به نام خدا

امنیت ابر سازمانی

Enterprise Cloud Security

ارائه دهنده:

تینا تعویذی

Tavizi.tina@gmail.com

Open Community of Cloud Computing

جامعه آزاد رایانش ابری ایران

۱۳۹۵/۰۹/۲۳

Cloud Security World

Key Challenges

- Identity Management (**SAML, OAuth, SSO, …**)
- Access Management **(Models:** DAC, MAC, RBAC, UCON, **language:** XACML**)**
- End-User Security: Safe surfing facilities, …
- Privacy
- Security Management
- Secure Storage (Encryption algorithms)
- Virtualization Security (**Attacks:** Communication between VMs or Between VMs and host VM Escape, VM monitoring from the host, VM monitoring from another VM, Denial of Service, Guest-to-Guest attack, External Modification of a VM, External modification of the hypervisor)

Emerging Threat Landscape

Based on Technology

Emerging Threat Landscape

- Emerging Technology Areas:
  - **Cloud Computing**
  - Mobile Computing
  - Cyber Physical Systems
  - IoT
  - Big Data
  - Network Virtualization and Software Defined Networks (SDN / 5G):

Emerging Threat	Threat Trend
1. Malicious code	↑
2. Web based attacks	↑
3. Web application attacks	↑
4. Botnets	↑
5. Denial of Service	↑
6. Insider threat	↑
7. Data breaches	↑
8. Cyber espionage	↑
9. Identity Theft	↑
10. Information leakage	↑

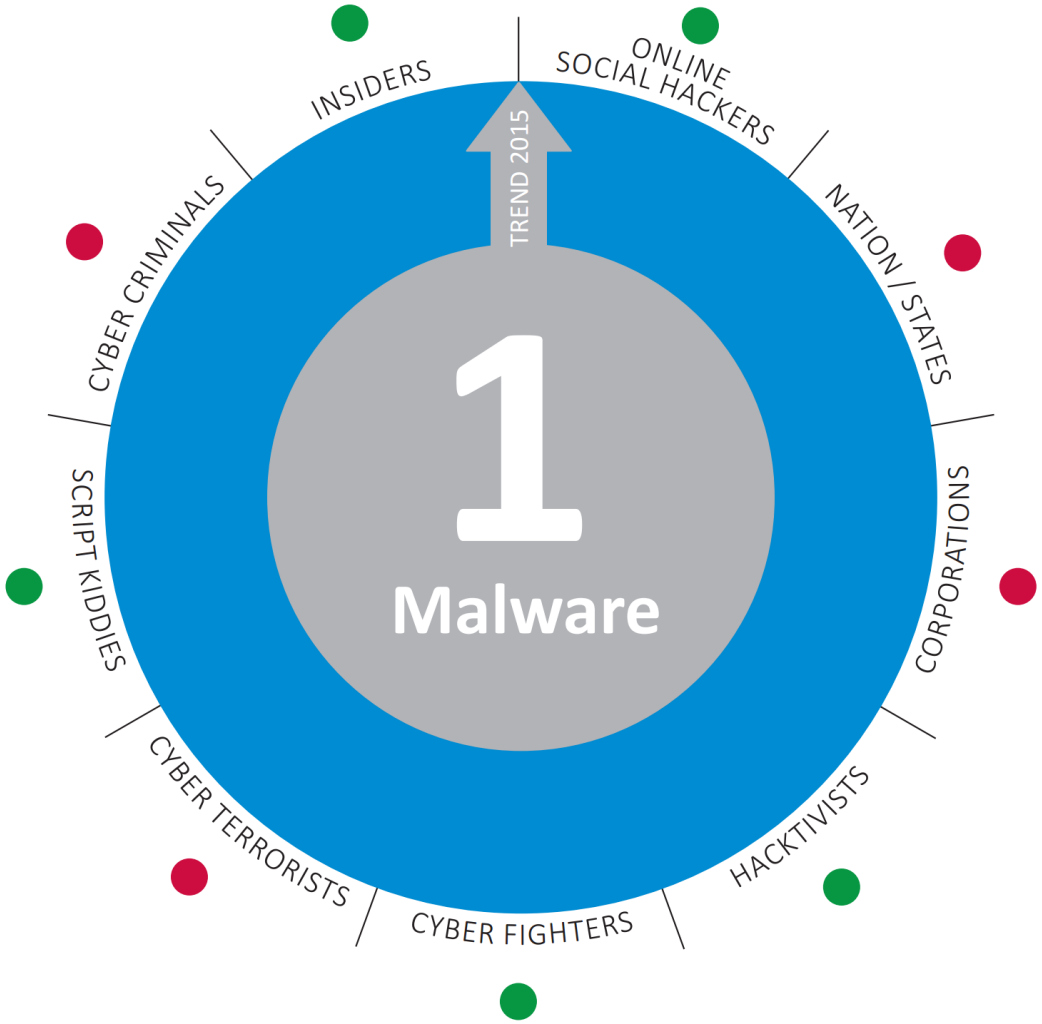
Legend: ↓ Declining, ➲ Stable, ↑ Increasing

