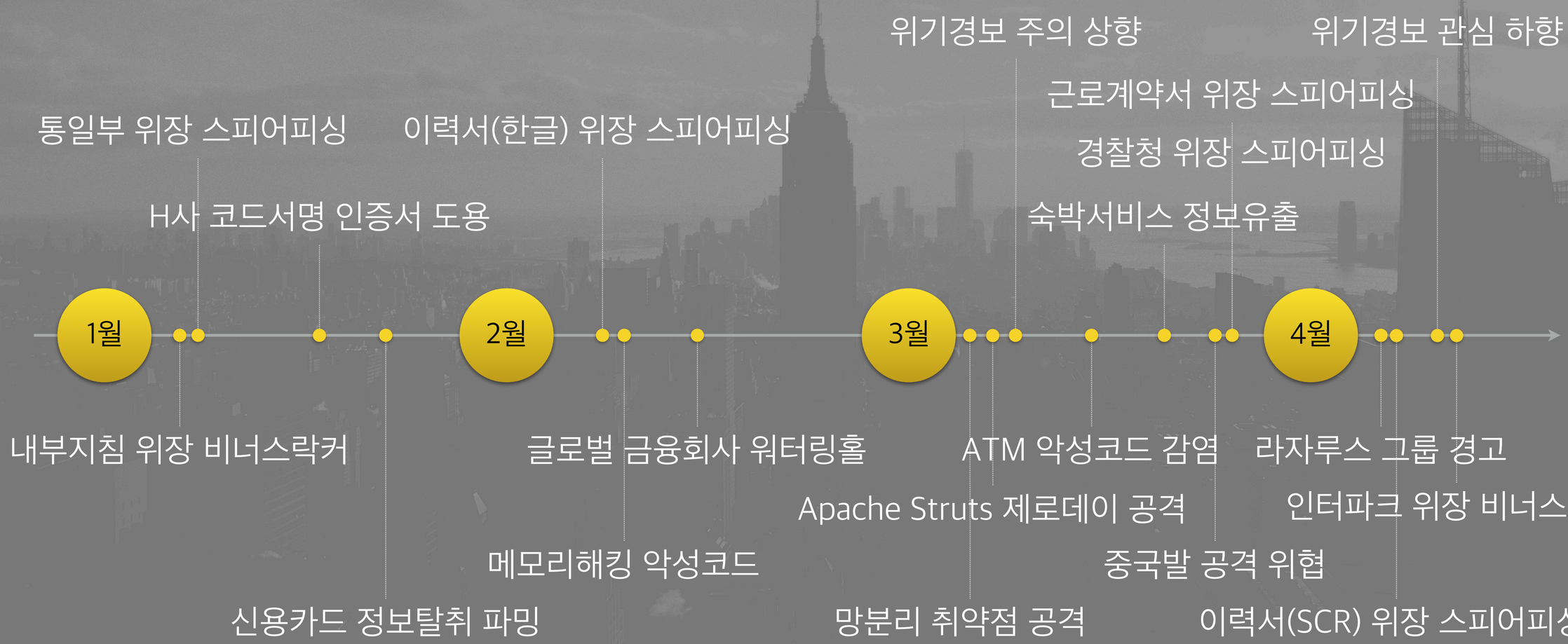
2017년 금융 사이버 공격 현황 및 전망

유정각

jglyu@fsec.or.kr

금융보안원
FINANCIAL SECURITY INSTITUTE

2017년 금융 사이버 공격



끝없는 파밍 & 메모리해킹 조직 귀환

Landing — Malvertising

→ Hopping #1

↓ Hopping #..n

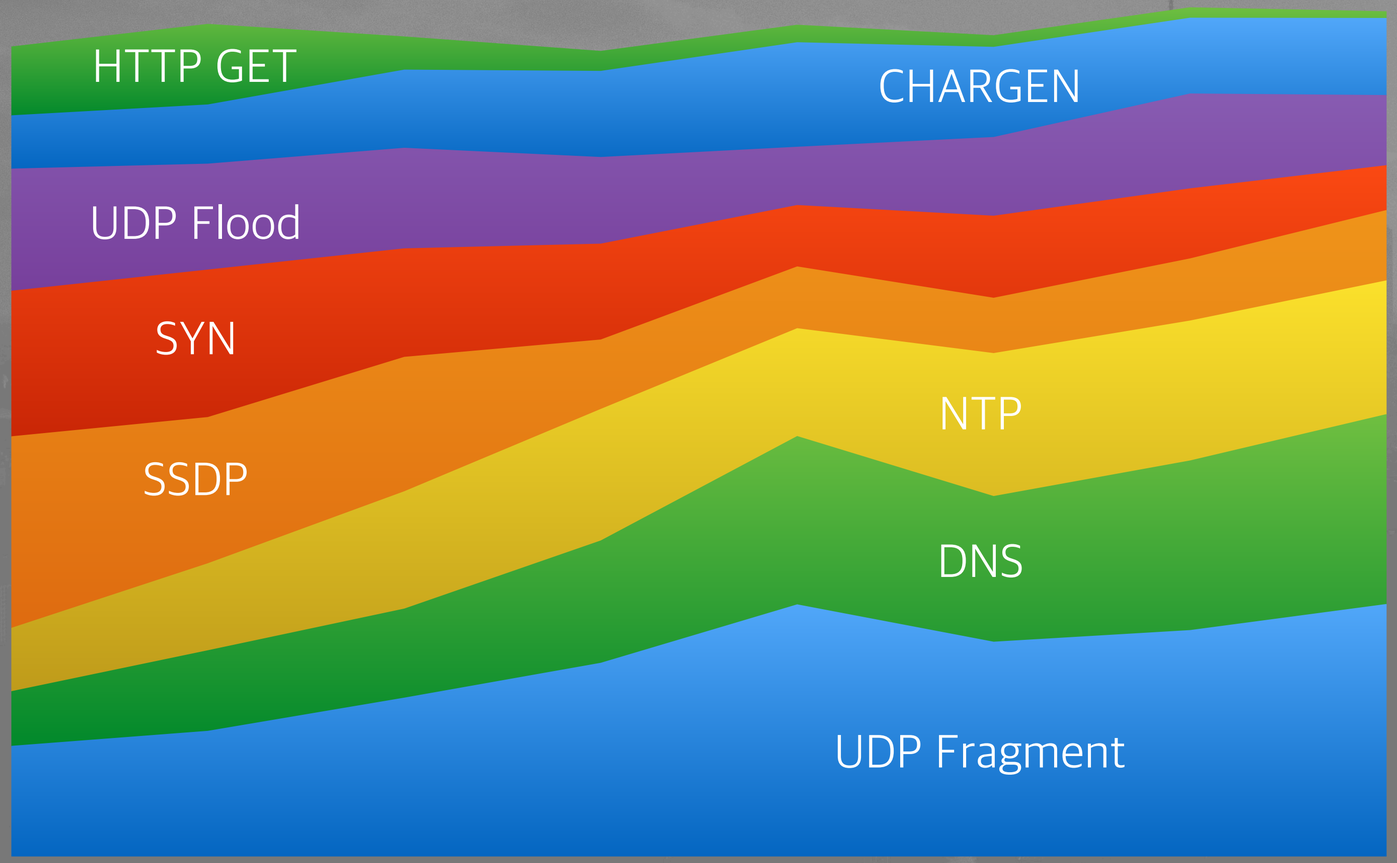
→ Exploit — Adobe Flash, Java, MS IE

Adware → Distribution

今日:49 昨日:1953 今日回访:1003 今日回率:1.1% 总数:91477 韩国:89027

223.38.61.194	02-0A-	Windows32	韩国	2016-11-11 12:11:58	2016-11-11 12:11:58
118.39.97.116	C0-F8-	Windows32	韩国	2016-11-11 12:11:02	2016-11-11 12:11:02
1.222.54.162	00-01-	Windows32	韩国	2016-11-11 12:01:35	2016-11-11 12:01:35
211.204.26.247	F0-79-	Windows32	韩国	2016-11-11 11:33:33	2016-11-11 11:33:33
222.110.162.59	00-1D-	Windows32	韩国	2016-11-11 11:33:30	2016-11-11 11:33:30
202.56.255.50	00-50-	Windows32	印度	2016-11-11 11:33:19	2016-11-11 11:33:19
180.81.19.65	B8-AE-	Windows32	韩国	2016-11-11 11:33:00	2016-11-11 11:33:00
118.131.21.171	D0-50-	Windows32	韩国	2016-11-11 11:28:21	2016-11-11 11:28:21
