March, 2024
금융보안관제센터

FSI Malicious IP 2023

금융권 주요 공격 IP 동향

Threat Hunting

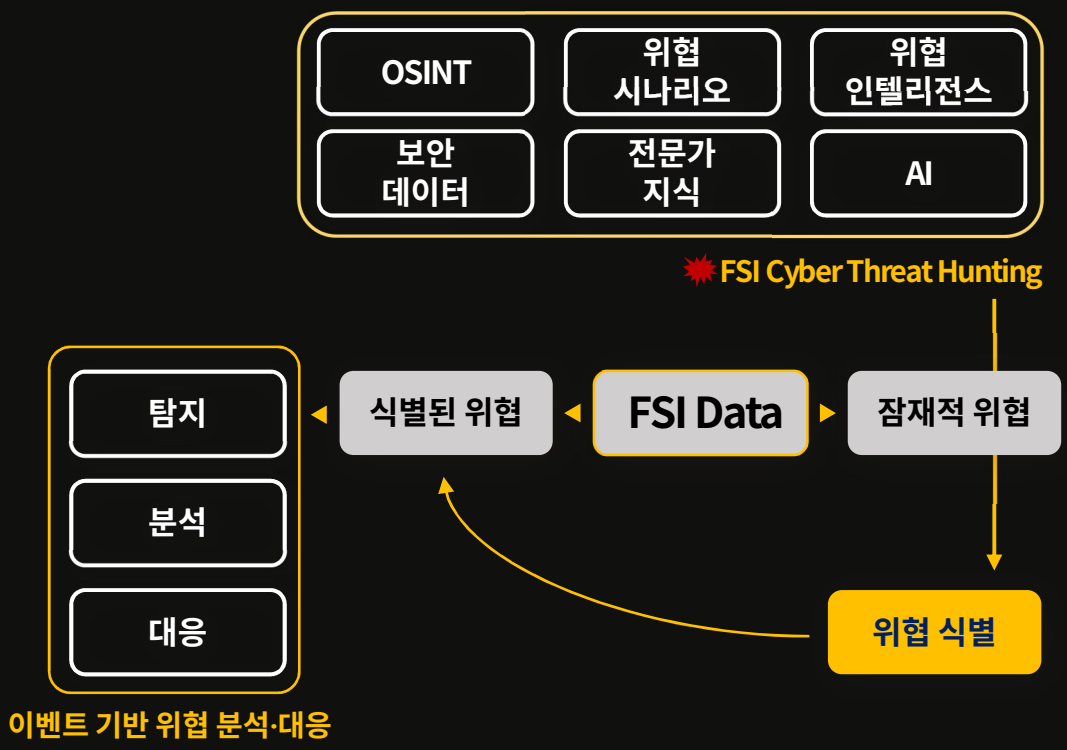
금융보안원
FINANCIAL SECURITY INSTITUTE

FSI Cyber Threat Hunting

사이버 위협 헌팅은 전문 정보보안 분석가 집단이 외부위협정보(OSINT), 위협 인텔리전스, 내부 보안 데이터, 위협 시나리오 등 다양한 경로로 수집한 정보와 전문가의 보안 지식 및 노하우를 기반으로 내부 시스템과 네트워크를 대상으로 잠재적인 사이버 위협을 식별하고 제거하는 활동이다.

금융보안원은 '23년부터 다수의 정보보안 분석가를 중심으로 국내 • 외 사이버 위협 정보와 금융회사에 설치된 200여개의 자체 보안관제 센서를 이용하여 금융권의 사이버 위협을 식별하고 제거하는 사이버 위협 헌팅을 수행해 왔으며, 이 보고서는 그 동안의 위협 헌팅 활동을 기록하고 분석한 보고서이다.

본 보고서를 통해 금융권의 사이버 위협 행위자들의 다양한 공격 방법과 기술을 이해하고, 이를 기반으로 조직의 잠재적 보안 위협을 파악하여, 사이버 위협을 사전에 제거하고 차단하기 위한 전략과 방법을 수립하는데 활용하기를 기대한다.

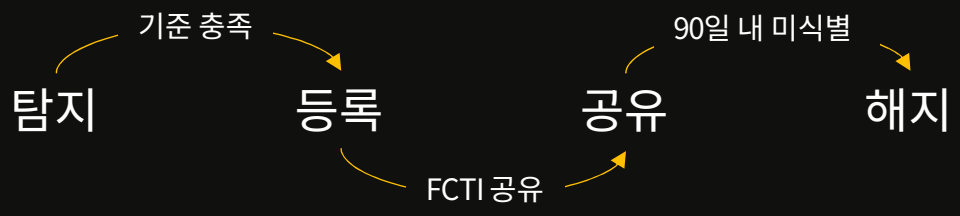


요주의 IP Malicious IP

금융보안원은 국내 200여개 금융회사의 전자금융서비스 구간을 대상으로 부문보안관제를 수행하고 있으며, 금융회사의 네트워크 구간에 자체 보안관제시스템(관제 센서)을 설치하여 다양한 위협 정보를 수집 • 분석하고 있다.

금융보안원에서는 일평균 6TB 이상 수집된 데이터와 위협 정보를 기반으로 금융권을 대상으로 하는 공격 IP**를 FSI 요주의 IP (Malicious IP)**로 별도 지정하여 공격 유형과 특징 등을 종합적으로 분석하고 지속적으로 추적 모니터링하고 있다.

요주의 IP로 지정되면 금융사이버위협정보공유시스템(FCTI)을 통해 금융회사에 공유가 되며, 요주의 IP로 지정한 IP가 90일간 추가 공격 활동이 없으면 요주의 IP에서 해지가 된다.



