REVSOC

REVOLUTIONIZING SECURITY OPERATIONS

Ransomware

How an Open-XDR protects you against todays most notable cyber threat

Introduction

From 2018 to 2020, the world has seen a doubling in the total number of breaches up to 1120 breaches in 2020 (Lessons from analyzing 100 data breaches). With the average cost of a data breach at $3.86 million dollars, companies around the world are searching for solutions to avoid such a costly consequence. Beyond the quantitative value, breaches result in a loss of trust from customers. Without the trust of the public, a company cannot hope to maintain and advance its goals.

Today's biggest threat in the cybersecurity world is ransom attacks. Ransom attacks set themselves apart by being a multi-pronged attack. Once inside an organization's environment, ransomware can quickly encrypt systems and data and hold them for ransom. The organization can pay the ransom in the hopes of retrieving their data and the loss is simply the cost of the ransom. Or, if the organization isn't able to or doesn't want to pay the ransom, they risk losing their data and having to rebuild systems and restore data from backups. Furthermore, if they don't pay the ransom there is an additional risk of having their data leaked or sold across the internet if the attacker made a copy. (Even if they do pay the ransom to obtain a decryption key to restore their systems and data, having their data exposed is still a risk and they may be extorted again by the attacker.)

As stated previously, ransom attacks are growing. This concern has spread to private sector and public sector organizations alike. A study by Sophos found that of the respondents, 40% of central governments and public bodies were hit with a ransomware attack and of those, 49% stated that the cybercriminals were successful in encrypting their data.

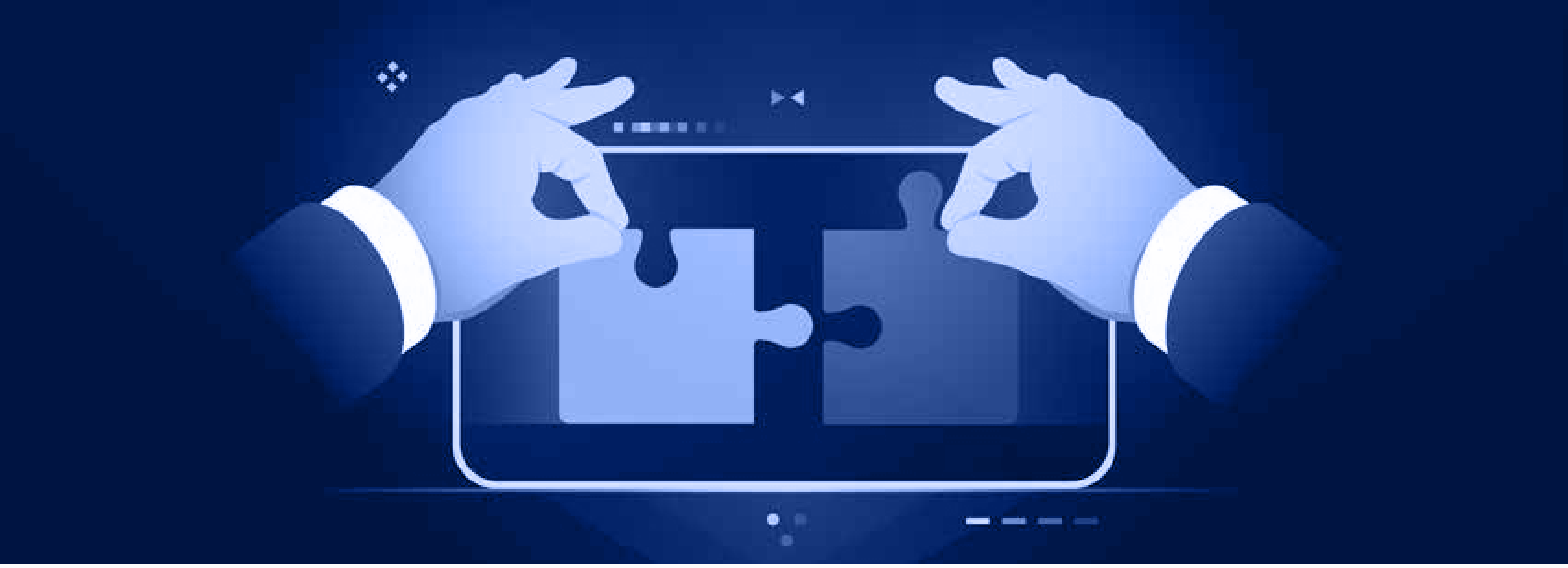
Background

In 2021 we saw the brutal reality of ransomware in action during the Kaseya cyber attack. Taking advantage of vulnerabilities in Kaseya's VSA, the attackers managed to take advantage of its central role in a far wider software supply chain. They leveraged various MSPs in order to attack their customers, small-medium sized businesses. In the end, the infiltration hit Kaseya, 50 of their direct customers, and 800-1500 businesses downstream which had their data and servers encrypted and workstations shut down.

In a similar circumstance, the Solarwinds attack is another example of the impact supply chain attacks can have and the need for strong security systems to combat hostile actors. In 2020, hackers managed to break into SolarWinds and infect their software system with malicious code. This code created a backdoor into the IT systems of all customers that used SolarWinds' product Orion. With this backdoor, hackers were able to install more malware in order to spy and take advantage of customers, which included the US Military, State Department, Pentagon, and 425 out of the US Fortune 500.

Given these events, it is clear this is an issue that can impact any organization regardless of size, stature, or overall security. Successful attack vectors will find their way into access points that have yet to be closed. With the advent of cloud and SaaS, access points are becoming too numerous and difficult to control, and organizations need solutions that can tackle modern threats.

