

CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

CTA-CN-2021-0228



중국계 해커 그룹 RedEcho,
국경 분쟁 고조 상황에서 인도
전력기관 사이버 공격 시도



이 보고서는 중국계 해커 그룹 RedEcho가 인도 전력기관을 대상으로 전개한 사이버 공격 캠페인의 내막을 분석한다. 이 공격은 대규모 자동 네트워크 트래픽 분석과 전문가 분석을 통해 확인되었다. 데이터 소스에는 레코디드 퓨처 플랫폼, SecurityTrails, Spur, Farsight와 일반적인 오픈소스 도구 및 기술이 포함된다. 이 보고서는 인도, 중국의 사이버 활동 동향에 대한 전략적 정보와 운영 정보를 다루는 담당자에게 가장 유용할 것이다.

레코디드 퓨처는 이번 침입 의심 사례를 발표하기 전에 인도 정부 해당 부서에 사고 대응과 조사 지원을 위해 피해 사실을 고지했다.

요약

인도와 중국의 관계는 세계 최대 인구를 가진 두 나라 사이에서 45년 만에 처음으로 전투 사망자가 발생한 2020년 5월 국경 분쟁 이후 악화일로를 걷고 있다. 2021년 1월 12일 Subrahmanyam Jaishankar 인도 외무장관은 인도와 중국 양국 간의 신뢰가 “대단히 불안한 상황”이라고 발표했다. 외교적, 경제적 요인 덕분에 전면전으로 확대되지 않고 최근 국경 병력 철수까지 이루어졌으나, 스파이 작전이나 향후 공격을 위한 네트워크 사전 침투 목적의 사이버 활동은 여전히 계속되고 있다.

레코디드 퓨처 Insikt Group은 2020년 초부터 중국 해커 그룹의 인도 기관을 대상으로 한 침투 의심 활동이 크게 증가한 것을 관찰했다. 2020년 중반부터 AXIOMATICASYMPTOTE라는 인프라의 사용이 급격히 증가했다. ShadowPad C2(command and control) 서버가 포함된 AXIOMATICASYMPTOTE는 방대한 인도 전력망을 겨냥한 것으로 나타났다. 인도 내 전력 수급과 전력망 운영을 담당하는 5개의 RLDC(Regional Load Despatch Centres) 중 4개를 포함해 10개의 인도 기관이 인도 주요 인프라를 노린 캠페인의 타겟으로 확인되었다. 2개의 인도 항구도 표적에 포함되었다.

공격자 인프라 사전 탐지, 도메인 분석, 레코디드 퓨처 네트워크 트래픽 분석(Recorded Future Network Traffic Analysis)을 통해 AXIOMATICASYMPTOTE 인프라가 이전에 보고된 여러 중국계 해커 그룹(APT41 및 Tonto Team 등)과 인프라 TTPs(tactics, techniques, procedures) 면에서 몇가지 공통점을 갖고 있음이 드러났다.

그러나 몇 가지 공통점에도 불구하고 현재 이 특정 캠페인의 활동을 기존 그룹 소행으로 확정할 만한 충분한 증거는 없다. 따라서 Insikt Group은 밀접한 관련이 있느냐 별개의 그룹인 RedEcho로 배후를 특정하여 계속 추적하고 있다.

주요 내용

- 인도 기간시설을 겨냥한 해킹은 경제적 스파이 행위와는 큰 연관이 없다. 그러나 향후 중국의 전략적 목표를 지원하기 위한 사전 포석으로 네트워크 침투 가능성이 크게 우려된다.
- 전력망 사전 침투는 양국 간 긴장 고조 시 재래전에 앞서 인도 전력망을 마비시키려는 전략적 의도를 비롯한 여러 가능성을 내포한다.
- RedEcho는 강력한 인프라를 보유하고 있으며 중국해커 그룹인 APT41/Barium, Tonto Team과 공격 대상이 일부 일치한다. 최소 5개의 중국 해커 그룹이 ShadowPad를 사용한다.
- 인도 주요 인프라 엔티티로 확인된 IP들이 수개월 간 집중적으로 RedEcho가 사용하는 AXIOMATICASYMPTOTE 서버의 하위집합과 통신한 것이 확인되었다. 이는 표적 공격이 진행되었음을 나타낸다. 레코디드 퓨처의 네트워크 텔레메트리에 광범위한 타겟팅에 대한 증거는 거의 없다.

