SAMPLE PRESENTATION FOR INSTITUTION EMPLOYEES

Corporate Account Takeover & Information Security Awareness

Floate(excepting dentry-of inde)-scrept statid struct encypting number of provident of the station of the encypting number of provident of the station of the encypting number of the

In the second of the second of the second information from the beater region of the file of the



ney the average key there a new and the second at the second of the second of the second of the second of the s the okey there (Ptha annex) - key the obey the autexployed annex unionk day the large autex Likely[ecryptic verbourty > 0]) (0 ecryptic prints(EEEE_DEEU0, "Yes size [sd]: begin", 0 crypt stat->key size(s) ecryptic durp 1 c_stat)0(0 (softest) = (crypt state-sum hander bytes at front) = (crypt state-sextent size (state-skey state)(0)(0)/sd) = erryptic C for estent (0;;lex); "0 "re [sd]n", (estent bare = estent offest)(0 co)d) gots out:0 [0 if (unitbely[ecryptic verbority s int 8 bytes after "0 "encryptions(n");0 acryptic dump hex[[ohin])[page address(and excent page)), 8);0 (Dout:0 record recor

The information contained in this session may contain privileged and confidential information. This presentation is for information purposes only. Before acting on any ideas presented in this session; security, legal, technical, and reputational risks should be independently evaluated considering the unique factual circumstances surrounding each institution. No computer system can provide absolute security under all conditions. Any views or opinions presented do not necessarily state or reflect those of **"Your Institution Name"** or any other entity.

Let dentry "ectyptic dentry,d and whit, fine t wirt feeld() not cell at a supplicative force borry the dentry-of mode, or brase necessary to do the encryption of " retrieved wie a prompt. Exactly what happens at this point should be pointy-dependent a write headers wirt(wirt, wirt ien, antre, crypt stet) is compting dentry) di it (inititely(to)) (0 point) SERN ESS var incordent a write headers wirt(wirt, wirt ien, antre, crypt stet) is compting dentry) di it (inititely(to)) (0 point) SERN ESS var incordent a write headers wirt(wirt, wirt ien, antre, crypt stet) is compting dentry) di it (inititely(to)) (0 point) SERN ESS var incordent a write headers wirt(wirt, wirt ien, antre, crypt stet) is compting dentry) di it (inititely(to)) (0 point) SERN ESS var incordent a write headers wirt(wirt, wirt ien, antre, crypt stet) is compting dentry) di it (inititely(to)) (0 point) SERN ESS var incordent a write headers wirt(wirt, different by test) is compting dentry) di it (inititely to)) (0 point) (SERN ESS var incordent of a stryptic dentry) = Worldate header ince: Whether to validate the header size while realing() to provide header date. The maintee of the stryptic to validate the header size while realing() to provide header date. The maintee of the strypt is an interference of the header size while realing() to private (ectyptics inde) of the struct inde) () a component of the struct dentry "lower dentry difference inden to private (ectyptics inde) of over 1



panney is at the of printing and the second standard the print (standard the second of the second standard). Incy that = the key these scatters will 10 10 if they the 10 (%ey_the) = Willin scatters (still00/* the>key these (fttle auter) = key the>key the untexyllouted auter unionk(skey the last survey

What will be covered?

- What is Corporate Account Takeover?
- How does it work?
- Types of Security Threats and Countermeasures
- Current Trends
- How to Protect?
- Bow to Detect?
- What to do when Fraud happens to me??

What is Corporate Account Takeover?

A fast growing electronic crime where thieves typically use some form of malware to obtain login credentials to Corporate Online Banking accounts and fraudulently transfer funds from the account(s).

Cyber threats to financial institutions and other national critical infrastructure is real and growing at an alarming rate.

