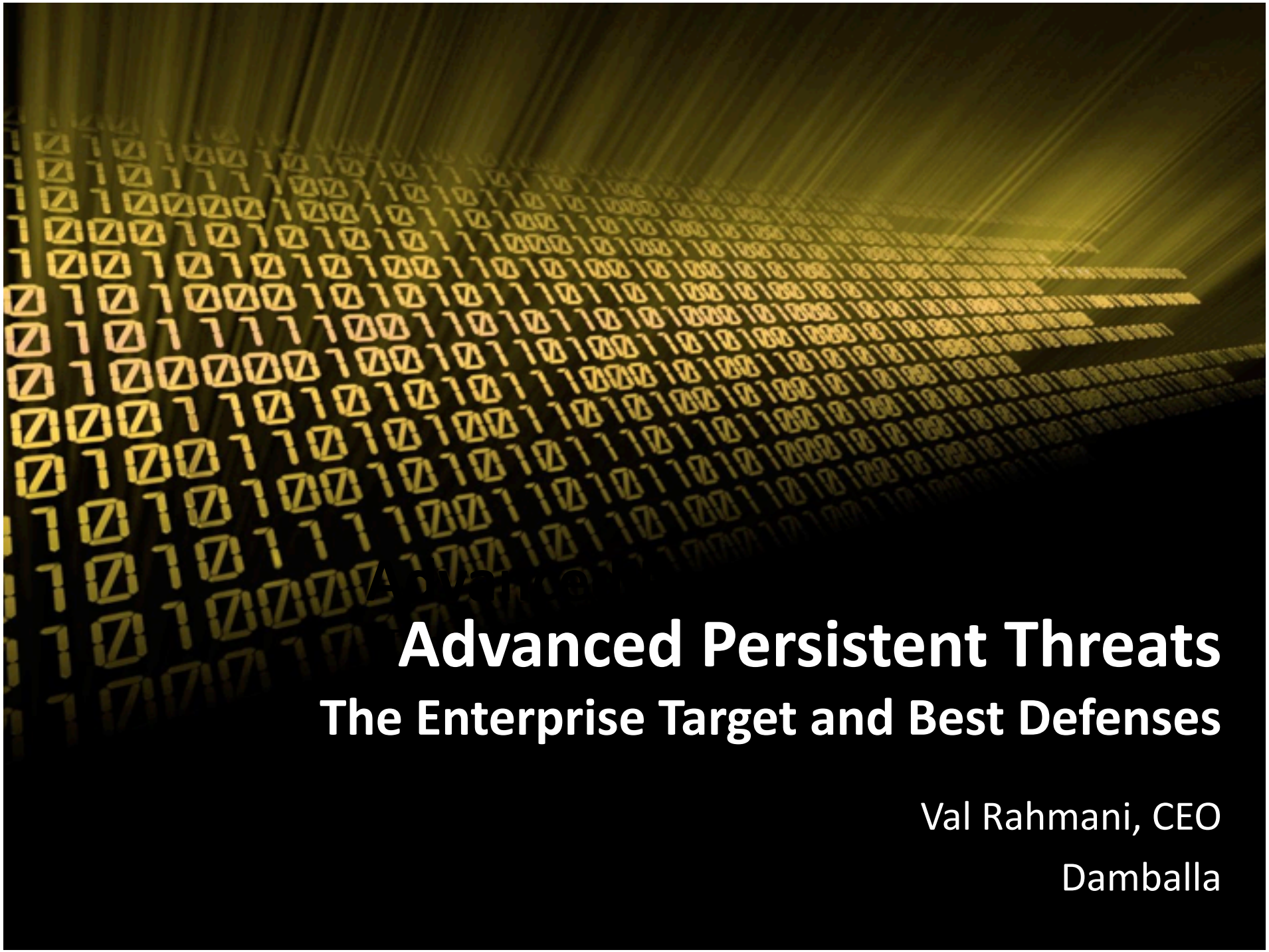


Advanced Persistent Threats

The Enterprise Target and Best Defenses

Val Rahmani, CEO

Damballa

What is an APT?

"An advanced and normally clandestine means to gain continual, persistent intelligence on an individual, or group of individuals such as a foreign nation state government"

Gartner's Definition:

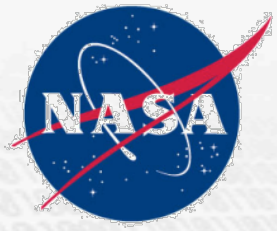
Advanced: Gets through your current level of protection

Persistent: It takes you too long to detect it got in

Threat: It causes you meaningful harm

Does not have to be state sponsored

APT in the News



Am I a Target? Yes!

Anything that can provide <u>competitive advantage and $</u>

- Intellectual Property
- Engineering Schematics
- Financial Information for Product Manufacturing
- Email for Business Strategies
- Legal Strategy Intelligence for Economic Trade

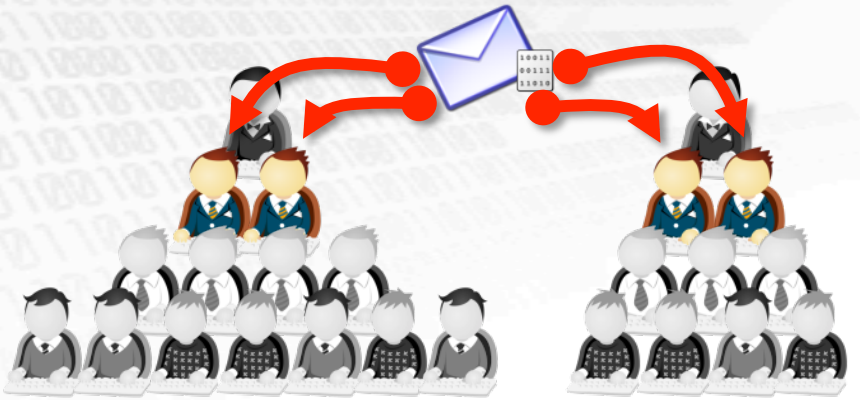
Targeting and Exploitation Cycle

Step 1	• Reconnaissance
Step 2	• Network Intrusion
Step 3	• Establish a Backdoor into the Network
Step 4	• Theft of User Credentials
Step 5	• Install Tools & Utilities
Step 6	• Privilege Escalation / Data Exfiltration
Step 7	• Maintain Persistence

Threat Vectors (How They Get In)

Social Engineering for Reconnaissance:

- Use Social Networks & Known Associations
- Phishing/Whaling
- Email attachments
- Links to Malicious Files
- Drive-by Downloads



Device Infections:

- From Inside or Outside the Network
- USB Drives/Storage Devices
- Mobile Endpoints (BYOD=BYO Malware?)

