cybereason

CYBEREASON'S 2020 SECURITY PREDICTIONS: NATION STATES VS MARKET INNOVATION_

The Adversaries, The Defenders, and the Hope for 2020.

THE FUTURE OF CYBERSECURITY_

It's that time of year again: trends and predictions.

Just like in 2019, as we go into 2020, it's time to reassess the past year before beginning strategic security planning. There are three dominant geopolitical events next year that will guide many cyber activities, either by providing opportunity and motivation for attackers or by muddying the waters and adding to the confusion: **the US presidential election, Brexit, and the upcoming 2020 Tokyo Olympics.**

Will that be all? No, of course not. Things will happen as they do every year, and cyber will both affect other means of conflict and be its own battlefield, just as it did in 2019.
These predictions should give you some insight into the coming year.
Prepare as you will, but don't forget - security always comes back to the basics.

Read the full predictions on:

- » The Landscape Today: Lemon Market, Living off the Land, and Advancing IOCs
- » The Adversaries of 2020: Nation States, Cybercrime Trickle Down, Threat Actors
- » The Defenders of 2020: Talent Gap, Assisted Intelligence, Evolving Vendors, IoT & Cloud
- » The Hope for 2020 and Beyond: Agile, Automation, Adaptation

SAM CURRY
CHIEF SECURITY OFFICER
CYBEREASON

THE LANDSCAPE TODAY: 2019_

SECURITY IS A LEMON MARKET

The security market remains a Lemon Market: in spite of innovation from some vendors, the overall poor quality products continue to command an increasing amount of money from customers with little expectation of improvement. This does not align with the needs of security teams, who face more advanced threats, understaffing, and alert fatigue than ever before. Legacy security vendors are past the point of bloat, causing security teams to look to other vendors for more advanced capabilities at a comparable or lower price.

ADVERSARIES ARE LIVING OFF THE LAND

Attackers are massively increasing their use of fileless malware, now more commonly referred to as living-off-the-land binaries (aka LOLbins). Fileless malware has been proven effective at evading antivirus, leading attackers to branch out from PowerShell exploits to leveraging the most ubiquitous, powerful, and indispensable tools, from Microsoft Office scripting to WMI and much more.

IOCS ARE NOT ENOUGH TO FACE ADVANCED ADVERSARIES

IOCs are no longer enough when defending advanced attacks. In Operation Soft Cell, we saw that the same binaries from the same attacker in the same kill chain with different hashes. At one point, the same dropped instance of Poison Ivy on subsequent machines in the same attack motion had distinct IOCs. IOCs are a building block for effective security, but they are no longer the end-all-be-all of defense. We need a common system around which to communicate threats, alongside a common language to back it up.

Attackers are finding their way around classic security tools like legacy antivirus. This is not to say these tools aren't important, but they are just a part of a strong defense, not the entirety of it. SIEM, antivirus, and firewalls are all still valuable, but they are no longer the lynchpin of a strong defense. New innovation, collaboration, and a renewed sense of urgency will lead to new and effective products of the future, instead of the ones for yesterday.

THE ADVERSARIES IN 2020_

NATION STATE ACTORS WILL EVOLVE FASTER

From the last few years alone, it's clear cyber is another tool adversaries use against one another for financial and political gain. In 2020, belligerent and attacked states will continue to take action, especially the usual suspects: Russia, China, North Korea, Turkey, Iran, and their preferred targets. This will be especially impactful around events like the 2020 US Presidential election, the ongoing chaos with Brexit, and the 2020 Tokyo Olympics.

Nation state actors have a unique advantage over other adversaries since they have arguably unlimited resources to accomplish their mission. They work at the leading edge of attacks with the fastest evolving toolkits. They will share some of these toolkits with allies and the adversary community at large, fueling a year of increasingly more advanced threats across the board.

THE CYBERCRIME TRICKLE DOWN EFFECT WILL GET WORSE

The most disturbing insight into 2020 is the trickle down effect that will take place between adversaries. Not only do adversaries often work together, but the tools from advanced nation-state labs often spread across the community soon after. Using nation-state tools gives less advanced adversaries an impressive toolset. Simultaneously, it also makes it much harder to attribute attacks to one particular nation states adversary, as much of the community is using their toolset.

CRITICAL INFRASTRUCTURE & NEW TECHNOLOGY WILL BE BIG TARGETS

Attacks targeting critical infrastructure and exploiting supply chain weaknesses will grow in 2020 alongside threats to emerging technologies. As we build more IoT devices, coupled with the rise of OT and advances in the rollout of 5G, it will be a critical year to control assets in the event of later, more heated conflict.

There will likely be big, showy attacks around geopolitical events, like DDoS attacks around the Tokyo Olympics or the US Presidential election. Simultaneously, expect more subtle infiltrations of infrastructure through non-traditional devices for corporate information and misinformation campaigns.

With regards to 5G, the bandwidth of a given cell will soar along with the number of devices, while latency and the size of the cell will decrease. All of this will put into question the physical security of these devices and the manufacturers credibility. Consider Huawei, whose 4G cells have a massive footprint throughout the world and can be upgraded, backed by the Chinese government. Watch out for threats to the supply chain and those directly to the cell, as well as espionage operations and DDoS attacks on IoT and OT devices.

