, Energy, and Manufacturing.



Case study

Medusa Ransomware attacks – January 2025

Illustration/Source: Ravie Lakshmana/The Hacker News

Medusa | 2021 | Russian-speaking/Eastern European Cybercriminals | Ransomware-as-a-Service (RaaS) | Leverages known security flaws in public-facing applications (**Microsoft Exchange Server**) to obtain initial access | Uses Initial Access Brokers for breaching networks of interest | Double Extorsion | Data Leak Site | Attack methods: Phishing/zero-day vulns/RDP brute force/Mimikatz | Healthcare/Fin Services/Mfg/Education/Gov't/Critical Infra.

Incident: In January 2025, Medusa ransomware group claimed responsibility for attacks on over **40** victims and has claimed nearly **400** victims since it first emerged in January 2023, with the financially motivated attacks witnessing a **42% increase** between 2023 and 2024.

Impact: Medusa has a track record of demanding ransoms anywhere between **$100,000 up to $15 million** from healthcare providers and non-profits, as well as targeting financial and government organizations.

Response: Affected organizations are advised to enhance security measures and monitor for suspicious activities.

Recovery: Organizations are working to restore systems and data, often without paying the ransom.

Case study

Lee Enterprises – February 2025

Illustration/Source: Sarah Grillo/Axios

Qilin (mythical Chinese creature) | Conti spin-off | Ransomware-as-a-Service (RaaS) group, performs targeted intrusions (spear-phishing, exploiting zero-day vulns, and brute-force attacks to gain unauthorized access) | double extortion | Healthcare/Manufacturing/Finance & Energy.

Incident: In February 2025, Lee Enterprises, the parent company of a dozen newspapers, including the *Richmond Times-Dispatch,* and *Charlottesville Daily Progress*, experienced a cyberattack attributed to the Russian-linked group Qilin.

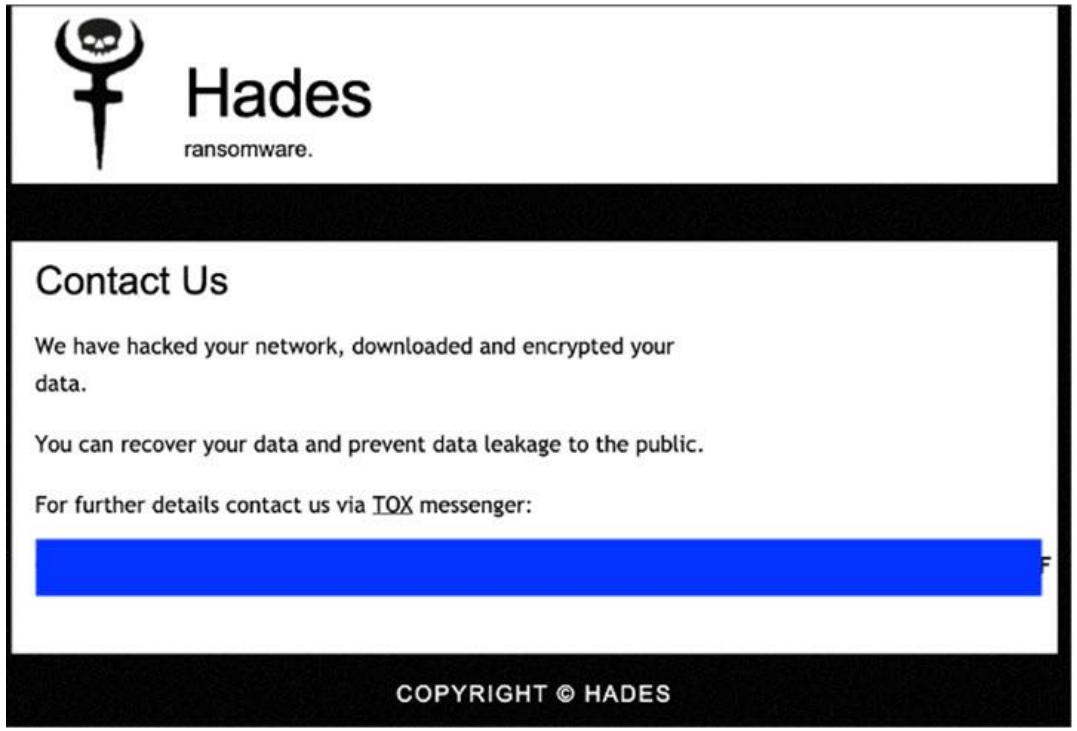
Impact: Attackers accessed Lee's network and files, stole **350GB** of files, including “investor records, financial arrangements that raise questions, payments to journalists and publishers, funding for tailored news stories, and approaches to obtaining insider information,” encrypted applications, and disrupted print and online operations across its portfolio, plus billing and vendor payments.