[1] *Sophos. (2021). The State of Ransomware in Government 2021.*



Solution

Before trying to define the solution, let’s first understand what the attack vector may look like. Knowing how an attack needs to progress provides the context needed to conceptualize what an effective solution would encompass. A typical scenario involving ransomware can begin in a number of ways:

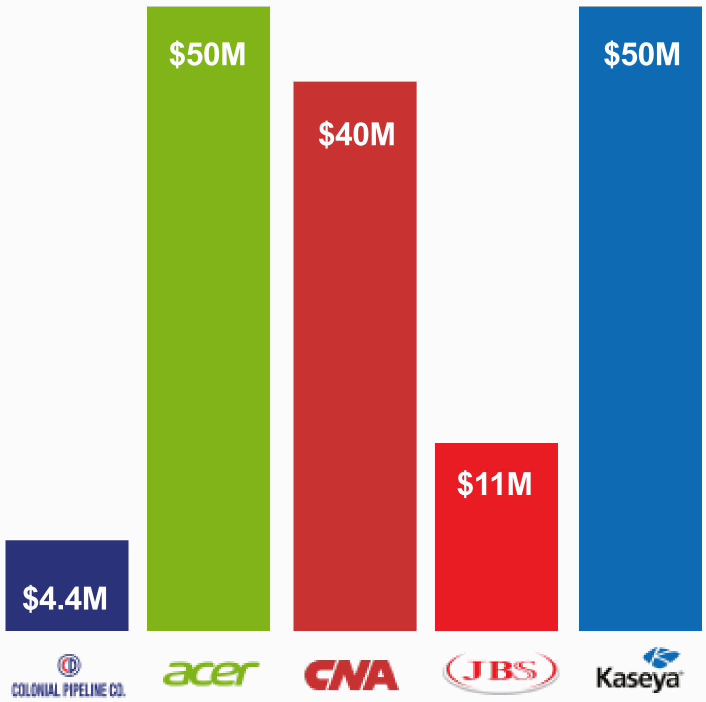
1. Leaked credentials are used to gain initial access
2. Social engineering phishing campaign where an internal user downloads a malicious executable from their email
3. A user accesses a malicious URL from within the corporate network where a malicious executable is triggered

In either case, an account has been compromised and a breach with the goal of locating sensitive data to hold hostage is underway. The attacker will proceed to determine the level of privilege this user has for places with sensitive employee or customer data such as CRMs (Salesforce, Netsuite), databases (MySQL, PostgreSQL, MongoDB, Elastic), data warehouses (SAP, Oracle, Snowflake), etc. If this user has admin-level privileges for any of these applications, then the attacker's job is easy and they can directly access the sensitive data. In the case where the compromised user has limited access, the attacker will communicate with an external command-and-control center to install tools that would enable them to find an admin account.

Now, the attacker can obtain credentials for this account through common hacking methods such as pass-the-hash, golden ticket, man-in-the-middle, or through obtaining SSH keys. If controls such as MFA are not implemented, the attacker has free reign to access sensitive data, encrypt it, and demand a ransom. It may seem like a daunting task to prevent a ransom incident due to the fact that it usually begins through internal user error, but there are a number of methods to both prevent and stay ahead of these attacks.

The saying, “identity is the new perimeter”, has recently generated a lot of buzz across the cybersecurity community. To expand, identity is one part of application configuration and with enterprises typically employing an average of 80 SaaS applications, it is near-impossible to have a grip on the configurations for each through manual processes. Furthermore, the disjointed nature of application ownership and security operations creates a shrouded veil that complicates any type of monitoring security operations teams can perform.

Significant Ransom Demands 2021



RevSoc AIR

Here at RevSoc, we believe the optimal way to prevent the escalation of ransomware is by vigilantly monitoring user access levels in the case that a breach does occur. With integrations for commonly used applications in place, we have a proven risk management model to provide visibility and raise red flags when a vulnerable user account is identified. A few risk scenarios we monitor include:

1. Admin access granted for a non-admin user (medium severity)
2. Non-admin user gains admin access, adds user(s), and grants admin access (high severity)
3. Spike in access attempts from a user (medium severity)
4. Rare storage access based on user and peer group analysis (medium severity)
5. Files download and emailed to external account or upload to file storage site (high severity)

These detections are derived from a combination of spike and rarity modeling which are then reinforced by deep learning to continuously improve the efficacy of these models.

Ultimately, the key to prevent ransomware is a two-pronged defense system consisting of thorough monitoring and robust threat hunting so that in the case that reconnaissance or account compromise does occur, it is identified, analyzed, and mitigated before the breach can escalate to a case of ransomware.

These alerts are correlated based on identity and are neatly packaged into an incident which is displayed in a chronological timeline view. This easy to understand history trail is supplemented with predictions from the RevSoc Brain that inform the analyst what event will occur next if there is no SOC intervention.

The models that provide both observed alerts as well as predictions are continuously tuned to ensure high-efficacy so that the SOC is not inundated with false positives. With this abundance of analysis all viewable in a single screen, the incident responder can confidently mitigate the breach before it even has a chance to progress to a more detrimental stage such as lateral movement or defense evasion.

In summary, ransomware is the most prominent threat facing businesses today and as we have seen with organizations such as Kaseya and SolarWinds, the slightest overlooked configuration error can do tremendous damage to a company's reputation and balance sheet. As unfortunate as these breaches were, these attacks are an opportunity for companies to learn and evolve through greater visibility and more advanced detection techniques. The RevSoc Autonomous Incident Responder (AIR) is the cloud-native, autonomous solution positioned to enable your SOC to preempt ransomware before you receive that ill-fated demand of payment.

[1] *Mlitz, K. (2021). Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2020. https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/.*