MEDIA ALERT: BugSec, Cynet Uncover Large-scale Vulnerability on Next Generation Firewalls

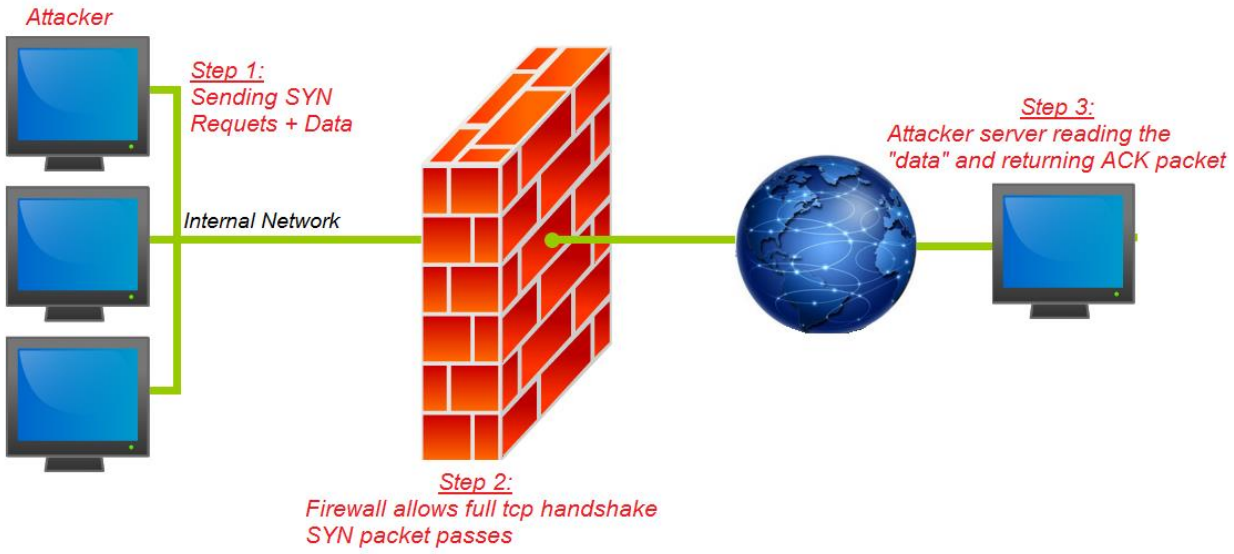
Hundreds of millions of enterprise networks worldwide open to attack

TEL AVIV, ISRAEL — December 9, 2015

BugSec Group Ltd., a leading provider of cyber security services (www.bugsec.com), and Cynet, pioneers of the all-in-one agentless solution for detection of advanced and unknown threats (www.cynet.com), announced today that they have discovered a severe vulnerability in next generation firewalls which allow an internal entity or malicious code to interact and extract data out of the organization, completely bypassing the firewall limitation.

Head of Offensive Security Stas Volfus discovered the vulnerability, dubbed FireStorm, on the application categorized module, which is designed to permit **full TCP handshake regardless of the packet destination.** This is done to allow the firewall to gather enough content for it to identify which application protocol is being used (web-browsing/telnet etc.). The firewalls allow web-browsing (HTTP/S) traffic from the LAN environment to specific locations on the internet (URL-Filtering).

This enabled the security research team to perform a full TCP Handshake via the HTTP port with a C&C (Command and Control) server hosted by BugSec. From there, the team was able to forge messages and tunnel them out through the TCP handshake process, bypassing the firewall to **any destination on the Internet regardless of firewall rules and restrictions.**



It is important to note that all traffic sent to the C&C server after the TCP handshake process was blocked immediately by the firewall, as the policy manager categorized the researchers' traffic as "Unknown-TCP" and the HTTP destination wasn't allowed.

“This is a critical flaw that enterprise networks need to be aware of,” said Chief Technology Officer Idan Cohen. “The ability to perform the TCP handshake process without any destination means that malware and hackers could hijack it to communicate with unauthorized servers on the web, completely removing the firewall block from the LAN to the outside world,” Cohen added.

Following the discovery, the security research team developed a tool that extracted sensitive data from the LAN, using only the TCP handshake. The tool allowed full tunneling over the TCP handshake.

The team disclosed full details of the vulnerability to major vendors affected by the flaw. One of the vendors, when informed of the issue, stated that they did not see it as a security threat. They said that once their state machine proceeded beyond the TCP handshake, they would recognize the application, matching a subsequent rule that applied to application traffic. The vendor added that if they did not recognize the application, they would treat the session as ‘unknown-TCP’ and, again, perform an additional security policy lookup to decide whether to allow or block the traffic.

The BugSec–Cynet security research team believes this is a major vulnerability, and recommends that monitor capability be added to provide blocking for repeated suspicious requests and to provide the ability to block a direct connection between an internal host and an unauthenticated foreign host.

To see full details of the vulnerability, read the blogpost at:
www.bugsec.com/blog
www.cynet.com/blog

About BugSec

BugSec Group is a leading offensive security consulting company, focused on ethical hacking, security research, cyber-attack simulations, SCADA, Incident Response, product security evaluation and other services to increase customer security. Since 2005, BugSec has been providing security consulting services to global companies in the fields of finance, defense, government, hi-tech, utilities and other markets. The BugSec team is made up of some of the world’s most talented offensive and defensive hacking experts and security research teams, who work together with intelligence and law enforcement organizations around the world to help our customers protect their assets.
www.bugsec.com

Follow BugSec at:
Facebook: www.facebook.com/bugsec
Twitter: www.twitter.com/bugsec_group
LinkedIn: www.linkedin.com/bugsec

About Cynet
Cynet is a pioneer of the all-in-one, agentless solution for detection and response of advanced and unknown threats, such as unsigned malware and zero day attacks. The company’s flagship product, Cynet 360, correlates and analyzes indicators from files, network, endpoints and user behavior to uncover threats, which have bypassed the prevention layer. Cynet’s integrated 24/7 SOC ensures the

validity of threats, assisting customers with remediation while eliminating false positives.
www.cynet.com

Follow Cynet at:
Facebook: www.facebook.com/cynet360
Twitter: www.twitter.com/cynet360
LinkedIn: www.linkedin.com/cynet-security

Press Contacts:
Inbal Aharoni
Marketing Manager
Mobile: +972-508776797
Email: inbala@cynet.com

David Leichner
VP Marketing & Sales
Mobile: +972-547799888
Email: davidl@cynet.com