Emerging threats and their trends in the area of cloud computing

Top 15 Cyber Threats 2015

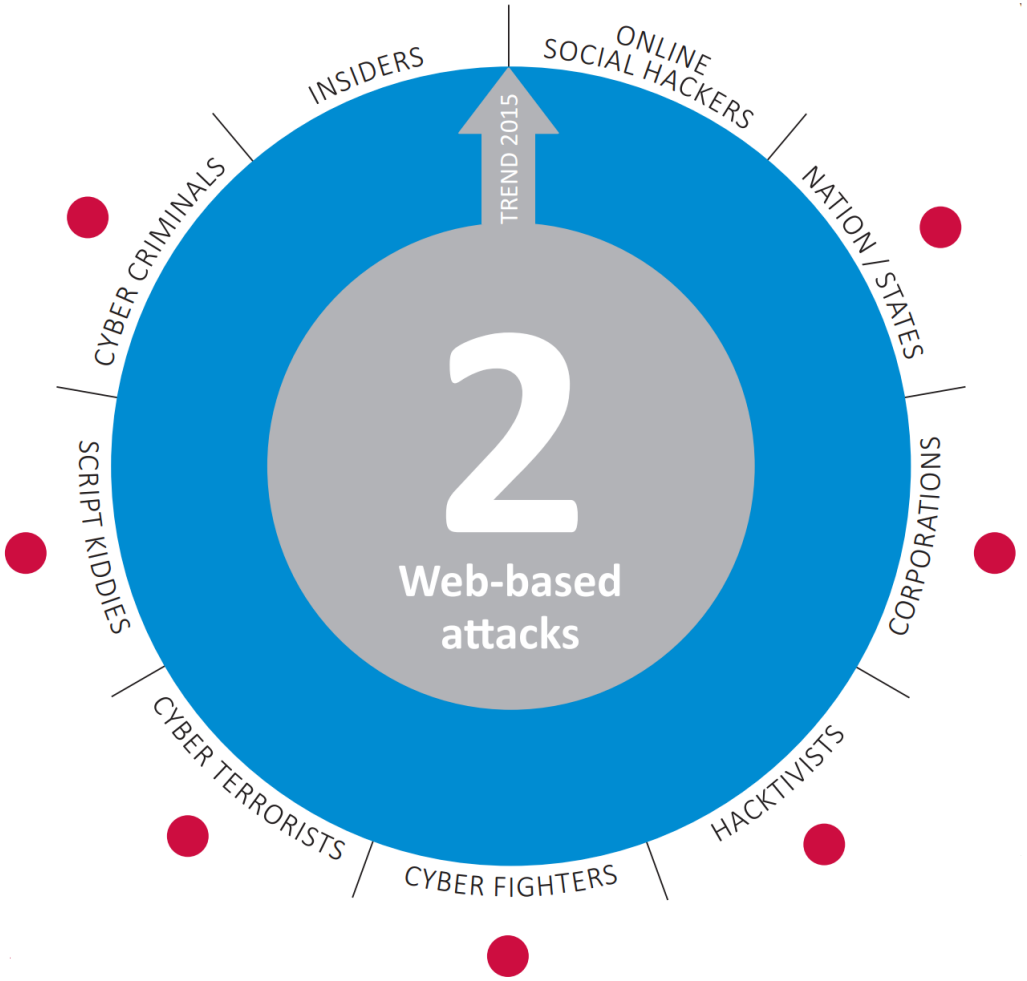
LEGEND

- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend



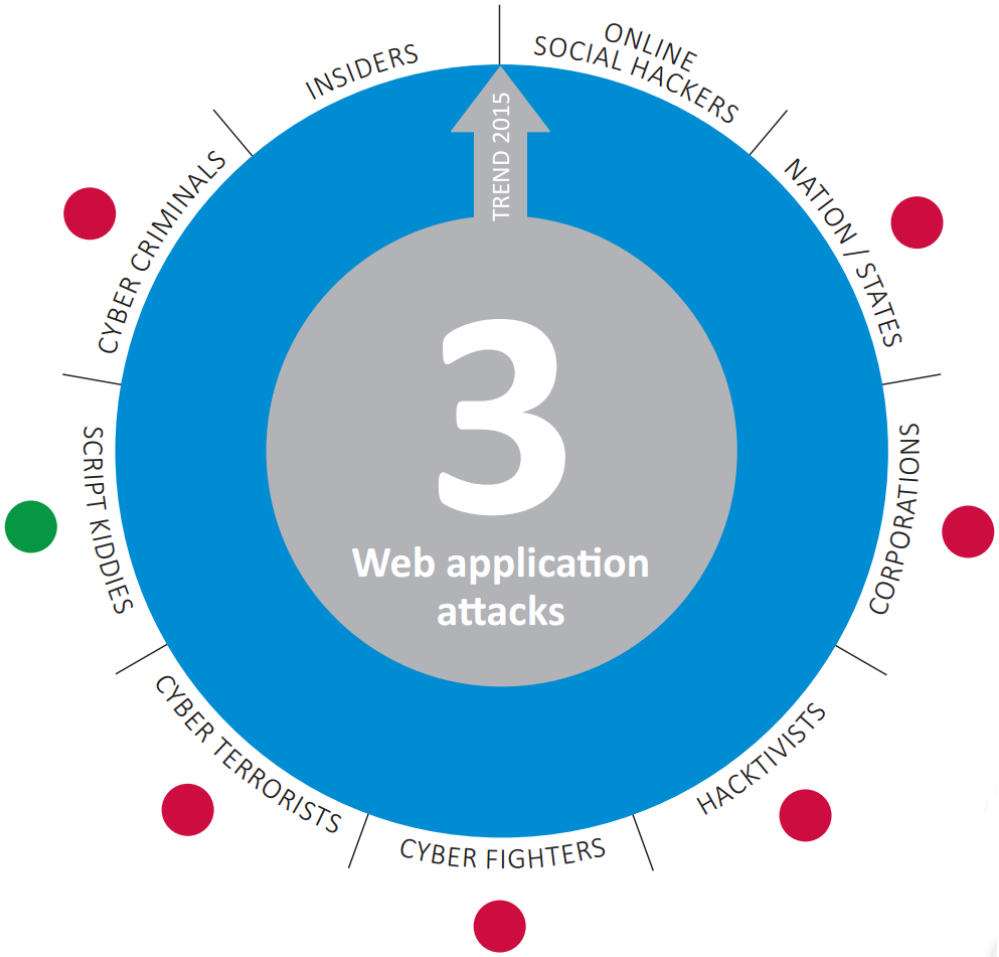
LEGEND

- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend



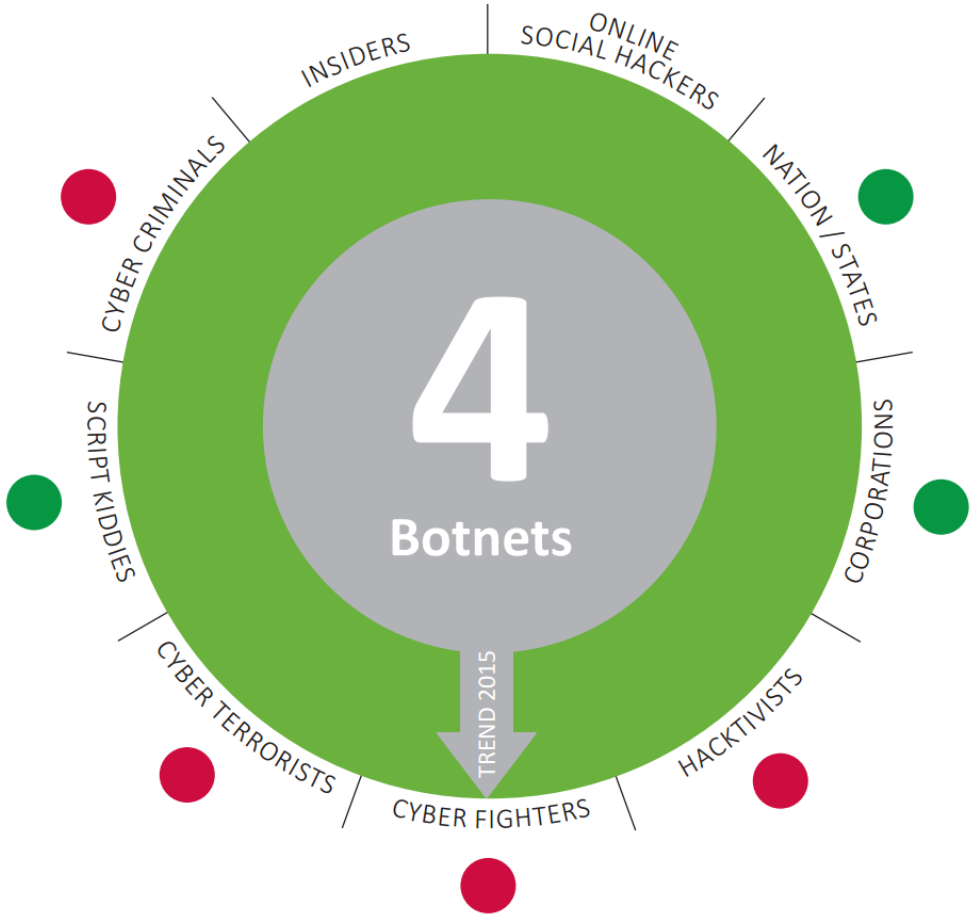
LEGEND

- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend



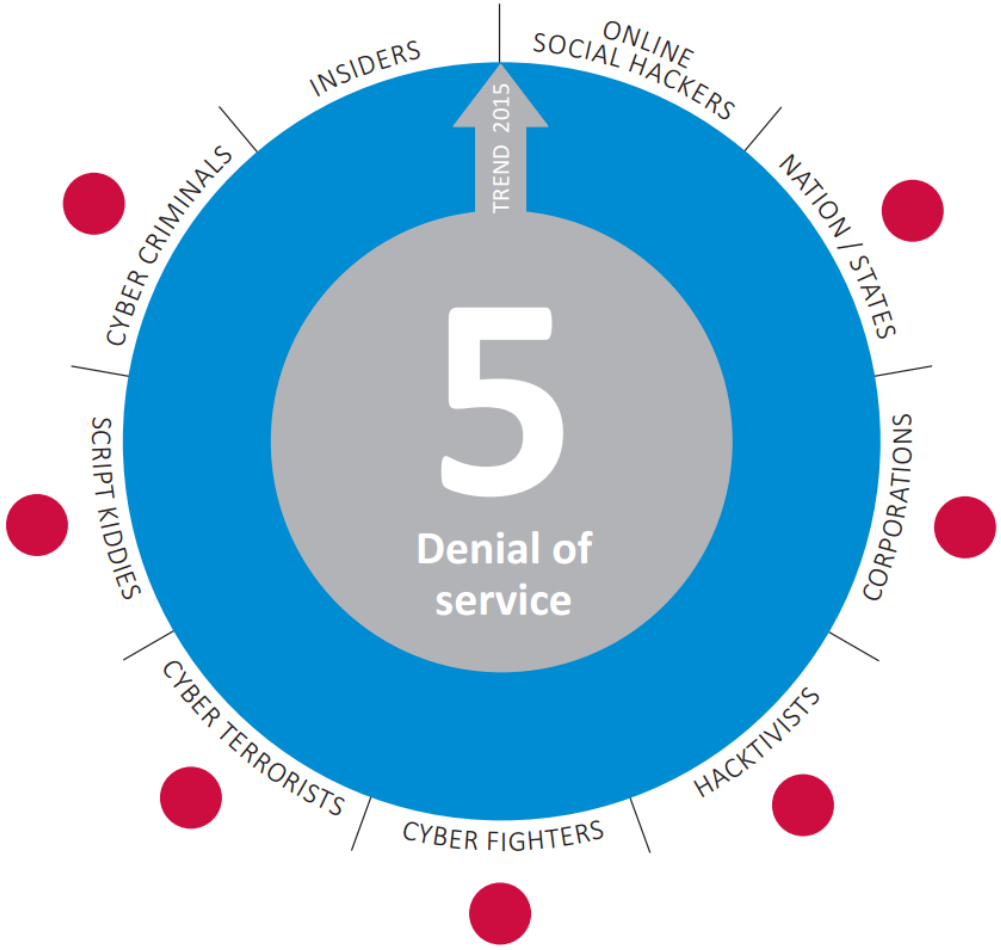
LEGEND

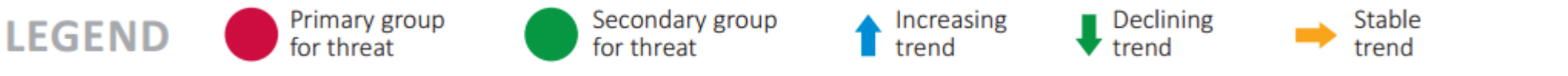
- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend

