Cisco 2015
Midyear Security Report

Combination Attacks Evade Point Solutions

In the first half of 2015, malicious actors demonstrated an elevated level of attack sophistication that leveraged agility, destruction, adaptability, and speed to achieve their objectives. Angler, Rombertik, Adware MultiPlug, and Dridex are the top four most well-known examples of how these combination attacks evade detection, infiltrate defenses, and destroy systems.

Angler

Agility is Its Strength

Obfuscates compromised landing pages

Over 75% of domain shadowing activity leads to Angler

Encrypts payload for delayed analysis

Continually throws different **'hooks'** to increase effectiveness

Targets and exploits **unpatched software**

40% user penetration

Rombertik

Destructive if Modified

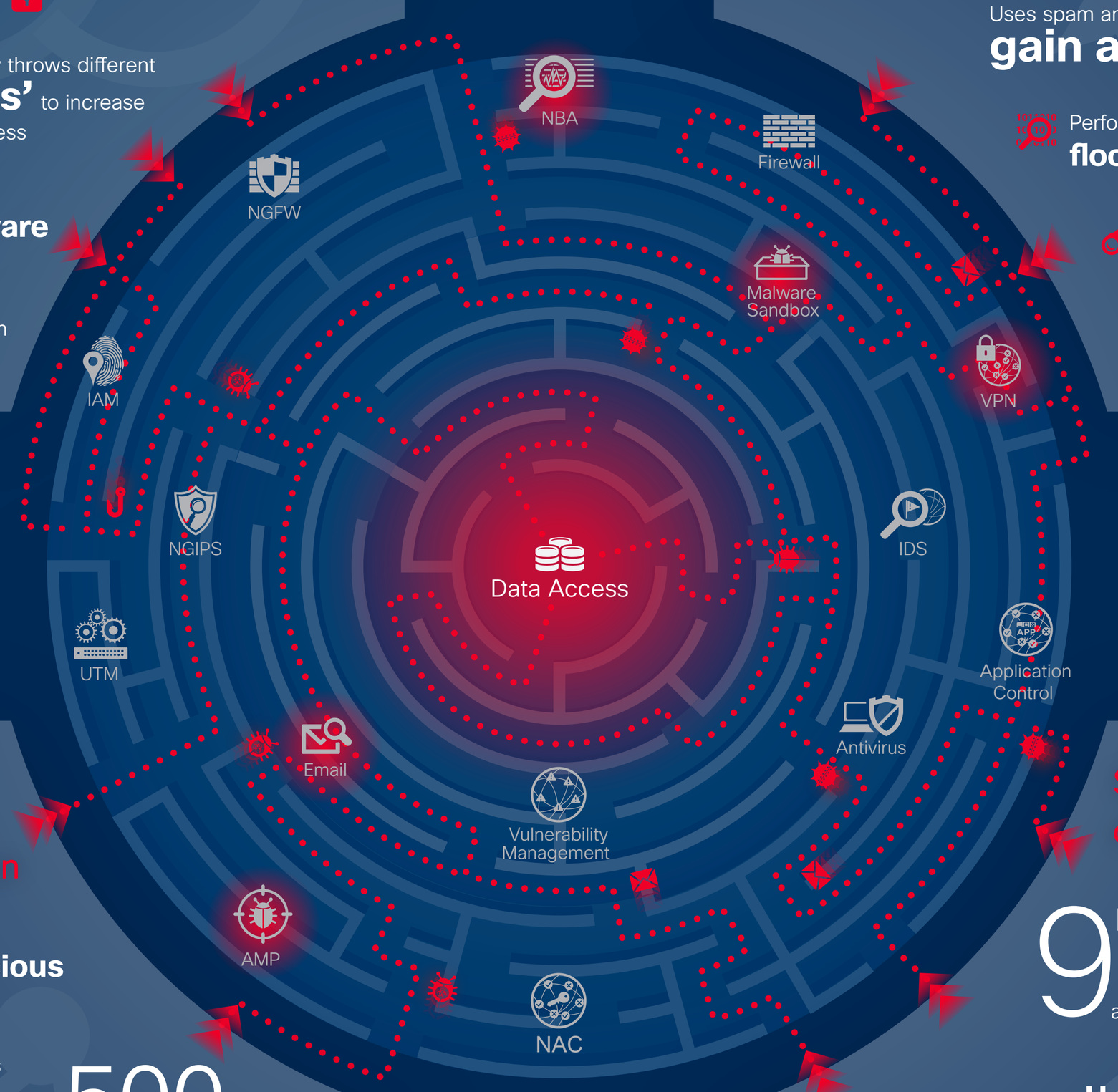
960M instructions to memory, creating a stalling tactic for sandboxes

Destroys master boot record and renders computer inoperable

Uses spam and phishing to **gain access**

Performs excessive activity to **flood tracing tools**

Once past sandbox, calls Windows API **335,000 times** as an anti-debugging mechanism



Adware MultiPlug

Adapts and Mutates to Evade Detection

Bundles malicious add-ons with seemingly useful yet unwanted applications

500 domains used across three month period

Shifted away from old URL-encoding scheme to increase penetration rate

4,000 add-on variants employed

Dridex

Speeding Ahead of the Sensors

9 hours to complete campaign, before traditional antivirus tools can react

Uses Microsoft® Office **macros** to quickly deliver banking Trojans

Up to 850 unique campaigns in time observed

Quickly morphs campaign content such as user agents, attachments, and referrers; and relaunches campaign

The security industry needs to move toward an integrated threat defense to keep pace with combination attacks. To learn more, download the 2015 Midyear Security Report.

www.cisco.com/go/msr2015