

Riding the Tide With Cyber Security & Limitations of Current Security Technologies

Srinivas Mukkamala

Institute for Complex Additive Systems and Analysis

CAaNES

Computational Analysis and Network Enterprise Solutions

Information Assurance Research as a Service (RaaS)

New Mexico Tech

Who Am I?

- Senior Research Scientist and Adjunct Faculty
 - New Mexico Tech - ICASA
 - PhD Computer Science
 - Computational Intelligent Techniques for Intrusion Detection
 - US Patent
 - Computational Intelligence for Intrusion Detection
 - One of the Most Cited and Downloaded Papers
 - Intrusion Detection Using Ensemble of Intelligent Paradigms
- Author – Co Author of 120 Peer Reviewed Publication
- CACTUS Project – One of the Leads
 - Computational Analysis of Cyber Terrorism Against the US
- Managed Several Security Engagements
 - Security Posture Assessments
 - Incident Response and Digital Forensics



7941855



Core Strengths

ICASA

NMT

Data Mining

Risk and Vulnerability Management

Digital Forensics and Electronic Discovery

DHS/NSA Center for Excellence

CACTUS

CAaNES - MVP™

CAaNES - KEMA™

Research

Open Web Mining and Blog Analysis

Malware Synthesis and Analytics

Information Retrieval

Phishing Detection and Media Analysis

BRAVE™ - Incident Response

Electronic Discovery

Education

Course Offering (NMT and Other CAEs)

Continuing Legal Education

Short Courses

Offsite and Out of State Seminars

Information Assurance

Digital Forensics (CLE)

Application and Web Security

Practicum Courses

Service

Several Clients in NM, CO, AZ, UT, NV

High Profile Lawsuits

Private Clients...

Federal Government

Assessments and Penetration Testing

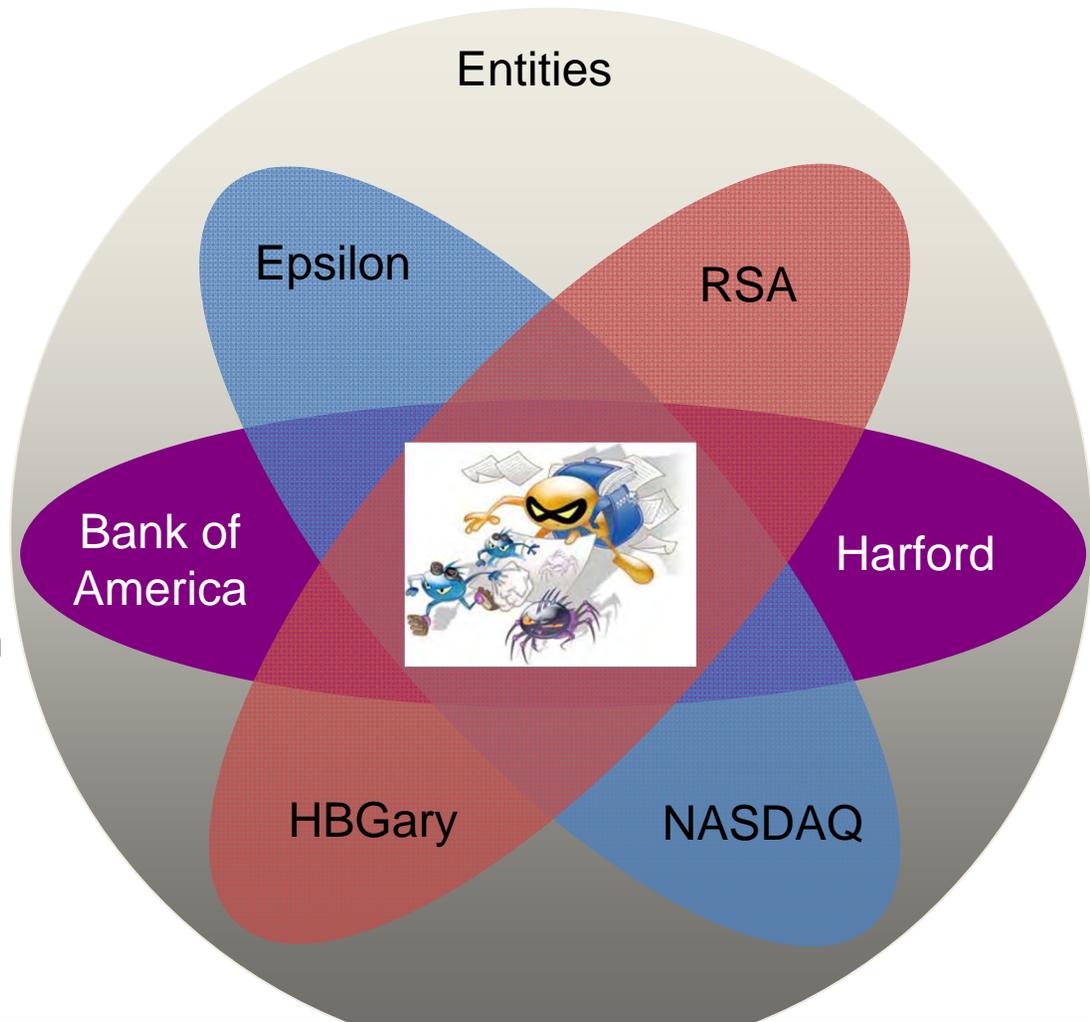
Electronic Discovery

Incident Response

Applied Research

Recent Notable Breaches

- Do we have adequate security controls ?
- If so what is the reason for high profile breaches
 - Epsilon | ??????
 - RSA | Flash Object – Excel
 - **CVE-2011-0609**
 - Hartford | W32-Qakbot Trojan
 - NASDAQ | ?????
 - HBGary | SQL Injection – SE
 - Bank of America | Zeus

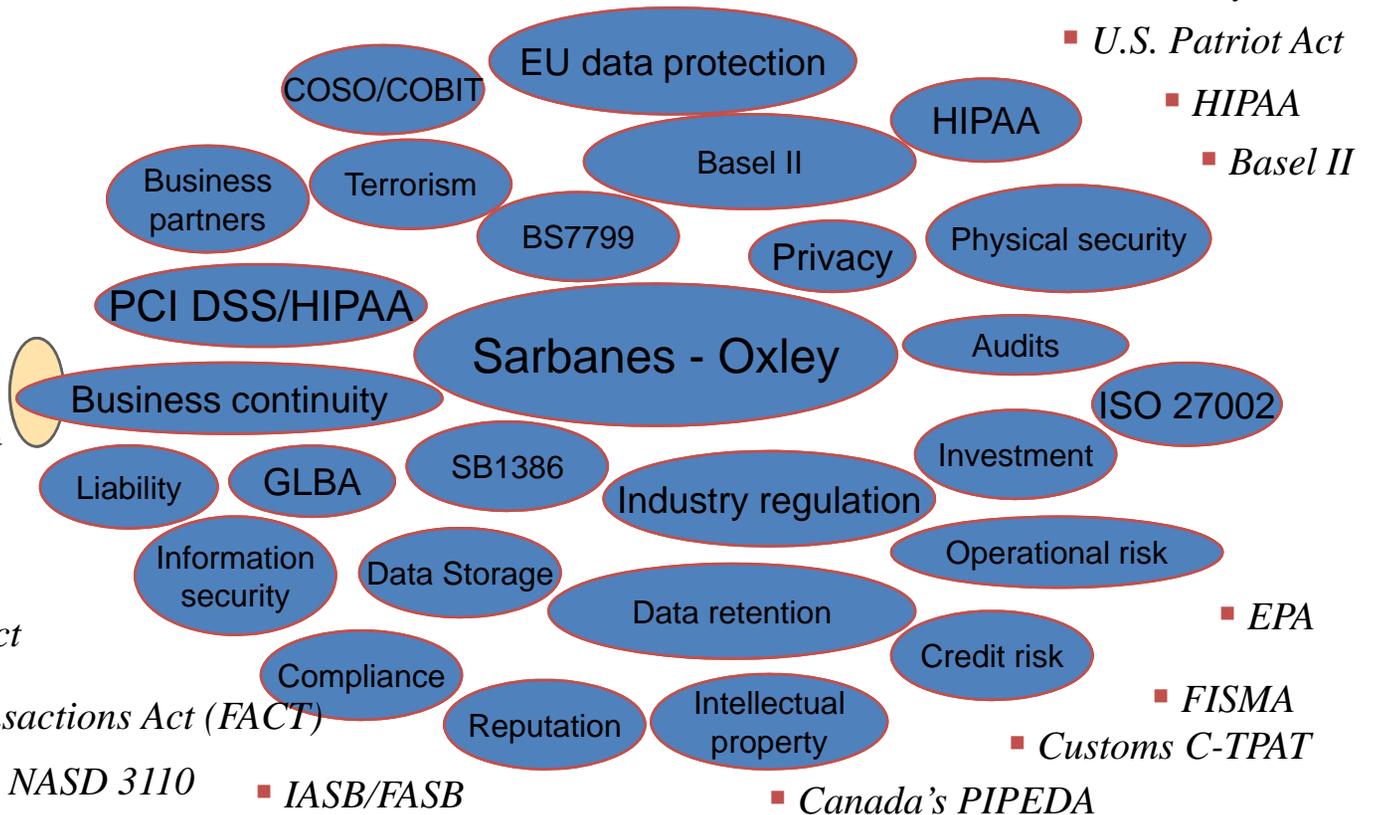


“Attacks Made Simple”

