
CLOUDSEC2017
LEVEL UP

CLOUDSEC2017

LEVEL UP

네이버 클라우드 플랫폼에 구현된 보안 기술

장노륜 부장
네이버 비즈니스 플랫폼
ron.jang@navercorp.com

퍼블릭 클라우드의 보안 위협들

- 취약한 계정과 비밀번호
- 클라우드 서비스를 이용한 사이버 공격
- 설정 실수로 인한 중요 정보 노출

클라우드 보안은 공동의 책임

CLOUDSEC2017

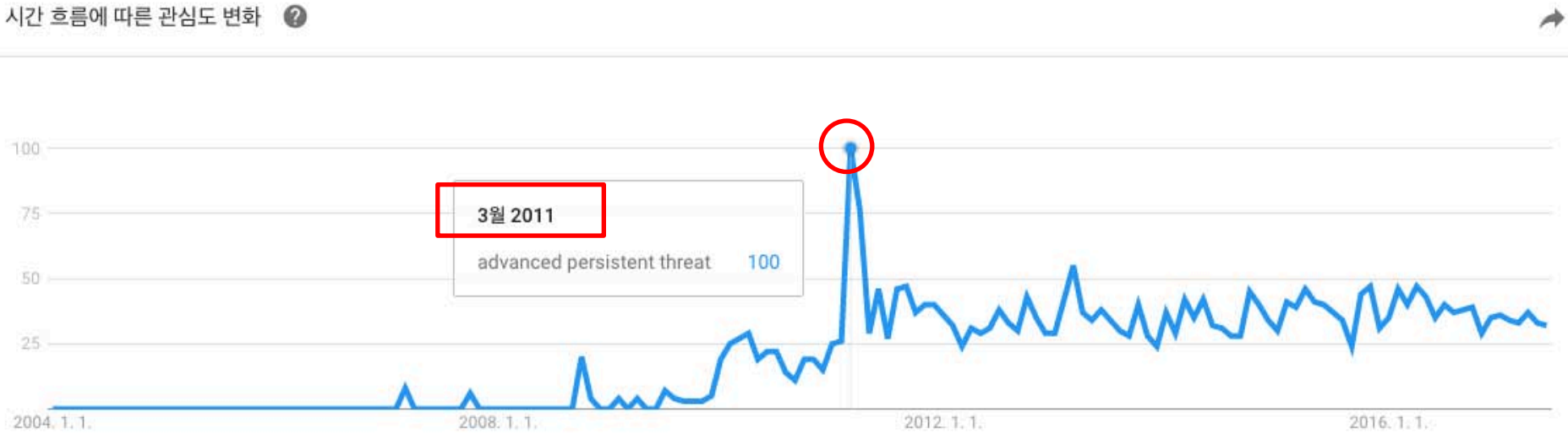
가트너 2016년 4월

여러가지 보안 위협 중에서...

대응하기 쉽지 않은 APT

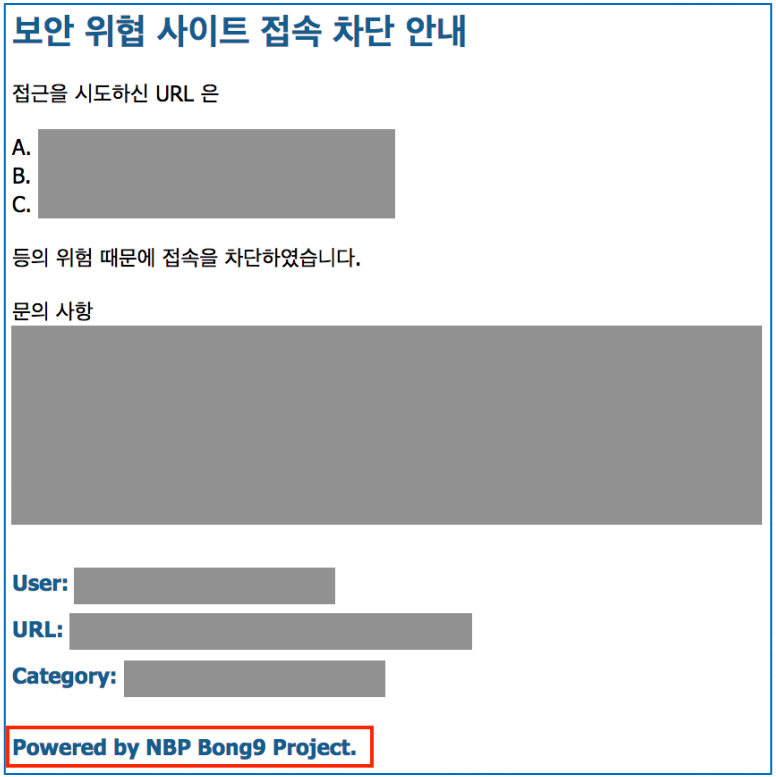
CLOUDSEC2017

구글 검색 트랜드: advanced persistent threat, 2004년 이후



네이버 클라우드 플랫폼의 대응

Bong9 프로젝트



유수의 글로벌 기업도 비슷한...

