‘String of Paerls’

Integrated Threat Defense – Visibility to Discover and Protect Against Socially Engineered Exploits

1 DISCOVERY

‘NEEDLE IN A HAYSTACK’

Email phishing campaign with a malicious Word invoice attachment undetected by traditional tools

Word launches malicious macro executable

Executable calls out to 3 external domains

- londonpaerl.co.uk
- selombiznet.in
- Dropbox

2 BIG DATA ANALYSIS

Real-time monitoring of londonpaerl.co.uk and selombiznet.in domain activity, directly tied to ‘String of Paerls’ attacker

Further analysis of the attacker’s network provides telemetry tying multiple other malware exploits to the same attacker

3 RETROSPECTIVE

AMP determined the Dropbox hosted files provide the payload and the two domains serve as command and control servers for the exploit

AMP tools were used throughout the discovery and analysis processs to expose the exploit

INTEGRATED THREAT DEFENSE

*Analysis was conducted on **45 days** worth of samples and clustered together based on a matching set of alert criteria. This process reduced more than **1 million** detailed sample reports to just over **15 thousand** sample clusters that exhibit similar behavior.*

For further reading:
blogs.cisco.com/security/a-string-of-paerls/
www.cisco.com/go/asafps

Source: research data gathered and analyzed by the Cisco Talos Security Intelligence and Research Group (Talos)