hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

VOL.16, NO. 12

BRUTE FORCING AND SUPPLY CHAIN ATTACKS

Build your own Brute Force Tool

Dictionary Attacks and Machine Learning

From Brute Force to Side Channel & Fault Injection

Securing the Supply Chain

AND MORE...

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Managing Editor

Magdalena Jarzębska
magdalena.jarzebska@hakin9.org

Editors:

Marta Sienicka
sienicka.marta@hakin9.com

Marta Strzelec
marta.strzelec@eforensicsmag.com

Bartek Adach
bartek.adach@pentestmag.com

Michalina Szpyrka
michalina.szpyrka@eforensicsmag.com

Proofreader:
Lee McKenzie

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP
Magdalena Jarzębska
magdalena.jarzebska@hakin9.org

Cover Design
Hiep Nguyen Duc
Joanna Kretowicz

Publisher
Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631

www.hakin9.org

BETATESTERS & PROOFREADERS

Lee McKenzie

Hammad Arshed

Avi Benchimol

Amit Chugh

Craig Thornton

Paul Mellen

Alexandre D'Hondt

Olivier Caleff

Gilles Lami

Daniel Sligar

Dinesh

Kashif Aftab

Jeff Smith

Gregory Chrysantou

Paul Oyola

Nasreddine Bencherchali

Da Co

Ricardo Puga

Jeff Barron

Daniel Dieterle

Tahir Saleem

Tom Updegrove

Michal Jachim

Dear readers,

Our November edition is finally here and it's entirely dedicated to brute forcing and supply chain attacks. We prepared a handful of articles, tutorials, and case studies, and we hope it will be a great read for you! Let's take a look at what's inside.

First things first, we have a tutorial about BruteX - a great, but not so popular tool for brute forcing. The author will guide you through the installation and performing an attack simulation. BruteX is an interesting tool that can expand your virtual toolbox.

Next, Daniel Garcia Baameiro will teach you how to build your own brute force tool in Bash. How cool is that? In the next article, you will learn about performing brute force attacks with Hydra - we recommend this article for beginners, as it is a great introduction to usage of this tool.

In the following articles you'll get a chance to read about some very useful techniques, i.e. configuring OSSEC to mitigate brute force attacks, or about dictionary attacks and machine learning. We also talk about side-channel attacks and fault injection.

Don't think we forgot about the supply chain part! If you'd like to read more about this topic, we have three great articles for you. You'll learn about the nature of supply chain attacks, how they are performed, and how to defend against them. Also, you'll read about supply chain exploitation with the usage of password spraying attacks.

Last but not least, if you still haven't had enough of Wi-Fi hacking, you'll learn about how the pattern of creating wireless network access passwords makes it easier for hackers to crack the password.

We hope that you will enjoy this edition and find something that will catch your interest. As always, we would like to send our gratitude to all our contributors, reviewers, and proofreaders.

We would also like to thank you for supporting us and being a part of this magazine! Stay safe during these weird times and enjoy the upcoming holidays with your loved ones. And most importantly - have fun hacking! :)

Enjoy the reading!

Magdalena Jarzębska and Hakin9 Editorial Team

Contents

SECURING THE SUPPLY CHAIN

SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering, and Cyber Security teams.

“Software is eating the world" – Marc Andressen

Introduction

At no time since the dawn of the Industrial Revolution have manufacturing businesses thrived on the diversification and choice of vendors, the globalization of suppliers and manpower services, and the accelerated growth of the customer base due to improved infrastructure, shipping routes, and the internet.