Response: Lee Enterprises acknowledged the breach, reporting a "systems outage" and is investigating the group's claims.

Recovery: The company is working to restore full operations and enhance cybersecurity measures.

Case study

healthcorps network – march 2025



Hades ransomware victim site. (Source: Secureworks)

Hades (Greek god of the underworld) | Conti spin-off | Ransomware-as-a-Service (RaaS) | Attack methods: Spear-phishing, exploiting zero-day vulns, and brute-force attacks to gain unauthorized access | double extorsion | Healthcare/Manufacturing & Energy/Gov't & Fin Services.

Incident: In March 2024, HealthCorps, a healthcare network operating across multiple U.S. states, experienced a significant ransomware attack attributed to the ransomware group Hades.

Impact: 5.6 million patient records, exposing sensitive information such as medical histories, insurance details, and personal identifiers. Substantial operational challenges, including the potential for delayed or disrupted patient care, as systems were taken offline for investigation and remediation. **$50M demand**, negotiated to $12M, which was not paid (recovery via backups).

Response: HealthCorps initiated a thorough investigation, collaborating with cybersecurity experts and law enforcement agencies. Affected individuals were notified about the breach and advised on protective measures. Efforts were made to secure and restore compromised systems, aiming to resume normal operations while ensuring data integrity and security.

Recovery: HealthCorps implemented strengthened cybersecurity protocols, including regular security assessments, advanced threat detection systems, and comprehensive employee training programs to prevent future attacks.

We got hit… now what?!

Average Restoration Times

- **CANNOT** recovery from backups = **19 days**
- **CAN** recover from backups = **12 days**
- Recovery time from **NO** attack = **0 days**

Loss Update

"Overall ransomware severity increased 68% in 1H 2024 to an average loss amount of $353,000."

Source: 2024 Coalition Cyber Claims Report

> Initial access to your network was purchased on the dark web. Then kerberoasting was carried out and we got passwords hashes. Then we just bruted these and got domain admin password. Spending weeks inside of your network we've managed to detect some fails we highly recommend to eliminate:

1. None of your employees should open suspicious emails, suspicious links or download any files, much less run them on their computer.

2. Use strong passwords, change them as often as possible (1-2 times per month at least). Passwords should not match or be repeated on different resources.

3. Install 2FA wherever possible.

4. Use the latest versions of operating systems, as they are less vulnerable to attacks.

5. Update all software versions.

6. Use antivirus solutions and traffic monitoring tools.

7. Create a jump host for your VPN. Use unique credentials on it that differ from domain one.

8. Use backup software with cloud storage which supports a token key.

9. Instruct your employees as often as possible about online safety precautions. The most vulnerable point is the human factor and the irresponsibility of your employees, system administrators, etc.

Akira ransomware gang

lessons learned

Containment & Forensics

1. Isolate Affected Systems
2. Identify Scope of the Attack
3. Disable Remote Access
4. Block Communication with Attackers
5. Ensure Backups are Safe
6. Preserve Evidence

Data & Systems Recovery

1. Assess the Impact
   - Perform thorough assessment of the systems, data, and infrastructure impacted by the attack.
2. Clean Infected Systems
   - Deploy EDR to fully remove ransomware from affected systems.
3. Establish Recovery Environment
   - Ascertain cleanliness before re-connecting servers & workstations to the network.
4. Restore from Backups
   - Restore data and systems from unaffected backups.
5. Decrypt Data (If Backups are Impacted/Unavailable)
   - Decyptor purchase conducted by DFIR/Negotiator.
6. Recover Applications, Workstations, and Repair Databases
7. Patch Vulnerabilities
   - Identify and patch any security vulnerabilities exploited during the attack.
8. Monitor for Further Signs of Attack
   - Continuously monitor network for signs of lingering malware, reinfection attempts, or abnormal activity.
   - Use endpoint detection and response (EDR) tools for continuous monitoring.
9. Implement Enhanced Security Measures

Ransomware Recovery Timeframes

Recovery is defined as back on-line in basic recovery mode.
This does not account for full remediation and networking infrastructure hardening.

The decisions you make will affect how quickly you recover, if at all.

