CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★

SC MAGAZINE Best SME Solution

Hot Company Web Application Security CDM

TU-Automotive AWARDS

Penta SECURITY
enterprise · iot · blockchain

Web Application Threat Trend Report

Trends for the 2018

펜타시큐리티시스템㈜

Penta SECURITY

목차

I. 개요

1. 보고서의 목적

II. 요약

1. 룰별 웹 공격 동향
2. 주요 공격자 동향
3. 산업별 웹 공격 동향
4. 국가별 웹 공격 동향
5. 시간대별 웹 공격 동향

III. 2018년 웹 공격 동향 분석

1. 룰별 웹 공격 동향
2. 주요 공격자 동향
3. Black IP 수 증감 추이
4. 산업별 웹 공격 동향
5. 국가별 웹 공격 동향
6. 시간대별 웹 공격 동향

IV. Appendix

1. 분석 방법
    1) 데이터 수집 방법, 대상, 기간
    2) 이전 보고서와의 차이점
    3) 기술 용어 정의
    4) Black IP List

I. 개요

1. 보고서의 목적

본 'Web Application Threat Trend Report(WATT Report)'는 전 세계에 설치되어 있는 아시아-태평양 웹방화벽 시장점유율 1위[1] 웹 방화벽 'WAPPLES'의 탐지 데이터를 기반으로 작성되었습니다. 본 보고서는 고객들이 수집 동의한 데이터만을 사용하며, 수집된 데이터를 자사의 'Intelligent Customer Support(ICS)' 시스템으로 분석한 정보를 기반으로 작성한 웹 공격 동향 분석 보고서입니다.

본 보고서는 최신 공격 동향 분석을 통해 웹 공격 패턴을 파악하고 예측한 결과를 향후 WAPPLES 운영에 반영하는 것이 하나의 목적입니다.

특히 2018년 WATT Report는 펜타시큐리티에서 연구 개발한 머신러닝 기술을 적용하여 아시아-태평양 웹방화벽 시장점유율 1위 바탕의 웹 공격 데이터 수집과 고도화된 학습 방법, 그리고 이를 적용할 수 있는 기술력을 바탕으로 작성되었습니다. 이를 통해 향후 웹 공격 예측에 대한 정확도를 향상시켰습니다.

위 보고서는 WAPPLES 고객들과 파트너, 기업 및 기관의 보안 관리자, 연구기관 등 웹 보안 동향에 관심 있는 모든 독자에게 웹 공격 동향에 대한 정보 제공을 목적으로 작성 및 배포됩니다.

독자는 본 보고서를 통해 WAPPLES 탐지 룰을 기반으로 주요 웹 공격에 관한 각종 통계 정보, 주요 공격자의 공격 유형과 Black IP에 대한 추이 정보, 주요 웹 공격 출발 국가 통계 정보, 산업별·시간대별 웹 공격 정보 등을 제공받을 수 있습니다.

1) Industry Quotient, Frost & Sullivan, 2015.

II. 요약

본 보고서는 WAPPLES의 탐지 룰 중 가장 중요하다고 판단되는 5가지 룰을 Top5로 선정하여 공격 데이터들을 분석하였으며, 해당 공격의 동향과 주요 공격자의 공격 및 Black IP 동향, 산업별 공격 유형, 공격 출발 국가, 시간대별 공격의 관점에서 분석하였습니다.

1. 룰별 웹 공격 동향

WAPPLES에서 탐지하는 Top5 웹 공격은 Extension Filtering(32.71%), Error Handling(17.22%), Cross Site Scripting(6.99%), Request header Filtering(6.27%), Stealth Commanding(5.77%) 순서로 선정되었습니다. 2017년과 비교하여 새로운 공격이 등장하였기 때문에 특별한 주의가 필요합니다. 또한 좀 더 살펴보면 Cross Site Scripting 공격과 Stealth Commanding 공격이 2017년에 이어 등장하였습니다. 따라서 다양한 웹 공격과 반복 선정된 공격들에 대한 대비책을 마련함과 동시에 Top5 웹 공격에 대해 지속적인 관심을 가지고 보안 대책을 마련해야 합니다.

2. 주요 공격자 동향

2018년 1월 1일부터 12월 31일까지 웹 공격 횟수 100만 건 이상, 웹 공격 위협 정도 등의 기준에 따라 점수를 부여하여 80점 이상인 공격자를 '주요 공격자(Black IP)'로 선정하였습니다. Black IP의 주요 웹 공격 동향은 전체 웹 공격 동향과 비율 차이가 있습니다. Request Header Filtering(69.81%), SQL Injection(13.21%), Stealth Commanding(9.36%), Cross Site Scripting(3.70%), Error Handling(2.11%)의 비율을 보였습니다. 이러한 내용은 룰별 웹 공격 동향에서 비율이 낮거나 Top5 웹 공격에 속하지 않았더라도 큰 피해로 이루어질 수 있으므로 안심할 수 없다는 것을 의미합니다.

또한 Black IP 증감 추이는 최대 1861건, 최소 87건으로 연 평균 942건으로 나타났습니다. 특히 1월, 5월, 6월은 평균보다 월등히 많은 공격 횟수가 발생하였기 때문에 지속적 모니터링을 통해 Black IP에 대한 주의를 기울여야 합니다.

3. 산업별 웹 공격 동향

WAPPLES을 사용하는 산업 분야를 기준으로 정탐된 웹 공격을 분류하여 나타냈습니다. 산업구분에 따라 크게 교육, 방송 통신, 유통 및 제조, 협회 및 단체, 공공, 엔터테인먼트로 구분하였습니다. 전체 산업별 공격 동향을 살펴보면 사내 직원 및 많은 고객 정보를 보유하고 있는 산업 위주로 공격들이 발생했으며, 주요 공격으로는 Cross Site Scripting, Include Injection, File Upload, SQL Injection, Stealth Commanding, Directory Traversal이 발생하였습니다.

4. 국가별 웹 공격 동향

한국에서 출발한 공격의 룰별 비율은 Extension Filtering(44.90%), Request Header Filtering(24.06%), Error Handling(19.31%), Cross Site Scripting(8.20%), Stealth Commanding(3.53%) 순서로 나타났습니다. 또한 한국을 포함한 대륙별 비율을 살펴보면 웹 공격에 대한 탐지수를 기준으로 아시아, 아메리카, 유럽, 오세아니아, 아프리카 순서로 웹 공격이 발생하였습니다. 특히 아시아, 유럽, 아메리카 대륙에서 Extension Filtering 공격이 가장 많이 발생하였습니다.

