



数字化时代 安全新生态

2016 中国网络安全峰会

庄敬贤 思科大中华区安全业务总经理

我们所处的网络环境是否足够安全？

数字化颠覆， 大规模展开

到2020年，网络互联
设备总量将达到500亿
台

孕育着19万亿美元的
业务机会

业务模型在变化

对手越来越活跃

攻击面更广

威胁源更多

攻击复杂度更高

安全挑战

动态的威胁格局

安全产业

安全企业数量激增

互通性差

开放性差

复杂且分散



网络安全防御状态

防御能力倍增 安全问题堆积如山





弥补安全有效性缺口

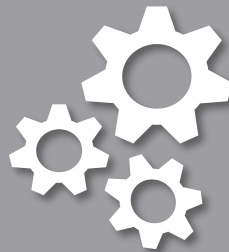
集成化



整合化



自动化



思科安全解决方案: 安全无处不在

最佳产品组合

集成化架构方法



安全无处不在

覆盖整个攻击周期

攻击前

攻击过程中

攻击后



终端



分支机
构



边界



园区网



数据中心



云



运作技术



服务





让所有威胁载体都能被看见

看见威胁是实施防御的前提



终端



分支机
构



边界



园区网



数据中心



云



运作技术

思科安全与众不同之处： 集成式架构




Ransomware (勒索软件)



Locky 勒索软件

发件人: Octavio Rodriquez [mailto:RodriquezOctavio72730@arcova.net]
发送时间: 2016年2月16日 3:59
收件人: [REDACTED]
主题: FW: Payment ACCEPTED M-145218

 payment_details_145218.zip(5.4 K)

Dear zhaoy,

Please check the payment confirmation attached to this email.
The Transaction should appear on your bank in 2 days.

Thank you.

Octavio Rodriquez
Financial Manager

!!!重要資訊 !!!

您的所有檔已被RSA-2048 和AES-128暗碼進行了加密。
欲獲取更多關於RSA的資訊，請參閱：

<http://zh.wikipedia.org/wiki/RSA加密演算法>
<http://zh.wikipedia.org/wiki/高級加密標準>
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

只有我們的機密伺服器上的私人金鑰和解密程式才能解密您的檔。
如要接收您的私人金鑰，請點擊以下其中一個連結：

1. <http://6dbxgqam4crv6rr6.tor2web.org/F708955F1927B0D1>
2. <http://6dbxgqam4crv6rr6.onion.to/F708955F1927B0D1>
3. <http://6dbxgqam4crv6rr6.onion.cab/F708955F1927B0D1>
4. <http://6dbxgqam4crv6rr6.onion.link/F708955F1927B0D1>

如果以上位址都無法打開，請按照以下步驟操作：

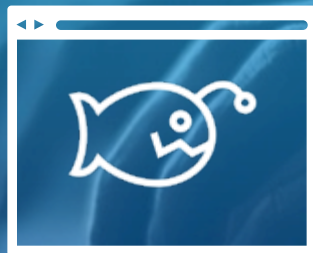
1. 下載並安裝洋葱瀏覽器 (Tor Browser) : <https://www.torproject.org/download/download-easy.html>
2. 安裝成功後，運行瀏覽器，等待初始化。
3. 在位址欄輸入: 6dbxgqam4crv6rr6.onion/F708955F1927B0D1
4. 按照網站上的說明進行操作。

!!! 您的個人識別ID: F708955F1927B0D1 !!!