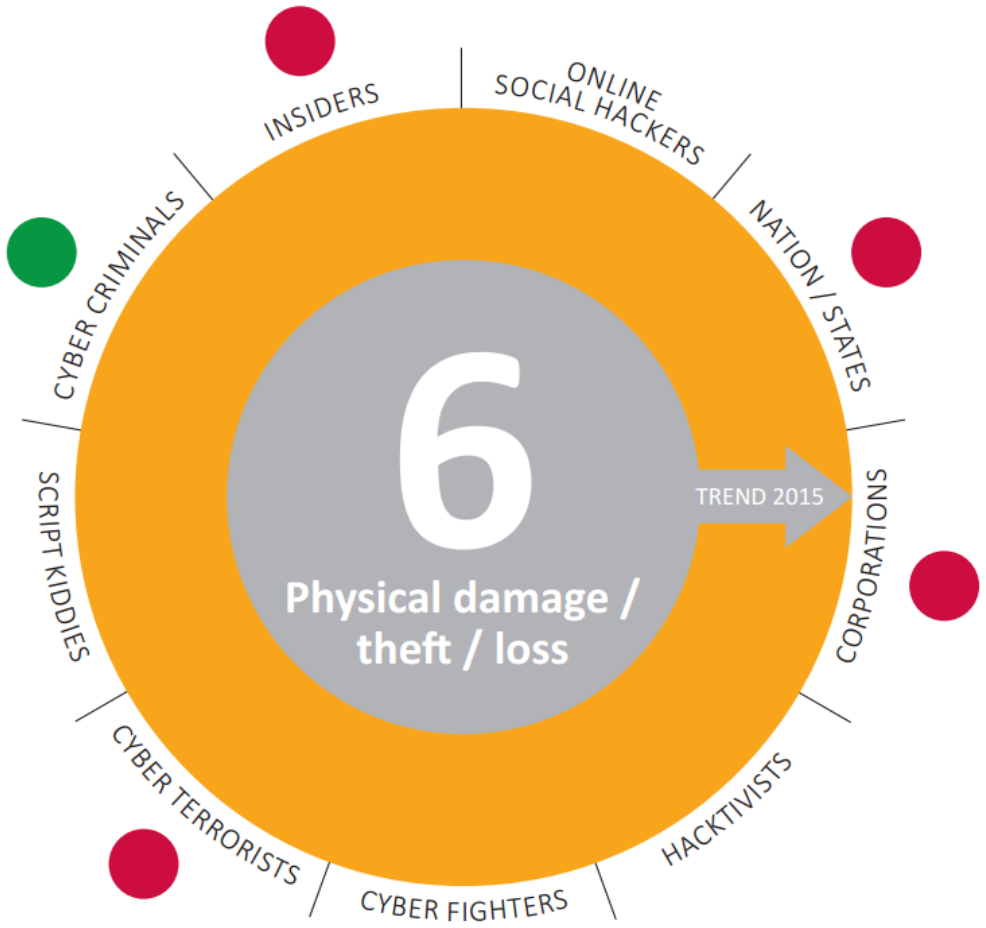


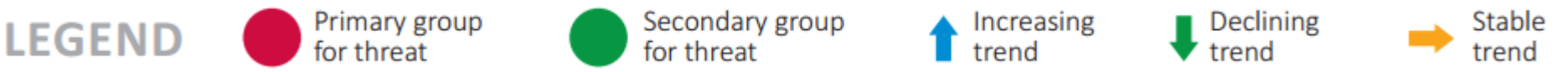
LEGEND

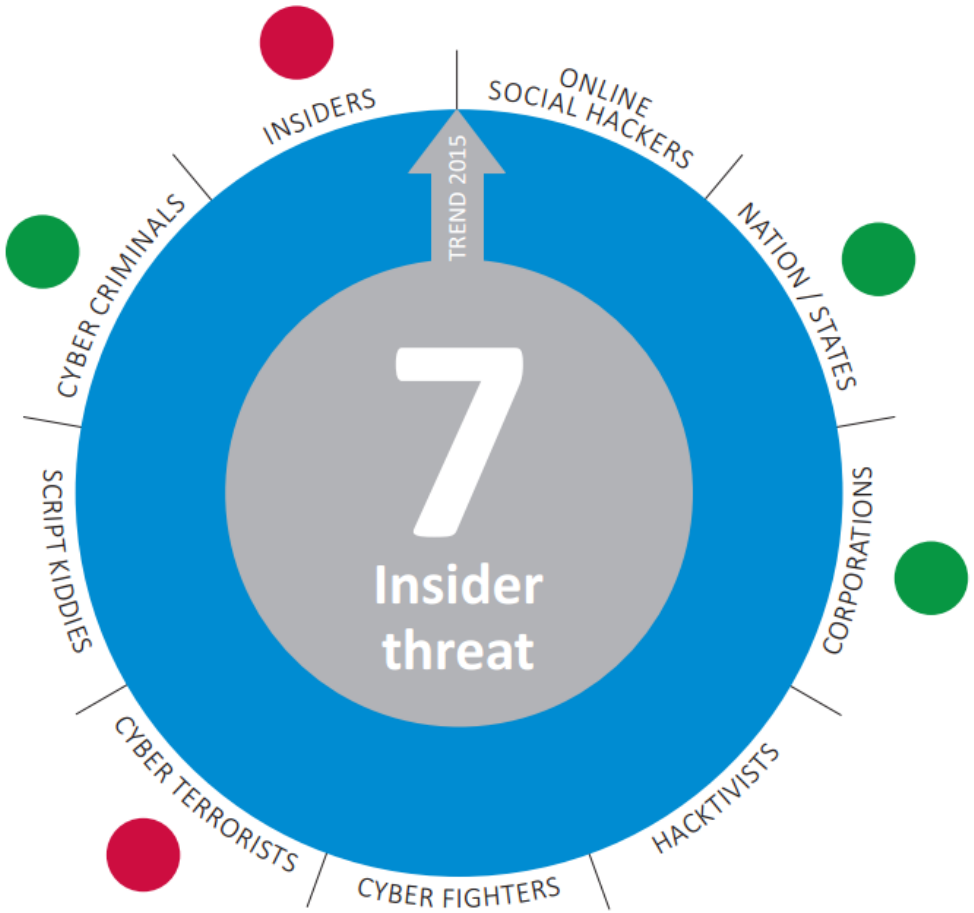
- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend




LEGEND
Primary group for threat
Secondary group for threat
Increasing trend
Declining trend
Stable trend


6
Physical damage / theft / loss
TREND 2015
INSIDERS
ONLINE SOCIAL HACKERS
NATION / STATES
CORPORATIONS
HACKTIVISTS
CYBER FIGHTERS
CYBER TERRORISTS
SCRIPT KIDDIES
CYBER CRIMINALS


LEGEND
Primary group for threat
Secondary group for threat
Increasing trend
Declining trend
Stable trend


7
Insider threat
TREND 2015
INSIDERS
ONLINE SOCIAL HACKERS
NATION / STATES
CORPORATIONS
HACKTIVISTS
CYBER FIGHTERS
CYBER TERRORISTS
SCRIPT KIDDIES
CYBER CRIMINALS

