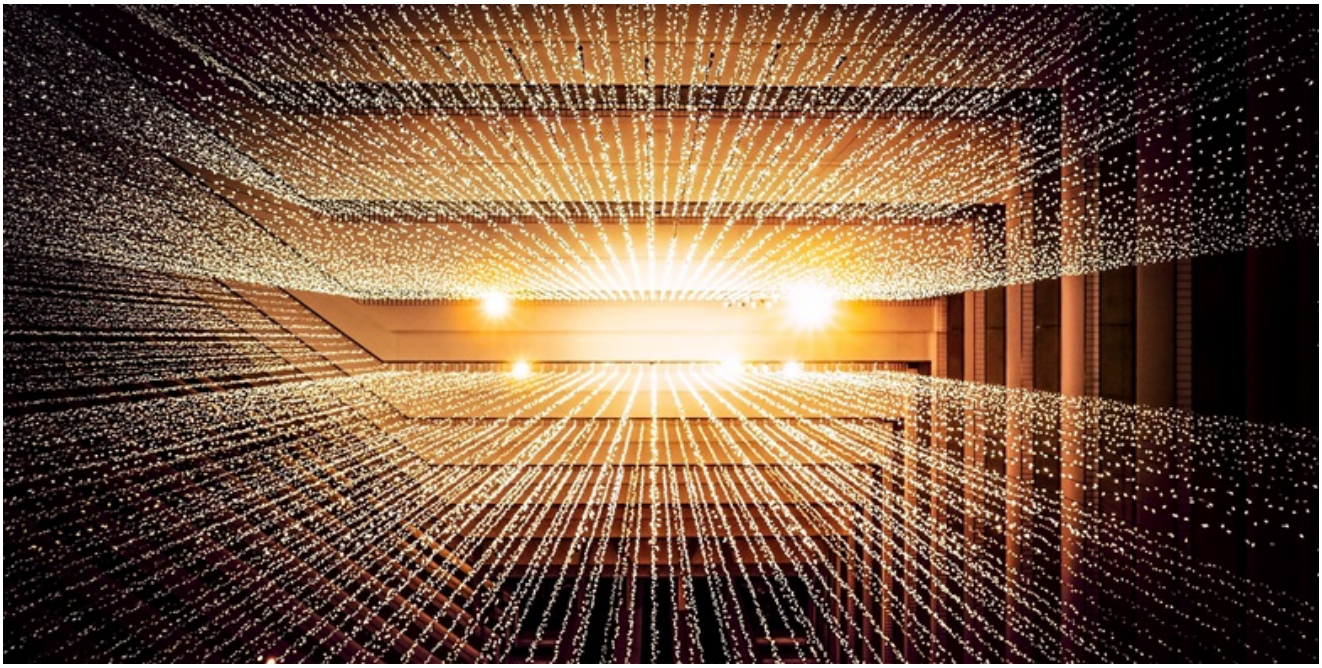
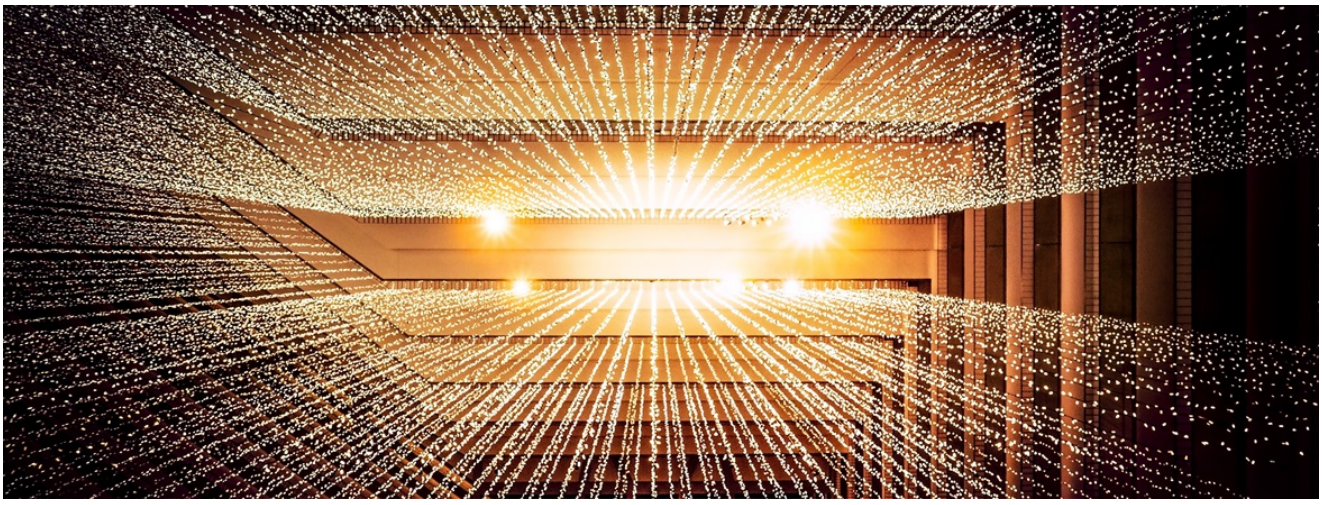
SNOWSTORM: Hacker-for-hire and physical surveillance targeted financial analyst

mishcon.com/news/snowstorm-hacker-for-hire-and-physical-surveillance-targeted-financial-analyst



Posted on *11 June 2020*



MDR Cyber has been investigating the use of ‘hackers for hire’ in the private investigations market after a client was attacked in 2016.