본 보고서는 2023년의 금융권 전자금융서비스를 대상으로 한 47,874개 공격 IP의 주요 활동과 특징을 추적 • 분석하여 새로운 공격 유형과 패턴을 식별하고, 요주의 IP의 중요성과 효과성 및 활용 지침을 제공하는 것을 목적으로 한다.

또한, 본 보고서를 통하여 2024년에 금융권 전자금융서비스를 대상으로 하는 사이버 위협을 전망하고, 사이버 위협의 탐지와 대응에 대한 통찰을 제공하고자 한다.

※ 권고사항 ※

금융보안원에서 제공하는 요주의 IP는 1차 선별된 공격 IP로서 각 금융회사의 서비스 상황과 요주의 IP의 공격 현황을 기반으로, 금융회사에서 자체적으로 활용할 수 있도록 제공되는 FSI Intelligence 정보입니다.

금융사이버위협정보공유시스템(FCTI)에서 제공하는 요주의 IP 목록은 Security Threat Intelligence 정보로 활용 권유드립니다.

요주의 IP (Malicious IP)

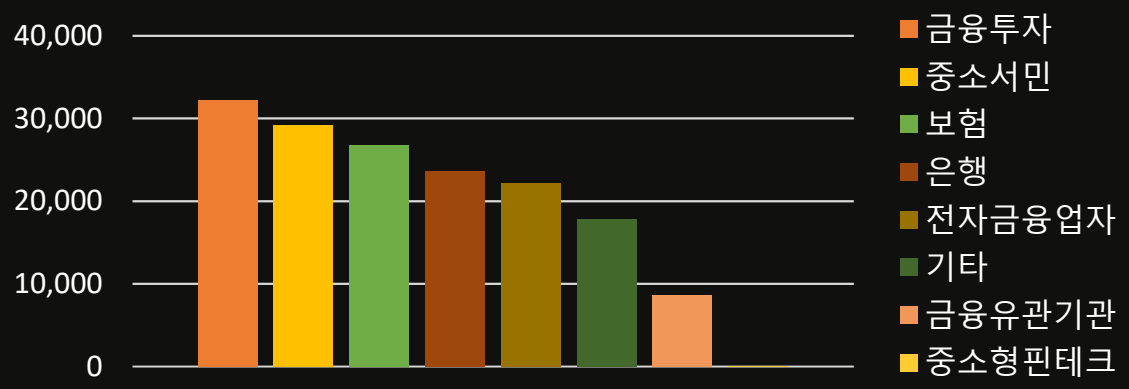
금융권의 전자금융서비스를 대상으로 **일일 4개 기관 이상, 7일 중 2회 이상 공격한 IP** 중 금융보안원이 정한 기준에 부합하는 IP
90일간 추가적인 공격 활동이 없으면 자동 해지

Overview Statistics of Malicious IP 2023

등록 IP 개수	등록 국가 수	등록 AS[1] 개수	전체 대응 건수	공격 IP 활동 수명 주기
47,874	180	6,889	29,482,974	**28일**

2023년 요주의 IP로 지정된 공격 IP는 총 47,874개로 180개국, 6,889개의 AS이고 **공격IP의 활동 수명 주기(Attack IP Activity Lifecycle)는 평균 28**일로 분석된다.

우리는 2023년 요주의 IP의 활동을 추적하고 분석한 결과, 많은 부분의 IP가 **일정 기간(평균 28일) 공격자들에 의해 이용된 후 더 이상 공격에 사용되지 않는 특징**을 확인했으며, 다수 금융회사에서 요주의 IP를 차단하는 등 적절한 대응을 하고 있어 공격자가 더 이상 활용가치가 없는 IP를 사용하지 않는 것으로 추정하고 있다. 우리는 이런 공격자의 IP 활용 주기를 **" 공격 IP의 활동 수명 주기 (Attack IP Activity Lifecycle) "** 이라 명명하고, 이 **주기를 단축시키는 것을 목표**로 지속적으로 활동을 추적 및 분석하고 있다.

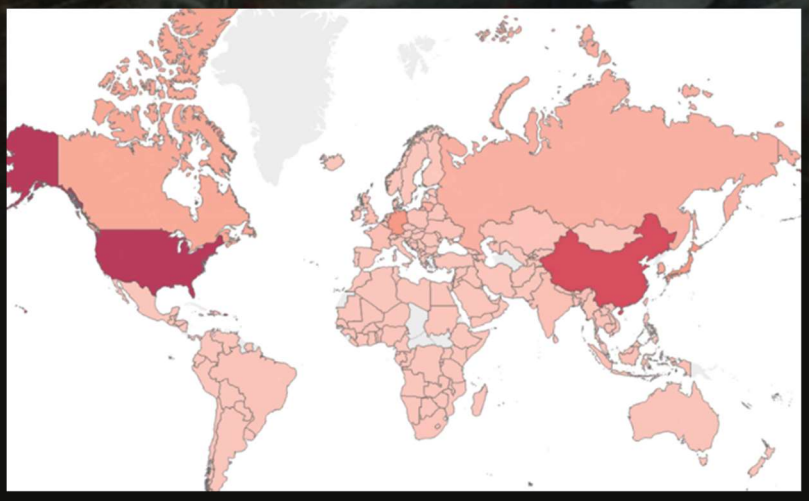


가장 많은 요주의 IP의 공격 대상 업권은 금융투자(32,206개)였으며, 중소서민(29,191개), 보험(26,741개), 은행(23,644개), 전자금융업자(22,227개), 기타(17,876개), 금융유관기관(8,565개), 중소형 핀테크(54개)순 이였다. 또한, 단일 업권에 대한 공격으로 확인되는 IP는 10,287개였으며, 이는 **약 20%의 IP가 특정 목표만을 대상으로 공격에 활용**되었다고 볼 수 있다.