LEGEND

- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend

LEGEND

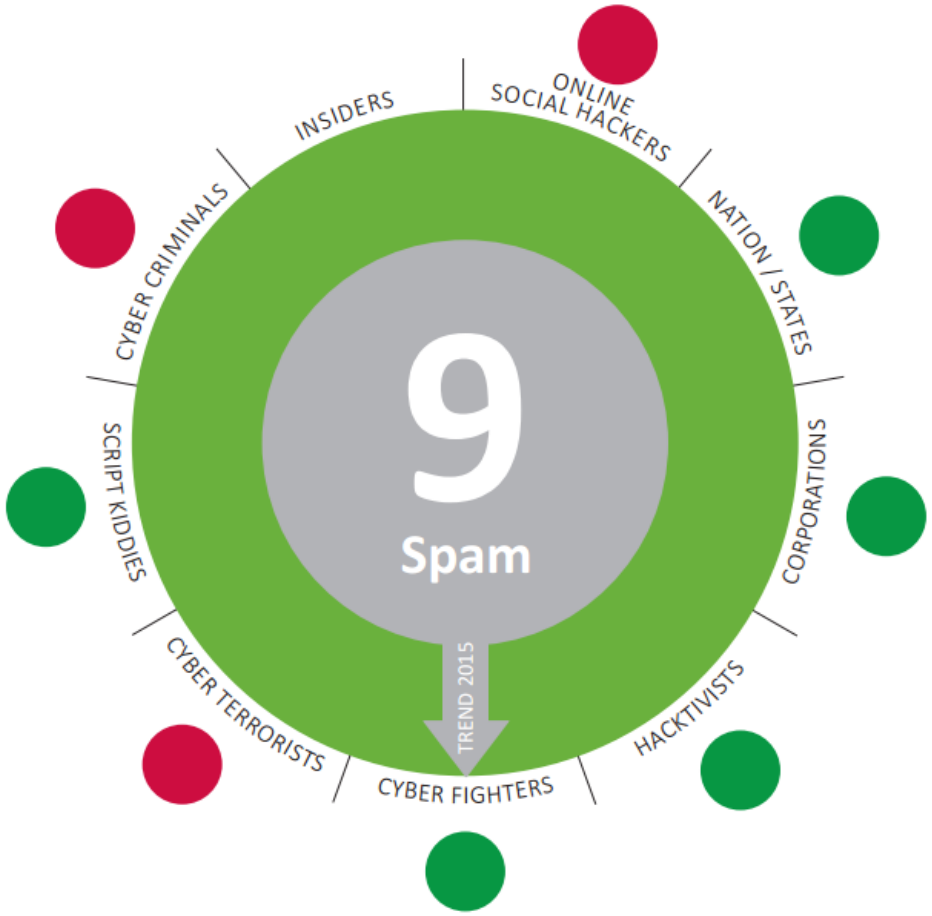
Primary group for threat

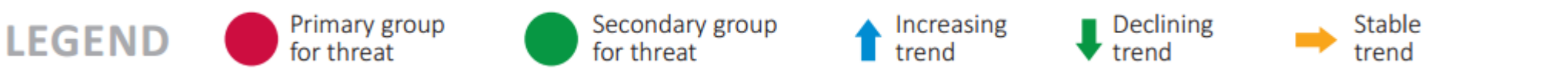
Secondary group for threat

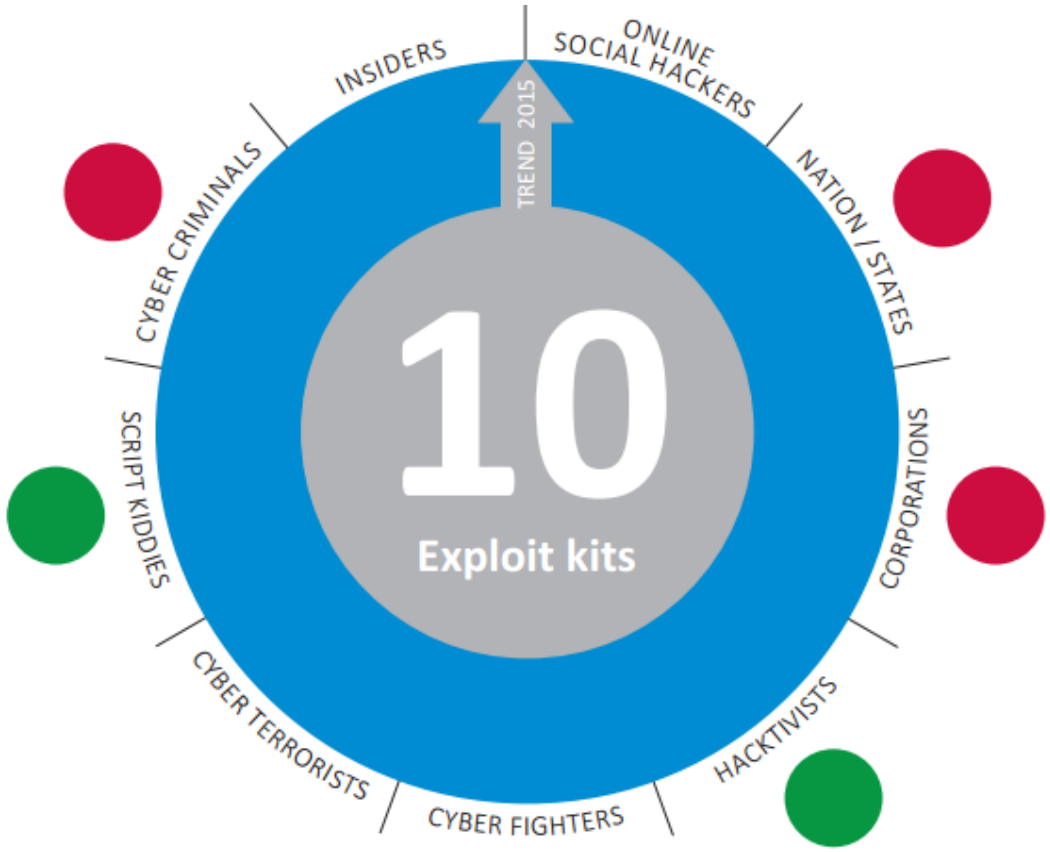
Increasing trend

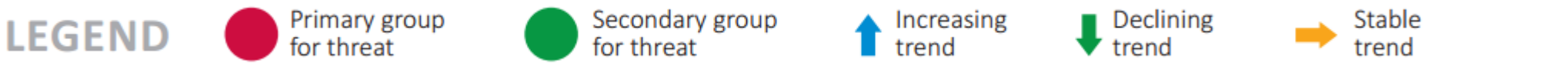
Declining trend

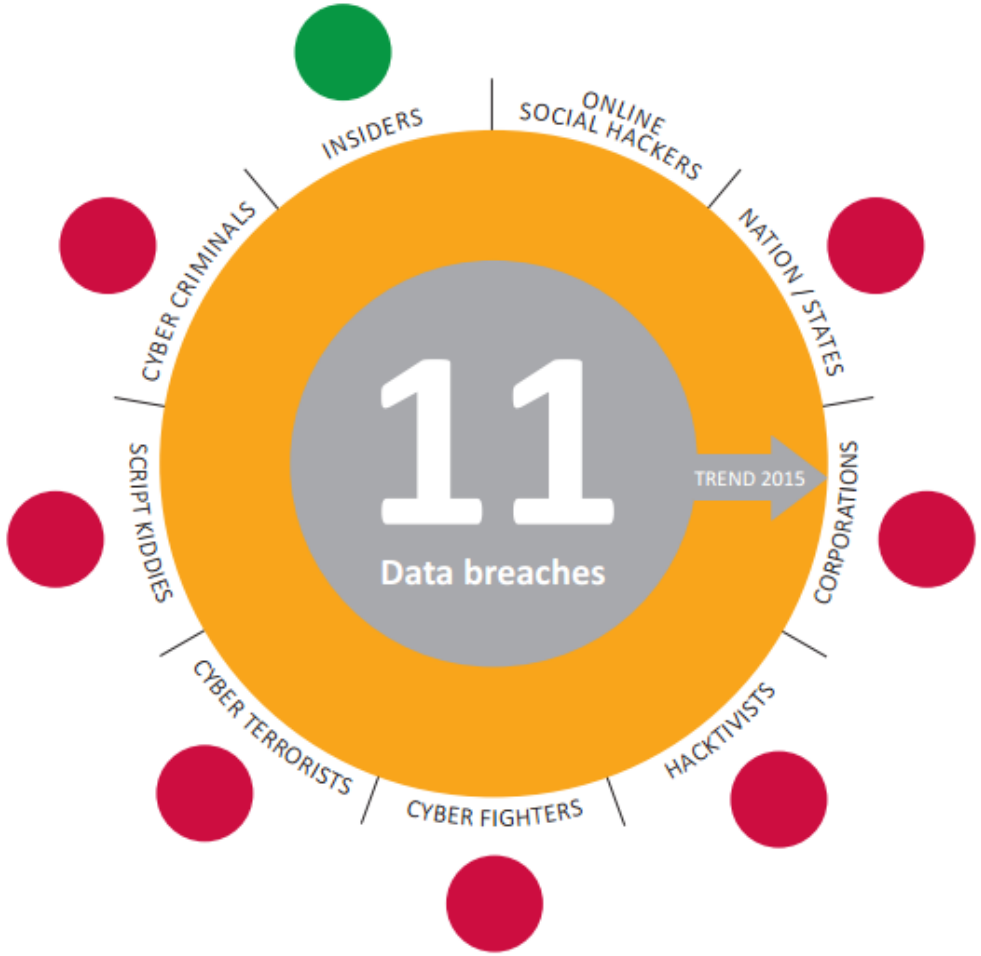
Stable trend




LEGEND
Primary group for threat
Secondary group for threat
Increasing trend
Declining trend
Stable trend


10
Exploit kits
TREND 2015
INSIDERS
ONLINE SOCIAL HACKERS
NATION / STATES
CORPORATIONS
HACKTIVISTS
CYBER FIGHTERS
CYBER TERRORISTS
SCRIPT KIDDIES
CYBER CRIMINALS


LEGEND
Primary group for threat
Secondary group for threat
Increasing trend
Declining trend
Stable trend

