FORTINET

WHITE PAPER

Advanced Threats: Keeping CISOs on Their Toes

Increasingly Complex Tactics by Adversaries Can Put Security Teams in Reactive Mode

Executive Summary

CISOs enjoy a greater status within organizations than ever before. But the reason for this new stature is that cybersecurity poses increasing and more direct threats to corporate profitability—and even survival. As if an expanding attack surface and growing security complexity were not enough, the threat landscape is evolving rapidly, requiring a strategic approach on the part of security teams.

Advanced threats are steadily increasing in volume, velocity, and sophistication, rendering traditional, manual approaches to security useless. Specifically, reliance on a fragmented security architecture requires manual processes that reduce efficiency, expand risk, and endanger network performance. CISOs who rely on reactive, tactical security approaches are simply unprepared to keep pace with the speed and sophistication of the threat landscape.

"[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]

Few executive roles have risen more in visibility and importance in the past decade than that of the CISO. The job title has existed for a decade or less at many organizations—and the world's first CISO was appointed just 25 years ago.[1] Over the years, the responsibilities of the CISO have grown steadily,[2] and CISOs find themselves in a more prominent position than ever before.[3] A majority now report directly to the CEO or even to the board of directors,[4] making them a peer to the CIO—leading a parallel organization focused solely on security.

But along with the increased prestige comes more scrutiny from top management than ever before. Once viewed as a back-office function, cybersecurity is now discussed in 89% of board meetings.[5] This increase in emphasis is warranted, as the risks and costs associated with cybersecurity have intensified dramatically over the past decade. As an example, one study found that cyber crime currently costs the typical organization $13 million—a 12% year-over-year increase and a 72% increase over five years.[6]

Facing Increasingly Sophisticated Foes

In a world of ever-increasing risk, protecting networks against the latest strategies and methods used by cyber criminals can seem daunting even to a seasoned cybersecurity leader. 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 sufficient in many instances, as threat actors' methods were less advanced and most IT assets were contained within the data center.

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 on the security team.

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

Increased Volume: Taxing Staff Resources

As threat actors move aggressively to research and carry out more automated methods of disseminating malware and other threats, CISOs and their 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 it has remained undaunted this year.[10] And Fortinet's Threat Landscape Index, developed a year ago, has so far showed 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 problems in the longer term.

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. Over one-third of security professionals list keeping up with the volume of security alerts as one of their top challenges.[14] And 42% of them say their organization ignores a significant number of alerts because they cannot keep up with the volume. The result is that exfiltration of corporate data can now happen in minutes while the discovery of the typical breach still takes months.[15]

42% of security professionals indicate they ignore a significant number of threat 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.[16]

Increasingly Velocity: Rendering Manual Response Useless

Historically, cyberattacks moved at human speed, with actual people manually executing each step of an attack.[17] This meant that manual processes at least 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.

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 now evidence that adversaries are laying the groundwork for using swarm technology to decrease the time required for a botnet to breach a system.[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] Further, there are indicators that cyber criminals are beginning to use AI to enable accelerated fuzzing to discover new application vulnerabilities—turning a longtime tool of the good guys into another method of attack.[21]

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 security 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,[22] 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.[23] 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 are a favored victim in recent months.[24] From the city of Baltimore to the San Francisco Muni system, these attacks have paralyzed operations and cost millions of dollars in ransoms and remediation costs in recent months and years.[25]

- Cryptojacking is now available "as a service" to cyber criminals with less expertise, with new features that disable security solutions and open communications ports on existing firewalls.[26] The cryptocurrency mining software installed on victims' machines leaches CPU resources and processing power, dramatically slowing system efficiency.
- Advanced 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 older Microsoft Windows systems have been made privately available within cyber-criminal networks—making the attack vector available to nonspecialists.[28]

Cyber criminals now use 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 ongoing conversations 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.

"The battleground of the future is digital, and AI is the undisputed weapon of choice."[30]

CISOs find themselves "not only carrying out **day-to-day operations,** but also **studying to learn of new risks."**[31]

Conclusion: A Different Approach Is Needed

The current advanced threat landscape makes it more challenging for CISOs and their teams to defend against exploits, exacerbating business risks that were already steadily growing. 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 and manual processes will inevitably fail—even if each individual tool is effective or even best of breed. This problem cannot be solved with another point product or a tweaking of policies and processes. Rather, CISOs must rethink their overall approach to security—in terms of technology, people, and processes.

[1] Steve Katz is credited as the first CISO, starting with Citigroup in 1994. See Demetrios Lazarikos, "CISO: The Evolution Of The Species," ITSP Magazine, September 19, 2016.

[2] Todd Fitzgerald, "The 5 Stages of CISO Success, Past & Future," Dark Reading, January 25, 2019.

[3] "2018 Global State of Information Security Survey," IDG, December 8, 2017.

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

[5] "NACD Director's Handbook on Cyber-Risk Oversight," National Association of Corporate Directors, January 12, 2017.

[6] "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture Security and Ponemon Institute, accessed March 12, 2019.

[7] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed September 11, 2018.

[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 Q4 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] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[16] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed August 1, 2019.

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

[18] Ibid.

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

[20] Ibid.

[21] Derek Manky, "Using Fuzzing to Mine for Zero-Days," Threatpost, December 7, 2018.

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

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

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

[31] Quote from survey respondent, "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

September 21, 2019 5:36 AM

D:\Fortinet\White Paper\CISO Problem Education\wp-advanced-threats-keeping-cisos-on-their-toes-v2.1

440502-0-0-EN