WHITE PAPER

AI-driven Cyber Crime Brings New Challenges to CISOs

Too Fast, Too Agile, Too Dangerous for Traditional Security Approaches

Executive Summary

The combination of accelerating threat evolution and expanded attack surfaces has brought enterprise security teams to a tipping point in the battle against cyber crime: they can no longer win by throwing more products and people at the problem. Facing budgetary and staffing constraints and a scarcity of white-hat security experts, security leaders often cannot fully execute on their security strategies. But even if they could, cyber criminals are leveraging artificial intelligence (AI) and agile development techniques to outpace human security analysts and outmaneuver even the newest network defenses.

Still, security leaders must prevail. Their organization's digital transformation (DX) rests on the assumption of a secure network environment. To avoid the damaging impact of debilitating attacks and data breaches (the cost of cyber crime has increased by 72% over the past five years[1]), executives must take security to a new level.

In Q4 2018, FortiGuard Labs recorded nearly 36,000 new malware variants from over 4,800 different malware families.[5] The increased targeting of exploits and automation of malware ratchets up the urgency for security leaders.

Number of companies experiencing a severe exploit in Q2 2018:

96%[6]

Average time to detect a network breach:

197 days[7]

Threat Volume and Sophistication Increasing

Cyber criminals are increasingly turning to automated and scripted techniques that exponentially increase the speed and scale of attacks. Mapping networks, finding attack targets, determining where those targets are weak, blueprinting each target to conduct virtual penetration testing, and then building and launching a custom attack can be fully automated using AI.[2] This dramatically increases the volume of attacks a criminal can launch in a given time period, and may be one reason why the number of exploits continues to explode, growing 129% from Q1 2018 to Q1 2019.[3]

At the same time, attacks are becoming more sophisticated. Polymorphic malware has been around for decades, using precoded algorithms to take on new forms to evade security controls and potentially producing more than a million virus variations per day. Next-generation polymorphic malware built around AI can spontaneously create entirely new, customized attacks that are more than variations based on a static algorithm. Instead, they may soon employ automation and machine learning (ML) techniques to design custom attacks to quickly compromise a targeted system and effectively evade detection.

Cyber criminals could potentially harness ML to perpetually analyze their attack code for vulnerabilities to detection by security vendors. Employing ML in this way enables attackers to automate on-the-fly code modifications that make malware less detectable. Criminals can further use ML to gather information in preparation for an attack, learn how a company's firewalls work, discover the analytics models the IT security team uses to detect attacks, and even monitor the times of day that the security team is in the office.[4]

The Inadequacy of People and Point Products

Why are enterprises unable to keep up with AI-driven cyberattacks? One culprit is the disaggregated topology of many network security architectures. Enterprises average more than 30 security-related point products within their environments,[8] which makes it difficult to share threat information in real time. Obtaining a high-level view of the organization's overall security posture requires manual effort by security and network staff to consolidate data from all the disparate security applications.

Furthermore, when an attack threatens the corporate network, the response is not coordinated and, therefore, is slower and less effective. While cyber criminals take every advantage of their rapidly shrinking exploit times, enterprise security teams struggle to move the needle on detection. The average breach detection gap (BDG)—the time elapsed between the initial breach of a network and the discovery of that breach—has hovered stubbornly around 200 days for the past several years.[9]

Finally, when security leaders try to gain some headway by bolstering their teams with security experts, they find those with the right skill sets and experience to be both costly and in short supply. And for those seeking to add staff with experience designing and implementing AI-driven security, they are very difficult to find, recruit, and retain. For example, of the 20 hard skills most commonly cited in resumes, AI security skills are nowhere to be found.[10]

Criminals Use AI to:

- Learn how enterprise firewalls work
- Discover attack detection models
- Monitor security team movements

Expanding Attack Surfaces Offer More to Exploit

DX is creating a growing security burden for security leaders. DX initiatives result in more mobile and Internet-of-Things (IoT) devices on the network, as well as a growing portfolio of cloud applications running on multiple cloud platforms. All of these increase the enterprise attack surface, providing more vectors for cyber criminals to enter the network, exfiltrate data, and exploit resources.

IoT: Headless and Heedless

IoT devices have been increasingly attractive targets, as they are often "headless," lacking the control and visibility provided by a traditional user interface. It should come as no surprise that more than 25% of enterprise attacks are predicted to target IoT devices by 2020.[12] This is especially disturbing due to the fact that compromised IoT devices can be used to attack vulnerable systems on a large scale using another application of AI: swarm technology. In a "swarm," IoT devices become malware proxies, attacking the corporate network from within and sharing local data with the malware creator via the internet.[13] To date, no known attacks have used swarm technology in this way, but if IoT devices were harnessed as swarms, they could simultaneously attack many victims and significantly impede threat mitigation and response.