유수의 글로벌 기업도 비슷한...

CLOUDSEC2017

Laika BOSS: Scalable File-Centric Malware Analysis and Intrusion Detection System

Matthew Arnao Charles Smutz Adam Zollman Andrew Richardson Eric Hutchins
Lockheed Martin Computer Incident Response Team

http://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/LaikaBOSS%20Whitepaper.pdf

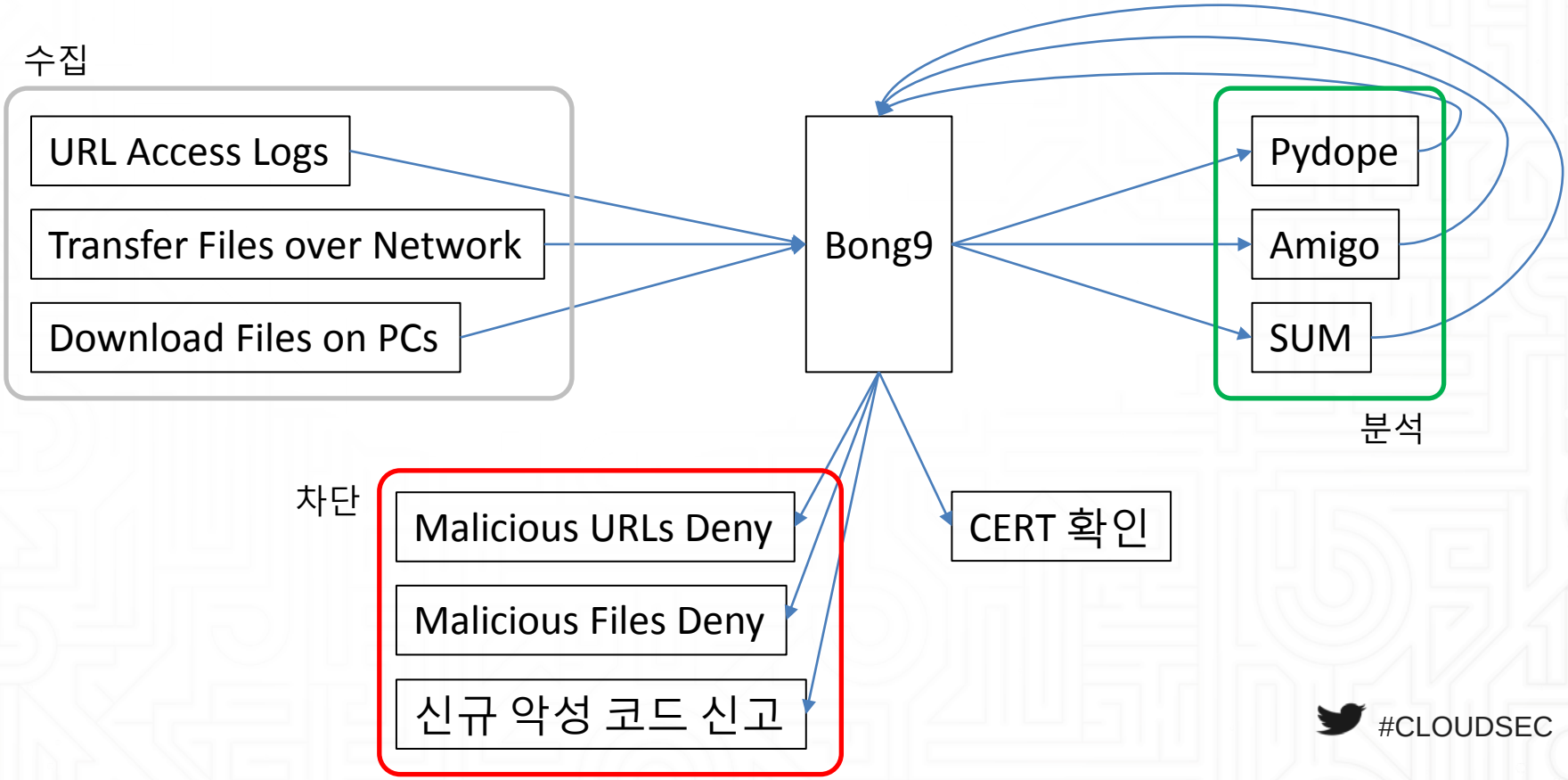
1 Introduction

Threat actors intent on gaining access to a network often choose file-based exploits because they can be easily and reliably delivered to intended targets. These actors often use the most common, critical protocols such as email, web, and social media as delivery vectors, and target widespread and critical applications. Wholesale blocks on those protocols or file types would cripple legitimate business activity and is generally not an option for network defenders. To defeat intrusions, defenders must be able to detect malicious files wherever they exist - either transiting a network or stored on disk.

There are a multitude of malware analysis tools and reverse engineering resources available to analyze malicious code, but these work best in one-off, isolated conditions and are not capable of real-time processing. As a result, most security teams have to manage a disparate set of analysis tools with different capabilities. This inefficient solution presents a frustration for many defenders: being able to detect malware in a lab, but not able to scale that approach to successfully detect malware and defend an enterprise.

Most intrusion detection systems are focused primarily on the medium they monitor (e.g. network-based, host-based). The medium-centric approach normalizes all collection, logging, and alerting around the medium. File features - with all their different formats, data structures, and metadata - are left as

Bong9


수집
URL Access Logs
Transfer Files over Network
Download Files on PCs
Bong9
Pydope
Amigo
SUM
분석
차단
Malicious URLs Deny
Malicious Files Deny
신규 악성 코드 신고
CERT 확인