	1-2 Weeks	2-4 Weeks	1 Month	2 Months or longer
Impact Level	Minimized	Painful	Debilitating	Company ending
Resources Available	Pro-level	Do it yourself	DIY with an inadequate team	DIY with wrong team on problematic network
Commitment Level	Full client cooperation	Little client cooperation	No professional leadership or processes	A lot of bad decisions

Source: Alvaka Ransomware Recovery Timeframes: How Long Does It Take to Recover? [2022]

Cyber Risk Mitigation

*"How do we **not** do that again?"*

1. **Employee Training & Awareness…**
   - Prevent human errors through ongoing education...
   - Execs & Boards **MUST** implement a layered $ecurity approach.
2. **Multi-Factor Authentication (MFA)**
   - Most effective measure to block unauthorized account access.
   - Adds an extra layer of security to account logins.
3. **Software Updates & Patch Management**
   - Cyberattacks exploit vulnerabilities… patch, patch, patch!
4. **Network Segmentation and Access Controls**
   - Limit lateral movement within the network.
5. **Advanced Threat Detection (ATD) and Endpoint Detection Response (EDR)**
   - Identify evasive threats that evade antivirus.
   - Real-time threat detection; minimizes damage.
   - Stop zero-day threats and breaches quickly.
   - Incident response capabilities to isolate, block, and remove threats.
   - Detailed logs & forensic data.
6. **Data Encryption**
   - Encrypting sensitive data at rest and in transit.
7. **Regular Backups & Backup Testing**
   - Crucial to ensure data integrity and availability, enabling quick recovery in case of a cyberattack, hardware failure, or data loss event.

Internet-Exposed Technologies

Risky Technologies

Other internet-exposed technologies were also found to increase the likelihood of a business experiencing a claim in 1H 2024:

1.7x more likely	**Remote Desktop Protocol**
1.8x more likely	**SonicWall Firewalls**
2.3x more likely	**Microsoft Remote Procedure Call**
2.4x more likely	**EOL Microsoft Internet Information Services**
2.7x more likely	**Remote Desktop Web Access**
2.8x more likely	**FortiOS SSL VPN**
5.1x more likely	**Cisco Adaptive Security Appliance**

Source: 2024 Coalition Cyber Claims Report

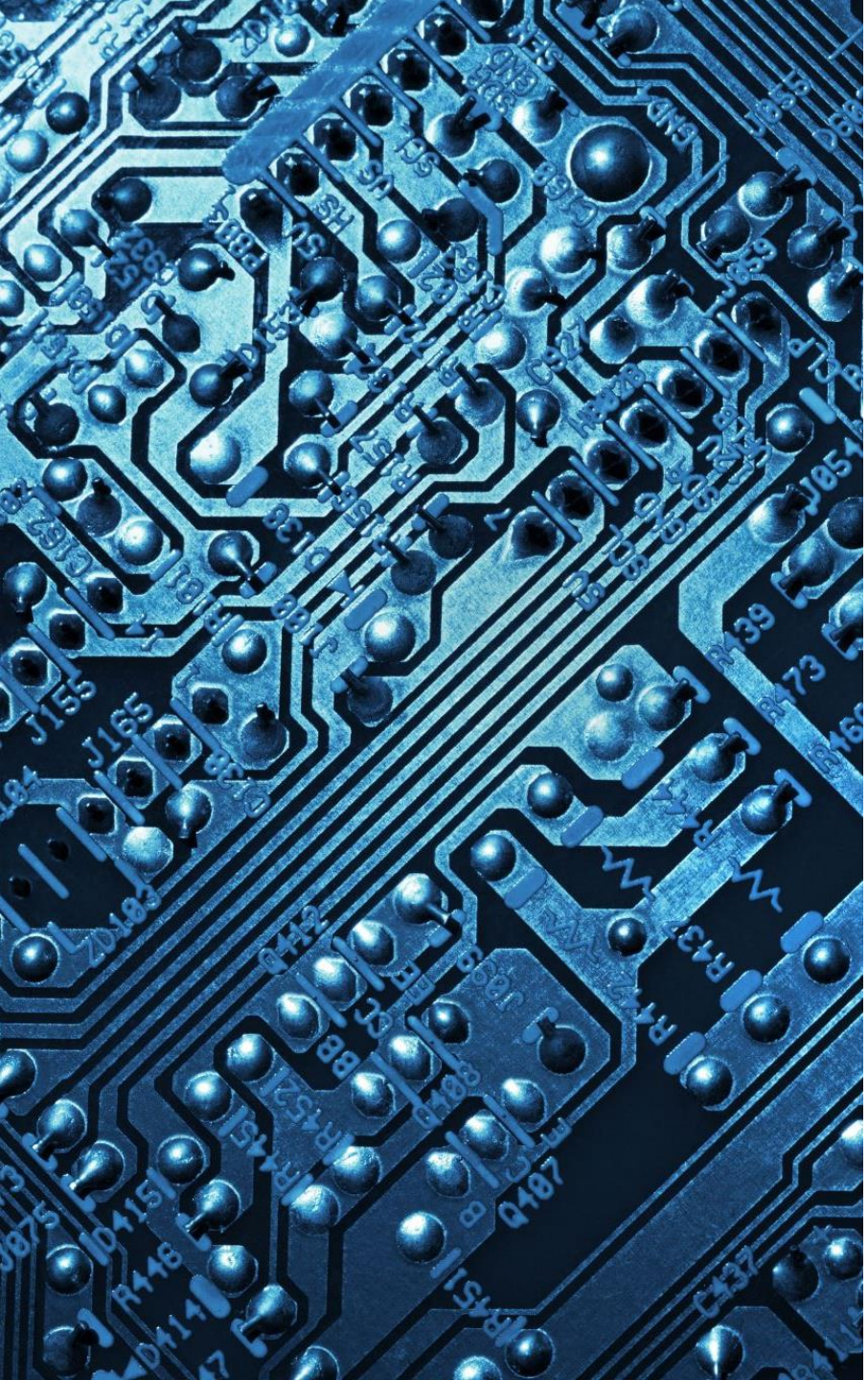
Description: Critical remote code execution vulnerability affecting Microsoft Exchange.
Exploitation: Used by ransomware groups like LockBit and Clop to gain initial access and later deploy ransomware.
Severity: High
Mitigation: Apply Microsoft's security updates.

