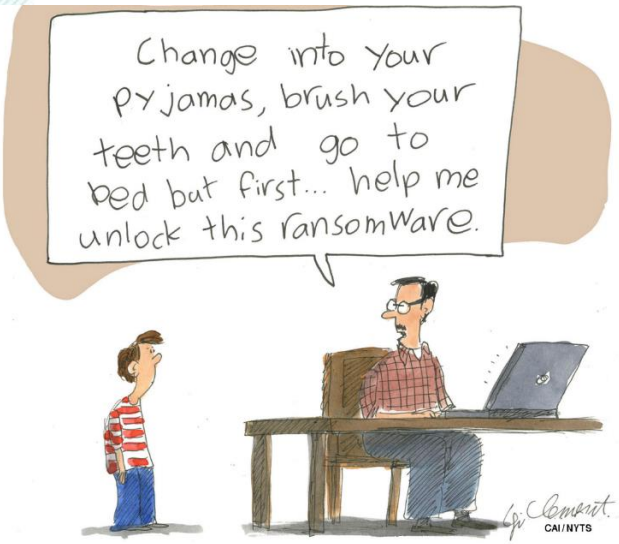
Security Incident Handling for Schools

Bernard Kan
Senior Consultant
HKCERT

Agenda

- About HKCERT
- Security Incidents that Impact Schools
- Incident Handling Life Cycle
- Challenge of Security Incident Handling
- Key Take Away



Hong Kong Computer Emergency Response Team Coordination Centre

HKCERT

香港電腦保安事故協調中心

- Established in 2001
- Funded by the HKSAR Government
- Operated by **Hong Kong Productivity Council (香港生產力促進局)**

- Mission
  - –As the coordination of local cyber security incidents, serving Internet Users and SMEs in Hong Kong
  - –As the Point of Contact of cyber security incidents across the border

Security Incidents that Impact Schools

What is a Security Incident

- Security incident broadly refer to those incidents resulting from deliberate malicious technical activities
- Can result from a malware (ransomware, worm, virus, etc.), other malicious codes, or a system intruder, either insider or outsider

Security Incidents that Impact Schools

Ransomware Incident

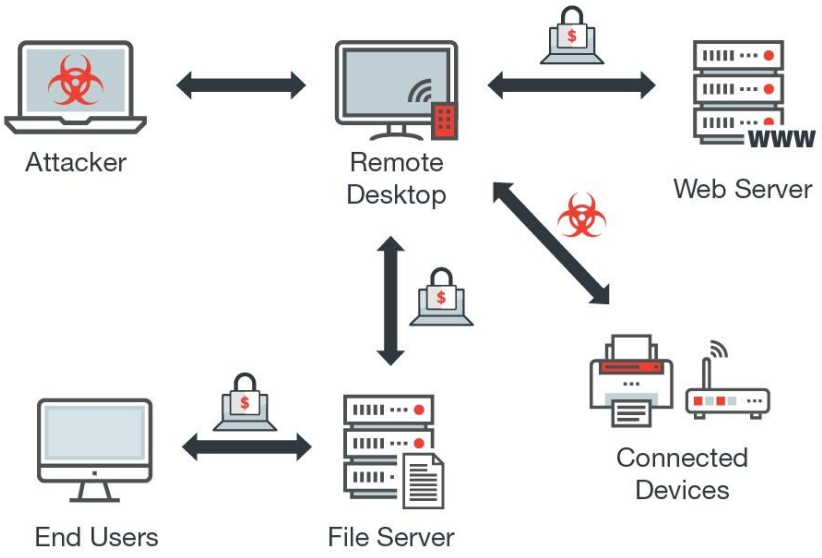
Hacking Extortions

WWPKG 縱橫遊 (Nov 2017)
Affected 200,000 Hong Kong users
Attacker demanded millions of HKD in Bitcoins

BigLine 大航假期 (Jan 2018)
Goldjoy 金怡假期 (Jan 2018)

Attacker claimed to compromise system obtaining customer data and demanded ransom