공격 IP 활동 수명 주기 (Attack IP Activity Lifecycle)

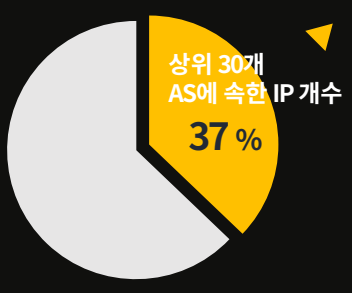
일 년 동안 금융보안관제 센서에서 공격 IP가 식별되어 일정기간 공격 활동을 한 후 종료(미식별)되는 공격 활동 주기

1) AS(Autonomous System) : 동일한 라우팅 정책으로 회사나 단체에서 관리하는 라우터 집단

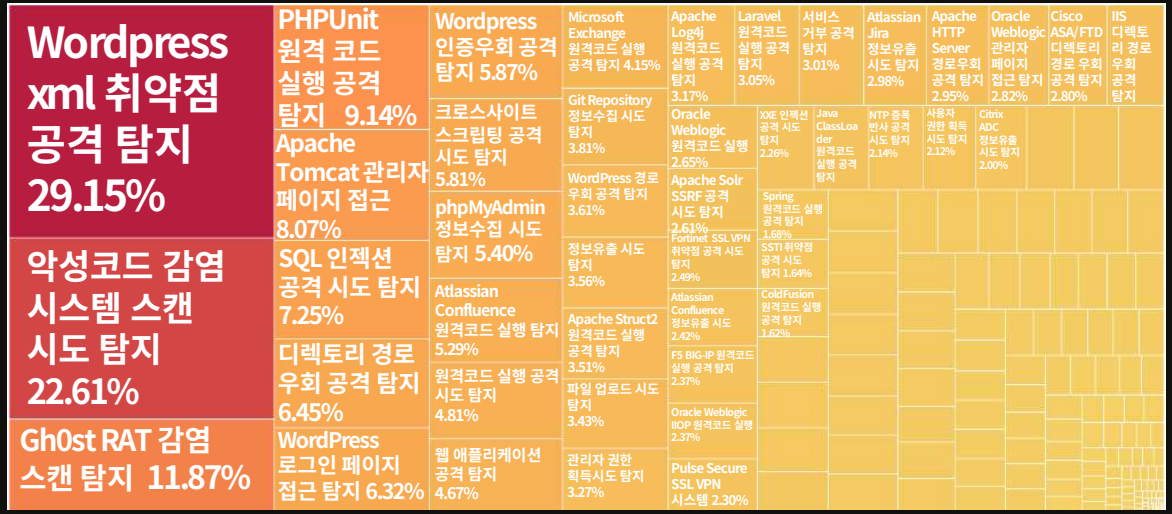


국가	IP 수	비율
미국	11,576	24.18%
중국	7,470	15.60%
베트남	2,495	5.21%
인도네시아	2,200	4.60%
인도	1,871	3.91%
싱가포르	1,559	3.26%
브라질	1,191	2.49%
독일	1,156	2.42%
영국	1,125	2.35%
러시아	906	1.89%

요주의 IP를 국가별로 살펴보면 미국(24.2%), 중국(15.6%), 베트남(5.21%)이 상위를 차지하고 있으며, 약 **37%(17,776개) IP가 상위 30개의 AS에 속해**있어 소수 AS에서 다수의 IP가 공격에 사용되는 것을 식별했다. 이 AS에 속한 **평균 국가 수는 7.75개로 다수 국가에 데이터센터를 구축한 클라우드 서비스를 통해 다량의 공격을 시도**하고 있다.

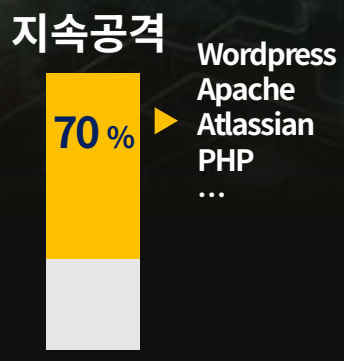


요주의 IP의 공격 유형별 통계에 따르면, **Wordpress xmlRPC(29%), 악성코드 감염 시스템 스캔 시도(23%), PHPUnit 원격코드 실행 공격(9%), Apache Tomcat 관리자 페이지 접근(8%) 등이 다수 확인**되었으며, 기간과 공격 유형, 국가 등에 따라 특이점을 확인할 수 있다.



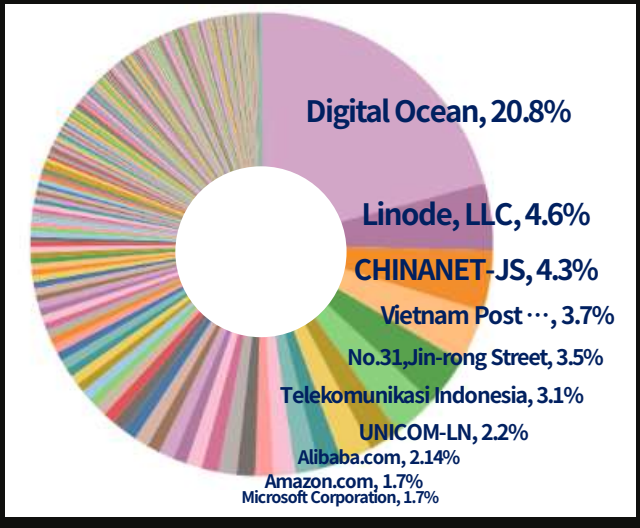
“다양한 시스템 대상으로 지속적인 공격을 시도하는 요주의 IP ”

최근 전세계적으로 이용되는 시스템에 대한 취약점 공격이 지속적으로 발생하고 증가함에 따라 2023년도 요주의 IP로부터 지속적으로 탐지되는 공격 유형을 분석하였다.
지속적인 공격이란, 일정 기간 이상 공격이 계속되는 행위를 의미하며 본 보고서에서는 **최소 9개월 이상의 지속적인 공격을 기준**으로 한다.



