

FORENSICS REPORT ON WANNACRY RANSOMWARE

by D.L PRASANNA

INTRODUCTION

In May 2017, a major cyber-attack occurred involving the WannaCry ransomware crypto-worm, affecting over 200,000 computer systems across 150 countries worldwide. WannaCry encrypted data on infected Windows machines and demanded ransom payments in Bitcoin cryptocurrency to restore access. Major organizations impacted included Britain's National Health Service (NHS), global shipping giant FedEx, telecommunications companies like Telefónica, automakers like Renault, and many other enterprises and government entities. WannaCry proliferated by exploiting a vulnerability in Microsoft's Server Message Block (SMB) protocol using an exploit called Eternal Blue, previously leaked from the U.S. National Security Agency. Unpatched systems running older versions of Windows were most vulnerable. The initial infection vector for WannaCry is still unknown, but once on a system it replicated itself across local networks and the internet without user interaction, behaving like a computer worm.

TECHNICAL OVERVIEW

WannaCry is categorized as a ransomware cryptoworm, embodying characteristics of a worm virus, trojan horse, and crypto-ransomware extortion attack. This malicious software primarily spread through a vulnerability in the Windows Server Message Block (SMB) protocol, exploiting Eternal Blue, a leaked NSA exploit, to propagate across networks autonomously. The initial infection likely stemmed from a malicious email attachment or through unpatched systems connected to the network. WannaCry employed robust encryption (AES-128) to encrypt files on compromised systems, rendering them inaccessible without the decryption key. Victims were confronted with a ransom note demanding payment in Bitcoin to acquire decryption keys, typically ranging from 300to600. The impact of WannaCry on [Organization] was profound, causing significant disruptions including downtime, data loss, and financial implications due to critical systems' unavailability. This ransomware employed various cryptographic techniques such as Diffie-Hellman key exchange for encryption key establishment, elliptic curve DSA digital signatures for verifying ransomware component authenticity, and the Tor anonymous network for communicating with remote command servers.

ATTACK ANALYSIS

The WannaCry attack unfolded through distinct stages based on forensic evidence. Initially, variants of WannaCry were compiled as early as February 2017, suggesting a lengthy development period. The malware's code incorporated components from previous malware associated with the Lazarus APT group, indicating a sophisticated and possibly state-sponsored origin.

The initial distribution method of WannaCry remains somewhat elusive, but it is suspected to have utilized phishing campaigns and malicious software bundles to infect target systems. Once inside a network, WannaCry exploited a critical vulnerability in the SMB protocol to gain access and automatically spread to connected machines.

Upon execution, WannaCry deployed a Double Pulsar kernel payload, enabling the injection and execution of the ransomware component. This ransomware swiftly encrypted files on local drives and network shares, rendering them inaccessible to users. Victims were presented with ransom notes demanding payment in Bitcoin, typically ranging from 300to600, with a deadline of 7 days.

WannaCry propagated aggressively, scanning for and infecting any vulnerable external IP addresses it encountered. It leveraged hardcoded Tor gateways and inter-

acted with Bitcoin wallet APIs over the Tor network to maintain anonymity and facilitate ransom payments. Notably, there was no evidence of traditional persistence mechanisms designed for long-term infiltration; instead, WannaCry aimed to spread rapidly and effectively before drawing attention to its activities.

DIGITAL FORENSICS FINDINGS

Forensic analysis of WannaCry revealed significant insights into its functionality and behavior. Notably, there was no evidence suggesting prior attacker access or staging was necessary for the encryption process. The ransomware utilized a pair of hardcoded Bitcoin wallet IDs to receive ransom payments, leveraging Tor and Bitcoin mixing services to obscure the transaction trail effectively. Unlike targeted attacks, WannaCry did not appear to have the capability to selectively target specific systems or data. Moreover, no apparent persistence mechanisms or backdoors for further access were identified, indicating a singular focus on encryption and ransom. The encryption mechanisms employed were robust, rendering file recovery impossible without the decryption keys. Despite its high disruption potential, WannaCry's intent seemed primarily geared towards indiscriminate economic disruption through crypto-ransomware, rather than traditional targeted intrusion behaviors.

ATTRIBUTION ANALYSIS

Identifying the individuals or groups responsible for WannaCry solely through forensic analysis presents formidable challenges. Bitcoin transactions associated with ransom payments are pseudonymous, lacking directly tied identities. Additionally, the use of Tor gateways and mixing services effectively conceals true network origins. Notably, WannaCry's code incorporated components reused from other malware with suspected North Korean origins, though no definitive links to previous Lazarus Group activity were established. Certain clues, such as the utilization of elite cyberattack tools typically attributed to nation-state groups, suggest a potentially state-sponsored operation. The ransomware also demonstrated relatively sophisticated anti-analysis and evasion capabilities, with evidence suggesting the existence of testing versions months before the widespread attack. Despite these indicators, no clear monetary motive was discerned, given the untraceable nature of ransom payments. Ultimately, while WannaCry displays characteristics consistent with a state-sponsored attack, concrete evidence linking it to a specific group remains elusive based on available forensic data alone.

