APT Groups Moving Down the Supply Chain

duo.com/decipher/apt-groups-moving-down-the-supply-chain

In August 2018, attackers broke into the network of Visma, a major managed services provider in Norway that does more than $1 billion in business each year. Using stolen Citrix credentials, the intruders made their way into the company's network, then installed a custom remote-access tool on an Active Directory controller and began moving around the network. Eventually, the attackers harvested employee usernames and password hashes, packaged them up, and exfiltrated the data to a Dropbox account.

The attack was part of a recent string of operations that some researchers say is the work of APT10, a group associated with the Chinese Ministry of State Security. APT10 has been operating for many years and has drawn the attention of law enforcement and intelligence agencies, including the Department of Justice, which indicted two Chinese citizens it says are members of APT10. That group has been blamed for intrusions at a broad range of organizations, including other managed services providers (MSP), in dozens of countries around the world. Researchers consider APT10 one of the more capable and dangerous cyberespionage groups operating at the moment, and the intrusion at Visma fits the group's pattern of targeting MSPs as a stepping stone to going after customers or other suppliers.

That strategy and targeting philosophy is one that more attack groups are adopting as primary targets such as defense contractors, technology vendors, and financial companies become more mature in their security programs and resilient to attack.

“We’ve seen a few groups do this, including several Chinese groups and some Russian groups, too. I think there’s two reasons for it. One is that it’s a more efficient and effective way of conducting operations. If you target an MSP or a cloud provider, you become part of this infrastructure that companies have already invested in and trust,” said Priscilla Moriuchi, director of strategic threat development at Recorded Future, a threat intelligence firm that helped Visma investigate the Visma intrusion.

“It’s an effective way of doing targeting. Groups are increasingly targeting the global supply chains and third parties because when you get in there, you have access to other targets.”

Although Recorded Future attributes the Visma intrusion to APT10, other researchers say it may be the work of a separate group in China known as APT31, or Zirconium. Benjamin Koehl of Microsoft's Threat Intelligence Center said on Twitter that the C2 infrastructure bore the hallmarks of APT31.

"This activity is not APT10. It is all APT31 (or ZIRCONIUM) in our terms. The C2 domains that you mention were all registered and the threat actors made subsequent changes in specific ways that we attribute (with other information) to ZIRCONIUM," he said.

Moriuchi said that APT10 and APT31 are both tied to the Chinese government and they share a number of attributes, tactics, and techniques.

"It’s our belief that regardless of attribution delineation between APT10 and APT31 in this case, the need for defenders to take action does not change, nor do our recommendations," she said.

We believe that APT10 and APT31 are closely linked and that Chinese state-sponsored actors are associated with both groups. Today, there is little information publicly available on APT31 and none that meaningfully separates it from the behavior or motivations of APT10; APT31 tactics, techniques, malware, victims, perpetrators, and more are largely unknown. We are now actively working to unearth everything we can on APT31 and have learned that both APT10 and APT31 may share very similar techniques, malware, and are likely attributed to the same Chinese state organization.

The August 2018 attack was a painful compromise, especially for a provider such as Visma, whose business depends on customer trust. But rather than quickly contain it and kick the dust under the rug, Visma officials decided to use the incident to show other organizations that could be targets exactly what happened and what to look for. This is rare for a number of reasons, mainly because of the embarrassment of the compromise and the potential effect it could have on the company’s business. But Moriuchi said there’s quite a bit of value in exposing the details of an operation like this.

“Visma is taking a stance to confront the attackers and say they’re not afraid,” she said. “We really see that there’s deterrent value in this.”

The operation against Visma followed a familiar pattern and used tools that researchers had previously seen, including the Trochilus RAT. The team also employed an interesting technique in which operators rename a legitimate binary and then sideload a malicious Windows DLL onto the compromised machine. That DLL then decrypts some shellcode and injects the Trochilus RAT into memory.

“After almost two weeks, on August 30, 2018, APT10 attackers used their access to the network to move laterally and made their first deployment of an RC4- and Salsa20-encrypted variant of the Trochilus malware using a previously associated DLL sideloading technique. Two separate infection chains leveraging this specific DLL sideloading technique were identified on the Visma network using legitimate known good binaries that had DLL search-order path issues. This means that APT10 actors had two separate access points into the Visma network,” the Recorded Future analysis of the intrusion says.

That’s a slick technique, but it’s important to note that what enabled the attackers to get to that point was stolen credentials. Sure, state-sponsored attack teams have custom malware, private C2 infrastructure, and in many cases political cover, but even with all of that, they still need a way in to a target network, and nothing suits that purpose like stolen credentials. Pilfered usernames and passwords have the advantage of giving the attackers a simple way in, and also let them avoid many network defenses. At least initially.

> "Groups are increasingly targeting the global supply chains and third parties because when you get in there, you have access to other targets.”

One of the things the Recorded Future researchers noticed is that the attackers authenticated to the Visma network outside of the typical working hours for employees. That’s a classic red flag, and Moriuchi said it’s a good reminder that these attackers are humans, not bots.

“We miss the human element when we talk about this. There are people behind these computers. They have lives and families and vacations. They make mistakes,” she said. “The hours of operation are important.”

The human part of these operations also affects the targeting. APT teams generally are not independent units making their own choices and selecting targets as they see fit. They have bosses like anyone else and get orders that they’re bound to carry out.

“The reality is, for nation state groups, they’re part of the military or an intelligence agency and are fulfilling the requirements of their bosses. You don’t just have one job. You’re seeking multiple targets and multiple sources of information,” Moriuchi said.

Which explains why the attackers also targeted a law firm in the United States and an international clothing company, intrusions that both involved the use of stolen Citrix credentials. The law firm handles intellectual property cases, which makes it a likely target for a cyberespionage team, but the apparel company is a less-obvious target at first blush.

But Moriuchi stressed that APT groups continuously learn from previous operations and adjust their tools, tactics, and targeting as they progress. With primary targets becoming more wary, moving down the supply chain becomes a more and more attractive option.

“It’s an interesting problem. We’ve seen that methodology migrate from the government and defense area as the ultimate target has become more difficult to get to and vendors and suppliers are targeted more often. We see this as behavior that will increase in the coming years,” Moriuchi said.

“The Ministry of State Security and APT3 have performed attacks against MSPs and vendors and they understand the vulnerability of the global supply chain.”

Apt