STORMSHIELD

OPINION ARTICLE

ATTACKS AGAINST CYBERSECURITY PROVIDERS AND SOLUTIONS: EVIDENCE OF A TREND?

Stéphane Prevost
Product Marketing
Manager, Stormshield

The IT security of software providers is being severely tested, with a growing list of attacks against them.

Destabilising IT security companies and compromising their security solutions has been the latest trend in the malicious ecosystem for some time now – and this trend is becoming more apparent in 2021. So, is it fair to say that software providers are on the way to becoming prime targets for cyberattacks? Precisely because of their central role in companies' defense shields against cybersecurity attacks, **cyber criminals have a strong interest in weakening and compromising them**. Providers will therefore need to redouble their support efforts in terms of security.

WHY CYBER-CRIMINALS ARE TARGETING CYBERSECURITY PLAYERS…

In April 2021, the Codecov company – a specialist in code auditing – notices that access to its Bash Uploader script has been hacked by attackers, and modified several times to inject malware. This problem affects no fewer than 29,000 companies, customers and potentially all collateral victims of the attack – such as Rapid7, a cybersecurity provider whose source code has been exploited for malicious purposes. For many experts, this attack on Codecov is a rerun of the "SolarWinds" scenario, and one which could be repeated again. Because, as cyber criminals are all too aware: **there are many advantages to attacking a cybersecurity provider**.

In essence, a provider, whatever their field of activity, is perceived as a benchmark by companies, who may therefore consider them to be invulnerable and unassailable. This is a boon for cyber criminals, who consequently see the growing benefits of attacking providers and then hijacking their solutions to infect several client companies in turn.

Naturally, "*the consequences of an attack on a provider vary according to that provider's business activities*", explains **Adrien Brochot**, Product Manager for Endpoint Security at Stormshield. And such supply chain attacks can indeed take many forms and scenarios. In a first "basic" hacking scenario, cyber criminals seek to directly infiltrate new software update or delivery mechanisms, in order to then gain access to customer infrastructures. And in a second scenario, in which a provider of cyber Cloud solutions falls victim to a DDoS attack; user companies are denied access to their various provider-hosted services, leaving them unable to function properly. In a third scenario, an attack against an antivirus software provider could result in the hijacking of the target company's workstations, using the administrator rights which antivirus software often enjoys... such an attack would therefore weaken the infrastructure of client companies. The theoretical scenario of modifications to software updates has even been observed in real life with the example of the Click Studios company, which provides thousands of companies with the Passwordstate password manager, and, last April, was infected with malware during an update.

An attack against a provider can also involve targeting its source code, in order to steal sensitive customer data, to identify a zero-day flaw that could be exploited, or to collect information for the purposes of commercial or industrial espionage. This is a zero-day exploit approach that could affect any provider, yet it turns out to be even more critical when it comes to a cybersecurity provider. Cybercriminals are particularly drawn to the source code of cybersecurity providers, as seen in the intrusions into the networks of Microsoft, SonicWall and even Stormshield in late 2020. With regard to Stormshield, the impact of the attack was limited and no code modification was observed during the investigations carried out with France's ANSSI cybersecurity agency. Publishers' source code is seen as attractive, even though the libraries used and features offered often rely on open source. But that's not the end of the devious exploits of cyber criminals who successfully compromise providers. By also compromising their solutions – for example, by injecting a backdoor – they can target the solution's other client organisations, or even take the attack to a wider audience. With potentially dramatic consequences ..

... AND THEIR SOLUTIONS

For a cybersecurity solution to be effective, it must be judiciously located with reference to the customer infrastructure, ensuring it captures as much information as possible. Cybersecurity solutions are therefore designed to be deployed as close as possible to a company's most sensitive assets. **An attack on a cyber solution therefore affords the opportunity of direct access to a very large amount of information on the machines it protects**, and at a high privilege level, enabling the exploit to take control of it, neutralise it in order to break the security locks, and thus conceal malicious exploits within an information system. Cyber criminals can also hijack solutions by exploiting a known vulnerability in them, in cases where the relevant patch has not been applied by the companies that use it. Hence the vital need for administrators to carry out very regular updates to security solutions, and for providers of trackers to continuously correct *flaws in their products*. A known vulnerability in the Pulse Connect Secure VPN solution from the Pulse Secure provider has recently been exploited for malicious purposes.

In short, when it comes to attacking cybersecurity solutions, the gloves are off for cyber criminals, who will eagerly find their way through any doorway to propagate their attacks. And some of these doorways may even have been left ajar by the providers themselves...

HIDDEN ENTRANCES: THE ISSUE OF BACKDOORS

Let's turn our attention to "backdoors", secret entrances that can be found in a security product for several reasons, as explained by **Sebastien Viou**, Consultant Cyber-Evangelist at Stormshield: "*Solutions can include unintentional backdoors – used for the development of the product by the provider, which were overlooked when the product went into production – and intentional backdoors, which are knowingly left by a provider to enable them to perform work on a customer's system.*" A backdoor could, for example, be used for debugging access during the development of the solution, then be left in the production version by mistake. Conversely, an editor might choose to retain the option of performing work on a customer's installation in the event of a problem by retaining an undocumented backdoor. There are also the state-level backdoors imposed on providers by national governments and brought to light by the Edward Snowden affair in particular, and the listening and espionage practices of the NSA in 2013 – and these practices are now back in the spotlight with revelations regarding Operation Dunhammer. At the time of the Snowden affair, the case that generated a lot of noise on the subject of backdoors concerned the provider Juniper Networks, some of whose solutions contained backdoors installed by the NSA, allowing access to the data of the provider's customers.