또한 웹 공격 룰에 대한 공격 출발 상위 국가 비율은 한국, 미국, 중국, 말레이시아, 러시아, 일본, 독일 순으로 나타났으며, 일반적으로 웹 활동이 활발한 국가들이 출발 공격수 상위 국가에 위치하고 있습니다.

5. 시간대별 웹 공격 동향

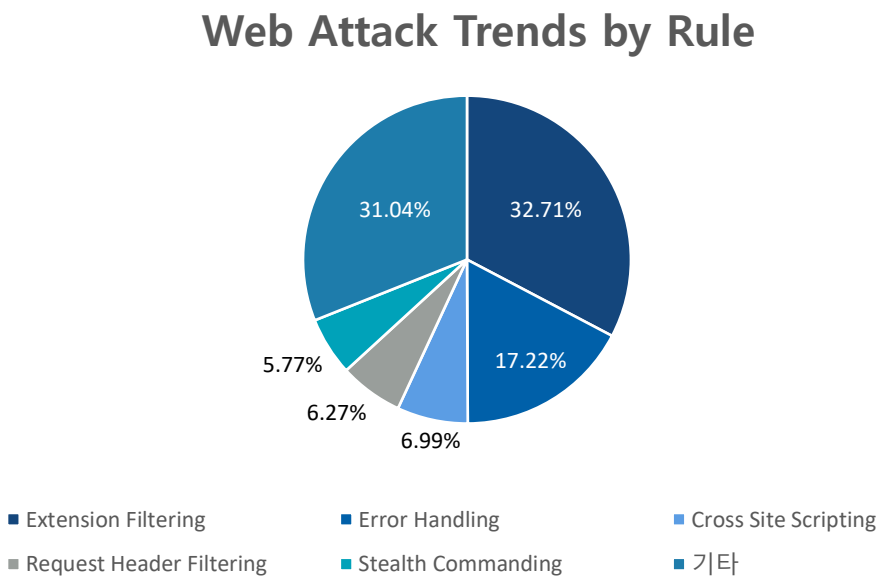
1일 24시간 기준으로 웹 공격이 탐지된 횟수를 표현합니다. 데이터를 분석해 보면 모든 시간대에서 60만 건이 넘는 웹 공격이 탐지되었습니다. 특히 10시 30분 ~ 12시 30분, 15시 ~ 17시에서 많은 수의 웹 공격이 탐지되었는데, 이는 보안 담당자들의 교대시간(식사 시간, 당직 교대 시간 등)과 업무가 과중된 시간 그리고 시스템 점검을 위해 보안 기능을 일시적으로 꺼 두는 틈을 노린 공격으로 추정됩니다. 따라서 위와 같은 시간대에 특히 주의를 기울여야 합니다.

III. 2018년 웹 공격 동향 분석

1. 룰별 웹 공격 동향

룰별 웹 공격 동향을 통해 한 해 동안 어떤 공격이 많았는지를 볼 수 있습니다. 또한 이를 바탕으로 기본적 웹 공격 대응 가이드라인을 수립함으로써 웹 공격에 대한 예방 및 대응책을 마련할 수 있습니다.

아래 그래프는 2018년 WAPPLES 탐지를 통해 정탐된 웹 공격들을 분석한 것입니다.



2018년 1월 1일부터 2018년 12월 31일까지 Extension Filtering(32.71%) 공격이 가장 많았으며, Error Handling(17.22%), Cross Site Scripting(6.99%), Request header Filtering(6.27%), Stealth Commanding(5.77%) 순으로 탐지되었습니다.

Extension Filtering 공격은 2015년에 가장 빈도가 높은 웹 공격으로서, 올해 다시 첫 번째로 등장하였습니다. Extension Filtering은 웹 사이트에서 일반적으로 사용하는 확장자 형식이 아닌 취약성이 존재하는 설정파일(예, dll, conf, ini 등)에 대한 접속 시도를 의미하며, 일반 사용자에게 접속이 허용될 경우 웹 서버의 동작과 웹 서비스에 직접적으로 영향을 미칠 수 있는 매우 위험한 공격입니다.

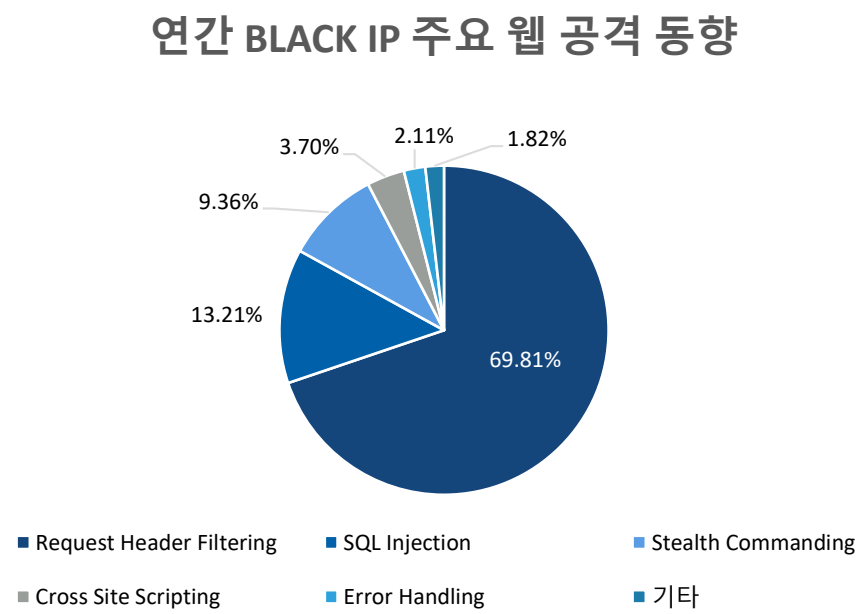
Error Handling 공격은 2012년에 세 번째로(12.2%) 많았던 공격입니다. 웹 애플리케이션 사용 시 발생할 수 있는 각종 에러의 부적절한 처리로 인해 악의적인 사용자들에게 해당 사이트가 가진 잠재적 취약점에 대한 힌트를 제공하는 등 다양한 보안 문제를 야기할 수 있습니다. 추가로 웹 서버, WAS, DBMS 서버 등에 대한 에러 메시지를 관리하지 않음으로써 정보 유출을 야기할 수 있습니다.

Cross Site Scripting(XSS) 공격은 2017년에 네 번째로(3.99%) 많았던 공격입니다. XSS 공격은 웹 애플리케이션 서버 뿐만 아니라 이를 사용하는 사용자까지 공격하여 시스템 관리자 권한과 사용자 개인 정보까지 한 번에 탈취하려는 시도 때문에 상승한 것으로 추정됩니다. XSS 공격을 허용할 시 쿠키/세션 ID 정보 탈취, 시스템 관리자 권한 탈취, 악성 코드 다운로드 등의 1차 피해를 받게 되고 이로 인해 개인정보, 국가/사내 기밀정보 유출 등의 심각한 2차 피해가 발생할 수 있습니다.