User is the Key

Malware is the Tool of Choice

Advanced Functionality / Simple to Obtain (DIY Kits)

- Keyloggers 

- RAT's (Remote Access Trojans) 

- Crimeware (Tuned for criminal purposes)

Maybe the "P" in APT should be Professional?

What Makes Today's Malware "Advanced"?

- Uses Zero-Day Vulnerabilities
- Tested to guarantee A/V evasion
- Aware of its Environment
- Virtual Machine Aware
- Uses Command-and-Control
- Domain Generation Algorithms/ Domain Fluxing

Easily Evades Prevention

Malware Evasion Testing

Virtest.com

Support:
e-mail: virtest@gmail.com
ICQ: 570352881

26 AV's

$1

Unlimited Scans
$50/mo

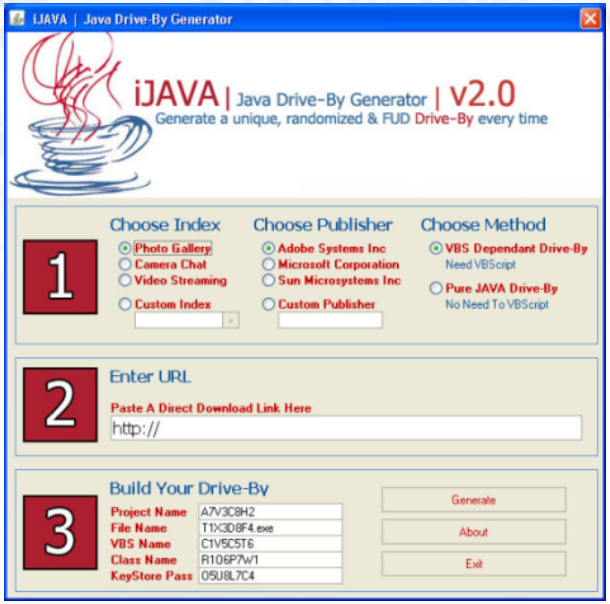
Antivirus	AV Versions
NOD32	3.0.684.0
IKARUS	IKARUS - T3SCAN V1.32.4.0, T3 V1.01.44
VirusBuster	1.4.3
DrWeb	4.44.5
Avast	4.8
McAfee	v5.10.0
BitDefender	v7.1 (build
Sophos	Sophos A
eTrust	v.31.06.00
AVG8	8.5.285
ClamWin	ClamAV 0.9
KAV8	Kaspersky
SAV	Symantec
Vba32	VirusBlokAda v.3.12.11
F-Prot	FRISK Software F-Prot Antivirus v.6.2.1.4201
A-Squared	3.0.0.126
TrendMicro	Ver 1.1
F-Secure	F-Secure Anti-Virus 2009 (v.9.00.149)
OneCare	Microsoft Live OneCare 2.5.2900.22 (только у нас)
Avira	AntiVir v.7.6.0.59
Ewido	Ewido 4.0
Panda	Panda 9.05.01

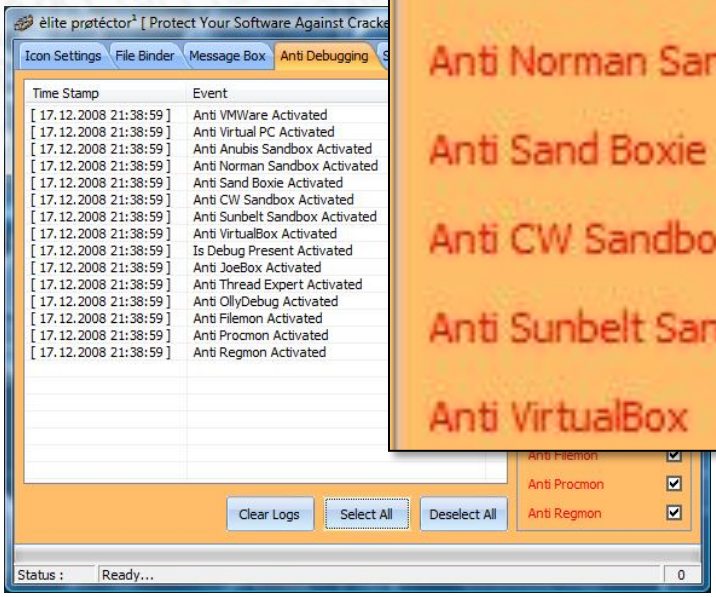
Malware Evasion Testing (Push Button)

The latest SpyEye kit has Virtest QA functionality built-in to ensure zero-day malware delivery.

Malware Environmental Awareness

- OS aware (Mac/Android/Windows)
- Tests for Live Internet Access
- Virtual Machine /Sandbox Aware
- Can Infect Master Boot Records