Entities Should Comply With Multiple Regulations

Growing lists of regulations can deplete resources

- *Gramm-Leach-Bliley*
- *Sarbanes-Oxley Act of 2002*
- *U.K. Public Records Office DOD 5015.2*
- *E.U. Data Protection Directive*
- *CA SB 1386, 1950*
- *FDA 21 CFR 11*
- *Homeland Security Act*



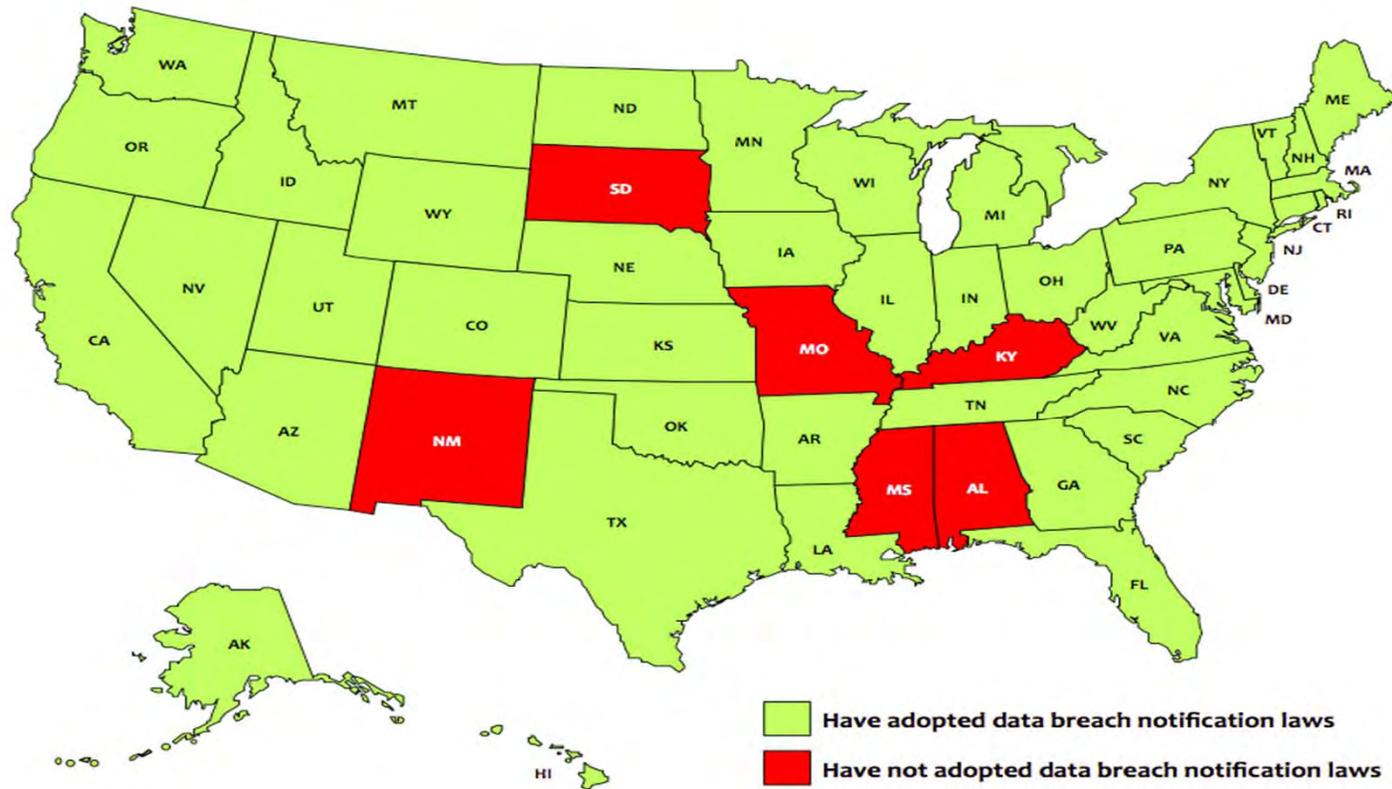
- *Computer Security Act*
- *Foreign Corrupt Practices Act*
- *SEC Rules 17a-3 and 17a-4*
- *Computer Fraud and Abuse Act*
- *Fair and Accurate Credit Transactions Act (FACT)*
- *TREAD Act*

- *NASD 3110*
- *IASB/FASB*

- *U.S. Patriot Act*
- *HIPAA*
- *Basel II*
- *EPA*
- *FISMA*
- *Canada's PIPEDA*

Regulations and Compliance Requirements

Breach Notification Laws



Data Source: National Conference of State Legislatures

Breach Notification Costs



Home

Start Calculator >>

DataBreachCalculator.com

About >>

Calculator >>

Results >>

Preventative Solutions >>



“Our research reinforces best practices for IT security and privacy and argues that those practices provide a positive return on investment.”

Results

Based on your inputs and our trend data, your risk exposure is:

- Companies in your industry with your risk profile have a likelihood of experiencing a data breach in the next 12 months of **9.4%**
- Your average cost per record is **\$224**
- Your average cost per breach is **\$16,808,333**

Customized Report

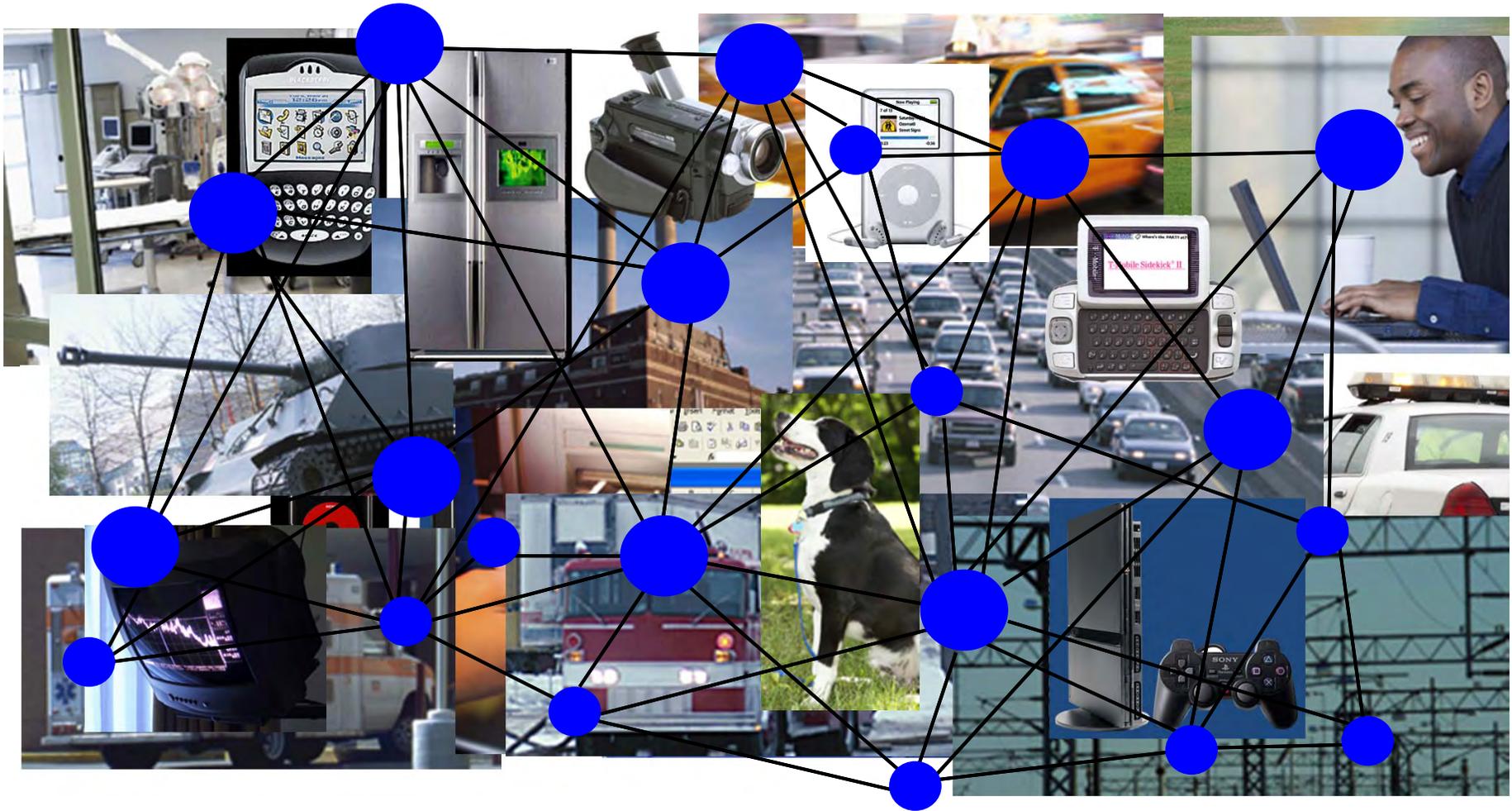
You can get a customized report with your risk profile data as well as details about how your risk profile compares with:

- Companies in your industry
- Companies in other industries
- Companies that have a CISO
- Companies that do not have a CISO
- Companies with same number of employees
- Companies with operations in one country
- Companies with operations in multiple countries

