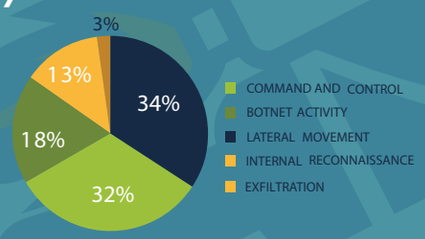
Cyberattacks: What happens post-intrusion?

The Vectra Networks **June 2015 Post-Intrusion Report** provides first-hand insight and analysis of active and persistent network threats inside organizations.

TARGETED ATTACKS

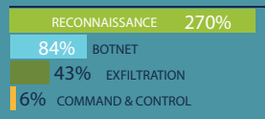
100% of networks showed signs attacks penetratrated the security perimeter

Threats detected by category



MOST DANGEROUS DETECTIONS ARE ON THE RISE

97% Increase



Percentage growth in the number of detections from 2Q14 to 2Q15

THE STRATEGIC PHASES OF ATTACK

Botnet Monetization
How criminals make money with ad click- fraud, spamming and DDoS attacks.

Command & Control
A wide range of malicious communication techniques

OPPORTUNISTC THREATS

TARGETED THREATS

Reconnaissance
Internal reconnaissance performed by an attacker inside the network.

Lateral Movement
Used to spread malware and authentication-based attacks such as using stolen passwords.

Exfiltration
Theft of data

BOTNETS FOLLOW THE MONEY

Top five activities of botnets

Abnormal ad activity	85%
Brute-force attack	5%
Outbound DoS	4%
Outbound scan	3%
Abnormal web activity	2%

HIDDEN TUNNELS SPIKE

Attackers send hidden communicaitons using HTTP, HTTPS and DNS

Five threat trends to watch

1. **Lateral Movement Detections**
Kerberos-based attacks grew **400%** compared to last year. Brute-force attacks accounted for **56%** of lateral movement detections.

2. **Internal Reconnaissance**
Port scans represented **53%**
Darknet scans represented **47%**

3. **Command and Control**
High-risk Tor detections jumped by more than **1200%**
External remote access jumped by **183%**

4. **Hidden pipelines of information**
Command and control and exfiltration are increasingly hidden in tunnels with in HTTP, HTTPS and DNS, with **HTTPS** being the most popular channel.

5. **Botnets**
Botnet monetization behavior grew linearly compared to last year. Ad click-fraud represented **85%** of all botnet detections.

Know what happens when attackers breach the perimeter.
Get the full Post-Intrusion Report at http://info.vectranetworks.com/post-intrusion-report-2015 or email us at info@vectranetworks.com.

VECTRA™
www.vectranetworks.com