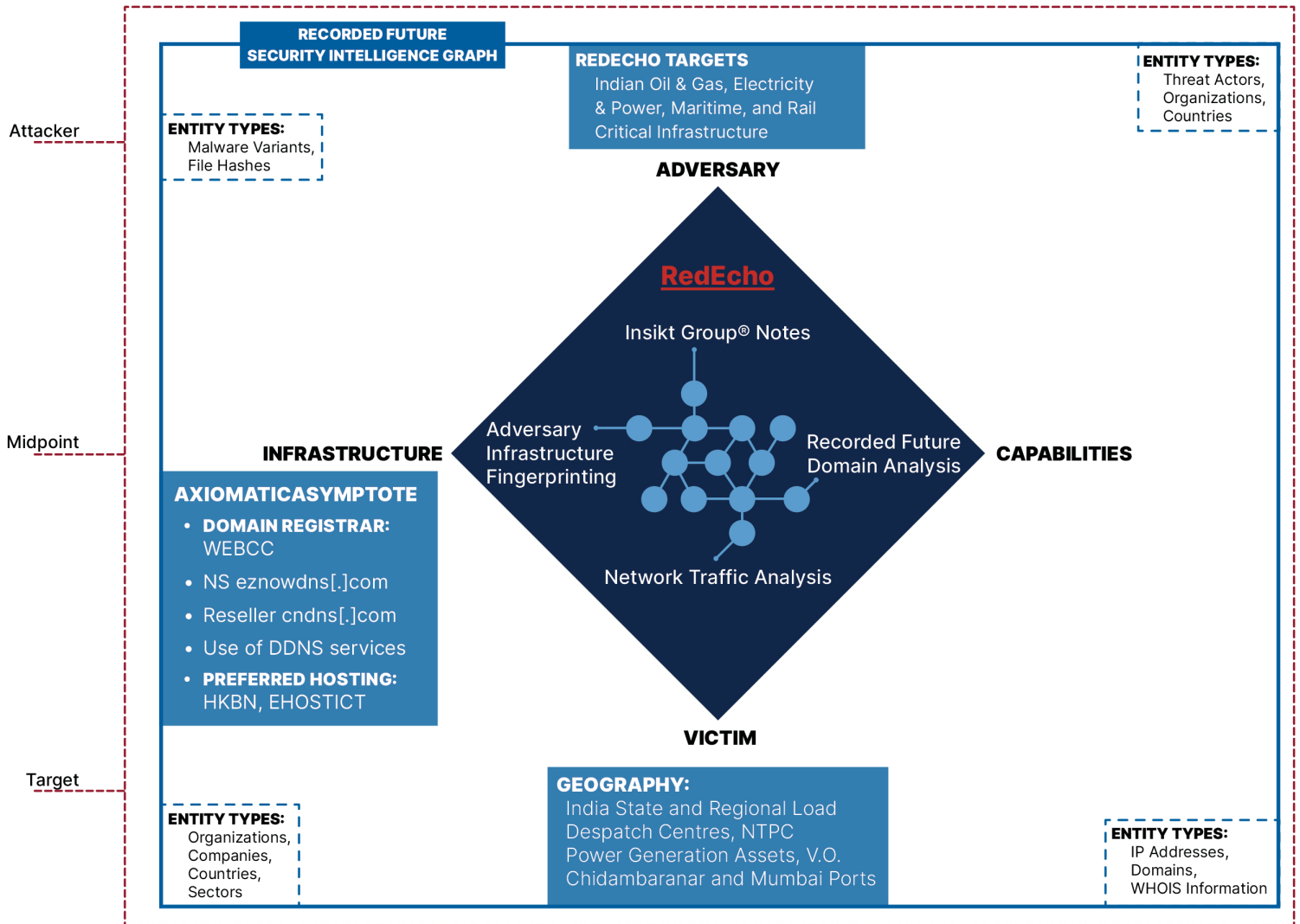


그림 1: RedEcho TTPs 및 레코디드 퓨처 데이터 소싱 그래프 (출처: Recorded Future)

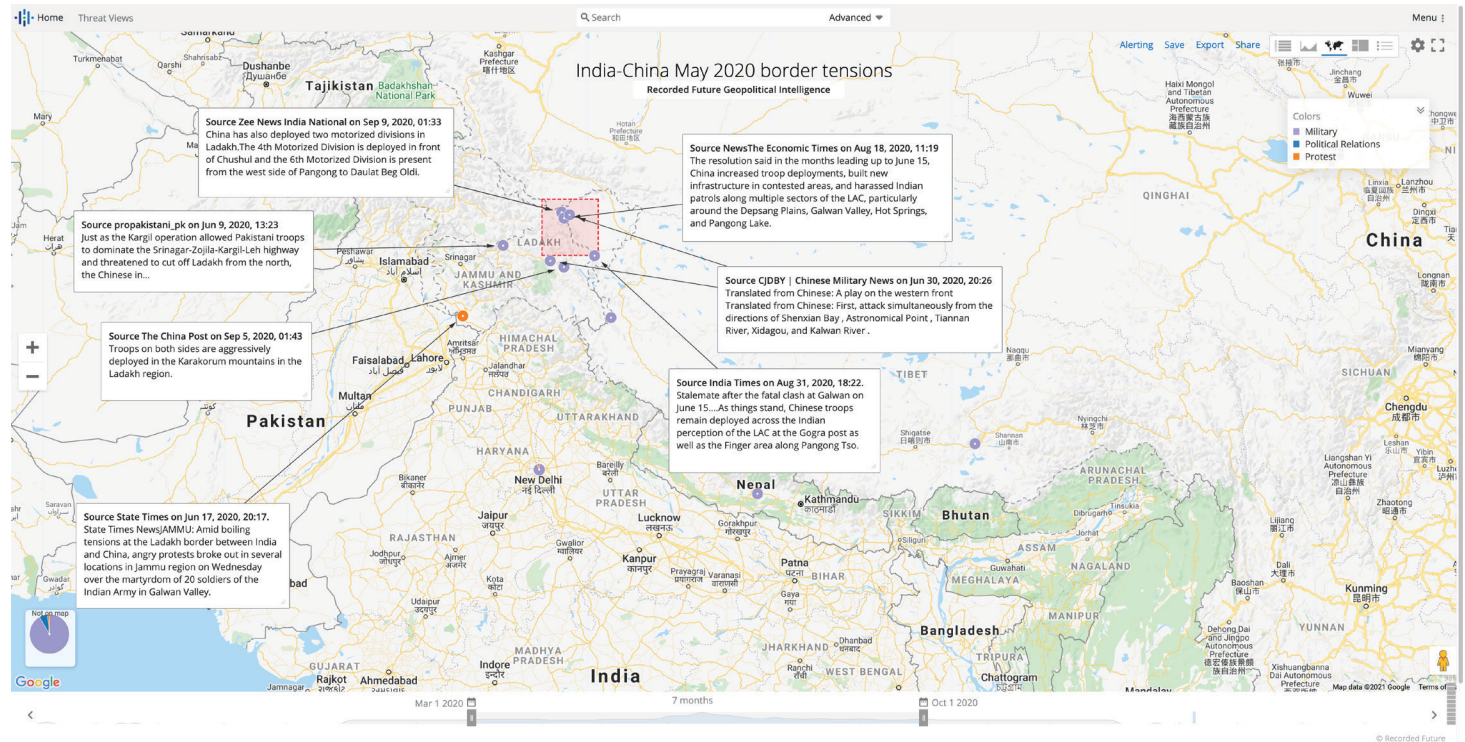


그림 2: 2020년 인도 갈완계곡에서 벌어진 인도군과 중국군의 국경 충돌 (출처: Recorded Future Geopolitical Intelligence)

