How to be ready to defend against APT

HOI Wai Khin, Member (ISACA Singapore Chapter)

28 August 2020

GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA®
Singapore Chapter

About me

HOI, Wai Khin

Director, Business Consulting

HoiWaiKhin@RSMSingapore.sg

- Certified Information Systems Security Professional (CISSP), (ISC)²
- Certified Information Security Manager (CISM), ISACA
- Certified in Risk and Information Systems Control (CRISC), ISACA
- Certified Business Continuity Professional (CBCP), DRI International
- Singapore Certified Management Consultant (PSCMC), TUV SUD PSB
- Master of Science Information Security, University of London, Royal Holloway
- Master of Science Software Engineering, University of Essex

One day

I was asked by my CIO on how to be ready to prevent or defend against an Advance Persistent Attack (“APT”).

Second day

I told my CIO,

First, we need to understand what is Advance Persistent Threat

- A kind of cybersecurity attack
- Gain unauthorized access to data or systems by an individual or a group for an extended period of time.
- Remain undetected for as long as possible while “harvesting” and sending as much sensitive data as possible.
- Simple financial gain to state-sponsored political maneuvering.
- Usually highly targeted, meticulously planned in advance and using sophistically techniques.

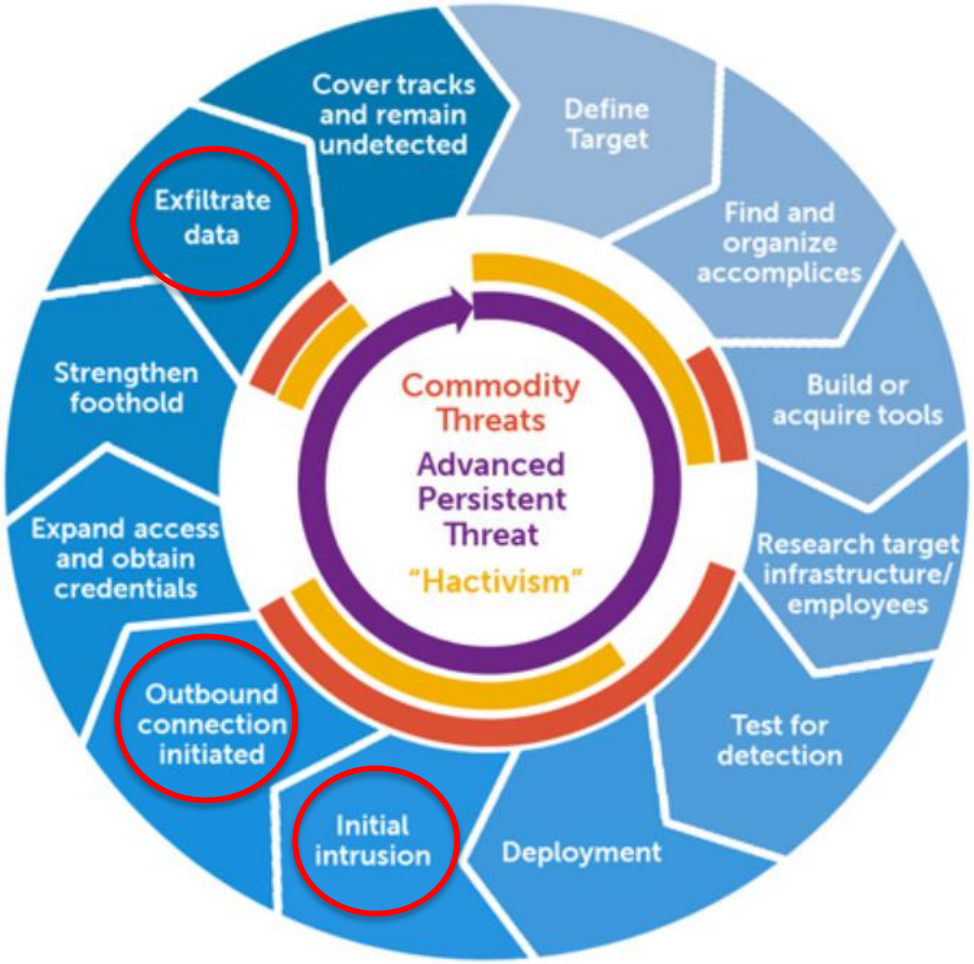
Third day

I told the CIO,

Secondly, we need to know the Advance Persistent Threat Attack Methods

- Spear Phishing:
- Social Engineering
- Rootkits:

