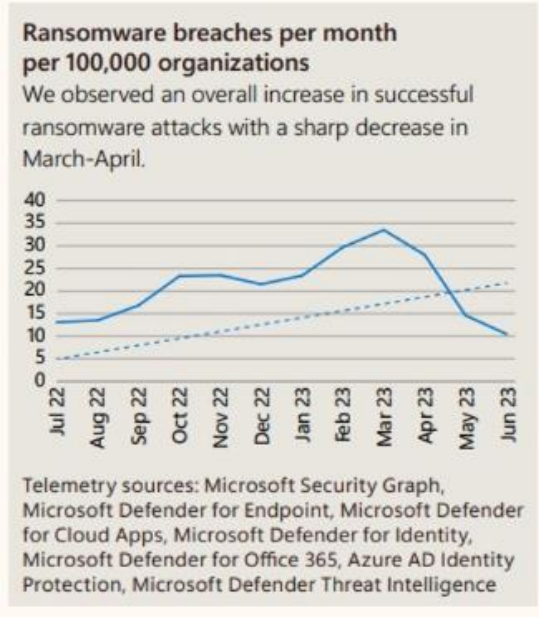
Fortifying Network Defenses: Advanced Strategies for Ransomware Prevention
By Ilya Feigin (CISSP, MBA)
2024.01.02

1. Introduction

The current cybersecurity landscape is marked by evolving and increasingly sophisticated threats. Cybercriminals are leveraging advanced techniques, exploiting vulnerabilities in human behavior and technology to conduct large-scale, effective attacks. Ransomware remains a significant threat, with attackers shifting towards more hands-on keyboard attacks and using remote encryption for concealment. Business Email Compromise (BEC) attacks have also seen a sharp rise. Additionally, the use of cloud resources by threat actors for Distributed Denial of Service (DDoS) attacks has become more prominent. The landscape underscores the need for robust, adaptable cybersecurity solutions to counter these diverse and evolving threats.

Network ransomware attacks are escalating in frequency and severity, posing a major threat to organizations worldwide. These attacks involve the encryption of a victim's data by malicious actors, who then demand a ransom for decryption. The impact of these attacks extends beyond data loss to significant operational disruptions and financial damages. Ransomware groups are continuously enhancing their tactics, targeting not just large corporations but also small and medium-sized businesses. The rise of ransomware-as-a-service (RaaS) models further complicates the landscape, making it easier for attackers to launch sophisticated attacks without advanced technical skills. This evolving threat underscores the urgent need for effective and advanced cybersecurity measures.



In response to the escalating threats in the cybersecurity landscape, there's a critical need for advanced security solutions. Traditional security measures are often insufficient against sophisticated cyber attacks, especially those involving ransomware. The complexity of modern IT environments, including cloud services and mobile computing, further complicates security management. Advanced solutions must provide comprehensive, multi-layered protection, integrating innovative technologies like AI and machine learning for proactive threat detection and response. Additionally, they need to ensure adaptability to rapidly evolving threats and compliance with stringent regulatory standards, making the development and implementation of such solutions imperative for safeguarding digital assets and maintaining operational continuity.

2. Understanding Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data until a sum of money is paid. There are various types of ransomware, including:

- Crypto Ransomware: Encrypts valuable files on a device, demanding payment for the decryption key.
- Locker Ransomware: Locks users out of their operating system, making it impossible to access files or applications.

- Scareware: Fakes the appearance of a security threat or pretends to be a security tool, coercing users to pay to fix non-existent issues.
- Doxware/Leakware: Threatens to publish stolen information online unless a ransom is paid.
- RaaS (Ransomware as a Service): Provides ransomware tools or services on a subscription basis, allowing cybercriminals without technical expertise to execute attacks.

Ransomware attacks typically follow certain methods:

- Phishing Emails: Using deceptive emails to trick recipients into downloading ransomware.
- Exploiting Network Vulnerabilities: Targeting unpatched software or network weaknesses to gain unauthorized access.
- Drive-By Downloads: Compromising legitimate websites to automatically download ransomware onto a visitor's device.
- Remote Desktop Protocol (RDP) Exploits: Gaining access through weakly secured RDP setups.
- Malvertising: Distributing malicious ads that install ransomware upon interaction.
- Social Engineering: Manipulating users into granting access or downloading ransomware.