144.202.228.214	7E-F3-	Windows32	美国	2016-11-11 10:38:19	2016-11-11 10:38:19
59.4.45.253	00-13-	Windows32	韩国	2016-11-11 10:32:11	2016-11-11 10:32:11
202.56.255.50	00-50-	Windows32	印度	2016-11-11 10:26:44	2016-11-11 10:26:44
202.56.255.50	00-50-	Windows32	印度	2016-11-11 10:26:43	2016-11-11 10:26:43
211.52.91.22	00-0C-	Windows32	韩国	2016-11-11 10:23:09	2016-11-11 10:23:09
14.55.137.147	80-FA-	Windows32	韩国	2016-11-11 09:52:29	2016-11-11 09:52:29
118.32.71.1	B8-97-	Windows32	韩国	2016-11-11 09:50:25	2016-11-11 09:50:25
64.139.47.106	08-00-	Windows32	美国	2016-11-11 09:43:24	2016-11-11 09:43:24

일상화된 DDoS 공격 및 협박



Lizard Squad

DD4BC

Kadyrovtsy

Stealth Ravens

Armada Collective

Mirai

✳ 출처: Akamai의 State of the Internet 보고서 재구성

치명적인 필수 SW 취약점

유포지

1. 취약점 발견 및 공격코드 개발
2. 악성코드 유포 환경설정

3. 악성코드 유포지 접속
4. 악성코드 감염: ActiveX 취약점 공격

공격자

5. 감염기록 전송
6. 추가 악성코드 전송
7. 원격조작(RAT)

8. 내부망 전파: 에이전트 SW 취약점 공격
9. 정보유출 및 조작 등 최종 목표 공격

C2서버

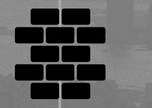
네트워크 분리 환경 맹목적 신뢰

인터넷서버