Command-and-Control Drives the Attack

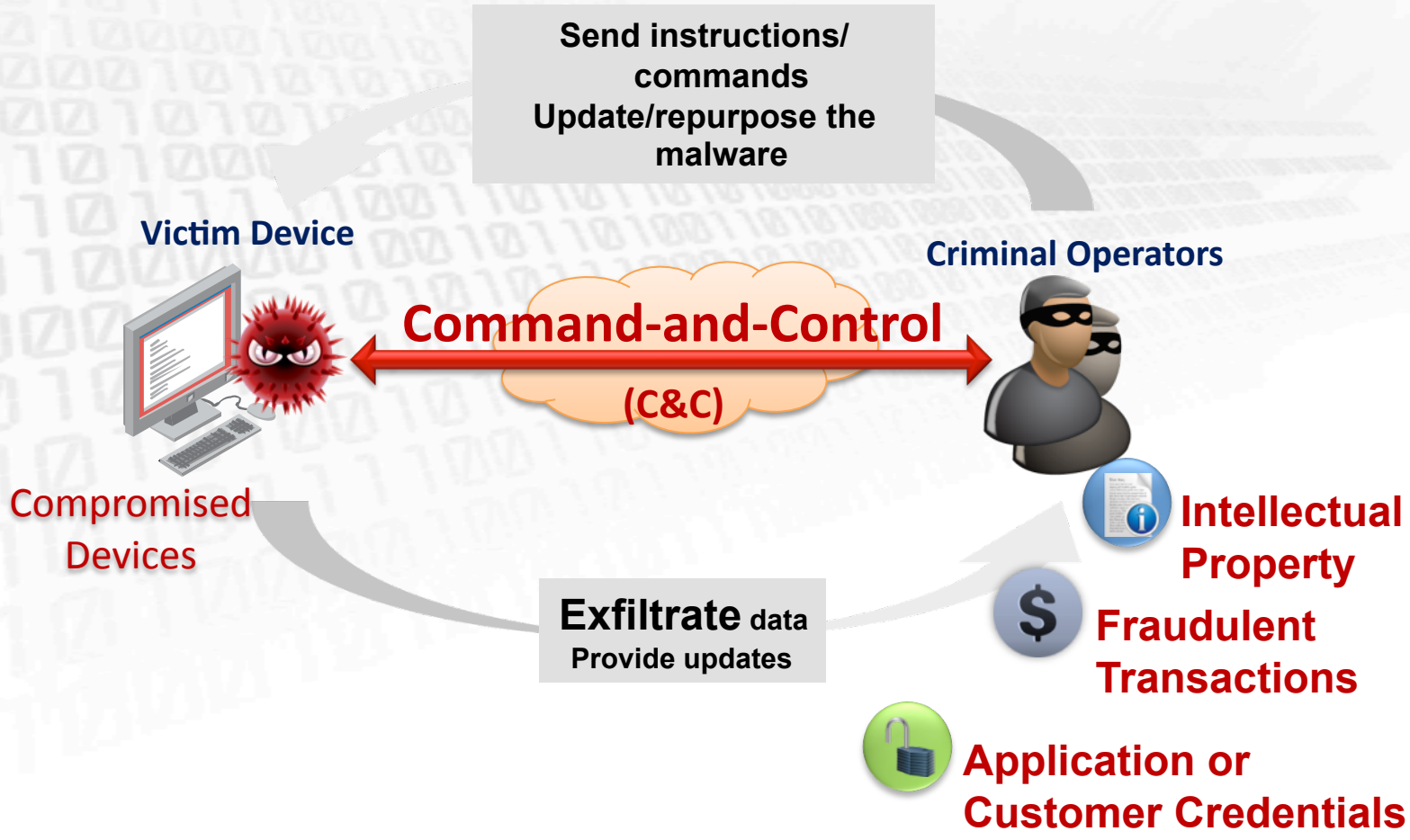
73%

of breaches involved command-and-control channel

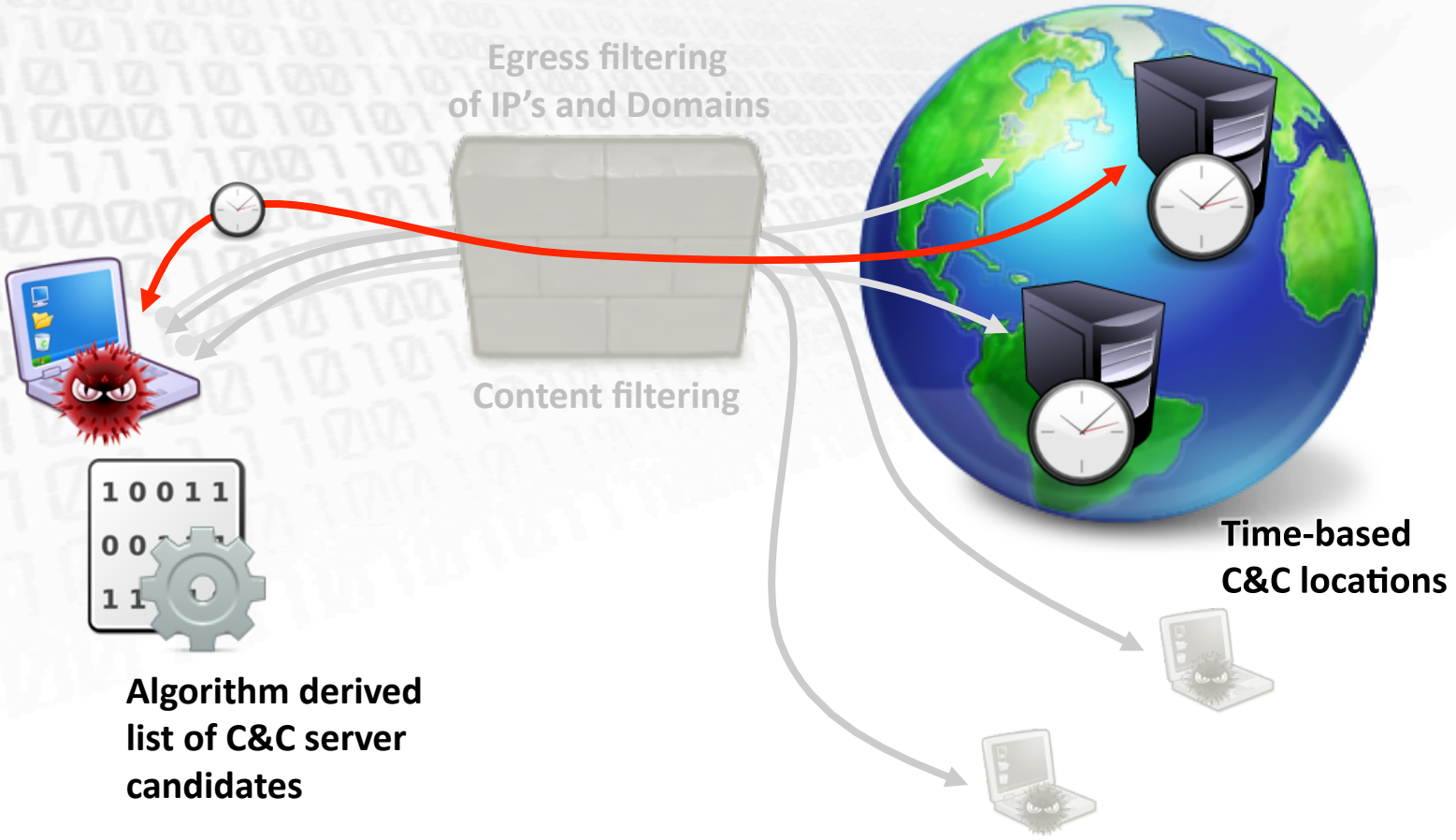
Data Breach Investigations Report - Verizon RISK team

- Establishes Backdoor
- Downloads Other Tools
- Updates Itself / Mission
- Looks like Normal Traffic
- Channel to Exfiltrate Data