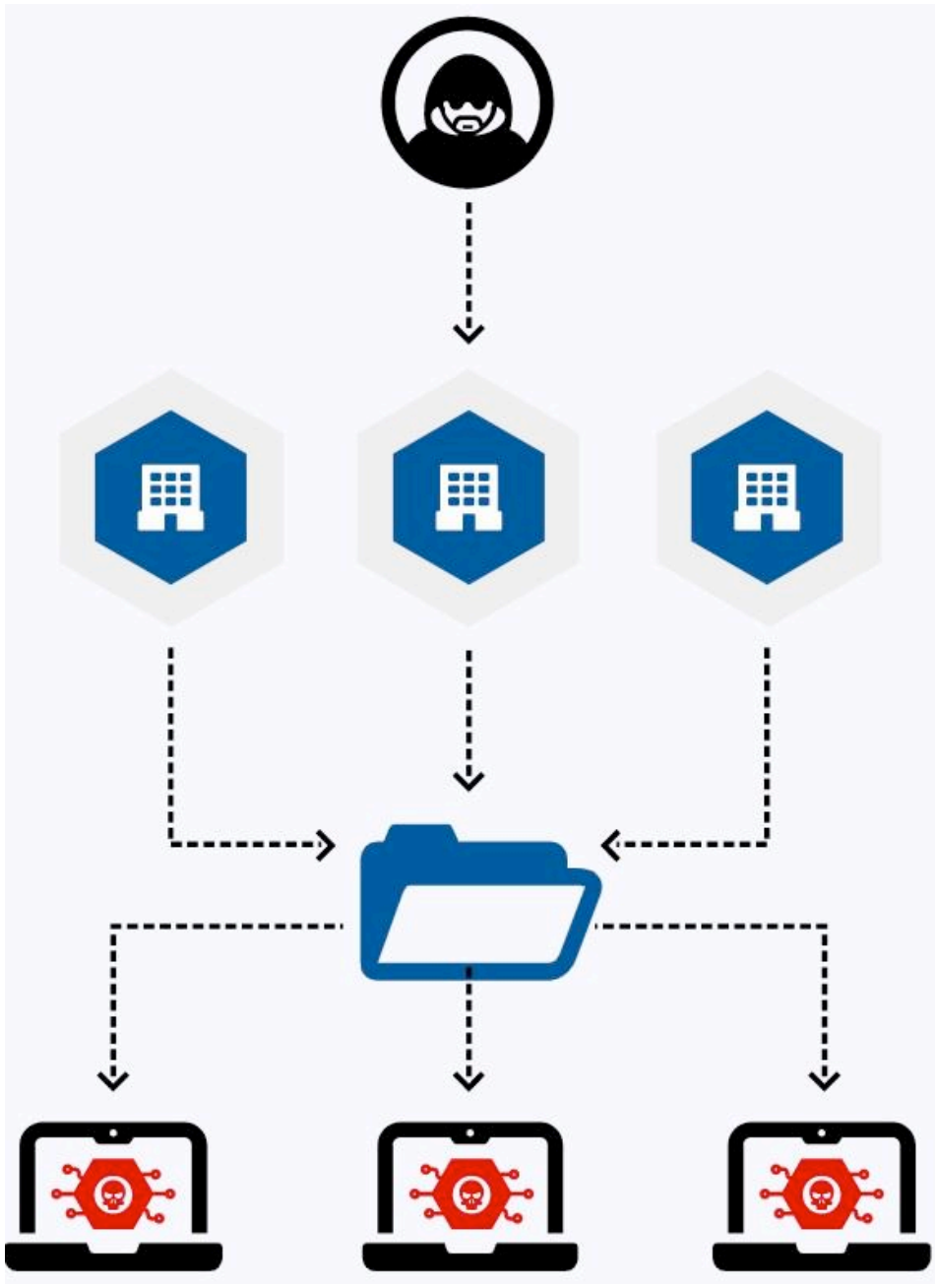
However, as software has brought immense accessibility and reach to billions of customers, it has also become an Achilles heel when used in concert with bad actors to disrupt, destroy and debilitate otherwise healthy and profitable organizations.

Definition

As defined by Wikipedia *"A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain. A supply chain attack can occur in any industry, from the financial sector, oil industry, to a government sector.”*. Although there are many ways to define and explain this term, the key takeaway from this definition is the “*less-secure*” element that is a constant in all forms of cyber security defense conversations.

Background

The “*modus operandi*” of a supply chain attack centers around an individual or team of bad actors targeting an organization not directly (as that would be too obvious) but rather through an external trusted partner or supplier who may have some manner of access to the organization’s systems. This new route for hackers has grown within the last few years and has transformed the attack surfaces significantly from not just the target organization itself but now across all companies, suppliers, and service providers that have any manner of touchpoints within the organization.