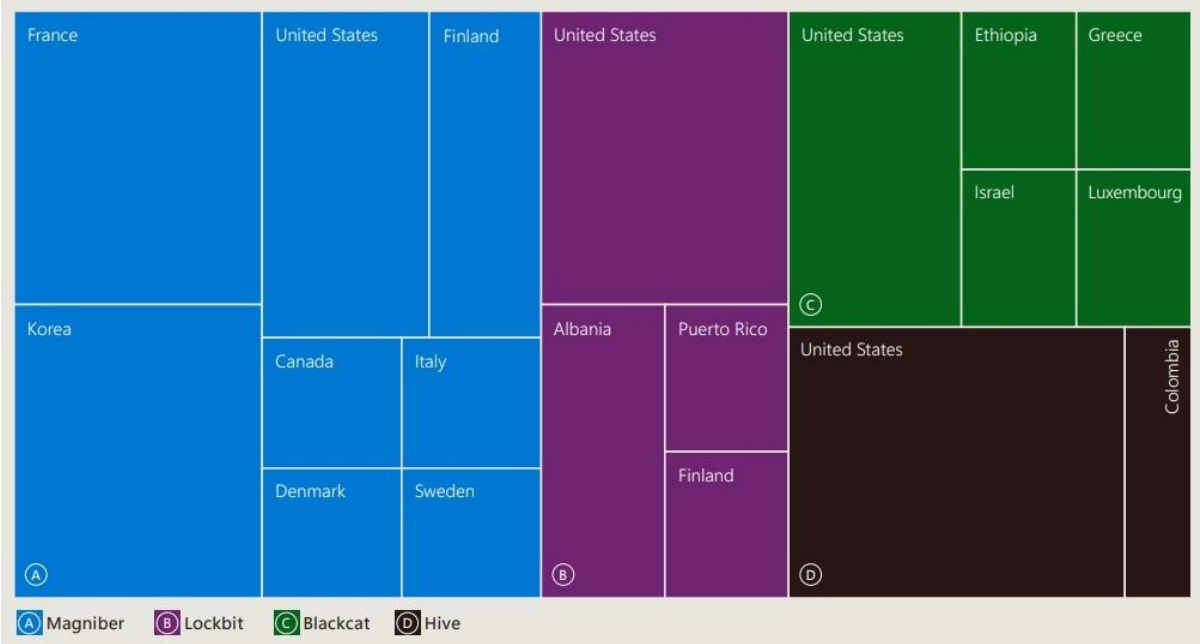
The target systems of ransomware attacks are mostly:

- External Remote Services: Adversaries leverage unsecured Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN). RDP and VPN vulnerabilities provide a direct pathway for attackers to gain remote access to a network.
- Public Facing Applications: Cybercriminals exploit vulnerabilities in public-facing applications, ranging from zero-day vulnerabilities to those that are several years old. Commonly targeted applications include Zoho, Java ManageEngine, Microsoft Exchange, MOVEit, and PaperCut print management software. These vulnerabilities provide an entry point for attackers to inject ransomware into the system

