FORTINET

Source: *Fortinet, Inc.*

August 12, 2020 09:00 ET

FortiGuard Labs Reports Cyber Adversaries Are Exploiting the Global Pandemic at Enormous Scale

Cyber Criminals Targeting Remote Work to Gain Access to Enterprise Networks and Critical Data

SUNNYVALE, Calif., Aug. 12, 2020 (GLOBE NEWSWIRE) --

Derek Manky, Chief, Security Insights & Global Threat Alliances, FortiGuard Labs

“The first six months of 2020 witnessed an unprecedented cyber threat landscape. The dramatic scale and rapid evolution of attack methods demonstrate the nimbleness of adversaries to quickly shift their strategies to maximize the current events centered around the COVID-19 pandemic across the globe. There has never been a clearer picture than now, of why organizations need to adjust their defense strategies going forward to fully take into account the network perimeter extending into the home. It is critical for organizations to take measures to protect their remote workers and help them secure their devices and home networks for the long term. It is also wise to consider adopting the same strategy for cyber viruses that we are adopting in the real world. Cyber social distancing is all about recognizing risks and keeping our distance.”

News Summary:
Fortinet® (NASDAQ: FTNT), a global leader in broad, integrated, and automated cybersecurity solutions, today announced the findings of the latest semiannual FortiGuard Labs Global Threat Landscape Report.

- FortiGuard Labs threat intelligence from the first half of 2020 demonstrates the dramatic scale at which cybercriminals and nation-state actors leveraged a global pandemic as an opportunity to implement a variety of cyberattacks around the world. The adaptability of adversaries enabled waves of attacks targeting the fear and uncertainty in current events as well as the sudden abundance of remote workers outside the corporate network, which quickly expanded the digital attack surface overnight.
- Although many compelling threat trends were related to the pandemic, some threats still had their own drivers. For example, ransomware and attacks targeting Internet-of-Things (IoT) devices as well as operational technology (OT) are not diminishing, but are instead evolving to become more targeted and more sophisticated.
- At a global level, the majority of threats are seen worldwide and across industries, with some regional or vertical variation. Similar to the COVID-19 pandemic, a certain threat might have started in one area but eventually spreads almost everywhere, meaning most organizations could face the threat. There are of course regional differences in infection rates based on factors such as policies, practices, or response.
- For a detailed view of the report, as well as some important takeaways, read the blog. Highlights of the report follow.

Seizing the Opportunity in Global Events: Attackers have used subjects in the news as social engineering lures before, but this moved to the next level in the first half of 2020. From opportunistic phishers to scheming nation-state actors, cyber adversaries found multiple ways to exploit the global pandemic for their benefit at enormous scale. This included phishing and business email compromise schemes, nation-state-backed campaigns and ransomware attacks. They worked to maximize the global nature of a pandemic that affected everyone around the world combined with an immediately expanded digital attack surface. These trends were seen with other newsworthy items and demonstrate how quickly attackers can move to take advantage of major developments with broad social impact at a global level.

The Perimeter Gets More Personal: The increase in remote work created a dramatic inverse of corporate networks almost overnight, which cyber adversaries immediately started to leverage as an opportunity. In the first half of 2020, exploit attempts against several consumer-grade routers and IoT devices were at the top of the list for IPS detections. In addition, Mirai and Gh0st dominated the most prevalent botnet detections, driven by an apparent growing interest of attackers targeting old and new vulnerabilities in IoT products. These trends are noteworthy because it demonstrates how the network perimeter has extended to the home with cybercriminals seeking to gain a foothold in enterprise networks by exploiting devices that remote workers might use to connect to their organizations' networks.

Browsers Are Targets Too: For attackers the shift to remote work was an unprecedented opportunity to target unsuspecting individuals in multiple ways. For example, web-based malware used in phishing campaigns and other scams outranked the more traditional email delivery vector earlier this year. In fact, a malware family that includes all variants of web-based phishing lures and scams ranked at the top for malware in January and February and only dropped out of the top five in June. This may demonstrate the attempt of cybercriminals to target their attacks when individuals are the most vulnerable and gullible—browsing the web at home. Web browsers, not just devices, are also prime targets for cybercriminals, perhaps more than usual, as cybercriminals continue to target remote workers.

Ransomware Not Running Away: Well-known threats such as ransomware have not diminished during the last six months. COVID-19-themed messages and attachments were used as lures in a number of different ransomware campaigns. Other ransomware was discovered rewriting the computer's master boot record (MBR) before encrypting the data. In addition, there was an increase in ransomware incidents where adversaries not only locked a victim organization's data but stole it as well and used the threat of widescale release as additional leverage to try and extort a ransom payment. The trend significantly heightens the risks of organizations losing invaluable information or other sensitive data in future ransomware attacks. Globally, no industry was spared from ransomware activity and data shows that the five most heavily targeted sectors for ransomware attacks are telco, MSSPs, education, government, and technology. Unfortunately, the rise of ransomware being sold as a service (RaaS) and the evolution of certain variants indicates that the situation with ransomware is not going away.