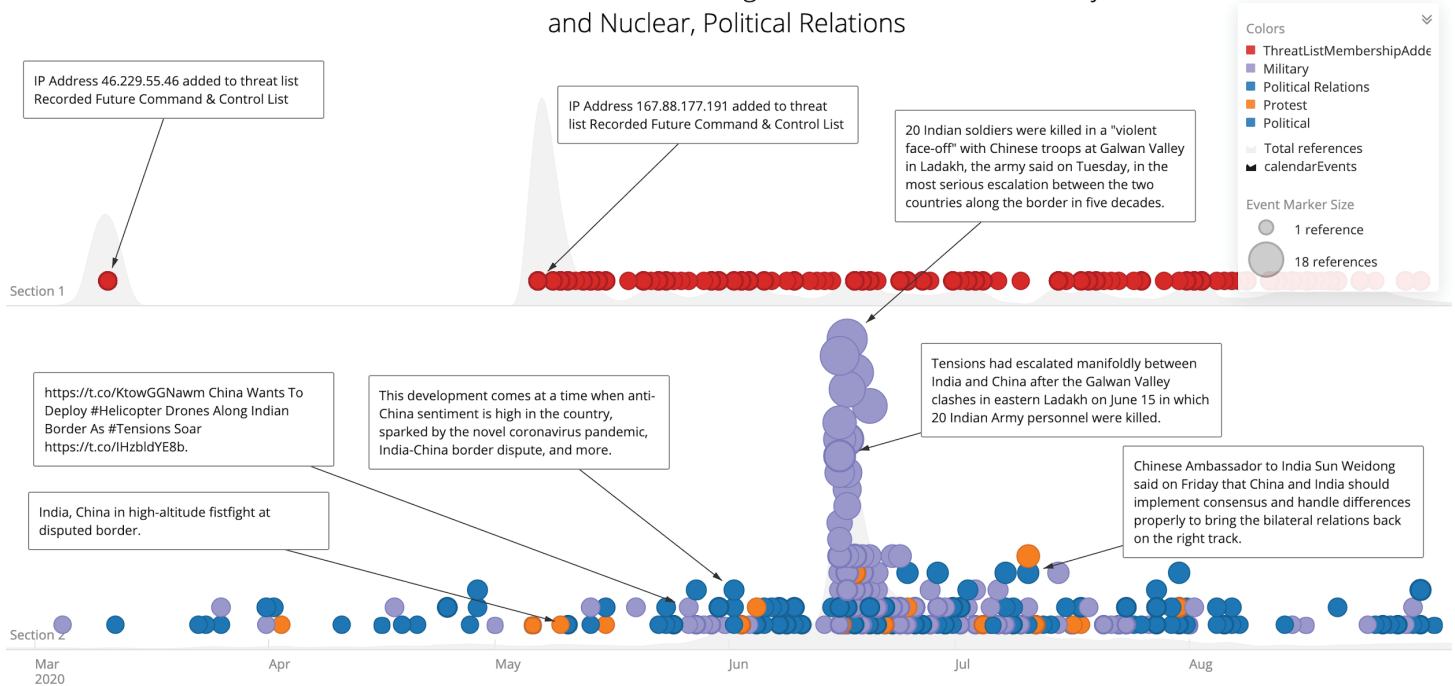
배경

인도와 중국 간의 긴장 고조

최근 몇 년 동안 인도의 경제적, 지정학적 야망이 중국과 충돌하면서 세계 최대 인구 보유국인 두 나라 사이의 갈등이 고조되고 있다. 2020년 5월 5일 이후로 인도와 중국의 군대가 국경 충돌을 거듭하고 있다. 보고서에 따르면 이처럼 갈등이 격화되는 데에는 COVID-19 팬데믹 처리에 대한 국제 사회의 압력을 고려한 중국의 국경 지역 공세 강화와 인도의 분쟁 지역 교통 인프라 건설 등 여러 원인이 있다. 중국은 국경 충돌이 시작된 이후 인도와의 접경 지역에 대규모 병력을 집중시킨 것으로 보고되었으며, 분쟁은 여전히 **미해결 상황**으로 보인다. 2020년 6월 인도 정부는 민간인 데이터 수집과 중국 정부의 스파이 활동에 사용될 수 있다는 우려로 다양한 **사이버보안법**을 통해 중국 기업 ByteDance의 동영상 공유 소셜 미디어 플랫폼인 TikTok을 **금지**했다. 2020년 11월 말에는 인도 정부가 **200개 이상의 중국산 앱에 대한 금지 조치**를 단행했다. 인도 기술부 장관은 중국-인도 국경 충돌에 대응하여 이를 “디지털 충돌(Digital Strike)”로 설명했다.

이처럼 갈등이 고조되면서 양국 간의 사이버 스파이 활동도 증가했다. 우리는 2020년 인도 정부가 배후로 의심되는 해커 그룹 Sidewinder가 중국 군대와 정부 기관들을 겨냥하고 있음을 확인했다. 이들의 활동은 최근 Trend Micro **조사**에서도 확인되었다. 2020년 5월 소규모 충돌을 앞두고 PlugX 멀웨어 C2 인프라의 프로 비저닝이 눈에 띄게 증가한 것이 관찰되었는데, 그 중 상당수가 이후 인도 조직을 대상으로 하는 침입 활동에 사용되었다. 최소한 2020년 5월부터 다수의 인도 정부, 공공 기관, 국방 조직을 대상으로 한 PlugX 활동이 확인되었다. 이러한 침입 의심 사례에 대한 자세한 보고가 레코디드 퓨처 고객에게 제공된다. 중국의 사이버 스파이 활동에만 국한되는 것은 아니지만, 수년 동안 중국계 그룹들이 PlugX를 활발히 사용했다. 2020년 나머지 기간 동안 우리는 다수의 중국 정부 주도 해커 그룹이 인도 정부와 민간 기업들을 대상으로 집중적인 공격을 시도하고 있음을 확인했다.

Recorded Future Command and Control List, PlugX India, China Protest, Military, Political, Arms and Nuclear, Political Relations



© Recorded Future

그림 3: 인도-중국 간 지정학적, 군사적 긴장 고조와 일치하는 레코디드 퓨처 PlugX C2 탐지 타임라인. (출처: Recorded Future)

ShadowPad — 중국 해커 그룹들이 널리 사용하는 도구로 발전

ShadowPad는 2017년 Netsarang 침해(compromise)에서 처음 확인된 모듈형 백도어이다. 이후 FireEye가 Netsarang의 배후로 APT41 (BARIUM)을 지목했다. ShadowPad는 처음에는 APT41 전용으로 간주되었으나, 2019년 말부터 다른 중국계 그룹들이 네트워크 침입 캠페인에 ShadowPad를 사용하기 시작했다. 현재 ShadowPad는 중국 국가안전부(Ministry of State Security, MSS)와 인민해방군(People's Liberation Army, PLA) 관련 그룹들 사이에서 널리 사용되고 있는 것으로 판단된다. 그리고 ShadowPad의 관리와 업데이트를 담당하는 중앙 개발자 또는 병참 장교가 존재할 가능성이 높다.

현재 우리는 APT41, Tonto Team, Icefog, KeyBoy, Tick을 포함해 최소 5개의 중국 해커 그룹이 ShadowPad를 사용하는 것을 알고 있다. 가장 최근에는 ShadowPad 인프라가 몽골의 비즈니스 관리 제품인 Able Software 침해에 관련되었다. 이 공격에 사용된 도구는 중국계 그룹 TA428 및 LuckyMouse와 유사성이 있다. 이러한 사실들은 ShadowPad가 중국 해커 그룹들 사이에서 계속 널리 공유되고 있음을 시사한다.