2.1. Case studies: High-profile ransomware incidents

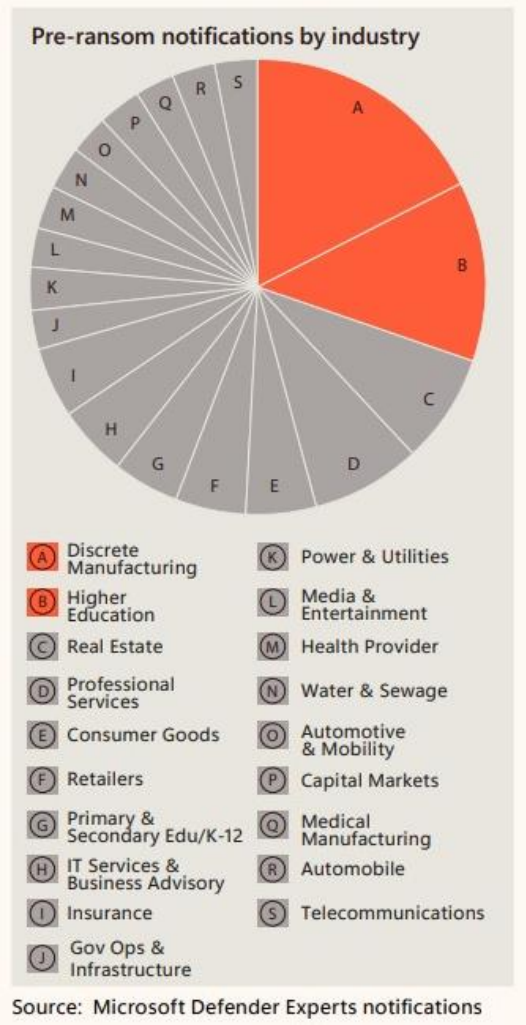
In recent years, several high-profile ransomware incidents made it to the front page news. Here are some examples:

- WannaCry (2017): This attack spread rapidly, affecting more than 200,000 computers across 150 countries. It targeted the Windows operating system using a vulnerability in the SMB protocol. The attackers demanded Bitcoin payments for decryption keys. The impact was extensive, crippling numerous organizations including the UK's National Health Service, causing widespread disruption in healthcare services.
- NotPetya (2017): Initially targeting organizations in Ukraine, NotPetya rapidly spread worldwide, causing billions of dollars in damages. Unlike typical ransomware, NotPetya's primary goal seemed to be widespread disruption rather than financial gain. It leveraged a vulnerability in Microsoft Windows and was particularly damaging due to its ability to spread within networks.
- Colonial Pipeline (2021): This attack on one of the largest pipeline operators in the United States led to significant disruptions in fuel supply across the East Coast. Colonial Pipeline paid a ransom of $4.4 million. The incident highlighted the vulnerability of critical infrastructure to ransomware attacks and had far-reaching implications for national security and the economy.



2 Ben Gurion road
B.S.R 1 Building
Ramat-Gan 5257334
Israel
Tel: +972-3-9190909
Fax: +972-3-9190910
info@embedded-solutions.co.il

3. Impact of Ransomware on Businesses



As this malicious software continues to evolve in complexity and potency, the ripple effects felt across the entire spectrum of business activities serve as a stark reminder of the vulnerability of our digital infrastructure:

- Economic implications: Ransomware attacks can be financially devastating. The direct costs include the ransom payment, if made, and the expenses related to data recovery and system restoration. Indirect costs include operational downtime, lost revenue during the period of disruption, and potential loss of future business. In some cases, the financial impact can be severe enough to threaten the company's solvency, especially for small and medium-sized enterprises.
- Impact on business operations and reputation: Operational impacts include the immediate cessation of critical business functions, which can lead to a halt in production, service disruptions, and loss of critical data. The recovery process can be lengthy and complex, further exacerbating operational delays. From a reputational standpoint, a ransomware attack can erode customer trust and confidence, potentially leading to a long-term decline in customer base and difficulty in acquiring new business.
- Legal and compliance considerations: Legal implications arise if customer or employee data is compromised, leading to potential lawsuits or regulatory penalties. Businesses are often subject to various data protection laws, and non-compliance due to a ransomware attack can result in significant fines. Additionally, companies may face increased scrutiny from regulatory bodies and a requirement to strengthen their cybersecurity measures to prevent future incidents.