통계에 따르면, 연내 9개월 이상 지속적으로 탐지된 공격은 Wordpress, Apache, PHP, Atlassian 등 세계적으로 사용되는 시스템을 대상으로 하고 있으며 **약 66%(127개)의 탐지유형이 이에 해당**된다. 그리고, 지속공격 분석에서 확인된 IP는 전체 IP의 52%(24,915개)를 차지한다.

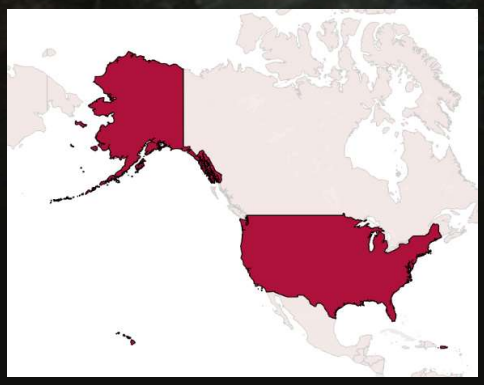
주요 **공격 유형의 대부분은 오래된 취약점을 대상**으로 하는 공격이며 이러한 공격이 여전히 유효하고 효과적이기 때문에 특정 국가를 가리지 않고 지속적으로 공격이 이루어지는 것으로 보인다.
실제로, **‘23년 중국 ’샤오치잉’ 국내 대규모 해킹[1], '24년 중국 '니엔' 국내 대규모 해킹 사건[2]** 처럼 국내 • 외 다수의 침해사고가 널리 알려진 과거의 취약점을 악용해 내부 침투한 후 정보를 유출한 사례가 확인되고 있으며 이에 대하여 많은 국가기관 및 보안회사에서 과거 발표된 취약점의 신속한 보안 조치를 권고하고 있다.

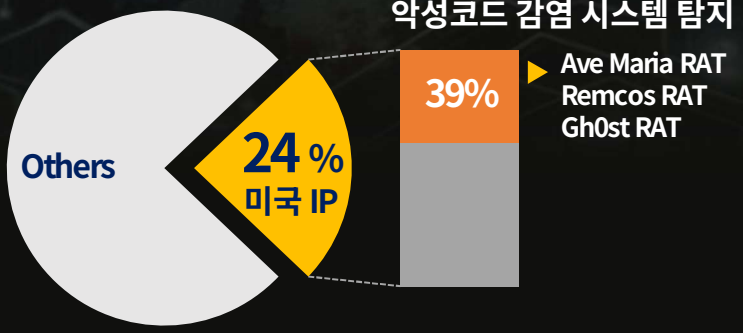


9개월 이상의 지속적인 공격을 분석한 결과, **지속공격에서 확인된 다수 AS가 클라우드 호스팅 서비스**이며, 이는 클라우드 서비스 특성 상 공격 IP 변경이 상대적으로 용이할 수 있다는 것을 의미한다. 또한, 전세계에서 활용되는 시스템들을 주요대상으로 꾸준하게 공격이 시도되고 있으므로 이에 대한 **보안 및 표면 관리 미흡 시 즉시 침해사고가 발생 할 수 있음**을 시사한다.
따라서, 보안 담당자는 단순 IP 차단 방식의 대응을 지양하고 알려진 취약점에 대해 선제적인 보안 대응 및 공격 표면 관리에 주의를 기울여야 한다.

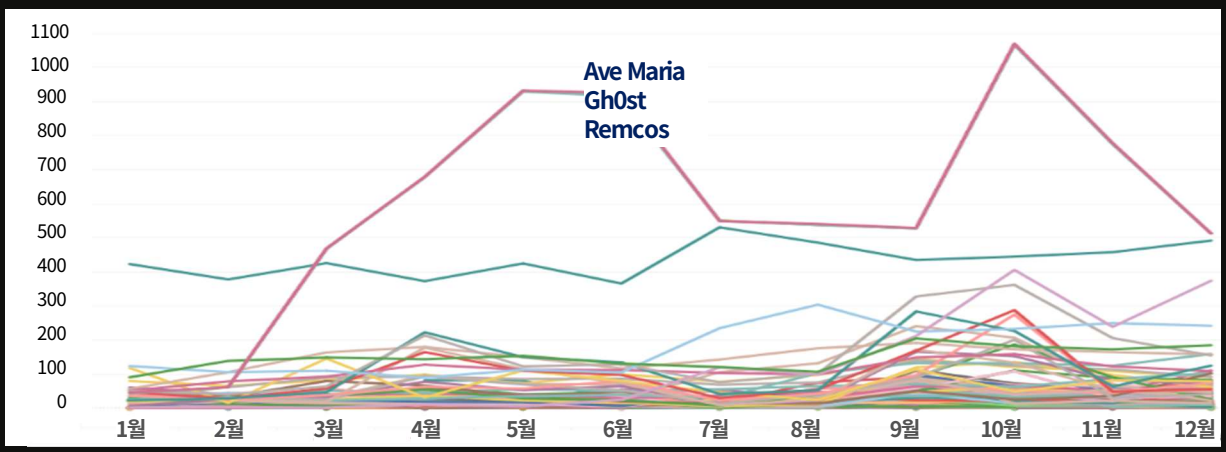
1) https://ngfcti.kfisac.or.kr/?pageid=TSIMasterDetail&tsi_id=29124D14-4EBD-F442-6EE3-515179D50286
2) https://ngfcti.kfisac.or.kr/?pageid=TIUMasterDetail&tiu_id=7FA3F5F5-92FF-06EE-743C-48CA7E791086

