BRACEWELL

INSIGHTS

# Sophisticated International Hackers Continue to Target the Public Sector

December 4, 2018

On November 26, 2018, the U.S. Department of Justice announced that it had ***secured an indictment*** of two hackers for using ransomware to extort over $6 million from municipalities, hospitals, and other public institutions. The very next day, a federal grand jury in Pennsylvania ***indicted Russian nationals*** for allegedly hacking into systems at a golf course as part of a fraudulent retail purchase scheme.[1] Although it is unclear if any of the defendants charged in either scheme will ever appear in court in the United States, these indictments demonstrate that a small group of far-flung wrongdoers can cause widespread disruption.

According to the ransomware ***indictment unsealed last week***, two hackers acting from Iran developed sophisticated malware that was able to forcibly encrypt data on targeted networks. Prosecutors allege that for three years, the men researched potential victims online, exploited software vulnerabilities to gain remote access to hundreds of networks, and then installed their self-made "SamSam" malware. Once the malware was widely deployed within a network, the hackers used it to encrypt the victim's data and, in effect, halt or seriously degrade business operations. They demanded a ransom—paid in hard-to-trace Bitcoin—in exchange for the decryption key.

The victims included the cities of Newark and Atlanta, the Port of San Diego, the Colorado Department of Transportation, a public university, and several major health care providers. As noted above, some victims paid the demanded ransom. The ransom note left on the City of Newark's system, for example, demanded 24 Bitcoins (worth about $27,000 at the time) within seven days. After seven days, the hackers claimed that they would destroy the decryption key and render the victim's data irrecoverable. This compressed timeframe was likely an attempt to limit the quantity and quality of the public entities' deliberate decision making and outside consultations.

In all, prosecutors allege that more than 200 victims across the U.S. and Canada incurred $30 million in total damages. Unraveling the scheme required coordination between at least five law-enforcement organizations in the U.S., U.K, and Canada.

Ransomware attacks have been a problem for years, but the SamSam indictment exemplifies the global nature of threat, the ever-evolving tactics and tools employed, and perhaps most interestingly: the precise targeting of the public sector.

We've ***previously warned*** of the cyber threats facing the public sector. In particular, transparent operations—usually required by open records and open meetings laws—make it easier for hackers to conduct reconnaissance on employees and transactions. Details of the

reconnaissance performed by the SamSam hackers have not emerged, but the indictment makes clear that the hackers preformed meticulous internet research to select and target their victims. This research may have included procurement documents that revealed technical network details or vulnerabilities, listings of personnel contact information, and assessments of which systems were most mission critical to the target. The open nature of the public sector will not change, so strong defensive measures and proactive planning are critical.

According to the indictment, the SamSam hackers allegedly exploited "known security vulnerabilities in common server software" in some instances. Many aspects of good cybersecurity are challenging and expensive but keeping software up-to-date can be a relatively low cost, frequently effective but often overlooked defensive measure. For example, the ***WannaCry ransomware*** affected more than 200,000 computers in 150 counties beginning in May 2017, two months *after* Microsoft ***had issued an update*** patching the underlying vulnerability.

Despite best efforts, ***even well-defended networks*** can be breached by determined actors who are developing cutting-edge hacking tools. Therefore, many public entities have a developed and tested response plan that includes technical and legal "first responders" who can be well-positioned to assess the implications of paying a "reasonable" ransom to make the problem go away. Additional incident response considerations include an understanding of any disclosure obligations to the public, to regulators and to law enforcement. These topics are best examined in advance, not while your network, e-mail, and public-facing services are inaccessible.

---

Authors' Note: Charges contained in an indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

---

[1] Adding to the already busy week of cyber news, ***Marriott announced*** a data breach that could affect up to 500 million guests. If so, the incident would be one of the largest ever breaches of personal information.