4. Recommended approach to counter ransomware via network by Israeli Cyber Security Authority:

A robust cybersecurity posture requires vigilant monitoring for any deviations from established network and application norms. Proactive measures should include the scrutiny of protocols, applications, and traffic behavior, with a particular focus on detecting and mitigating actions that fall outside typical patterns. By implementing strict controls and monitoring, especially concerning high-risk IPs and domains, and by being alert to sophisticated tactics like multiple encapsulation layers, organizations can better shield themselves against the diverse and evolving landscape of cyber threats. Specifically organizations must deploy devices that detect and block such unusual network activity as:

- DNS over HTTP
- APP-ID doesn't fit the protocol
- Port doesn't fit the usual protocol/application behavior
- Unexpected bandwidth use
- Unexpected session quantity
- Activity in unusual time of day/year
- Unusual Decoding/Encoding methods
- Access to low reputation IPs/Domains such as VPN servers, Proxy, Known Attack Servers
- Use of multiple encapsulation layers

5. Current Solutions and Their Limitations

5.1. Existing cybersecurity measures against ransomware

- Current cybersecurity strategies against ransomware encompass a range of tools and practices. Antivirus software plays a crucial role, constantly scanning systems for known ransomware signatures to prevent infection. Firewalls are another line of defense, designed to block unauthorized access attempts and filter out potentially harmful traffic. Intrusion Detection Systems (IDS) monitor network activities, identifying and alerting on any unusual patterns or potential threats.
- Regular data backups, preferably stored off-site or on isolated networks, are pivotal for disaster recovery. These backups should be updated frequently to ensure minimal data loss in the event of an attack. Moreover, keeping software and systems up-to-date with the latest patches and security updates is vital. These updates often address known vulnerabilities that ransomware attackers exploit.
- Beyond technical measures, human factor mitigation plays a critical role. Employee education and awareness training are essential in reducing susceptibility to phishing attacks, which are common entry points for ransomware. This training typically includes identifying suspicious emails, understanding safe internet practices, and promoting a culture of cybersecurity awareness within the organization.

5.2. Limitations and gaps in current solutions

While essential, antivirus software often falls short against new ransomware variants. 'Locky', for example, evades detection by frequently altering its digital signature, a method known as polymorphism. This technique allows it to slip past signature-based antivirus defenses, compromising systems before they can be updated with the new signatures. This demonstrates a critical gap in traditional antivirus approaches, which rely heavily on known virus databases and struggle to keep up with rapidly evolving malware.

Firewalls and Intrusion Detection Systems (IDS) are fundamental but not infallible. The 'EternalBlue' exploit showcased this vulnerability. It leveraged a weakness in Windows' SMB protocol, a flaw not recognized by many firewalls or IDS. As a result, it facilitated the rapid spread of the WannaCry ransomware across networks that believed they were protected. This incident underscores the need for more advanced network monitoring tools that can detect unusual patterns and behaviors, rather than just relying on known threat signatures. In addition, firewalls themselves are targets of attack, and are often leveraged by attackers to compromise the network.

The role of backups in ransomware mitigation is critical but can be undermined if not properly managed. The 'SamSam' ransomware attacks highlighted this, as they targeted organizations with poorly protected or outdated backups, encrypting them alongside primary data. This incident illustrates the importance of not only regular backups but also ensuring these backups are isolated from the network and updated in real-time to prevent simultaneous compromise.

- Training and Human Error: Human error remains a significant vulnerability in cybersecurity. Even with extensive training, employees can be tricked by sophisticated phishing schemes, as seen in the 'Ryuk' ransomware attacks. These attacks often began with a spear-phishing email that appeared legitimate but contained malicious links or attachments. This highlights the necessity for continuous education and the implementation of advanced email filtering technologies that can detect and block sophisticated phishing attempts.
- Static Solutions and Evolving Threats: Traditional cybersecurity solutions often struggle to adapt to new threats. The 'WannaCry' ransomware capitalized on this by targeting unpatched systems with a known security vulnerability. The speed and scale of the WannaCry outbreak emphasized the need for dynamic security solutions that not only address known threats but also proactively identify and mitigate emerging vulnerabilities through advanced analytics and machine learning techniques.

6. BNS (Bit Net Sentry) by Embedded Solutions 3000

Embedded Solutions 3000, a leading Israeli cybersecurity company, has been at the forefront of innovative cybersecurity solutions. It is known for its advanced technology initially designed for the Israeli Armed Forces and later adapted for civilian use. Recognizing the evolving cybersecurity threats, the company developed the Bit Net Sentry (BNS), a cutting-edge network security appliance. BNS represents a culmination of years of expertise in cyber defense, integrating advanced features like invisibility to attackers, white box cryptography, and zero-trust architecture to provide robust protection against sophisticated cyber threats. This development showcases the company's commitment to evolving cybersecurity needs and its capability to deliver solutions for both defense and civilian applications.