> *"A backdoor is a vulnerability in a solution; it may be hidden, but it is a vulnerability nonetheless"*
>
> **Simon Dansette,** Product Manager Network Security Stormshield

In all cases, **whatever the reasons for the presence of a backdoor in a security product, it presents a risk when it falls into the hands of a bad actor**. "*A backdoor adds risk since it provides you with invisible access to a solution,*" explains **Simon Dansette**, Network Security Product Manager at Stormshield. *If an attacker realises that there is a backdoor in the solution, he can exploit it to hijack that solution for malicious purposes. In other words, a backdoor is a vulnerability in a solution; it may be hidden, but it is a vulnerability nonetheless*". As ANSSI pointed out in 2016 in a note written by Guillaume Poupard, a backdoor in an encryption system "*would have the disastrous effect of forcing the designers of security products and services to weaken cryptographic mechanisms*". Such a risk should obviously be avoided.

AWARENESS, SECURITY, TRUST: THE WEAPONS PROVIDERS NEED FOR MOUNTING A COUNTER-ATTACK

"*For several months, there has been a clear and well-established trend towards attacking cybersecurity vendors and their solutions. The question that must be asked now is: when will attacks of this type occur, and how can providers protect themselves from them?*", Viou warns. More than ever, providers need to be aware that they may be targeted by cyber criminals, and will have to adapt their defense strategies accordingly.

> *"The question that must be asked now is: when will attacks of this type occur, and how can providers protect themselves from them?"*
>
> **Sébastien Viou,** Consultant Cyber-Evangelist, Stormshield

Raising the awareness of individuals – whether they are employees of a provider or end customers who use the solution – is a critically important step. "*Some supply chain attacks target the end user*" Brochot points out. This means that providers must continue to recommend that their customers' IT security policies should be compliant with essential best practices, especially including always updating their solutions as soon as new patches have been published. This will help to avoid scenarios such as the one suffered by the Fortinet editor and its FortiOS solution -an example that clearly shows **the critical importance of cyber awareness**.

On the technical side, it is (vitally) important not to overlook the intrinsic safety of the product, with monitoring by the provider of the vulnerabilities of the integrated components, a hardening of the solution, or even respect for the principles of defensive programming… "*You have to follow certain general principles for securing products; for example, by adopting secure architectures that apply the principle of least privilege. The golden rule is to properly develop your solution so that it limits access to an attacker*," Brochot explains.

This approach also concerns client companies who can address the issue themselves by developing structured processes for reliably updating the products they use. Another approach would be to promote variety in the choice of security solutions (and thus avoid uniformity); firstly, this ensures better coverage of threats, and secondly, it limits the consequences if an individual provider is compromised. Customers must also make the critical choice of the "right" solution to be deployed on their systems. Such a choice can be problematic in practice, because it oscillates between two options: is a solution's robustness more important, or its catalogue of features?

ROBUSTNESS VS FEATURES: WHICH TO CHOOSE?

"*Digitisation means accelerated requirements in terms of features, speed, performance, etc. – and companies often tend to focus in the first instance on functional richness, believing robustness to be an automatic given in a solution,*" Dansette notes. Indeed, many companies have a fairly low awareness of the issue of product safety, and will naturally favour a device that offers a catalogue of features they don't really need. However, **first and foremost, a security product must continue to provide a security function**: it must precisely fulfil the purpose it was designed for. Moreover, such functional richness actually introduces additional complexity… and more complexity means more risks of weaknesses, and therefore a larger attack surface. Brochot believes it is necessary to "*choose a solution that meets the challenges the company has set for itself, and is robust*," and that "*You need to find the right balance between robustness and features, but robustness must always be the No.1 priority*".

This involves a whole range of techniques and processes that providers must incorporate in full to ensure the integrity of their products. At the same time, it also involves an entire chain of trust to be established with the users of these products.

THE IMPORTANCE OF HAVING A CHAIN OF TRUST

How can you still trust a provider or a solution, at a time when computer attacks targeting them are becoming legion? It's a legitimate question that businesses are asking themselves, and to which providers can offer tangible answers. Because although it is impossible to guarantee a flawless security product, there are several ways of challenging providers on their security and their products.

First there is the impartial third party, a **strong link in the chain of trust**. "*The use of a trusted third party is essential for a provider. This enables us to take a look from the outside and gain a general overview of the product and its code. The fact that this is* *carried out by an impartial third party provides an additional guarantee of serious intent*", explains Simon Dansette. It is therefore in the interest of providers to have their products audited by third-party companies: code reviews, pentests and bug bounties are all valid ways of detecting potential flaws and testing a solution.

It is also important to **offer solutions that have been qualified by European standards organisations**; e.g. ANSSI for France, BSI for Germany and CCN for Spain. These qualifications provide a guarantee that the security product in question, approved (for example) by ANSSI, first and foremost meets the needs of end customers: it is a clear indicator of trust. In addition, these qualifications are often based on an assessment of the development environment, in addition to product robustness tests. Finally, provider transparency on the security vulnerabilities found in its products is crucial, as is listening and taking into account customer feedback; these things are vitally important when optimising a solution, along with the regular supply of product fixes.

Despite the growing trend of threats, providers – using the educational and technical means and expertise at their disposal – still have plenty of cards to play.

Version 1.1 - Copyright Stormshield 2022