Chris Evans
Prof. Shuai Hao
CS 465 Information Assurance
April 20, 2022

Information Assurance Report Project

Summary

On January 1st, 2022 ABC Inc. experienced a security incident that compromised our internal networks which provided administrative and financial operations. This incident crippled our operations for 16 days. An employee in our administrative support section received a phishing email that appeared to be coming from an authentic source, which contained an Excel spreadsheet attachment. Quickly after opening the spreadsheet, 4 minutes from our review, a program named Zloader began stealing sensitive data which included but not limited to logins and passwords. After being active in our system for 3 weeks our financial and administrative network segments were attacked with Ryuk ransomware software and locked down with a ransomware program that demanded payment to the amount of $50,000,000.00 USD. After Ryuk ransomware was loaded onto more than 40 hosts on our ABC IT network, ABC Inc. experienced approximately 3 weeks where it was unable to carry out normal operations like customer billing, or paying vendor invoices. Luckily not all systems were affected and engineering and manufacturing activities were operational. The Computer Security Incident Response Team (CSIRT) team was able to identify, contain and remove all malware that created the ransomware attack. Our networks, hosts, servers and backups were all then reviewed to make sure they were operational, and unchanged. After ensuring the networks and hosts were no longer affected normal operations resumed.

Background

ABC Inc is the leading widget manufacturer in North America, with operations extending to Asia, South America, and Europe. We source materials and component parts from all over the world before assembly at our 10,000 sq-ft Norfolk, Virginia assembly plant. ABC Inc. has copy written an unique manufacturing processes that combines Adamantium and Unobtanium in our widget production process. This unique intellectual property is a closely guarded secret and one that gives us an advantage over competitors in the marketplace with consumers who value quality. ABC has been pursuing a policy of vertical integration and seeking to gain ownership overall strategic partners who contribute to our productions. This policy of acquisition has led our governance board to attempt to integrate computer systems and networks as efficiently

and simply as possible in an attempt to develop elegant solutions. Currently we have are 3 companies including ABC Inc with network infrastructure of note. ABC Inc. has its a logically segmented network that divides administrative and financial network from the engineering and manufacturing segment. This divide helped contain the spread of the Ryuk ransomware inside ABC Inc. and also from spreading to our 2 partners, 123 Co. and XYZ Corp. 123 Company provides us bobbles for our flux capacitors and our work at the IT team has been on streamlining ordering and inventory information networks into ABC Inc. 123 Co.'s network is divided into manufacturing and administrative and has a small team of 4 who divide the responsibilities of manufacturing operations, security, and employee help desk support. XYZ Corp is the partner who provides us the Kryptonite liners needed for our warp engines, used on our Unobtanium skirt couplings. The network structure of XYZ Corp. is their administrative, financial, and manufacturing are all on an unsegmented network and hosted with one online server hosting service. As our newest acquisition we are still on boarding XYZ Corp. but have integrated inventory and invoices. The strength of not fully integrating our partners was compartmentalization of the spread of Ryuk and Zloader. The weakness is the need for more IT support staff and solutions that are not optimized for our use cases.

Consequences

ABC Inc. as a result of the ransomware attack has experienced effects in multiple ways. Professionally ABC Inc.'s reputation in the marketplace has suffered, as we are no longer seen with the professionalism and excellence by customers that we previously had. This has reflected in our stock price dropping 8% after the announcement of our systems being attacked. We are hopeful investors and consumers will give us a chance to demonstrate the commitment to change and continue our relationships with them.

In the regulatory sphere the Federal Bureau of Investigations (FBI) CyberDivision is investigating our networks for a full case study, and to ensure we were in compliance with all regulatory standards before the attack. Our Computer Security Incident Response Team (CSIRT) is also being audited by myself and the Chief Information Officer to ensure we were maintaining our own ISO standard commitments.

Operationally we were closed for business effectively for 3 weeks. This means we could not accept orders, coordinate internally, process payments or fulfill and ship existing orders. We estimate the downtime cost approximately $4.6 million USD in lost productive capacity. Additionally there will be operational cost to update computer systems with new hardware, create new user accounts with secure passwords, and retrain all employees on safe and secure computer usage.

Vulnerability assessment

A vulnerability assessment was performed on ABC's network for the purpose of finding any weaknesses in our network structure or host configurations. We used a network mapping tools called nmap and Nessus to see all our hosts and connections and what type of information was being sent through our network. We also inventoried all of the computer and networking assets we have. We found 287 hosts, 14 routers/access points, 16 firewalls, and 3 servers off site. All hosts were up to date on their software and operating systems were scanned for unauthorized processes or configurations that were unsafe. Our routers/access points were found to be running an older firmware and were updated as well as configured to allow the use of IPV6 IP protocols, future proofing ourselves for when the majority of the internet changes over. Our 3 offsite servers were assessed and found to be up to date and secure as well.

Threat Matrix

Priority **9 High** **1 Low** **0 Unrelated**	**Vulnerability**	Firewall	Data transmission	Physical security	Password strength	Application architecture	Databases	Power loss
Threats	**Priority**	9	4	6	7	6	3	1
Intrusion	9	7	2	6	6	1	2	1
Server Failure	4	9	6	6	5	9	5	5
Extortion	2	3	9	2	4	5	2	7
Human Error	9	2	9	5	3	1	5	3
Malicious Code	9	5	1	1	3	7	2	1
Denial Of Service	2	9	4	3	5	3	7	3
Physical Damage	2	1	3	4	1	4	6	5

As you can see above we believe our biggest threats are still intrusions getting past our firewalls, and human error.

Recommendations Communication Plan

The recommended changes we are proposing are to limit the ability of outside data to be sent to our personal email networks. Any email coming from outside our organization should be scanned for any type of malicious file before being sent to the user. All users should have limited authority in our network and be prevented from installing any type of executable file. All firewalls should be configured to black probing attacks and to block unusual or suspicious activity using an Intrusion Prevention Tool to compare normal traffic to suspicious traffic.

Future Response Plan

To prevent this situation from happening in the future we will be creating new rules to govern our networks and employee behavior. The CSIRT will be responsible for developing and implementing our new documentation detailing our plans going forward. A new employee handbook will be created taking the lessons of this incident and new employee education tools and practice devices will be fielded. The new response plan will guidance for how to respond to incidents quickly and with an understanding of all responsibilities and stakeholders roles involved. CSIRT will also be empowered to gain access to networks and react quickly to threats. Employees will receive new training on appropriate user behaviors. And our IT team will create new rules in our Intrusions Detection Software and Firewalls that will prevent the reception of suspicious emails, the execution of code from Microsoft Excel, and will block all software known to be malware. Additionally we will be making sure our software is updated and our data backed up more often to ensure more resiliency and faster restoration times.

We recommend ABC Inc. learn from the situation, cooperate with any law enforcement, and empower the CSIRT, IT and stakeholders to bolster security and spend the financial resources preventing future incidents.