인터넷 메일
업무PC 전달

업무서버

망구분 없이
에이전트 관리



인터넷PC에서
업무서버 접속

업무PC에서
인터넷서버 접속

망연계시스템

악성파일 필터링 실패

인터넷PC

가상환경 탈출

업무PC

업무PC에 휴대폰 연결
업무PC에 USB 연결

업무PC에서 무선인터넷 접속

금융회사 타겟 공격 고도화

SWIFT

에콰도르 Banco del Austro

베트남 Tien phong Bank

방글라데시 Central Bank

우크라이나 10여개 은행

인도 Union Bank

터키 Akbank

인도 국책은행

2015 — 2016 — 2017

카스퍼스키랩 Carbanak 그룹 경고

시만텍 Odinaff 그룹 경고

시만텍 등 Lazarus 그룹 경고

ATM

인도 Yes Bank

대만 First Commercial Bank

태국 Government Savings Bank

인도 Corporation Bank

청호 이지캐쉬

카스퍼스키랩 Carbanak 그룹 경고

카스퍼스키랩 Metel 그룹 경고

카스퍼스키랩 ATM 공급업체경고

Group-IB Cobalt 그룹 경고

FBI ATM 위협 경고

ESET Buhtrap 그룹 경고

파이어아이 Suceful 발견

Proofpoint GreenDispenser 발견

파이어아이 ATMRipper 발견

트렌드마이크로 Alice 발견

파이어아이 Ploutus.D 발견

카스퍼스키랩 ATMitch 발견

치밀하고 은밀한 사이버테러

1. 공격대상 이메일 수집
2. 악성코드 개발 및 이메일 작성
3. 이메일 발송

스피어피싱

4. 이메일 열람 및 첨부파일 실행
5. 악성코드 감염

공격자

C2서버

6. 감염기록 전송
7. 추가 악성코드 전송
8. 원격조작(RAT)

9. 내부망 전파
10. 사이버테러

1. 공격대상 정보수집
2. 취약점 발견 및 공격코드 개발
3. 악성코드 유포 환경설정

워터링홀

4. 악성코드 유포지 접속
5. 악성코드 감염