Courtesy keepersecurity.com

This now presents a clear and present danger to organizations as sensitive data inside the organization that is accessible by trusted partners outside the organization can now become the source of a data breach or worse still a malware injection. This danger can be compounded if the target organization is a “supplier-of-suppliers” who happen to house sensitive information about other suppliers on their systems. Like almost everything in the internet age, the danger growth curve is exponential in nature.

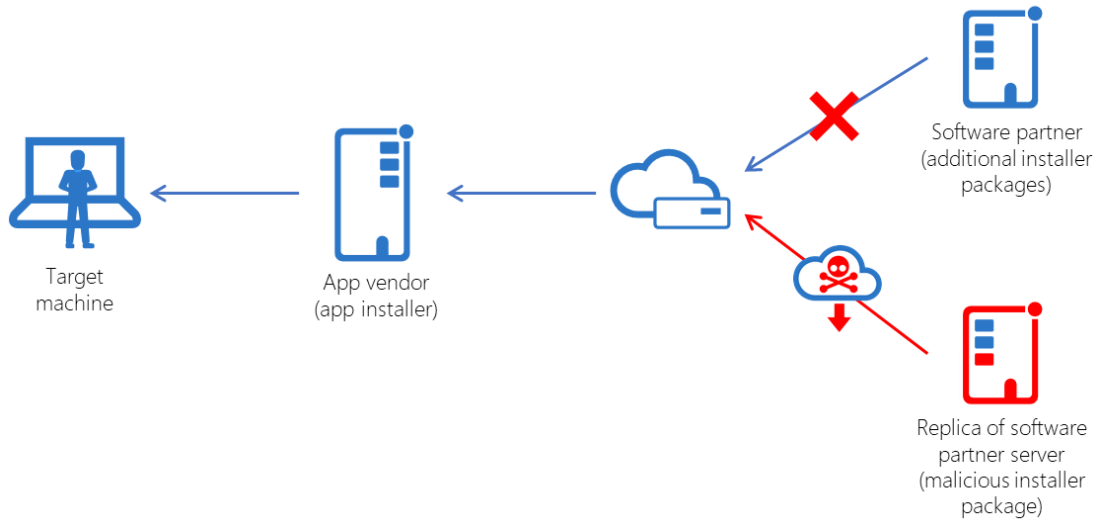
Preventing Cyber Attacks

Besides the basic rule of thumb to always work to reduce the attack surface of an organization, a number of steps can be taken both by manufacturers and suppliers to prevent attacks and harden system integrity.

- **Supplier Security Standards and Policy**: Manufacturers should hold suppliers in their supply chain accountable by issuing necessary Cyber Security Standard documents or policies that they must abide by to win business and orders from the manufacturer. Larger industry vendors may already be following this regime with their customers, so it’s only a mat-

ter of validating compliance for them, but smaller vendors will be challenged in this area due to increased staffing costs and skills needed to comply.

- **Software Development Life Cycle Hardening**: Suppliers should implement improved controls on their code delivery platforms that aggregate, compile, build and distribute software to prevent malware injection and root-kit infusion into the customer deliverable. The recent Solar Winds debacle is just one of the most notable instances of an upgrade installer being compromised and affecting hundreds of customers. Ironically, one of the highest-profile companies compromised in that attack was FireEye, a notable cybersecurity provider itself. Other firms, like MalwareBytes, were also targeted together with behemoths like Microsoft.



Courtesy securityaffairs.co

- **Secure Access and Privileges**: Organizations should ensure that Suppliers' Access and Privileges are regularly reviewed and strengthened as part of the Annual Risk Assessment Cycle. Too often, organizations are engrossed in their perimeter defenses looking both inwards and outwards without realizing that their most potent adversary may be using the front door to enter their compound.

- **Industry Security Certification**: Manufacturers may demand that their suppliers work towards implementing a recognized industry supply chain security certification standard such as ISO 28000. This may not be reasonable for smaller outfits but the largest suppliers will have no trouble implementing the necessary framework and obtaining the associated certification. Attackers will frequently seek out some of the smaller suppliers knowing full well that they may not have the finances or expertise in-house to implement sophisticated controls necessary to thwart their intrusion.