<http://databreachcalculator.com.sapin.arvixe.com/Calculator/Result.aspx>

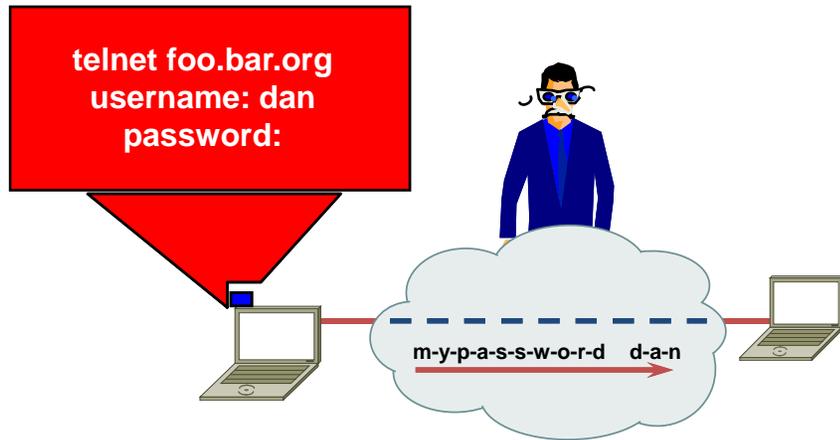
<http://www.networkworld.com/news/2011/030811-ponemon-data-breach.html>

Hyper Connectivity

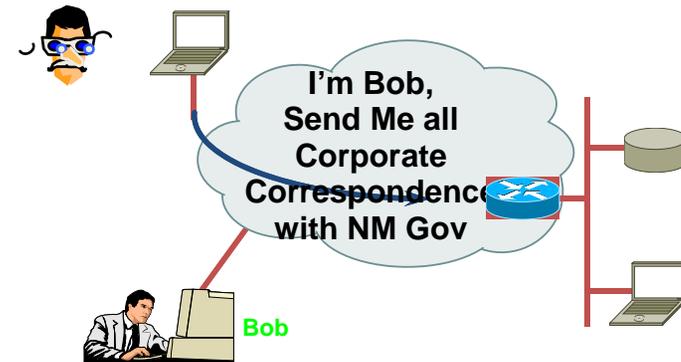


**Anything that *can* be connected will be connected.
What about security?**

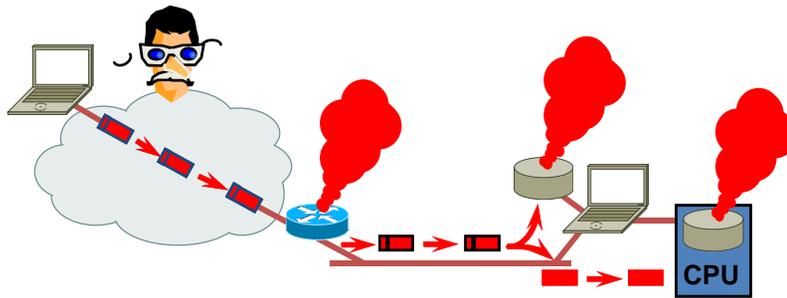
Why Information Assurance ?



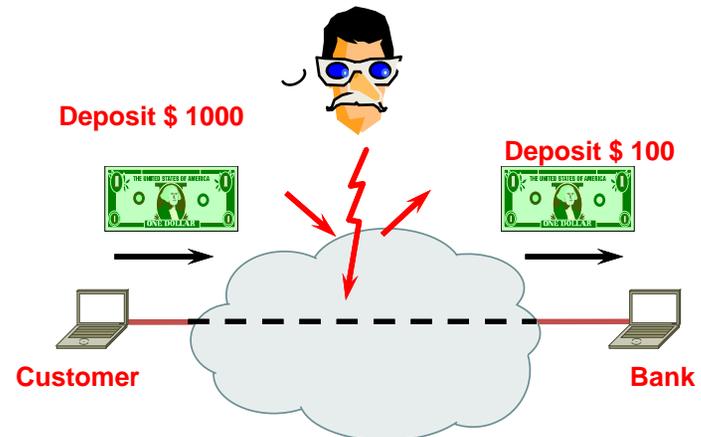
Loss of privacy



Loss of confidentiality

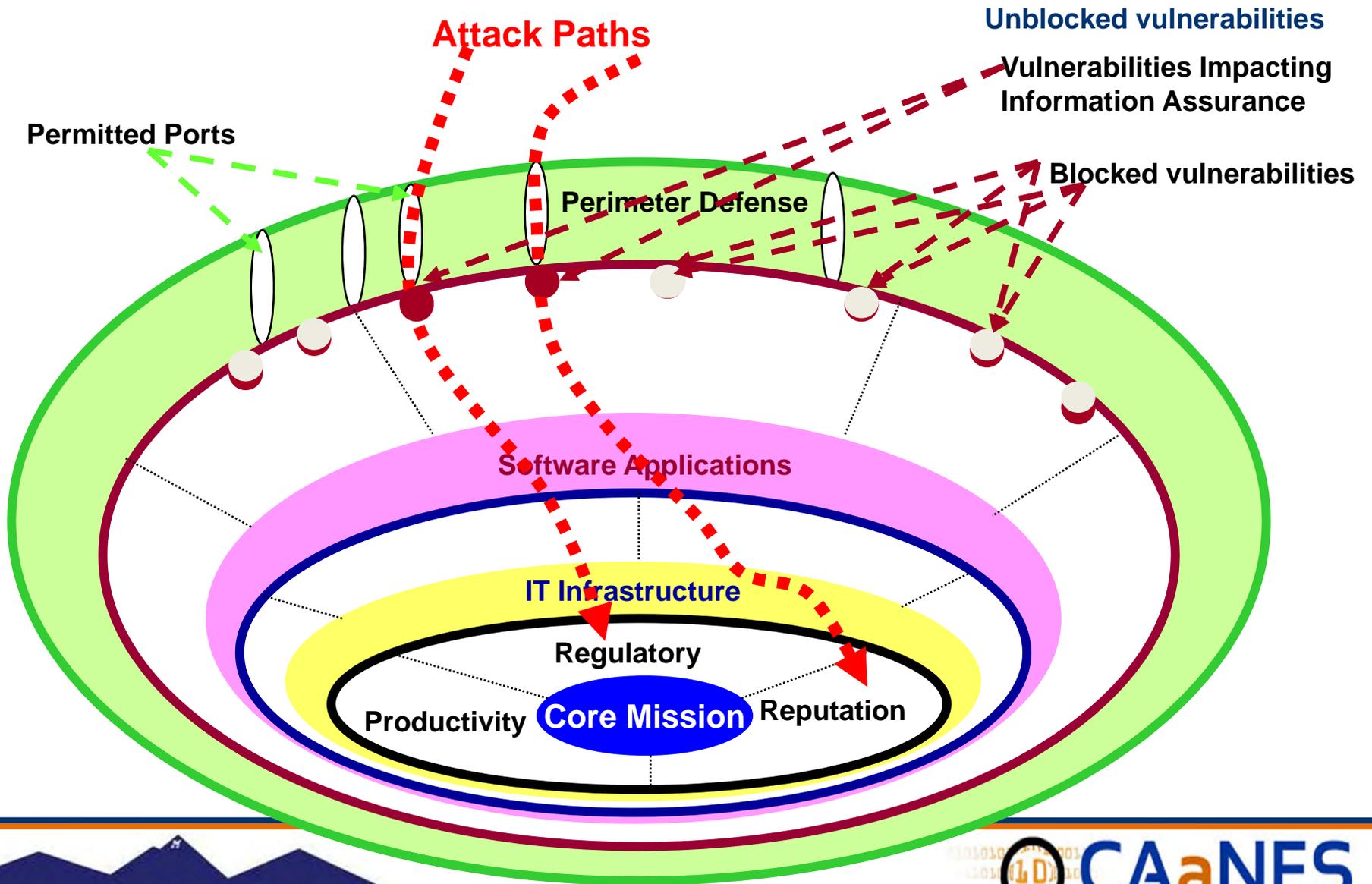


Denial of service



Loss of integrity

Everyone Has A Problem - No One is Immune



Financial Crimeware - DIY

- Attack Techniques, Sources and Monetization
 - Complex Spread Techniques
 - Automated Exploitation Systems, Ready-Made Exploit Packs
 - Packed



manhat Peon

PPI Affiliate Program - pmssoftware.us

Looking for an interesting solution for your traffic?
Check out our [ppi affiliate](#) program, you will be pleasantly surprised with how much you can get from it!
Registration is invite only. Rates are individual for any traffic.

Emerging Threats | RATs!

- They Evade Anti-virus
- Remain Undetected by most Security Technologies
 - IDPS | IDS!
- Defeat Under-equipped Security Teams
 - Remaining undetected on the target's network
 - Playing a game of cat and mice
- Packed and Encrypted



