DIGITAL FORENSIC ON APPLIED MATERIALS RANSOMWARE CYBERATTACK

by D.L PRASANNA

INTRODUCTION

Applied Materials is a major American company that supplies manufacturing equipment, services and software to the semiconductor, display and related industries worldwide. As a critical supplier in the global semiconductor supply chain, any disruption to Applied Materials can have widespread impacts. In March 2023, Applied Materials was hit by a devastating ransomware cyberattack that crippled its operations across multiple sites. The culprit was identified as the LockerGoga ransomware strain, known for its ability to rapidly encrypt files across networks and demand hefty ransom payments. This attack laid bare the vulnerabilities semiconductor companies face from increasingly sophisticated and disruptive cyberthreats targeting their complex manufacturing processes and intellectual property. The fallout highlighted the pressing need for robust cybersecurity measures to secure critical technology infrastructure supply chains.

INCIDENT IDENTIFICATION

Incident identification is the crucial first step in responding to a ransomware attack. Applied Materials likely employs a combination of automated monitoring tools and human vigilance to detect signs of unauthorized access, suspicious activities, or system malfunctions. These monitoring mechanisms continuously analyze network traffic, system logs, and security alerts to identify anomalies that may indicate a potential security incident. In the case of a ransomware attack, indicators such as unusual file encryption patterns, unauthorized access attempts, or the presence of known malware signatures may trigger alerts within Applied Materials' security operations center (SOC) or incident response team. Additionally, employees may report unusual system behavior or error messages, prompting further investigation by the IT security team. Once an incident is identified, Applied Materials' response team springs into action to assess the situation, contain the threat, and initiate the incident response process. This may involve isolating affected systems, disabling compromised user accounts, and escalating the incident to higher levels of management for additional support and resources. Timely and accurate incident identification is critical for minimizing the impact of a ransomware attack and restoring normal operations as quickly as possible.

SCOPE OF THE INCIDENT

Understanding the scope of a ransomware incident is essential for effectively managing the response and minimizing its impact on Applied Materials' operations. The scope encompasses the breadth and depth of the attack, including the number of systems and networks affected, the types of data compromised, and the extent of disruption to business processes. Applied Materials' incident response team conducts a thorough assessment to determine the scope of the incident, leveraging a combination of technical tools, forensic analysis, and collaboration with internal stakeholders. This assessment helps identify the full extent of the attack, including any lateral movement by the attackers, data exfiltration activities, and potential backdoor access points left behind. By accurately defining the scope of the incident, Applied Materials can prioritize response efforts, allocate resources effectively, and communicate transparently with internal and external stakeholders. This enables the organization to focus its efforts on restoring critical systems and data, while also implementing measures to prevent similar incidents in the future. Additionally, understanding the scope of the incident is crucial for complying with regulatory requirements and reporting obligations.

TIMELINE RECONSTRUCTION

Timeline reconstruction is a critical aspect of incident response, providing a chronological sequence of events leading up to and following the ransomware attack on Applied Materials. The timeline helps the incident response team understand the attack's progression, identify potential entry points, and determine the attackers' tactics, techniques, and procedures (TTPs). Applied Materials' incident response team begins by gathering relevant data sources, including system logs, network traffic captures, and security alerts. They analyze these sources to piece together a timeline of key events, such as the initial compromise, lateral movement within the network, deployment of ransomware, and any attempts to exfiltrate data or establish persistence. By reconstructing the timeline, Applied Materials can identify gaps in its security posture, determine the effectiveness of existing controls, and refine incident response procedures for future incidents. Additionally, the timeline serves as a valuable resource for communicating with stakeholders, documenting the incident for regulatory compliance purposes, and conducting post-incident analysis to extract lessons learned.

EVIDENCE COLLECTION

Evidence collection is a meticulous process aimed at preserving digital artifacts related to the ransomware attack on Applied Materials. This includes gathering a wide range of data sources, such as system logs, memory dumps, file metadata, and network traffic captures, to support forensic analysis and attribution efforts. Applied Materials' incident response team follows established protocols to ensure the integrity and admissibility of collected evidence. They use specialized tools and techniques to acquire forensic images of affected systems, capturing volatile data such as running processes and network connections. Additionally, the team maintains detailed documentation of the evidence collection process, including timestamps, chain of custody records, and relevant contextual information. The collected evidence serves multiple purposes, including identifying the attackers' tactics and methods, supporting legal and regulatory investigations, and strengthening the organization's overall cybersecurity posture. By carefully preserving and analyzing digital evidence, Applied Materials can gain valuable insights into the ransomware attack and take proactive measures to prevent similar incidents in the future.

