RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: STR-W11

Learnings from the Cloud: What to Watch When Watching for Breach

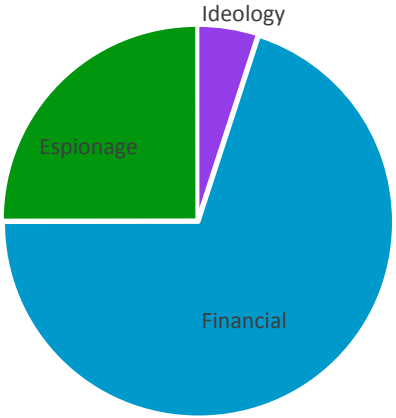
Sara Manning Dawson
Principle Group Program Manager, Office 365 Security
Microsoft Corporation

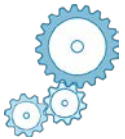
We will shed light on

- What are common attack patterns?
- How do I watch for them?
- How do I protect myself and my organization?

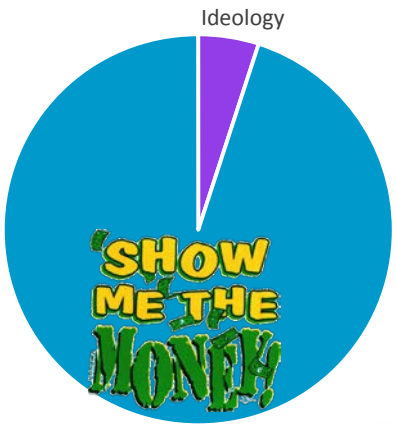
Risk

In Theory





In Cloud Practice

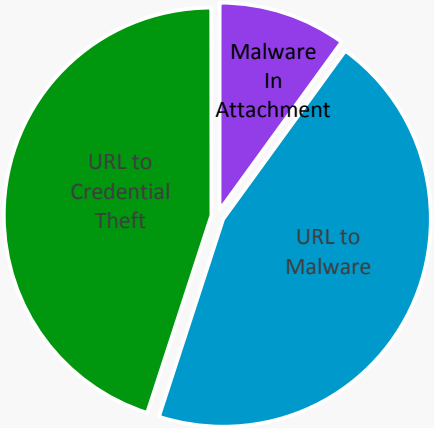


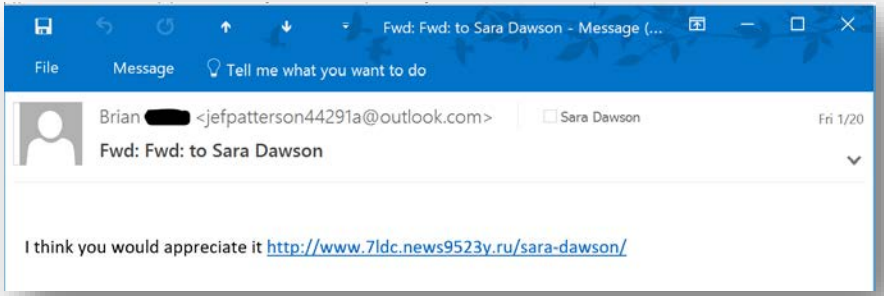
- Data Loss Prevention
- Compliance Audits
- Data Encryption
- Account Protection Controls
- External User Controls
- App, Mobile Connectivity

- Account Protection Controls

Foot In

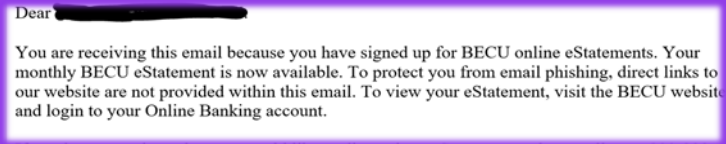
Phish→ Identity Theft→ Fraud





What To Do About It

Keep people safe


Dear [redacted]

You are receiving this email because you have signed up for BECU online eStatements. Your monthly BECU eStatement is now available. To protect you from email phishing, direct links to our website are not provided within this email. To view your eStatement, visit the BECU website and login to your Online Banking account.