2020년 9월, 미국 정부가 Chengdu 404 Network Technology라는 위장 기업으로 활동하는 중국 APT41 운영자 5명을 기소했다. 피고 중 한 명이 중국 국가안전부(MSS)와 밀접한 관계임이 드러나면서 중국 민간 업체와 위장 기업들이 MSS를 대신하여 사이버 스파이 활동을 수행하고 있음이 기정사실로 확인되었다. Tonto Team은 인민해방군(PLA), 특히 선양군사지역 기술정찰국과 관련된 것으로 드러났다. ShadowPad는 중국 해커 그룹들이 사이버 스파이 활동에 사용하는 다양한 맞춤형 기능 가운데 가장 최신 도구이다.

위협 분석

Insikt Group은 ShadowPad 감염에 사용된 네트워크 인프라를 AXIOMATICASYMPTOTE로 추적한다. 이 기술은 해더 응답, 유사한 네트워크 구성요소를 비롯한 고유한 특징을 알아낸다. 우리는 선제적 인프라 탐지, 도메인 분석, 네트워크 트래픽 분석을 사용하여 이러한 AXIOMATICASYMPTOTE 서버들이 RedEcho라는 중국계 해커 그룹의 인도 전력망 공격에 사용되고 있음을 확인했다.

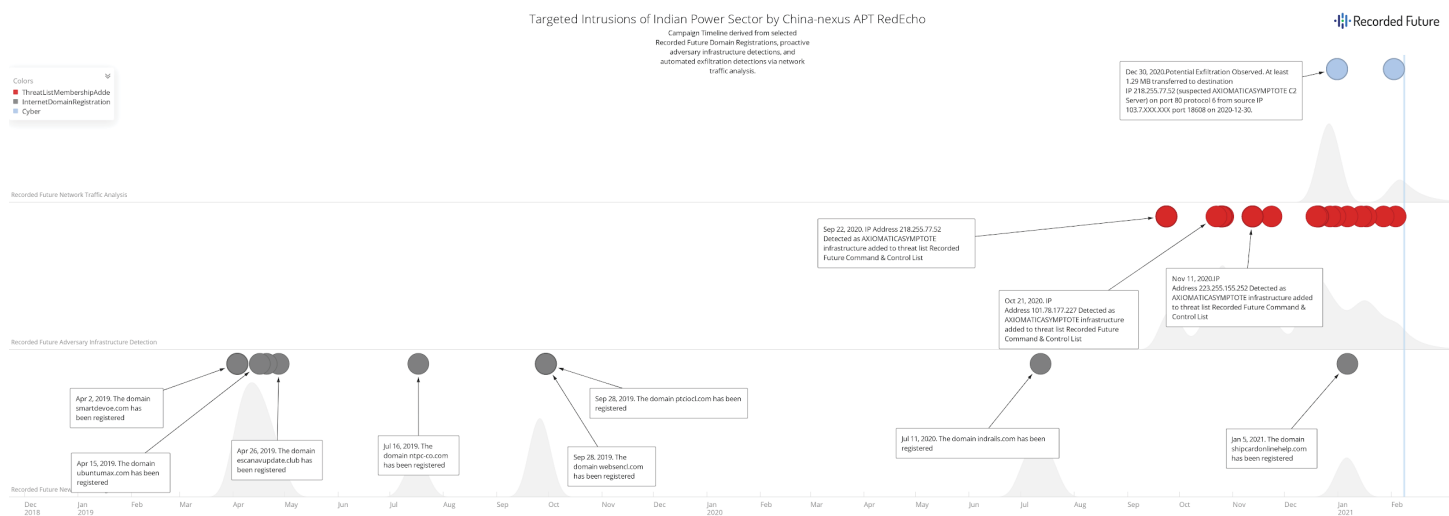


그림 4: 레코디드 퓨처 Network Traffic Analysis를 통해 신규 도메인 등록, 선제적 공격자 인프라 탐지, 타겟 네트워크의 유출(Exfiltration) 이벤트를 보여주는 RedEcho 캠페인 타임라인. (출처: Recorded Future)

RedEcho 인프라 TTP

아래 표 1에 나와있는 RedEcho AXIOMATICASYMPTOTE 서버들은 인도 발전소와 송전소들을 스프링하는 도메인으로 구성되었다. 예를 들어 ntpc-co[.]com 도메인은 인도 발전회사인 NTPC Limited의 웹사이트 ntpc[.]co[.]in의 타이포스쿼트일 가능성이 높다. 이 도메인은 2019년 7월에 처음 등록된 것으로 레코디드 퓨처 신규 도메인 등록 피드에 명시되어 있다.

FIRST REFERENCE

Domain Registration

"The domain ntpc-co.com has been registered"

Source New Domain Registrations on Jul 16, 2019, 09:00 • [Reference Actions](#)

그림 5: 레코디드 퓨처 포털의 신규 도메인 등록 레퍼런스 (출처: Recorded Future)

타이포스쿼트(Typosquat – 유명한 웹사이트의 스펠링을 조금 바꿔서 도메인 이름을 차지하는 행위) 및 브랜드 남용(Brand Abuse) 탐지는 레코디드 퓨처의 Brand Intelligence 모듈이 제공하는 여러 기능 중 하나로 공격자가 수상한 인프라 구축을 획책하는 즉시 이를 파악할 수 있도록 해준다.

AXIOMATICASYMPTOTE IP Address	Domain(s)	First Seen	Hosting Provider
101[.]78[.]177[.]227	websenc1[.]com ptciocl[.]com	2020-06-12	HKBN Enterprise Solutions HK Limited
101[.]78[.]177[.]252	ptciocl[.]com	2020-12-25	HKBN Enterprise Solutions HK Limited
210[.]92[.]18[.]132	ntpc-co[.]com	2020-12-14	EHOSTICT
218[.]255[.]77[.]52	ptciocl[.]com	2019-09-29	HKBN Enterprise Solutions HK Limited
223[.]255[.]151[.]74	websenc1[.]com	2020-11-18	HKBN Enterprise Solutions HK Limited
223[.]255[.]155[.]231	ubuntumax[.]com	2021-01-25	HKBN Enterprise Solutions HK Limited
27[.]255[.]92[.]83	ubuntumax[.]com	2021-02-06	EHOSTICT
223[.]255[.]155[.]238	www.shipcardonlinehelp[.]com	2020-10-12	HKBN Enterprise Solutions HK Limited
27[.]255[.]94[.]29	ntpc-co[.]com	2020-08-20	EHOSTICT
218[.]255[.]77[.]54	www.smartdevoef[.]com	2020-02-05	HKBN Enterprise Solutions HK Limited
223[.]255[.]151[.]85	www.smartdevoef[.]com	2020-12-19	HKBN Enterprise Solutions HK Limited
101[.]78[.]177[.]242	www.smartdevoef[.]com	2020-07-21	HKBN Enterprise Solutions HK Limited
218[.]255[.]77[.]40	ptciocl[.]com	2020-11-24	HKBN Enterprise Solutions HK Limited

표 1: 인도 전력 부문 침입에 사용된 RedEcho AXIOMATICASYMPTOTE 인프라 클러스터 목록 (최초 파악된 목록)

Insikt Group은 RedEcho 인프라를 프로파일링하고, 네트워크 지표를 **복합 객체(Composite Object)**로 보는 개념에 따라 활동 패턴을 파악했다. 확인된 침입 캠페인에서 RedEcho의 인프라 운영 방식은 다음과 같이 요약할 수 있다.

