www.pipelinepub.com
Volume 20, Issue 1

Ransomware Defense: Cutting the Kill Chain

By: Koroush Saraf - VP Product Management, ZPE Systems

Ransomware attacks plague organizations with major disruptions and financial losses. Gartner has gone so far as to describe ransomware as the modern-day disaster, with a Sophos survey showing that over 70% of affected organizations require more than two weeks to fully recover from an attack. Recent high-profile breaches on organizations like MGM and Caesars, as well as the thousands of organizations using the MOVEit protocol, have underscored the resilience and adaptability of threats despite there being thousands of modern cybersecurity products in use. Although security products are vital to protecting systems, the crux of the issue is rooted in what cybersecurity expert John Kindervag dubs the "chewy center" of the network – the people who operate IT.

Ransomware Threat Vector 1: Human Weakness & Social Engineering

Humans are the weakest link in any ransomware defense strategy. This is why they are the prime target for savvy attackers. Even the most keen-eyed administrators and network engineers can be tricked into opening a malicious file, clicking a deceptive link, or like in MGM's case, creating an admin account for a seemingly real user. Ransomware groups leverage an organization's trusted users to perform these minor actions, which then kick off the rest of the attack.

Verizon's 2023 Data Breach Investigations Report (DBIR) shows that 74% of all successful cyberattacks involve some form of human engagement (see Figure 1 on next page). "Engagement" refers to errors, privilege misuse, the use of stolen credentials, or succumbing to social engineering tactics. Of these breaches, 83% involve external actors, with financial gain being the primary motivation for 95% of all breaches (see Figure 2 on next page). Attackers gain access mostly by stealing credentials, phishing, or exploiting vulnerabilities.

Social engineering is a highly effective tactic for cybercriminals. Business Email Compromise (BEC) attacks, a form of pretexting, have nearly doubled across the DBIR dataset. (Figure 3 on next page) shows that pretexting attacks now account for more than 50% of social engineering incidents.

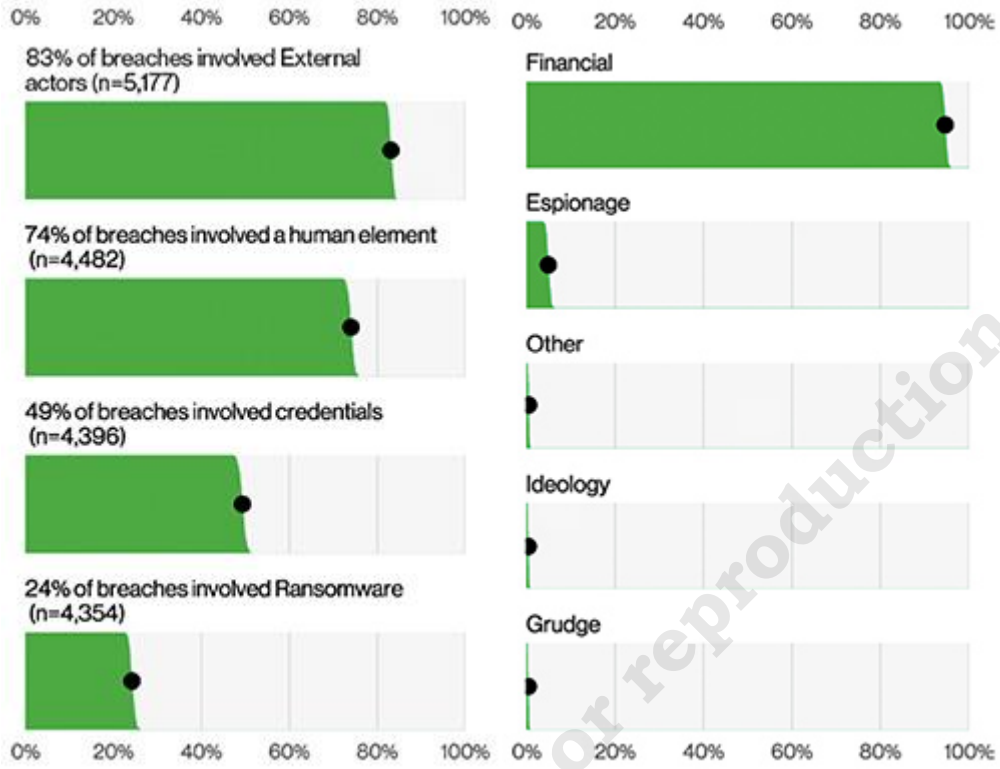

Figure 1: Select key enumerations. Figure 2: Threat actor motives in breaches.
Source: Verizon's 2023 Data Breach Investigations Report (DBIR)

Recent high-profile attacks prove how simple and effective it can be to exploit humans through social engineering:

- **MGM attack:** In September 2023, adversaries used "vishing" — a form of phishing over the phone — to convince an MGM staff member to create an administrator account for the attacker. This set in motion the entire kill chain, with the compromised account being used to create additional accounts, propagate the attack, and ultimately force MGM to shut down revenue-generating operations.

