SCvirtualconference

The Pillars of APT Defense

March 23, 2017

M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
Department of Computing
School of Business & Management
College of Professional Schools
Norwich University

Topics

- What are APTs?
- Fundamental Difficulties for IA Statistics
- Examples of Publicized APTs
- Perimeter Defenses
- Human Defenses
- SIEM
- Incident Response
- Business Continuity

SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.

What are APTs?

- Advanced persistent threats
- Long-term undetected access to systems
- Usually associated with data leakage
  - Unauthorized access to confidential information
  - E.g., strategic planning, mission-critical data, competitive-positioning information
- May be used for sabotage
  - Unauthorized use of resources (e.g., botnet activity)
  - Data corruption
  - Data deletion
  - Denial of service

SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.

Fundamental Difficulties for IA Statistics

- Ascertainment
  - May not detect problem at all
  - May detect attack only after it's succeeded
- Documentation
  - Victims may maintain secrecy
  - Concerned about strategic consequences
    - Damage to reputation
    - Loss of credibility
    - Legal penalties
  - Laws changing
    - Some requirements for disclosure; e.g., compromised PII*

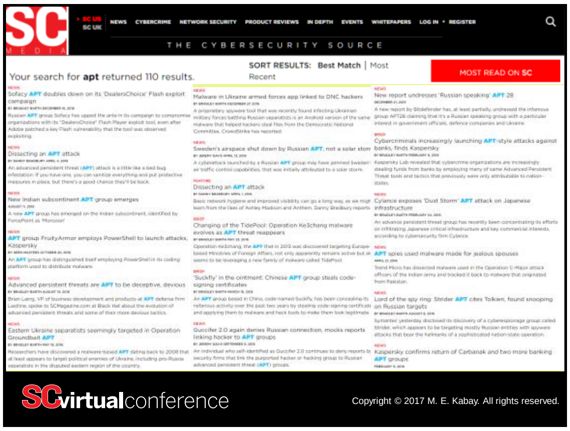
*PII = personally identifiable information

SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.

Examples of Publicized APTs

- Titan Rain (2003) – Chinese hackers vs US govt
- Sykipot (2006) – spear-phishing using malware
- GhostNet (2009) – Chinese INFOWAR for intel
- Stuxnet (2010) – US/Israeli attack on Iranian Siemens centrifuge controllers
- Deep Panda (2015) – China vs US Office of Personnel Management – 4M people's records
- Poison Ivy RAT (2016) – FBI reported ATP6 group infiltrated US govt systems since 2011

SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



Your search for **apt** returned 110 results.

NEWS
Sofacy APT doubles down on its 'DealersChoice' Flash exploit campaign
BY BRADLEY BARTH DECEMBER 16, 2016
Russian APT group Sofacy has upped the ante in its campaign to compromise organizations with its "DealersChoice" Flash Player exploit tool, even after Adobe patched a key Flash vulnerability that the tool was observed exploiting.

NEWS
Dissecting an APT attack
BY DANNY BRADBURY APRIL 4, 2016
An advanced persistent threat (APT) attack is a little like a bed bug infestation: if you have one, you can sanitize everything and put protective measures in place, but there's a good chance they'll be back.

NEWS
New Indian subcontinent APT group emerges
AUGUST 11, 2016
A new APT group has emerged on the Indian subcontinent, identified by ForcePoint as 'Monsoon'

NEWS
APT group FruityArmor employs PowerShell to launch attacks, Kaspersky
BY [illegible] OCTOBER 20, 2016
An APT group has distinguished itself employing PowerShell in its coding platform used to distribute malware.

NEWS
Advanced persistent threats are APT to be deceptive, devious
BY BRADLEY BARTH AUGUST 16, 2016
Brian Laing, VP of business development and products at APT defense firm Lastline, spoke to SCMagazine.com at Black Hat about the evolution of advanced persistent threats and some of their more devious tactics.