Estimated 40,000 Chinese hacking groups

Average age ~ 2X years

Income: \$2-3 Million per year

The thread anis(virt) 50 crypt than 'num breader bytes at front "d" ((mine t)min hasher extents at front) [dire t) braann extent he stryptic dentry(" Busidets header mine Whether to validate the header mine while realing("D" Acad/parts the header sate. The h authouting trik virkstow; (D' argutt printle FIRM WARNER, 'File variant is fulls only "D" file variant (a) is supported by this "D a(this 'page virt, struct inde 'corputs inderFIRM WARNER, 'File variant is fulls only "D" file variant (a) is supported by this "D a(this 'page virt, struct inde 'corputs inderFIRM WARNER, 'File variant is fulls only "D" file variant (a) is supported by this "D a(this 'page virt, struct inde 'corputs inderFIRM berg, et coulds' retrieve the header information from the header region of the file,"D at the extended and the information of the file,"D' (over divisite on alcounced without the header region of the file,"D' to method and y in the extended attribute "D' (mine FIRM FER' "has Doable to alcounced without 'D' (action report apport of a starto method and only in the extended attribute "D' (mine 'Anther') is a submething of the file,"D' (action report and attribut 'D' (action and the constant) and the transmitting by the information of the file,"D' no started attribute (a the 'D' (action attribut 'D' (action and attribut 'D' (action at

How does it work?

- Criminals target victims by scams
- Victim unknowingly installs software by clicking on a link or visiting an infected Internet site.
- Fraudsters begin monitoring the accounts
- Victim logs on to their Online Banking
- Fraudsters Collect Login Credentials
- Fraudsters wait for the right time and then depending on your controls – they login after hours or if you are utilizing a token they wait until you enter your code and then they hijack the session and send you a message that Online Banking is temporarily unavailable.

Types of Security Threats

<u>&</u>

Countermeasures

nter to in a page to depin writing the matter cole Str. map elam (D char claims strike) (S (ap(clphet_issue, "AeS") == 0) (D suitch lack and balidate hander region(char "data D 6(cld header extents ar front, virt)of ("ord Data Extent G:D = Lower data (CBC encry) truct depiny "ecryptic dentry,D char "

ptic write headers virt(virt, virt im, saits = get unmingted head (virt)/d crypt that with The stryptic dentryd = heading header nice s purfurted prix VERSION) (d antiputs print) (fun (that "page virt, struct incle "corryptic p on entry point for reading file metalics. For e_1, GFP (DER) if if ('page virt) (d cc = -DEC) with metalers only in the evented attribute



Malware

- Short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent.
- Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, crimeware, most rootkits, and other malicious and unwanted software.

Viruses

- A computer program that can copy itself and infect a computer.
- The term "virus" is also commonly, but incorrectly used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability.
- Some viruses try to avoid detection by killing the tasks associated with antivirus software before it can detect them.

Spyware

- Type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge.
- The presence of spyware is typically hidden from the user, and can be difficult to detect.
- It can install additional software, redirecting Web browser, change computer settings, different home pages, and/or loss of Internet.

Full Protection Activate Registration Registration		uite to get full pr	otection against potentially unwa	anted software,	cenalitier a hist) (0 ecryptic h) (0)(D)/+70 cryptic (0)
Sample Scan results 19 po	tential threats f	ound.	JIMIEUTEN:		atali crypej te tovat pa
Advice: Please register to clean up p	ootentially harmful i	tems.		Register NOW!	ge address (ged 11 br
Name	Alert level	Action	Status		DATES AND
Virus.BAT.IBBM.ClsV	Critical	Remove	Not cleaned	^	are by sie
3 Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned		ellestracype
Trojan-IM.Win32.Faker.a	Low	Remove	Not cleaned		The THE PERSON
Trojan-Spy.HTML.Bankfraud.ra	Critical	Fix	Potentially Infected		- Gall olge
Trojan-PSW.VBS.Half	Critical	Remove	Not cleaned		
Virus.Win32.Faker.a	Critical	Remove	Not cleaned	~	primer (1920M
Threat name:	Virus, Win32, Fake	er.a			HUB-BEELOOK
Possible risk level:		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			SHIEL [3=]: ENGORT FIG
T COSIGIO TORIO TORI					tatle vola
File at risk of infection:	C:\Documents ar	d Settings\Bleeping	\Recent\snl2w.exe		mentil henes
Description:	These programs password. The p to the virus write	rogram terminates o	er passwords using a fake dialogue box onnection and advises re-connecting,	for entering MSN and info entered is sent	t rent 40 e) Cadhe Terry D 7 Retuine
					denury->d_d

Phishing

0		y fraudulent process of ng to acquire sensitive	
	•		
	informat	on (usernames, passwords,	
	credit ca	d details) by masquerading as	; a
	trustwor	Advanced card verification	
	commur	VISA Advanced verification.	
0	Commor	For security reasons please provide information requested below	
	Social	Card Number Expiration	
	🧧 Auctio	Date /	
	🤨 Online	Process	
	🧵 IT adm		