URL 분석 @Bong9

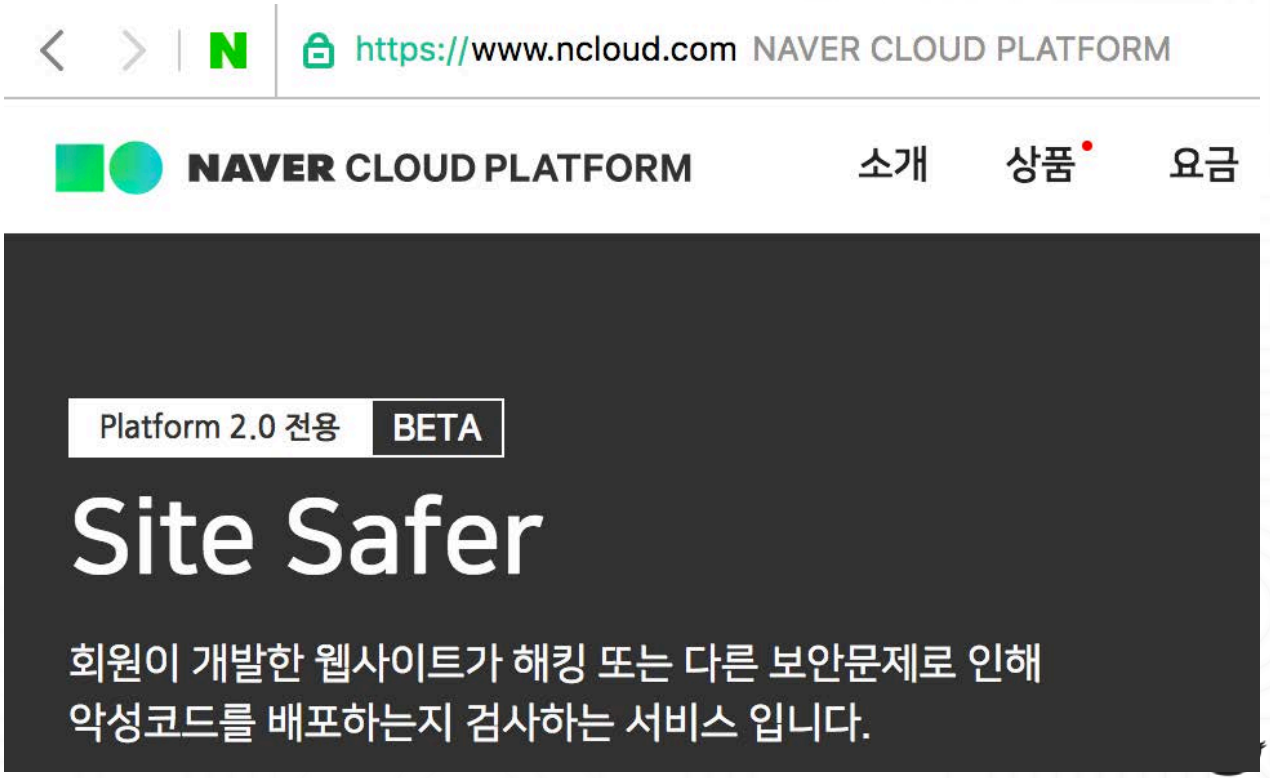
- Pydope: 정적 분석기
- Amigo: 동적 분석기

File 분석 @Bong9