Description: Unauthenticated remote code execution via SSL VPN feature in FortiOS.
Exploitation: Actively exploited by Clop ransomware to gain footholds within networks.
Severity: Critical
Mitigation: Patch FortiOS immediately.

Description: Privilege escalation in Windows Netlogon allowing attackers to take over domain controllers.
Exploitation: Used by groups like Ryuk and REvil.
Severity: Critical
Mitigation: Apply security patches and restrict domain controller access.

Description: RCE in Cisco ASA and Firepower devices via SSL VPN.
Exploitation: Exploited by BlackCat and DarkSide to gain access to entire networks and deploy ransomware.
Severity: Critical
Mitigation: Update Cisco ASA/Firepower firmware.

Description: Command injection vulnerability in Zoho ManageEngine API.
Exploitation: Exploited by Conti and Hive groups.
Severity: High
Mitigation: Apply Zoho patch and restrict API access.



2025 CYBERSECURITY THREAT STATISTICS

- **Surge in CVE Disclosures: 45,500+** CVEs to be disclosed in 2025.
- **Rising Threat Complexity**: The integration of advanced technologies, including artificial intelligence (AI), has led to more sophisticated cyber threats, necessitating enhanced detection and response strategies.
- **Increased Business Email Compromise (BEC) Attacks:** Increase in scams targeting corporate accounts, with cybercriminals employing AI to craft convincing emails from trusted sources, leading to significant financial losses—Per FBI, in 2023, 305,033 BEC incidents, with total losses of **$55.5 billion**.
- **AI-Driven Phishing Attacks:** Cybersecurity experts are alerting users to a new wave of AI-powered email scams that analyze social media activity to create hyper-personalized phishing emails, making them challenging to identify as fraudulent.
- **Escalating Costs of Cybercrime:** Cybersecurity Ventures estimates cybercrime damages will reach **$10.5 trillion** globally by 2025, reflecting increasing sophistication and frequency of cyber attacks.

TIPS & TAKEAWAYS

Cybersecurity Tips

- Keep systems patched & updated
- Do not use open Wi-Fi
- Multi-factor Authentication (MFA)
- Use secure VPN
- Practice Good Web Hygiene
- Secure Your Email
- If it's too good to be true… it is!

- ISC2 Pledges One Million FREE ISC2 Certified in Cybersecurity Courses and Exams
- Webcasts, White Papers, Posters & Cheat Sheets, Blogs, Templates, FREE Tools
- Google Cybersecurity Certificate
- FREE Cybersecurity Education Courses
- FREE Cyber Security Courses Online With Certificates

ALVAKA

Thank You!

Contact Alvaka 24x7 – restore@alvaka.net – (949) 428-5001
Dave Cunningham – (949) 307-5249 cell