- 도메인은 WEBCC를 통해 등록되었으며 흔치 않은 ANS(authoritative name server)인 eznowdns[.]com을 사용했다.
- RedEcho 인프라는 중국 도메인 및 인프라 리셀러 cndns[.]com와 관련되었다.
- WhoisProtection WHOIS 개인정보보호 서비스를 사용했다.
- AXIOMATICASYMPTOTE 인프라는 HKBN Enterprise Solutions HK Limited (AS9381) 및 EHOSTICT (AS45382)에서 호스팅되었다.
- 인도 엔티티를 스푸핑(유사한 어휘)하거나 인도를 지칭하는 문자열이 포함된 도메인
- 일반적인 최상위 도메인(.com) 사용
- 운영 인프라에 DDNS(dynamic DNS) 도메인 사용 (자세한 내용은 아래 참조)

이러한 각각의 특징들이 RedEcho에만 국한되는 것은 아니다. 하지만 이 모드를 종합하여 전체적으로 보면 RedEcho 고유의 활동을 나타낼 수 있다. 우리는 이러한 TTP를 기반으로 하여 알려진 AXIOMATICASYMPTOTE 서버 및 인프라 클러스터 내 도메인에 대한 과거 호스팅 데이터와 겹치는 관련 가능성이 있는 추가 도메인을 파악했다.

과거 호스팅 인프라와 중복되는 도메인을 피벗하여 동일한 인도 관련 도메인 네이밍 패턴을 갖고 AXIOMATICASYMPTOTE 서버로 연결되는 RedEcho DDNS(dynamic DNS) 도메인의 추가 클러스터를 파악했다.

RedEcho 피해 대상

우리는 Recorded Future 네트워크 트래픽 분석(Network Traffic Analysis)을 바탕으로 공격자 인프라로 전송되는 네트워크 트래픽의 행동 프로파일링(behavioral profiling)을 실행했다. 이를 통해 피해 대상이 된 인도 기관들 사이에 명확하고 일관된 패턴이 있음이 확인되었다. AXIOMATICASYMPTOTE 인프라를 향한 인바운드 네트워크 활동의 대부분은 TCP 포트 443에서 SSL을 통해 이루어졌다. 또한 AXIOMATICASYMPTOTE 인프라로 가는 대량의 인바운드 트래픽이 TCP 8080을 통한 HTTP 프록시 활동과 AXIOMATICASYMPTOTE 서버에서 호스팅되는 C2 도메인에 대한 DNS 요청(UDP 53)임을 확인했다. (아래 인프라 섹션 참조)

Domain	IP Address	Comment
indiasunsung[.]com	223[.]255[.]155[.]243 180[.]150[.]226[.]216	180[.]150[.]226[.]216 — Confirmed AXIOMATICASYMPTOTE server.
ixrails[.]com	223[.]255[.]155[.]243 101[.]78[.]177[.]227	101[.]78[.]177[.]227 — Confirmed AXIOMATICASYMPTOTE server.
pandorarve[.]com	223[.]255[.]155[.]247 223[.]255[.]155[.]252	223[.]255[.]155[.]252 — Confirmed AXIOMATICASYMPTOTE server.
indrails[.]com	223[.]255[.]155[.]237	Matches infrastructure TTPs and Indian railway-themed.
escanavupdate[.]club	218[.]255[.]77[.]60	Multiple hosting overlaps within the infrastructure cluster. Likely spoofing Indian antivirus provider eScan AV.
astudycarsceu[.]net	27[.]255[.]94[.]21	Confirmed AXIOMATICASYMPTOTE server, matches infrastructure TTPs, and overlapping victimology.

표 2: 인프라 TTPs와 일치하는 추가 RedEcho 도메인

Domain	AXIOMATICASYMPTOTE IP Address
railway.sytes[.]net	223[.]255[.]155[.]235
modibest.sytes[.]net	223[.]255[.]155[.]235
indrira.ddns[.]net	218[.]103[.]197[.]112
indianrailway.hopto[.]org	223[.]255[.]155[.]235
inraja.ddns[.]net	218[.]103[.]197[.]112
railways.hopto[.]org	223[.]255[.]155[.]235