Use Cloud Tooling

SPF, DMARC, DKIM, EXTERNAL

Account Access = Keys To The Kingdom

Permissions

Trust

Goodwill

What To Do About It

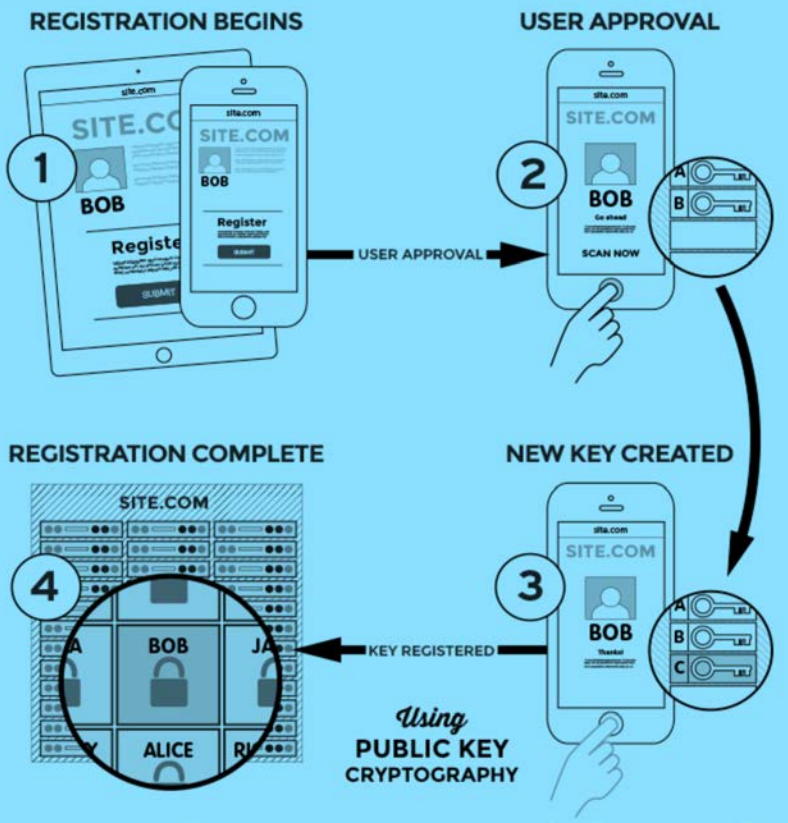
MFA

PKI, Hardware

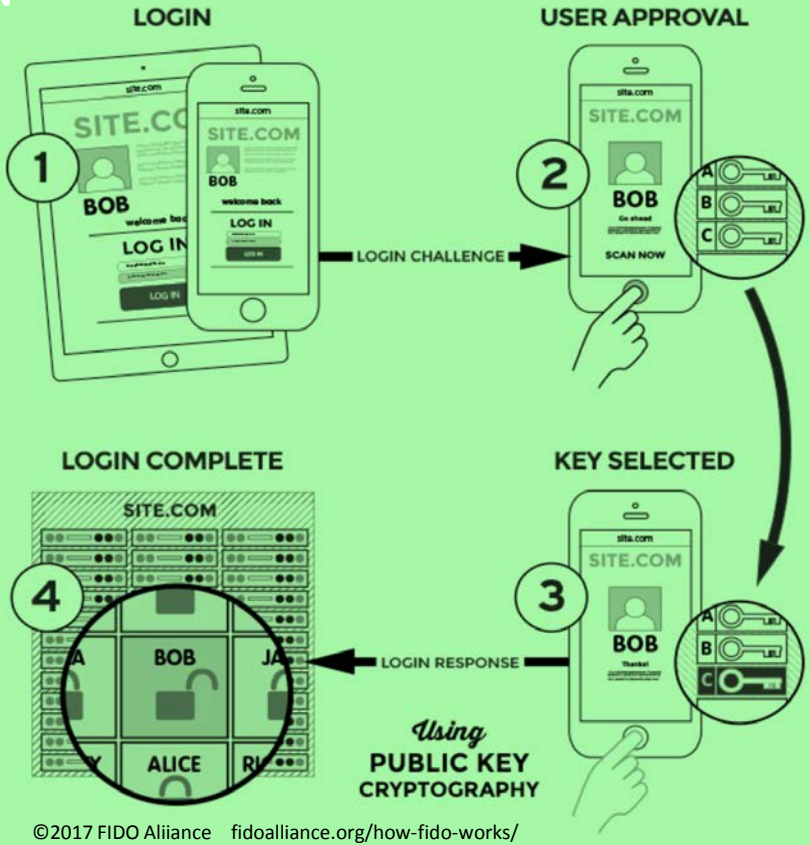
PKI, Biometrics

FIDO

REGISTRATION



LOGIN



Organization Attacks: Case Study #1

- Initial Breach
  - Phishing email from consumer email provider
  - “invoice.doc” embedded malware
- Method
  - Targeted initial breach, likely researched. Account creds dumped to C2.
  - Exec admin account used to send invoice.doc malware to rest of company, expanding account breach.
  - Spoofed email sent to CFO from CEO asking for bank transfer
  - Hmmm…Discovery point by CFO
- Impact
  - Nearly successful whaling attempt with potential **high five figure** loss.