NEWS
Eastern Ukraine separatists seemingly targeted in Operation Groundbait APT
BY BRADLEY BARTH MAY 18, 2016
Researchers have discovered a malware-based APT dating back to 2008 that at least appears to target political enemies of Ukraine, including pro-Russia separatists in the disputed eastern region of the country.

NEWS
Malware in Ukraine armed forces app linked to DNC hackers
BY BRADLEY BARTH DECEMBER 27, 2016
A proprietary spyware tool that was recently found infecting Ukrainian military forces battling Russian separatists is an Android version of the same malware that helped hackers steal files from the Democratic National Committee, CrowdStrike has reported.

NEWS
Sweden's airspace shut down by Russian APT, not a solar storm
BY JEREMY DAVIS APRIL 13, 2016
A cyberattack launched by a Russian APT group may have jammed Sweden's air traffic control capabilities, that was initially attributed to a solar storm.

FEATURE
Dissecting an APT attack
BY DANNY BRADBURY APRIL 1, 2016
Basic network hygiene and improved visibility can go a long way, as we might learn from the likes of Ashley Madison and Anthem. Danny Bradbury reports.

BRIEF
Changing of the TidePool: Operation Ke3chang malware evolves as APT threat reappears
BY BRADLEY BARTH MAY 23, 2016
Operation Ke3chang, the APT that in 2013 was discovered targeting Europe-based Ministries of Foreign Affairs, not only apparently remains active but also seems to be leveraging a new family of malware called TidePool.

BRIEF
'Suckfly' in the ointment: Chinese APT group steals code-signing certificates
BY BRADLEY BARTH MARCH 15, 2016
An APT group based in China, code-named Suckfly, has been concealing its nefarious activity over the past two years by stealing code-signing certificates and applying them to malware and hack tools to make them look legitimate.

NEWS
Guccifer 2.0 again denies Russian connection, mocks reports linking hacker to APT groups
BY JEREMY DAVIS SEPTEMBER 6, 2016
An individual who self-identified as Guccifer 2.0 continues to deny reports by security firms that link the purported hacker or hacking group to Russian advanced persistent threat (APT) groups.

NEWS
New report undresses 'Russian speaking' APT 28
DECEMBER 21, 2015
A new report by Bitdefender has, at least partially, undressed the infamous group APT28 claiming that it's a Russian speaking group with a particular interest in government officials, defence companies and Ukraine.

BRIEF
Cybercriminals increasingly launching APT-style attacks against banks, finds Kaspersky
BY BRADLEY BARTH FEBRUARY 8, 2016
Kaspersky Lab revealed that cybercrime organizations are increasingly stealing funds from banks by employing many of same Advanced Persistent Threat tools and tactics that previously were only attributable to nation-states.

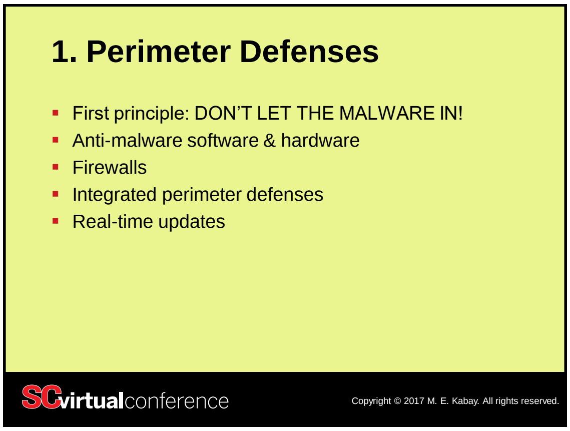
NEWS
Cylance exposes 'Dust Storm' APT attack on Japanese infrastructure
BY BRADLEY BARTH FEBRUARY 24, 2016
An advance persistent threat group has recently been concentrating its efforts on infiltrating Japanese critical infrastructure and key commercial interests, according to cybersecurity firm Cylance.