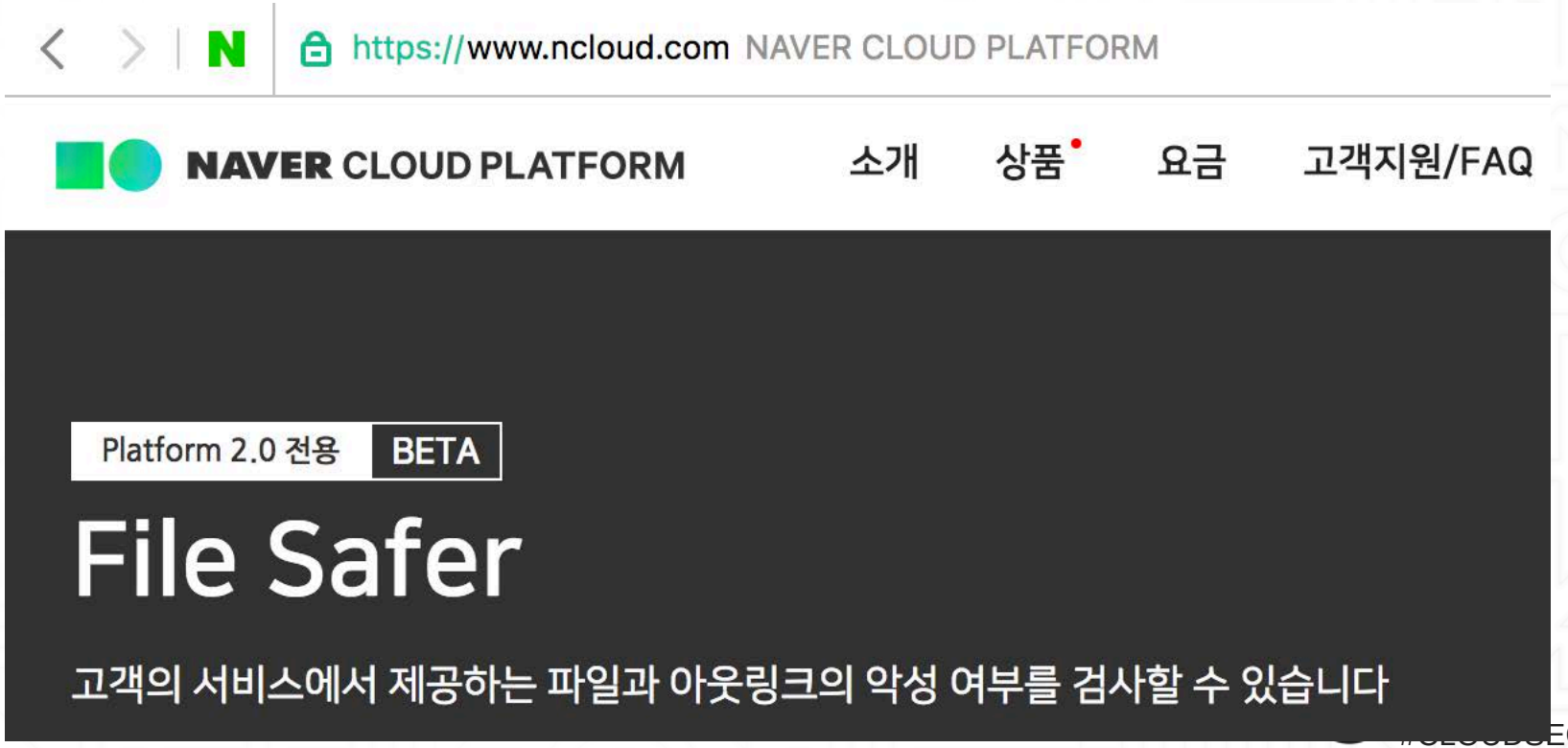
- SUM
  - File → 클린셋DB

    → 정적 분석기 → 멀티 스캔 → 동적 분석기

네이버 클라우드 플랫폼에서도...