표 3: RedEcho DDNS(dynamic DNS) 도메인

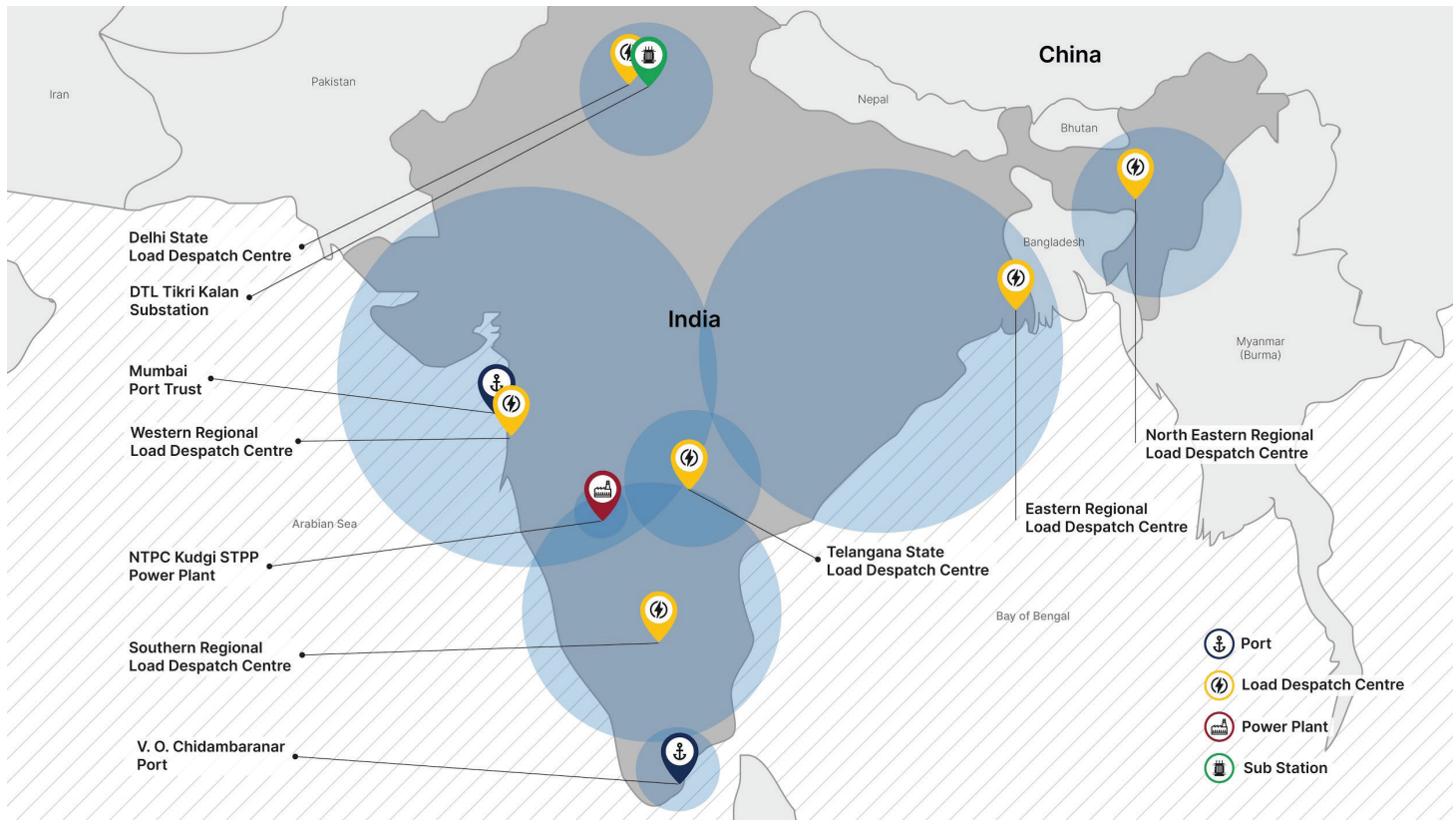


그림 6: RedEcho 피해 대상으로 의심되는 인도 전력 기관 (출처: Recorded Future, Map data ©2021 Google)

우리는 확인된 총 21개의 IP 주소에서 인도 발전 및 송전 부문 10개 기관과 해상 부문 추가 2개 기관을 파악했다. 인도 NCIIPC(National Critical Information Infrastructure Protection Center)에 따르면 12개 조직 모두가 주요 기간시설에 해당한다.

RedEcho는 인도의 5개 RLDC(Regional Load Despatch Center) 중 최소 4개와 2개의 SLDC(State Load Despatch Center)를 대상으로 네트워크 침입을 자행했다. RLDC와 SLDC는 전력 수급 균형을 통한 인도 전력망의 안정적인 실시간 통합 운영을 **담당한다**.

지역 언론은 2020년 10월 뭄바이에서 발생한 대규모 정전 사태가 SLDC의 멀웨어와 **관련**됐을 가능성이 있다고 보도한 바 있다. 현재까지 뭄바이 정전과 멀웨어 변종 간의 관련성 의혹은 입증되지 않은 상태이다. 그러나 이번에 공개된 캠페인은 인도 전력기관을 대상으로 조직적인 사이버 공격 시도가 있었음을 시사하는 추가 증거를 제공한다.

피해 대상으로 의심되는 기관	설명
Power System Operation Corporation Limited	인도 전력부(Ministry of power) 산하 정부 소유 기업
NTPC Limited	발전 및 관련 사업에 관심을 가진 인도 에너지 대기업
NTPC Kudgi STPP	발전소
Western Regional Load Despatch Centre	RLDC
Southern Regional Load Despatch Centre	RLDC
North Eastern Regional Load Despatch Centre	RLDC
Eastern Regional Load Despatch Centre	RLDC
Telangana State Load Despatch Centre	SLDC
Delhi State Load Despatch Centre	SLDC
DTL Tikri Kalan (Mundka), Delhi Transco Ltd	변전소
V. O. Chidambaranar Port	항만
Mumbai Port Trust	항만

표 4: 2020년 인도 주요 기간시설을 겨냥한 RedEcho 캠페인의 피해 대상으로 의심되는 기관 목록

인도 고전압 변전소와 석탄 화력 발전소도 RedEcho가 노린 인도 전력 기관에 포함되었다. 이러한 주요 전력 시설들을 공격 대상으로 삼은 것은 경제적 스파이 행위와는 큰 연관이 없는 반면에, 향후 중국의 전략적 목표를 지원하기 위한 사전 포석으로 네트워크 침투 가능성이 크게 우려된다.

RedEcho의 타겟 중에는 두 개의 인도 항만도 있다. 인도 주요 인프라 엔티티로 확인된 IP들이 수개월 간 집중적으로 AXIOMATICASYMPTOTE 서버의 하위집합과 통신한 것이 확인되었다. 이는 표적 공격이 진행되었음을 나타낸다. 레코디드 퓨처의 네트워크 텔레메트리에 광범위한 타겟팅의 증거는 거의 없었다.

RedEcho 배후

2020년 11월 인도 석유 가스 부문을 겨냥한 APT41/Barium이 연관된 캠페인에서 최소 3개의 인도 IP 주소가 발견되었다.

RedEcho가 노린 인도 IP 주소 중 대다수가 DDNS 도메인 (91.204.224[.]114 및 91.204.225[.]216)을 호스팅하는 2개의 AXIOMATICASYMPTOTE 서버와 통신하는 것이 관찰되었다. 이것은 도메인 bguha.serveuser[.]com과 같이 Microsoft가 이전에 보고한 APT41/Barium 캠페인과 중복되는 부분이 있다.

RedEcho DDNS 도메인 railway.sytes[.]net과 이전에 보고된 APT41/Barium 클러스터 간에도 과거 호스팅 중복이 존재한다. 그러나 Microsoft가 Barium의 것으로 지목한 여러 DDNS 도메인이 이전에 Trend Micro 보고서에서 Tonto Team 위험 활동과 관련되어 있었음을 주목할 필요가 있다. Trend Micro는 보고서에서 Tonto Team이 인도 석유 가스 에너지 산업을 공격 대상으로 삼았다고 지적했다.

이전에 탐지된 APT41/Barium 활동과 일부 겹치는 부분이 있고 Tonto Team 활동과도 추가적으로 중복될 수 있는 부분이 있지만, 현재로서는 인도 전력 기관을 대상으로 한 이번 침투가 이들의 소행이라고 단정할만한 충분한 증거가 없다. 따라서 이들과 밀접하게 연관되어 있으나 별개의 활동 그룹인 RedEcho로 계속해서 추적을 진행 중이다.