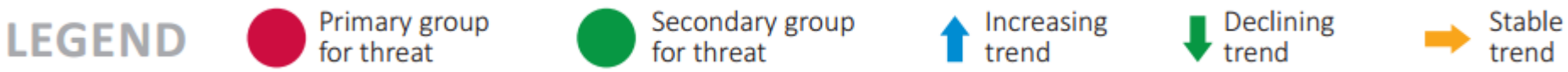

INSIDERS
ONLINE SOCIAL HACKERS
NATION / STATES
CORPORATIONS
HACKTIVISTS
CYBER FIGHTERS
CYBER TERRORISTS
SCRIPT KIDDIES
CYBER CRIMINALS
11
Data breaches
TREND 2015

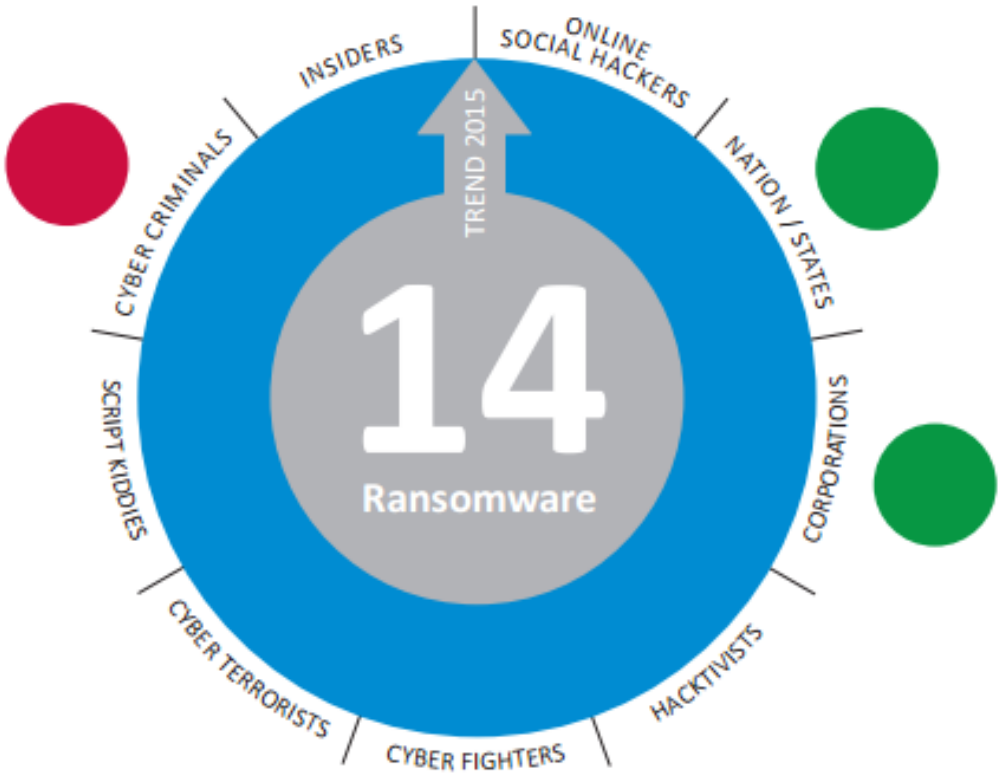
LEGEND

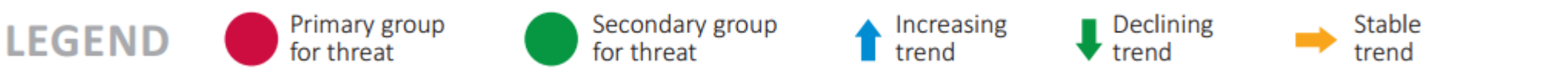
- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend

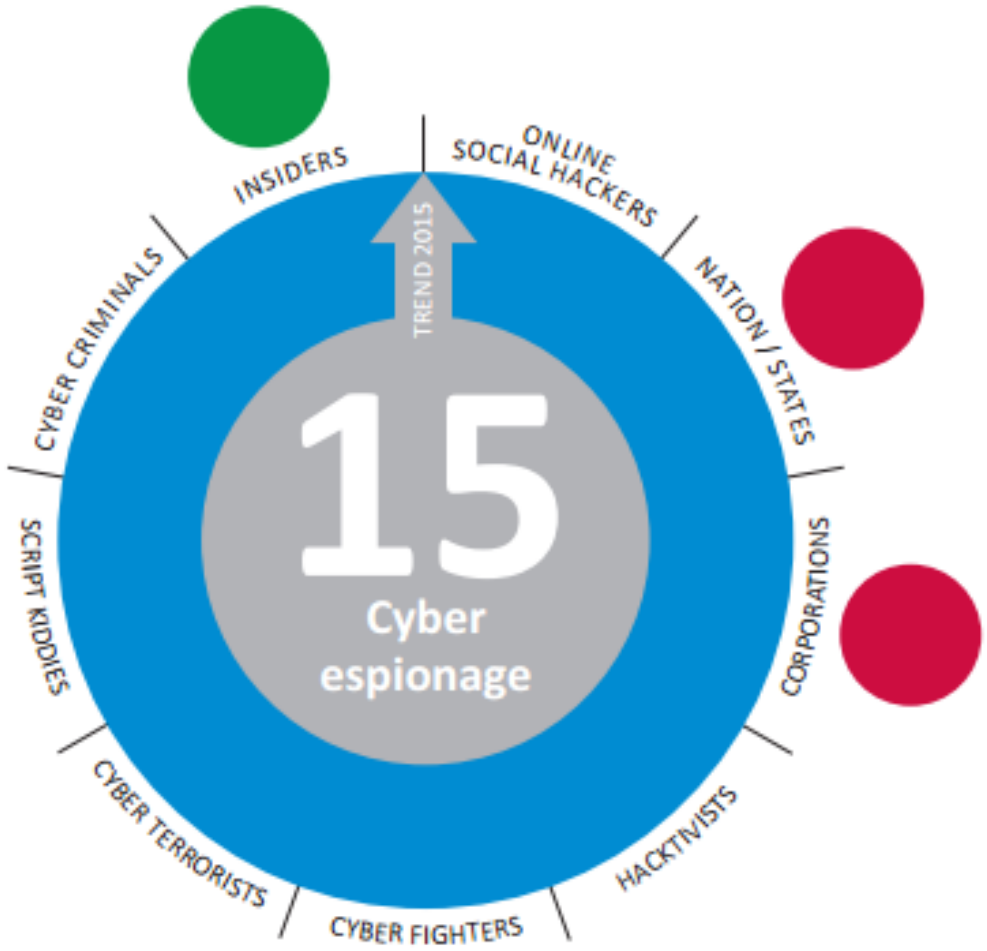
LEGEND

- Primary group for threat
- Secondary group for threat
- Increasing trend
- Declining trend
- Stable trend


LEGEND
Primary group for threat
Secondary group for threat
Increasing trend
Declining trend
Stable trend


14
Ransomware
TREND 2015
INSIDERS
ONLINE SOCIAL HACKERS
NATION / STATES
CORPORATIONS
HACKTIVISTS
CYBER FIGHTERS
CYBER TERRORISTS
SCRIPT KIDDIES
CYBER CRIMINALS





ENISA threat landscape Top 15 Cyber Threats 2015

2013 and 2014 Trends:

RANKING OF ASSESSED CYBER THREATS

LEGEND: Primary group for threat; Secondary group for threat; Increasing trend; Declining trend; Stable trend

2014	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TREND	↑	↑	↑	↓	↑	↓	↑	↓	↑	↑	→	↑	↑	↑	↓
TOP 15	Malicious code: Worms / Trojans	Web-based attacks	Web application / Injection attacks	Botnets	Denial of service	Spam	Phishing	Exploit kits	Data breaches	Physical damage / theft / loss	Insider threat	Information leakage	Identity theft / fraud	Cyber espionage	Ransomware / Rogueware / Scareware

2013	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
TREND	↑	↑	↑	↑	→	↑	↑	↑	↑	→	↑	↑	↑	↑	↑
TOP 15	Drive by downloads	Worms / Trojans	Code Injection	Exploit kits	Botnets	Physical damage / theft / loss	Identity theft / fraud	Denial of service	Phishing	Spam	Ransomware / Rogueware / Scareware	Data breaches	Information leakage	Targeted Attacks	Watering Hole

Cloud Security Services

Service Type Segments

- DevSecOps
- Data Loss Prevention
- Cloud IAM (CASBs, …)
- Cloud Database Security
- Encryption,
- Tokenization,
- Activity monitoring,
- Malware detection
- Email and Web Security
- Others (including network security, virtualization security etc.)