Fourth day



I told my CIO,

Next, we need to understand the Advance Persistent Threat Life Cycle and identify the key risk areas.

Ref: https://en.wikipedia.org/wiki/Advanced_persistent_threat

Fifth day

I told my CIO,

Now we know the attack methods and life cycle, let's conduct an assessment and define the scope before preparing the audit plan and programme.

1. Identify the key department e.g. CEO office
2. Identify the key stakeholders e.g. CEO
3. Identify the valuable or confidential data e.g. Strategy, M&A etc
4. Identify the IT systems used
5. Identify the key confidential data

Sixth day

I told my CIO the analysis has been done and below is the threat assessment

Target : CEO

Method	Probability	Source	Common Channels	Common outgoing channels
Spear Phishing	High	Laptop	Company Email	Company Firewall
		Tablets	Company Internet	
		Mobile Phones		
Social Engineering	Medium	Tablets	Internet	Home Firewall
		Mobile Phones		
Rootkit	Medium	Laptop	Internet	Company/Home firewall
		Mobile phone	USB	

Seventh day

I told my CIO since the threat assessment has been done, let's identify the basic key controls

Target : CEO, **Attack Method** : Social Engineering, **Probability** : High

Source	Common Channels	Common outgoing channels
Laptop	Company Email	Company Firewall
Tablets	Company Internet	
Mobile Phones		

Basic audit cnsiderations

- Network security policy
- Vulnerability assessment operation
- Patch management
- Change management
- Logging and monitoring
- Intrusion detection
- Incident alert/response

Basic audit considerations

1. End point hardening policy
2. **KNOWN** Malware, phishing & virus protection
3. Patch management
4. Host based intrusion
5. Rouge software/ unlicensed software
6. User awareness
7. Restriction of local admin account

Basic audit consideration

- Internet and email policy
- Email access control
- Email monitoring
- Website filtering

Seventh day

I told my CIO since the threat assessment has been done, let's identify the basic key controls

Target : CEO, **Attack Method** : Social Engineering, **Probability** : Medium

Source	Common Channels	Common outgoing channels
Tablets	Internet	Home Firewall
Mobile Phones		

Basic audit considerations

- NA

Basic audit considerations

1. End point hardening policy
2. **KNOWN** Malware, phishing & virus protection
3. Patch management
4. Rouge software/ unlicensed software
5. User awareness

Basic audit consideration

- NA

Seventh day

I told my CIO since the threat assessment has been done, let's identify the basic key controls

Target : CEO, **Attack Method** : Rootkit, **Probability** : Medium

Source	Common Channels	Common outgoing channels
Laptop	Internet	Home/Company Firewall
Mobile Phones	Email	
	USB	

Basic audit considerations

- Network security policy
- Vulnerability assessment operation
- Patch management
- Change management
- Logging and monitoring
- Intrusion detection
- Incident alert/response

Basic audit considerations

1. End point hardening policy
2. **KNOWN** Malware, phishing & virus protection
3. Patch management
4. Host based intrusion
5. Rouge software/ unlicensed software
6. User awareness
7. Restriction of local admin account
8. USB restriction

Basic audit consideration

- Internet and email policy
- Email access control
- Email monitoring
- Website filtering

Eighth day

I told my CIO since the threat assessment has been done, let's identify the **advance** controls (if any)

Source	Common Channels	Common outgoing channels
Laptop	Internet	Home/Company Firewall
Mobile Phones	Email	
	USB	

