# As cyber defences strengthen, threat actors adopt new tactics

**By Shawn Gillooly, Senior Digital Investigations Analyst**



As corporate cyber defences have improved over recent years, organised criminal groups and malicious state actors have discovered new ways of penetrating company systems, based around the exploitation of their digital vulnerabilities, rather than just cyber security or technical weaknesses.

Cyber defences are now so resilient that it's much harder for hackers to brute force their way into firms' IT systems than it was a decade ago. In other words, the level of defence has often evolved quicker than the level of offence. But in the digital space—which encompasses things like social media, personal blogs, and other avenues for collecting personally identifiable information (PII)—relative defence remains quite low. Thus, we've seen a strategic-level shift, where exploiting the digital space to attack an organisation now has a risk-reward ratio that was once only possible with purely cyber or technical-based security breaches.

Central to threat actors' enhanced strategy is the increased use of so-called social engineering—essentially the mass gathering and use of information posted on social media platforms and the dark web—either to aid in penetrating IT infrastructure, or to trick the target for some personal gain.

This publicly available digital material related to companies and their employees, which has ballooned in the last ten years, is providing hackers with multiple new opportunities to hold companies to ransom, disrupt their operations, and steal confidential information.

While cyberattacks remain a clear and persistent threat to organisations, the hacking groups behind them—particularly those linked to state actors—have come to realise that they can achieve the same results through exploiting digital vulnerabilities, with a fraction of the resources, funds and time.

These methods come in a variety of forms, relying mostly on a combination of criminal deception and ingenuity. It's quite an opportunistic approach, centred around exploring social media accounts and the dark web

to develop ruses and tricks that could ultimately lead to the unlocking of a company's systems. Uncovering PII can also be used to make it easier to exploit cyber vulnerabilities, like finding old passwords or compromised websites a senior member of staff had a personal account on.

So, for example, threat actors employing fake profiles and/or AI technologies are able to masquerade on business networking sites as former colleagues or old university acquaintances of key company employees, the aim being to dupe them into revealing information – perhaps an internal policy, procedure or protocol – that could leave their firms vulnerable to attack. The targeted individuals

> “Why brute force your way into a system when someone is using the same password they used ten years ago?

would likely be in charge of a sensitive area of the company, but not so senior that their communications are closely regulated.

Another scenario could involve threat actors trawling the dark web to find out whether middle-ranking company personnel had worked for companies in the past whose emails and passwords had been hacked and leaked. The hackers then simply see if these employees are still using their old passwords in their current roles. And, if they are, break into protected areas of the company. Why brute force your way into a system when someone is using the same password they used ten years ago?

> “...threat actors can also inflict damage on an organisation without necessarily ever penetrating them.

Yet threat actors can also inflict damage on an organisation without necessarily ever penetrating them. They can, for instance, undermine its reputation at critical times, say when it is engaged in bidding negotiations for a big contract. Social accounts of personnel involved in the negotiations can be doctored, after which the threat actors might use inauthentic social media accounts and leverage networks of unwitting individuals to amplify the false information. If picked up by the media, it could potentially jeopardise the company's chances of securing the contract.

Just as with cyber security, there are ways to address new and increasing threats from digital vulnerabilities. In terms of practical steps, it would obviously not be practical or advisable to try to curb employees use of social accounts or mobile communications tools. But companies can reduce the risk of being compromised through rigorous management of data flows within their organisations and becoming more alert to new digital threats they may face.

On the data flow side, decision-makers should ensure policies around the use of laptops and

cell phones are strictly adhered to—instituting regular checks to confirm that they are—and siloing off sensitive information from parts of company that have no need to have access to that information (aka Identity and Access Management).
As for horizon scanning, senior executives would be wise to better understand how threat actors engaged in digital manipulation are operating in the wild, so to speak, and then using the intelligence gleaned to reinforce company defences.

For instance, if there are reports of upticks in organisations receiving audio or video conferencing calls from fraudsters masquerading as clients, it would be sensible to strengthen device management policies about who can be contacted by an external source on the firm's internal communications network.

Of course, companies should not just confine themselves to addressing their own digital weaknesses, but also those of their employees (private social media profiles, in particular) and vendors or supply chain partners. And here, it's all about raising awareness among staff of threat actors' modus operandi in the digital space, and doing what you can to integrate digital vulnerability mitigation into your vendor and supply chain agreements. Even small red flags like unexpected LinkedIn messages from people claiming to be old college friends, or a surge in unanticipated profile visits or searches, could suggest the reconnaissance phase of a targeted campaign against your organisation.

> "...companies should not just confine themselves to addressing their own digital weaknesses, but also those of their employees

Threat intelligence gathering, then, is broadly about identifying suspicious activity in the digital realm that might impact your company. So, is its name popping up in major groups on Telegram – a common platform for threat actors to organise on? Is the firm being mentioned in hacking forums? Or has some of its data just been dumped on the dark web? Better to act on such intelligence to ready for a potential attack when you still have time.

Threat actors are moving into the wider digital realm because they are following the path of least resistance to achieve their goals. That used to be the brute forcing of weak cybersecurity measures. But with heavy investment in cyber defences, they have found new weaknesses to exploit. Addressing these is less about installing costly protective tools than being on the front foot: alert to the threats and having the processes in place to ward them off.

**Shawn Gillooly is a Senior Digital Investigations Analyst at PGI, specialising in due diligence and reputation risk management. If you would like to speak with Shawn or one of the team, please contact us:**

**Phone: +44 20 4566 6600**
**findoutmore@pgitl.com**

Originally published in Management Today on 24 March 2025 with the title '[Now the cyber criminals are coming for your social media]'