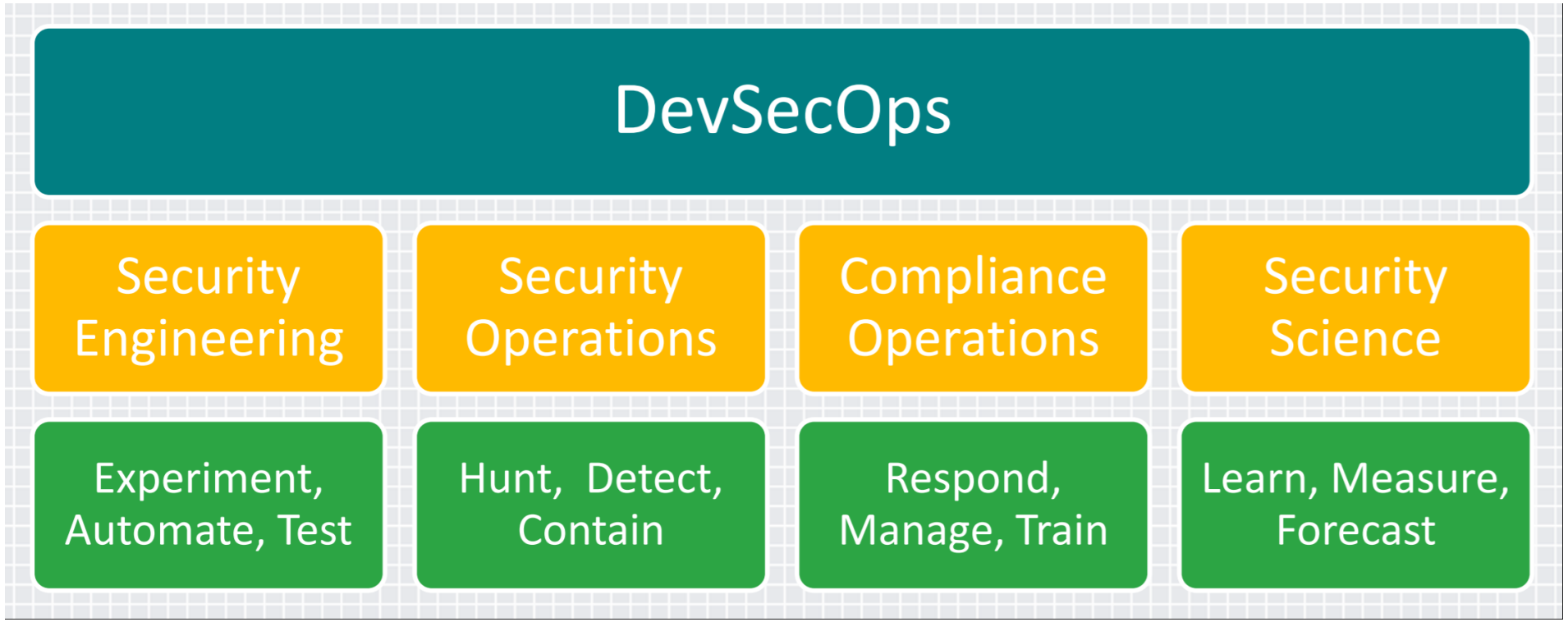
DevSecOps

SDL is Mandatory!

Training	Requirements	Design	Implementation	Verification	Release	Response
1. Core Security Training	2. Establish Security Requirements 3. Create Quality Gates/Bug Bars 4. Perform Security and Privacy Risk Assessments	5. Establish Design Requirements 6. Perform Attack Surface Analysis/ Reduction 7. Use Threat Modeling	8. Use Approved Tools 9. Deprecate Unsafe Functions 10. Perform Static Analysis	11. Perform Dynamic Analysis 12. Perform Fuzz Testing 13. Conduct Attack Surface Review	14. Create an Incident Response Plan 15. Conduct Final Security Review 16. Certify Release and Archive	Execute Incident Response Plan

What is DevSecOps ?

- != Devops + Security



Principles

- **1) Customer Focused Mindset**
- **2) Scale, Scale, Scale**
- **3) Objective Criteria**
- **4) Proactive Hunting**
- **5) Continuous Detection & Response**

1) Customer Focused Mindset

- Aligning business and security strategies to ensure just right, just enough security that everyone in an organization can support and implement.

Security professionals tend to think about how to keep business assets safe,

Business professionals focus on how to take risk to meet customer demands to increase revenues

2) Scale, Scale, Scale

- Achieving security scale:
  - Solving problems by reducing the amount of manual processes
  - Not easy for security professionals to make security transparent and easier for everyone to implement
  - Adapt and develop automation that allows for risk decisions to be made via self-service that allows for security to be scaled.

Security as Code has the added benefit of being portable, shared, and made better over time because its not a document that gets read once, shelved and forgotten. Instead, Security as Code has the advantage of being a living part of the system that supports business outcomes.

3) Objective Criteria

- Objective criteria can help business professionals know how, when, and in what order to improve the security profile of its business resources.
- Measuring the security of business assets is ideal for producing actionable requirements that business partners can use to make quick decisions.

Security Scorecard

- What can security rating do for us?
  - Make smarter security investments, and compare performance against peers and competitors.
  - Discover the security posture of any third party vendor or business partner
  - Get on-demand security intelligence for your firm.

4) Proactive Hunting

- By increasing internal security testing and making it proactive, an organization benefits because remediation guidance becomes immediately actionable and integrated with business processes.

- Implementing a Red Team function forced to build automation, leverage its own information, and identify defects before they become attack targets goes a long way towards establishing proactive hunting.

5) Continuous Detection & Response

- To complete information discovery and real-time attack detection.
- Security Science:
  - Question -> Hypotheses -> Experiment -> Analyze -> Repeat

Data Loss Prevention (DLP)

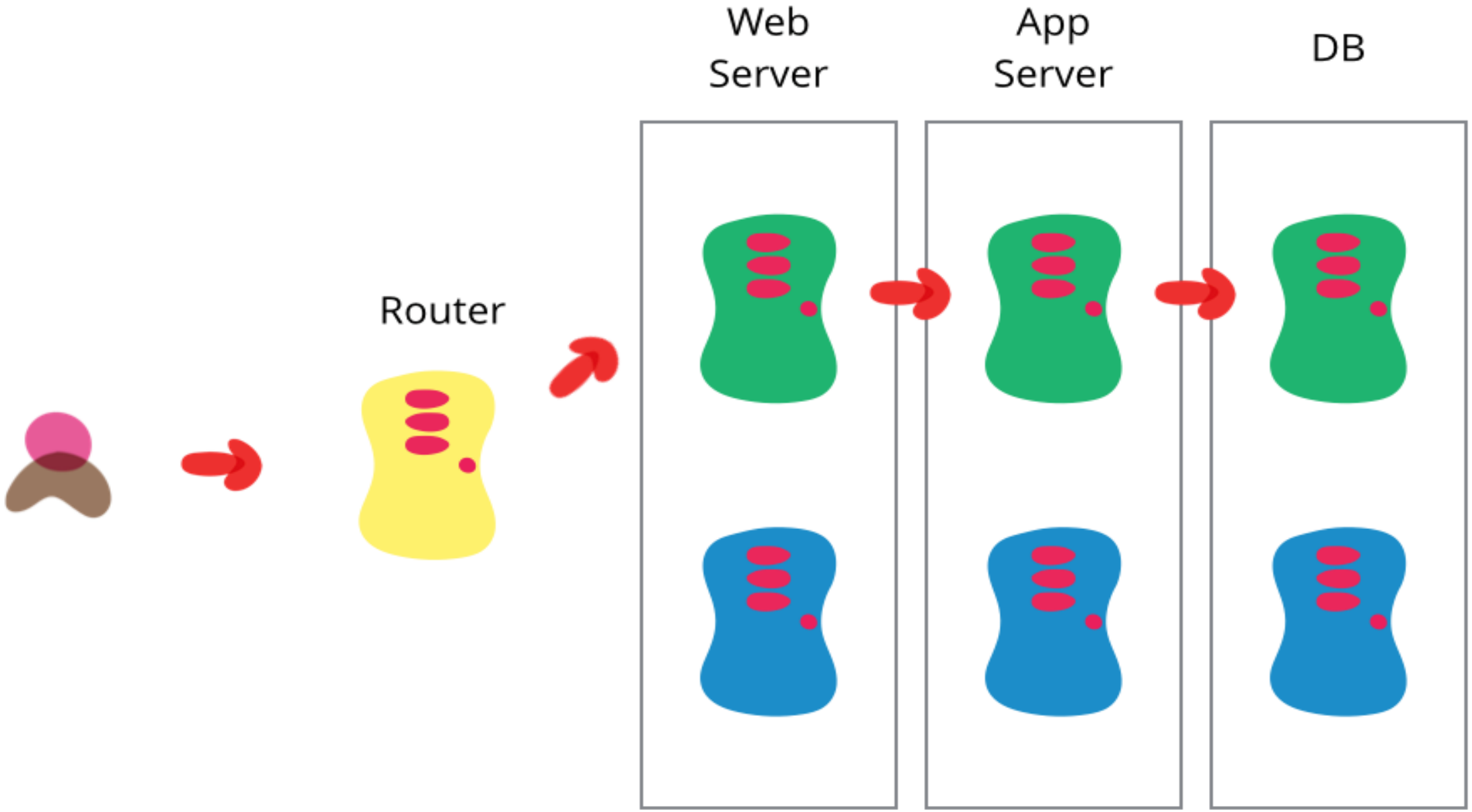
Data loss prevention software

- Designed to detect potential data breaches / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while:
  - **In-use** (endpoint actions),
  - **In-motion** (network traffic),
  - **At-rest** (data storage).

