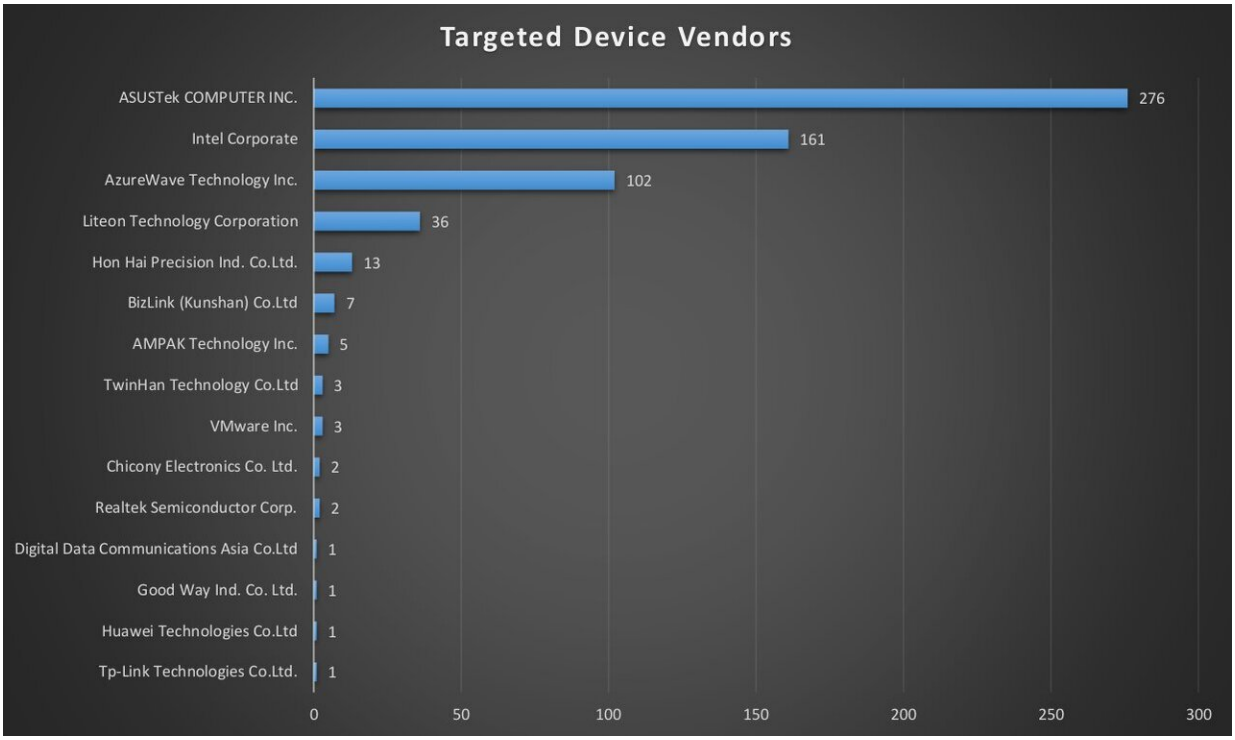
Supply-chain hack attacks are worrying investigators

May 5 2019, by Nancy Cohen



Credit: Securelist

What do you know about supply-chain attacks? In January, an article in *CSO* said it's when a weak link in your enterprise security might lie with partners and suppliers. It's when someone infiltrates your system through an outside partner or provider with access to your systems and data.

In the past few years, said Maria Korolov in *CSO*, more suppliers and service providers were touching sensitive data than ever before.

Unfortunately, the supply-chain attack in recent times is far more than a park-and-save definition; it's a top of mind headline maker, as a hacking group is meddling with software updates through malware. *Wired* on Friday called it a supply chain hijacking spree.

In this instance, Microsoft's site carried a definition that hits home with the current spree.

"Supply chain attacks are an emerging kind of threat that target software developers and suppliers. The goal is to access source codes, build processes, or update mechanisms by infecting legitimate apps to distribute malware. Attackers hunt for unsecure network protocols, unprotected server infrastructures, and unsafe coding practices. They break in, change source codes, and hide malware in build and update processes."

The apps and updates are signed and certified; vendors are likely unaware that their apps or updates are infected with malicious code when released. The malicious code runs with the same trust and permissions as the app.

Paul Lilly in *PC Gamer* described the hair-pulling of it all—a hacking group "actively mucking with trusted downloads, and nobody can seem to figure out the group's exact identity." Note the word trusted—no downloads are safe.

While identity remains to be discovered, names are being given to it, including ShadowHammer and Wicked Panda.

There were indications that (1) the group is bent on spying, and (2) its

targeting suggests it's not a profit-focused cybercriminal operation. "Yet by all appearances, the group is casting its vast net to spy on only a tiny fraction of the computers it compromises."

The discomforting aspect of all this might be courses of action, such as avoiding software updates yet ignoring updates would seem to be risky too.

As for Kaspersky Lab, they had this to say: software vendors should introduce "another line in their software building conveyor that additionally checks their software for potential malware injections even after the code is digitally signed."

Fahmida Rashid in *IEEE Spectrum* said the operation was especially insidious in that it had sabotaged developer tools, "an approach that could spread malware much faster and more discreetly than conventional methods."

Indeed, Andy Greenberg in *Wired* raised the implications. By breaking into a developer's network and hiding malicious code in apps and trusted software updates, hijackers can smuggle malware onto "hundreds of thousands—or millions—of computers in a single operation, without the slightest sign of foul play."

As tech news sites provided details on the supply chain attack, an often cited information source was Kaspersky Lab—for good reason. Kaspersky has been eyeing this for some time. They were the ones who gave it the name, ShadowHammer.

"At the end of January 2019, Kaspersky Lab researchers discovered what appeared to be a new attack on a large manufacturer in Asia... Some of the executable files, which were downloaded from the official domain of a reputable and trusted large manufacturer, contained

apparent malware features. Careful analysis confirmed that the binary had been tampered with by malicious attackers...We quickly realized that we were dealing with a case of a compromised digital signature."

The Kaspersky article discussed digital signatures.

"A lot of computer security software deployed today relies on integrity control of trusted executables. Digital signature verification is one such method. In this attack, the attackers managed to get their code signed with a certificate of a big vendor. How was that possible? We do not have definitive answers."

They noticed that all backdoored ASUS binaries were signed with two different certificates. "The same two certificates have been used in the past to sign at least 3000 legitimate ASUS files (i.e. ASUS GPU Tweak, ASUS PC Link and others), which makes it very hard to revoke these certificates."

As important, it looks like Asus wasted no time in addressing the attack.

"We appreciate a quick response from our ASUS colleagues just days before one of the largest holidays in Asia (Lunar New Year). This helped us to confirm that the attack was in a deactivated stage and there was no immediate risk to new infections and gave us more time to collect further artefacts. However, all compromised ASUS binaries had to be properly flagged as containing malware and removed from Kaspersky Lab users' computers."

The malware problem is seen elsewhere. "In our search for similar malware, we came across other digitally signed binaries from three other vendors in Asia." A figure caption in *Wired* said that a "single group of hackers appears responsible for supply chain hacks of CCleaner, Asus, and more, planting backdoors on millions of machines."

More information: securelist.com/operation-shado … -chain-attack/90380/