WHITE PAPER

Advanced Threats: The CIO's Time Bomb

Increasingly Complex Tactics by Adversaries Threaten IT Assets and Budgets

Executive Summary

CIOs are more influential in their organizations than ever as IT contributes more directly to the bottom line. However, their jobs are much more complex than they were a few years ago. And as cybersecurity becomes a boardroom topic, the CIO often spends more time dealing with security issues, even as the CISO has moved into a parallel reporting structure at many organizations.

At the same time, cyber criminals are becoming progressively more sophisticated, resulting in an advanced threat landscape that requires a strategic approach. Threats are increasing in volume, velocity, and sophistication—and traditional approaches to security are no longer adequate. Specifically, reliance on a fragmented security architecture requires manual processes that reduce efficiency, diminish security, and endanger network performance.

For today's CIO, the words of Charles Dickens might vaguely resonate: *"It was the best of times, it was the worst of times."*

In some ways, it is a great time to be a CIO. No longer is the CIO viewed as the leader of a back-office team providing tactical services for the "money-making" parts of the company. Rather, CIOs are now seen as drivers of the business, playing key roles in corporate strategic planning and delivering projects that are acknowledged to have a direct impact on the bottom line.[1]

> "[A]dversarial automation is being used to create and launch new attacks at such a rate and volume that **every strain of malware** must now be considered a **zero day**, and **every attack** considered an **advanced persistent threat**."[8]

Unfortunately, one result of this new status and visibility is added stress and complexity for the CIO. IT systems are now so critical that downtime often means full cessation of business. Yet, technology sprawl and siloed infrastructures mean that latency—if not downtime—is always a possibility. Half of CIOs rate their IT/business alignment at moderate or worse,[2] and 65% expect the skills shortage to impact their teams in the short to medium term.[3]

Security: An Added Stressor for IT Leaders

Cybersecurity is another consistent headache for CIOs. Once viewed as a back-office function, it is now discussed in 89% of board meetings.[4] This increased visibility means that at many organizations, the CISO is now a peer to the CIO,[5] reporting to the CEO or even to the board of directors. Other CIOs retain full responsibility for security—especially at smaller enterprises.

Whether the CISO is a member of the CIO's team or not, it is clear CIOs spend significant time on security issues,[6] with special focus on how security incidents—and security controls—affect operations. Changes in the threat landscape can seem daunting from the CIO's new, sometimes less direct vantage point. Not too long ago, threat detection and prevention were more clearly defined, and incident response was more tactical. Reactive approaches involving manual processes and disconnected tools were adequate, as threat actors' tactics were less advanced.

This is no longer the case. Organizations now must protect a widely distributed network that includes services in multiple public and private clouds, network traffic on the public internet, and data from a rapidly growing array of Internet-of-Things (IoT) devices.[7] This expanded attack surface is a big contributor to the increasing complexity of the security architecture—and a driver of operational inefficiency and increased cost.

These factors would pose problems for the CIO even if the threat landscape were static, which is far from the case. In fact, threats are dramatically increasing in *volume*, *velocity*, and *sophistication*, and this exacerbates the problem exponentially.

Increased Volume: Taxing Staff Resources

As threat actors move to more automated methods of disseminating malware and other threats, CIOs and security teams can be overwhelmed by the sheer volume of threat alerts, eliciting a feeling that they are "constantly firefighting."[9] According to data from FortiGuard Labs, the number of new malware variants increased by 129% over the course of this past year—and the trend has remained undaunted this year.[10] Additionally, Fortinet's Threat Landscape Index, first developed a year ago, shows high volatility and an upward trend in overall threats.[11]

What is more, some of the most staff-intensive incidents—unknown or zero-day attacks—are increasing exponentially. Analysis by FortiGuard Labs shows that up to 40% of new malware detected on a given day is now zero day or previously unknown.[12] When zero-day attacks occur, overwhelmed IT and security staff is forced into a reactive mode, doing what they can do to manually remediate things quickly—and this can cause operational problems in the longer term.

"The battleground of the future is digital, and AI is the undisputed weapon of choice."[23]

One study, for example, finds that 47% of security professionals do not believe their teams collect adequate information on attacks to take proactive action.[13] But even when the information exists, IT and security teams are not able to act on it in many cases. More than one-third of security professionals list keeping up with the volume of security alerts as a top incident response challenge.[14] And 42% say their organization ignores a significant number of alerts because they cannot keep up with the volume.

To make matters worse, the proliferation of IoT devices, many of which have little or no security built in, is one indicator that threat volumes will only accelerate. One analysis finds that 1 million IoT devices are being added to corporate networks every day and projects that 25% of all attacks will target IoT devices by 2020.[15]

Increased Velocity: Rendering Manual Response Useless

Historically, cyberattacks moved at human speed, with actual people manually executing each step of an attack.[16] This meant that manual processes, at bare minimum, had a decent chance of catching an exploit before it caused major damage. Now, bad cyber actors are automating many of their practices to enable them to carry out attacks at machine speed. The result: it still takes months for an organization to discover the typical breach, but exfiltration of corporate data can now occur in a matter of minutes.[17]

Early automation efforts by cyber criminals involved highly repeatable actions, exemplified by the distributed denial-of-service (DDoS) attack.[18] Adversaries are now raising the stakes by using emerging technologies to accelerate the execution of attacks of all kinds. For example, there is evidence that adversaries are now laying the groundwork for using swarm technology to decrease the time required for a botnet to breach a system or disrupt customer-facing services.[19] The Hide 'N Seek IoT botnet is something of a prototype of this approach, "communicat[ing] in a decentralized manner using custom-built peer-to-peer communication to implement a variety of malicious routines."[20]

As the velocity of attacks increases, any manual step in the process of detecting and responding to threats poses risk to an organization. It also reduces operational efficiency and places more burden on already overwhelmed IT and cybersecurity team members.