Command-and-Control Drives the Attack



Domain Generation Algorithms in C&C



Persistence: Establish Foothold, Lay Low

Average

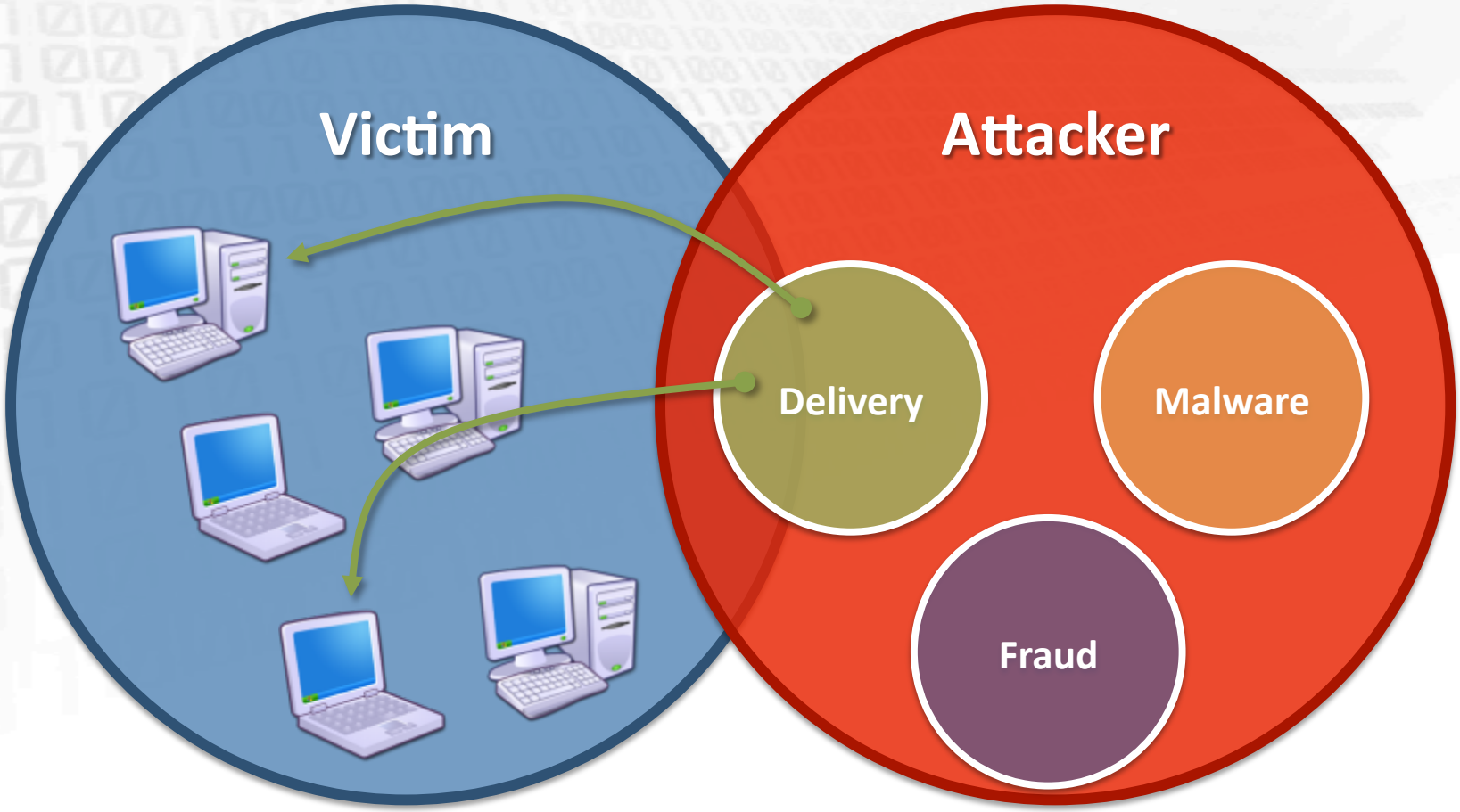
156

Days Before
a Breach is Discovered

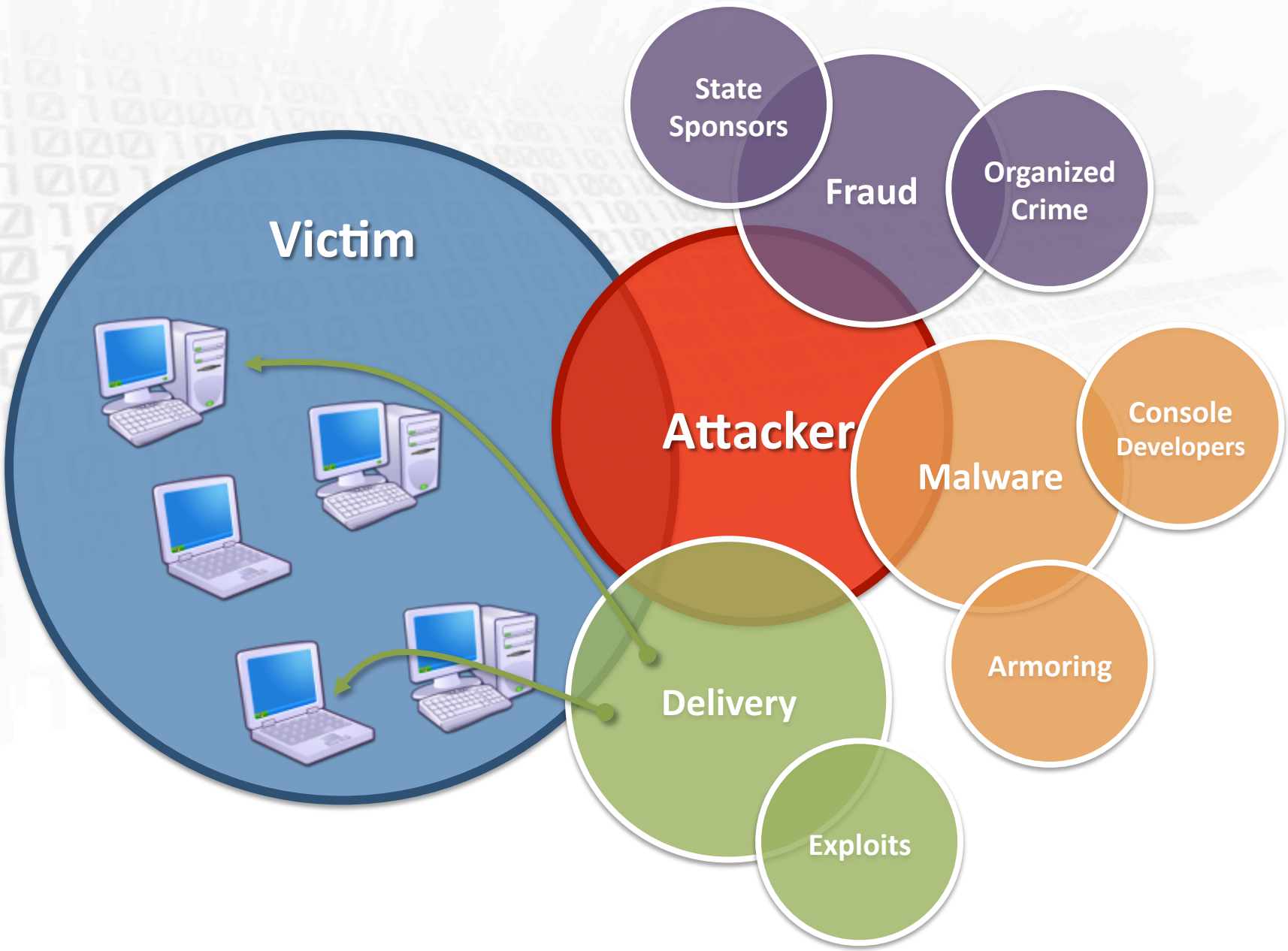
- ROI (Return on Infection)
- Find additional entry vectors if "door" closes
- Timeliness/fullness of stolen data = higher resale value
- Subleasing of services
- Access and resources leased to other criminals