NEWS
APT spies used malware made for jealous spouses
APRIL 21, 2016
Trend Micro has dissected malware used in the Operation C-Major attack officers of the Indian army and tracked it back to malware that originated from Pakistan.

NEWS
Lord of the spy ring: Strider APT cites Tolkien, found snooping on Russian targets
BY BRADLEY BARTH AUGUST 8, 2016
Symantec yesterday disclosed its discovery of a cyberespionage group called Strider, which appears to be targeting mostly Russian entities with spyware attacks that bear the hallmarks of a sophisticated nation-state operation.

NEWS
Kaspersky confirms return of Carbanak and two more banking APT groups
FEBRUARY 9, 2016

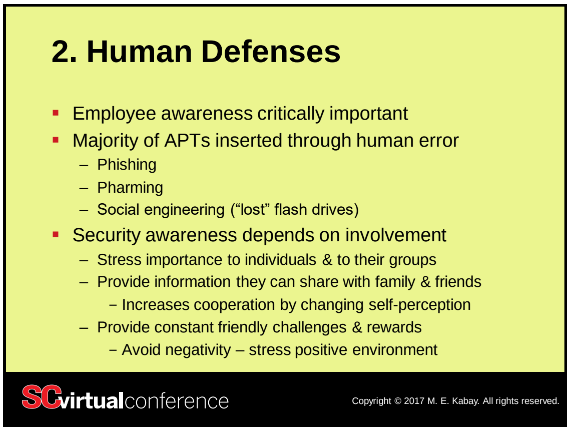
SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



1. Perimeter Defenses

- First principle: DON'T LET THE MALWARE IN!
- Anti-malware software & hardware
- Firewalls
- Integrated perimeter defenses
- Real-time updates

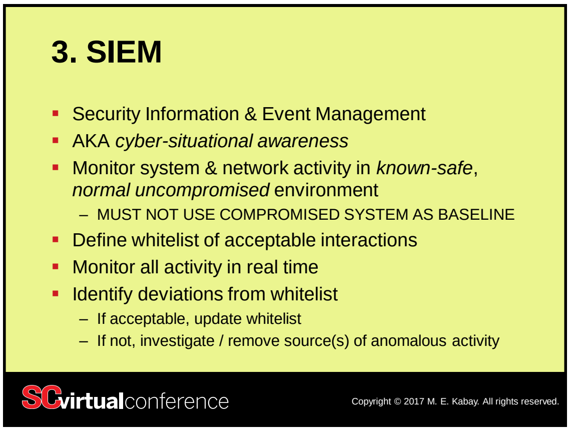
SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



2. Human Defenses

- Employee awareness critically important
- Majority of APTs inserted through human error
  - Phishing
  - Pharming
  - Social engineering ("lost" flash drives)
- Security awareness depends on involvement
  - Stress importance to individuals & to their groups
  - Provide information they can share with family & friends
    - Increases cooperation by changing self-perception
  - Provide constant friendly challenges & rewards
    - Avoid negativity – stress positive environment

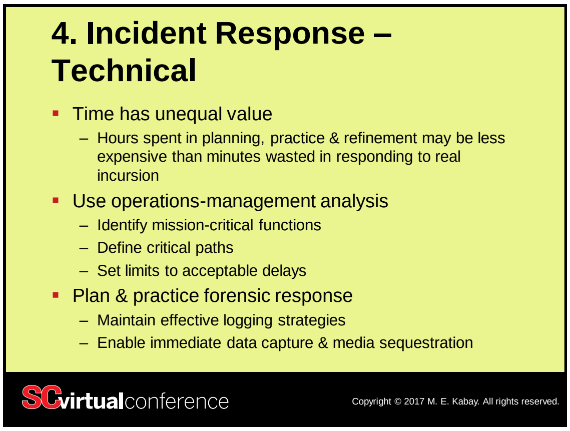
SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