THE ATTACK VECTOR

While the initial infection vector is still under investigation, evidence suggests the LockerGoga ransomware gained initial access to Applied Materials' network likely through a security vulnerability in internet-exposed systems or via a malware-laced phishing email opened by an employee. Once inside, LockerGoga employed techniques to harvest administrator credentials and rapidly deploy malicious encryption across interconnected systems and manufacturing equipment. Its worm-like lateral movement abilities allowed it to cascade across Applied's networks globally within hours. The ransomware encrypted critical data and rendered many of Applied's systems inoperable by overwriting master boot records. This in effect "bricked" manufacturing equipment, as rebooting failed without access to the now-encrypted data required for operations.

SYSTEM ANALYSIS

System analysis is a crucial component of incident response, allowing Applied Materials' security team to examine affected systems for signs of compromise and identify the impact of the ransomware attack. This process involves forensic examination of system artifacts, including file system metadata, registry entries, and memory dumps, to understand the attackers' actions and restore the integrity of affected systems. Applied Materials' incident response team uses specialized tools and techniques to conduct system analysis, focusing on identifying indicators of compromise (IOCs), such as malware executables, malicious registry keys, and anomalous user account activity. They also analyze system logs and event records to trace the attack's progression and identify any unauthorized access or data manipulation. By conducting thorough system analysis, Applied Materials can assess the extent of the damage caused by the ransomware attack, prioritize restoration efforts, and implement measures to prevent future incidents. Additionally, the findings from system analysis may inform incident response procedures, threat intelligence sharing, and security awareness training for employees.

NETWORK TRAFFIC ANALYSIS

Network traffic analysis is a critical aspect of incident response, enabling Applied Materials' security team to monitor and analyze network communications for signs of malicious activity. This process involves capturing and examining network packets to identify indicators of compromise (IOCs), anomalous behavior, and potential security threats. Applied Materials' incident response team utilizes network monitoring tools and intrusion detection systems to collect and analyze network traffic in real-time. They look for patterns indicative of ransomware activity, such as large volumes of encrypted traffic, communication with known malicious domains, or suspicious command-and-control (C2) communications. By conducting network traffic analysis, Applied Materials can detect ransomware attacks early in their lifecycle, contain the spread of malware, and mitigate the impact on critical systems and data. Additionally, the findings from network traffic analysis may inform threat intelligence sharing, network security enhancements, and incident response procedures to improve the organization's over-

all cybersecurity posture.

USER BEHAVIOR ANALYSIS

User behavior analysis plays a crucial role in incident response, helping Applied Materials' security team identify and investigate anomalous activities that may indicate unauthorized access or insider threats. This process involves monitoring and analyzing user behavior patterns across the organization's IT infrastructure to detect deviations from normal activity. Applied Materials' incident response team leverages user activity logs, authentication records, and access control lists to conduct user behavior analysis. They look for indicators such as unusual login times, multiple failed login attempts, or access to sensitive files and systems outside of normal working hours. By analyzing user behavior, Applied Materials can detect potential signs of compromise early in the attack lifecycle, enabling prompt response and containment efforts. Additionally, user behavior analysis helps identify areas for improving security awareness training and implementing stronger access controls to prevent unauthorized access to sensitive data and systems.

DIGITAL FOOTPRINT EXAMINATION

Digital footprint examination is a comprehensive assessment of Applied Materials' online presence, including internet-facing assets, cloud services, and third-party connections. This process helps identify potential attack vectors and vulnerabilities that could be exploited by threat actors to gain unauthorized access or compromise sensitive data. Applied Materials' incident response team conducts digital footprint examination using a combination of automated scanning tools, manual reconnaissance, and threat intelligence analysis. They assess the organization's exposure to external threats, such as open ports, misconfigured cloud services, or outdated software versions, and prioritize remediation efforts accordingly. By examining its digital footprint, Applied Materials can identify and mitigate security risks proactively, reducing the likelihood of successful cyberattacks and minimizing the impact of potential incidents. Additionally, digital footprint examination helps improve visibility into the organization's attack surface, enabling more effective threat detection and response capabilities.

