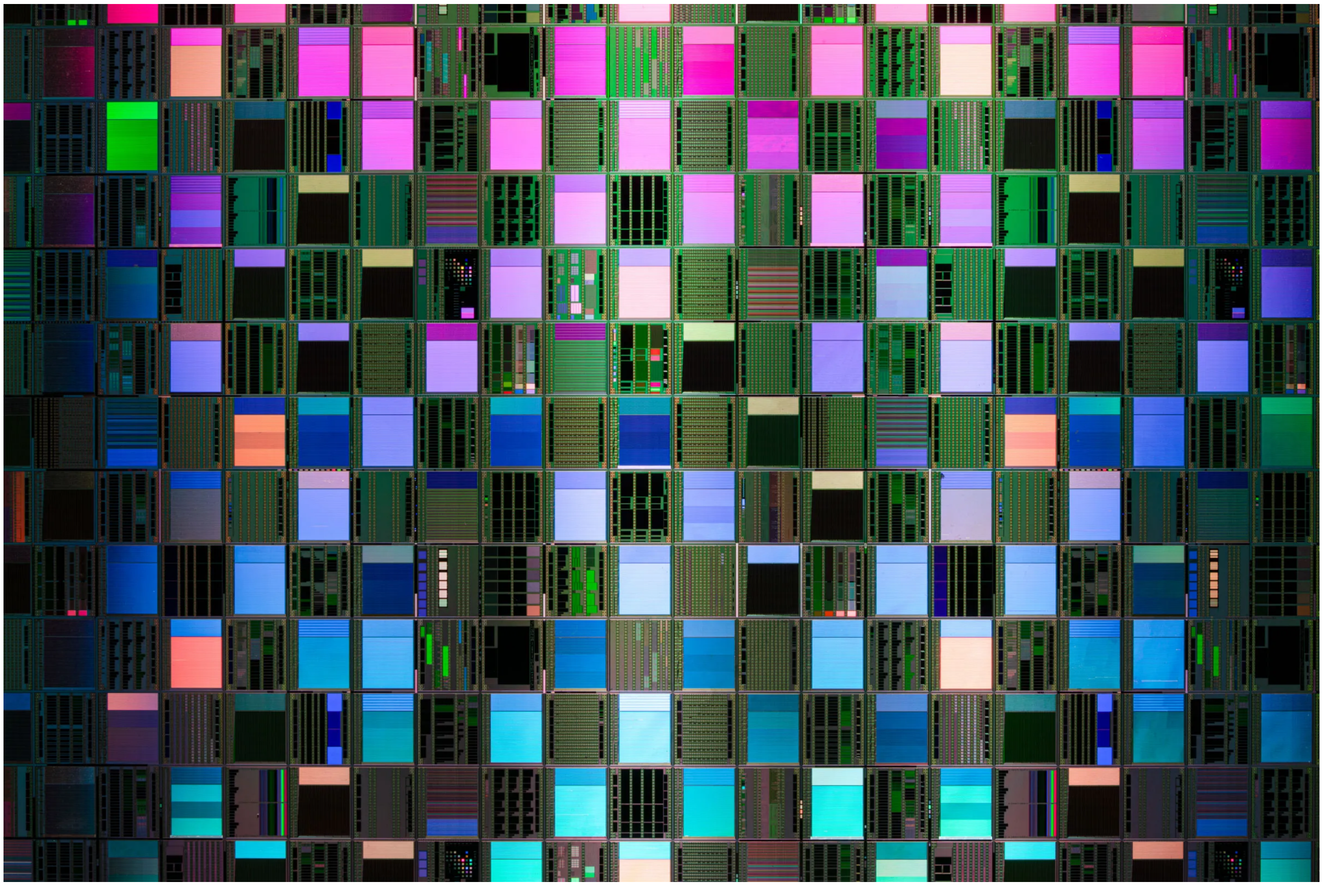
Chinese Hackers Have Pillaged Taiwan's Semiconductor Industry

wired.com/story/chinese-hackers-taiwan-semiconductor-industry-skeleton-key/

Andy Greenberg

August 6, 2020



Taiwan has faced existential conflict with China for its entire existence and has been targeted by China's state-sponsored hackers for years. But an investigation by one Taiwanese security firm has revealed just how deeply a single group of Chinese hackers was able to penetrate an industry at the core of the Taiwanese economy, pillaging practically its entire semiconductor industry.

At the Black Hat security conference today, researchers from the Taiwanese cybersecurity firm CyCraft plan to present new details of a hacking campaign that compromised at least seven Taiwanese chip firms over the past two years. The series of deep intrusions—called Operation Skeleton Key due to the attackers' use of a "skeleton key injector" technique—appeared aimed at stealing as much intellectual property as possible, including source code, software development kits, and chip designs. And while CyCraft has previously given this group of hackers the name Chimera, the company's new findings include evidence that ties them to mainland China and loosely links them to the notorious Chinese state-sponsored hacker group Winnti, also sometimes known as Barium, or Axiom.

"This is very much a state-based attack trying to manipulate Taiwan's standing and power," says Chad Duffy, one of the CyCraft researchers who worked on the company's long-running investigation. The sort of wholesale theft of intellectual property CyCraft observed "fundamentally damages a corporation's entire ability to do business," adds Chung-Kuan Chen, another CyCraft researcher who will present the company's research at Black Hat today. "It's a strategic attack on the entire industry."