Subject:	Capital One Bank: urgent security notification [message id: 8892754772]	
-	Capital One	
	This email is fraudulent. URGENT messages with LOG IN links which hide the	
Capit	tal One web address should be considered fraudulent. Form are ready	0100
We would be criticated be criticated be criticated be criticated by the contract of the criticated be criticated by the criticated be criticated by the crit	a new version of LowerNET Form. This form is required to are a former customer of the North Fork bank, using Treasury ase use the same button to login and choose Treasury Optimizer are a former to access the Form. w in order to access the Form.	
Please	add our address book add our address—shown in the "From" line above—to your electronic address book to make sure that nt account messages don't get blocked by a SPAM filter.	
Importa	nt Information from Capital One	01 0 *0 21_12 67_0
40%55.T	ail was sent to john@acme.com and contains information directly related to your account with us, other services to	





rom: o: c:	service@paypal.com Sent: Wed 8/6/2008 12:22 AN John Doe	
ubject:	Update your credit card information with PayPal	
	PayPal	- introt Sittot (D) =
	Dear John Doe,	
	Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps:	12 44 12 56 12 56
	 Log in to your PayPal account. Go to the Profile subtab and click Credit Cards in the Financial Information column. Choose the credit card that needs updating and click Edit. Enter the updat https://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup 	chinidh hA, mpi tes, Thi HAP25 F(662 HYP25
	Or simply get the PayPa ^{Click} to follow link approved almost instantly, and there's no annual fee. Apply today.	nn se 1_mon y-dep Arror reinr_1
	PayPal	- 2413 19 301 16 1-9 10 10 1-2 1
	Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click the Help link in the top right corner of any PayPal page.	L go to emphile - ear Cilenei F Beau
	To receive email notifications in plain text instead of HTML, update your preferences.	(pinth) W

the dependence of the second with the second with the second of the second second with the second se

Subject: Update your credit card information with PayPal PayPal Dear John Doe, Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps: 1. Log in to your PayPal account. 2. Go to the Profile subtab and click Credit Cards in the Financial Information column. 3. Choose the credit card that needs updating and click Edit. 4. Enter the upda(https://www.paypal.com/us/cgi-bin/webs/cfrade_bc-signup) Or simply get the PayPa Webs/cfrade_bc-signup Or simply get the PayPa Vision Please do not reply to this error assistance, loa in to your Pay age. To receive email notifications	From: To: Cc	service@paypal.com John Doe	Se	nt: Wed 8/6/2008 12:22 AM
Dear John Doe, Surge credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, lease update your credit card expiration date by following these steps: 1. Log in to your PayPal account. 2. Log in to your PayPal account. 3. Go to the Profile subtab and click Credit Cards in the Financial Information column. 3. Choose the credit card that needs updating and click Edit. 4. Enter the upda https://www.paypal.com/us/cgi-bin/webscr?cmd=bc-signup 9. Sincerely, PayPal Sincerely, PayPal Please do not reply to this endit is authentic. 1. Lis addressed to you personally. This email is authentic. 1. Lis addressed to you personally. The sender appears to know the last 4 digits of your account number. The links are obscured but hovering on the	Subject:	Update your credit card informa	tion with PayPal	
Your credit card ending in 9595 will expire soon. To avoid any disruption to your PayPal service, please update your credit card expiration date by following these steps: 1. Log in to your PayPal account. 2. Go to the Profile subtab and click Credit Cards in the Financial Information column. 3. Choose the credit card that needs updating and click Edit. 4. Enter the updathtps://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup Or simply get the PayPa Or simply get the PayPa Sincerely, PayPal Please do not reply to this errage. Please do not reply to this errage. This email is authentic. It is addressed to you personally. The sender appears to know the last 4 digits of your account number. The links are obscured but hovering on the		PayPal		
please update your credit card expiration date by following these steps: Log in to your PayPal account. Go to the Profile subtab and click Credit Cards in the Financial Information column. Choose the credit card that needs updating and click Edit. Enter the updathttps://www.paypal.com/us/cgi-bin/ webscr?cmd=_bc-signup Or simply get the PayPa Or simply get the PayPa Click to follow link approved almost instantly, and there's no annual fee. Apply today. Sincerely, PayPa This email is authentic. It is addressed to you personally. The sender appears to know the last 4 digits of your Pay Page. The links are obscured but hovering on the 		Dear John Doe,		
 2. Go to the Profile subtab and click Credit Cards in the Financial Information column. 3. Choose the credit card that needs updating and click Edit. 4. Enter the updathttps://www.paypal.com/us/cgi-bin/webscr?cmd=_bc-signup Or simply get the Paypa Or simply get the Paypa Click to follow link approved almost instantly, and there's approved almost instantly, and there's Sincerely, PayPa Please do not reply to this err assistance, log in to your Paypage. This email is authentic. It is addressed to you personally. The sender appears to know the last 4 digits of your account number. The links are obscured but hovering on the 		Your credit card ending in 95 please update your credit ca	rd expiration date by following these steps:	al service,
Or simply get the PayPa Click to follow link no annual fee. Apply today. Sincerely, PayPal Please do not reply to this en assistance, loa in to your Pay page.		 Go to the Profile sub Choose the credit can Enter the updat https://websc 	tab and click Credit Cards in the Financial Information c rd that needs updating and click Edit. //www.paypal.com/us/cgi-bin/ r?cmd= bc-signup	olumn.
PayPal This email is authentic. It is addressed to you personally. The sender appears to know the last 4 digits of your account number. The links are obscured but hovering on the		Or simply get the PayPa ^{Click t} no annual fee. Apply today.	approved almost instantly, an	d there's
Please do not reply to this emails addressed to you personally. Please do not reply to this emails addressed to you personally. The sender appears to know the last 4 digits of your account number. page. The links are obscured but hovering on the				100 C
of your account number.			It is addressed to you personally.	
The links are obscured but hovering on the				e. For al
To receive email notifications link shows a valid PayPal address.			The links are obscured but hovering on the	
		To receive email notifications	link shows a valid PayPal address.	