Increased Sophistication: Creating a Technology Arms Race

Cyber actors' efforts to speed up their attacks is just one element of their use of advanced technology to make their attacks more targeted—and more effective. Not too long ago, a signature-based antivirus solution stopped a good percentage of threats, as malware was mass-produced and reused repeatedly in identical form. That is no longer the case. In fact, 97% of viruses now change their characteristics on the fly using polymorphism,[21] meaning that a signature extracted minutes ago could be useless in thwarting a virus's spread. It is an example of the increased technological sophistication that is inherent in the current threat landscape.

There are many other examples of growing sophistication of threats. To name just a few:

- Spear phishing uses natural language processing (NLP) and data-scraping technology to target specific individuals with credible-looking malicious emails based on their social and work context.[22] Such advances threaten to disrupt operations because even employees who are able to spot traditional phishing emails may not recognize a spear-phishing message as a threat.

- Ransomware is becoming more targeted to specific organizations, and U.S. local governments have been a favored victim in recent months.[24] From Baltimore to the San Francisco Muni system, these attacks have paralyzed operations and cost millions of dollars in ransoms and remediation costs in recent years and even months.[25]
- Cryptojacking is now available "as a service" to cyber criminals who possess little expertise and comes with new features that disable security solutions and open communications ports on existing firewalls.[26] The cryptocurrency mining software installed on victims' machines leeches CPU resources and processing power, dramatically slowing system efficiency.
- Advanced post-intrusion obfuscation and anti-analysis techniques enable malware to detect when it is running in a sandbox or emulator, disable security tools on infected systems, and use junk data to make disassembly harder.[27]
- Exploits targeting the remote desktop protocol (RDP) on Microsoft Windows systems have been made privately available within cyber-criminal networks—making the attack vector available to nonspecialists.[28]

"Cybersecurity is no longer just a technology concern but an existential enterprise threat, and organizations are looking to CIOs to manage this major category of business risk." [31]

Cyber criminals are now using some of the most advanced technology available to accomplish their aims. The Emotet Trojan is an example of a prototype attack that is truly powered by artificial intelligence (AI) and machine learning (ML).[29] Distributed via email and typically sent in the form of invoices that are supposedly owed by the recipient, the authors recently added a module that exfiltrates email threads and enables cyberattackers to insert themselves into email threads using contextually accurate language that is fully automated. Impersonating trusted users in a convincing way increases the likelihood that recipients will open the attachment that installs malware on their machines.

Conclusion: A Different Approach Is Needed

Cyber crime becomes more costly every year,[30] and the current advanced threat landscape exacerbates the risk by making it more challenging for organizations to defend against exploits. Today's threat actors employ advanced technologies that enable targeted multivector attacks, propagate polymorphic malware, and shrink windows for detection, prevention, and response. Many businesses are simply unable to keep pace with the sophistication, volume, and velocity of threats.

In this context, traditional approaches based on an assortment of disaggregated security solutions will inevitably fail. Whether or not a CIO retains ownership of day-to-day security, he or she should challenge the organization to rethink its overall approach to security—in terms of technology, people, and processes.

[1] "Mastering the New Business Executive Job of the CIO: Insights From the 2018 CIO Agenda Report," Gartner Executive Programs, accessed August 1, 2019.

[2] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, accessed August 1, 2019.

[3] Ibid.

[4] "NACD Director's Handbook on Cyber-Risk Oversight," National Association of Corporate Directors, January 11, 2017.

[5] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[6] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[7] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed August 1, 2019.

[8] Saumitra Das, "When Every Attack Is a Zero Day," Dark Reading, April 23, 2019.

[9] "Security Teams Overwhelmed by Rising Volume of Attacks," Dark Reading, May 31, 2017.

[10] "Threat Landscape Report Q3 2018," Fortinet, accessed August 1, 2019.

[11] "Threat Landscape Report Q1 2019," Fortinet, accessed August 1, 2019.

[12] According to internal data from FortiGuard Labs.

[13] "Security Teams Overwhelmed by Rising Volume of Attacks," Dark Reading, May 31, 2017.

[14] Jon Oltsik, "Dealing with Overwhelming Volumes of Security Alerts," ESG, March 3, 2017.

[15] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed August 1, 2019.

[16] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

[17] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[18] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

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

[20] Ibid.

[21] Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[22] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

[23] William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.

[24] "Threat Landscape Report Q2 2019," Fortinet, accessed August 7, 2019.

[25] Niraj Chokshi, "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next," The New York Times, May 22, 2019; Samuel Gibbs, "Ransomware attack on San Francisco public transit gives everyone a free ride," The Guardian, November 28, 2016.

[26] Jon Bove, "An Approach for Securing Advanced Threats for Your Customers," Fortinet, January 30, 2019.

[27] "Threat Landscape Report Q2 2019," Fortinet, accessed August 7, 2019.

[28] Ibid.

[29] Meg King and Jacob Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," The Wilson Center, November 28, 2018.

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

[31] Stephanie Overby, "7 security to-do's for CIOs in 2019," The Enterprisers Project, December 12, 2018.

www.fortinet.com

August 27, 2019 9:37 AM

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:WP-Advanced-Threat-CIOs-Time-Bomb:wp-advanced-threats-cios-time-bomb Folder:wp-advanced-threats-cios-time-bomb