Q Are your company laptops secure?

matta

Q Are your company laptops secure?

- Data Theft
- VPN Compromise
- Account Credential Compromise

matta

About Matta

Security Consultancy since 2001:

- Penetration Testing
- Application Testing
- Code Review
- Binary Evaluation
- Training
- Vulnerability Assessment

Largest Clients:

- Financial
- Retail
- e-Commerce

The Team Today

James Tusini - Technical Director

Nick Baskett - Managing Director

matta

Where we Work

In the last 12 months:

- UK
- Netherlands
- USA
- Singapore
- Hong Kong
- China
- India
- Saudi Arabia

matta

A Short Chronology in Security

matta

First Virus Ever Discovered
1981

Elk Cloner on Apple II

First Extensive Spreading Worm
1988

Morris Worm, Vax and Unix machines, spreads over the internet. Used Buffer Overflows

CERT Founded
1989

Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses

FIRST Founded
1990

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

First Phishing Attack
1996

Originally described in 1987, was used on AOL accounts after AOL put in measures to prevent fake CC number generation. Attackers posed as AOL staff member and asked for username and password credentails on IM

OWASP Founded
2001

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Ni Hao mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

1985 1990 1995 2000 2005 2010 2015

Vulnerbility History


First Virus Ever Discovered
1981
Elk Cloner on Apple II
CERT Founded
1989
Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses
FIRST Founded
1990
Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS
First Vulnerability Scanner
1995
SATAN
Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools
First Phishing Attack
1996
1985
1990
1995

First Extensive Spreading Worm
1988

Morris Worm, Vax and Unix machines, spreads over the internet. Used Buffer Overflows

CERT Founded
1989

Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses

FIRST Founded
1990

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

OWASP Founded
2001

Non profit organisation with widespread acceptance.

PCI Standard Formed
2006

Client Side Vulnerabilities
2007

Fake Cisco Kit
2008

Ni Hao mass SQL injection
2008

First Extensive Spreading Worm
1988

Morris Worm, Vax and Unix machines, spreads over the internet. Used Buffer Overflows

CERT Founded
1989

Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses

FIRST Founded
1990

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

First Phishing Attack
1996

Originally described in 1987, was used on AOL accounts after AOL put in measures to prevent fake CC number generation. Attackers posed as AOL staff member and asked for username password credentials on IM

OWASP Founded
2001

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

First Extensive Spreading Worm
1988

Morris Worm, Vax and Unix machines, spreads over the internet. Used Buffer Overflows

CERT Founded
1989

Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses

FIRST Founded
1990

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

First Phishing Attack
1996

Originally described in 1987, was used on AOL accounts after AOL put in measures to prevent fake CC number generation. Attackers posed as AOL staff member and asked for username and password credentails on IM

OWASP Founded
2001

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2005

Fake Cisco Kit
2008

$1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Hi Hac mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

2000 2005 2010

Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses

FIRST Founded
1990

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

First Phishing Attack
1996

Originally described in 1987, was used on AOL accounts after AOL put in measures to prevent fake CC number generation. Attackers posed as AOL staff member and asked for username and password credentails on IM

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

NI Hao mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

1995 2000 2005 2010 2015

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

First Phishing Attack
1996

Originally described in 1987, was used on AOL accounts after AOL put in measures to prevent fake CC number generation. Attackers posed as AOL staff member and asked for username and password credentails on IM

suggested wireless was as secure as
d strong encryption. Wired Equivelancy Protocol
(WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit

1990
1995
2000
2005
2010
2015

OWASP Founded
2001

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit

m

achines, spreads over the
s

ency Response Team. Part of the
neering Institute. Helps with training
entres that study and coordinate

rks closely

OWASP Founded
2001

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adapt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

SQL injection

...flaws in MS SQL server

...s, spreads over the

...Response Team. Part of the
...ng Institute. Helps with training
...s that study and coordinate