Vulnerability Management

Blue-Green Deployments to Release and Maintain Software Safely

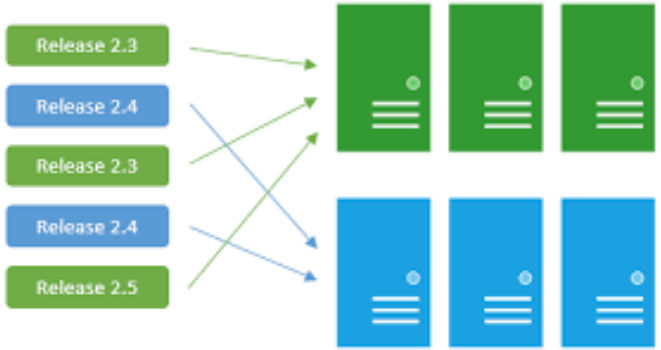
- Distinguish between deploying and releasing software
- Maintaining two separate production-capable environments, nicknamed blue and green for ease of discussion
- Only one of these environments is active and receiving production traffic at any one time
- The non-active environment functions as a final staging environment


Web
Server
App
Server
DB
Router

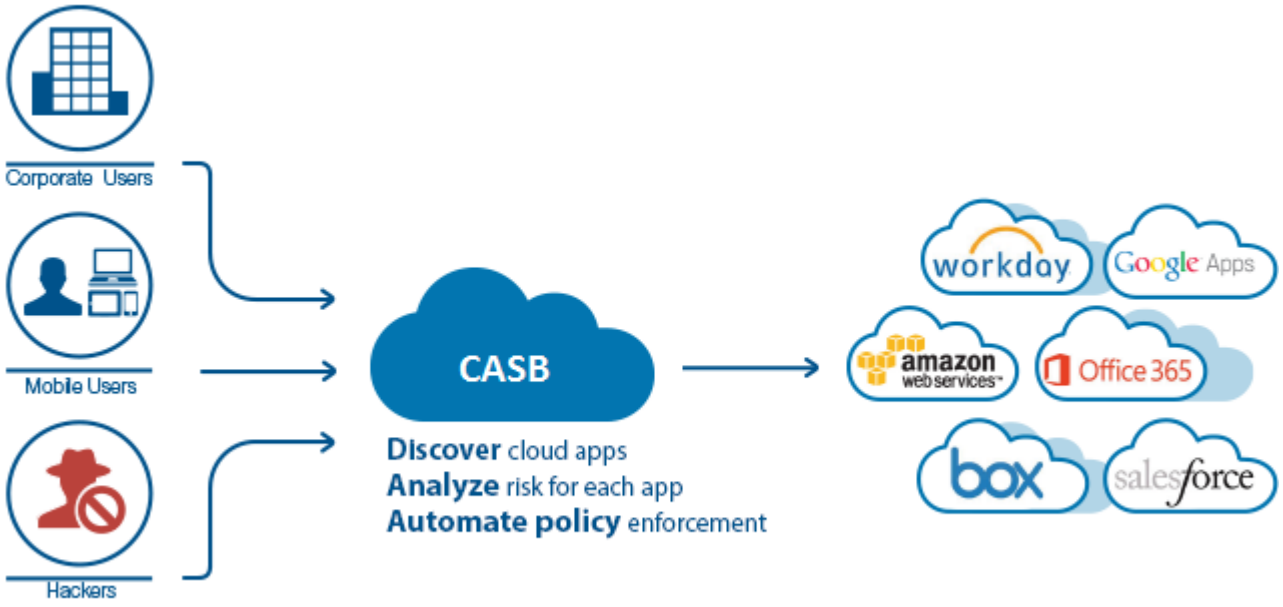
Blue-Green Deployments

- As you prepare a new release of your software you do your final stage of testing in the green environment. Once the software is working in the green environment, you switch the router so that all incoming requests go to the green environment - the blue one is now idle.

- Rapid way to rollback



CASBs


Corporate Users
Mobile Users
Hackers
CASB
Discover cloud apps
Analyze risk for each app
Automate policy enforcement
workday
Google Apps
amazon web services
Office 365
box
salesforce

Cloud access security brokers (CASBs)

- Critical control point for the secure and compliant use of cloud services across multiple cloud providers.

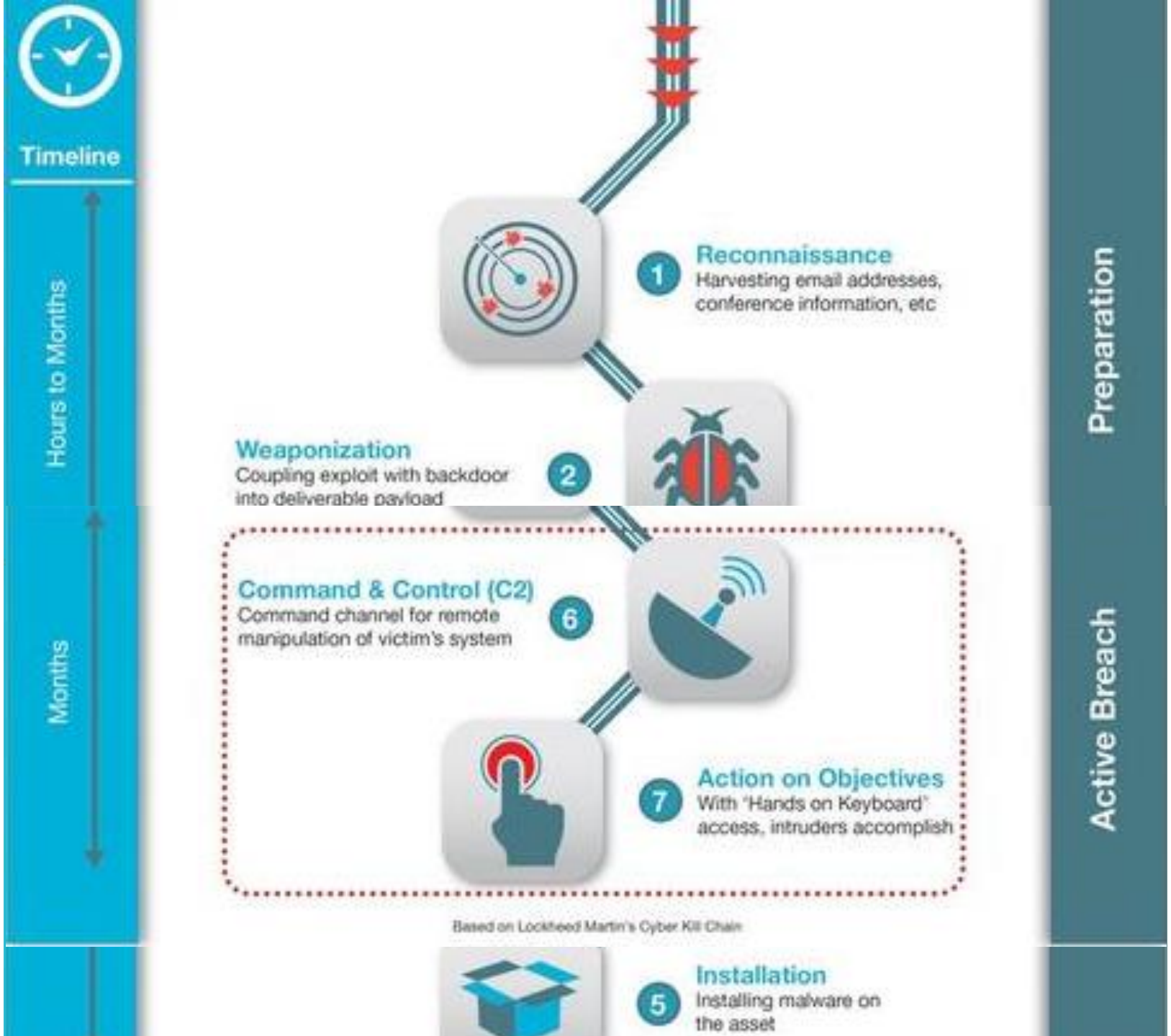
- CASB solutions fill many of the gaps in individual cloud services, and allow chief information security officers (CISOs) to do it simultaneously across a growing set of cloud services, including infrastructure as a service (IaaS) and platform as a service (PaaS) providers.

