Rapid Evolution and the Creation of a New Class of Cyber Criminal.

October 04, 2022

Editors Note: Jason Sgro, Senior Partner and Head of Cybersecurity & Human Privacy at ATOM, shares information here about cybersecurity risks especially in times of geopolitical tension. This written piece accompanies Jason's Town Fair presentation about creating cyber resiliency. In addition to his role at ATOM, Jason is also President of the FBI's InfraGard Program in NH, Director of the NH Office for Cooperation in Cybersecurity, and Executive Director of The Overwatch Foundation.

> It is, however, a call to action to decision-makers everywhere. Many select boards have assigned or outsourced cyber protection to third parties or teams deep within their organizations without direct proven knowledge of how those decisions will play out in an emergency.

As recently as a year ago, we were focused on discussing two classifications of cyber criminal. The first classification was the Advanced Persistent Threats (APTs) which consisted of the largest and most prolific cybercrime organizations, including state-sponsored threat actors and terrorist organizations sanctioned by the Office for Foreign Asset Control. The second, and most common, were pop-up cybercrime organizations that used as-a-service tools, known exploits, ransoms, and fraud schemes to make easy money and essentially disappear into the ether of the digital landscape. Occasionally we would see a larger and more capable organization emerge around a new ransomware technology or zero-day threat and do some damage, but those were fewer and farther between. **Our day-to-day battle was one where we fought opportunistic but unsophisticated criminals finding the paths of least resistance, casting wide nets, and catching whatever organizations fell into them.**

However, the recent geopolitical tensions and the resulting Russian invasion of Ukraine have catalyzed the emergence of a whole new classification of cyber criminals that pose a direct threat to our municipal institutions. Certainly, the opportunity for criminal activity has always

existed inside major conflicts, and criminal organizations have long hidden inside conflict areas to escape prosecution. This conflict is no different in that regard, but it's also unique for one crucial reason.

> This new type of criminal is far more patient, capable, and tactically diverse than the previous pop-up criminal organizations.

The Russia-Ukraine conflict is one of, if not the first major conflict that included a significant asymmetric cyber component before and during traditional military operations. Multiple open-source reports suggest this cyber component drew in APTs and well-known hacking organizations providing support to both sides of the conflict in addition to whatever Electronic Warfare (EW) tactics may have been deployed by the Russian Federation and other nation-states in the days preceding the invasion. This global consolidation, or focusing of cyber capabilities, released a massive amount of novel technology and new exploits into the conflict over an extremely short period, providing an environment rich in opportunities to test, iterate, and evolve attack vectors against real infrastructure.

As a result, we have watched the emergence of a third classification of cyber criminals measured between the capabilities of the previous two. **This new type of criminal is far more patient, capable, and tactically diverse than the previous pop-up criminal organizations.** Threat analysts at major cyber firm Sophos independently confirmed the finding that cyber criminals have "raised the professionalism of the [cyber] business." They are armed with APT and military-level cyber technologies and tactics they have witnessed, collected, or developed within this conflict and elsewhere in the world.

The most capable cybercrime organizations are polishing as-a-service tools to distribute these advanced capabilities far and wide. As a result, we have seen the first multi-type attacks, such as ransomware, mixed with financial fraud. We have seen a major uptick in persistent monitoring of email systems and networks, where the victims are monitored for at least six months and up to three years before any cyber event is triggered. These increases in patience, stealth, and capabilities are noteworthy and cause for concern.

All of this is important to those of us dedicated to protecting our institutions because our enemy is evolving at a rate never before seen. The domestic lull in ransomware attacks we've enjoyed in the last few months is gaining momentum again, with renewed techniques and higher-level capabilities. All of this is happening during a time when our most vulnerable and

critical New England entities are still struggling with the basics of cybersecurity. Adoption of multi-factor authentication, log aggregation techniques, incident response, and disaster recovery are inching forward while our enemy evolves at a rapid rate. Cyber jobs remain unfilled, and IT professionals, wearing many hats, are burning out under the strain of the tasks ahead.

Even though the trend we've just discussed is less than ideal, I believe it isn't at all a hopeless scenario. It is, however, a call to action to decision makers everywhere. Many select boards have assigned or outsourced cyber protection to third parties or teams deep within their organizations without direct proven knowledge of how those decisions will play out in an emergency. I routinely meet with municipal leadership teams at risk of abdicating aspects of cyber risk management testing and validation to the point where their understanding of those functions is either vastly overstated or widely misunderstood. The correction, unsurprisingly, requires board-level consideration and intervention. It requires the allocation of capital and an investment in our most valuable resources, people. Together we can turn the tide of this threat, but only if we work together, in partnership, at the highest levels of our organizations. Cyber is now far beyond an IT issue. It is a board-level issue. **It is a community-level issue. And with this understanding, we can move swiftly and efficiently toward a solution that will safeguard the trust and institutions we've vowed to protect.**