



SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

QUANG M. TRAN - VIETTEL CYBER SECURITY

SECURITY WORLD 2018

ANATOMY OF APT ATTACKS IN VIETNAM

ABOUT ME

- ▶ **Quang M. Tran**
- ▶ Manager of Malware Research Dept. - Viettel Cyber Security
- ▶ Reverser, Malware Analyst, Security Researcher, Programmer
- ▶ Love traveling and sport
- ▶  quangking  quangtrm



AGENDA

- ▶ APT overview
- ▶ APT life cycle - Red vs. Blue
- ▶ Conclusion



SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

ANATOMY OF APT ATTACKS IN VIETNAM

ADVANCE PERSISTENCE THREAT

APT OVERVIEW

Advanced

Persistent

Threat

APT OVERVIEW

► Timeline

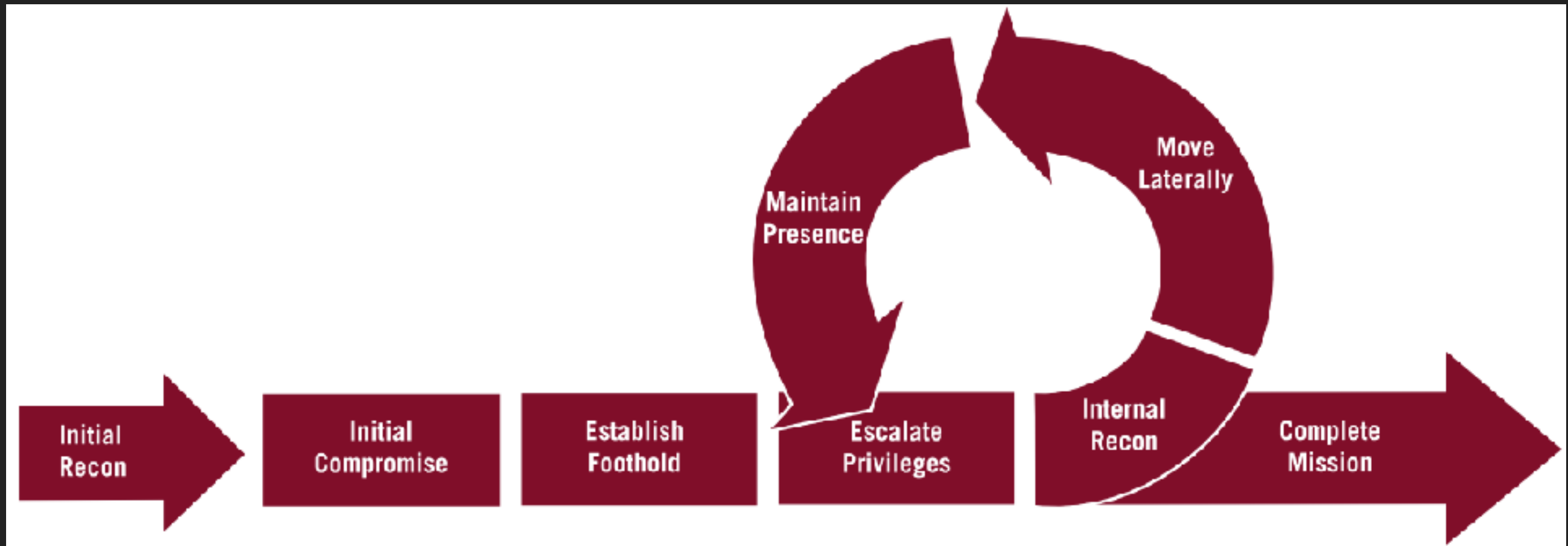
First Sample	
2007	Satellite Turla, FinSpy, Turla
2008	Hacking Team
2009	Lazarus, Naikon
2010	Penguin Turla
2011	
2012	Spring Dragon
2013	
2014	
2015	
2016	
2017	

Discovery	
2007	
2008	
2009	
2010	
2011	FinSpy, Hacking Team, Naikon
2012	
2013	
2014	Penguin Turla, Turla
2015	Satellite Turla
2016	Lazarus
2017	Spring Dragon

Source: apt.securelist.com

APT OVERVIEW

▶ APT life cycle





SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

ANATOMY OF APT ATTACKS IN VIETNAM

APT LIFE CYCLE – RED VS. BLUE

INITIAL COMPROMISE

▶ Red team

- ▶ Phishing email
- ▶ Drive-by download
- ▶ Web attack

▶ Blue team

- ▶ Email security
- ▶ Web gateway
- ▶ Web application firewall

INITIAL COMPROMISE

► Phishing email - Fake Gmail Error Message



Tài liệu được bảo vệ bằng Google Mail !