- A Mishcon de Reya client, Matthew Earl, was almost certainly targeted by a hacker-for-hire group named as “Dark Basin” in a concerted phishing campaign with the intention of compromising their accounts. We have been tracking this group as “SNOWSTORM” since late 2016.

- “Dark Basin” (AKA SNOWSTORM) have been publicly linked to the Indian technology company “BellTroX” by University of Toronto cyber research group Citizen Lab in a June 2020 report.
- As well as the electronic phishing campaign, the client was most likely placed under physical surveillance at a time coinciding with the beginning of the email phishing campaign.
- The client was a financial analyst holding a short position on a large business entity at the time and was involved in a dispute due to research they had published alleging fraud.
- The Tactics, Techniques and Procedures (TTPs) used by the cyber-attackers included the use of tailored targeted “spear-phishing” emails, URL shortening techniques, and Amazon AWS cloud infrastructure for delivery of the emails.
- The group also used commercial marketing email tracking software to monitor the “opened” status of emails sent to targets and to manage the campaign.
- The TTPs tracked closely to those reported by Citizen Lab and the report listed several domains we identified as linked to SNOWSTORM, strongly suggesting that Dark Basin was responsible for the activity we tracked under the name SNOWSTORM.
- Although almost certainly illegal, hacking techniques have been used by some unscrupulous private investigators. Compromising email accounts of targets offers interested parties a deep insight into the activities of their target.

The Citizen Lab Dark Basin analysis

University of Toronto body, The Citizen Lab, have published an extensive analysis on the activities of an alleged hacker-for-hire group they call “Dark Basin”. MDR Cyber have been tracking this group as SNOWSTORM since late 2016 following the targeting of a Mishcon de Reya client.

Dark Basin have a wide targeting arc including financial services, legal services, the energy sector and Government bodies. The Citizen Lab assessed that the group were likely engaged in commercial espionage, noting targets included opponents in high-profile public events, criminal cases, financial transactions, news stories, and advocacy. The researchers linked the group “with high confidence” to BellTroX InfoTech Services (“BellTroX”), an Indian technology company.

The target

One of the Dark Basin campaigns targeted financial journalists, short sellers and hedge funds. Our client Matthew Earl, was a financial analyst, who had published allegations of fraud at a large business entity at the time and held a short position.

Matthew instructed our Reputation Protection team, as he was threatened with defamation proceedings by the firm he was investigating. At the same time as receiving aggressive legal correspondence, he started to receive highly targeted phishing attacks, which attempted to steal credentials. We identified that a specific group was likely behind the attacks. As part of our investigation we began tracking the group behind the attacks using the name SNOWSTORM.

It was likely that the objectives of the attack were to understand if our client had been the recipient of whistleblowing or other inside information or evidence that would substantiate his allegations of fraud.

Attribution and Links to Private Investigators

Our client came under targeted physical surveillance at the same time as the cyber-attacks started, which included an intimidating doorstep visit from high-profile private investigators and overt surveillance. The coordinated cyber and physical surveillance was extremely stressful for our client and his young family, causing fears for their physical security.

We cannot determine how SNOWSTORM became involved or who hired them. It is unlikely to be the firm Matthew was investigating as Hacker-for-hire groups do not advertise widely. Once we ascertained that private investigators were involved our team began to look further into the hacking for hire market.

Conversely the information in the targeted emails and the phishing lures could only have come from someone deeply involved in the matter, most probably either the ultimate client or other interested party. This indicates that the hacking operation was being orchestrated as part of a larger campaign.

When investigating SNOWSTORM, we were made aware by The Citizen Lab that an Indian firm was involved in hacking for hire. Enquiries by our team in the private investigations market provided anecdotal evidence that a group was being used as part of these types of investigations and was also connected to India supporting their assessment.

This led us to the conclusion that an Indian hacking for hire firm was being likely being used by private investigators.

Tactics, techniques and procedures

We saw an increase in attempts to access our clients account and those of connected family members. This indicated a level of open source intelligence gathering to identify family members, as well as potential password guessing attempts.

The group used highly targeted phishing emails with subject matter that directly involved the target. The sender addresses and emails mimicked media organizations. The content of the emails stood out as more tailored and sophisticated than those we usually see, alongside more generic phishing emails.

In the attacks we investigated, SNOWSTORM used a public URL-shortener and the emails used a commercial marketing email tracking service to see if the emails had been opened or read.

The links contained in the emails led to fake login pages that attempted to capture credentials.

The impact

Many of the targets of sophisticated cyber-attacks are nameless, or their experience is tempered by being part of an organization which can protect them. We worked closely with Matthew during the incident, and have over the last three and a half years continued to investigate what occurred.

Matthew describes the experience of being targeted by the group. *"The receipt of aggressive legal correspondence, targeted physical surveillance and sophisticated digital hacking are each, at a singular level, stressful enough. However, the sudden and coordinated combination of all three was traumatising for my family and myself. Especially in light of the scale and significant resources that were used."*

Conclusion

Cyber-attacks now affect every industry. It may come as no surprise that errant investigators, who may previously have relied on pretexting or paying for information, have now turned to bringing in cyber expertise.

We are grateful to Matthew for continuing to support our investigation. Matthew commented that *"A key reason my family managed to get through that period was due to the help and support from Mishcon de Reya, which gave comfort that despite the overwhelming nature of the experience, we were in fact not alone and it could be dealt with."*

We are continuing to monitor groups who operate in this area along with their use by some elements of private investigations market. We believe that commercial espionage has the potential to be as high-profile as that conducted by nation states.