Advance audit considerations

- Deployment of web application firewall
- Detection though SIEM monitoring
- Threat hunting / Intelligence monitoring
- Database monitoring

Advance audit considerations

1. Logging and monitoring
2. Behavioral analysis
3. Lock down

Advance audit consideration

- NA

Ninth day

Developing the audit programme

Basic audit considerations

1. End point hardening policy
2. **KNOWN** Malware, phishing & virus protection
3. Patch management
4. Host based intrusion
5. Rouge software/ unlicensed software
6. User awareness
7. Restriction of local admin account

Basic audit consideration

- Internet and email policy
- Email access control & monitoring
- Website filtering

Basic audit cnsiderations

- Network security policy
- Vulnerability assessment operation
- Patch management
- Change management
- Logging and monitoring
- Intrusion detection
- Incident alert/response

References

Figure 3—Sources of Assurance/Good Practice

Source	Description
ISACA	COBIT 5[10] White papers[11] Cloud computing guidance[12] Cyber security resources[13]
US Department of Defense	Security Technical Implementation Guides (STIGs)[14]
CIS	Center for Internet Security Benchmarks[15]
ISO	International Organization for Standardization, ISO/IEC 27000 family—*Information security management systems*[16]
CSA	Cloud Security Alliance[17]
NIST	US National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity[18] Security and Privacy Controls for Federal Information Systems and Organizations[19] NIST publications[20]
PCI DSS	Payment Card Industry Data Security Standard[21]*
ITIL	Information Technology Infrastructure Library[22]

*ISO and PCI DSS can also be used as sources of best practice even where compliance is not required.

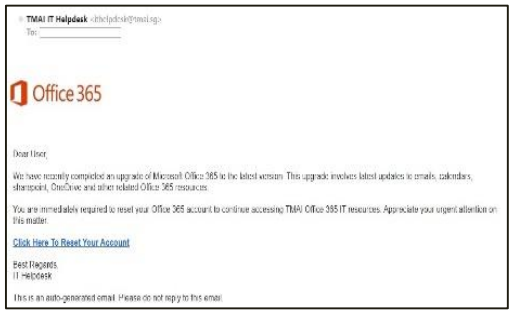
Source: Ian Cooke. Reprinted with permission.

Tenth day

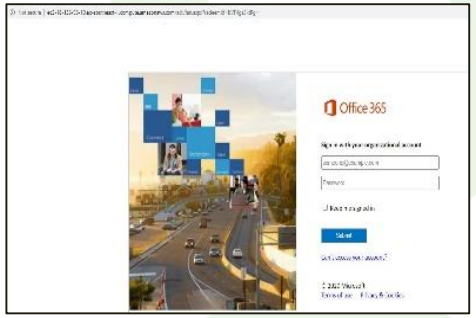
I told my CIO why don't we do a phishing simulation exercise to test the awareness of all our users

1. Select & set up Campaign

2. User receive phishing email



3. Users enter username and password



4. Redirect back to landing page

Designed for users to click on a link to reset their email account. After clicking on the "reset" link, Users' will be redirected to a webpage where they are required to sign in using their individual email account. When credentials are submitted, they will be forwarded to a "You've Been Phished!" landing page. We then compile the results and report this to the management

No. of Phishing Clicks	1	2	3	4	5	6	7	8	9	11	18	Total by department
[redacted]	10	10	11	2	2	0	0	0	0	0	0	35
	3	2	1	0	0	0	0	0	0	1	0	7
	4	2	0	0	0	0	0	0	0	0	0	6
	0	1	0	0	0	0	0	0	0	0	0	1
	12	8	5	1	0	0	0	0	1	0	0	27
	52	48	23	10	10	3	1	1	0	0	1	149
	4	6	4	2	4	0	0	0	0	0	0	20
	6	9	7	4	2	0	0	0	0	0	0	28
Total by whole company	91	86	51	19	18	3	1	1	1	1	1	

GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA®

Singapore Chapter