나머지 Stealth Commanding 등의 공격들도 수법이 많이 알려져 있고 큰 피해를 일으킬 수 있는 공격들이므로 관심을 가지고 보안 대책을 수립해야 합니다.

III. 2018년 웹 공격 동향 분석

2. 주요 공격자 동향



위 표는 2018년 1월 1일부터 12월 31일까지 웹 공격 횟수가 100만 건 이상, 웹 공격 위협 정도 기준에 따라 점수를 부여하여 80점 이상인 공격자를 주요 공격자(Black IP)로 선정하고, 이들의 웹 공격 동향을 분석한 결과입니다. 그러한 악의적 공격자의 행동은 실제 피해를 발생시킬 가능성이 높기 때문에 주요 공격자(Black IP)를 선정하여 그들의 웹 공격 동향을 살펴보는 것은 중요합니다. 따라서 주요 공격자(Black IP)의 웹 공격 동향을 주의 깊게 살펴볼 필요가 있습니다.

2018년도 웹 공격 동향 분석에 기반하여 주요 공격자(Black IP)가 사용한 웹 공격은 Request Header Filtering(69.81%), SQL Injection(13.21%), Stealth Commanding(9.36%), Cross Site Scripting(3.70%), Error Handling(2.11%) 순입니다.

그래프에서 첫 번째를 차지한 Request Header Filtering 공격은 웹 브라우저에서 보내는 HTTP Request 요청문을 이용한 공격입니다. 정상적인 HTTP Request 요청문과 달리 해커가 요청문 중 Header에 필수 요소를 빼거나, 다른 요소를 기입하여 비정상적인 혹은 해커의 목적이 담긴 HTTP Request를 전송하는 공격입니다. 이러한 공격은 웹서버의 정보가 변조되거나 제한적이지만 웹 서버가 피해를 입을 수 있는 공격 기법으로서 제 2의 피해를 야기할 수 있습니다.

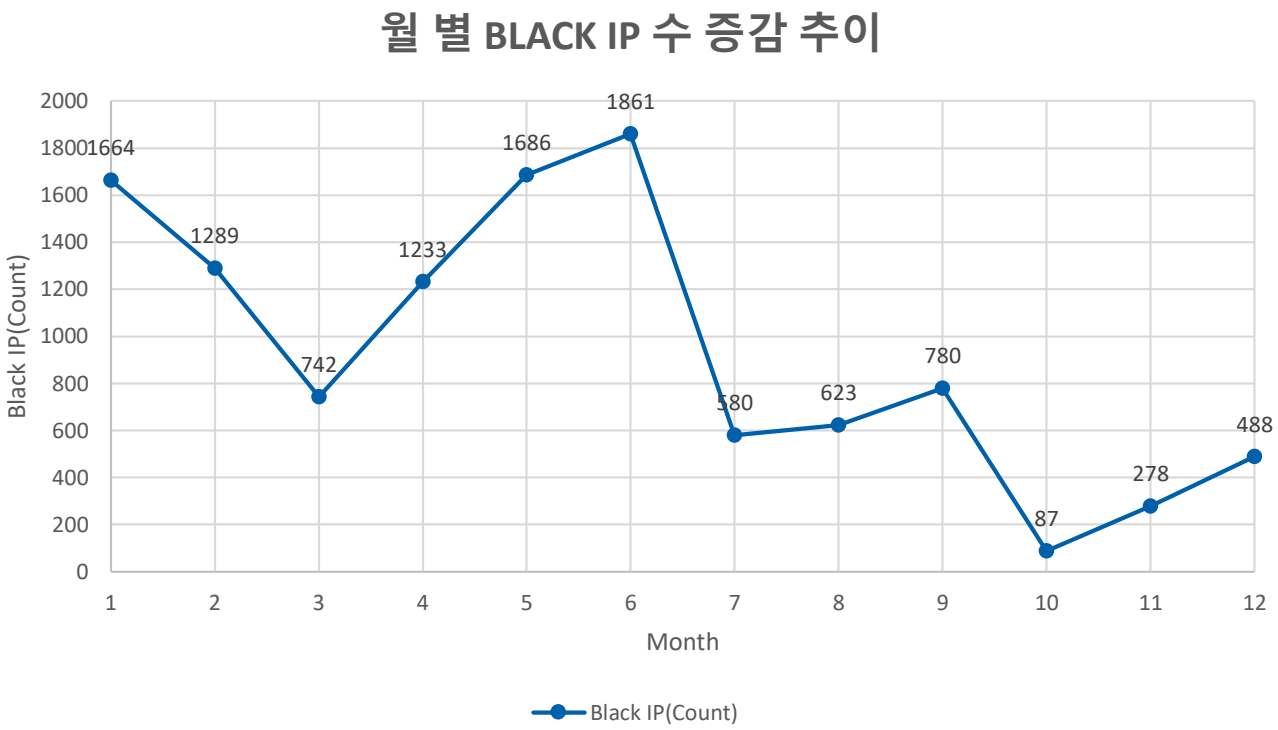
다음으로 큰 비중을 차지하는 SQL Injection 공격은 Injection의 한 기법으로서, 허용되지 않거나 업무와 무관한 SQL문을 실행함으로써 데이터베이스를 공격하는 수법입니다. 가장 흔한 공격이면서도 대량의 정보 유출이 발생할 수 있는 공격 기법이므로 많은 주의가 필요합니다. 이미 다양한 SQL Injection 공격 방법이 알려져 있는 만큼, 상시 SQL Injection 공격에 대한 대비가 필요합니다.

마지막으로 세 번째 큰 비중을 차지하는 Stealth Commanding 공격 기법은 웹 애플리케이션이 HTTP 요청을 받아 해당 정보를 외부로 전달할 때 주로 일어납니다. 공격자가 해당 정보에 악의적 명령어를 정보의 일부로서 삽입하면, 웹 애플리케이션은 이 정보를 그대로 외부 프로그램에 전달하여 실행됩니다. 공격자는 이러한 취약점을 이용하여 트로이 목마 바이러스를 심거나 악성 코드를 실행할 수 있습니다. 이로 인하여 자료 삭제, 정보 탈취 등 사이버 테러까지 이어질 수 있는 위험한 공격입니다.