righer vann) – h) (H in (ney mann) likey nami - tap key tradu rennañ bin 11 H in in (key tradu (jkey man) - Mulph se , robd goto outri (H)((jim) - key na Skey trad) fitz nurez) - key tra-Skey nam untexdiourtô murez uniork(stey r

rom: p: C:	United Parcel Service of America [onlineservices@lufthansa.com] Sent: Mon 6/1/2	009 5:00 AI
ubject:	Postal Tracking #UY6LG72236FH1Y7	
🔄 Message	e UPSNR_976120012.zip (37 KB)	
because Please	e not able to deliver postal package you sent on the 14th of March in time e the recipient's address is not correct. print out the invoice copy attached and collect the package at our office. nited Parcel Service of America	Ξ



E-mail Usage

- Some experts feel e-mail is the biggest security threat of all.
- The fastest, most-effective method of spreading malicious code to the largest number of users.
- Also a large source of wasted technology resources.
- Examples of corporate e-mail waste:
 - Electronic Greeting Cards
 - Chain Letters
 - Jokes and graphics
 - Spam and junk e-mail

Hoaxes

Hoaxes attempt to trick or defraud users.

- A hoax could be malicious, instructing users to delete a file necessary to the operating system by claiming it is a virus.
- It could also be a scam that convinces users to send money or personal information.
- Phishing attacks fall into this category.

Statistics

Where does it come from?

- Malicious websites (including Social Networking sites)
- 🤨 Email
- P2P Downloads (e.g. LimeWire)
- Ads from popular web sites

Web-borne infections:

According to researchers in the first quarter of 2011, 76% of web resources used to spread malicious programs were found in 5 countries worldwide ~ United States, Russian Federation, Netherlands, China, & Ukraine.

PROTECT

²Know your Customers - Develop a Risk Assessment:

Determine which customers are high-risk

Types of transactions – wires, institution to institution, SEC Code, daily files, high limits/frequencies, financial stability

Provide Ongoing Security Awareness Training for BOTH Employees & Corporate Customers

TRAIN! TRAIN! TRAIN!

- Make sure that your Customers are Aware of Basic Online Security Practices
- Review your Contracts

Make sure that you clearly state roles & responsibilities of both parties and dispute resolution processes

Stay Informed

- Attend webinars/seminars & other user group meetings
- Develop a layered security approach
- Perform a Due Diligence review of any third-party service providers for Online Banking Services

DETECT

Detection is closely associated with protection because some measures that protect also help identify fraud.

