Spotlight Article
November 2022

European Repository of Cyber Incidents

Turning the tables on the attackers: how to hack the hackers' supply chains

Kerstin Zettl-Schabath

How supply-chains became increasingly digitalised

Today, supply chains are longer, more complicated, and more global than ever. As an ever-increasing spectrum of products, tools, and systems is becoming electronically interconnected, these often non-transparent and heavily-intertwined supply chains are increasingly subjected to various kinds of cyber attacks. Stuxnet is an earlier example of initial infiltration of third-party systems (the Siemens SIMATIC WinCC and PCS 7 control systems) with the goal of physically disrupting the actual target (the Iranian nuclear facility at Natanz) controlled by those systems. Last year's financially-motivated supply chain attack against the Kaseya software resulted in thousands of managed-service providers being infected with REvil ransomware. Existing power structures, normative frameworks, and the free flow of information come under pressure in times of crisis, such as the Corona pandemic, the war in Ukraine, or during physical blockades (e.g., Suez Canal, Port of Shanghai). Disruptive attacks against the information infrastructure of supply chains can then unfold critical effects not only for the original target and its branch but also for other interdependent sectors. In this article, I argue that this growing interdependency is no exclusive phenomenon for the targets of supply chain attacks. Instead, the increasing diversification of the cybercrime ecosystem offers multiple options for states and law enforcement agencies to disrupt its services.

This article starts by summarising the saliency of offline- and online-shaped supply chain attacks and current political and private-sector counter-initiatives. Subsequent sections focus on the division of labor logic of the cybercrime scene and what measures could be further used to exploit vulnerabilities on the part of criminals. The concluding section addresses the European Union's Network and Information Security 2 (NIS 2) regulation and how it approaches supply chain cybersecurity within the EU.

On July 8th, Juhan Lepassaar, Executive Director of the EU Agency for Cybersecurity (ENISA), stated that from 300 observed "cyber events" related to Russia's war in Ukraine, 100 of them were "spillover incidents" that affected not only the original target, but other countries as well. These intended and unintended (spillover) effects underline the often-diffuse cause-effect relations inherent to cyber attacks, not necessarily targeting the affected supply chain by intent.

The balance between off- and online-induced "real" supply chain attacks is increasingly tilting in favor of the latter, e.g., via 1) using software vendors or third parties and their widespread updates for the infiltration of a vast spectrum of targets, as it was the case for the Solarwinds campaign, 2) compromising legitimate websites through website builders used by targeted actors, 3) compromising third-party data stores, or 4) conducting watering-hole attacks (compromising a website used by targeted actors in order to distribute malware). This provides ample reason for a more robust interrogation of the safety of supply chains. Our EuRepoC database and its coding of "initial access" for cyber incidents reported since 2022, based on the MITRE ATT&CK framework, provides us with needed insights into potential patterns of supply chain-induced cyberattacks. This is because we also code information on the most frequently targeted sectors and countries, but also accompanying impact types, such as data theft or destruction.

One more recent example of the coding of "supply chain compromise" as the initial access vector is the hack against Viasat and its KA-SAT satellite internet. Taken together, cases such as Solarwinds and Viasat demonstrate the significant (intended) effects and the collateral damage those attacks compromising third-party software within the supply chain can cause. With their intended or unintended spillover effects, supply chain attacks can (potentially) change the risk assessments and strategies of various stakeholders, such as governments seeking to establish efficient cybersecurity legislation, e.g., common standards of soft- and hardware security for particularly critical sectors.

They also require interdisciplinarity to answer serious questions about legal principles, such as due diligence, or the geopolitically-influenced connotation of an incident as "malicious."

In the European Union, the Cyber Diplomacy Toolbox entails restrictive measures against "malicious" cyber incidents based on the EU`s Council Decision (CFSP) 2019/797. An interdisciplinary and data-based understanding of the expanding threat environment (as offered by the EuRepoC database) is vital in order to combine those measurements with the EU´s strengthened focus on the security of ICT supply chains under the guidance of the Czech Council Presidency which called for the creation of a "ICT supply chain toolbox."