위 내용들의 공통점은 취약점을 이용해 회사 및 개인의 정보를 탈취하거나 서버를 장악할 목적으로 웹 공격을 한다는 사실입니다. 이렇게 취약점을 이용하여 정보유출을 목적으로 한 웹 공격에 대해 예방하고 사고 발생 시 빠르게 대응할 수 있는 매뉴얼이 필요합니다.

III. 2018년 웹 공격 동향 분석

3. Black IP 수 증감 추이



위 그래프는 웹 공격으로 큰 피해를 발생시키는 주요 공격자(Black IP) 수에 대한 증감 추이를 나타냅니다. 주요 공격자(Black IP)의 증감 추이를 살펴보는 이유는 주요 공격자(Black IP)의 수가 증가함에 따라 웹 공격 빈도 또한 증가할 수 있기 때문입니다. 주요 공격자(Black IP)의 수가 감소하거나 또는 많지 않다고 해서 웹 공격 빈도가 감소하는 것은 아닙니다. 한 명의 해커가 여러 개의 IP를 사용할 수 있고, 하나의 주요 공격자(Black IP)만으로도 큰 피해가 발생할 수 있기 때문입니다.

주요 공격자(Black IP)를 선정하는 기준에 따라 증감 추이가 상이할 수 있으므로 100% 객관적인 데이터라고 하기엔 무리가 있습니다. 하지만 주요 공격자(Black IP)의 증감 추이와 2018년도의 특정 사건과의 연관성 등을 연계해 추정함으로써 공격자 패턴을 파악하고, 향후 유사한 패턴 및 공격이 예상되는 시기에 웹 공격에 대한 보안을 한 층 더 강화하는 일에 도움이 될 것입니다.

2018년도 Black IP 증감 추이는 최대 1861건, 최소 87건, 평균 942건으로 나타났으며, 관심있게 지켜봐야 할 부분은 2017년 대비 월별 1000건이 넘는 Black IP가 발생하였다는 점입니다. 특히 1월, 5월, 6월은 Black IP 발생 건수가 1000건을 넘는 달 중 상위에 해당합니다. 2018년 한국에서 일어난 사건과 연계해 보면 [1]통일부 해킹 및 사이버 공격 시도 탐지 현황에 근거한 2018년 사이버 공격 증가, [2]끊임없이 발생하고 있는 암호화폐 거래소 대상의 해킹 공격 [3]사생활 침해로 이어지는 IP 카메라 해킹 사건 등 다양한 사건들이 맞물려 있다는 것을 알 수 있습니다.

물론 각종 사건과 Black IP간의 연관성을 밝히는 데에는 한계가 있습니다. 하지만 다양한 웹 공격의 위험에 대해 대비하고 점검하며, 공격 발생 시 매뉴얼에 따라 신속 정확하게 대응할 수 있도록 준비하는 것은 중요합니다. 이러한 준비는 언제 발생할지 모르는 사회적 이슈와 정치적 사건 그리고 이와 연관될 수 있는 웹 공격에 대한 최선의 대응이 될 것입니다.

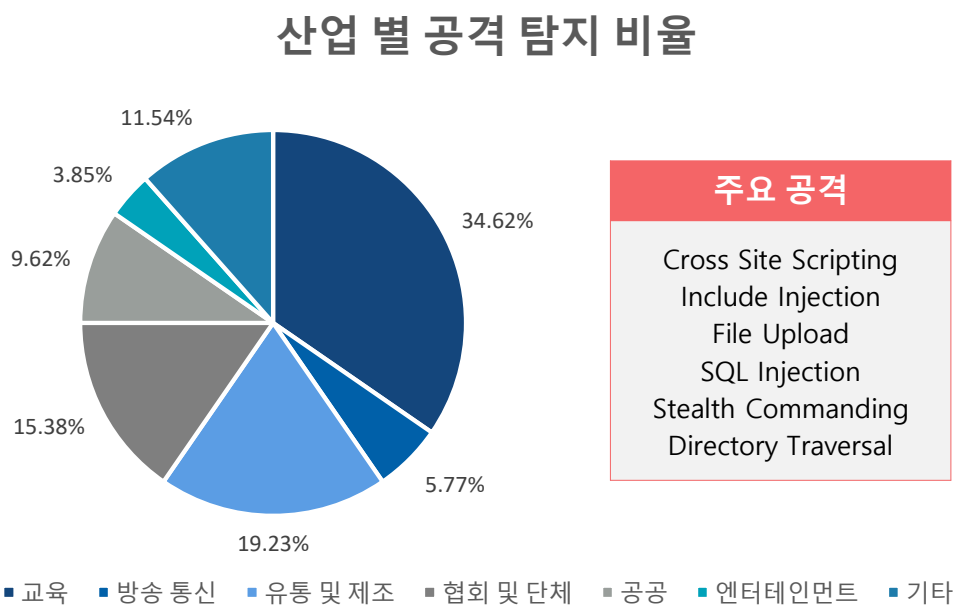
1) "통일부 대상 해킹 공격, 5년간 1800건…매년 증가세", http://m.chosun.com/svc/article.html?sname=news&contid=2019092301651#Redyho, 조선일보, 2019년09월23일.

2) "3년간 암호화폐 거래소 해킹 피해 1139억원", https://www.zdnet.co.kr/view/?no=20180709113121, ZDNet Korea, 2018년07월09일.

3) "IP카메라 해킹, 여성 5000명 은밀한 사생활 털렸다.", https://news.mt.co.kr/mtview.php?no=2018110108340165896, 머니투데이, 2018년11월01일.

III. 2018년 웹 공격 동향 분석

4. 산업별 웹 공격 동향



위 표는 웹 보안 제품 WAPPLES을 사용하는 산업 분야를 기준으로 정탐된 웹 공격을 분류하여 어떤 산업에서 웹 공격이 일어났는지를 나타냅니다. '룰 별 웹 공격 동향' 외에도 다양한 공격들이 탐지되었습니다. 따라서 공격이 탐지된 산업군의 특징을 살펴보고 이에 따른 산업별 대책 마련이 필요합니다.

위 표를 살펴보면 교육, 방송 통신, 유통 및 제조, 협회, 및 단체 공공, 엔터테인먼트 산업에서 다양한 공격이 이루어졌음을 알 수 있습니다. 특히 교육기관에 가장 많은 웹 공격이 발생하였는데 이는 교육 산업이 수 많은 학생과 교직원의 개인정보 및 민감정보를 다루고 있어 해커가 이러한 데이터베이스를 탈취하기 위해 공격한 것으로 해석됩니다. 보안 담당자들은 개인정보를 포함한 다양한 정보의 보호에 각별한 주의를 기울여야 합니다.