钓鱼邮件



用户点击恶意链接或恶意广告



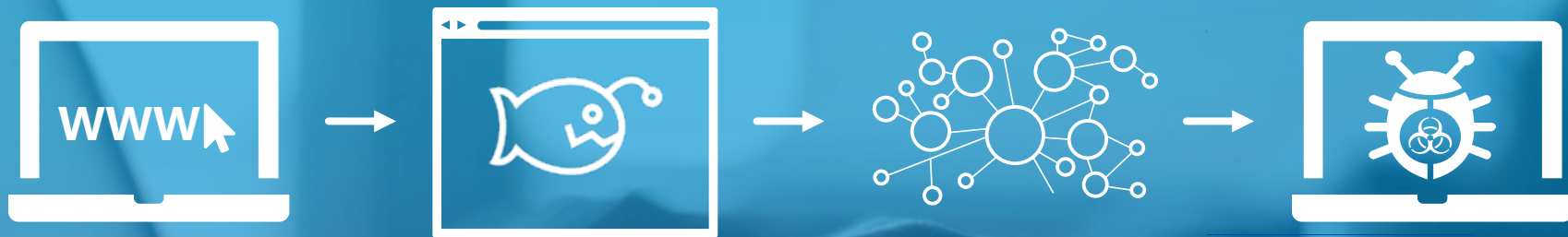
恶意代码植入



用户连接到黑客基础架构



用户被植入勒索软件



或者是...



包含恶意附件邮件



用户被植入勒索
软件

你的文件被加密了!