Nhấn **"Enable Editing"**, sau đó nhấn **"Enable Content"**

Hoặc nhấn **"Option"** sau đó nhấn **"Enable this content"** để hiển thị nội dung được bảo vệ.

Error: 0x234625678

INITIAL COMPROMISE

► Phishing email - Fake Text Encoding Error Message

H?P ??NG CUNG C?P D?CH V? PH?N M?M

(S? H?DV-310317/DYNO-VTC)

zæÁeÜÉ!øøfci¶Ú:

Êdæ@'jððç•ÔeÄä

zæÁeÜÉ!øøfci¶Ú:

zæÁeÜÉ!øøfci¶Ú:

ÔÁÒçj·VY&}zæÁel

úa-&)}9<ð&á#G

Êdæ@'jððç•ÔeÄä

#G)ððñ ÔÁÒçj·VY.

ÔÁÒçj·VY&}zæÁeÜÉ!øøfci¶Ú3Ænã €×

9<ð&á#G)ððñ ÔÁÒçj·VY&}zæÁeÜÉ!øøfci¶Ú3Ænã €×13!Î™Ú4&H H»,%oLÊdæ@'jð

Êdæ@'jððç•ÔeÄä>ÔÁÒçj·VY&}zæÁeÜÉ!øøfci¶Ú3Ænã H

ÔÁÒçj·VY&}zæÁeÜÉ!øøfci¶Ú3Ænã%Äç2Ô€×13!Î™Ú4&H H»,%oLÊdæ@'jðŽ6

úa-&)}
- C?n c? Lu?t Th??ng M?l s? 36/2005/QH11 ???c ban h?nh ng?y 14/06/2005 c?a Qu?c H?l n??c
C?ng H?a X? H?l Ch? Ngh?a Vi?t Nam;



H»,%o

æ@'jð

INITIAL COMPROMISE - PHISHING EMAIL - DETECTION

✖ Event detail

Event:

Email nguồn đáng ngờ đính kèm chứa mã độc

Detail:

Phát hiện email có tiêu đề [Chung huyen với backend side - Tran Trung Nghia [HIT_HRFA_HIRWARIDHI]] gửi từ [ng [REDACTED]@gmail.com] tới [tuyendung@vietel.com.vn] có file đính kèm chứa mã độc << View less

✖ Advanced View

Search

26RESULTS

Showentries

No. ▲	Key	Value
1	alert_id	171220_017775
2	category	Malware
3	correlation_engine_id	SIG
4	datetime	10.23.33 20/12/2017
5	description	Phát hiện email có tiêu đề [Chung huyen với backend side - Tran Trung Nghia [HIT_HRFA_HIRWARIDHI]] gửi từ [REDACTED]@gmail.com] tới [tuyendung@vietel.com.vn] có file đính kèm chứa mã độc << View less
6	device_product	Correlation Engine
7	device_vendor	SIG
8	device_version	1.0.0
9	extra_data	[{"attachment": [{"sha1": "8507FA9215F389FFF17F84FF2975A9B31C07A49F", "name": "CV - TranTrungNghia.doc", "comment": "Exploit AS/ R?", "url": null, "blocked_url": ""}]] << View less
10	mailfrom	[REDACTED]@gmail.com

ESTABLISH Foothold

▶ Red team

- ▶ Install first-stage malware

▶ Blue team

- ▶ Host-based security endpoint

ESTABLISH FOOTHOLD

- ▶ **First-stage malware**
 - ▶ <ảnh minh họa file mã độc bypass antivirus>

ESTABLISH FOOTHOLD

- ▶ **First-stage malware**

- ▶ <ảnh minh hoạ cảnh báo cài đặt phần mềm + server kết nối outbound>

ESCALATE PRIVILEGES

▶ Red team

- ▶ Harvest access credentials from the compromised PC
- ▶ Escalate privilege on non-administrative users

▶ Blue team

- ▶ Password dumping detection & keylogger detection
- ▶ Privilege escalation detection