다음으로 주의해야 할 산업으로는 유통 및 제조 산업과 협회 및 단체 산업 그리고 기타 산업(문자 서비스 산업 등)을 꼽을 수 있습니다. 다수의 단체 및 개인들이 소속될 수 있는 협회와 다수에게 개인정보(핸드폰 번호)를 활용한 서비스를 활용하는 문자 서비스 산업은 각종 악성 파일 및 보이스피싱 등 2차 피해로 이루어질 수 있습니다. 따라서 보안 담당자들은 이중의 보안 대책을 수립하여 개인정보 보호 및 관리에 관심을 가져야 합니다.

위 언급된 공격이 이루어진 산업군의 사례를 살펴보면, 대학교 뿐만 아니라 해당 부속 기관까지 영향을 준 홈페이지 해킹 사고[1], 대학 서버 해킹에 의한 학생 및 교직원 4만 3천명 개인정보 유출 사고[2] 등 끊임 없는 해킹 사고가 이루어지고 있습니다.

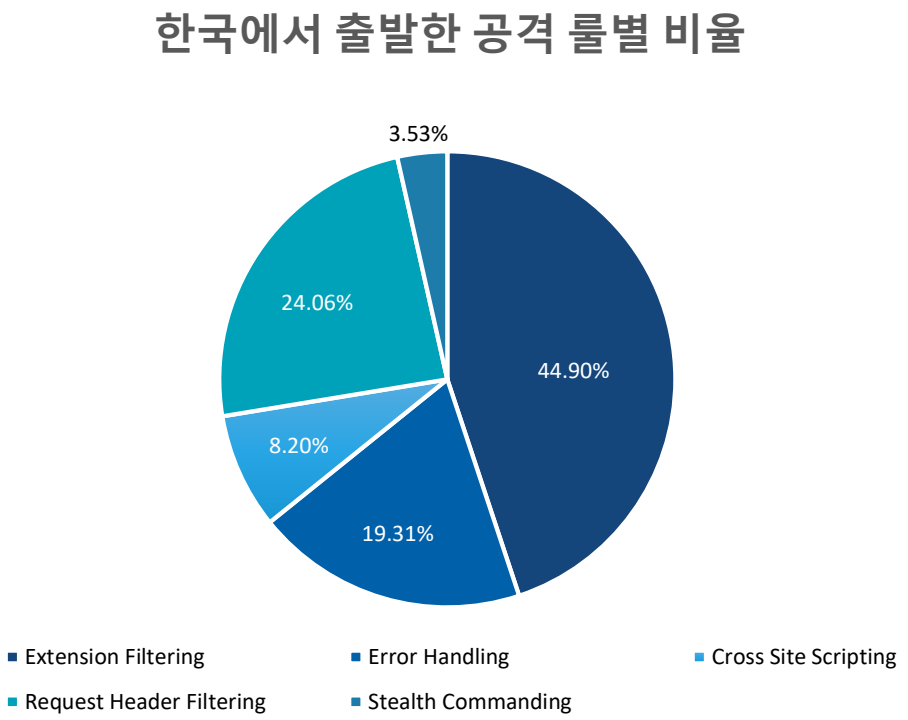
이렇게 산업을 대상으로 발생하는 공격은 개인정보 뿐만 아니라 중요 산업정보의 탈취까지 우려될 수 있기 때문에 항상 웹 공격에 대한 철저한 보안 대책을 마련하고 운영해야 합니다.

1) "3개 대학 9곳 또 디페이스! 계속되는 대학관련 홈피 해킹", https://www.boannews.com/media/view.asp?idx=68516,
- 보안뉴스, 2018년4월17일.

2) "대학 서버 해킹해 학생 및 교직원 4만 3천명 개인정보 유출", https://www.yna.co.kr/view/AKR20180509078400063,
- 연합뉴스, 2018년5월09일.

III. 2018년 웹 공격 동향 분석

5. 국가별 웹 공격 동향

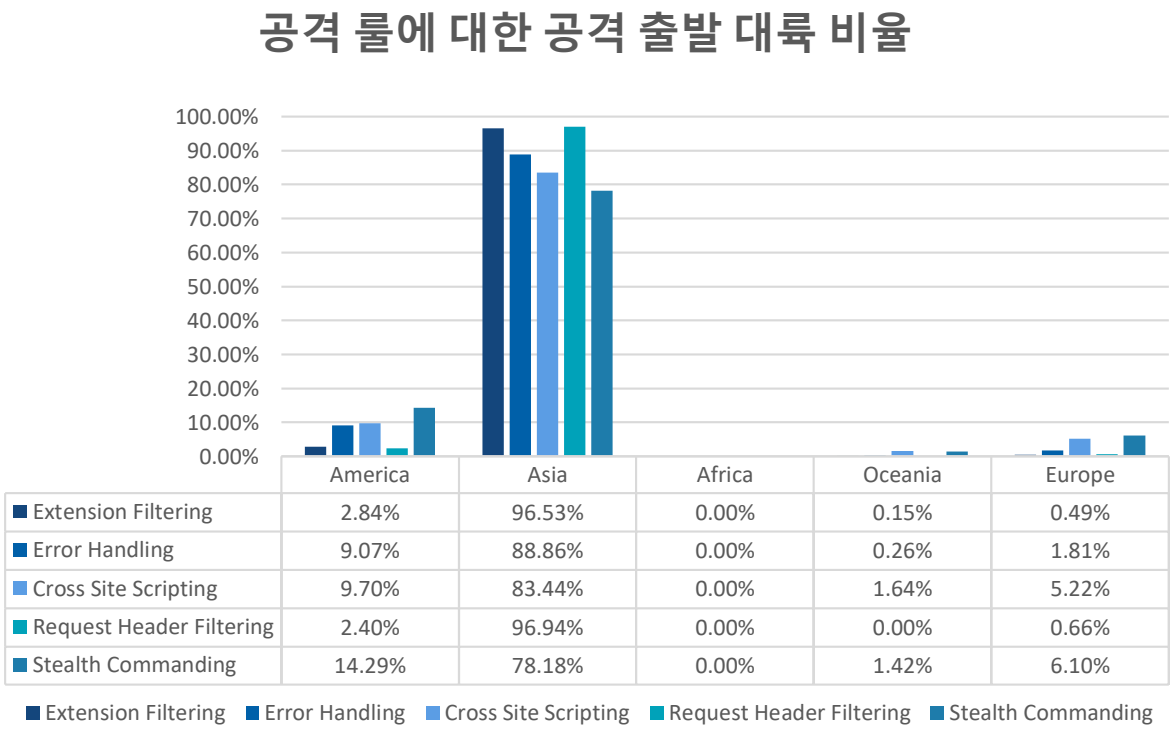


위 그래프는 2018년 국가별 웹 공격 동향에 대한 분석에 앞서, 한국에서 출발한 웹 공격들의 룰별 비율을 보여줍니다. WAPPLES 제품을 사용하는 보안 담당자뿐 아니라 WATT Report를 구독하는 독자 중 한국에서 웹 서비스를 제공하는 경우가 상당수를 차지할 것입니다. 따라서 한국에서 출발하는 공격 룰에 대한 분석을 별도로 분석했습니다.