...onse Security Teams. Works closely
...s standards like CVSS

First Vulnerability Scanner
1995

...ticated, but caught the imagination of
...d spawned a whole industry

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Ni Hao mass SQL injection
2008

mass SQL injection attack uses flaws in MS SQL server

Vulnerbility History

Original founder

Vulnerabilities

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Ni Hao mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

d, but caught the imagination of
and spawned a whole industry

87, was used on AOL accounts after
revent fake CC number generation.
taff member and asked for username
IM

2010

2015

Vulnerbility History

aught the imagination of
awned a whole industry

s used on AOL accounts after
fake CC number generation.
mber and asked for username

as secure as
ed Equivelancy Protocol

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Ni Hao mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

Vulnerbility History

2005

2010

2015

t caught the imagination of
spawned a whole industry

vas used on AOL accounts after
nt fake CC number generation.
nember and asked for username
IM

seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Ni Hao mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

Vulnerbility History

2005

2010

2015

First Virus Ever Discovered
1981

Elk Cloner on Apple II

First Extensive Spreading Worm
1988

Morris Worm, Vax and Unix machines, spreads over the internet. Used Buffer Overflows

CERT Founded
1989

Carnegie Mellon - Emergency Response Team. Part of the University Software Engineering Institute. Helps with training and planning, and has centres that study and coordinate emergency responses

FIRST Founded
1990

Forum for Incident Response Security Teams. Works closely with CERT, and promotes standards like CVSS

First Vulnerability Scanner
1995

SATAN

Not easy to use or sophisticated, but caught the imagination of network engineers at the time, and spawned a whole industry in security tools

First Phishing Attack
1996

Originally described in 1987, was used on AOL accounts after AOL put in measures to prevent fake CC number generation. Attackers posed as AOL staff member and asked for username and password credentails on IM

OWASP Founded
2001

Non profit organisation with widespread acceptance.

Publishes top 10 list of web based vulnerabilities

Mark Curphey original founder

Wireless becomes mainstream
2001

Initial propegander suggested wireless was as secure as wired due to strong encryption. Wired Equivelancy Protocol (WEP)

PCI Standard Formed
2006

Visa and Mastercard founded PCI Co to put a framework in place that would force retailers to adopt security more seriously.

Client Side Vulnerabilities
2007

SANS noted that hackers found rich pickings amongst client applications

Fake Cisco Kit
2008

£1.75m of fake Cisco kit was seized by FBI. US Navy and Air Force had purchased some of the chinese knock-offs.

Researcher Samuel King demonstrated virtually un-detectable backdoors were possible with modified chips

Ni Hao mass SQL injection
2008

First mass SQL injection attack uses flaws in MS SQL server

1985 1990 1995 2000 2005 2010 2015

Vulnerbility History

20 Years on...

Attackers still find new ways, and interesting new methods on old ways to compromise systems

matta

Client Side Exploitation

Why attackers have been focusing on Clients

matta

Why?

- Very few internet-facing services nowadays
- Enterprise OS's are getting more secure
- Webapps are still vulnerable but frameworks are providing some security
- More stealthy - who cares if a user's machine crashes?
- Easier to find vulnerabilities in client-side software

matta

What?

- XSS - Malicious HTML / Javascript in injected on the clients' browsers
- Memory corruption vulnerabilities in client-applications (Browsers + plugins and commonly used third party software)
- Network foo - Intercepting traffic in various ways (ARP / DNS / DHCP Spoofing, MiTM, TCP Session Hijacking, etc.)

matta

How?

- Social Engineering - click on this link / open this file
- Running a rogue network? Rogue AP?
- Polluting online sites with malware

matta

Rogue AP

- Essentially an Access Point in promiscuous mode
- Personally tested in various locations. On plane, within seconds 30+ connections. Customer sites, many associations within seconds.
- Big problem because it’s hard to detect, even for a savvy guy with security expertise

matta

How does it work?

