Alvaka Patchworx℠ Patch Management as a Service

Hopefully, you have seen the news about the growing reality of ransomware and how it is impacting companies and government entities on a global scale. While ransomware is not new, the severity, reach and costs associated with this cyber threat are increasing exponentially. It has risen to the level of a national security threat. Ransomware is an existential threat to every business large and small. You do not need to be large or targeted for them to attack you.

As a network security provider with years of in the trenches ransomware defense and enterprise level recovery experience, we understand the real threat and what the long and painful road to recovery can involve. We have seen firsthand, companies that were successful for hundreds of years, put out of business due to a ransomware event. Companies from a single lawyer to hundreds of employees have ceased operations. Owners have liquidated 401ks and their life savings to just keep the company going after an event. Even where insurance is involved, the process takes days to months and always has costs above and beyond coverages.

The average ransom amount for just one of the hundreds of ransomware variants has risen to $939,063 per victim. We are here to tell you that this is also just the beginning of the costs of becoming a victim. Lawyers, incident response including forensics & remediations, reputational damage, new computing devices, potential breach notification, lawsuits, fines, and more are all normal recovery expenses. Many also lose employees and clients because of these attacks. These expenses are often multiples of the ransom paid. You must pay them, even when you choose not to pay the threat actor's ransom demand or you have a fully viable back-up. So, help us help you and act now in working to not become a victim.

Apply the following mitigations to reduce the risk of compromise by ransomware and other cyber-attacks:

- **Require** multi-factor authentication for local and remote network access of any nature and additionally for all admin / domain and application management functions.
- **Patch ALL** systems and patch frequently**.** This includes all OS patches AND third-party software. Patches should be deployed with a short period of time from vendor release. Our recommendation is patch at least once-a-month. Emergency security patches for zero-day exploits should be deployed within 3-5 days.
- **Manage or Remove** Deprecated or End-Of-Life systems to prevent them from being compromised through known security vulnerabilities that the vendor is no-longer addressing. If the system cannot be deprecated, then place the system into a 'DMZ' in which a security device is filtering down only specific source, destination addresses and port numbers to minimize your risk.
- **Update** Firewalls and other network device firmware

- **Enable** strong spam (email) filters to prevent phishing emails from reaching users. Filter emails to stop executable files.
- **Implement** user training and simulated attacks to discourage users from actions that typically cause malware infections and credential capture like opening email with malicious attachments or going to infected websites, etc.
- **Filter** network traffic to stop communications with known malicious IP addresses.
- **Implement** URL reputation services to block known malicious websites and classes of websites such as pornography, gambling, hacking, etc.
- **Limit** access to data and other assets to an as needed basis, internally and externally. Segment your network.
- **Restrict** remote systems access and implement best practices such as VPN, an RDP gateway and requiring multi-factor authentication.
- **Use** active scan antivirus/antimalware to conduct scans using up-to-date signatures.
- **Remove** all local admin rights and restrict non-IT staff rights to that of a standard user. Never use accounts with admin level rights to complete non-admin functions.
- **Disable** Office macros and/or consider using browser isolation or Office Viewer software to open Microsoft Office files not received or created internally.
- **Implement** a backup system that covers all critical data and system states. Be sure to do full restore testing and follow emergency procedures to ensure that they will work when you need them. Ensure that full restores of backups are regularly tested.
- **Protect** your ability to get back to business by:
    - **a.** isolating back-ups from the network; and
    - **b.** instituting insider protections. Many threat actors get domain level access. Remember, if you can delete, corrupt, or encrypt your back-up, so can the threat actor. This includes all forms of back-up including cloud. If they are acting as an admin, have access to documentation, email, passwords, etc., (which they most often do) even cloud services or "offline" copies will not help you; and
    - **c.** storing offline image templates with the appropriate preconfigured operating systems and applications to rebuild more quickly; and
    - **d.** storing license keys, source code and copies of executables.
- **Get** breach insurance that covers ransomware … this is significant subject we only touch on here due to the complexity and importance.
- **Ensure** your exception-based monitoring can immediately trigger alerts on common indicators of a security breach and that there are escalation procedures in place such that an engineer will assess the situation very quickly, regardless of the day of the week or time of day. CRITICAL NOTE: The starting of the encryption process for most large-scale ransomware events occurs during the night and on weekends, but most often on holiday weekends.
- **Create** a Business Continuity Plan (BCP) for security events**.** Do table-top simulations to ensure that all teams know what to do as rapidly and flawlessly as possible… **MINUTES** matter in ransomware breaches.

If you think you may have ransomware or even the known precursors, do not panic because that often causes mistakes. If you make the wrong move early in the process you can destroy any chance of full recovery. Please take it very seriously and act quickly. Disconnect all devices from the Internet (and all wireless) then call us immediately and we will begin to guide you through response. Hesitation can be a HUGE mistake. Waiting a few hours or until the next morning has resulted in infections that could have been stopped.

We have seen cases where swift action on first awareness would have saved 100s of thousands to millions of dollars in costs, months of negative impacts and even jobs. If you make the wrong move, threat actors will often know you have discovered them and pull the trigger on their plans early. You have potentially minutes to take action to stop them from executing.

a. Do not search for help, information on ransomware or any other thing that may tip off the attackers. They are very often watching what is happening on your actual computer and the network and will trigger their encryption earlier than planned.
b. Do NOT shut down a device that is known to be in the process of encryption. You may corrupt the OS or other applications and make recovery using the keys impossible.
c. Do not communicate on the network, company related email, IP phones, Teams, Slack, etc., as they are VERY OFTEN listening to and reading your communications.
d. Do not communicate with the threat actor until you have the support you need. This often starts a timer and having the right negotiator can have a massive impact on the results.

There is much more to this than what is written here, but we can help you. Call us if you would like to discuss your defensive posture, ransomware readiness and network security or our management solutions.

Please, do not hesitate to call if you need help in recovery from any cyber incident. If we cannot help with your specific issues, we will work to assist you with Alchemy Communications & CloudTrek in finding the support you require.

We are truly all in this fight together.

Alvaka Networks

Kevin B. McDonald
CISO & COO
Kevin@alvaka.net
Cell: 714-719-3191
www.alvaka.net