6.1. Key capabilities of BNS

- Invisibility: BNS's unique feature of operating without an IP or MAC address renders it invisible and undetectable to attackers. This stealth mode significantly enhances network security by obscuring the presence of the defense mechanism, thus reducing the attack surface.
- Firewall Concealment: BNS can conceal an existing firewall within its framework. This not only protects the firewall from direct attacks but also allows it to function unimpeded, maintaining its filtering capabilities while being shielded from potential threats.
- Advanced Encryption: Utilizing white box cryptography, BNS encrypts each data frame with a new algorithm and key. This approach ensures a highly secure communication tunnel, free from the vulnerabilities associated with traditional password-based systems.

- Anomaly Detection: BNS's ability to detect and block anomalous traffic is based on various parameters like IP/MAC addresses and bandwidth. This feature is crucial for identifying and mitigating unusual network activities that could signify a cyber threat.
- Network Separation: The appliance can effectively segregate Operational Technology (OT) and Information Technology (IT) networks. This separation is compliant with the IEC62443 standard and includes features like bidirectional separation, deep packet inspection, and custom rule implementation, ensuring secure and controlled access to OT environments.

7. BNS: A Solution Tailored for Ransomware Defense

   BNS (Bit Net Sentry) from Embedded Solutions 3000 effectively counters common ransomware attack vectors through its unique features. Its invisibility feature, which operates without an IP or MAC address, significantly reduces the chances of being targeted by ransomware that scans for network vulnerabilities. The advanced encryption capabilities, utilizing white box cryptography, ensure secure communication channels, preventing interception and encryption of data by ransomware. Moreover, the anomaly detection system of BNS, capable of identifying unusual network activities, is crucial for early detection and mitigation of ransomware attacks. By addressing these vectors, BNS offers a robust defense against ransomware threats. Some key features include:

   - Invisibility: BNS's lack of an IP or MAC address is a strategic advantage. This invisibility means it doesn't appear on network scans, a common method used by ransomware like 'WannaCry' to find targets. By being invisible, BNS effectively removes itself from the radar of potential attackers, reducing the risk of being directly targeted or compromised by ransomware seeking vulnerable network nodes.
   - White Box Cryptography: Unlike traditional encryption methods, white box cryptography used by BNS offers a more secure way to protect data. This method encrypts data in a way that makes the encryption key extremely difficult to extract, even if the attacker has full access to the encrypted data. This level of security is critical in protecting against ransomware attacks that attempt to hijack data transmission or storage processes to encrypt data for ransom.
   - Zero-Trust Microsegmentation: Implementing zero-trust principles, BNS does not automatically trust any entity inside or outside its network. By segmenting the network, BNS ensures that even if a part of the network is compromised, the ransomware cannot easily propagate to other segments. This microsegmentation is particularly effective against ransomware strains like 'Ryuk' and 'Petya', which spread laterally across networks after initial infection.

   Each of these features contributes to a robust defensive posture against ransomware attacks, addressing different aspects of network vulnerability and attack methodologies.

8. Case Studies: BNS in Action

   8.1. In the deployment at a Traffic Light Control Center, BNS is effectively preventing ransomware attacks by ensuring secure communication between the traffic lights (TLs) and the Traffic Management Center (TMC). The configuration blocks any unauthorized traffic to the TLs, only allowing defined, approved communication. Attempts to send traffic to unicast addresses of TLs

not part of the current session or to a multicast group are identified and blocked by BNS. This deployment led to the decision to equip additional TLs with BNS, enhancing security through encrypted, micro-segmented traffic control, thereby successfully thwarting potential ransomware threats.