Ransomware via RDP – CrySIS / Dharma



Encrypted files with extension .aerna

DDoS Attack

Largest Ever 1.3Tbps DDoS Attack Includes Embedded Ransom Demands

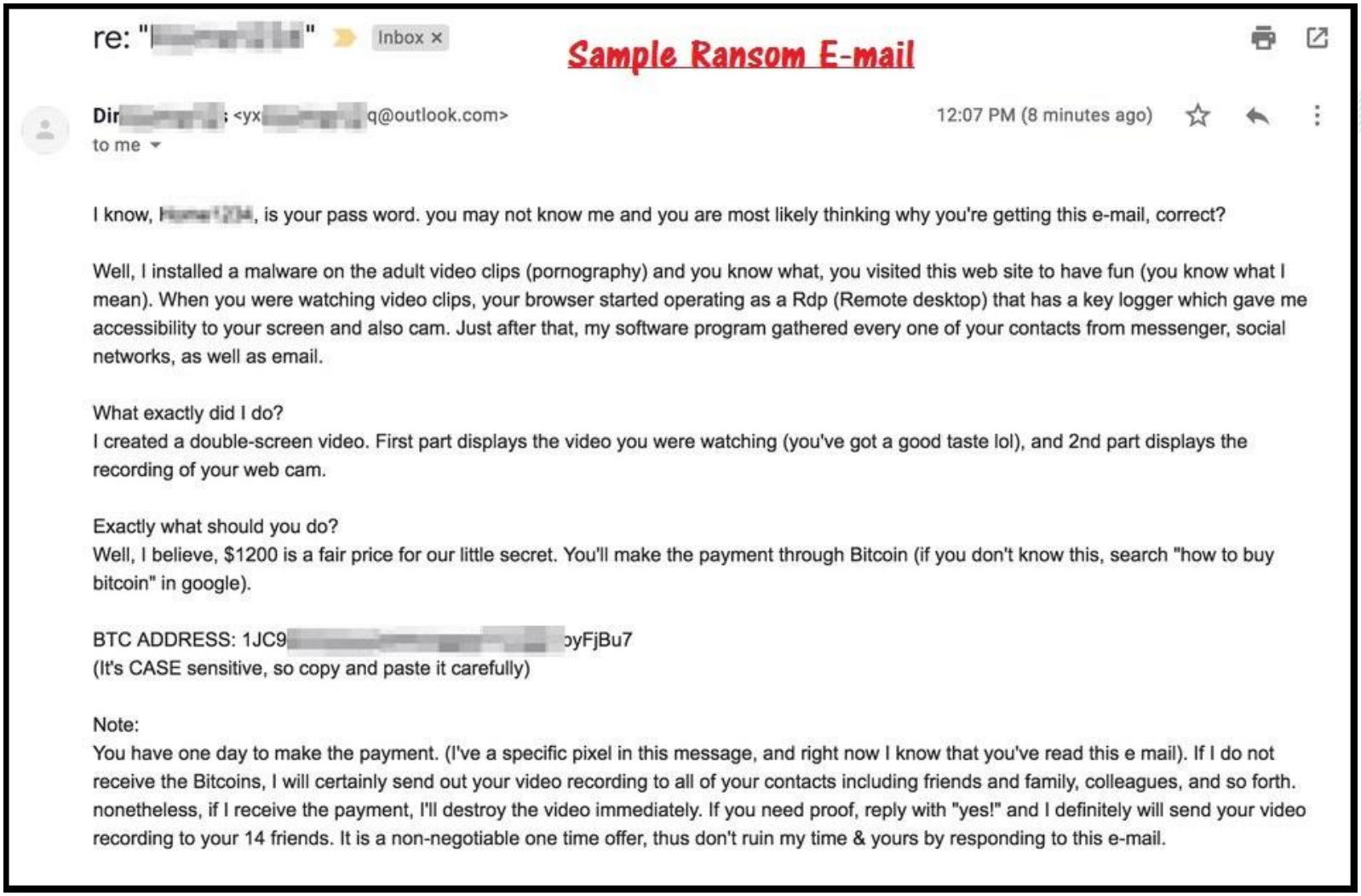
By Kevin Townsend on March 05, 2018

[UPDATED - New record set at 1.7Tbs] On Tuesday, February 27, three major DDoS mitigation service providers (Akamai, Cloudflare and Arbor) **warned** that they had seen spikes in a relatively rare form of reflection/amplification DDoS attack via Memcached servers. Each service provider warned that this type of reflection attack had the potential to deliver far larger attacks.

One day later, Wednesday, February 28, GitHub was hit by the largest DDoS attack that had ever been disclosed -- more than twice the size of the **Mirai attack of 2016**, peaking at 1.3Tbps. And still the potential, in the short term at least, is for even larger attacks.