The Targeted Enterprise

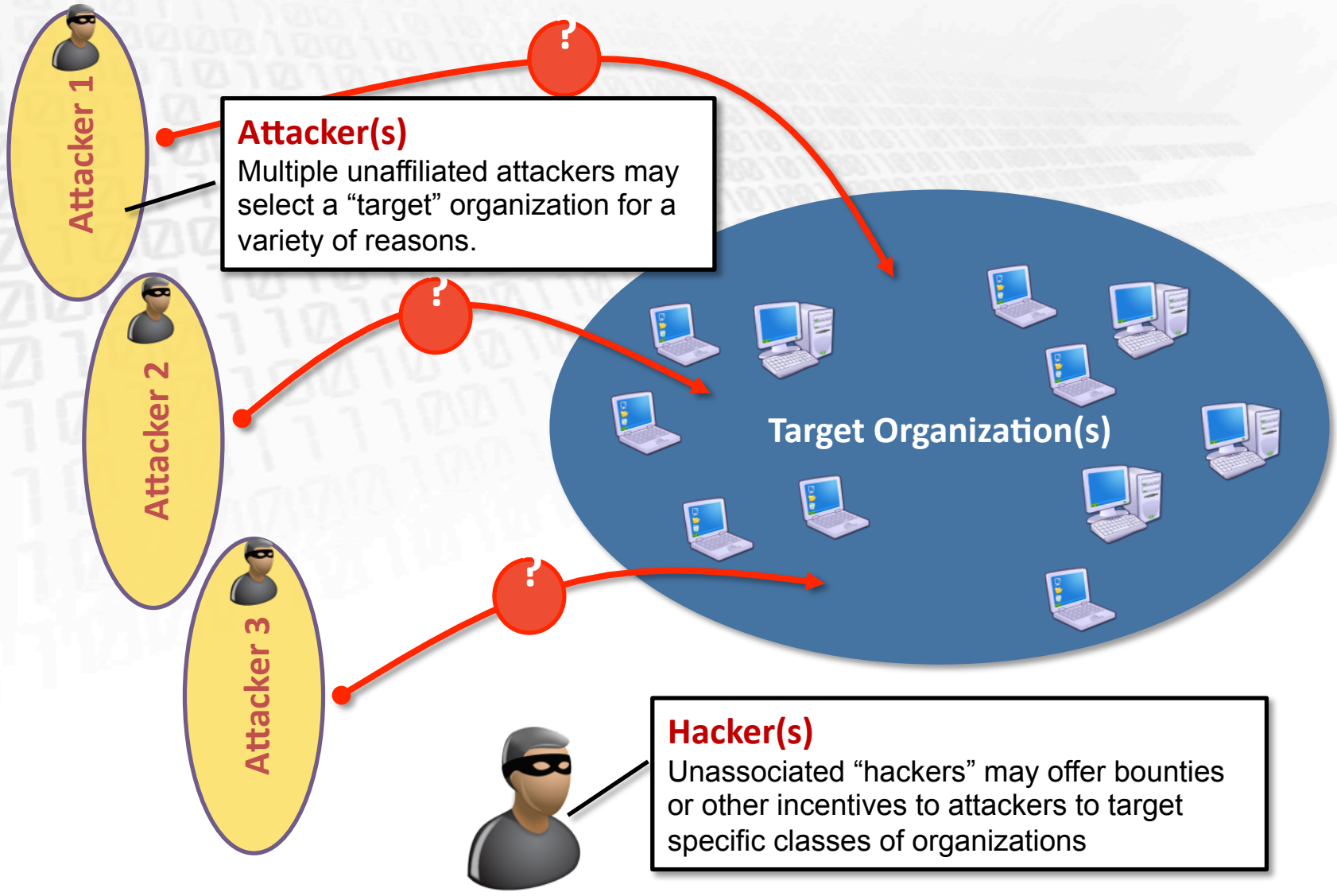
Common Perception of Attacks



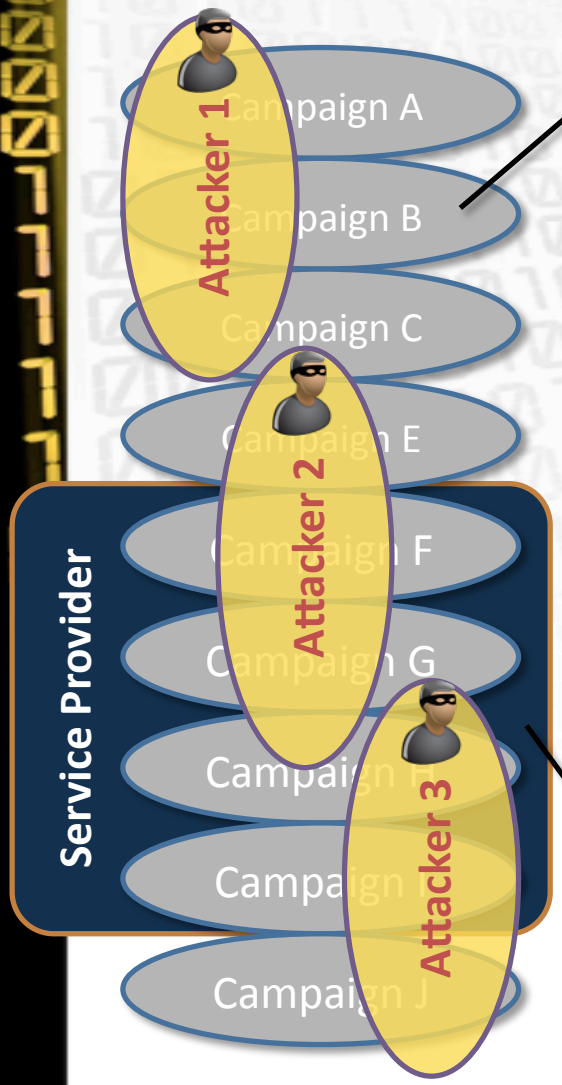
Reality: Federated Operations



Lifecycle of a Breach



Lifecycle of a Breach