- Address a critical CISO requirement to set policy, monitor behavior and manage risk across the entire set of enterprise cloud services being consumed.

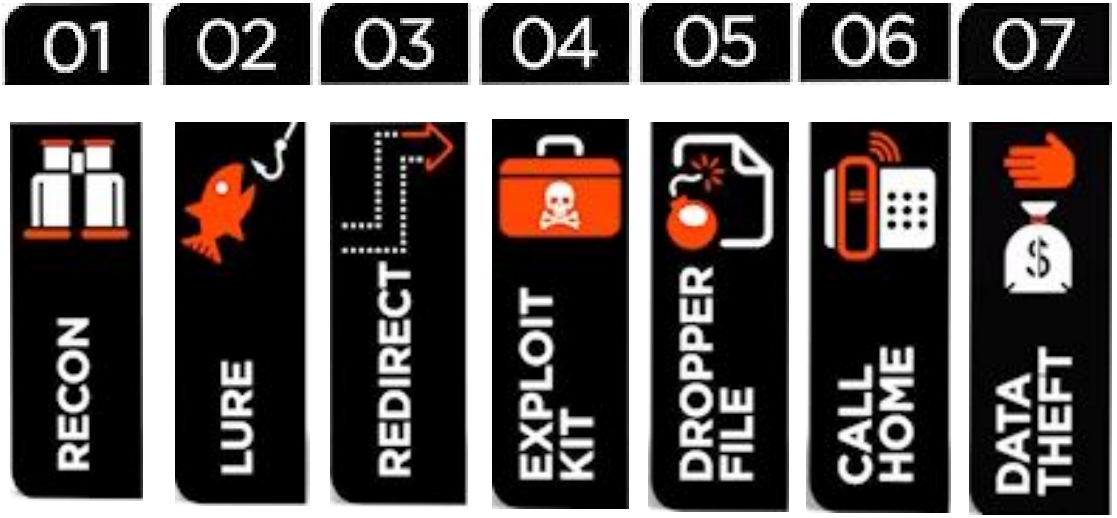
DDoS Mitigation Mechanism

DDoS Basics

Lockheed Martin Cyber Kill Chain



Websense 7 Stages of Advanced Threats



DDoS Mitigation Aspects

- Omit opportuni
- Using Software n configuration in different layers
  - Defense in De

Attack Possibilities by OSI Layer

OSI Layer	Protocol Data Unit (PDU)	Layer Description	Protocols		Examples of Denial of Service Techniques at Each Level		Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	begins. DB access is on this level. End-user protocols such as FTP, SMTP, Telnet, and RAS work at this layer	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway		PDF GET requests, HTTP GET, HTTP POST, – website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks	
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the Protocols Compression & Encryption		Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host	
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the Protocol Logon/Logoff		Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability	
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP		SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holing is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service	
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device		ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance	
Data Link (2)	Frame	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and it's devices are NICs, switches bridges & WAPs		MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advanced switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered	
Physical (1)	Bits	Includes, but not limited to cables, jacks, and hubs	Uses the Protocols 100Base-T & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices		Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets	

Application Attacks

Standards and Best Practices

- OWASP
- ASVS
- ISSAF
- OSSTMM
- CVE, CWE, CAPEC, …

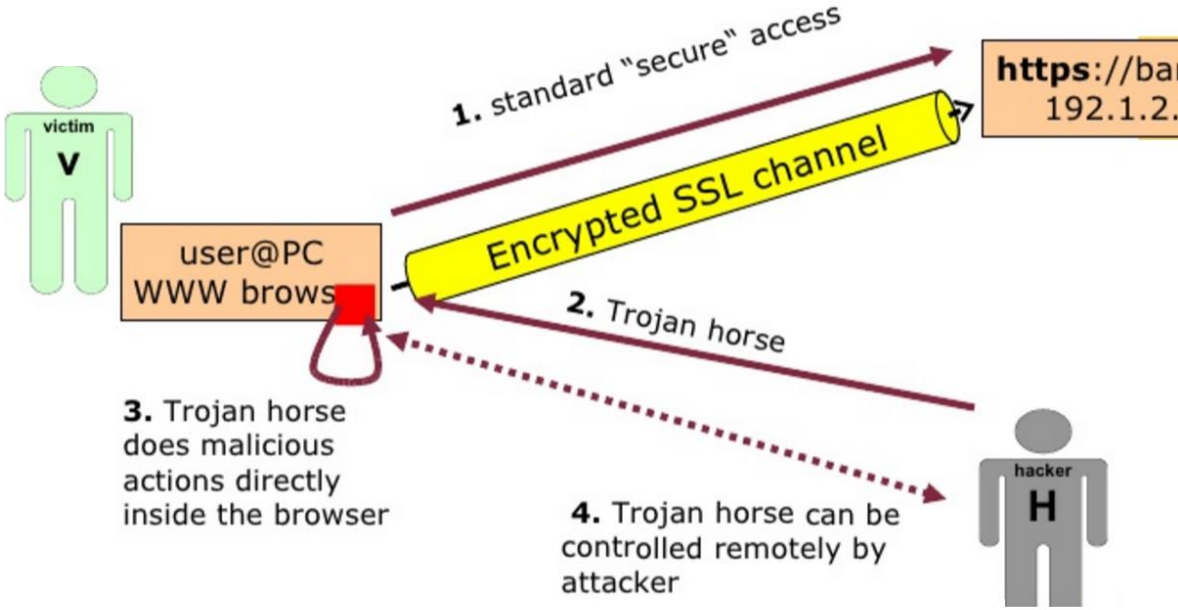
Remote Browser: Browser Attacks

Browser Attacks

➢ MITB

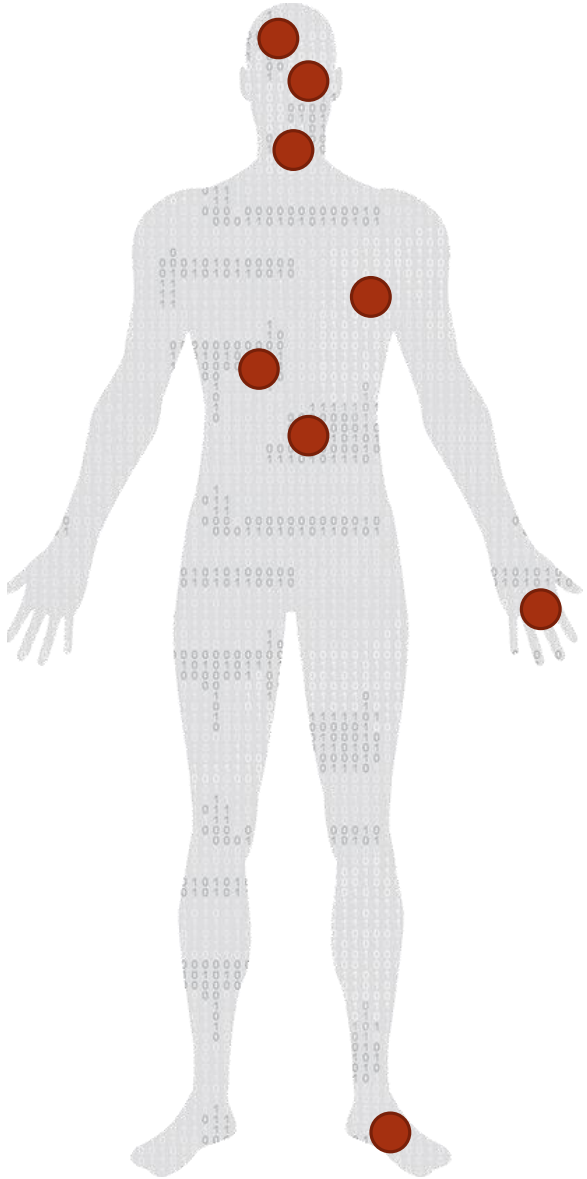
- **One of the most concerning types of malware attacks is called "Man-In-The-Browser" (MITB).**
- Typically the result of a Trojan infection, MITB permits a cybercriminal to modify the infected machine's browser and harvest user credentials.
- Infected browser looks like an unifected browser, many times prompting the user for token generated passwords and / or transaction PINs.

Scenario:



Enterprise Security Related Pain Points

- I’ve got too many alerts and don’t have the right resources to make sense of them.
- I can’t see what’s happening on my endpoints.
- I have security products from multiple vendors giving me integration heartburn.
- I’m worried about protecting the heart of my network: my and my customers’ data.
- I’d breathe easier if I had help preparing for an attack.
- I can’t rely on gut feel to know what to patch first.
- We spend more time researching threats than taking action on them.
- The sophistication of attacks is outpacing our defenses.



http://www-03.ibm.com/security/
http://www-03.ibm.com/software/products/en/category/cloud-security

با سپاس

تینا تعویذی

Gmail : tavizi.tina@gmail.com

Telegram : @tinatavizi