Anatomy of Malware



**1- The Enabling
Vulnerability**

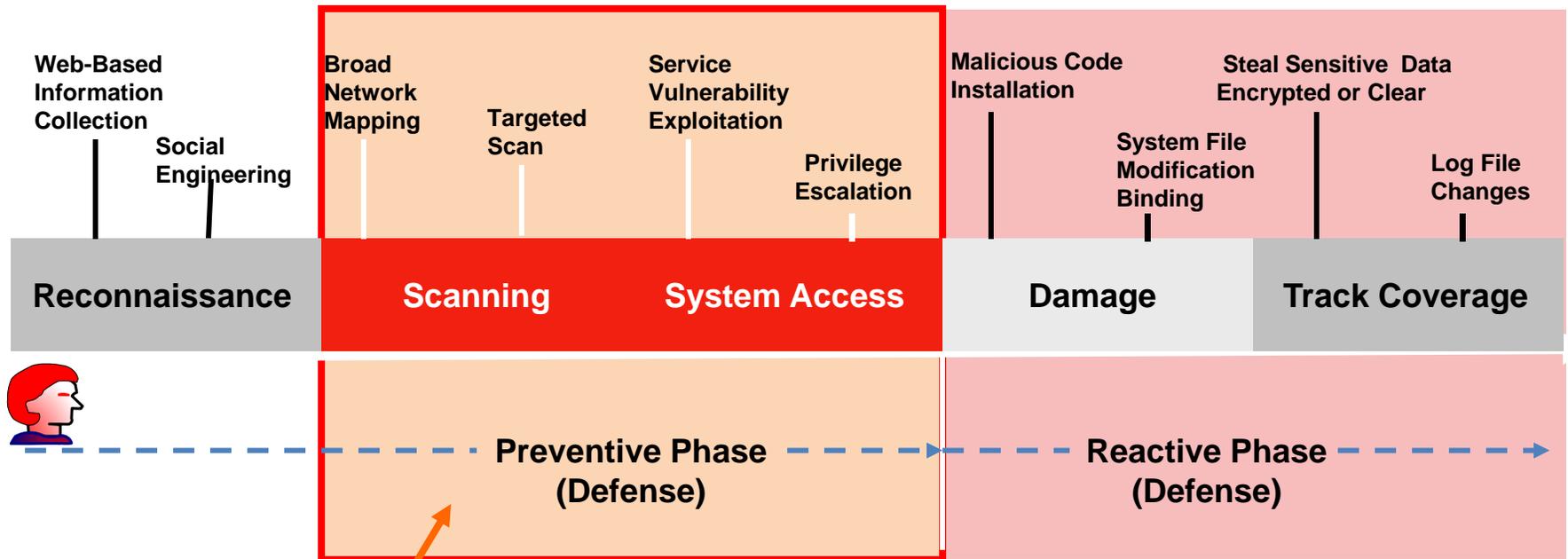


**2- Propagation
Mechanism**



3- Payload

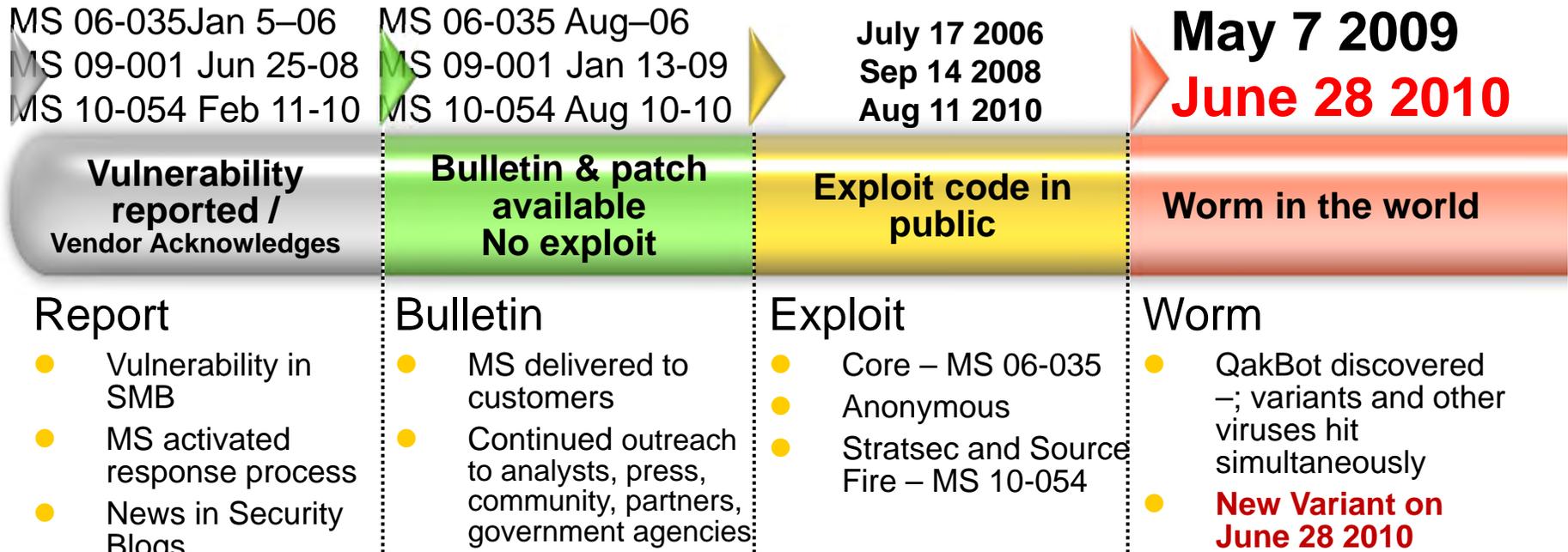
Common Hacker Attack Technique (CHAT)



Best Opportunities for Real Time Network Security And Stall the Attacker

Indications and Warning Threshold (Defense) - - - - - Incident Response

The Forensics of a QakBot/Variant



MS 06-035 Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution

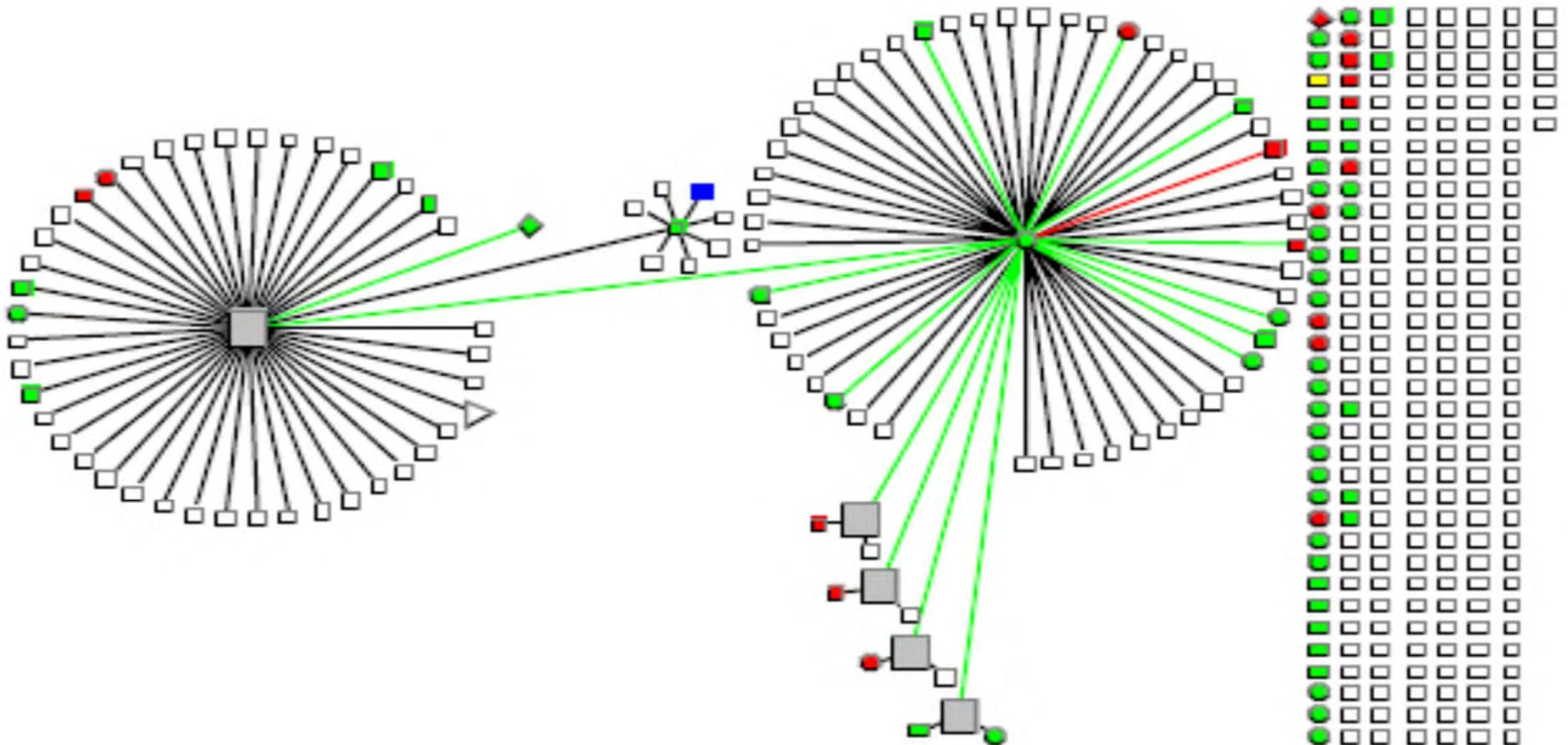
MS 09-001 Vulnerabilities in SMB Could Allow Remote Code Execution