ATTRIBUTION

Attribution involves identifying the perpetrators behind a ransomware attack, understanding their motives, and determining their capabilities. While attributing attacks with absolute certainty can be challenging, Applied Materials' incident response team collaborates with external threat intelligence sources, law enforcement agencies, and cybersecurity partners to gather evidence and attribute the attack to specific threat actors or groups. Attribution efforts may involve analyzing malware signatures, command-and-control infrastructure, and TTPs used in the attack. Additionally, threat intelligence sharing and analysis of historical attack patterns may provide valuable insights into the attackers' identity and motivations. While attribution is important for understanding the broader threat landscape and informing strategic cybersecurity decisions, Applied Materials' primary focus is on mitigating the immediate impact of the ransomware attack, restoring operations, and strengthening its defenses against future incidents.

BUSINESS DISRUPTIONS

As LockerGoga ransomware took hold, Applied Materials was forced to completely halt production at multiple factories and service centers across the United States starting on March 31, 2023. Impacted sites included major manufacturing plants in Texas, California and Massachusetts among others. Key capabilities lost included atomic layer deposition, plasma-enhanced chemical vapor deposition and epitaxy tools critical for semiconductor fabrication processes. With systems no longer functioning, Applied could neither take new orders, load recipes for production runs nor ship completed products. This brought significant disruption to Applied's customers, many of whom are leading semiconductor manufacturers reliant on the company's equipment and services for their operations. Industry analysts estimated potential product shipment delays across the chipmaking supply chain.

COST & REVENUE IMPACT

While the full costs are still being calculated, analysts initially estimated the ransomware attack could have cost Applied Materials between $300 million to 500 million in lost productivity, delayed revenue and other direct expenses from system restoration efforts in the incident's first few weeks alone. With major manufacturing lines idled for days, Applied warned investors it was unable to fulfill product shipments generating hundreds of millions in expected quarterly sales during the disruption timeframe. This forced the company to substantially lower its revenue guidance for the quarter. The impacts rippled down Applied's supply chain as semiconductor fabricators were unable to receive expected equipment and services, potentially disrupting their production schedules. Some announced plans to implement additional inventory buffers against future supply chain shocks.

RESPONSE & CONTAINMENT

Upon detecting the ransomware encryption activity, Applied Materials quickly activated cybersecurity incident response protocols to attempt to stop its spread and regain control of systems. This included proactively taking some manufacturing networks offline while affected equipment was isolated from corporate networks.

The company engaged third-party cybersecurity forensics experts as well as collaborating closely with law enforcement agencies like the FBI in their investigation efforts. However, LockerGoga had already achieved a widespread encryption footprint before being contained days later. Rather than pay the ransom demand, Applied Materials instead opted to undertake a lengthy process of restoring impacted systems from available backups, where possible. This still required reconstructing some data and retooling manufacturing lines - an immense technical challenge.

MITIGATION & RECOVERY

Mitigation and recovery efforts are essential for minimizing the impact of a ransomware attack and restoring normal operations at Applied Materials. The organization's incident response team employs a multi-faceted approach to address immediate threats, restore affected systems and data, and strengthen its cybersecurity posture against future incidents. Mitigation measures may include isolating affected systems, disabling compromised accounts, and deploying temporary workarounds to mitigate the impact of the ransomware attack. Additionally, Applied Materials implements security patches, updates endpoint protection solutions, and enhances security configurations to prevent further exploitation of vulnerabilities. Recovery efforts focus on restoring critical systems and data from backups, decrypting encrypted files, and ensuring the integrity of restored data. Applied Materials' incident response team works closely with internal stakeholders, third-party vendors, and regulatory authorities to coordinate recovery efforts and minimize disruption to business operations.

DATA COMPROMISE ASSESSMENT

In a small relief, Applied Materials stated that its investigation found no evidence that the LockerGoga ransomware operators had exfiltrated any customer data or other confidential information during the attack and encryption spree. This helped avoid an additional data breach compounding the ransomware incident. However, the extent of internal data encrypted by LockerGoga is still being assessed. Much of Applied's proprietary manufacturing process documentation, equipment schematics, software codebase and other intellectual property was potentially at risk of permanent compromise or loss if restoration from backups proved imperfect. Securing this trove of sensitive data was a top priority as Applied undertook measured steps to remediating engineering workstations and resurrecting manufacturing systems without enabling any lingering backdoor access for the ransomware threat actors.