3. SIEM

- Security Information & Event Management
- AKA *cyber-situational awareness*
- Monitor system & network activity in *known-safe*, *normal uncompromised* environment
  - MUST NOT USE COMPROMISED SYSTEM AS BASELINE
- Define whitelist of acceptable interactions
- Monitor all activity in real time
- Identify deviations from whitelist
  - If acceptable, update whitelist
  - If not, investigate / remove source(s) of anomalous activity

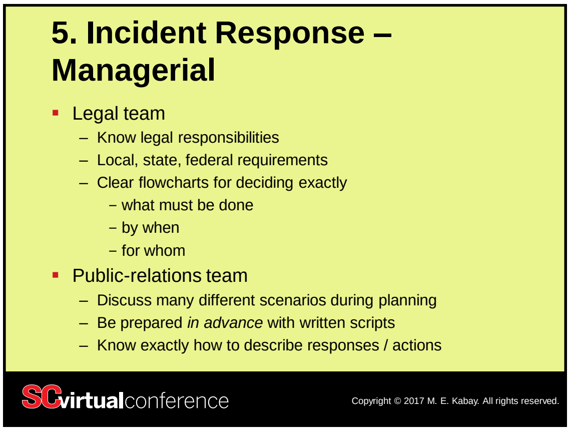
SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



4. Incident Response – Technical

- Time has unequal value
  - Hours spent in planning, practice & refinement may be less expensive than minutes wasted in responding to real incursion
- Use operations-management analysis
  - Identify mission-critical functions
  - Define critical paths
  - Set limits to acceptable delays
- Plan & practice forensic response
  - Maintain effective logging strategies
  - Enable immediate data capture & media sequestration

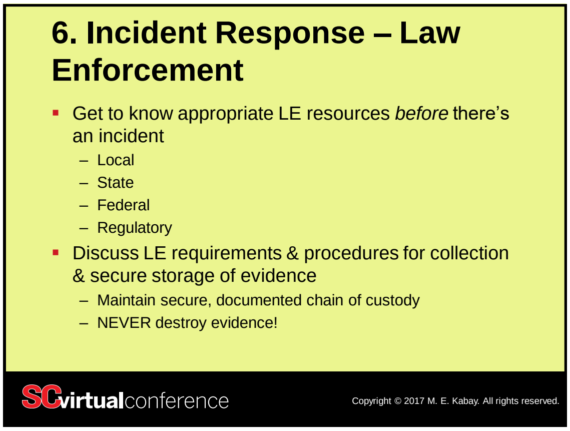
SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



5. Incident Response – Managerial

- Legal team
  - Know legal responsibilities
  - Local, state, federal requirements
  - Clear flowcharts for deciding exactly
    - what must be done
    - by when
    - for whom
- Public-relations team
  - Discuss many different scenarios during planning
  - Be prepared *in advance* with written scripts
  - Know exactly how to describe responses / actions

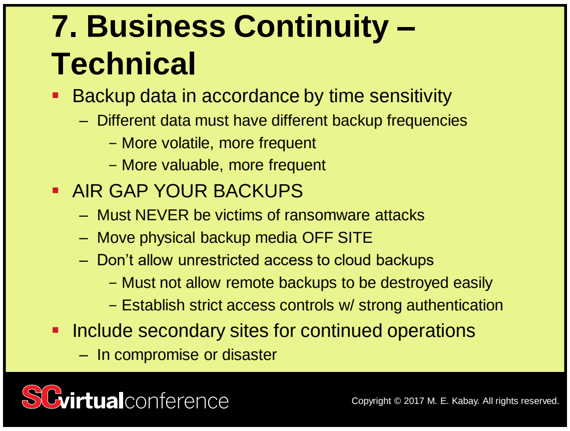
SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.