한국에서 출발한 공격의 룰별 비율은 Extension Filtering(44.90%), Request Header Filtering(24.06%), Error Handling(19.31%), Cross Site Scripting(8.20%), Stealth Commanding(3.53%) 순서로 나타났습니다. 이는 '룰별 웹 공격 비율'의 순위와 대체로 유사한 경향을 보였습니다. 이러한 비율을 바탕으로 한국에서 제공되는 서비스의 보안 담당자 또는 한국을 대상으로 하는 기업 및 기관의 보안담당자는 Extension Filtering(44.90%), Request Header Filtering(24.06%), Error Handling(19.31%)가 전체의 80%를 넘는 만큼 특별한 주의가 요구됩니다. 그 이유는 한국은 가장 활발한 경제활동을 하는 국가이자 해커들이 원하는 개인/중요 정보가 많이 있는 국가 중 한 곳이기 때문입니다. 정보 유출 및 제 2의 공격을 위해 스크립트를 통한 비정상 기능을 수행하거나, 웹서버 정보를 변조하여 비정상적인 행동을 유도하는 등 끊임없는 해커의 공격이 예상되기 때문에 이에 대한 대비가 항상 이루어져야 합니다.

III. 2018년 웹 공격 동향 분석

5. 국가별 웹 공격 동향



	America	Asia	Africa	Oceania	Europe
Extension Filtering	2.84%	96.53%	0.00%	0.15%	0.49%
Error Handling	9.07%	88.86%	0.00%	0.26%	1.81%
Cross Site Scripting	9.70%	83.44%	0.00%	1.64%	5.22%
Request Header Filtering	2.40%	96.94%	0.00%	0.00%	0.66%
Stealth Commanding	14.29%	78.18%	0.00%	1.42%	6.10%

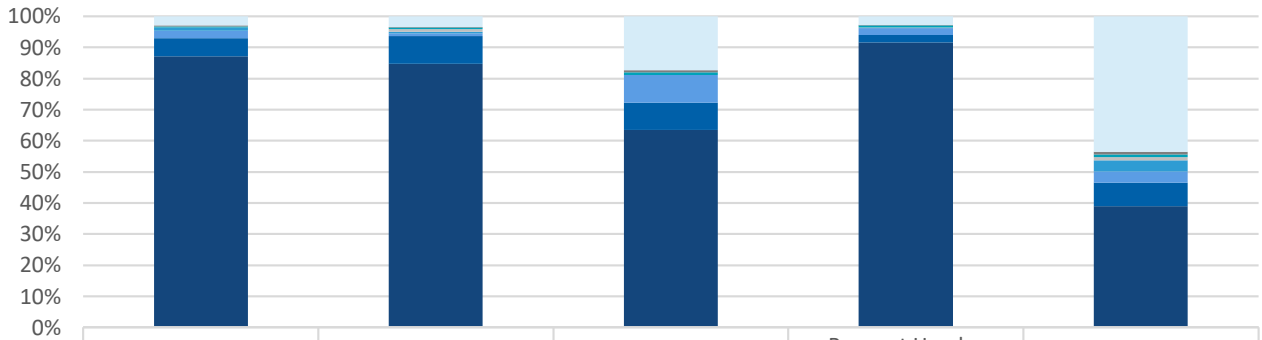
위 그래프는 2018년 탐지 공격들이 출발한 대륙을 기준으로 분류하여 보여줍니다. 그래프를 살펴보면 작년과 동일하게 웹 공격에 대한 탐지수를 기준으로 아시아, 아메리카, 유럽, 아프리카, 오세아니아 순서로 웹 공격이 발생했습니다. 작년대비 차이점은 유럽 대륙으로부터 출발한 비율은 감소하였고, 아시아와 아메리카 대륙에서 많은 웹 공격이 발생했다는 점입니다. 물론 웹 공격의 종류는 달라졌지만, 해커들은 경제활동이 활발하고 대륙간 교류가 많은 국가를 웹 공격 출발지로 이용한 것으로 추정할 수 있습니다.. 따라서 보안관리자는 특히 위 세 대륙으로부터 출발하는 웹 공격에 대비해야 할 것입니다.

또한 대륙별 전체 웹 공격의 출발 구성을 살펴보면 Extension Filtering이 가장 큰 비율을 차지하였으며, 나머지는 Request Header Filtering, Error Handling, Cross Site Scripting, Stealth Commanding순서입니다. 좀 더 세분화하여 관찰하면, 아시아에서는 Extension Filtering, Request Header Filtering이, 아메리카와 유럽에서는 에서는 Stealth Commanding, Cross Site Scripting 공격이 두드러집니다. 이러한 대륙 단위의 공격 동향에 따라 보안대책을 강화해야 합니다. 특히 작년과 달리 새롭게 웹 공격 비중 상위를 차지한 Extension Filtering, Requesting Header Filtering 등의 공격에 대해 특별한 관심을 가져야 합니다.

III. 2018년 웹 공격 동향 분석

5. 국가별 웹 공격 동향

공격 룰에 대한 공격 출발 국가 비율



	Extension Filtering	Error Handling	Cross Site Scripting	Request Header Filtering	Stealth Commanding
Others	2.95%	3.37%	17.37%	2.82%	43.50%
Germany	0.24%	0.29%	0.63%	0.14%	0.83%
Japan	0.33%	0.43%	0.85%	0.66%	0.84%
Russia	0.00%	0.95%	0.00%	0.15%	1.16%
Malaysia	1.15%	0.49%	0.00%	0.00%	3.49%
China	2.33%	0.83%	8.89%	2.26%	3.58%
USA	5.93%	8.86%	8.70%	2.35%	7.56%
Korea	87.06%	84.79%	63.57%	91.62%	39.04%

Korea USA China Malaysia Russia Japan Germany Others

위 그래프는 2018년 탐지 공격들이 출발한 장소들을 대륙으로 구분하고, 공격 출발 비율이 상위 7위 안에 속한 국가들을 나타낸 것입니다. 이를 통해 어떤 국가에서 어떤 웹 공격이 주로 출발했는지에 대한 내용을 살펴보고 해당 국가에서 출발하는 웹 공격에 대해 대비할 수 있습니다.

