UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00078

FIREEYE SUFFERS SUSPECTED STATE ATTACK

DATE ISSUED: 15th December 2020

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	[✓ HARD]	MEDIUM	EASY

OVERVIEW

FireEye has become the recent victim of a highly sophisticated attack, suspected to be state based, in which their RedTeam hacking tools have been uplifted. Attackers also sought to exfiltrate information about FireEye's customer base, particularly those with governmental associations.

BREAKDOWN

The manner in which the attack was been conducted have lead the team at FireEye to believe the attack seen last week was state-sponsored. The team appeared to be highly-skilled and disciplined with intricate knowledge of operational security and displaying highly advanced techniques. The breach has brought to light many never before seen attack methods and evasion techniques. With their custom penetration testing toolkit having been stolen, FireEye have released an advisory to assist those who may have concerns about future threats or compromise of their own networks. FireEye's choice to publicly announce the breach themselves as well as provide advice, assistance, and guidance is commendable and will hopefully encourage others to do the same in an effort to bring change to a positive reporting and disclosure culture globally.

REMEDIATION STEPS

- Check FireEye's advisory, countermeasures, and Indicators of Compromise (IOC) articles via their GitHub https://github.com/fireeye/red_team_tool_countermeasures
- Monitor networks and set up alerts to admins for suspicious behaviours

REFERENCES & RESOURCES

ZDNet:	https://www.zdnet.com/article/fireeye-one-of-the-worlds-largest-security-firms-discloses-security-breach/?ftag=TRE49e8aa0&bhid=29606343124056600886148366084033&mid=13195603&cid=2352480217