Organization Attacks: Case Study #2

- Initial Breach
  - Cred harvesting (likely through spoofed login page)
- Method
  - Attacker created shadow admin account, used to create regular user account. Cleaned up.
  - Granted delegate perms to payables clerk account, created mail forwarding rules to external domain.
  - Gathered intelligence on accounting and downstream payments.
  - Spoofed downstream supplier from external domain, asked for bank routing update.
  - Six weeks of $30K+ weekly, before actual downstream supplier asked about missing payment.
- Impact
  - **Six figure** loss.
  - Customer reputation impact

Organization Attacks

Phishing is the “foot in” 90% of the time

Attackers take time to learn financial processes

FADS aren’t just a fad

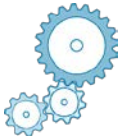
Forwarding
Admins
Delegates
Searches

What To Do About It

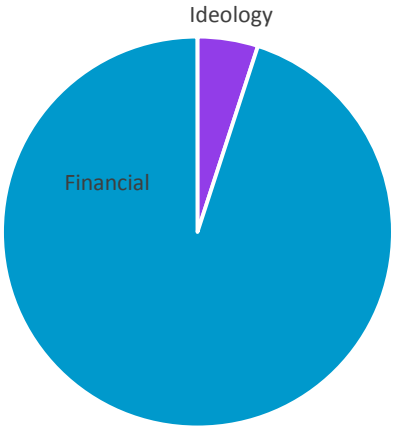
Audit FADS

Assessment and Monitoring

Malicious Insiders



In Practice



Analytic Indicator Category	Analytic Indicator	Attack Types: Accidental Leak	Espionage	Financial Fraud	Misuse	Opportunistic Data Theft	Physical Theft	Product Alteration	Sabotage	Violence
Content-Based Analytics										
Social	Disregard	2			1	1	1	2		1
	Personal Inflexibility	2	2	2	2	2		2	2	2
	Unusual Business Travel		1				2	1		2
	Unusual Personal Travel		1			2	2	1		2
	Unauthorized or Inappropriate Associations		1			2	2	1		2
	Withdrawal					2	1	2	2	1
	Workplace Events		2		2	2	1	2	2	1
	Workplace Satisfaction			2		2	1	1	1	1
Health	Mental Instability				2			2	1	1
	Impulse Control			1		1	1			
Human Resources	Major Life Event			1			1	1	1	1
	Complaints Against the User								2	2
	Negative Reviews		2	1	1	2	1	2	1	1
Inferential Analytics										
Financial	Observed Temporal Change in Means		1	1			1	1	1	2
	Observed Change in Means Relative to Peers		1	1			1	1	1	2
	Financial Reporting		1	1				1	1	2
Security	Change in Violation Patterns		2	2	2		1	2	1	2
	Duration and Regularity of Security Events	1		2	2		1	2	1	2
	Unauthorized or Inappropriate Use of Tools							2		
Criminal	Restraining Orders				2					1
	Wage Garnishments, etc.			1						
	Violence Outside Workplace				2				1	2
	Recent Increase in Criminal Events						1	2		

http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_451069.pdf

Mistaken Insiders

Sharing

Sending

Syncing

Saving

What To Do About It

Retention and Deletion

Device and App Management

DLP

Attacks on a Cloud Service

BIGGER SURFACE AREA but FEWER VECTORS

Lean and Automated = minimal human interaction

Control and Uniformity in code execution and communications stack

Difficult to target at scale: 100,000's of machines

In Theory

Espionage via Judicial Systems

In Practice

blogs.microsoft.com /on-the-issues

Key Takeaways

- It’s all about the money, honey
- Invest in account and identity protection
- Watch for FADS
- Mind your inner “Hmm…”

Stay Safe

- Account Breach
  - https://blogs.technet.microsoft.com/office365security/how-to-fix-a-compromised-hacked-microsoft-office-365-account/
  - https://blogs.office.com/2016/06/01/gain-enhanced-visibility-and-control-with-office-365-advanced-security-management/
  - https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection
- Phishing
  - https://products.office.com/en-us/exchange/online-email-threat-protection
- Protect Identity through FIDO
  - https://fidoalliance.org
- Asses and Protect yourself in Office 365
  - https://securescore.office.com/
  - https://products.office.com/en-us/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy
- Ransomware
  - https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
  - https://blogs.technet.microsoft.com/sposupport/2016/09/19/handling-ransomware-in-sharepoint-online/