The Threat That Never Goes Away

Digital Technology Gives, Digital Technology Takes Away

Table of Contents

Executive Overview

While digital acceleration and work-from-anywhere strategies may have been driven by the uncertain times brought about by the global pandemic, they remain essential for any organization competing in today's digital marketplace. However, that network transformation has also expanded the attack surface organizations need to protect, much of it in new, vulnerable edges. And cyber criminals have already begun targeting these new threat vectors with advanced malware and attack strategies.

Part of the challenge for IT teams is that there is just a lot more to protect. The need for new devices and software to support digital acceleration efforts has contributed to the growing volume of vulnerabilities being targeted by new or improved cyber threats. Keeping solutions patched and updated has always been a challenge for many organizations, but today's distributed devices and applications have made this even more difficult. And the problem is complicated further as the growing number of home networks leverages personal technologies to access business applications deployed in hybrid cloud and on-premises environments. And the opportunities for compromise continue to grow due to Common Vulnerabilities and Exposures (CVEs)—the list of publicly disclosed computer security flaws—reaching an all-time high in 2021[1] and expected to continue to grow further during 2022.

Is There Such a Thing as Bad AI?

Organizations are also seeing increasingly sophisticated threats—many enhanced with automation and artificial intelligence (AI)—targeting high-priority sectors such as critical infrastructure, healthcare, information technology, financial services, and energy. Ransomware, in particular, has become a significant concern to most organizations. 85% of respondents to a recent survey[2] indicated that they are more concerned about ransomware than any other cyber threat. That may be, in part, due to two-thirds of those organizations reporting they have already been a ransomware target—with nearly half saying they have been targeted more than once.

If It Works, Why Change?

Part of the reason for the prevalence of ransomware is that it offers a low-investment, high-profit business model that's irresistible to cyber criminals. In fact, according to the mid-year 2021 FortiGuard Labs Threat Landscape Report,[3] ransomware incidents increased nearly elevenfold from 2020 to 2021. While there are several tangible reasons behind that growth, it is clearly being driven by new Ransomware-as-a-Service (RaaS) solutions being offered on the dark web that make it much easier for less technically competent criminals to get involved. And in addition to renting ransomware, some criminal operations have begun selling access to compromised corporate networks, adding help desk services, and providing additional services, such as determining optimal ransom amounts, negotiating ransoms, and laundering money.

“Bad actors now operate as large, distributed businesses, complete with call centers to handle ransom payments. Many such organizations target large corporations and industries or high-profile individuals to get the best payouts—a strategy known as ‘Big Game Hunting’ (BGH).”[4]

But it's not just the volume of ransomware attacks that has increased. It's also their ferocity. Cyber criminals have added new levels of extortion to get victims to pay. These include combining encryption with doxing (the threat of publicly exposing internal data), adding distributed denial-of-service (DDoS) attacks to create additional confusion and panic, and most recently, reaching out directly to victims' customers and stakeholders to have them put further pressure on the victim to pay. And according to the FBI,[5] cyber criminals are also actively searching for organizations nearing the completion of a significant financial event, such as a merger or public stock offering. Once such a target has been located, they breach the network to obtain confidential details of these activities before launching their ransomware attack. Then, if the victim doesn't quickly pay their ransom, they threaten to disclose this information publicly, potentially resulting in investor backlash or causing such activities to be postponed or fail.

There's More Than One Game in Town

Ransomware is not the only form of malware on the rise. According to Microsoft,[6] increasingly sophisticated attacks use techniques that make them harder to detect. For example, "nation-state actors are engaging in new reconnaissance techniques that increase their chances of compromising high-value targets, criminal groups targeting businesses have moved their infrastructure to the cloud to hide among legitimate services, and attackers have developed new ways to scour the internet for systems vulnerable to ransomware."

Similarly, the number of phishing sites reported to the Anti-Phishing Working Group (APWG) is now 10 times what it was a decade ago, with phishing attacks doubling since 2020.[7] FortiGuard Labs reported that botnet activity jumped from 35% to 51% of all companies during the first six months of 2021. And threat actors are increasing their investment in automation and AI,[8] purchasing tools and developing attacks that allow them to increase their criminal activities' speed, effectiveness, and value.

Phishing remains an effective and profitable activity for cyber criminals, with credential phishing being used in many of the most damaging attacks.[9]

Effective Protection Begins With Change

Today's sophisticated threats, especially multi-step attacks, require a unified defense that can automatically prevent, disrupt, and limit attacks in real time. However, the increasing complexity of security deployments, with literally dozens of tools operating in silos across the network, contributes to an inability to effectively detect and respond to threats.

Organizations need to add new detection and response-oriented tools to their traditional prevention controls. This includes moving toward a structured platform architecture that supports the convergence of security and networking functions and consolidates traditionally disparate devices into a unified solution. Unless security technologies are deeply integrated, automated detection and response to threats are nearly impossible. Even AI-enhanced systems cannot compensate for the inherent inability of legacy security devices to share and correlate threat intelligence or participate in a coordinated response, let alone detect complex attacks designed to evade detection.

This structured approach to cybersecurity is the most effective strategy for addressing the rise of today's sophisticated security threats, providing seamless visibility and granular control across the entire digital attack surface—even those networks that are highly distributed or in a constant state of flux. It starts by consolidating key security technologies onto a universally deployable security platform and then deeply integrating traditionally disparate solutions through open application programming interfaces (APIs) and common standards.

This approach helps minimize or eliminate the complexity of deploying and supporting multiple point products. It also enables the automation of security workflows to increase the speed and accuracy of detection and respond to threats in a coordinated fashion. It also allows security to be more deeply integrated with the underlying network, eliminating issues that arise when hybrid networks, cloud-based applications and services, and connectivity constantly shift to meet evolving business and user requirements.

[1] "A record number of software vulnerabilities was reported in 2021," The Stack, December 7, 2021.

[2] "Fortinet Ransomware Survey Shows Many Organizations Unprepared," Fortinet, September 29, 2021.

[3] "FortiGuard Labs Threat Landscape Report Highlights Tenfold Increase in Ransomware," FortiGuard Labs, August 23, 2021.

[4] Aamir Lakhani, "Analyzing the History of Ransomware Across Industries," Fortinet, May 17, 2021.

[5] "Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims," FBI, November 3, 2021.

[6] "Microsoft Digital Defense Report," Microsoft, September 2020.

[7] "Phishing Smashes All Previous Records in Q3, 2021; Phishing Attacks Double Since Early 2020," APWG, November 22, 2021.

[8] Kyle Wiggers, "Dear enterprise IT: Cybercriminals use AI too," VentureBeat, June 17, 2021.

[9] "Phishing Activity Trends Report, APWG, November 24, 2021.

FORTINET®

www.fortinet.com

February 2, 2022 11:29 PM

1413321-0-0-EN