6. Incident Response – Law Enforcement

- Get to know appropriate LE resources *before* there's an incident
  - Local
  - State
  - Federal
  - Regulatory
- Discuss LE requirements & procedures for collection & secure storage of evidence
  - Maintain secure, documented chain of custody
  - NEVER destroy evidence!

SCvirtualconference Copyright © 2017 M. E. Kabay. All rights reserved.

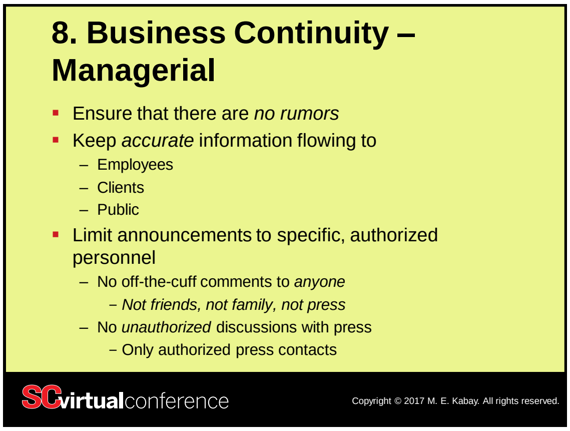


7. Business Continuity – Technical

- Backup data in accordance by time sensitivity
  - Different data must have different backup frequencies
    - More volatile, more frequent
    - More valuable, more frequent
- AIR GAP YOUR BACKUPS
  - Must NEVER be victims of ransomware attacks
  - Move physical backup media OFF SITE
  - Don't allow unrestricted access to cloud backups
    - Must not allow remote backups to be destroyed easily
    - Establish strict access controls w/ strong authentication
- Include secondary sites for continued operations
  - In compromise or disaster

SCvirtualconference

Copyright © 2017 M. E. Kabay. All rights reserved.

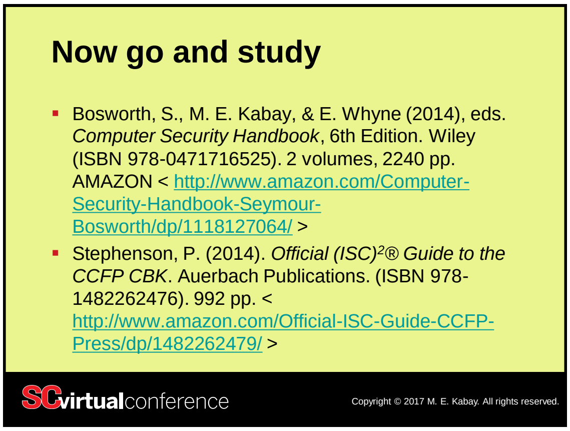


8. Business Continuity – Managerial

- Ensure that there are *no rumors*
- Keep *accurate* information flowing to
  - Employees
  - Clients
  - Public
- Limit announcements to specific, authorized personnel
  - No off-the-cuff comments to *anyone*
    - *Not friends, not family, not press*
  - No *unauthorized* discussions with press
    - Only authorized press contacts

SCvirtualconference

Copyright © 2017 M. E. Kabay. All rights reserved.



Now go and study

- Bosworth, S., M. E. Kabay, & E. Whyne (2014), eds. *Computer Security Handbook*, 6th Edition. Wiley (ISBN 978-0471716525). 2 volumes, 2240 pp. AMAZON < http://www.amazon.com/Computer-Security-Handbook-Seymour-Bosworth/dp/1118127064/ >
- Stephenson, P. (2014). *Official (ISC)^{2}® Guide to the CCFP CBK*. Auerbach Publications. (ISBN 978-1482262476). 992 pp. < http://www.amazon.com/Official-ISC-Guide-CCFP-Press/dp/1482262479/ >

SCvirtualconference

Copyright © 2017 M. E. Kabay. All rights reserved.

DISCUSSION

SCvirtualconference

Copyright © 2017 M. E. Kabay. All rights reserved.