New initiatives have been developed within the private sector to create a more systematic and aggregated information system for software security metadata. Google claims that its *Graph for Understanding Artifact Composition* (GUAC) offers a freely accessible graph database that can be queried for supply chain-related questions. Examples include the ability to identify risky dependencies or which part of an organisation's inventory is affected by a new vulnerability.

The "doubling down" on the effects of supply chains in both the public and private domains maximises the potential fall-outs of one single attack. Supply chain cyber attacks against vendors in the physical world are therefore a threat scenario with severe consequences. In May 2021, US President Biden specified with his Cyber Security Executive Order a set of basic security standards that software vendors must comply with. Among them are (among other things) measures such as strengthened vulnerability disclosure, data encryption, and the establishment of multi-factor, risk-based authentication. Regarding the physical sphere, however, a set of different challenges and obstacles to strengthened cybersecurity standards, especially among private vendors with industrial control systems, still loom large today. For complex industrial systems that often depend on long-expired software versions, operators traditionally strive for security regarding their Operational Technology (OT). Operational imperatives, such as easy functionality and economic profitability, can easily trump the high and fast-evolving standards of Information Technology (IT). However, a growing array of digital access points, such as those for remote access and maintenance, create the urgent need to integrate OT with IT in order to mitigate cyber threats that exploit the digital realm and affect the physical supply chain.

Hacking supply chains within the cybercrime economy: an attacker's Achilles' heel?

This risk-prone environment creates a multifold spectrum of vulnerabilities that cyber villains can use to infiltrate, manipulate, and even physically sabotage their victims' systems. Workarounds, such as using software from vendors and subcontractors in order to get access to an extensive range of primary or random targets, are just one of many examples (see NotPetya and Solarwinds as prominent cases). Moreover, cybercriminals further complicate the situation since their crime-as-a-service ecosystem is not purely economically-motivated or economically-oriented anymore. In general, cyber defence measures against the same attack type from different attackers will be basically the same in technical terms. However, attribution of the actual attackers, their resources, agency structures, motivations (and thus expectable next steps), and their potential principles is nevertheless crucial to maximise prevention and resilience efforts against these threats. Evaluating ransomware as a purely criminal activity, without a genuine interest in using the blocked or encrypted data for intelligence or geopolitical purposes on the attacker's side, is different from knowing that the criminal attackers are only the final element in a longer, ever-changing chain of command.

In this case, the original state client will get access to the obtained data and can use it now or in the future for sabotage, disinformation, or simply for espionage purposes. This access is essential for possible second-order effects of so-called "double extortion" ransomware attacks, where data is not only encrypted, but stolen and partially leaked if the victim refuses to pay the demanded ransom. It is crucial to understand the complexity and diversification of the parts involved in the "hacking supply chain," which targets all kinds of organisations through ransomware operations, for the advantage of cyber defense, which is undergoing a similar diversification.

Recent law enforcement activities, such as sinkholing malicious domains used for cyber attacks, are one example of how state authorities and technology companies authorised by court orders can disrupt the infrastructures of cyber attackers. Even if the shutdown of a botnet (e.g., Emotet) does not automatically hinder its reconstruction, the defenders can raise the stakes and costs for the attackers in what is often described as a "whack-a-mole game."

