Hackers Corner
MSP Attacks

Background

Over the last two years, managed service providers (MSPs) have experienced first-hand the growing trend in supply chain attacks. In April 2017, amid growing tensions between the United States and China, US-CERT issued an alert[1] detailing an emerging threat impacting service providers across multiple sectors. In late 2018, a more specific warning[2] about advanced persistent threats (APT's) actively targeting MSPs was released, and the first alert was updated two months later following the indictment[3] of two Chinese hackers who were associated with the Chinese Ministry of State.

Radware researchers, in parallel with Radware's Emergency Response Team (ERT), have been monitoring this growing trend targeting MSPs. While this vertical is typically targeted by APTs, several events over the last few months indicate that less sophisticated groups are looking to attack MSPs, thereby exploiting the relationship between MSPs and their clients.

MSPs provide remote management services for their clients' infrastructure, including the ability to push an update or install applications. Because of this, hackers (both sophisticated and non-sophisticated) are targeting the networks of global MSPs with the goal of maximizing their impact via a trickle-down strategy.

Corporate Insight

While threat actors are increasingly targeting supply chains, they each bring a different set of Tactics, Techniques, and Procedures (TTP), as well as objectives to the table. Understanding your company's exposure could help prevent future attacks. APT's and nation-state hackers typically target MSPs for espionage purposes while organized cybercriminals are looking for any data or Personal Identifiable Information (PII) they can sell or commit fraud with. Even extortionist have been observed launching ransomware campaigns against MSPs.

Advice

Implementing the right defensive barriers makes it more difficult for cybercriminals and APTs to gain access and maintain persistence inside your network. For protection against these types of advanced threats, organizations should consider a defense in depth defense solution that delivers visibility, resilience, scalability, security, and control to mitigate today's most sophisticated risks for their clients effectively.

---

[1] https://www.us-cert.gov/ncas/alerts/TA17-117A

[2] https://www.us-cert.gov/ncas/alerts/TA18-276B

[3] https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Under Attack and in Need of Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.