OT Threats After Stuxnet: June marked the 10th anniversary of Stuxnet, which was instrumental in the evolution of threats to, and security of, operational technology. Now, many years later, OT networks remain a target for cyber adversaries. The EKANS ransomware from earlier this year shows how adversaries continue to broaden the focus of ransomware attacks to include OT environments. Also, the Ramsay espionage framework, designed for the collection and exfiltration of sensitive files within air-gapped or highly restricted networks, is an example of threat actors looking for fresh ways to infiltrate these types of networks. The prevalence of threats targeting supervisory control and data acquisition (SCADA) systems and other types of industrial control systems (ICS) is less in volume than those affecting IT, but that does not diminish the importance of this trend.

Mapping Exploitation Trends: A review of the CVE List shows the number of published vulnerabilities added has risen over the last few years, sparking discussion over the prioritization of patching. Even though 2020 looks to be on pace to break the number of published vulnerabilities in a single year, vulnerabilities from this year also have the lowest rate of exploitation ever recorded in the 20-year history of the CVE List. Meanwhile, vulnerabilities from 2018 claimed the highest exploitation prevalence at 65%, and more than a quarter of organizations registered attempts to exploit 15-year-old CVEs. For cyber adversaries, exploit development at scale and distribution via legitimate and malicious hacking tools continues to take time.

The Urgency to Secure the Network Perimeter Extending Into the Home
With the increase in connectivity, devices, and ongoing need for remote work, the digital attack surface is expanding. With the corporate network perimeter extending to the home, attackers are looking for the weakest link and fresh attack opportunities. Organizations need to prepare by taking concrete steps to protect their users, devices and information in ways similar to the corporate network. Threat intelligence and research organizations can help by providing broad insight as the threat landscape evolves as well as in-depth analysis of attack methods, actors, and new tactics to help supplement the cyber knowledge of organizations. The need for secure teleworker solutions to enable secure access to critical resources while scaling to meet the demands of the entire workforce has never been greater. Only a cybersecurity platform designed to provide comprehensive visibility and protection across the entire digital attack surface–including networked, application, multi-cloud, or mobile environments–is able to secure today's rapidly evolving networks.

Report Overview
This latest Global Threat Threat Landscape Report is a view representing the collective intelligence of FortiGuard Labs, drawn from Fortinet's vast array of sensors collecting billions of threat events observed around the world during the first half of 2020. It covers global and regional perspectives as well as research into three central and complementary aspects of that landscape: exploits, malware, and botnets.

Additional Resources

- Read our blog for valuable takeaways from this research or access the full report.
- Read about how Fortinet telework solutions enable secure remote access at scale to support employees with a wide array of access requirements.
- Learn more about FortiGuard Labs threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.
- Find out how the Fortinet Security Fabric platform delivers broad, integrated, and automated protection across an organization's entire digital infrastructure.
- Learn more about Fortinet's free cybersecurity training initiative or about the Fortinet Network Security Expert program, Network Security Academy program, and FortiVet program.
- Engage in our Fortinet user community (Fuse). Share ideas and feedback, learn more about our products and technology, or connect with peers.
- Follow Fortinet on Twitter, LinkedIn, Facebook, YouTube, and Instagram.

About FortiGuard Labs
FortiGuard Labs is the threat intelligence and research organization at Fortinet. Its mission is to provide Fortinet customers with the industry's best threat intelligence designed to protect them from malicious activity and sophisticated cyberattacks. It is comprised of some of the industry's most knowledgeable threat hunters, researchers, analysts, engineers and data scientists in the industry, working in dedicated threat research labs all around the world. FortiGuard Labs continuously monitors the worldwide attack surface using millions of network sensors and hundreds of intelligence-sharing partners. It analyzes and processes this information using artificial intelligence (AI) and other innovative technology to mine that data for new threats. These efforts result in timely, actionable threat intelligence in the form of Fortinet security product updates, proactive threat research to help our customers better understand the threats and threat actors they face, and by providing specialized consulting services to help our customers identify and strengthen their security exposures. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networked, application, multi-cloud or edge environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 465,000 customers trust Fortinet to protect their businesses. Both a technology company and a learning organization, the Fortinet Network Security Expert (NSE) Training Institute has one of the largest and broadest cybersecurity training programs in the industry. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, contract, binding specification or other binding commitment by Fortinet or any indication of intent related to a binding commitment, and performance and other specification information herein may be unique to certain environments. This news release may contain forward-looking statements that involve uncertainties and assumptions, such as statements regarding technology releases among others. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

Media Contact:	**Investor Contact:**	**Analyst Contact:**
John Welton	Peter Salkowski	Ron Davis
Fortinet, Inc.	Fortinet, Inc.	Fortinet, Inc.
408-235-7700	408-331-4595	415-806-9892
pr@fortinet.com	psalkowski@fortinet.com	rdavis@fortinet.com