“미국 IP로부터 다수 시도되는 악성 RAT 감염 시스템 스캔 공격 ”





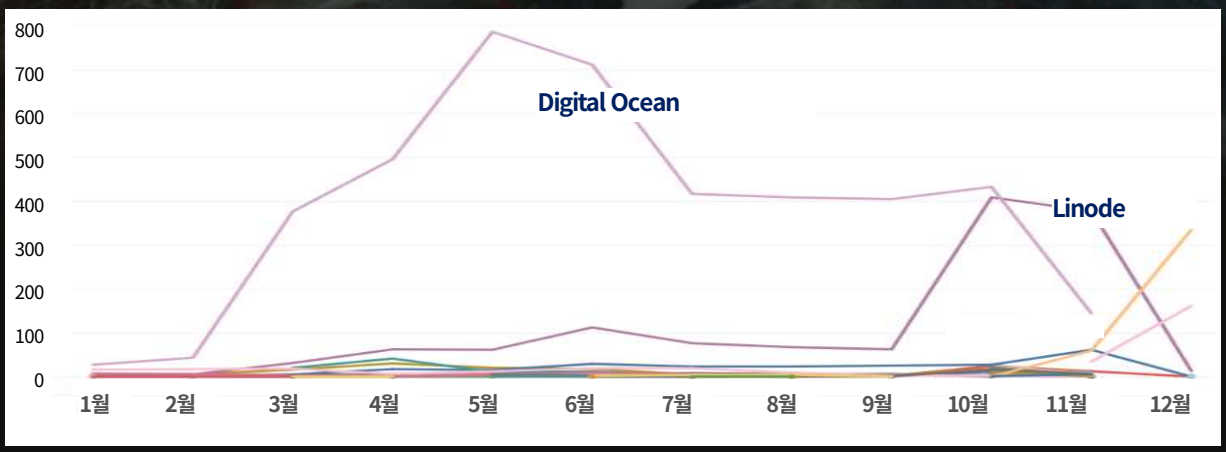
2023년 요주의 IP 국가 중 **미국이 약 24%(11,576)로 가장 많은 비율을 차지**하고 있으며, 월 평균 964.7개의 IP가 요주의 IP로 등록되었다. 이 중 **약 38.8%의 IP가 악성코드 감염 시스템 공격 시도**이며 , 특히 **RAT(Remote Access Trojan) 악성코드에 감염된 시스템을 탐색**하는 스캔 공격이 주를 이루었다. 주로 대상이 되는 **악성코드는 Ave Maria, Gh0st, Remcos 이다**.



Ave Maria는 Warzon RAT[1]라고도 불리며, 2023년 월 38달러(1년 동안 196달러)에 서비스형 멀웨어(Malware-as-a-Service) 모델을 판매하던 판매자가 검거된 바 있다[2]. Remcos RAT는 23년 전국적으로 가짜 링크, 피싱 메일, 가짜 소프트웨어 배포 페이지 등 다양한 피싱 기법을 통해 다량 배포되었으며[3], 2008년 중국의 해킹그룹이 제작한 Gh0st RAT는 출시 후 15년이 지났음에도 23년 의료기관 대상 피싱에 사용되는 등 여전히 광범위하게 사용되고 있다.[4]

국내 금융권도 위와 같은 외부 위협 동향에 민감하게 영향 받아 악성코드 감염 시스템 공격 시도가 증가한 것으로 볼 수 있다.

1) https://www.splunk.com/en_us/blog/security/defending-the-gates-understanding-and-detecting-ave-maria-warzone-rat.html
2) https://thehackernews.com/2024/02/us-doj-dismantles-warzone-rat.html
3) https://asec.ahnlab.com/ko/58004/ , https://thehackernews.com/2023/07/fruity-trojan-uses-deceptive-software.html
4) https://cofense.com/blog/open-source-gh0st-rat-still-haunting-inboxes-15-years-after-release/

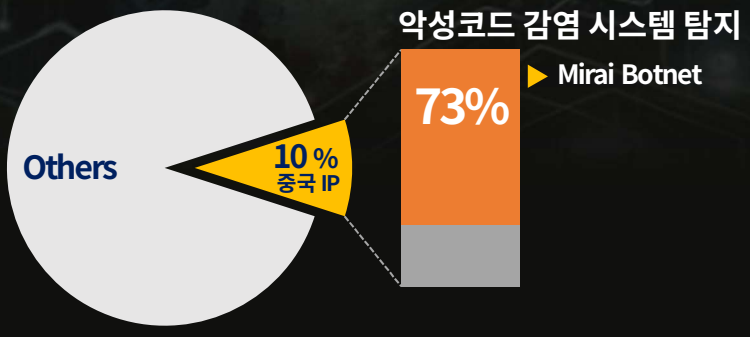


미국 IP로부터 유입된 악성코드 감염 시스템 스캔 시도는 대부분 DigitalOcean과 Linode AS 등에 속한 **클라우드 호스팅 서비스 IP를 이용한 공격**이다. 또한, 각 공격에 활용된 IP의 수가 시계열 분석에 따라 유사한 패턴을 보이고 있으므로 **동일한 목적과 도구를 가진 다수 혹은 단일 공격자가 다양한 클라우드 IP를 각종 악성코드 감염 시스템 스캔에 악용**하는 것으로 볼 수 있다.