8.2. In a European Industrial Company, the deployment of BNS successfully counters a severe ransomware attacks. BNS was installed on both WAN and LAN sides of the company's firewall. It was configured to replicate the firewall's rules and block any external or internal attempts to access the firewall's management ports. This strategy effectively concealed the firewall from network mapping attempts and unauthorized access, both externally and internally. The implementation of BNS led to the discovery of a persistent backdoor in the firewall and ongoing malware activity within the network, highlighting its effectiveness in enhancing network security. The success of this deployment prompted the company to expand BNS usage to other branches and key network hubs.

8.3. In the case involving an Eastern European Company, BNS effectively prevented insider-led ransomware attacks via legal VPN connections. BNS was deployed across multiple branches and the data center, configured to allow only White Box Cryptography (WBC) protected tunnels. This setup led to the redirection of a non-WBC protected VPN, used by the attacker, to a 'honey trap' server. This deployment of BNS successfully identified and neutralized the insider threat, leading to the company-wide adoption of BNS for enhanced security.

9. Why BNS is best for ransomware defense

Ransomware typically infiltrates an organization through phishing attacks or network vulnerabilities and then spreads laterally, encrypting data. BNS addresses these challenges effectively:

9.1. Infiltration Prevention with Invisibility: BNS's unique feature of invisibility, lacking an IP or MAC address, makes it undetectable to ransomware that scans networks for vulnerabilities. This significantly lowers the risk of initial infiltration, as ransomware often relies on identifying network devices to target.

9.2. Robust Encryption Defense with White Box Cryptography: Once inside a network, ransomware attempts to encrypt data. BNS employs white box cryptography to encrypt data in transit, making it far more challenging for ransomware to intercept and encrypt this data. This advanced encryption ensures that even if ransomware penetrates a network, its ability to access and manipulate data is severely hindered.

9.3. Propagation Block with Zero-Trust Microsegmentation: After initial infiltration, ransomware typically tries to spread laterally across the network. BNS's zero-trust microsegmentation effectively segments the network, rigorously controlling access and traffic flow within it. This approach is crucial in limiting the movement of ransomware within the network, preventing it from reaching critical data or systems.

These features collectively make BNS a robust solution for ransomware defense. By addressing both the entry and spread of ransomware, BNS provides comprehensive protection against these increasingly sophisticated cyber threats.

10. Future-Proofing with BNS

10.1. BNS’s adaptability to evolving ransomware tactics

BNS is uniquely designed to keep pace with changing ransomware strategies. Its core features, like network invisibility and sophisticated white box cryptography, provide robust defense

mechanisms that remain relevant against new and evolving ransomware methods. BNS's adaptability is further enhanced by its configurable nature, allowing it to be tailored to counter specific emerging threats. This flexibility ensures that BNS remains a powerful tool against both current and future ransomware tactics.

10.2. Ongoing development and support

The commitment to ongoing development and support by Embedded Solutions 3000 is a critical aspect of BNS's effectiveness. Regular updates to its algorithms and threat databases ensure that BNS stays ahead of the latest cybersecurity threats, including new variants of ransomware. This ongoing support and development mean that BNS is not just a solution for today's security challenges but is continually evolving to address the cyber threats of tomorrow. By ensuring constant improvements and updates, BNS remains a future-proof solution in the rapidly evolving landscape of cybersecurity.

11. Conclusion

In today's digital age, the increasing frequency and sophistication of ransomware attacks highlight the critical need for advanced cybersecurity solutions like BNS. Its unique features, including network invisibility, advanced white box cryptography, and comprehensive zero-trust microsegmentation, provide an unmatched level of security. These capabilities are essential for effectively combating the multifaceted nature of modern cyber threats and protecting vital digital assets.

Organizations across various sectors are adopting BNS as a strategic move towards enhancing their cybersecurity posture. The adoption of BNS not only offers immediate protection against existing ransomware threats but also ensures resilience against future cyber challenges. By integrating BNS into their cybersecurity strategy, organizations can significantly mitigate the risk of devastating cyber attacks, safeguard their operations, and maintain the trust of their stakeholders.

Learn more at www.embedded-solutions.co.il

2 Ben Gurion road
B.S.R 1 Building
Ramat-Gan 5257334
Israel
Tel: +972-3-9190909
Fax: +972-3-9190910
info@embedded-solutions.co.il