ESCALATE PRIVILEGES

- ▶ Password dumpping
 - ▶ <ảnh minh hoạ sử dụng mimikatz>

ESCALATE PRIVILEGES

- ▶ **Password dumping**
 - ▶ <ảnh minh hoạ cảnh bao mimikatz>

ESCALATE PRIVILEGES

- ▶ **Privilege escalation**
 - ▶ <ảnh minh hoạ leo quyền Windows>

ESCALATE PRIVILEGES

- ▶ **Privilege escalation**

- ▶ <ảnh minh họa detect leo quyền windows>

INTERNAL RECON

▶ Red team

- ▶ Port scanning

▶ Blue team

- ▶ Network-based port scanning detection
- ▶ Host-based port scanning detection

INTERNAL RECON

- ▶ **Port scanning**

- ▶ <ảnh minh hoạ scanline>

INTERNAL RECON

- ▶ **Port scanning**
 - ▶ <ảnh minh hoạ detect scanline>

MOVE Laterally

▶ Red team

- ▶ Network login
 - ▶ Remote execution/task schedule
- ▶ Remote desktop
- ▶ Tunneling
 - ▶ Tools
 - ▶ Windows mechanism

▶ Blue team

- ▶ Network login detection
 - ▶ Event log analysis
 - ▶ Host-based & network-based detection
- ▶ Anomaly RDP detection
- ▶ Tunneling detection

MOVE Laterally

- ▶ Remote network login
 - ▶ <ảnh minh họa sử dụng psexec>

MOVE Laterally

- ▶ Remote network login
 - ▶ <ảnh minh họa detect psexec>

MOVE Laterally

- ▶ **Tunneling**
 - ▶ <ảnh minh họa sử dụng HTran>

MOVE Laterally

- ▶ **Tunneling**

- ▶ <ảnh minh họa cảnh báo phát hiện tunnel>

MAINTAIN PERSISTENCE

▶ Red team

- ▶ Install additional backdoors
 - ▶ Multiple backdoors
 - ▶ IIS backdoor
 - ▶ sethc backdoor
 - ▶ Stealth webshells
 - ▶ ...

▶ Blue team

- ▶ Host-based backdoor installing detection
- ▶ Directory monitoring/ webshell detection

MAINTAIN PERSISTENCE

- ▶ **sethc backdoor**
 - ▶ <ảnh minh hoạ sethc backdoor>

MAINTAIN PERSISTENCE

- ▶ **sethc backdoor**

- ▶ <ảnh minh họa detect sethc backdoor>

MAINTAIN PERSISTENCE

- ▶ **Stealth webshell**
 - ▶ <ảnh minh hoạ exchange backdoor>

MAINTAIN PERSISTENCE

- ▶ **Stealth webshell**

- ▶ <ảnh minh hoạ detect exchange backdoor bang giam sat thu muc>

COMPLETE MISSION

▶ Red team

- ▶ Compress, encrypt data
 - ▶ rar.exe
- ▶ Exfiltrate
 - ▶ FTP
 - ▶ Backdoor

▶ Blue team

- ▶ Data compression detection
- ▶ Data exfiltration detection
- ▶ Data Loss Prevention (DLP)

MAINTAIN PERSISTENCE

- ▶ **Compress & encrypt data**
 - ▶ <ảnh minh hoạ rar nén data>

MAINTAIN PERSISTENCE

- ▶ **Compress & encrypt data**
 - ▶ <ảnh minh hoạ detect rar nen data>

MAINTAIN PERSISTENCE

- ▶ **Data exfiltration**

- ▶ <ảnh minh hoạ upload FTP>

MAINTAIN PERSISTENCE

- ▶ **Data exfiltration**
 - ▶ <ảnh minh họa detect upload FTP>



SECURITY WORLD 2018

5 | 4 | 2018


JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

ANATOMY OF APT ATTACKS IN VIETNAM

CONCLUSION

CONCLUSION

- ▶ Vietnam is one of the hottest targets for APT attacks
- ▶ Traditional solutions (AV, Firewall, IPS/IDS...) is not enough
- ▶ Advanced solutions help (PC/Server Security Endpoint, Email Security, Big Data & Data Mining...)
- ▶ 24/7 Security Operation Center is the best solution

Hosted by:  MINISTRY OF PUBLIC SECURITY

Organized
Supported by: CYBER SECURITY DEPARTMENT - MPS AUTHORITY OF INFORMATION SECURITY - MIC  IDG



SECURITY WORLD 2018

5 | 4 | 2018

JW Marriott Hotel Hanoi, No 8 Do Duc Duc Road, Hanoi Vietnam

THANK YOU!