그림 7: 피해 대상으로 의심되는 NTPC Kudgi STPP의 위치 (출처: Imagery ©2021 CNES/Airbus, Maxar Technologies, Map data ©Google)

최신 공격 수법 파악

레코디드 퓨처의 [Security Intelligence Graph](#)는 방대한 양의 오픈소스, 다크웹, 기술 데이터와 최신 공격 수법에 정통한 보안 분석가의 전문 지식이 결합되어 계속 발전한다. 최신 Network Traffic Analysis 분석은 사용자가 검증된 기술 데이터 소스에서 침입 의심 활동을 간파하고 추적할 수 있도록 해준다. Insikt Group과 Data Science에서 개척된 Network Traffic Analysis가 이 연구의 핵심 기반이 되었다.

최근 [2020 공격자 인프라 보고서](#)에서 언급된 바와 같이 우리는 패시브 스캐닝과 액티브 스캐닝 방식을 결합하여 악성 인프라를 선제적으로 탐지한다. 이러한 방식으로 2020년에 위협 행위자가 사용하는 10,000개 이상의 서버를 파악했다. 일련의 필터와 알고리즘을 적용하여 악성 서버와 관련된 의심스러운 네트워크 트래픽을 찾아내고 특정 대상을 겨냥한 침입 활동을 식별한다. 사용자는 레코디드 퓨처 플랫폼에서 Intelligence Card를 통해 SecurityTrails와 같은 파트너 데이터를 사용하여 이러한 정보를 보강(enrich)할 수 있다. 그리고 [레코디드퓨처의 'Threat Intelligence 모듈' 또는 'SecOps 모듈'](#) 사용자는 예상되는 공격자 캠페인을 효율적으로 매핑할 수 있다.

대응 방안 (Mitigations)

RedEcho 관련 활동을 탐지하고 완화하기 위해 다음과 같은 조치를 취할 것을 사용자에게 권고한다.

- 기존 IDS(intrusion detection systems), IPS(intrusion prevention systems) 또는 기타 네트워크 방어 메커니즘이 목록에 나와있는 외부 IP 주소 및 도메인 연결 시도를 경고하고 차단하도록 설정할 것.
- 레코디드퓨처의 C2-SCF(Command and Control - Security Control Feed)는 악성 서버 구성을 선제적으로 탐지하고 로깅한다. C2 목록에는 RedEcho와 중국 정부 해커그룹이 사용하는 도구(예: AXIOMATICASYMPTOTE)가 포함된다. 레코디드 퓨처 클라이언트는 이러한 C2 서버에 대한 경고 및 차단을 설정하여 침입을 탐지하고 방어할 수 있다.
- 다수의 국가 차원 해커 그룹과 돈을 목적으로 하는 해커 그룹이 네트워크 침입 활동에서 DDNS 도메인을 계속 사용하고 있다. DDNS 서브도메인과 관련된 모든 TCP/UDP 네트워크 트래픽을 차단하고 로깅할 것. ([DNS RPZ](#) 또는 이와 유사한 것을 사용)
- [eznowdns\[.\]com](#)을 ANS(authoritative name server)로 사용하는 모든 도메인을 차단하고 로깅할 것. ([DNS RPZ](#) 또는 이와 유사한 것을 사용)
- 레코디드 퓨처 Threat Intelligence, Third-Party Intelligence, SecOps Intelligence [모듈](#) 사용자는 Network Traffic Analysis 실시간 분석을 모니터링하여 자사 또는 공급업체, 파트너와 관련된 침입 의심 활동을 파악할 수 있다.
- 레코디드 퓨처 Brand Intelligence [모듈](#)을 통해 타이포스쿼트(typosquat) 도메인과 같은 도메인 남용을 모니터링할 것.

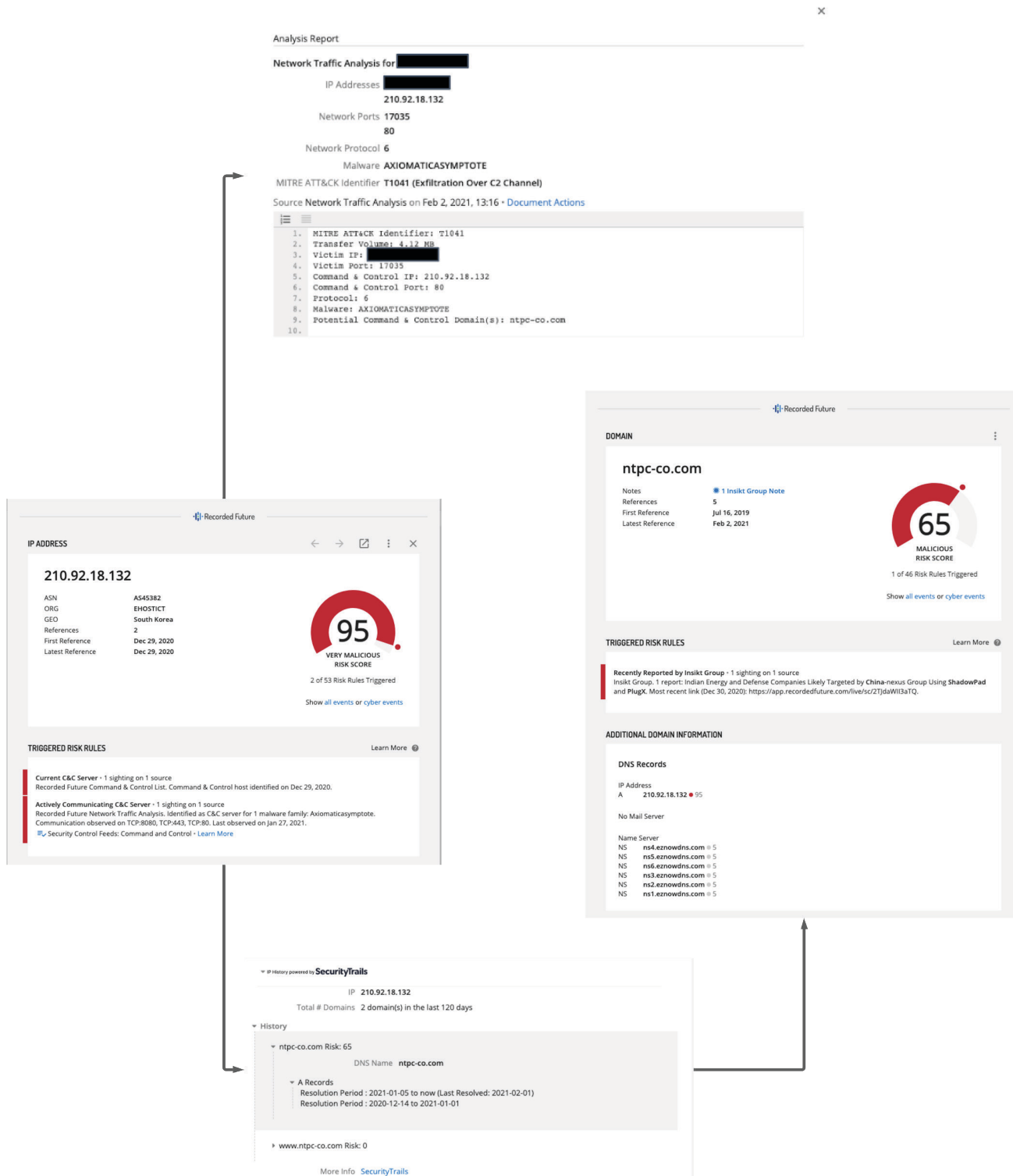


그림 8: 레코디드 퓨처 포털에서 기술 데이터 세트 간 피벗(Pivot) 실행 (출처: Recorded Future)