The "industrialisation of the cybercrime economy" opened new opportunities for actors willing to engage in or profit from criminal activity. They also do not have to develop the attack infrastructures themselves to conduct the attacks if they offer hacking-for-hire services to their customers (e.g., Ransomware-as-a-service, RaaS). At the same time, observers have criticised especially the US approach of court-authorised botnet takedowns by private companies and law enforcement agencies, often done via a public-private partnership. This criticism stems from their underestimated collateral damages to third parties and the lack of transparency and scrutiny concerning court decisions about highly technical questions of the impact, consequences, and actual benefits of different takedown requests. Furthermore, this approach would, at the same time, act as a short-term-oriented substitution for urgently needed long-term legislative approaches. This observation reflects how private actors and their actions can be used by governments unable or unwilling to take decisive actions against cyber threats. Defensive cyber-proxies, as has already been argued for the attribution process, could also gain more and more traction for the growing cyber insurance sector. This regulatory governance pattern, where governments tolerate or even initiate private actor self-help, was also discussed for so-called "cyber letters of marque" in order to manage hack-backs by private actors.

Strategies for supply chain guardians

Disrupting botnets as substantial parts of daily cybercrime infrastructure is one potential part of the solution. Different actors with different goals and motivations depend on botnets. The fight against cybercrime should therefore target infrastructures necessary for as many operations and which are used by as many actors as possible, so their unavailability cannot be easily compensated for by switching to other tools. Accordingly, the goal must be to create vulnerability, rather than short-term sensitivity, on the part of the criminals by scaling up disruptive effects on their business model. Thus, hitting access brokers may be more effective than going after botnet operators because the former are usually the first links in the ransomware chain, on which all other actors rely (at least if they are not capable or willing to create their own gateway into the target's network). Since access brokers primarily sell stolen credentials, which still rank among the most common initial access vectors for ransomware in 2022, their targeting could significantly disrupt the supply and demand balance within the cybercrime ecosystem.

Focusing on later parts of the ransomware chain would therefore not necessarily have the same impact on actors involved earlier in the process, such as access brokers who sell the access and immediately profit, compared to RaaS operators who receive only a portion of the final profit. Therefore, if an operation fails due to the disruption of an earlier part of the hacking supply chain, it does not just affect the cybercriminal at the very end of the chain. As a result, this would constitute some sort of "reverse engineering" of the supply chain hacking logic on the part of the defence.

One approach could also be to cripple crypto exchanges rather than widespread botnets; however, this could cause potential collateral damage. Overall, attackers must be forced into a situation where they "waste resources and lose control." Australia, for example, recently stepped up its approach against ransomware gangs and initiated a whole-of-government approach to combat cybercrime cases such as the Medibank hack. Additionally, the country introduced new legislation with significantly-increased financial penalties for data breaches, which should pressure companies to safeguard their systems more effectively.

Ultimately, technical-legal prevention and response options against the hacker supply chain should be developed and tested for their short- and long-term effects and should be risk-free for uninvolved parties. Despite numerous scientific studies on this subject, many countries, such as Germany, still lack sufficiently-defined concepts discussed in this context, such as hack-backs, offensive and defensive/active and passive cyber defence. They instead tend to define them ad hoc in terms of their use cases, demonstrated not least by the discussions in the run-up to the national cybersecurity agenda presented by the Federal Ministry of the Interior in July 2022.

Supply chain security within the EU: the NIS 2 directive

For the European Union, the NIS 2 directive sets ambitious goals for strengthening the cybersecurity of critical infrastructures, especially in terms of supply chains. Enhanced incident-reporting requirements, more comprehensive information-sharing on a national and supranational level, and regular evaluations of national cybersecurity strategies are subject to the regulation. Ideally, this could close existing legislative gaps regarding the practical and comprehensive networking of incident-reporting mechanisms, thus increasing supply chain security in cyberspace for the EU as a unified single economic market.

In the worst case, the directive would not be effectively and timely implemented by the EU member states, all of which have diverse political agendas and ambitions and which possess highly-varied national capacities to enforce such cybersecurity rules. Effective and efficient cooperation of (in some cases still to be established) national *Computer Security Incident Response Teams* (CSIRTs) under the guidance of a planned EU CSIRT network will be just one crucial step in making this a success story. An even more interconnected and timely information-sharing European Union could thus successively turn the supply chain logic against the attackers themselves, who also rely heavily on it.