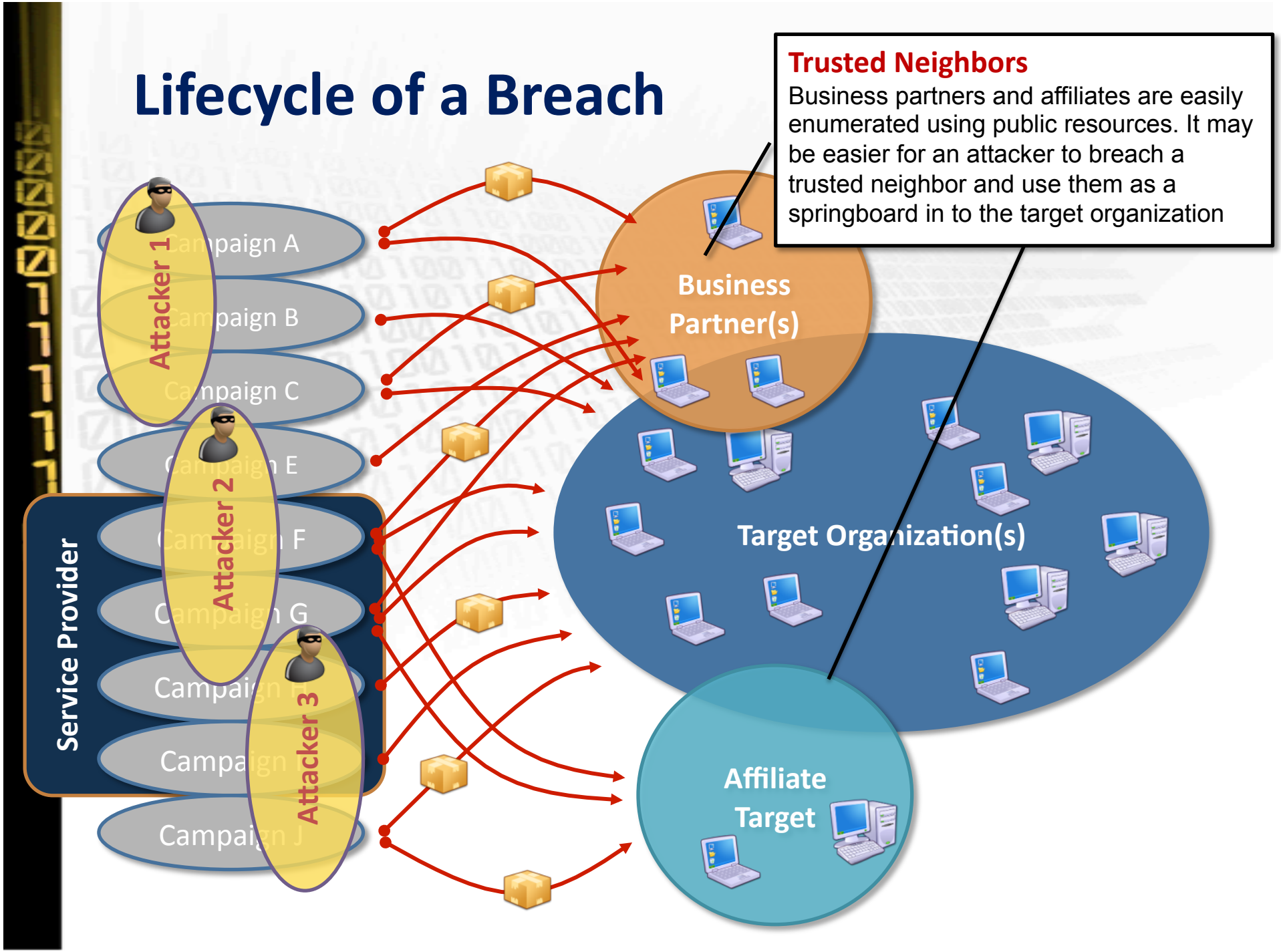
Multiple Campaigns

Attackers will launch multiple campaigns against a selection of targets. Campaigns operate independently of one another, and will purposefully make use of different attack vectors.