MS 10-054 Vulnerabilities in SMB Server Could Allow Remote Code Execution

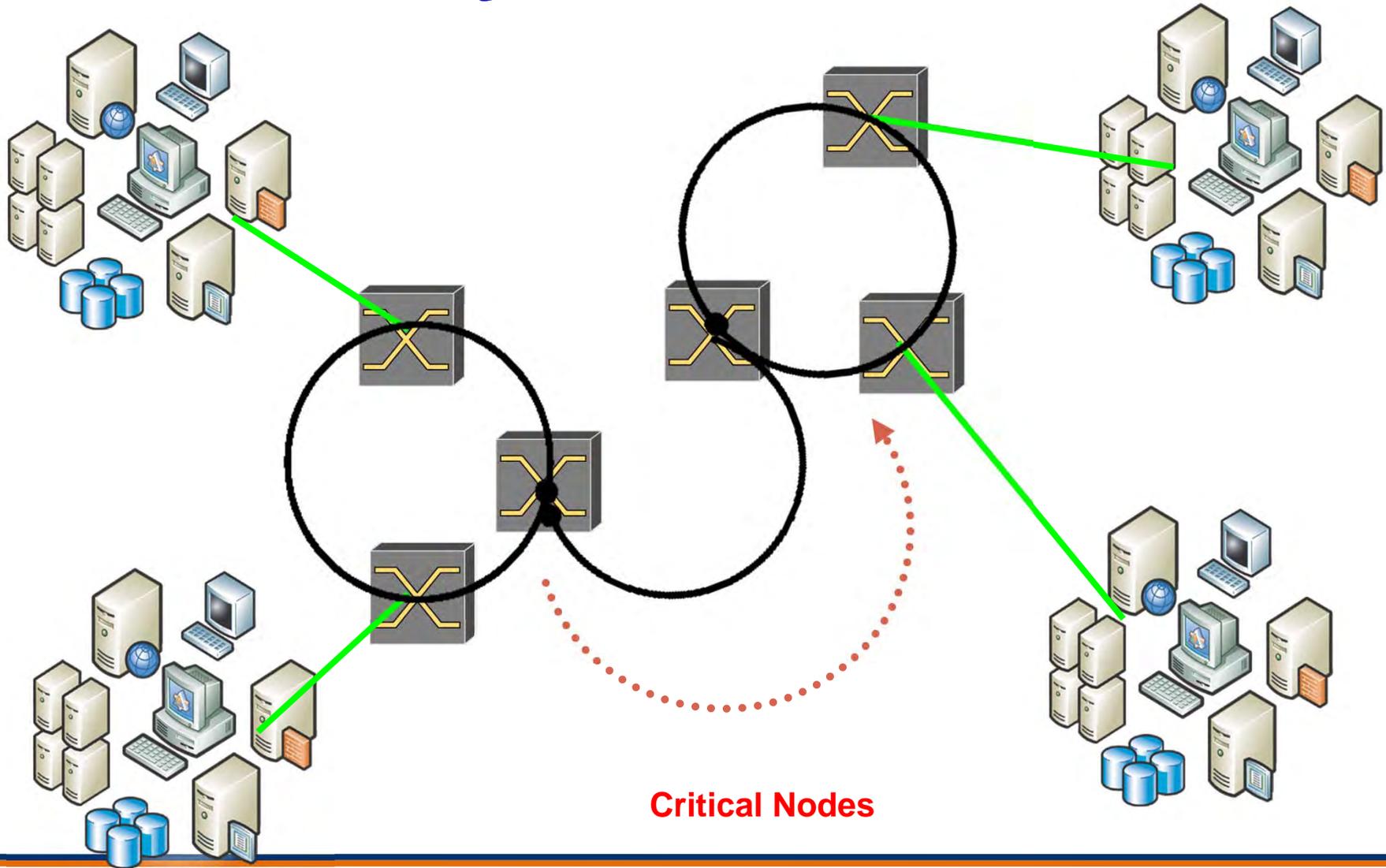
Backdoor:Win32/Qakbot.gen!arc (Trojan.Win32.Bzud.a (Kaspersky)) is a generic detection for an archive file that contains a copy of **Backdoor:Win32/Qakbot**



Do You Know Your Complete Network Topology ?



Identify Critical Nodes



Critical Nodes

Human Connectivity – Hard To Define Perimeters Complex ?

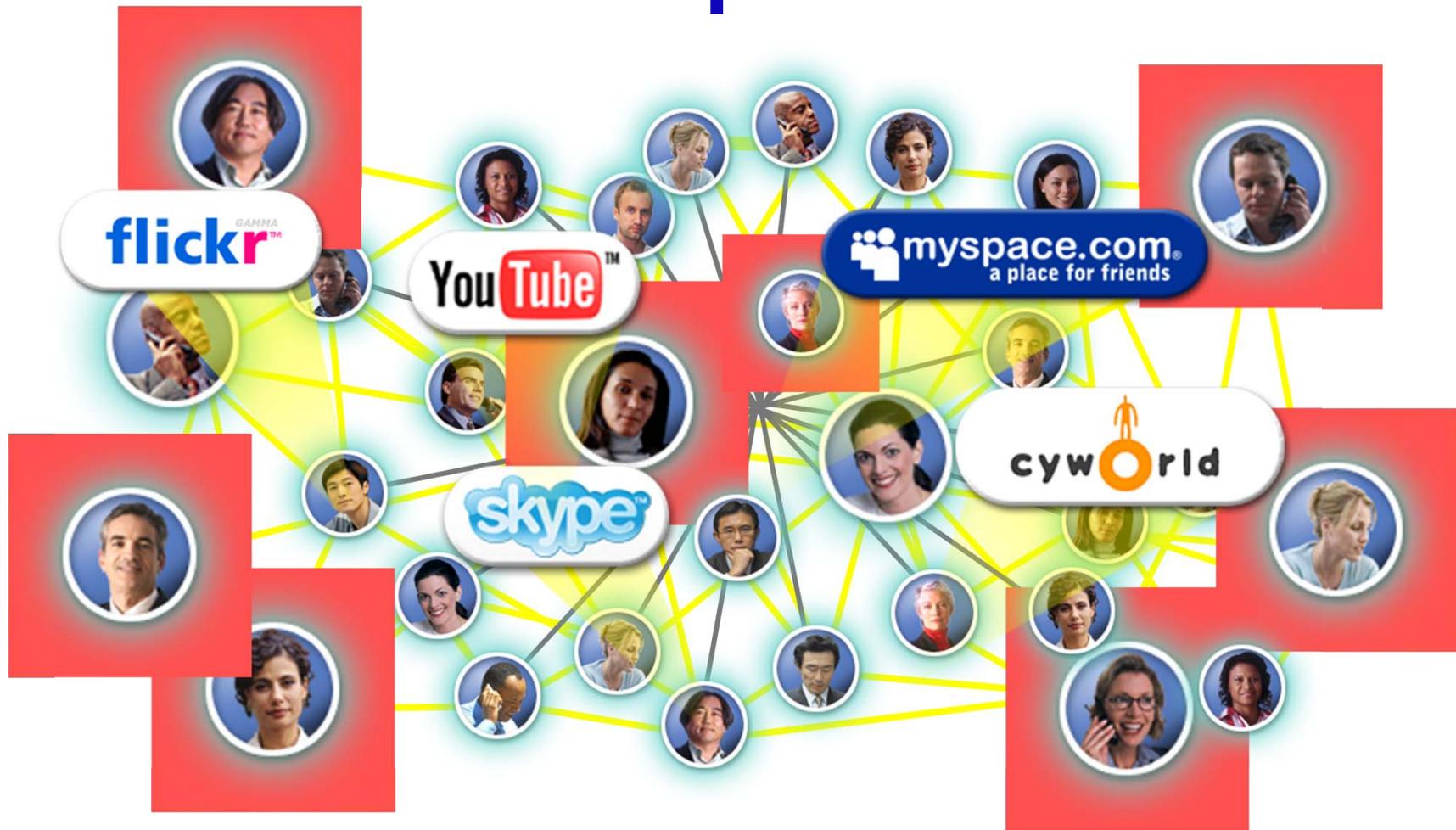


Image Source: CISCO

Performance of Antivirus Scanners

	N	M ¹	M ²	D	P	K	F	A	SAVE
Mydoom.A	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mydoom.A V1	✗	✓	✓	✗	✗	✓	✓	✗	✓
Bika	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bika V1	✗	✗	✗	✓	✗	✓	✓	✓	✓
Beagle.B	✓	✓	✓	✓	✓	✓	✓	✓	✓
Beagle.B V1	✓	✓	✓	✗	✗	✓	✓	✗	✓
Blaster	✓	✓	✓	✓	✓	✓	✓	✓	✓
Blaster V4	✗	✗	✗	✗	✗	✓	✓	✗	✓

N – Norton, M¹ – McAfee UNIX Scanner, M² – McAfee, D – Dr. Web, P – Panda, K – Kaspersky, F – F-Secure, A – Anti Ghostbusters, **SAVE** – Static Analyzer for Vicious Executable, **CAaNES/NMT Propriety Analysis Methodology.**

Published in Computer Journal of Virology and **ACASA in 2004!**

Similarity Analysis of Financial Malware

	Bugat.A.exe	Bugat.B.exe	Silentbanker.exe	SpyZeus.exe	Torpig.C.exe	Torpig.E.exe	Trojan.Spy.ZBot.FT.exe	Trojan.Spy.Zbot.HX.exe	Vundo.exe	VUNDO5.exe
Bugat.A.exe	100	69.34	82.66874281	68.0818	75.1207	79.2867	64.554347	78.793716	79.91435	79.91435
Bugat.B.exe	69.3398	100	60.66962719	44.286	72.6221	56.8586	72.484332	73.943752	76.20991	76.20991
Silentbanker.exe	82.6687	60.67	100	45.5969	61.7166	84.189	61.107125	46.395796	64.31942	64.31942
SpyZeus.exe	68.0818	44.286	45.59686811	100	70.7812	73.4072	66.732794	62.472766	85.14385	85.14385
Torpig.C.exe	75.1207	72.622	61.71664101	70.7812	100	76.5477	50.407706	52.802112	63.13616	63.13616
Torpig.E.exe	79.2867	56.859	84.18895526	73.4072	76.5477	100	18.931941	26.277059	62.99658	62.99658
Trojan.Spy.ZBot.FT.exe	64.5543	72.484	61.10712514	66.7328	50.4077	18.9319	100	60.194147	78.35206	78.35206
Trojan.Spy.Zbot.HX.exe	78.7937	73.944	46.39579613	62.4728	52.8021	26.2771	60.194147	100	59.75553	59.75553
Vundo.exe	79.9143	76.21	64.31941936	85.1438	63.1362	62.9966	78.352059	59.755528	100	100
VUNDO5.exe	79.9143	76.21	64.31941936	85.1438	63.1362	62.9966	78.352059	59.755528	100	100