Layered Security

It has already been proven that a single layer is easy for hackers to get through. If one layer develops a security weakness then hopefully the other layers will provide sufficient protection.

Monitoring of IP Addresses

New User Controls

Calendar File – Frequencies and Limits

Dual Control

Fax or Out of Band Confirmation

Secure Brower or Secure Browser Key

Pattern Recognition Software

Train institution employees on Fraud warning signs

RESPOND

- Make sure your Incident Response Plan(IRP) includes procedures for a Corporate Account Takeover (Make sure that your IRP includes after-hours contact information for Corporate Customers)
- Make sure that "all" employees are trained, with specialized training for employees that process Wires or ACH Transactions.
- Update IRP to include the directory for FED ACH routing number contact information http://www.fededirectory.frb.org/search ACH.cfm
- Make sure you have a Notice of Fraudulent Activity in your IRP
- Procedures for processing a Fraudulent ACH file alert
- Establish procedures for customer relations and documentation of recovery efforts
- Develop a contingency plan to recover or suspend any systems suspected of being compromised
- Make sure your IRP has procedures and contact information for the US Secret Service as well as other law enforcement and regulatory agencies

RESPOND (Cont.)

- Contact customer to verify fraudulent transactions
- Reverse all suspected fraudulent transactions
- Send a "fraudulent ACH file or wire alert" through FedLine
- Distribute list of transactions to a group of employees with calling assignments and instructions to call on the largest items first
- Ask the institutions to place a hold on the funds send Notice of Fraudulent Activity letter

SAMPLE

Forwarded by /MPLS/FRS

From. Julin Doe/MPLS/FRS To: MPLS/FRS@FRS Date: 11/26/2010 05:35 PM Subject: Fw: Templates

A FRAUDULENT file was processed for (Bank Name & ABA) in error on (mm/dd/vy). The original file was processed on ______(mm/dd/yy) with settlement of ______(mm/dd/yy). The FRAUDULENT file was processed on (mm/dd/yy) and will settle on ______(mm/dd/yy). A reversal file was processed on (mm/dd/yy) and will settle on ______(mm/dd/yy). For additional information, contact _______(Bank Name) at (Bank's phone number).

(Bank Name & ABA) hereby assumes all responsibility and liability for any processing errors, losses, damages and hability in any way arising out of the transmission of the broadcast message _______(Bank Name and ABA) also agrees to indemnify and hold harmless the Federal Reserve Bank, its agents and employees, from and against all claims, damages, lawsuits, and expenses, including reasonable attorneys' fees, in any way arising out of the transmission of the broadcast message

>mapping=>host=0 crypt_stat =[a) all it (suppt_stat=>hesh_stat)0 c 0 matex_uniod(temport_crypt_stat 0 shir == remainder_ct_paped) =>key_state() 0 etrypt1s dum_le ent_ptat)(0)(D)=t1 = seript1s unitkely(ecrypt1s_defbortby > 8)(B_IDoutcD_reform_refb(DD)) (apping=>host=0 crypt_stat =[) c

What your Customers can do!

PROTECT

- Education is Key Train employees
- Install and Maintain Real Time Anti-virus/Anti-spyware/ Firewall software and keep it up to date
- Secure your computer and networks
- Limit Administrative Rights
 - Do not allow employees to install any software without receiving prior approval.
- Install and Maintain Spam Filters
- Surf the Internet carefully
- Install security updates to operating systems and all applications as they become available
- Block Pop-Ups
- Do not open attachments from e-mail
- Do not use public Internet access points
- Recommend dual control from separate devices

What your Customers can do!

DETECT

Education is Key – Train their employees

Reconcile Accounts Daily

Be on the alert for suspicious emails

Anti-virus/Anti-spyware/Firewall software and keep it up to date

Perform a full scan at least once a month

Note any changes in the performance of your computer

> Dramatic loss of speed, computer locks up, unexpected rebooting, unusual popups, etc.

What your Customers can do!

RESPOND

Education is Key – Train their employees

Make sure that their employees know how and to whom to report suspicious activity to at the Company & the Institution

Contact the institution:

>If they Suspect a Fraudulent Transaction

>If they are trying to process an Online Wire or ACH Batch & receive a maintenance page.

>If they receive an email claiming to be from the institution and it is requesting personal/company information.

Questions

or Comments