Amplification attacks are generated when a server can be 'tricked' into sending a larger response than the initial query. Reflection occurs when the requesting IP is spoofed. The result is that multiple servers can be tricked into sending large responses to a single target IP, rapidly overwhelming it with the volume sent.

Ransom E-mails



re: "[redacted]" Inbox ×

Sample Ransom E-mail

Dir[redacted] <yx[redacted]q@outlook.com> 12:07 PM (8 minutes ago)

to me

I know, [redacted], is your pass word. you may not know me and you are most likely thinking why you're getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What exactly did I do?
I created a double-screen video. First part displays the video you were watching (you've got a good taste lol), and 2nd part displays the recording of your web cam.

Exactly what should you do?
Well, I believe, $1200 is a fair price for our little secret. You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in google).

BTC ADDRESS: 1JC9[redacted]oyFjBu7
(It's CASE sensitive, so copy and paste it carefully)

Note:
You have one day to make the payment. (I've a specific pixel in this message, and right now I know that you've read this e mail). If I do not receive the Bitcoins, I will certainly send out your video recording to all of your contacts including friends and family, colleagues, and so forth. nonetheless, if I receive the payment, I'll destroy the video immediately. If you need proof, reply with "yes!" and I definitely will send your video recording to your 14 friends. It is a non-negotiable one time offer, thus don't ruin my time & yours by responding to this e-mail.

Information Leakage

- Loss of devices
  - –Disks / USB

    Thumb Drive
  - –Mobile Devices

Loss of Notebook

Laptops containing 3.7 m ×

www.scmp.com/news/hong-kong/politics/article/2082566/laptops-containing-37-million-hong-kong-voters-data-stolen

South China Morning Post HK CHINA ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT WEEK IN ASIA POST MAG STYLE .TV

374 SHARES

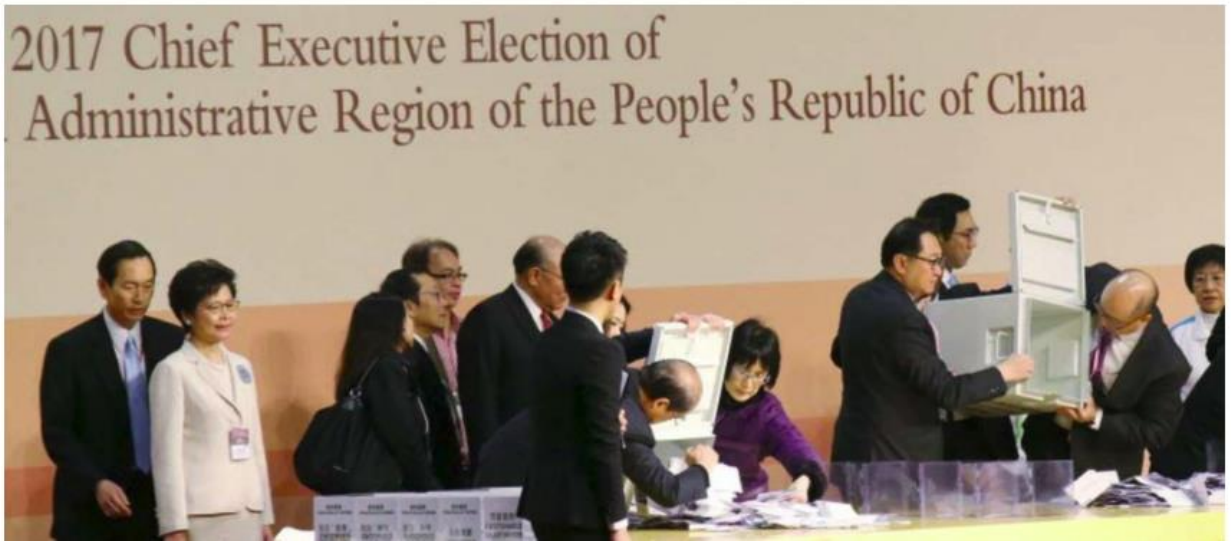
NOW READING Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive

Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive election

Devices contained ID card numbers, addresses and mobile numbers

PUBLISHED : Tuesday, 28 March, 2017, 12:30am
UPDATED : Tuesday, 28 March, 2017, 1:42am

COMMENTS: 24



How Do We Handle Incidents?