VULNERABILITY ANALYSIS

The successful LockerGoga ransomware infection exposed potential gaps in Applied Materials' cybersecurity posture that enabled the threat actors' broad access across its interconnected environments. This raised questions around patch management processes, network segmentation strategies and personnel security awareness. Applied Materials' size, geographic distribution and technology integration made securing its sprawling IT/OT footprint incredibly complex. Sophisticated threat actors had likely conducted thorough reconnaissance to map out attack paths and strike manufacturing operations. Experts warned many other semiconductor and technology companies could have similar unaddressed cybersecurity vulnerabilities, especially in securing proprietary manufacturing processes traditionally prioritized for safety and functional integrity over cyber resilience.

INDUSTRY WAKE-UP CALL

Applied Materials' cyber incident represented one of the most impactful and disruptive ransomware attacks on the semiconductor industry and broader technology supply chain. It served as a dramatic wake-up call on the existential cybersecurity risks these companies face from determined threat actors. In the aftermath, there were forceful calls from government and industry leaders for companies to dramatically increase investments in cybersecurity capabilities, personnel, and processes to better defend against crippling attacks that could cause cascading disruptions. Cybersecurity risk management and resilience planning was thrust into the spotlight as a critical issue for semiconductor supply chains. There were also renewed concerns around overreliance on tools and components from untrusted sources that could potentially introduce vulnerabilities.

GOVERNMENT's ROLE

Given the national security implications of semiconductor technologies, the U.S. government closely monitored and provided assistance to Applied Materials in responding to this cybersecurity incident impacting a key domestic chipmaking supplier. Applied Materials collaborated with agencies like the Department of Energy and the Cybersecurity and Infrastructure Security Agency (CISA) as part of the investigation and remediation process. The FBI also joined efforts to identify and potentially pursue the LockerGoga ransomware perpetrators. This high-profile attack helped catalyze efforts around implementing cybersecurity policies and regulations to enhance protection for critical technology companies. It also renewed discussions around public-private data sharing partnerships to improve cyber threat intelligence across industry.

DOCUMENTATION & REPORTING

Documentation and reporting are essential components of the incident response process, providing a com-

prehensive record of the ransomware attack on Applied Materials, response efforts, and lessons learned. The organization maintains detailed documentation of all aspects of the incident response, including incident identification, scope assessment, evidence collection, and mitigation measures implemented. Applied Materials' incident response team prepares incident reports for internal stakeholders, executive management, and regulatory authorities, as required by applicable laws and industry regulations. These reports outline the timeline of events, impact assessment, response actions taken, and recommendations for improving cybersecurity posture. Additionally, Applied Materials conducts post-incident reviews to identify areas for improvement in incident response procedures, security controls, and employee training. Documentation and reporting facilitate knowledge sharing, accountability, and continuous improvement in Applied Materials' cybersecurity practices.

LESSONS & THE PATH FORWARD

The ransomware attack on Applied Materials served as a stark reminder of the severe disruptions that destructive cyber threats can inflict on global semiconductor supply chains. One key takeaway was the industry's vulnerability due to underinvestment in cybersecurity. It underscored the critical need for comprehensive risk assessments encompassing both IT and operational technology (OT) environments. Strong backup, restoration capabilities, and well-defined incident response plans were highlighted as crucial elements for mitigating ransomware impacts. Proactive threat hunting and containment strategies were emphasized as preferable alternatives to paying ransoms. Moreover, bolstering the skilled cybersecurity workforce emerged as an imperative for the future.

While no organization can prevent all incidents, the scale of Applied Materials' breach emphasized the existential importance of implementing cybersecurity best practices and building resilience across semiconductor and critical infrastructure supply chains. Continued collaboration between industry and government is essential to confront the evolving cyber threat landscape. Such collaboration fosters the development of new defensive innovations and enables coordinated responses to systematically reduce cybersecurity risks over time. By embracing these principles and fostering collaboration, the semiconductor industry can fortify its defenses and safeguard against future cyber threats.