Improve Ransomware Attack Resiliency with NetSPI's New Ransomware Attack Simulation

written by Team NetSPI | June 17, 2021

Through the tech-enabled service, organizations can put their ransomware prevention and detection capabilities to the test.

Minneapolis, Minnesota – NetSPI, the leader in enterprise penetration testing and attack surface management, today announced its new ransomware attack simulation service. In collaboration with its ransomware security experts, the new service enables organizations to emulate real world ransomware families to find and fix critical vulnerabilities in their cybersecurity defenses.

Recent ransomware attacks have exposed major cybersecurity gaps globally. In the U.S., the Biden administration is urging business leaders to take immediate steps to prepare for ransomware attacks. In a recent memo, deputy national security advisor for cyber and emerging technology Anne Neuberger recommends organizations, "use a third-party pentester to test the security of your systems and your ability to defend against a sophisticated [ransomware] attack."

"Paying a ransom doesn't guarantee your data is returned safely, yet, one in four companies worldwide pay the adversaries[I]," said Scott Sutherland, Practice Director at NetSPI. "Organizations must get more proactive with their security efforts to avoid paying the ransom and funding the cybercriminals. Ransomware families are both opportunistic and targeted – and no industry is exempt from falling victim to an attack."

“NetSPI is eager to help organizations achieve a more scalable and continuous assessment of their environment from the perspective of an adversary,” said Charles Horton, COO at NetSPI. “The addition of the ransomware attack simulation service to our adversary simulation solutions will further help organizations strengthen their defenses and become more resilient against ransomware attacks.”

During a ransomware attack simulation engagement, NetSPI closely collaborates with organizations to simulate sophisticated ransomware tactics, techniques, and procedures (TTPs) using its custom-built breach and attack simulation technology. Following each engagement, organizations gain access to NetSPI’s technology to run custom plays on their own and continuously evaluate how well their cybersecurity program will hold up to a ransomware attack.

Learn more about NetSPI’s ransomware attack simulation online here and download The Ultimate Guide to Ransomware Attacks for insights on how to prevent and respond to a ransomware attack.

[I] SonicWall 2021 Cyber Threat Report; https://www.sonicwall.com/2021-cyber-threat-report/

About NetSPI

NetSPI is the leader in enterprise security testing and attack surface management, partnering with nine of the top 10 U.S. banks, three of the world's five largest healthcare companies, the largest global cloud providers, and many of the Fortune® 500. NetSPI experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces, historically testing over 1 million assets to find 4 million unique vulnerabilities. NetSPI offers Penetration Testing as a Service (PTaaS) through its Resolve™ platform and adversary simulation through its Red Team Toolkit. NetSPI is headquartered in Minneapolis, MN and is a portfolio company of private equity firms Sunstone Partners, KKR, and Ten Eleven Ventures. Follow us on Facebook, Twitter, and LinkedIn.

Contact:
Tori Norris
Marketing Manager, NetSPI
victoria.norris@netspi.com
(630) 258-0277