- **RagnarLocker attack:** In September and October 2023, cybercriminal group RagnarLocker used BEC to attack many organizations. Using a form of email stuffing, they tricked IT staff into opening seemingly legitimate files that would then encrypt systems for ransom. This affected critical operations for many organizations and their customers.To make this vector even more enticing, attackers know that it's common for organizations to give administrator privileges to every IT admin. Virtually anyone within a large IT organization can be exploited to trigger an attack. Also, many IT teams don't follow the practice of requiring dual-admin approvals, which means they can create accounts or make significant changes without a second pair of eyes checking their work. Once an attack is initiated, it often results in major collateral damage due to the second significant threat vector.

Ransomware Threat Vector 2: Weak Systems

Once a breach is successful, it spreads at machine speed to discover and exploit weaknesses within the system itself. The MGM attack is a perfect example of this. The adversary, having gained elevated Okta privileges, deployed a ransomware "vending machine." This began to automatically spit out scripts to every server and encrypt critical applications within minutes. The casino giant was left with no option other than to shut down revenue-generating services.

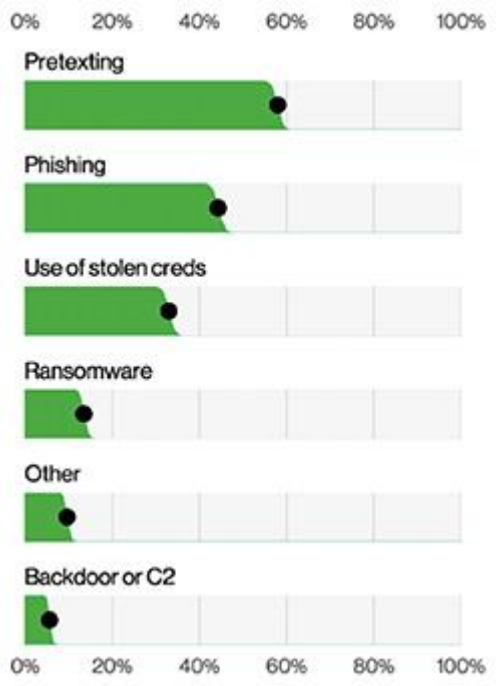

Figure 3: Action varieties in Social Engineering incidents.

Weaknesses typically look like:

- **Unpatched systems:** A joint study from 2022 showed that 76% of vulnerabilities still being exploited were discovered between 2010 and 2019. Attackers know that admins are reluctant to update systems due to the potential to cause outages, which means the landscape is rife with outdated and vulnerable targets.
- **In-band management:** Many organizations use a management network that relies on their production network. When attacks occur, this makes it impossible to take systems offline to sanitize, rebuild, and restore. If attackers have persisted in this network for any length of time, it's likely that they've also compromised backups, making it impossible to recover quickly.

Why it's difficult to cut the ransomware kill chain

There are several ways organizations can reinforce their defenses against ransomware. These address the processes and systemic challenges described in the threat vectors above, and include: There are several ways organizations can reinforce their defenses against ransomware. These address the processes and systemic challenges described in the threat vectors above, and include:

- More training: Extensive training empowers IT staff to more effectively identify, detect, and prevent cyber exploits, such as phishing/vishing and malicious emails.
- NetDevOps automation: NetDevOps involves integrating software development lifecycle practices into IT operations. Rather than IT staff making changes directly to systems, this approach mandates approvals from a secondary party before changes are deployed through an automation framework.
- Frequent patching: Regular system patching ensures organizations are protected from novel malware and CVEs (Common Vulnerabilities and Exploits).
- Segmentation and Zero Trust Security: Network segmentation, in the form of nano- or even pico-segmentation, reduces the attack surface as well as minimizes collateral damage. This involves segmenting user traffic and isolating management interfaces.

Every IT team can benefit from additional training, rigorous system patching, and comprehensive segmentation and zero trust measures. But, regardless of how prescriptive or precise their tactics may be, there's a significant gap to overcome: teams simply don't know where or how to start.

For instance, days before the MGM attack, Okta published an article outlining tactics to detect and prevent cross-tenant impersonation (the kind of attack that affected MGM). Even if staff had read up on the prescriptive, low-level approaches described in the article, they would still need to answer questions, like:

- In what environment do we implement these changes?
- How can we be sure that our changes won't break anything?
- If an attack is successful, can we stop it? How fast? And what will it cost?

As previously mentioned, cybersecurity products are one critical component to combating attacks. But the other component is an organization's ability to recover. Due to recent ransomware incidents, CISA, the FBI, and NetDevOps practitioners have described isolation as the key to combating ransomware.

