



Evolving Cyber Attack Trends and Common Mistakes When Responding

Paige Boshell

***Partner,
Bradley***

Erik Rasmussen

***Associate Managing Director,
Kroll Cyber Security***

June 15, 2016

My Background

Paige Boshell



- Team Leader, Privacy & Information Security Team
- Partner, Birmingham Office
- www.babc.com/privacy-and-information-security-team-practices

My Background

Erik Rasmussen



- Associate Managing Director, Cyber Security and Investigations
- Former Director, Visa Inc.
- Former Secret Service agent, Cyber Intelligence Section
- Former Deputy Prosecuting Attorney
- CISSP, QSA certified

Bradley

Outline

Trends and Mistakes

Trends	Mistakes
File-less Malware	Not Taking Care of the Small Stuff
Business Email Compromises	Governance
Ransomware and Data Destruction	Lack of Escalation

File-less Malware: PowerShell

- Problem
 - Increasing use of malware that does not create or maintain a file to the hard drive.
 - This can create issues for AV that only searches files on disk.
 - May complicate forensic review of compromised machines.
 - Reduces the effectiveness of whitelisting.

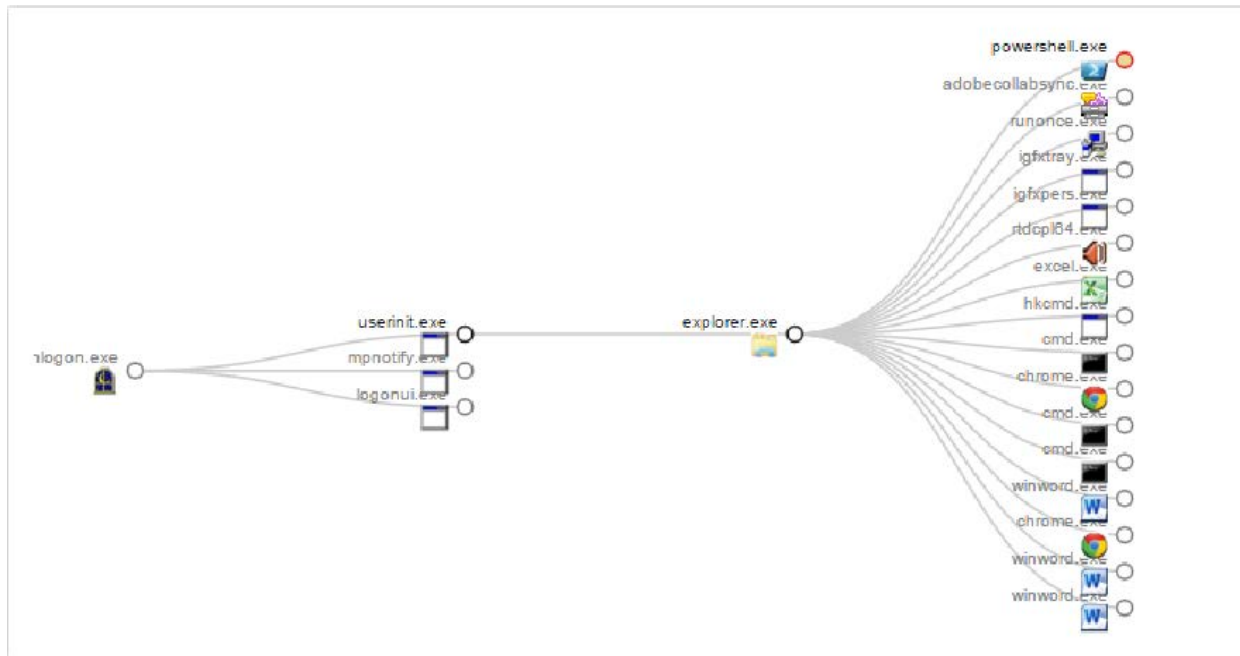
File-less Malware: PowerShell (cont'd)

- How We Have Seen The Attack
 - PowerShell pulling base64 encoded commands from registry
 - Poweliks interpreting obfuscated javascript
- Response
 - PowerShell leaves minimal useful artifacts as to what actually happened.
 - Memory capture and analysis
 - Real time endpoint monitoring
- Mitigating Controls
 - Mainly detection or disabling

PowerShell

- Command line shows that PowerShell is loading something encoded in Base64 from the registry key HKCU\Software\Classes\GJUgkdHgZJNnb\QAHYDAU

Command line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nopprofile -windowstyle hidden -executionpolicy bypass lex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((gp HKCU:\Software\Classes\GJUgkdHgZJNnb).QAHYDAU))); less