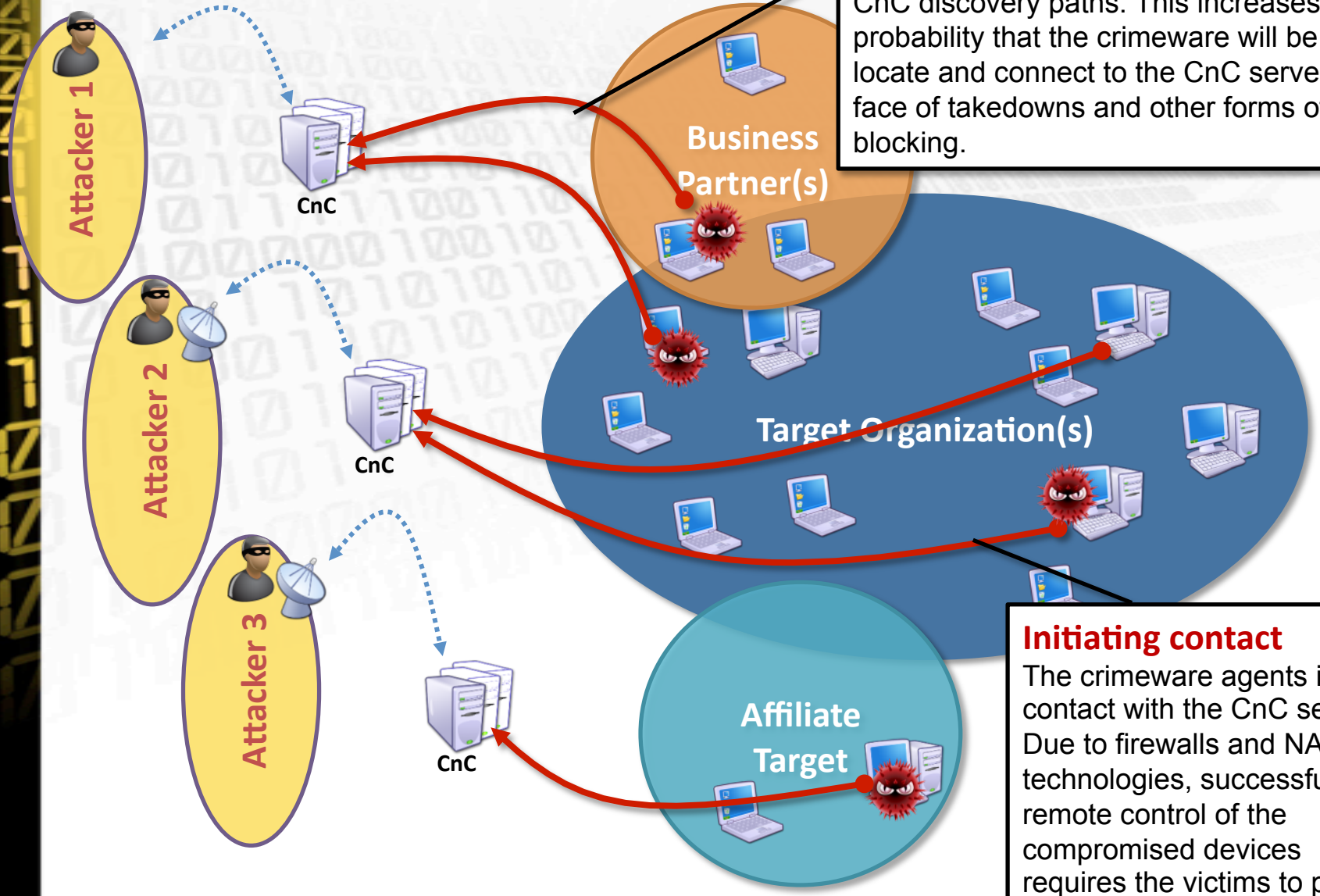
Service Providers

The services of third-party professional cybercrime providers may be purchased by the attacker(s). These services can range from spear phishing message delivery through to specific 0-day exploit manufacture.

Lifecycle of a Breach



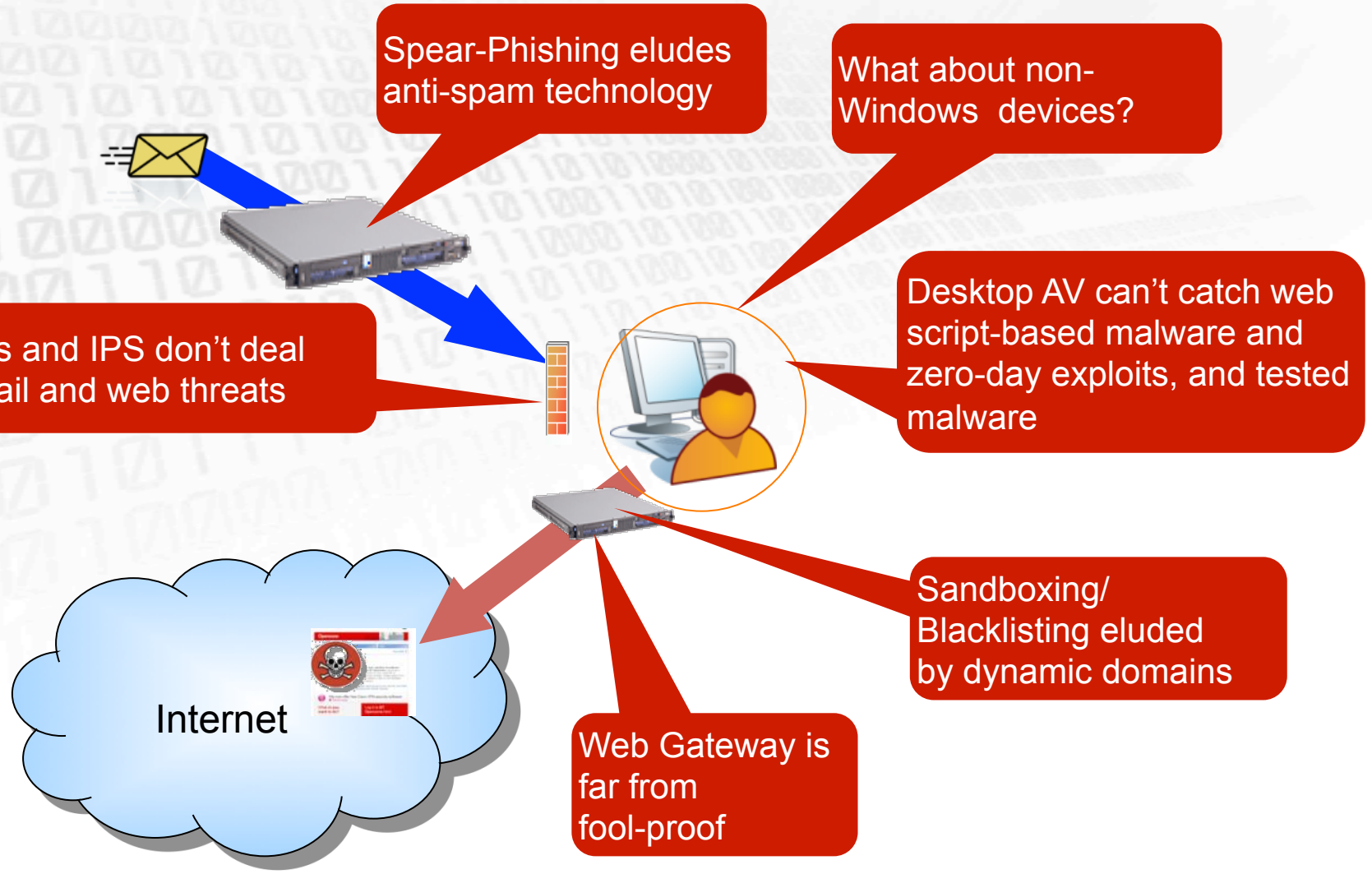
Lifecycle of a Breach



Multiple CnC's
Attackers will employ multiple CnC servers & CnC discovery paths. This increases the probability that the crimeware will be able to locate and connect to the CnC servers in the face of takedowns and other forms of blocking.

Initiating contact
The crimeware agents initiate contact with the CnC servers. Due to firewalls and NAT technologies, successful remote control of the compromised devices requires the victims to phone home (regularly).

Existing Security Measures Aren't Enough



What Can We Do to Defend Against This?

Recommendations

- Better User Awareness
- Better malware/exploit detection
- Comprehensive, real-time visibility and analysis of your network
- Monitor & Correlate events; Review your logs
- Contextual / situational awareness to determine true network behavior and intentions
- All devices covered

DAMBALLA

The Leader in Advanced Threat Protection

How is Damballa different?