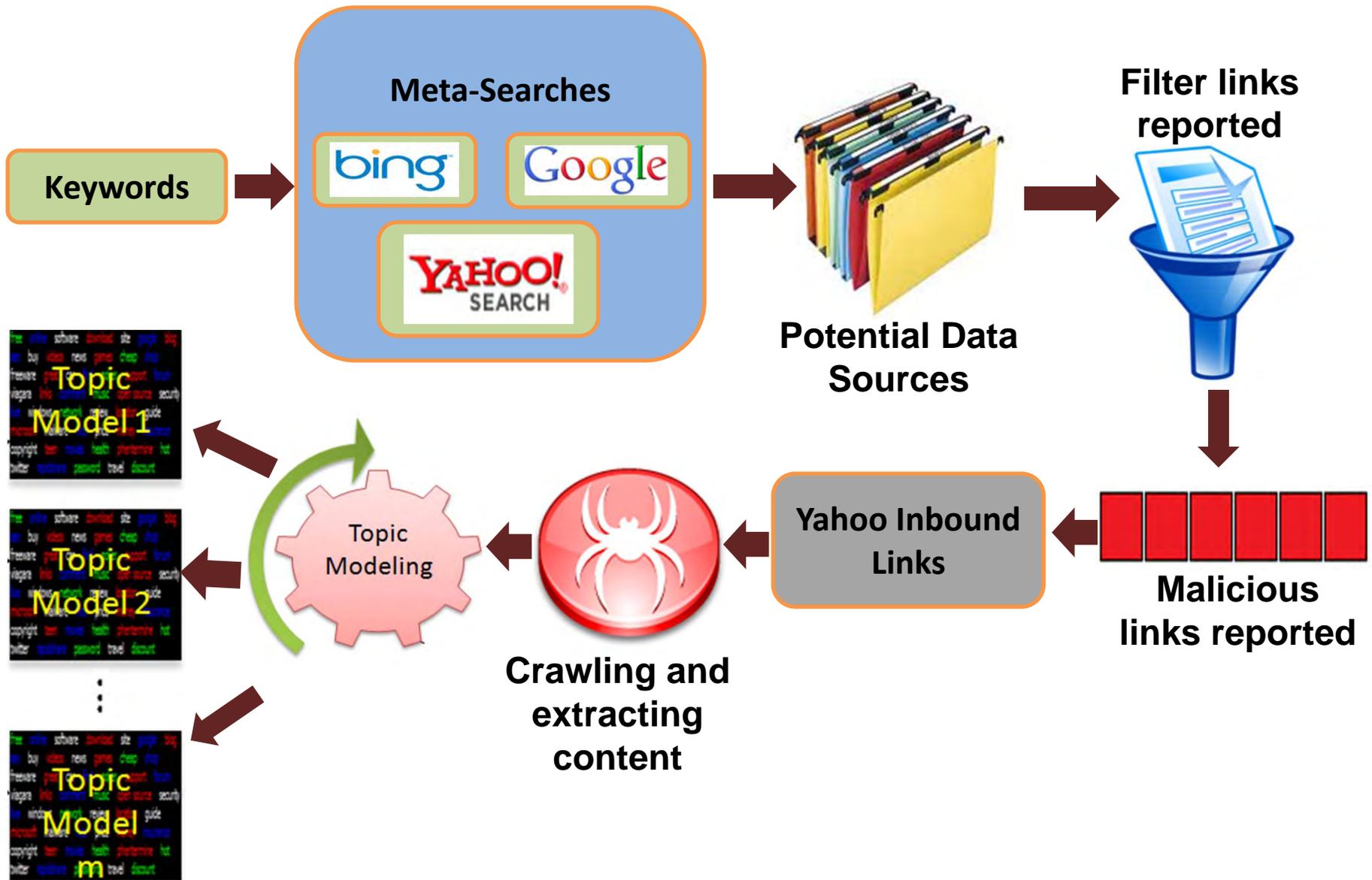
Presented at International Conference on Cyber Warfare 2011

Similarity of Crime Packs

	Cry	Eleonore	Fragus	Ice	IEKit	Impassion	MPack	MyPolySploit	Phoenix	x88	ZeroExploit
Cry	1	0.06308	0.739008	0.89965	0.905587	0.744702	0.995681	0.89964997	0.966491	0.683691	0.06163512
Eleonore	0.06308	1	0.298666	0.085231	0.071373	0.299771	0.028277	0.085230679	0.051724	0.123543	0.99745267
Fragus	0.739008	0.298666	1	0.665042	0.675199	0.991469	0.673784	0.66504176	0.71989	0.590564	0.33427078
Ice	0.89965	0.085231	0.665042	1	0.980034	0.710132	0.897692	1	0.941945	0.892742	0.07425452
IEKit	0.905587	0.071373	0.675199	0.980034	1	0.713353	0.902551	0.980033907	0.958627	0.881532	0.06589455
Impassioned	0.744702	0.299771	0.991469	0.710132	0.713353	1	0.682516	0.710132495	0.749393	0.66603	0.33139057
Mpack	0.995681	0.028277	0.673784	0.897692	0.902551	0.682516	1	0.897691934	0.963532	0.67298	0.02159523
MyPolySploit	0.89965	0.085231	0.665042	1	0.980034	0.710132	0.897692	1	0.941945	0.892742	0.07425452
Phoenix	0.966491	0.051724	0.71989	0.941945	0.958627	0.749393	0.963532	0.941944851	1	0.814384	0.04739393
x88	0.683691	0.123543	0.590564	0.892742	0.881532	0.66603	0.67298	0.892742407	0.814384	1	0.11586388
ZeroExploit	0.061635	0.997453	0.334271	0.074255	0.065895	0.331391	0.021595	0.074254515	0.047394	0.115864	1

Similarity Analysis of Popular Malware

	Win32.Bagle.c.mal	Bagle.O.mal	Mydoom.b.mal	Win32.NetSky.ad.mal	Win32.NetSky.aa.mal	Worm.Sasser.D.mal	Worm.Sasser.C.mal	Win32.Sircam.c.mal	Sircam.A.mal	Vundo.FCC.mal	Vundo-2075.mal
Win32.Bagle.c.mal	100	100	11.98579	11.01129	11.98579	88.3069	88.3069	88.3069	14.1887	14.1887	14.1887
Bagle.j.mal	90.69986	65.59547	61.35457	64.03873	64.03873	64.03873	64.03873	50.17392	50.17392	76.56955	80.24496
Bagle.al.mal	99.42608	36.59488	66.43398	57.88603	87.88603	37.88603	87.88603	25.3252	25.3252	55.35997	52.68773
Win32.Bagle.o.mal	97.48856	100	73.71068	97.73258	97.73258	97.73258	97.73258	48.85909	48.85909	82.69381	71.75364
Win32.Klez.h.mal	96.64575	11.98579	48.50764	88.3069	88.3069	88.3069	88.3069	14.1887	14.1887	62.47964	17.39779
Win32.NetSky.c.mal	98.14567	71.55218	67.70674	80.20834	80.20834	80.20834	80.20834	50.58495	50.58495	93.65291	74.65301
Blaster.dam.mal	97.48856	100	73.71068	97.73258	97.73258	97.73258	97.73258	48.85909	48.85909	82.69381	71.75364
MSWord.Blast.e.c.mal	98.14567	71.55218	67.70674	80.20834	80.20834	80.20834	80.20834	50.58495	50.58495	93.65291	74.65301
CodeRed.c.mal	66.14461	80.93707	57.67036	62.46689	57.67036	64.03873	64.03873	64.03873	40.96598	40.96598	40.96598
CodeRed.a.mal	98.14567	71.55218	67.70674	80.20834	80.20834	80.20834	80.20834	50.58495	50.58495	93.65291	74.65301
Worm.LoveLetter.DK.mal	66.14461	12.2884	48.85909	66.14461	65.40386	65.40386	11.70592	3.493751	12.2884	67.62279	81.14634
VBS.LoveLetter.D.mal	90.69986	65.59547	61.35457	64.03873	64.03873	64.03873	64.03873	50.17392	50.17392	76.56955	80.24496
Worm.Sasser.C.mal	97.48856	100	73.71068	97.73258	97.73258	97.73258	97.73258	48.85909	48.85909	82.69381	71.75364
Mydoom.b.mal	92.45689	21.85249	100	76.27815	76.27815	76.27815	76.27815	19.26173	19.26173	84.64828	57.33075
Win32.Sircam.c.mal	98.80203	70.05651	72.64135	88.91945	88.91945	88.91945	88.91945	100	100	66.91638	65.34238
Vundo.FCC.mal	99.03418	11.70592	30.69936	100	100	100	100	11.32529	11.32529	100	36.11959
Vundo-2075.mal	81.18607	33.90044	74.77176	79.91469	79.91469	79.91469	79.91469	26.36764	26.36764	76.20991	100
Vundo.ELC.mal	97.92501	58.23748	71.91817	81.19189	81.19189	81.19189	81.19189	40.21969	40.21969	79.91435	69.33983
Vundo-1991.mal	99.03418	11.70592	30.69936	100	100	100	100	11.32529	11.32529	100	36.11959
Vundo.FCC.mal	72.75943	39.51834	60.72317	54.45216	54.45216	54.45216	54.45216	33.51456	33.51456	70.22576	69.5021