LINES BETWEEN THREAT ACTORS WILL BE BLURRED

Attribution is highly unreliable already, but with the trickle down effect among cybercriminals increasing, it will be nearly impossible in 2020. The degree of specialization from nation states, hacktivists, and cybercriminals will increase regardless of the level of technical prowess, especially as MaaS continues to spread. Be wary of attempts at attribution, especially those without clear evidence. Effective attribution may no longer be possible, or at least need a massive rewrite for any level of fidelity.

THE DEFENDERS IN 2020_

THE TALENT GAP WORSENS

Though the security industry is producing more talent than ever before, the talent gap still continues to widen. This will only get worse in 2020. To some degree, the industry has created the talent gap by making it harder and harder to become a qualified cyber professional. They have not made cybersecurity jobs easier to do, instead doubling down on deep industry knowledge of dozens of tools that don't work well together.

Thus far, the industry has not done a good job of opening our recruitment to look at non-traditional background for cyber talent. Cybersecurity professionals aren't born and don't fit one particular mold, and recruiting efforts should reflect that. Without changing current trends and finding talent in non-traditional places, the talent gap will get worse in 2020.

TECHNOLOGY MUST SUPPORT ANALYSTS

Instead of artificial intelligence, vendors will adopt assisted intelligence. Cybersecurity professionals need help to be more effective, not necessarily replaced. Automation and improved context will help cybersecurity professionals succeed by decreasing their workload and letting them focus on more advanced threats The security vendors that will shine in 2020 will be those that help security professionals become more efficient and capable, not ones that replace them.

SECURITY VENDORS MUST EVOLVE

The legacy security vendors aren't likely to make tasks easier or innovate because of their existing momentum and hodge-podge feature set of merger after merger. They will continue to be disrupted or in other cases acquired, merged, and potentially even broken up in 2020 as they were in 2019: Symantec by Broadcom, Carbon Black by VMWare, Recorded Future by Insight, Demisto by Palo Alto, BlackBerry finishes acquisition of Cylance, and many, many more. Meanwhile new security vendors are innovating to address advanced threats and make security easier for defenders. While SIEM and antivirus are still necessary, the industry in 2020 will see the brands that have dominated for 20 years fade and a new crop of midsize, inventive companies emerge in a healthy rejuvenation of the industry.

IOT WILL MEET CLOUD SECURITY

There will be a host of innovation and new companies around mobile, OT and IoT security. It's worth paying attention to these as, when combined with cloud security, the nature of IT is drastically changing. It's inevitable that with new players and new technologies, security will have to change too.

THE HOPE FOR 2020 & BEYOND_

ADOPT AGILE

Security operations teams must adopt more agile to bring intelligent processes to defense. Security technology and practices must adapt to remove waste from critical processes and make security easier for the user. Users need to be able to investigate advanced threats, instead of getting bogged down in everyday commodity malware. It's time for security to embrace Agile and transform itself in much the same way that DevOps transformed IT and R&D.

AUTOMATE AWAY UNNECESSARY TASKS

Security must pursue an ever more autonomous security operations function that assists analysts, rather than replacing them. Thinking about it broadly, security falls into two sets of activities. First, prevention tools, identity and access projects, and vulnerability and patch management processes can be broadly considered IT security functions. Second, EDR, SIEM, SOAR, NTA, UeBA, EPP, and more can be broadly considered cyber functions. Both are critical to a strong security posture, and they should be closely integrated for an effective security strategy.

Telemetry beyond IOCs will also be a critical asset, including Indicators of Behavior that have more permanence and are able to track attackers regardless of their innovation and evasive techniques. Vendors must build systems that innovate away from solely IOCs and advance to IOBs to address modern threats.

SECURITY VENDORS MUST ADAPT & INNOVATE

Commodities will be forced to innovate into 2020. Brand strength without substance is no substitute for adaptation, innovation and antifragility in tools and operations. The post-breach mindset and acceptance that risk will never go away completely will be a theme with larger 2020 attacks. But acceptance does not mean security should give in; make minimum risk acceptable and take steps in 2020 to reverse the asymmetry in cyber conflict to give defenders the advantage. Get rid of false positives, make security tools more effective together, give your security team more context, and improve the efficiency of the analyst.

CONCLUSION_

There's only one way to get to the future we hope for: continuing our education and making bold moves.

Visit our website to learn more about our solutions that integrate:

INDICATORS OF BEHAVIOR | ASSISTED INTELLIGENCE | ADDRESS ADVANCED THREATS

ABOUT CYBEREASON

Cybereason gives the advantage back to the defender through a completely new approach to cybersecurity: the Cybereason Defense Platform. Cybereason offers managed, as-a-service, and on-premise prevention, detection and response solutions. Cybereason technology delivers multi-layer endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Cybereason is privately held and is headquartered in Boston, MA with offices around the globe.

FOLLOW OUR BLOG TO KEEP UP ON THE LATEST HAPPENINGS IN CYBERSECURITY, OR FOLLOW US ON SOCIAL MEDIA.

cybereason