As if that was not enough, IoT devices—especially media devices—are now a target for cryptojacking: criminals are exploiting the powerful GPUs in these always-on devices to mine cryptocurrency, potentially hobbling IoT devices' intended enterprise applications.[14]

Clouds Out of Reach

If far-flung corporate assets such as remote servers, endpoints, and IoT devices seem vulnerable, consider assets owned by a third party, such as a cloud service provider. Enterprises must rely on their cloud providers to secure the facilities, hardware, and operating systems supporting their applications, and this lack of direct control can pose a significant risk. To wit, hackers have recognized the lucrative potential of using cloud providers as a conduit to spread malware to enterprise subscribers, and the number of such attacks increased 200% in the past year.[15]

Compounding this risk is the fact that most companies deal with more than one cloud provider. One survey of enterprises with at least 1,000 employees found that 84% of respondents' organizations use hybrid clouds, multiple public clouds, or multiple private clouds.[16] According to research from Fortinet, organizations now use a median of 62 different cloud applications, accounting for roughly one-third of their applications.[17]

Enterprises are scrambling to secure networks with more than 30 security-related point products, on average.[7]

53% of organizations report a problematic shortage of cybersecurity skills.[11]

By 2020, IoT devices will be the target of 25% of enterprise attacks.[12]

Stopgap Security Thwarts Visibility and Control

As attack surfaces grow rapidly through network expansion and cloud adoption, security leaders may be tempted to close each security gap with a targeted solution. This strategy is questionable in several regards. First, it is hard for security budgets to keep pace with security gaps. Even when cybersecurity is top of mind in the boardroom, it can be edged out by budget priorities such as operational efficiency, improved customer experience, and business growth.[18] Without adequate funding, security coverage will lag behind network expansion, weakening the security posture.

Second, the larger a security product portfolio, the harder and costlier it is to manage. Security teams are stretched thinner and thinner; tool-specific proficiencies become harder to maintain. Plus, technology licensing and maintenance spend must be spread over an increasing number of vendors.

Third, because disparate products do not always integrate seamlessly, security teams do not have the end-to-end visibility and control they need to quickly detect and remediate attacks that may jump from mobile end-users to cloud providers to data centers in a matter of minutes.

Enterprises have experienced a 200% growth in attacks through their service providers.[15]

It Is Time to Reevaluate Security Technology Strategies

For all their organizational might, enterprises have so far proven to be no match for the guerilla tactics of the global cyber-crime industry. It is safe to say that every enterprise has already been compromised in some way.

Security leaders can level the playing field by taking a few pages from the playbook of cyber criminals as they reevaluate their security technology strategies. It does not take a hacker to realize, for example, that a common code base reduces costs and speeds implementation, efficient information sharing improves the odds of success, and AI is a powerful analytical lever.

That said, the terms AI and ML are used frequently these days in marketing materials for security solutions—and what these terms signify is not always clear. Following are several questions that security leaders can ask as they explore potential solutions:

1. **How long has AI-based analysis been in place?** Since AI systems get more accurate over time by training themselves using ever-increasing volumes of data, this question is critical.
2. **Is AI-based threat intelligence supplemented by robust and scalable sandbox analysis?** As threats become more customized, a greater percentage of attacks are zero-day. A layered approach that monitors the characteristics of files using AI combined with analysis of specific files provides the most complete protection.
3. **Can comprehensive threat intelligence be shared automatically across the infrastructure?** Threat intelligence is less effective if it is not available in real time by all the security tools in the network. An integrated security architecture helps organizations thwart today's advanced persistent threats that move at machine speed.

[1] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, March 6, 2019.

[2] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[3] "Threat Landscape Report Q4 2018," Fortinet, accessed May 24, 2019.

[4] Mike Lynch, "AI cyberattacks will be almost impossible for humans to stop," WIRED UK, December 28, 2017.

[5] "Threat Landscape Report Q4 2018," Fortinet, accessed May 24, 2019.

[6] Ibid.

[7] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, March 6, 2019.

[8] "Security Transformation Requires a Security Fabric," Fortinet, February 22, 2018.

[9] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, March 6, 2019.

[10] "The CISO Ascends from Technologist to Strategic Business Enabler: Understanding the Cybersecurity Skills Shortage," Fortinet, August 15, 2018.

[11] Jon Oltsik, "The cybersecurity skills shortage is getting worse," CSO, January 10, 2019.

[12] "Fortinet Security Fabric Powers Digital Transformation: Broad, Integrated, and Automated," Fortinet, March 29, 2019.

[13] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[14] "Threat Landscape Report Q1 2018," Fortinet, May 14, 2018.

[15] David Bond, "Hackers target cloud services," ft.com, July 12, 2018.

[16] "RightScale 2019 State of the Cloud Report," RightScale, accessed May 24, 2019.

[17] "Threat Landscape Report Q3 2017," Fortinet, November 17, 2017.

[18] Sharon Florentine, "Top IT spending priorities for 2019," CIO, March 12, 2019.