Supply Chains Attacks on Healthcare
And other reasons why you might think twice about that elective surgery

As **BleepingComputer reported, July 7, 2022**:

> **Professional Finance Company Inc. (PFC), a full-service accounts receivables management company, says that a ransomware attack in late February led to a data breach affecting over 600 healthcare organizations... Founded in 1904, PFC helps thousands of healthcare, government, and utility organizations across the U.S. ensure that customers pay their invoices on time.**

Further investigation revealed "**that an unauthorized third party had access to systems that contained information about patients of its healthcare provider clients, and files containing patient data were accessed**." Security researchers at AdvIntel, "**detected the PFC attack via signal collections on February 23, 2022 from the Cobalt Strike infrastructure with the early warning details following the attack flow**."

It wasn't until May 5, 2022 that PFC "**sent notification letters to all affected healthcare provider clients... and has since issued notification letters to all affected individuals**." PFC also published a list of healthcare related entities who were victims of the data breach. That document is 15 pages long of fairly small type. **The list can be found here**. And, of course, the breached financial services provider offered up the cyberattack equivalent of "thoughts and prayers."

> **PFC said it is providing complimentary credit monitoring and identity theft protection services to affected individuals.**

In all the reporting about this incident there is no discussion which I can discern of the fact that, if the hackers were inside the systems to steal data, were they not then able to plant more malware? And are these 657 victim entities now exposed to any other kind of attack? Are the 657 entities now possible, if not certain, future victims of other ransomware? How are those 657 different systems going to be cleaned?

This attack stands as a textbook definition of a supply chain attack, and why supply chain attacks do have downstream ripple affects that can be truly frightening in scope. 657 different systems that are by definition networked via the Internet, each connecting to various networks outside of its own network, begins to sound like "**In This Reporter's Opinion**," the scenario for a cyber based 1970s disaster movie. Are cascading network failures, only tangentially related to healthcare, about to cause even greater mass malware infections? Are any of the not so rhetorical questions asked above answered? No.

I wish that were the end of the problems the healthcare industry experienced in June and July 2022, but healtcare providers really took a beating in early summer 2022.

On July 6, 2022, **CISA** — you know, the cyber feds — along with the F.B.I. and the Treasury Department, released **Alert (AA22-187A)** with the inspiring title of "**North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector**." The stated purpose of the Alert release was rather complex and quite a deep dive.

> **This joint CSA provides information—including tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs)—on Maui ransomware obtained from FBI incident response activities and industry analysis of a Maui sample. The FBI, CISA, and Treasury urge HPH Sector organizations as well as other critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the**

> **likelihood of compromise from ransomware operations. Victims of Maui ransomware should report the incident to their local FBI field office or CISA.**

Among the mitigation procedures was the recommendation that affected network admins "**Turn off network device management interfaces such as Telnet, SSH, Winbox, and HTTP for wide area networks (WANs).**" Cutting the **WAN** cord, I read to mean: "Disconnect from the Internet."

Why attack healthcare entities seems a fair question to ask. To which, CISA replied:

> **The North Korean state-sponsored cyber actors likely assume healthcare organizations are willing to pay ransoms because these organizations provide services that are critical to human life and health. Because of this assumption, the FBI, CISA, and Treasury assess North Korean state-sponsored actors are likely to continue targeting HPH Sector organizations.**

Moreover, according to the Alert, the activity has been ongoing since May 2021. As **DarkReading reported**:

> **Since May 2021, there have been multiple incidents where threat actors operating the malware have encrypted servers responsible for critical healthcare services, including diagnostic services, electronic health records servers, and imaging servers at organizations in the targeted sectors. In some instances, the Maui attacks disrupted services at the victim organizations for a prolonged period, the three agencies said in an advisory.**

As reported by **threatpost.com, July 8, 2022**, the Maui strain of ransomware is unique in that the attacker does not offer up a ransom note on how to get back the encrypted files. Another unusual characteristic of this ransonware is that an attack seems to instigated by a human and not simply following the preset programming of the malware on autopilot. Maui will attack specific files and not just the entire directory structure.

The attacks on healthcare providers and entities are a real and present danger to us all. They are occurring right now and continue apace. Anyone — everyone — is or will be, at some time or another, a consumer of healthcare goods and/or services. And we see how this is the very model of a supply chain attack that cripples industries often far removed from the actual attack victim. And the fallout of a cyberattack on a hospital can easily become life threatening. Remember the case of **Baby Nicko Silar**.

Oh, gee. More good news.

Sending my most sincere Tots & Pears
to the many current & future victims of
the cyberattacks on medical facilities.

source: https://i.imgflip.com/3u7zmk.jpg

This ain't no party, this ain't no disco,
This ain't no fooling around
No time for dancing, or lovey dovey,
I ain't got time for that now
— Life During Wartime, David Byrne (Talking Heads)

Back to Top

Gerald Reiff

Back to Top

next post ⟶