Incident Handling Life Cycle

Preparation (1)

- Senior management assign someone responsible for security incident (e.g. IT staff, security staff, etc.) & setup an incident response team
- Design the flow and process of incident handling, tools & resources needed
  - R&R of staff
  - Contact list (senior management, staff, vendors, etc.)
  - Incident report mechanisms – forms, emails, IM, etc.
  - Secure communication channels & storage
  - War room & conference equipment (e.g. con call no.)

Preparation (2)

- Implement monitoring & response capability
  - –Centralized logging (e.g. server logs, IDS/IPS logs, MRTG, anti-virus, etc.)
  - –Prepare forensic tools & skills (forensic workstations, backup devices, USBs, packet sniffers / protocol analyzers, forensic software, skills) – can consider outsource to vendor
  - –System documentations (e.g. system manuals, network diagrams, hardware & software inventory, firewall rules, etc.)
  - –Need to build a baseline: what is normal & abnormal

Detection and Analysis (1)

- Detection:
  - –Users (teachers, students, etc.) needed be aware of incident handling flow and report to helpdesk or IT staff when abnormality is detected
  - –IT staff needed be aware of abnormality happened in systems & network (from logs, system alerts, user reports, etc.)
  - –IT or security staff needed be aware of publicly available or external intelligence (e.g. new vulnerabilities & attack information, incidents of related organizations, external reports, etc.) – HKCERT plays a role here

Detection and Analysis (2)

- Analysis
  - –Need someone understand the normal behavior & determine if reported behavior is abnormal - a process called "Triage"
  - –If confirmed to be a security incident, then handle the incident according to pre-defined incident handling process
  - –Centralized logs can be used in "event correlation" (need time synchronization as well)
  - –Determine of the scope of impact (what systems are involved, what data is involved, what users are involved, etc.) - an important process called "Impact Assessment"

Detection and Analysis (3)

- Analysis (con't)
  - –Documentation & logging during handling is important (especially for potential court cases)
  - –Document discovered events & time, phone conversations, file changes made, etc.
  - –Work in team of two, one do the work, one check the work (or sign)
  - –Maintain the "Chain of Custody"
  - –Keep senior management informed of the progress

Detection and Analysis (4)

- Prioritization
  - –If many events happen in quick succession then need to prioritize them
    - root compromise vs worm spreading
    - public web server vs internal file server
  - –Need to consider service level agreement SLA (if any)
    - Maximum down time
    - Minimum respond time

Detection and Analysis (5)

- Notifications
  - –Senior Management
  - –Head of information security
  - –Other incident teams
  - –System owner
  - –Human resources (if it involves employees)
  - –Public affairs (if it might generate publicity)
  - –Legal dept
  - –Public stake holders
  - –HKCERT, EDB ITE Section and/or HKPF if necessary

Containment, Eradication and Recovery (1)

- Containment Strategy
  - –Method
    - Shut down
    - Disconnect from the network (wired or wireless)
    - Segment the network
    - Disable functions
    - Block hosts or ports at the perimeter
    - Rebuild or clean
    - Check with HKCERT for malware/ransomware solution (if any)

Containment, Eradication and Recovery (2)

- Containment Strategy
  - Considerations
    - Potential damage to and reduce of resources
    - Need for evidence preservation
    - Service availability
    - Time needed to implement the strategy
    - Effectiveness of the strategy
    - Duration of the solution
      - Emergency work around (several hours)
      - Temporary work around (several weeks)

Post Incident Activities

- Lessons learned
- Policy updates
- Improvements be made to Preparation phase

- Pursue legal action (work with HKPF)

Challenges of Incident Handling

- Users awareness problem – incidents keep on repeating
- New system vulnerabilities discovered frequently – difficulties in keep up with security patches
- New security issues with new technologies e.g. mobile devices, IoT devices, etc.
- Lack of security resources e.g. budget & personnel

Points to Take Away

- Security incidents are common nowadays in organizations and schools are also impacted by incidents
- Security incident handling capability needed be setup in order to minimize risk and impact when incidents happened
- Incident Handling Life Cycle involved 4 phases: Preparation, Detection & Analysis, Containment Eradication & Recovery and Post Incident Activities
- Organizations / Schools need to allocate appropriate security resources to get prepared for potential security incidents

Thanks