네이버 클라우드 플랫폼에서도...



네이버 클라우드 플랫폼과 함께!

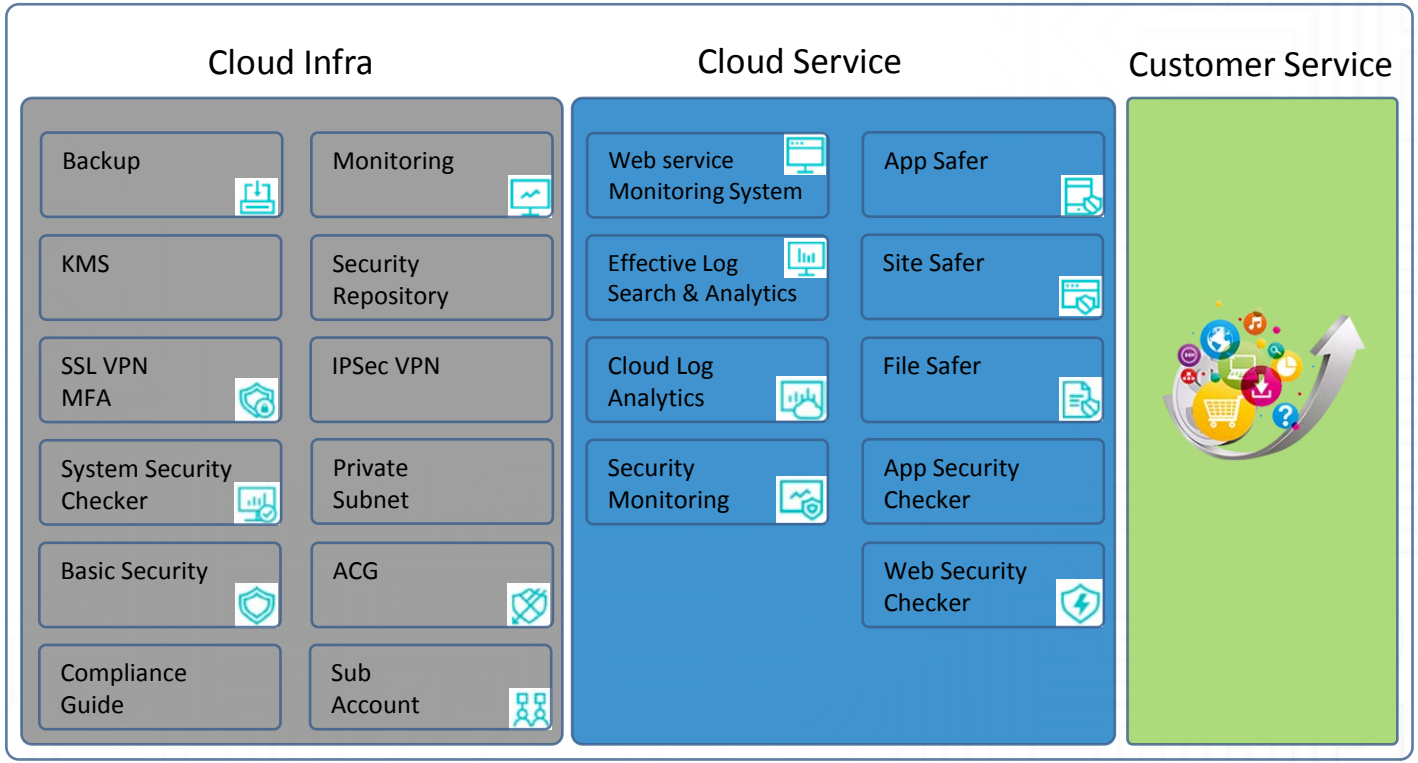
CLOUDSEC2017

Backup	Monitoring	Web service Monitoring System	App Safer
KMS	Security Repository	Effective Log Search & Analytics	Site Safer
SSL VPN MFA	IPSec VPN	Cloud Log Analytics	File Safer
System Security Checker	Private Subnet	Security Monitoring	App Security Checker
Basic Security	ACG		Web Security Checker
Compliance Guide	Sub Account		

#CLOUDSEC

네이버 클라우드 플랫폼과 함께!

CLOUDSEC2017



#CLOUDSEC

CLOUDSEC2017

LEVEL UP

THANK YOU

장노륜 부장
네이버 비즈니스 플랫폼
ron.jang@navercorp.com