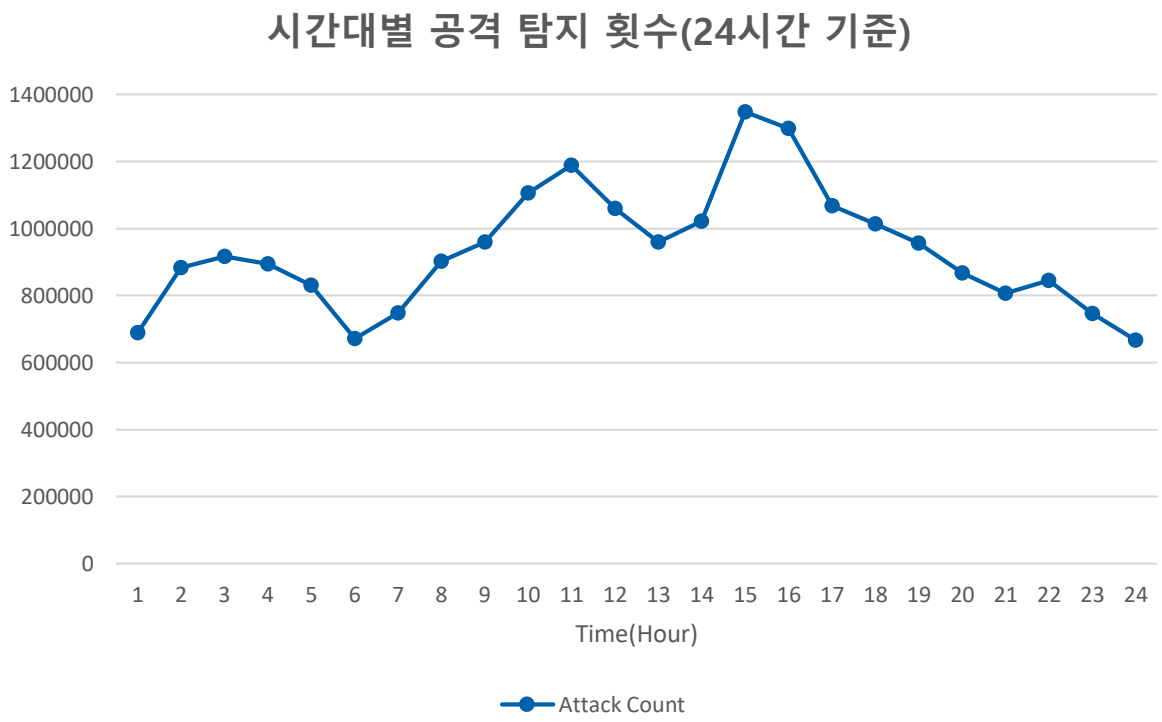
2017 WATT Report와 비교하면 말레이시아와 독일이 새롭게 등장하였습니다. 한국을 포함한 미국, 중국, 러시아, 일본은 2016년과 2017년에 이어 웹 공격 출발 국가 Top7에 들었습니다. 다소 변화는 있지만 '공격 룰에 대한 공격 출발 국가 비율' 상위에 속한 국가들이 지속적인 웹 공격 출발지임을 볼 수 있습니다.

위 그래프를 살펴보면 주요 국가에서 공통적으로 Extension Filtering, Stealth Commanding 공격이 발생하였습니다. 또한 미국, 중국, 러시아 등 강대국이 공격수 상위 국가에 위치하고 있음을 볼 수 있습니다. 따라서 해당 국가들을 대상으로 한 웹 공격 대비를 한층 더 강화할 필요가 있습니다.

Others에 속하는 국가들은 무수히 많습니다. 특히 Stealth Commanding 공격의 40%이상이 Other에 속하는 국가에서 발생하였기 때문에 Top7 국가들 외에도 많은 웹 공격이 발생할 수 있음을 일 수 있습니다. 따라서 앞서 소개해 드린 내용을 바탕으로 주요 국가뿐 아니라 모든 국가에 대해 순차적으로 웹 공격 보안 설정이 필요합니다.

III. 2018년 웹 공격 동향 분석

6. 시간대별 웹 공격 동향



위 그래프는 2018년 탐지된 웹 공격들의 탐지 시간(Local Time)을 기준으로 1시간 간격으로 구분하여 매 시간 웹 공격 비율을 나타낸 것입니다. 이를 바탕으로 주로 어떤 시간대에 웹 공격이 발생하는지 알 수 있습니다.

데이터를 분석해 보면 모든 시간에서 60만 건이 넘는 웹 공격이 탐지되었습니다. 이것은 항상 많은 수의 웹 공격이 발생하며, 이에 대비해야 한다는 것을 의미합니다. 특히 관심을 가져야할 시간은 10시 30분 ~ 12시 30분, 15시 ~ 17시입니다. 각각 점심시간 직전과 저녁시간 직전 시간으로서 업무적으로 집중도가 떨어질 수 있는 시간입니다.

보안을 중요하게 생각하는 기관들은 24시간 모니터링을 실시하고 있을 것입니다. 하지만 업무 집중도가 떨어지는 시간이나 담당자들의 식사시간이나 교대시간, 시스템 점검으로 인해 보안 기능을 잠시 꺼 둘 때 등 공격자들이 공격의 기회로 노릴 틈은 많이 있습니다.

데이터에서 보여지듯 24시간 모니터링을 통한 웹 공격의 감시와 혹시라도 발생할 수 있는 웹 공격에 대비하는 대응 매뉴얼이 갖춰져야 합니다. 또한 대응 매뉴얼에 따른 정기적 훈련과 비상 훈련을 통해 웹 공격에 대응할 수 있는 능력을 키워야 합니다. 이를 위해 웹 공격의 탐지와 분석이 필요합니다.

IV. APPENDIX

1. 분석 방법

1) 데이터 수집 대상, 기간

본 WATT Report작성에 사용된 데이터는 주로 아시아-태평양 지역에 보급된 웹 방화벽 WAPPLES를 통해 2018년 1월 1일부터 2018년 12월 31일까지 탐지된 로그를 분석한 결과입니다.