IMPACT ASSESSMENT

The WannaCry cyberattack in May 2017 had a profound and widespread disruptive impact globally. Over 200,000 systems across more than 150 countries were

affected during the wave of attacks. Major hospitals, manufacturers, and telecommunication companies experienced significant operational disruptions. The financial costs stemming from operational downtime were estimated to be in the billions, underscoring the severity of the attack. WannaCry highlighted critical cyber risk exposures in both the public and private sectors, prompting urgent reassessment of cybersecurity strategies. High-profile victims included Britain's National Health Service (NHS), global logistics giant FedEx, Spanish telecom firm Telefónica, and French automaker Renault, among numerous other enterprises, universities, and government agencies. Fortunately, many organizations mitigated ultimate losses through backup data sources, but the attack underscored systemic vulnerabilities in IT patch management, emphasizing the critical importance of timely updates and robust cybersecurity measures in defending against such threats.

MITIGATION RECOMMENDATIONS

To mitigate threats from similar large-scale ransomware incidents like WannaCry, organizations should implement comprehensive strategies across multiple fronts. Firstly, prioritizing patch management is crucial. This involves implementing rigorous programs to promptly apply security patches, especially for operating system vulnerabilities. Immediate application of the Microsoft MS17-010 patch to address the SMB vulnerability exploited by WannaCry is essential. Additionally, upgrading from older, unsupported Windows versions like XP or Server 2003 can reduce exposure to known vulnerabilities.

Secondly, system hardening measures are essential. Organizations should enable firewalls to block SMB ports from external networks, implement application whitelisting to restrict unauthorized software execution, and enforce strict administrative privileges to limit the impact of potential breaches. Using reputable anti-malware tools and keeping signatures updated further enhances system defenses.

Thirdly, proactive network monitoring is critical. Continuous monitoring for signs of malicious scanning or propagation can help detect and mitigate threats early. Analyzing outbound encrypted traffic for suspicious activity can also uncover potential ransomware communication attempts.

In terms of data protection, maintaining verified backups of critical data is imperative. Backups should be stored offline or with air gapping to prevent them from being compromised in a ransomware attack. Additionally, utilizing whitelisting techniques to prevent the execution of unapproved software on endpoints can limit the impact of ransomware infections.

Lastly, organizations should prioritize incident response preparedness. Developing and regularly testing comprehensive incident response and recovery plans en-

sures readiness in the event of a ransomware attack. Conducting security awareness training for the workforce on current threats and best practices for cybersecurity enhances overall organizational resilience against ransomware and other cyber threats. By implementing these measures, organizations can significantly reduce the risk and impact of large-scale ransomware incidents similar to WannaCry.

STRATEGIC ANALYSIS

The WannaCry ransomware attack underscored several critical strategic implications that organizations must address to enhance cybersecurity resilience. Firstly, the widespread use of obsolete and unpatched software was a key factor enabling the global propagation of WannaCry. This highlights the urgent need for organizations to prioritize upgrade cycles and deploy patches promptly to mitigate software lifecycle risks.

Secondly, interconnected systems and networks pose supply chain risks by allowing lateral movement and spreading of ransomware. Organizations must recognize and address third-party dependencies that can introduce new threat vectors into their systems.

Thirdly, the evolving cyber-threat landscape presents challenges as cyberattacks become more potent, autonomous, and indiscriminate. Destructive malware like WannaCry now poses a significant risk to any vulnerable system, emphasizing the importance of robust cybersecurity measures.

Furthermore, allegations of state involvement in cyberattacks raise concerns about escalating cyber conflict. The leak of cyberweapons, as seen with WannaCry's use of NSA exploits, may empower rogue actors and proxy groups to conduct large-scale cyber operations.

While ransomware attacks have existed for years, the unprecedented scale, pace, and sophistication of WannaCry demonstrate an escalating cyber-threat environment that demands proactive preparation from all organizations. By addressing these strategic implications and adopting comprehensive cybersecurity strategies, organizations can better defend against evolving cyber threats and mitigate the impact of future ransomware incidents.

RECOMMENDATIONS

To enhance resilience against ransomware attacks like

WannaCry, organizations should adopt comprehensive cybersecurity strategies. Firstly, prioritize patch management by ensuring all systems are promptly updated with the latest security patches. Patching known vulnerabilities can significantly reduce the risk of exploitation by ransomware and other malicious threats.

Deploying and maintaining robust endpoint protection solutions is essential. These solutions should be capable of detecting and blocking ransomware threats at the endpoint level, preventing malicious software from executing and spreading across the network.

Regular security awareness training for employees is crucial. Educate staff on recognizing phishing attempts and suspicious attachments, as these are common vectors for ransomware infections. Building a security-conscious workforce can significantly reduce the likelihood of successful ransomware attacks.

Implementing and maintaining regular backups of critical data is imperative. In the event of a ransomware attack, having up-to-date and verified backups enables swift recovery without succumbing to ransom demands. Data backups should be stored securely and offline to prevent them from being compromised in a cyberattack.

By integrating these measures into a comprehensive cybersecurity strategy, organizations can bolster their defenses against ransomware attacks and minimize the impact of potential incidents. Proactive mitigation efforts and employee education are key components in safeguarding against evolving cyber threats like WannaCry.

CONCLUSION

The WannaCry ransomware attack was one of the most widespread, disruptive cyber incidents to date, affecting systems globally across the public and private sectors. Its worm-like propagation ability combined with crypto-ransomware tactics revealed how brittle many organizational IT environments remain to potential cyberthreats. While the full origins and motives behind WannaCry's development and release remain unclear, the attack reinforced the need for robust vulnerability management, system hardening, data protection, and incident response capabilities. As cyber threats continue to escalate in scope and sophistication, entities of all types must prioritize investments in cyber resilience and preparedness to ensure operational continuity and data security against future widespread malware incidents.