STRATEGIES TO COMBAT TODAY AND TOMORROWS THREAT LANDSCAPE

Neil Thacker, Information Security & Strategy Officer, EMEA

TRITON STOPS MORE THREATS. WE CAN PROVE IT.
Background

- 34 years as a Thacker - 20 years as a hacker
- 15+ years Information Security (Swiss Re, Deutsche Bank, Camelot, Websense)
- ENISA (European Union Agency for Network & Information Security) stakeholder
- Co-founder of the Security Advisor Alliance
- Certified Information Systems Security Professional (CISSP) + Trainer
- Certified Ethical Hacker (CEH)
- Open-systems Professional Security Tester (OPST)
- Blogger, speaker and podcaster on all things InfoSec
- LinkedIn, Twitter: nt_hacker, Security Advisor Alliance podcast (iTunes)
Rethinking the Security Journey

- Ad Hoc
- Compliance Based
- Risk Based / Data Centric
- Business Risk Discussion
- Business Threat Discussion
- Infrastructure Based
- Threat Based
OWNERS

Wish to minimise risks wishing to abuse, steal and/or damage.

VULNERABILITIES

May be aware of threats that may be reduced by countermeasures.

COUNTERMEASURES

Reduce value that wish to exploit leading to increase risks.

RISKS

Assets wish to abuse, steal and/or damage.

THREAT

Give rise to threats that may be aware of.

THREAT AGENT

May be aware of threats that increase risks leading to.

ASSETS
Ponemon – Exposing the security cracks

The study surveyed 4,881 IT security practitioners in 15 countries with an average of 10 years’ experience in the field. This report covers the consolidated global findings.

- 57% of respondents do not think their organization is protected from advanced cyber attacks and 63% doubt they can stop the exfiltration of confidential information.
- 80% of respondents say their company’s leaders do not equate losing confidential data with a potential loss of revenue.
- 35% of those who had lost sensitive or confidential information did not know exactly what data had been stolen.

Source: http://www.websense.com/content/2014-ponemon-report.aspx
### InfoSec spend - 2014

**Data Security Is A Hot Spot For Security Spending**

*In 2014, what percentage of your firm’s IT security budget will go to the following technology areas?*

<table>
<thead>
<tr>
<th>Category</th>
<th>1,678</th>
<th>1,712</th>
<th>1,766</th>
<th>1,812</th>
<th>1,848</th>
<th>1,875</th>
<th>1,902</th>
<th>2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Email Gateway</td>
<td>2,033</td>
<td>2,160</td>
<td>2,337</td>
<td>2,514</td>
<td>2,691</td>
<td>2,861</td>
<td>3,040</td>
<td>7.1</td>
</tr>
<tr>
<td>Secure Web Gateway</td>
<td>573</td>
<td>724</td>
<td>931</td>
<td>1,190</td>
<td>1,497</td>
<td>1,857</td>
<td>2,291</td>
<td>25.9</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>61,670</td>
<td>66,377</td>
<td>71,959</td>
<td>78,025</td>
<td>84,528</td>
<td>91,546</td>
<td>98,285</td>
<td>8.4</td>
</tr>
</tbody>
</table>

**Grand Total**: 61,670  66,377  71,959  78,025  84,528  91,546  98,285  8.4
<table>
<thead>
<tr>
<th>Top Threats</th>
<th>Current Trends</th>
<th>Top 10 Threat Trends in Emerging Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Worms/Trojans</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>4. Exploit Kits</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>
Self-Encryption and Self-Decryption

- Some viruses can encrypt and decrypt their virus code bodies.
- Viruses that employ encryption might use multiple layers of encryption, which make each instance of the virus appear to be different.
Polymorphism

- A polymorphic virus generally makes several changes to the default encryption settings.
- In a polymorphic virus, the content of the underlying virus code body does not change; encryption alters its appearance only.
Stealth

A stealth virus uses various techniques to conceal the characteristics of an infection.
The idea behind metamorphism is to alter the content of the virus itself, rather than hiding the content with encryption.
Armoring

- The intent of armoring is to write a virus so that it attempts to prevent antivirus software or human experts from analyzing the viruses functions through disassembly, traces, and other means.
Tunneling

- A virus that employs tunneling inserts itself into a low level of the OS so that it can intercept low-level OS calls.
- By placing itself below software, the virus attempts to manipulate the OS to prevent detection by antivirus.
Threat agent

Motivation

- Personal Gain
- Personal Fame
- Curiosity

Attackers’ Expertise

- Hacktivist
- Hacker
- Author

User of tools

Organised Cyber Crime

Author of tools

Tools created by experts now used by less-skilled criminals, for personal gain
Which role would you choose?