Link Analysis

- Malware Link Visualization

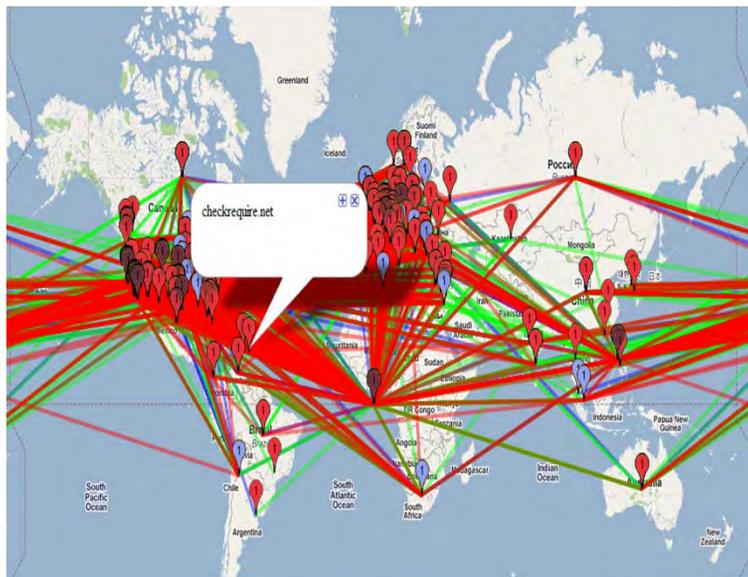


Figure : Visualization of malicious websites connected through the facilitating websites

castrohostingreview.com
loferemafia.blogspot.com
billard-sports.com
ownedbitch.com
fullpackportables.com
home-yard.com
free-daddytitlef.com
buy-figurative-painting-art-dealer.com
interior-designer.com
mindmagnetsoftware.com
highboobedtips.com
xobile.com
zoony.com
sydney.craigslst.com.au
infotrucks.com
thefreakscock.com
thatjstworks.com
shatt-al-arab.com
artec-2012.us
loopd.com
oracle.com
epage.com
wap.ethio.net
sex-in-bams.com
ariscool.com

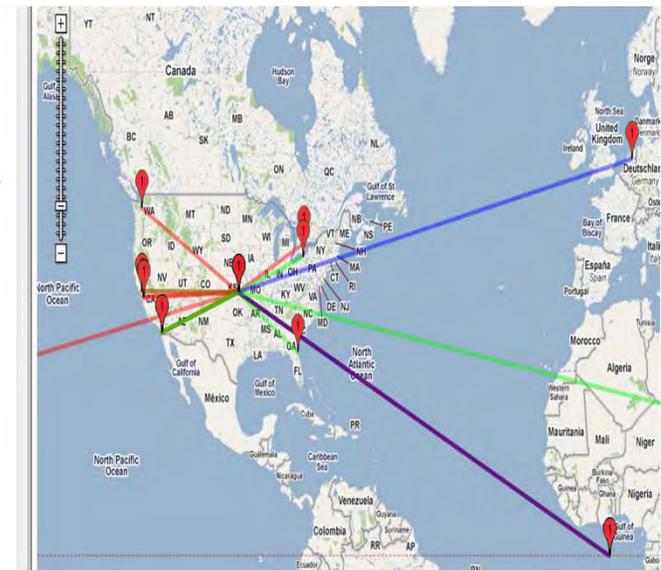
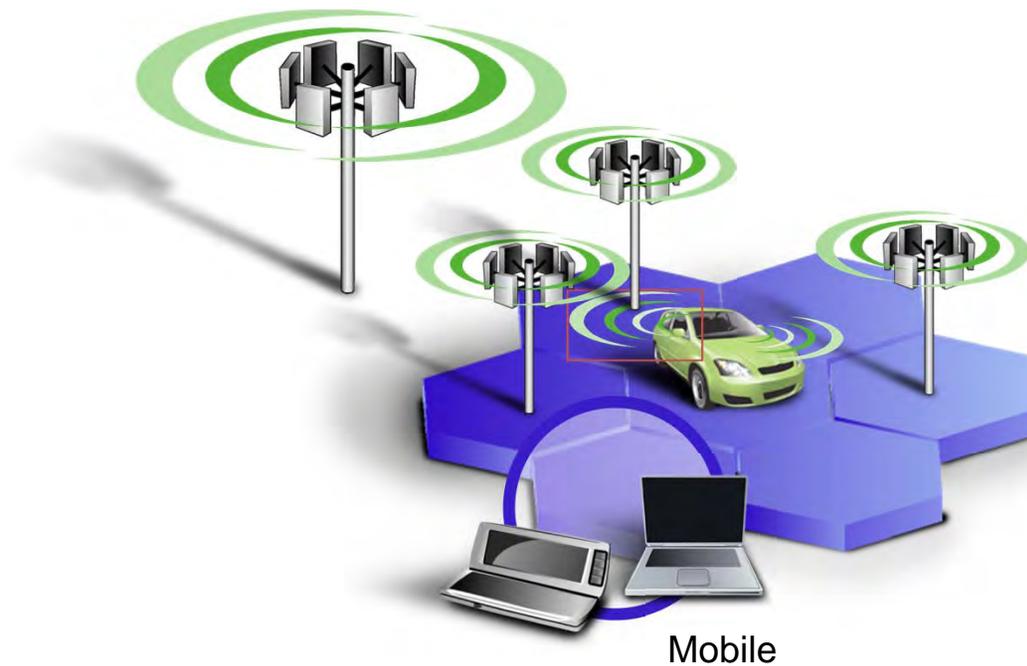


Figure : Shows customized link visualization where domains exist in the left pane

World Wide Web and Social Networking

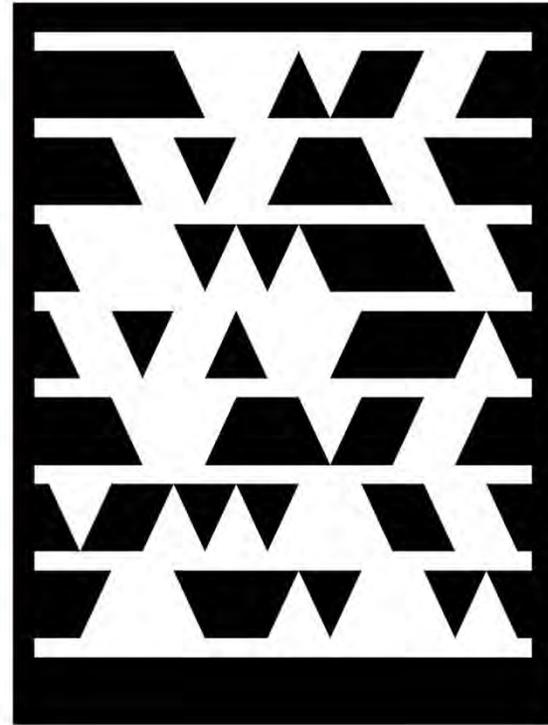
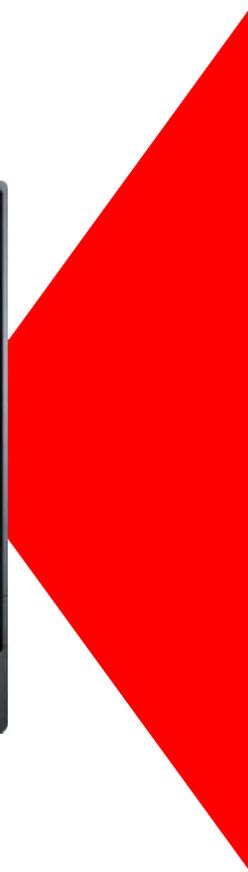


Non Traditional Computing Yet Information Centric!