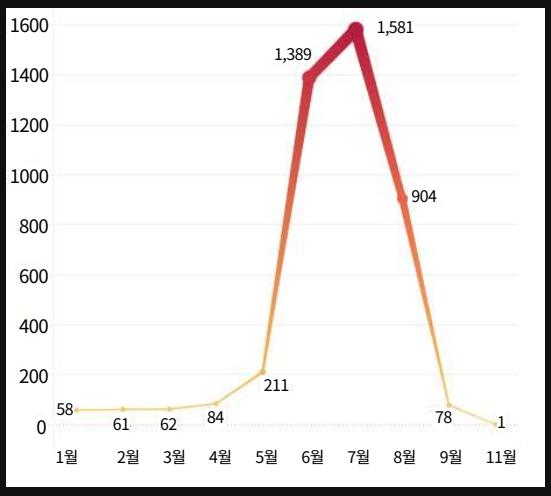
클라우드 호스팅 서비스를 통한 공격은 IP 변경이 상대적으로 용이하고 공격의 패턴이 지속적인 형태를 나타내고 있으므로 **IP 차단 방식의 대응보다는 반드시 선행되어야 하는 초기 악성코드 감염 등에 주의**해야 한다.

특히, **피싱 메일, 가짜 사이트 접근 등 각종 피싱 기법에 의한 적극적인 주의 태세와 임직원 교육을 통한 보안 인식 제고가 각별히 요구**된다.

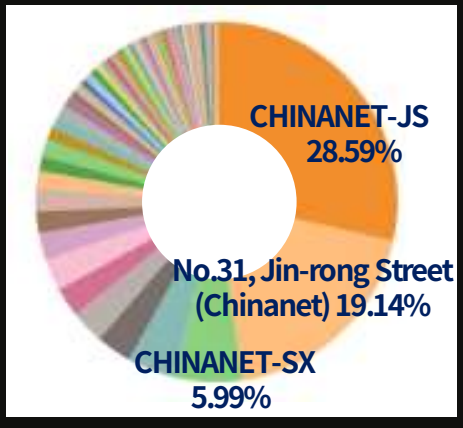
“중국 IP로 집중 시도된 Mirai Botnet 스캔 공격 ”



전체 요주의 IP 중 두 번째로 많은 비율을 차지하고 있는 **중국 IP는 전체의 10%**로 월 평균 622.5개의 IP가 공격에 사용되었다. 이 중 **3,470개의 IP가 악성코드 감염 시스템 공격 시도이며**, 앞서 언급한 미국 IP와는 조금 다른 공격 형태를 보인다. **중국 IP는 6~7월에 급증 후 점차 줄어드는 추세**를 보이는데, 앞서 분석한 미국 IP와 같이 지속적으로 공격하는 패턴과는 달리 특정 이슈에 의한 급증 패턴을 나타내고 있다. **공격의 대부분은 Mirai Botnet 악성코드 스캔**으로, 중국의 대형 공영 인터넷 네트워크인 Chinanet AS 위주로 **금융투자 업권을 대상으로 집중**되었다.



금융투자 업권
100 %



Mirai Botnet은 IoT 기기에 침투하여 원격으로 기기를 조작하고 DDoS 등에 악용하는 Botnet의 일종이다.

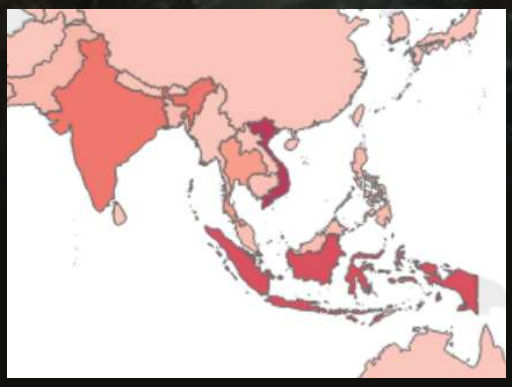
해외 보안 전문가는 Mirai Campaign 분석[1]에서 23년 3월부터 D-Link, Zyxel, Netgear 기기 등의 여러 결함을 노린 Mirai Botnet 변종이 확산되어 6월까지 공격 행위가 확인되었다고 발표하였으며, **5월 금융보안원에서 Hikvision IoT 봇넷(Mirai)을 통한 DDoS 주의**[2]를 권고하기도 했다.

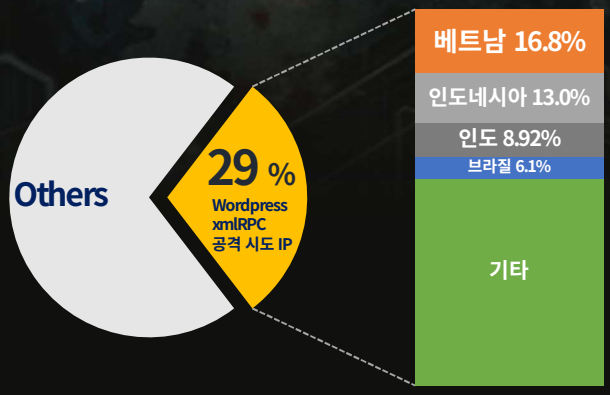
관련성은 확인되지 않았으나 **해당 공격이 급증하였던 6~7월에 금융권 대상(카드사) DDoS 공격이 증가**[3]하였다.

금융권은 Botnet 감염 등에 대한 보안이 비교적 철저하지만, **23년 Mirai Campaign이 전세계적으로 발생하여 24년도 DDoS 공격에 주의가 필요**하다.