Skeleton Key

The CyCraft researchers declined to tell WIRED the names of any victim companies. Some were CyCraft customers, while the firm analyzed other intrusions in cooperation with an investigative group known as the Forum of Incident Response and Security Teams. Several of the semiconductor company victims were headquartered at the Hsinchu Industrial Park, a technology hub in the Northwest Taiwanese city of Hsinchu.

The researchers found that in at least some cases, the hackers appeared to gain initial access to victim networks by compromising virtual private networks, though it wasn't clear if they obtained credentials for that VPN access or if they directly exploited vulnerabilities in the VPN servers. The hackers then typically used a customized version of the penetration testing tool Cobalt Strike, disguising the malware they planted by giving it the same name as a Google Chrome update file. They also used a command-and-control server hosted on Google's or Microsoft's cloud services, making its communications harder to detect as anomalous.

From their initial access points, the hackers would attempt to move to other machines on the network by accessing databases of passwords protected with cryptographic hashing and attempting to crack them. Whenever possible, CyCraft's analyst say, the hackers used stolen credentials and legitimate features available to users to move through the network and gain further access, rather than infect machines with malware that might reveal their fingerprints.

The most distinctive tactic that CyCraft found the hackers using repeatedly in victim networks, however, was a technique to manipulate domain controllers, the powerful servers that set the rules for access in large networks. With a custom-built program that combined code from the common hacking tools Dumpert and Mimikatz, the hackers would add a new, additional password for every user in the domain controller's memory—the same one for each user—a trick known as skeleton key injection. With that new password the hackers would have surreptitious access to machines across the company. "It's like a skeleton key that lets them go anywhere," Duffy says

China Ties

CyCraft quietly published most of these findings about Operation Skeleton Key in April of this year. But in its Black Hat talk, it plans to add several new findings that help to tie the hacking campaign to mainland China.

Perhaps the most remarkable of those new clues came from essentially hacking the hackers. CyCraft researchers observed the Chimera group exfiltrating data from a victim's network and were able to intercept a authentication token from their communications to a command-and-control server. Using that same token, CyCraft's analysts were able browse the contents of the cloud server, which included what they describe as a "cheat sheet" for the hackers, outlining their standard operating procedure for typical intrusions. That document was notably written in simplified Chinese characters, used in mainland China but not Taiwan.

The hackers also appeared to operate largely within Beijing's time zone, to follow a "996" work schedule—the 9am to 9pm, six-days-a-week regimen common in the Chinese tech industry—and to take off Mainland Chinese holidays. Finally, CyCraft says they've learned from their cooperation with Taiwanese and foreign intelligence agencies that a hacker group using similar techniques also targeted Taiwanese government agencies.

Most specifically revealing, though, was the presence of one backdoor program on multiple victims' networks that CyCraft says was previously used by the Winnti group, a large collection of hackers who have operated for over a decade and who are widely believed to be based in mainland China. In recent years, Winnti has become known for carrying out a mix of what appears to be state-sponsored hacking aligned with China's interests and for-profit criminal hacking, often targeting videogame firms. In 2015, Symantec found that Winnti also appeared to be using skeleton key injection attacks like the kind CyCraft found used against the Taiwanese semiconductor companies. (CyCraft notes that it's still not certain that Chimera is in fact Winnti, but considers it a likely possibility.)

Kaspersky, which first spotted and named the Winnti group in an investigation published in 2013, last year linked the group to an attack that hijacked the update mechanism for computers sold by Taiwan-based Asus. Costin Raiu, the director of Kaspersky's Global Research & Analysis Team, says Winnti is responsible for other attacks on a broad range of Taiwanese companies beyond the semiconductor makers CyCraft has focused on, from telecoms to tech firms.

"It's possible that what they’re seeing is just a small fragment of a larger picture," Raiu says. Winnti isn't unique among China-linked groups in their widespread targeting of Taiwan, Raiu adds. But he says Winnti's innovative tactics, like the hijacking of Asus's software updates, set them apart.

Even amidst China's wholesale hacking of its island neighbor, though, CyCraft's Duffy argues that the semiconductor industry represents a particularly dangerous target. Stealing chip schematics, he points out, could potentially allow Chinese hackers to more easily dig up vulnerabilities hidden in computing hardware. "If you have a really deep understanding of these chips at a schematic level, you can run all sorts of simulated attacks on them and find vulnerabilities before they even get released," Duffy says. "By the time the devices hit the market, they're already compromised."

CyCraft concedes it can't determine what the hackers are doing with the stolen chip design documents and code. And the more likely motivation of the hacking campaign is simply to give China's own semiconductor makers a leg up over their rivals. "This is a way to cripple a part of Taiwan's economy, to hurt their long-term viability," Duffy says. "If you look at the scope of this attack, pretty much the entire industry, up and down the supply chain, it seems like it's about trying to shift the power relationship there. If all the intellectual property is in China's hands, they have a lot more power."

Correction 8/7/2020 10:30 AM EST: *This story has been updated to more accurately explain the skeleton key injection technique.*

More Great WIRED Stories

- There’s no such thing as family secrets in the age of 23andMe
- My friend was struck by ALS. To fight back, he built a movement
- How Taiwan’s unlikely digital minister hacked the pandemic
- Linkin Park T-shirts are all the rage in China
- How two-factor authentication keeps your accounts safe
- 🎙️ Listen to Get WIRED, our new podcast about how the future is realized. Catch the latest episodes and subscribe to the 📩 newsletter to keep up with all our shows
- 🏃‍♀️ Want the best tools to get healthy? Check out our Gear team’s picks for the best fitness trackers, running gear (including shoes and socks), and best headphones