How Isolation cuts the ransomware kill chain

In response to global vulnerabilities related to open management ports, CISA issued a binding operational directive that mandates organizations to establish an Isolated Management Infrastructure (IMI). As shown in Figure 4 on next page), the IMI fullyseparates the management network from the production network, so that production is not directly managed and that management does not depend on production infrastructure. Additionally, the IMI calls for segmenting the management network, and routing BMC and IPMI ports to terminate on top-of-rack switches, which prevents the creation of a wide and exposed IT network. This architecture also incorporates zero trust using NetDevOps processes. In order for changes to be made, change requests must be reviewed and approved by a committee.

The IMI offers the following benefits:

- No more automation anxiety: The IMI is an environment where staff can build their automation skills, without worrying whether they'll break the production network.
- No more outdated systems: The IMI is where staff can build end-to-end pipelines for automated patching, so their systems are always up to date.
- No more collateral damage: The IMI incorporates zero trust security and segmentation. If an attack slips through the cracks, it can't spread beyond the entry point.

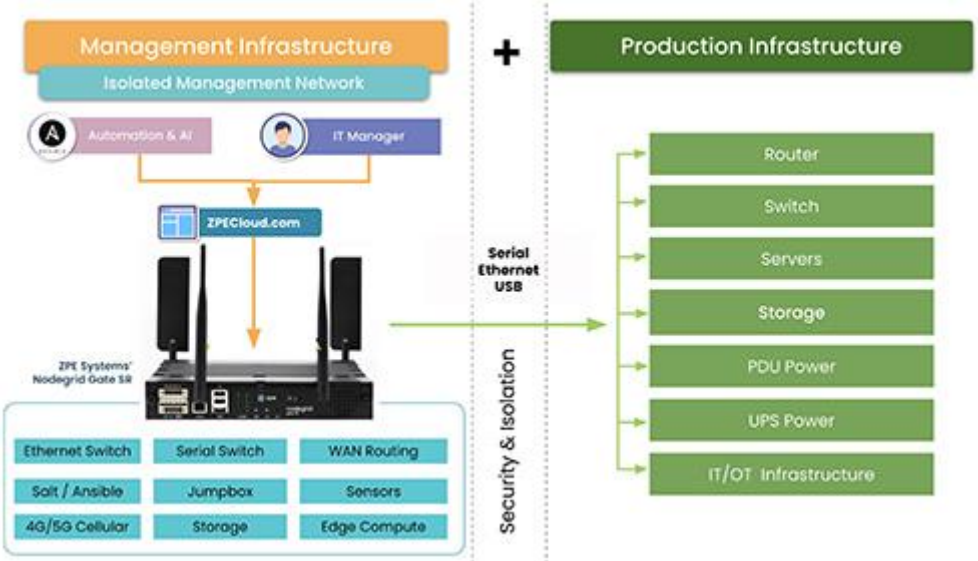

Figure 4: The Isolated Management Infrastructure (IMI) creates a management network that is fully separate from the production infrastructure.
Click to Enlarge

IMI addresses both ransomware attack vectors

Implementing an IMI is crucial to addressing both ransomware attack vectors. It offers a safe environment for teams to experiment with implementing new cybersecurity products or defense strategies. But more importantly, the IMI is a secret weapon that allows organizations to fight back against ransomware and recover quickly.

Closing the Social Engineering Attack Vector

Human errors and social engineering trigger significant ransomware attacks. Creating accounts and opening malicious files on non-segmented, in-band management networks results in widespread infrastructure damage and millions in financial losses. But the IMI closes this attack vector, by providing administrators with an environment that's completely separate from production systems. This allows them to experiment with new training and tools, develop their automation skills, and gradually implement NetDevOps practices. The IMI helps to ensure that any change, whether it be creating a new account or installing a file, goes through an approval process. This drastically increases the chances of cutting the kill chain before the attack can even begin.

Strengthening Weak Systems

Attackers find it easy to fracture traditional systems, because they're usually outdated and offer feeble options for recovery. But with an IMI, they get to implement both defensive and offensive tactics. For defense, the IMI lets them safely test automation workflows to ensure system integrity and achieve a lights-out approach that automatically installs the latest patches. If an attack does breach their defenses, teams get to fight back using dedicated management access to every piece of infrastructure. They can deploy what Gartner calls an Isolated Recovery Environment (IRE). Using the IMI's fully isolated management interfaces, teams can use the IRE to take affected systems offline, wipe configurations/devices clean, and restore systems without risking reinfection.

Make sure you can cut the ransomware kill chain

Despite thousands of modern cybersecurity products, combating ransomware depends on an organization's ability to avoid social engineering exploits and system weaknesses. Recovery is now just as important as prevention. This involves implementing adequate defenses in the form of automated patching, and also having the ability to fight back against attacks by using NetDevOps and segmentation. The critical step any organization can take right now is to implement an Isolated Management Infrastructure (IMI), which is a best practice that has been in use by Big Tech for nearly a decade.