- Attacker sets up Powerful Wireless Card in Master mode (Acting as an Access Point in promiscuous mode)
- Clients probe their favorite networks on a regular basis, we respond to all requests (linksys, NETGEAR, BT_Openzone, etc.)
- Associated already? - no problem send DEAUTH

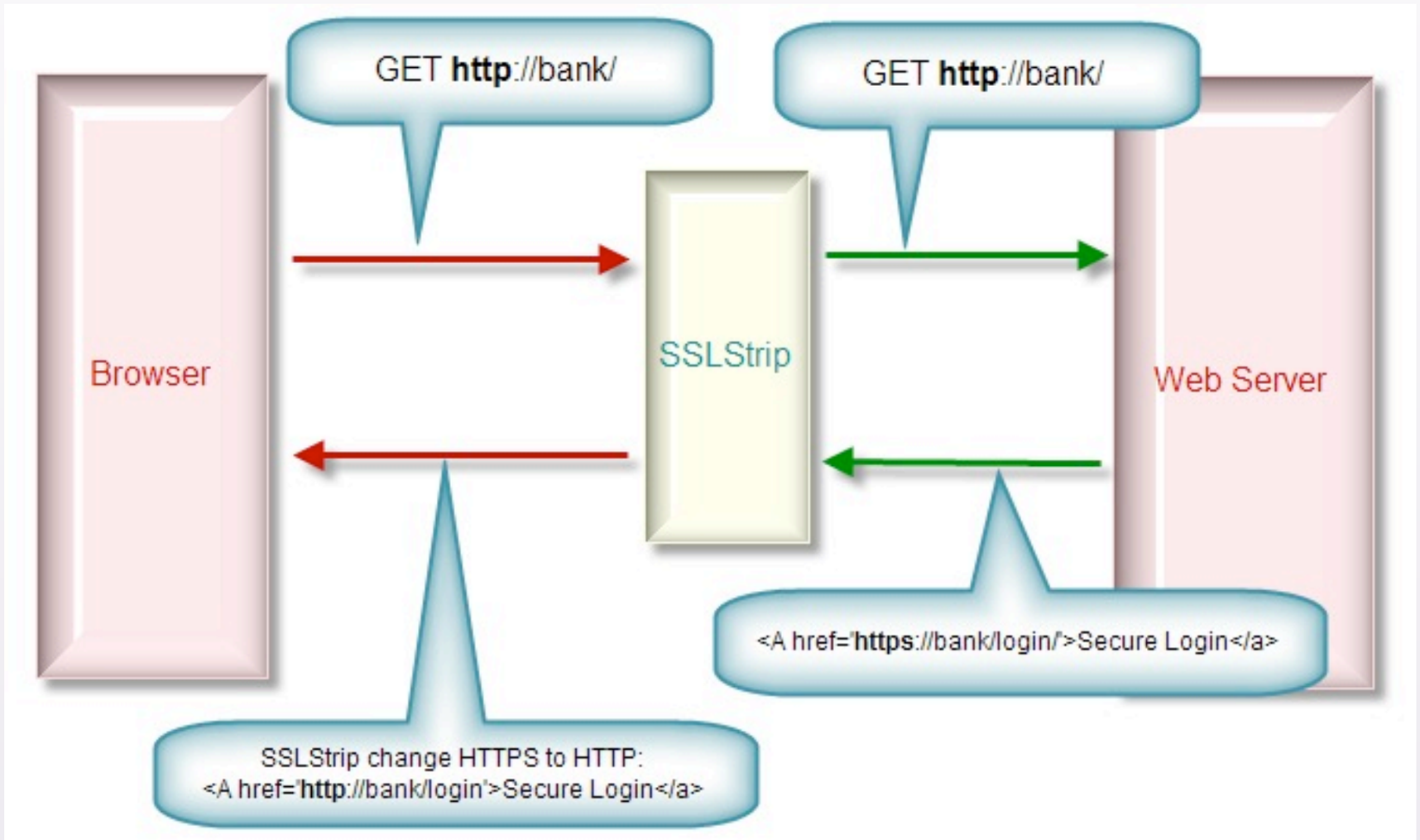
matta

What can we do?

- Everything!
- We control DNS
- We route your traffic - modify / inject packets
- MiTM SSL or better strip it
- Poison your cache with malicious JS
- Are your updates secure? I think not

matta

SSLStrip



matta

Questions

matta