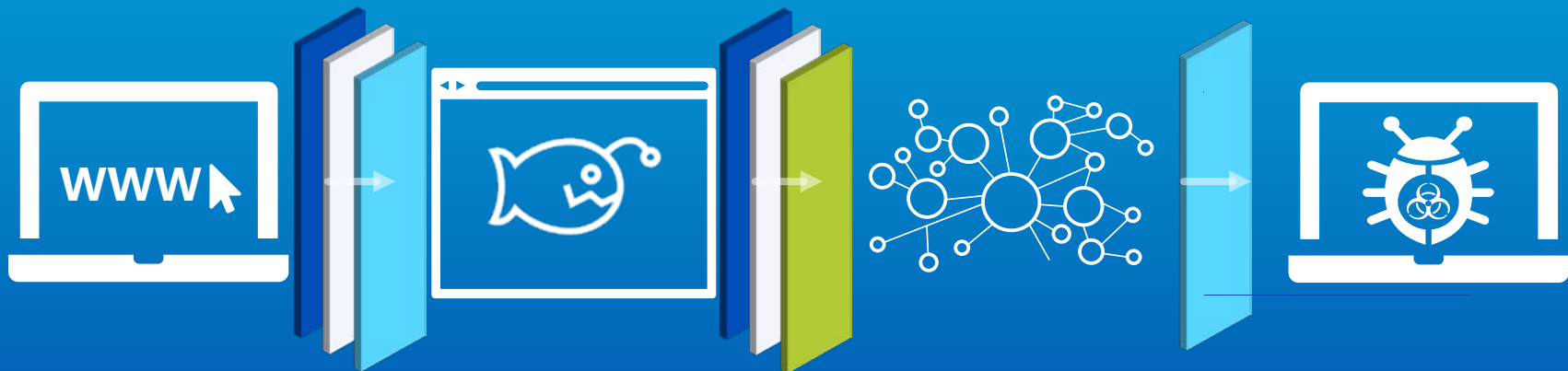
思科如何保护用户

● OpenDNS

● Next-Gen Firewall

● AMP

● Stealthwatch



OpenDNS 阻止恶意链接访问
NGFW 阻断连接
Web安全/AMP 阻止恶意软件下载

OpenDNS 阻止对恶意地址访问
NGFW 阻断链接
Lancop 检测恶意活动

终端高级恶意软件防护(AMP) 阻止
恶意软件植入和防止回传连接

● OpenDNS

● 下一代防火墙

● AMP

● Stealthwatch



从架构上强化安全防御能力

思科安全防护覆盖网络，终端和云平台



OpenDNS

云安全

可以在导致破坏之前阻断95%的威胁



高级恶意软件防护

以威胁防护为中心，安全防护无处不在
这是针对已知和高级别威胁最有效的安全解决方案



下一代防火墙

威胁分级

自动响应

提高恶意软件防护

完全集成管理



Stealthwatch

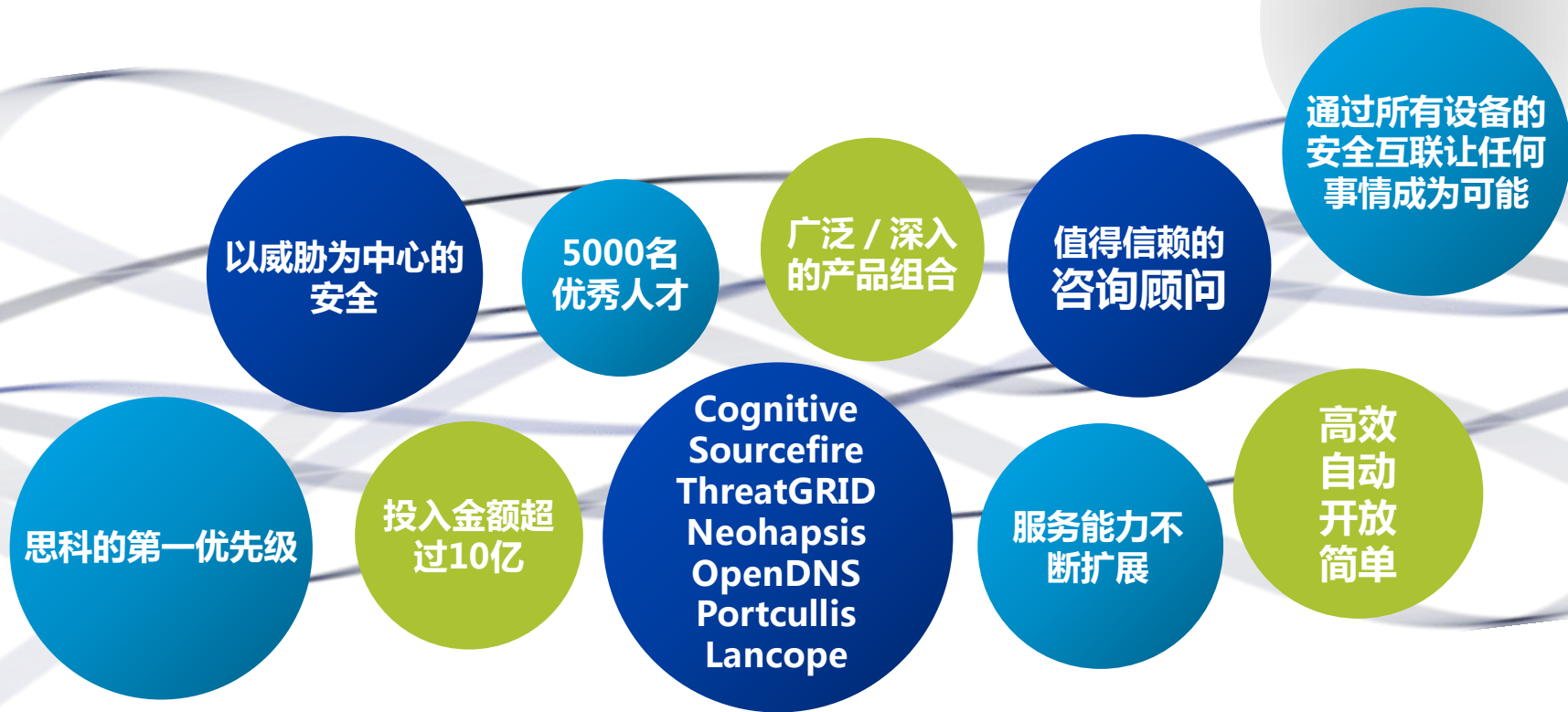
和感染主机通讯时产生告警

防止网络中感染主机间通讯

使用网络作为探测器控制和减缓威胁



思科安全的承诺



思科是全球网络安全领导者



思科的安全防御无处不在 ... “做得非常出色”

CRN

“Palo Alto、FireEye等企业所依赖的技术已经过时”

CIO 的客户偏好情况
调查结果

PiperJaffray  UBS  BARCLAYS

Gartner

“需要通过新的产品和 / 或服务让网络安全架构成为安全事件检测和响应策略必不可少的一部分。”

SC
MAGAZINE

2016年最佳网络安全技术公司

William Blair

“思科总能正确出招.....比如开发了基于软件的云产品组合、网络安全业务呈现双位数增长率、成功收购OpenDNS等企业.....”

citi

“思科在网络安全业务方面的能力反映出它并不是一家‘守旧的’科技公司。”

简单| 开放| 自动| 高效

思科 安全