1) https://unit42.paloaltonetworks.com/mirai-variant-targets-iot-exploits/
2) https://ngfcti.kfisac.or.kr/?pageid=TSIMasterDetail&tsi_id=557D4643-5A31-8BDE-7A43-A6B55619DBD7

“다수 국가 IP로 동시다발적 발생한 Wordpress xmlRPC 스캔 ”

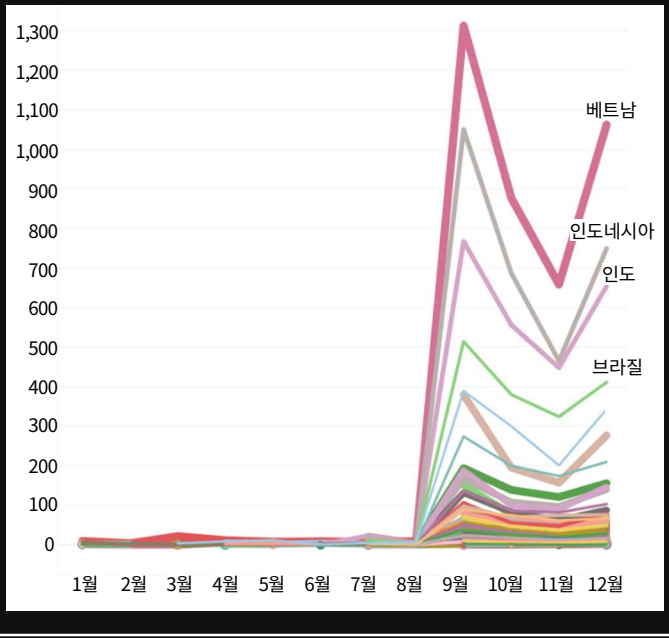




2023년 가장 많은 요주의 IP가 공격을 시도한 **Wordpress xmlRPC 취약점 공격은 9월부터 베트남 IP를 필두로 인도네시아, 인도 등 다수의 동남아시아 지역 IP 위주로 발생**하였다. **월 최대 8,344개의 IP가 공격을 시도**하였으며, **전체 요주의 IP의 약 29%(13,950개)의 IP가 공격에 사용**되었다.

Wordpress xmlRPC 취약점은 Wordpress가 다른 웹사이트 및 소프트웨어와 xml을 통해 상호작용하도록 지원하는 모듈에서 발생한다. 이 취약점으로 API를 통한 BruteForce, SQL Injection, CSRF, Pingback을 활용한 DoS 공격 등에 활용되고 있다.

해당 공격의 **페이로드 97%는 wp.gerUserBlogs Method를 통해 admin/admin 로그인을 시도**하였다. 이는 공격자들이 유사한 목표를 가지고 공격을 시도하였다고 볼 수 있으며, **나아가 동일 공격자의 가능성을 내포**한다.



해당 취약점은 확인된 지 **15년이 지났음에도 위와 같이 대량 공격에 활용**되었다. 기술 발전으로 광범위한 공격이 용이해짐에 따라 과거 취약점 기반의 대량 공격을 시도하는 사례가 존재하므로 주의가 필요하다.

관련성은 확인되지 않았으나, **12월 다수의 베트남, 인도네시아 IP에서 User-Agent를 변경하며 금융권 대상 DDoS를 시도**[1]하기도 하였다.

1) https://ngfcti.kfisac.or.kr/?pageid=TSIMasterDetail&tsi_id=2C84B767-1984-1192-928E-1209D2B7FFE7

2023 Malicious IP Trends

23년 요주의 IP를 기반으로 확인한 결과, 최신의 취약점 및 시스템을 대상으로 하는 공격 방식 보다 **시일이 지난 공격 방식**을 기반으로 **지속적이고 광범위한** 공격 시도가 주를 이루었다. 이는 공격자가 적은 노력과 비용으로 큰 효과를 얻을 수 있기 때문으로 판단된다. 이러한 오래된 취약점을 지속적으로 찾아내고 공격하는 행위는 앞으로도 계속 성행할 것으로 보이기 때문에 보안 취약점 관리와 패치에 대한 각별한 주의가 필요하다.

특히, '악성프로그램이 설치되어 있다'는 가정하에 수행되는 다수 **악성 프로그램 감염 시스템 스캔 시도**로 보아 공격자는 **피싱 기법** 혹은 취약점 공격을 기반으로 악성 프로그램을 설치하려는 시도를 다수 행했음을 알 수 있다. 악성프로그램은 **RAT와 같이 감염 시스템을 제어하기 위한 용도** 외에, **Mirai Botnet처럼 감염 시스템을 활용하여 DDoS와 같은 공격 매개체**로도 사용된다. 따라서, 24년에도 Botnet에 의한 DDoS 공격이 발생할 가능성이 높다.

23년 금융권에서는 굳건한 방어태세로 실제 악성코드 감염 및 피해 사례가 거의 없었으나, 피싱 기법을 통한 배포와 감염 시스템을 이용한 DDoS 공격, 자주 쓰이는 시스템을 대상으로 하는 위협이 앞으로도 계속 발생할 가능성이 존재하므로 **피싱 기법에 대한 임직원 교육과 시스템의 신규 공격 표면 발생 주의가 필요**하다.

끝으로 본 보고서를 통해 단순 공격 IP 차단방식으로는 신속한 사이버 위협 대응에 한계가 있다는 것을 공격 IP의 활동 주기(28일)를 통해 수치적으로 확인하고, 무엇보다 침해사고 예방을 위해 취약점 패치와 관리가 중요하다는 것을 알 수 있다.