2) 이전 보고서와의 차이점

본 WATT Report는 2015년까지 발간되었던 ICS Report와 2016년, 2017년 WATT Report를 토대로, ICS 서버에서 수집되는 WAPPLES 탐지 룰의 정탐 로그만을 활용하여 작성되었습니다. 또한 2018년 WATT Report 부터는 펜타시큐리티에서 연구 개발한 머신러닝 기술을 적용하여 향후 웹 공격 예측에 대한 정확도를 향상시켜 작성되었습니다. 매년 발간하고 있는 WATT Report는 WAPPLES 사용 고객, 기업, 기관의 보안관리자 등 기존 독자, 나아가 웹 보안 동향에 관심 있는 국가/사설 연구기관 및 대학 연구실을 포함한 일반 독자를 대상으로 이해하기 쉽도록 분석 및 작성되었습니다. 향후 지속적 연구와 분석을 통해 정보를 업데이트하여 연간 동향을 발간할 것입니다. 이로써 연간 동향 파악 및 연도별 동향 비교 자료로도 사용될 것입니다.

3) 기술 용어 정의

▪ Extension Filtering

소개 : Extension은 파일이름에 파일 형식을 기록하는 확장자를 의미합니다. 이를 악용하여 해커가 악의적인 목적으로 정상적이지 않은 확장자를 사용하여 파일 다운로드, 파일 실행 등을 유도하여 해커가 원하는 동작을 수행하게 됩니다.

예상 피해 : 스크립트를 통한 비정상 기능 수행

▪ Error Handling

소개 : 서버에서 응답해주는 패킷에 포함되는 Code를 이용해서 서버의 처리 결과를 클라이언트에게 알려주게 됩니다. 이때 특정 오류 메시지의 경우, Web Server, Web Application, DBMS의 종류 및 버전 정보를 함께 전달하기도 합니다. 이러한 오류 메시지에 대한 탐지 및 차단 정책의 부재는 정보 유출로 이어져 큰 피해로 이루어질 수 있습니다.

예상 피해 : 정보 유출, 제 2의 공격을 위한 준비

▪ Cross Site Scripting

소개 : 게시판, 웹 메일 등에 삽입된 악의적인 스크립트를 통해 사용자가 원하지 않는 동작을 수행하게 하는 공격 기법입니다. 예를 들면 해커가 서버에 악성코드가 포함된 글을 작성하게 되고, 이 글을 일반 사용자가 읽게 되었을 경우 실행이 되게 되며, 이로써 사용자의 정보가 해커에게 들어가게 됩니다.

예상 피해 : 사용자 쿠키 탈취, 사용자 세션 탈취, 스크립트를 통한 비정상기능 수행

IV. APPENDIX

▪ Request Header Filtering

소개 : 웹 브라우저에서 정상적으로 보내는 HTTP Request 요청문과 달리 악의적인 목적을 가지고 있는 해커가 Header에 필수 요소를 빼거나, 다른 요소를 기입하여 잘못 되어있는 형태로 전송하는 공격 기법입니다. 자동화된 공격 도구 등에서 자주 활용하는 공격 기법입니다. 이러한 공격은 웹 서버의 정보가 변조되거나 제한적이지만 웹 서버가 피해를 입을 수 있습니다.

예상 피해 : 웹 서버 정보 변조, 웹 서버의 비 정상적인 행동 유도

▪ Stealth Commanding

소개 : 웹 서버의 System 명령어를 이용하여, 웹 서버 외부에서 공격자들이 웹 서버에서 실행 가능한 명령어를 입력하여 비정상적인 행동을 유도하거나 정보를 획득하는 공격 기법입니다. System 명령어가 적용되는 파라미터에 명령어를 주입하는 방법으로 공격을 수행합니다.

예상 피해 : 웹 서버의 비정상적인 행동 유도, 정보 유출

위에 소개해드린 기술 용어들은 모두 정보 유출을 통한 피해 및 서비스 장애 등을 유발할 수 있는 취약점 및 공격 기법입니다. 펜타시큐리티에서 발간한 WATT Report를 바탕으로 자체적인 보안 예방 및 대응책을 마련하여 소중한 기업정보 및 개인정보를 지켜야 할 것입니다.

IV. APPENDIX

4) Black IP List

순위	공격지 IP	국가	위험도
1	211.253.x.x	Korea	98.11
2	211.233.x.x	Korea	97.66
3	61.97.x.x	Korea	97.31
4	1.223.x.x	Korea	96.75
5	116.120.x.x	Korea	96.23
6	115.95.x.x	Korea	96.01
7	100.210.x.x	United States	95.54
8	222.231.x.x	Korea	95.22
9	36.234.x.x	Taiwan	93.89
10	10.206.x.x	United States	93.41
11	104.155.x.x	United States	92.88
12	210.94.x.x	Korea	91.09
13	211.218.x.x	Korea	91.01
14	211.253.x.x	Korea	89.71
15	211.253.x.x	Korea	89.44
16	35.197.x.x	United States	89.04
17	175.192.x.x	Korea	88.91
18	103.29.x.x	Japan	88.89
19	51.15.x.x	United Kingdom	88.51
20	118.129.x.x	Korea	87.78
21	222.239.x.x	Korea	87.64
22	122.54.x.x	Philippines	87.55
23	211.253.x.x	Korea	87.13
24	106.248.x.x	Korea	87.07
25	1.244.x.x	Korea	86.98
26	91.247.x.x	Ukraine	86.93
27	222.106.x.x	Korea	86.68
28	14.47.x.x	Korea	86.49
29	100.210.x.x	United States	86.21
30	54.249.x.x	United States	86
31	115.60.x.x	China	85.88
32	1.215.x.x	Korea	85.71
33	183.111.x.x	Korea	85.27
34	58.246.x.x	China	84.95
35	211.176.x.x	Korea	84.76
36	59.3.x.x	Korea	84.11
37	210.179.x.x	Korea	84.03
38	115.22.x.x	Korea	83.95
39	185.222.x.x	United States	82.64
40	125.133.x.x	Korea	81.23

Penta SECURITY

enterprise · iot · blockchain

KOREA www.pentasecurity.co.kr

GLOBAL www.pentasecurity.com

JAPAN www.pentasecurity.co.jp

TU-Automotive AWARDS

TU-Automotive Awards
Best Auto Cybersecurity
Product/Service 2019

CYBER SECURITY EXCELLENCE AWARDS WINNER 2018

Cybersecurity
Excellence Awards
Winner 2018

CDM

Hot Company in
Web Application
Security for 2016

SC MAGAZINE

SC Magazine Europe
Best SME Solution

FROST & SULLIVAN

Asian Cyber
Security Vendor
of the Year

Gartner

Recognized on the
Gartner WAF
Magic Quadrant

1

No.1 WAF
Vendor in the
APAC Region

ICSA labs CERTIFIED

ICSA Labs
Certified WAF

The First and Only
CCEAL4 Certified
WAF

PCI DSS COMPLIANT

PCI-DSS
Compliance