1. Preemptive threat detection – the Unknown Threat
   - Big Data analysis for profiling of criminal "neighborhoods"
     - Identify never-before-seen sites
     - Obsolete the use of blacklists
   - Automated correlation and attribution to threat operators
2. Rapid, easy incident response
   - Automatically Identify the infection, threat and risk
   - Provide **actionable intelligence**
   - Avoid manual analysis of logs and false alerts
3. Option of terminating malicious communications
4. Device agnostic – PC, Mac, iPad, Android, Blackberry

Fundamentally different approach

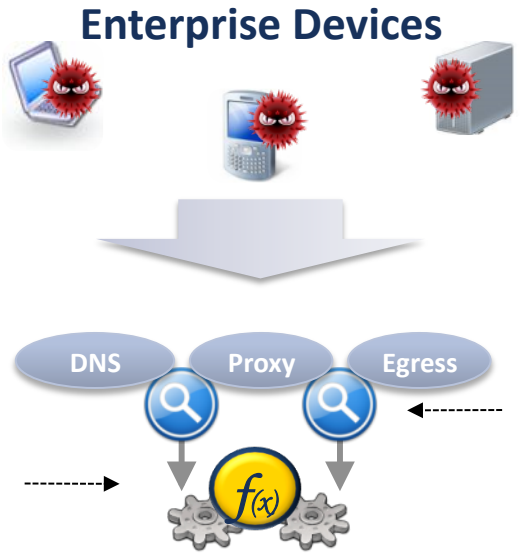
- Research backed by leading Government, academic and business organizations
- Six patents-pending

World-Class Customers

- **Over 125 million assets** protected worldwide
- Global enterprise (F2000), ISP/Telco, Higher Education, Government
- 100% customer renewals

Seamless integration into existing environments

Damballa® Failsafe



Damballa Sensor(s)
Deep Packet Inspection of All Internet Traffic

Damballa Cyber Threat Intelligence

Is the destination shady?
- Suspicious destination, low reputation or known bad

Is the traffic suspicious?
- Suspicious content, DPI of payload / executables / files

Is the behavior automated?
- Do the events appear to be software or human driven

Correlation of 'behaviors seen' pinpoints infected devices

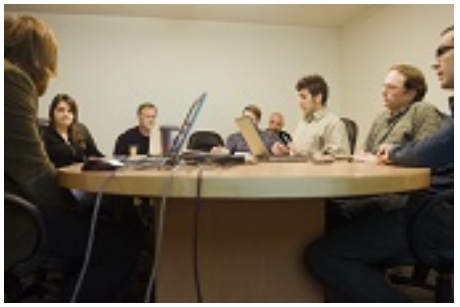
Damballa Failsafe identifies the 'unknown' threat, victim machines actively communicating with cyber criminals.

Case Studies

Fortune 50 Company

- Discovered malware associated with targeted attack

  "We could find nothing that had the capabilities of the Damballa products and also have the intelligence part updating and driving the changes."



Top 3 Energy Company

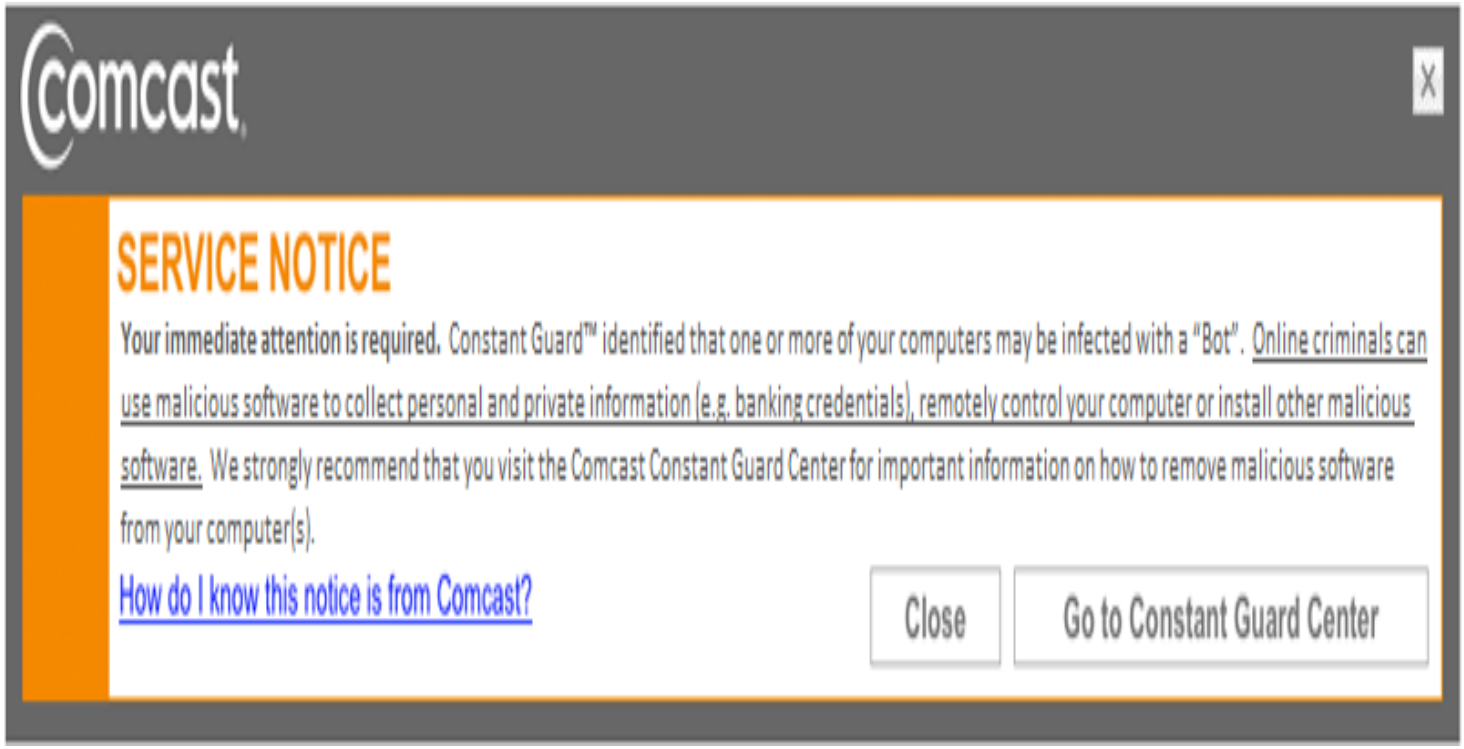
- Found State sponsored threat with data flowing to China
- And Eastern Europe crime ring stealing data from corporate SAP server

Major Bank

- Within 30 minutes discovered that 5 of 10 contractor laptops were infected and actively communicating with malware
- Contractors escorted from premises with 30 minutes

Damballa CSP for ISP and Telco

- Captures and analyzes DNS traffic to identify infected subscribers
- Provides compromised subscriber IP, “threat intent” & known remediation options
- Provides reports, data export, SIEM and third party integration



DAMBALLA

Thank You!

Visit Our table for more Information
(or setup a free evaluation)

www.damballa.com