따라서, 우리가 제공하고 있는 요주의 IP를 금융회사에서 적극적으로 활용하고 대응하면 공격 IP의 활동 주기는 더 단축될 것이며, 이러한 적극적 대응은 공격자의 시간과 자원을 소모시키고, 궁극적으로 국내 금융권에 대한 공격을 줄일 수 있을 것이라 기대한다.

금융보안원에서는 **위협 헌팅의 요소로 요주의 IP의 생성, 분석의 고도화를 계속해서 진행하고 공격 IP를 지속적으로 추적하고 모니터링할 것이다.**

2024 Threat Hunting Strategy

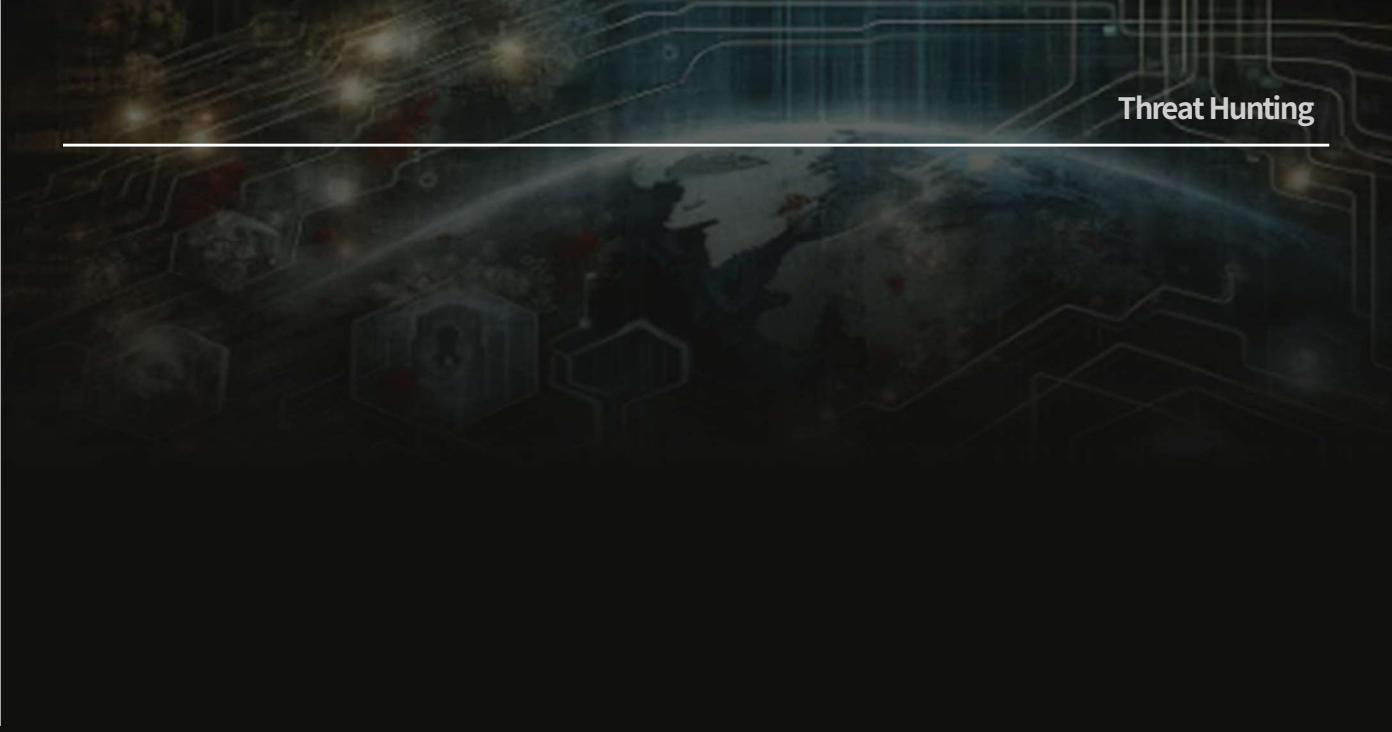
금융보안원은 **금융권 대상 CVE, FCTI TI** 등 금융권 위협 정보를 다양한 경로를 통해 제공하고 있으며, 해당 정보들과 AI, OSINT, 전문가 지식 등을 통해 Threat Hunting 연구를 진행하고 있다.

2023년 Malicious IP 동향은 금융보안원의 요주의 IP 정보를 바탕으로 한 Threat Hunting 기반 연구의 일환으로, 본 보고서에서 확인된 RAT, 피싱 메일 , ASM(공격표면관리) 등 잠재적 위협 요소에 대해 Threat Hunting 연구를 2023년부터 수행하고 있다. 추후 누적된 결과를 바탕으로 금융권의 위협 동향을 추가로 공개 할 것이다.

또한, 2024년에도 금융보안원은 **다양한 기반 정보를 연구하여 잠재적 위협 요소를 찾고, 이를 상세히 분석 • 대응하기 위한 Threat Hunting 연구**를 진행할 것이며, **기존 Threat Hunting 모델[1] 및 위협 인텔리전스 요소를 고도화**하는 Threat Hunting 프로세스를 수행할 것 이다.

이러한 결과로, FSI Threat Hunting은 금융권 보안 사각지대의 잠재적 위협 요소를 적시에 식별하고 금융회사와 공동 대응하여 금융권에 대한 위협 수준을 낮추는 것을 목표로 한다.

1) 식별된 잠재적 위협 요소를 분석 • 대응하기 위한 위협 헌팅 이벤트 생성 모델



FSI Malicious IP 2023

작성자 금융보안원 금융보안관제센터