“I just think it’s a pretty dangerous thing – there are some big guys behind this money. They don’t ask who you are or why you are doing this. They’ll just break both your arms”

ICQ discussion negotiating the sale of data
Hackers in reality
<table>
<thead>
<tr>
<th>Service</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa or MasterCard</td>
<td>$3</td>
</tr>
<tr>
<td>with Track 1 and 2 Data</td>
<td>$5</td>
</tr>
<tr>
<td>Name, Address &amp; DOB</td>
<td>$10</td>
</tr>
<tr>
<td>Doxing (Social)</td>
<td>$30</td>
</tr>
<tr>
<td>Online bank login</td>
<td>$100</td>
</tr>
<tr>
<td>IP</td>
<td>$50k</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>RAT</td>
<td>$20</td>
</tr>
<tr>
<td>RAT + FUD (premium)</td>
<td>$30</td>
</tr>
<tr>
<td>Botnet (15,000)</td>
<td>$200</td>
</tr>
<tr>
<td>Exploit Kit (weekly lease)</td>
<td>$250</td>
</tr>
</tbody>
</table>
STRUCTURED DATA
3742-4963-5398-4312

EASY TO PROTECT

UNSTRUCTURED DATA

INTELLECTUAL PROPERTY
Merger Acquisitions
Customer

HARD TO PROTECT
What am I trying to protect?

How am I trying to protect it?
Twin fundamentals to success
7 stage kill-chain

Target Organisation

Employee → Email server → Compromised machine → Attacker

Web proxy

Compromised Website

Control server
### Tier 1
- Firewall or NGFW
- Endpoint Antivirus
- Secure web gateway
- Secure email gateway
- IDS/IPS
- Encryption
- SIEM

### Tier 2 (context layer)
- Breach Detection Systems
- Network/Desktop forensics
- Data Leakage Prevention (network/endpoint)
- Behavioral-based analytics
- Threat intelligence feeds
- Threat forecasting and modeling

“T1 security technologies are mainly geared for attacks that are known by the security community. Additionally, most of these T1 security technologies are typically accounted for in the fiscal year budget cycle” John Pirc, NSS Labs
Company stalking in Maltego
Company stalking

### Templates

Please select the tree to view available templates

**Available Templates:**

- OWA template
- Twitter New Follower Template
- eBay Account Suspension

### HTML/Modifier View

```
[[Alias Target: Target]],
You have a new follower on Twitter!
```

```
[[Twitter Profile Name: From Profile Name]]
@[[Alias Find: From Profile]]

[[Twitter Profile Bio: From Profile Bio]]
```
Why spear-phishing is still successful...

Source: Causal Loop Diagram of Social Engineering of Insiders by Outsiders (CERT CMU)
HOW WE SECURE THE PERIMETER TODAY
HOW WE SECURE THE PERIMETER TODAY

MAJORITY OF THE SECURITY SPEND HAS BEEN FOCUSED IN STOPPING OR DETECTING THE THREATS ON THE NETWORK OR DEVICE
HOW WE SECURE THE PERIMETER TODAY

IN COMPARISON LITTLE SPEND HAS BEEN PUT TOWARDS USER ACTIVITY AND DATA PROTECTION. MOST ORGANIZATIONS ARE IMMATURE IN UNDERSTANDING USER AND DATA BEHAVIOUR.

Device -> Application -> User -> Network -> Data
New EU Data Protection Legislation

- Appointment of Data Protection Officer
- Right to be “Erased” requirement
- Mandatory disclosure of data incidents within 72hrs
- Data Controller and Processor Accountable
- Fines 5% of WW revenue or 100m Euro
Strategy change
From prevent to predict (+ prevent)

Ad Hoc & Infrastructure Based

EVOLVED TO

Business Enablement & Threat Based Discussions
Source of threat...sometimes unlikely

Network Admin Allegedly Hacked Navy—While on an Aircraft Carrier
BY KIM ZETTER  05.07.14  |  8:05 PM  |  PERMALINK

How to Use Your Cat to Hack Your Neighbor’s Wi-Fi
BY ANDY GREENBERG  08.08.14  |  6:30 AM  |  PERMALINK

Image: Paul Farley/U.S. Navy

Coco, modeling the WarKitty collar. ☺ Gene Bransfield
<table>
<thead>
<tr>
<th>PEOPLE</th>
<th>TECHNOLOGY</th>
<th>PROCESS</th>
<th>METRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness</td>
<td>DLP (Network/Client)</td>
<td>IRM</td>
<td>Business Process</td>
</tr>
<tr>
<td></td>
<td>SIEM</td>
<td>Device Management</td>
<td>Data Classification</td>
</tr>
<tr>
<td></td>
<td>Network/Desktop Forensics</td>
<td>DAP</td>
<td>Incident Response</td>
</tr>
<tr>
<td></td>
<td>Behaviour-Analytics</td>
<td>ACL</td>
<td>Sentiment analysis</td>
</tr>
<tr>
<td></td>
<td>FIM</td>
<td></td>
<td>Security Awareness</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Indicators</td>
</tr>
</tbody>
</table>
ML + TI = PA

Asset-centric
- Assets
- Ownership
- Business Context

Attacker-centric
- Threats
- Vectors
- Kill-chain

THREAT INTELLIGENCE

MACHINE LEARNING

Pre-incident
- Pattern
- Triage
- Action

PREDICTIVE ANALYTICS
Summary

1. Improve relationship between owner and asset

2. Context layer from security events – primary source DLP

3. Review tier 1/tier 2 tech strategy – apply context to all

4. Threat model based on kill-chain to ID patterns/countermeasure

5. Use Machine Learning to reduce false positives

5a. Move forward with risk-based, data centric…FTW!
THANK YOU – QUESTIONS
NTHACKER@WEBSENSE.COM

Neil Thacker, Information Security & Strategy Officer, EMEA

TRITON STOPS MORE THREATS. WE CAN PROVE IT.