- **Zero Trust Architecture (ZTA)**: When dealing with vendors' interactions, their customers should be prepared to adopt a Zero Trust Architecture (ZTA) approach. All network activity with the vendor must be considered malicious by default. Only after each connection request passes a strict list of policies is it permitted to access the sensitive and intellectual property within the customer systems.

- **Cyber Security Awareness Program**: Manufacturers may require their suppliers to institute a meaningful Cyber Security Awareness Program in-house to educate their staff and all data-facing team members of the dangers of malicious attacks and methods of recognizing a threat vector. Even the most administrative of roles such as accounting, payroll, and

HR would have access to some of the most sensitive data yet are oblivious of the simplest of measures required to improve their security posture whilst being targeted continually by phishing emails. Awareness programs should not be treated as a panacea but rather another complementary tool in the armor to improve defenses, as too often humans present the most vulnerable of interfaces for hackers.

- **Open Source Software & Platforms**: Vendors should regularly review the usage and suitability of Open Source software to ensure that the tools they take for granted have not been compromised and are contributing to disseminating malware to their customers. Software build tools require particular attention here as they are the ones responsible for packaging the final executable for distribution that ships to the customer at large. In fact, according to Sonatype's 2020 State of the Software Supply Chain Report, 90 % of all apps use open-source code, and 11 % of them have known vulnerabilities.

- **Independent 3rd party Risk Assessments**: Although we all try to abide by an honor system in our daily lives and business transactions, this may not be the same when working with vendors. Rather than leaving this to chance, manufacturers are encouraged to require vendors to allow access to Third Party Risk Assessments that generate reports to be returned to the manufacturer to validate their trust. Vendors will rarely do this voluntarily so it's up to their customers to insist on these checks and balances being in place. Such third-party risk assessments will demonstrate clearly to customers the security posture of vendors and if they need to improve their position further or risk losing business because of it.

- **Reduce Outsourcing**: The globalization of manufacturing and services during the last three decades has led to a web of interdependencies that has been brought into sharp contrast due to the COVID-19 pandemic and its associated restrictions. This has expanded the attack surface greatly, allowing hackers to focus on low-hanging fruit, such as poorly prepared and defended downstream supply chain vendors, thereby getting backdoor access to some of the largest corporations and their systems through the supplied products. Compromised electronics and semiconductors products used within the US military, government, and vital civilian platforms provide foreign adversaries with possible backdoors to attack these systems at will. This is especially concerning in the energy and power distribution industry with many IoT devices being supplied from abroad.

This list is by no means final or conclusive of all opportunities for improving the supply chain conundrum. At best, it provides some minimum guidelines on areas that need to be addressed to reduce the attack surface.

Conclusion

For businesses, both large and small, all the reasons above, and probably some not listed, demonstrate how the threat landscape has changed when building products and services are reliant on an advanced supply chain of trusted partners and 3rd party tools. The seaports in Los Angeles account for around 60% of all in-bound import merchandise and products arriving into the US. Yet they have been backed up for months with a whole armada of container ships waiting to dock and unload. The pandemic of 2019/2020/2021 has laid bare just how fragile our supply chain networks are with shortages predicted in the near and long term. Car dealerships are flush with pre-owned models while the latest models float aimlessly in the holds of ships anchored at the Pacific ports waiting their turn to unload. Manufacturers are unable to meet or ship orders due to

chip shortages that may not recede for months to come. The supply chain is the oxygen of the world economy and needs to be protected if industry and the whole economic system is to survive.

References:

1. Wikipedia Definition: https://en.wikipedia.org/wiki/Supply_chain_attack

2. 11 Ways to Prevent Supply Chain Attacks in 2021 (Highly Effective) https://www.upguard.com/blog/how-to-prevent-supply-chain-attacks

3. Hacker Lexicon: What Is a Supply Chain Attack? https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/

4. Sonatype 2020 State of the Software Supply Chain Report https://www.sonatype.com/resources/white-paper-state-of-the-software-supply-chain-2020