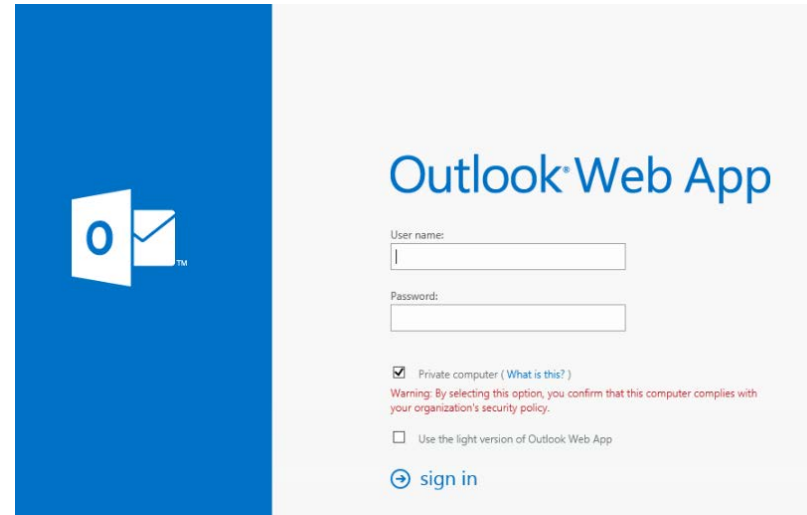
Business Email Compromise: 2 versions

Phishing attack collects email username and passwords

1) Targeted: Attacker compromises an email account and reads the contents waiting for a specific time to strike and send financial instructions

2) Shotgun: Spoof an executive's email and ask for wiring instructions

- Social engineering: Does not need to use malware
- Can occur over a prolonged period of time
- Sometimes caught by system errors or chance review of logins
- Lack of visibility once the device is outside the perimeter



Webmail

Email Address

Password

Log in


Bradley

Phishing Example

Phishing message detected by Gmail

Citibank secure account resolution



 **Be careful with this message.** Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information.



Citi Online to Recipients ↕

Apr 28 ⋮

Dear Customer,

We noticed some unusual activity in your Citibank account. To help protect you, we've temporarily blocked your account.

[Why are you seeing this?](#)

Due to possible errors, Your account violates our Terms of Service.

[How can you unblock your account?](#)

The fastest way to unblock your Citibank account is to [verify your account](#).

If you haven't setup a mobile phone in your account, please contact Customer Support.

Bradley

Business Email Compromise

Helpful controls and response procedures

1. SPF checking
2. Buy up lookalike domains
3. Adequate SPAM traps
4. Two factor authentication
5. Wire transfer authentication outside of email/out of band communication
6. Email access logging and monitoring
7. Bad email forwarding to help desk by users
8. OWA access logs with bad IP addresses
9. 1 IP address accessing multiple email boxes
10. Fake credentials

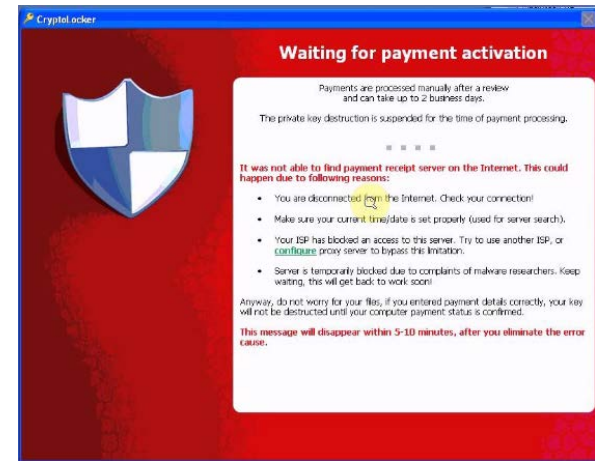
Ransomware

Multiple methods and uses for this malware

Malware that encrypts a victim's data and then demands ransom to unlock the data.

Variations on its use:

- Click and install
- Intrusion and install
- Cover your tracks install



Bradley

Common Corporate Mistakes When Responding to Incidents

Not Taking Care of the Small Stuff

LESSON: Many large breaches are the product of smaller unmitigated breaches.

- Lack of root cause analysis
- Lack of complete mitigation
- Block, wipe, repeat
- Metaphor: if you come home late at night and find the back door open in your house
 - The problem is not the door, that is the symptom.
 - The problem is that the attacker may still be in your house.
 - Closing the back door does not necessarily solve your problem until you can answer the question as to whether the house is safe.
- Most companies are just closing the door



Escalation and Employee Security Awareness

- Define how incidents should be reported and escalated.
- Case: Intrusion identified 2 months prior to significant destruction.



Governance

The person that planned, lobbied, and built the gate.....

Should not be the person who investigates when someone gets over the gate.



Bradley

 **Kroll.**

Paige Boshell

205-521-8639

pboshell@Bradley.com

Erik Rasmussen

571-926-4592

erik.rasmussen@kroll.com

Bradley