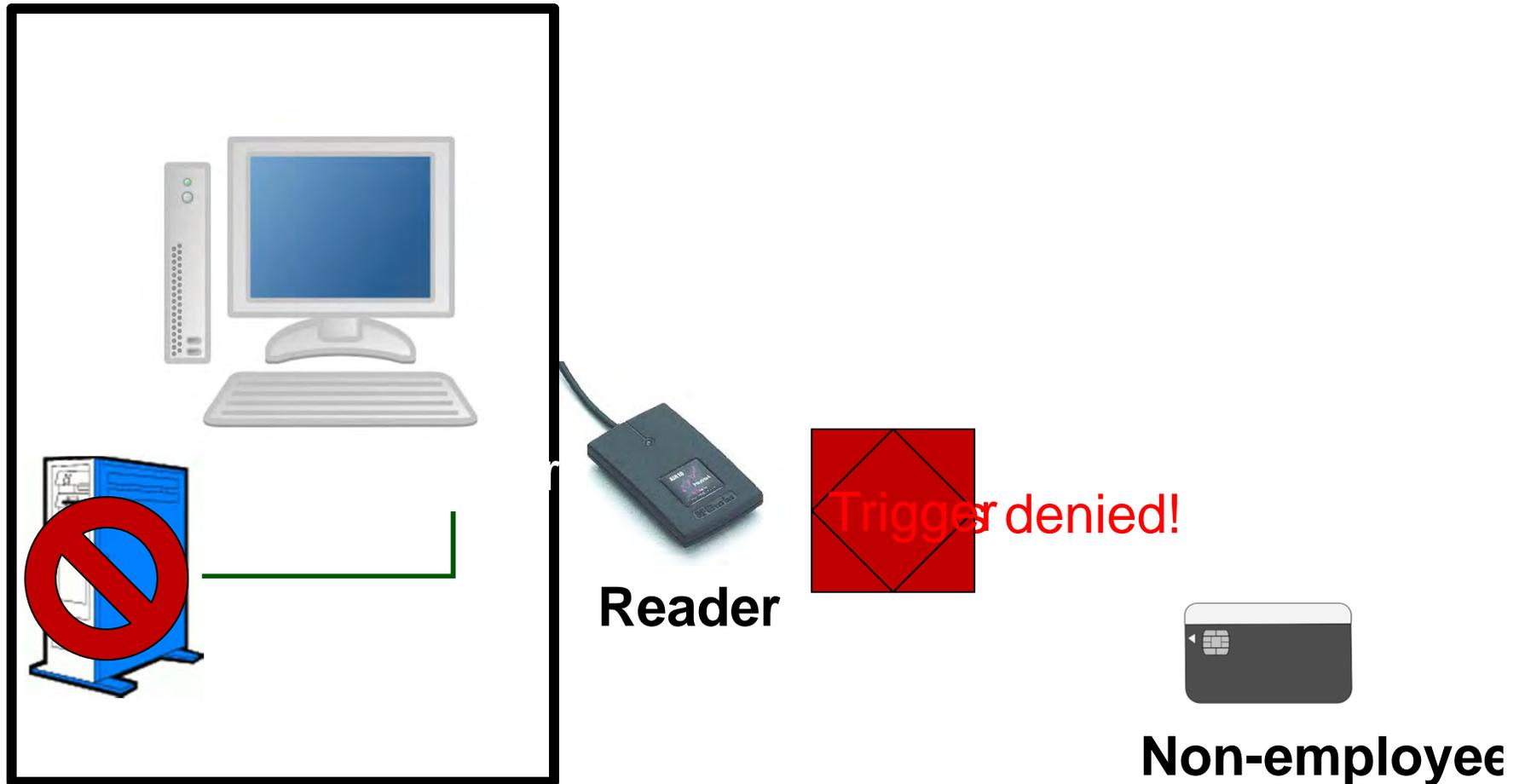


Is This Safe!

Scan the
Tag
to evaluate
this
session
now on



Fragmentation Attack



Presented at European Conference on Cyber Warfare
and
Publishes Computer Journal of Virology

RFID Attack – Can Human Health Be Impacted

Which means that those implants that are vital to a human's health and survival could, if corrupted, compromise the health--and potentially the survival--of the carrier.

"This means that, like mainstream computers, they can be infected by viruses, and the technology will need to keep pace with this so that implants, including medical devices, can be safely used in the future."



Presented at European Conference on Cyber Warfare and Invited to Computer Journal of Virology

Amazon EC2/S3

We are excited to hear about your interest in moving to EC2. We do not and will not provide a written agreement attesting compliance and assuming responsibility for cardholder data. Please see below for our general guidance on PCI compliance.

From a compliance and risk management perspective, we recommend customers not to store sensitive credit card payment information on EC2/S3 systems as they are not inherently PCI level 1 compliant. It is quite feasible one to run an entire application in AWS cloud while keeping the credit card data stored on within the local servers at the customer site, which are available for auditing, scanning, and on-site review at any time. As for PCI level 2 compliance, that requires external scanning via a 3rd party, PCI-approved vendor. It is possible for you to build a PCI level 2 compliant app in our AWS cloud using EC2 and S3.

<http://developer.amazonwebservices.com/connect/thread.jspa?threadID=34960>

We are not responsible for any unauthorized access to, alteration of, or the **deletion, destruction, damage, loss or failure to store any of, Your Content** (as defined in Section 10.2), your Applications, or other data which you submit or use in connection with your account or the Services

<http://aws.amazon.com/agreement/>

No Customer Audit Allowed

How do you respond to fears about the insider threat of data breaches affecting Google and therefore its customers?

Firstly, the data does not belong to us, it belongs to our customers. We'll only hold it as long as our customers request us to, and if they want to leave we'll give them the tools to take their data with them. All our employees go through security training and sign a code of conduct, and internally we practice least privileged access and role-based security, only giving access to those who need it and only giving them the least amount of access they need to get the job done. We're saying put all your eggs in one basket and then guard that really well. **We don't allow outside auditors** from our customers to come in, but that's the point of our own SaS 70 accreditation.

“We're saying put all your eggs in one basket and then guard that really well”

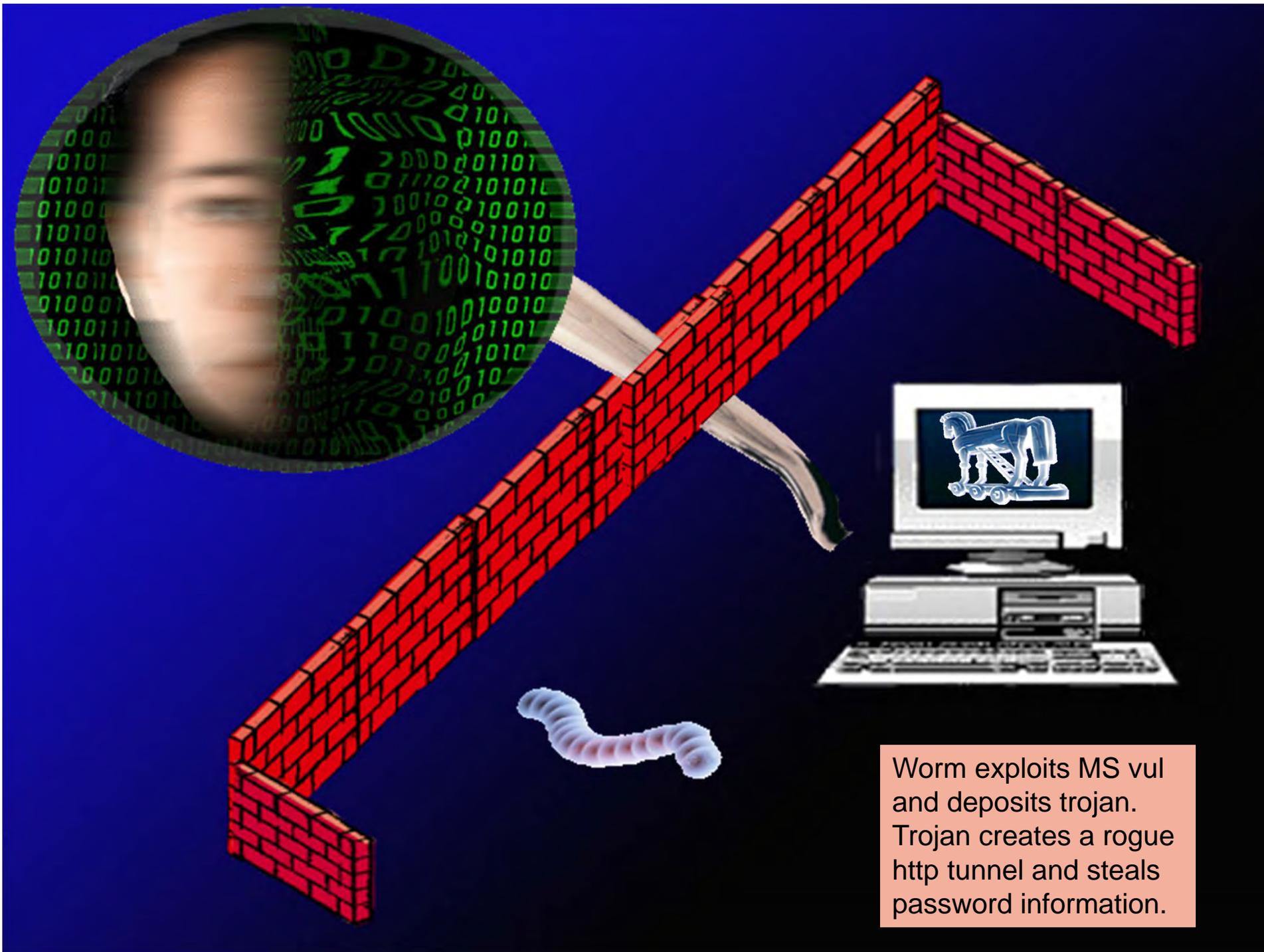
Eran Feigenbaum Google Apps director of security

...It is possible for you to build a PCI level 2 compliant app in our AWS cloud using EC2 and S3, but **you cannot achieve level 1 compliance**. And you have to provide the appropriate encryption mechanisms and key management processes. If you have a data breach, you automatically need to become level 1 compliant which requires **on-site auditing; that is something we cannot extend to our customers**. ... I recommend businesses always plan for level 1 compliance. So, from a compliance and risk management perspective, we recommend that you do not store sensitive credit card payment information in our EC2/S3 system because it is not inherently PCI level 1 compliant. It is quite feasible for you to run your entire app in our cloud but keep the credit card data stored on your own local servers which are available for auditing, scanning, and on-site review at any time.

Cloud Extensively Used for Attacks

For three pennies an hour, hackers can rent Amazon's servers to wage cyber attacks such as the one that crippled [Sony Corp. \(6758\)](#)'s PlayStation Network and led to the second-largest online data breach in U.S. history.

Security experts have identified Zeus botnet executing an illegal command and control channel on cloud computing infrastructure EC2 of Amazon, an application that permits users to hire computers so as to run their computer applications on that system.



Worm exploits MS vul and deposits trojan. Trojan creates a rogue http tunnel and steals password information.



Can We Predict The Next Vulnerability

and how will it impact your business

Conclusion

1

Who Are We
What do We Do?

2

Emerging and
Persistent Threats?

3

Why ICASA
Questions?