Reconnaissance Report: Trillium Technologies Inc.

Executive Summary

Identify a potential target by searching a job posting with basic names of technologies in Indeed.com

* Name of a known technology (NAT-Network Address Translation)
* Analyze vulnerabilities and extend search based on names technologies found in job postings such as Infoblox NetMRI, and Cisco Prime Infrastructure
* Compile other type of information and reconnaissance to prepare a possible attack on the company or to target some of the company’s employees.
* Describe all steps taken to develop a plan and propose some solutions to avoid a breach or a cyber-attack on the identified or potential victim.

Scope

In Indeed.com I was able to search for jobs related to the network address translation (NAT) in the Philadelphia region and a few results came up.

A Network Operations Engineer is needed in Horsham PA for company Trillium Solutions Group Inc. primarily to serve as an Architect to support various infrastructure projects. Some of the tools and applications needed for this position are the operations and maintenance of Infoblox NetMRI, Orion Solarwinds, Cisco Prime Infrastructure, Solarwinds IPAM, Syslog and Netflow.

Based on the reconnaissance in the information I will propose a possible attack and provide information on tools used to discover any vulnerability in their systems. Also provide evidence that users are exposed to social media attacks due to the personal information posted and I will provide some solutions to mitigate a possible attack to this victim.

The possible attack

A basic Google search took me to two different sites where I was able to find current network vulnerabilities on two of the tools and application mentioned in the job search.

Infoblox NetMRI and Network Automation are vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input by the login.tdf script. This details also describes how a remote attacker could exploit this vulnerability using the multiple parameters to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information, to ultimately gain access (Exchange, 2016).

The Cisco Prime Infrastructure is a vulnerability in the web interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack.

This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. An exploit could allow the attacker to conduct clickjacking or other client-side browser attacks.

As of today, there is no released software updated that address this vulnerability or workarounds that address this issue (Cisco.com, 2016).

So my first outbreak will begin by searching any online information on Trillium Technologies Inc. and some of their employees.

Trillium Solutions Group, Inc. is a professional services firm based in Chicago, and provides technology consulting and strategic sourcing services for industries such as trade associations, financial services, telecommunications, and healthcare.

The Indeed.com job ad was posted by Ms. Niki Price, at 1954 First Street, Suite 20 Highland Park, IL 60035

Price has a professional Linkedin.com page as a personal Facebook account listing some of her personal hobbies, to which we discovered that she is a golfer and she likes to exercise.

A potential social engineer attack on Price would be to send her a malicious USB drive infected with malware or spyware under a golf brand that she can relate to. This could potentially help an attacker to gain access to her personal or work computer, and eventually escalate the attack based on access permitted.

I also performed a domain name search to find out all details needed for a remote network attack on the company’s network. Things like registration expiration date, registrant’s name, and company’s address, as the technical email address and servers names within their network. Then I did an nmap scan to find open ports in their network with very revealing results.

When trying to expand my social engineering plan to see if there was a better target than Price, I came across Steve Adelstein, and Donna Lenczycki President and vice President of Trillium Solutions Group. On Facebook.com I was able to find some personal information about Lenczycki alone with some of her family members for another potential phishing attack to gain access to personal information assets of her and her organization.

Mitigation and recommendations

For professional interest to the company, employees should protect their identities in social media and public accessed websites with pseudonymous names to protect their identities, reduce or avoid exposure to unauthorized users to anticipate unwanted access and authentication in their system, increase perimeter defense in servers and other network devises, and efficiently update systems and patches needed for software and hardware to protect customers, and vendors personal identifiable information.

References

Cisco.com. (2016, 09 20). *tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-cpi*. Retrieved from https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-cpi:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-cpiExchange, I. X.-F. (2016, 09 21). *exchange.xforce.ibmcloud.com/vulnerabilities/116641*. Retrieved from https://exchange.xforce.ibmcloud.com/vulnerabilities/116641:

https://exchange.xforce.ibmcloud.com/vulnerabilities/116641Facebook.com. (2016, 09 21). *https://www.facebook.com/niki.price1*. Retrieved from Facebook.com:

https://www.facebook.com/niki.price1https://www.linkedin.com/in/priceniki?authType=NAME\_SEARCH&authToken=I7Lu&locale=en\_US&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2CclickedEntityId%3A11767866%2CauthType%3ANAME\_SEARCH%2Cidx%3A1-1-1%2CtarId%3A1474827191127%2Ctas%3Anikki%20price%20trilliu. (2016, 09 21). *Linkedin.com*. Retrieved from Nikki Price:

https://www.linkedin.com/in/priceniki?authType=NAME\_SEARCH&authToken=I7Lu&locale=en\_US&trk=tyah&trkInfo=clickedVertical%3Amynetwork%2CclickedEntityId%3A11767866%2CauthType%3ANAME\_SEARCH%2Cidx%3A1-1-1%2CtarId%3A1474827191127%2Ctas%3Anikki%20price%20trilliu