향후 전망

이 연구에서 우리는 2020년 중반부터 관찰된 인도 전력 부문을 대상으로 한 일련의 의심스러운 침입을 분석했다. 이 침입은 RedEcho로 명명된 중국계 해커 그룹에 의해 수행되었다.

RedEcho는 ShadowPad C2 서버들로 이루어진 XIOMATICASYMPTOTE 인프라를 활발히 사용했다. XIOMATICASYMPTOTE는 APT41/Barium, Tonto Team, Icefog Cluster, KeyBoy, Tick 등 여러 중국계 해커 그룹 간에 공유되는 인프라이다.

이 침입은 역시 AXIOMATICASYMPTOTE 인프라를 사용한 2020년 중국 해커 그룹의 인도 에너지 섹터 공격과 공통점이 있다. 인도 전력 시스템을 주요 타겟으로 삼았다는 점에서 인도의 에너지 인프라에 접근하려는 중국의 꾸준한 전략적 의도를 엿볼 수 있다. RLDC(Regional Load Despatch Center) 네트워크 침투는 경제적 목적의 스파이 행위라기 보다는 다음과 같은 다양한 목적을 염두에 둔 사전 포석과 전략적 의도로 평가된다.

- 세력 과시를 위한 강력한 메시지 전달
- 외교적 대립 상황에서 영향력 공작(Influence Operations)을 통한 여론 물이
- 주요 인프라에 대한 향후 사이버 공격 작전 지원

계속해서 양국 간 긴장이 고조됨에 따라 RedEcho와 같은 중국 해커 그룹이 국가의 전략적 이해 관계에 따라 사이버 작전을 지속적으로 수행할 것으로 예상된다. 양국 모두 코로나 바이러스 팬데믹 이후의 경제 회복이 우선이겠지만 국경 분쟁과 관련된 거센 발언과 충돌이 증가한다는 것은 각 정부 내에 불신과 불확실성이 존재함을 시사한다. 또한 중국은 다른 국가들, 특히 일대일로(BRI, Belt and Road Initiative) 사업의 범위에 있는 나라들에 대해 계속해서 영향력을 행사할 가능성이 높으며, 이는 전략적 이익 강화를 목표로 한 사이버 작전 증가로 이어질 수 있다.

부록 — 지표

당사 Insikt Group Github 저장소에서 아래 나열된 지표를 확인할 수 있다. <https://github.com/Insikt-Group/Research> (RedEcho - 2021년 2월)

```
ntpc-co[.]com
websencl[.]com
ptciocl[.]com
ubuntumax[.]com
www.shipcardonlinehelp[.]com
www.smartdevoe[.]com
www.astudycarsceu[.]net
www[.]indiasunsung[.]com
ixrails[.]com
pandorarve[.]com
indrails[.]com
escanavupdate[.]club
railway.sytes[.]net
modibest.sytes[.]net
indrra.ddns[.]net
indianrailway.hopto[.]org
inraja.ddns[.]net
railways.hopto[.]org
101[.]78[.]177[.]227
101[.]78[.]177[.]252
210[.]92[.]18[.]132
218[.]255[.]77[.]52
223[.]255[.]151[.]74
223[.]255[.]155[.]231
223[.]255[.]155[.]235
223[.]255[.]155[.]238
27[.]255[.]94[.]29
27[.]255[.]94[.]21
27[.]255[.]92[.]83
223[.]255[.]151[.]85
101[.]78[.]177[.]242
218[.]255[.]77[.]40
218[.]255[.]77[.]54
223[.]255[.]155[.]243
180[.]150[.]226[.]216
223[.]255[.]155[.]247
223[.]255[.]155[.]252
223[.]255[.]155[.]237
218[.]255[.]77[.]60
```

레코디드 퓨처 위협 활동 그룹 및 멀웨어 분류

레코디드 퓨처의 연구기관인 Insikt Group은 중국, 이란, 러시아, 북한의 국가 차원 해커 집단과 러시아, 독립국가연합(CIS), 중국, 이란, 브라질의 사이버 범죄자(개인 및 그룹)를 중심으로 위협 행위자와 그들의 활동을 추적한다. 우리는 위협 행위 집단을 추적하고 가능한 경우 이들의 배후에 있는 국가, 조직, 관련 기관을 파악하고자 한다.

주요 분석 범위는 다음과 같다.

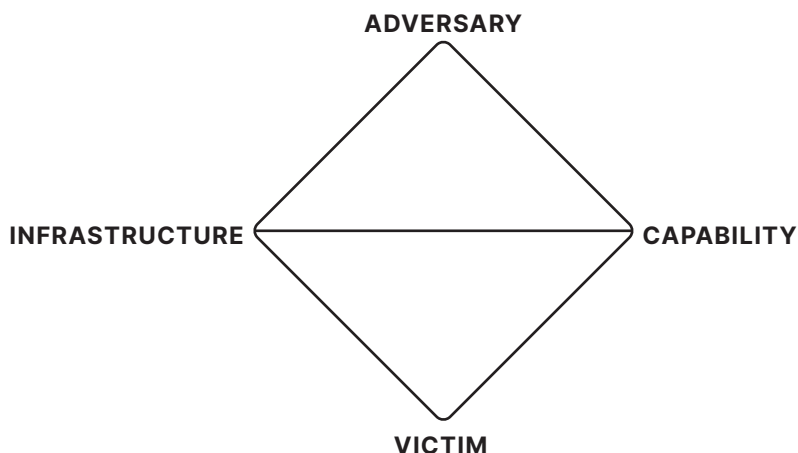
- 정부 조직 및 정보 기관, 관련 연구소, 파트너, 업계 협력자, 프록시 엔티티, 개별 위협 행위자
- 레코디드 퓨처가 파악한 국가 주도 해커 그룹 (RedAlpha, RedBravo, Red Delta, BlueAlpha 등) 및 기타 업계 유명 해커 그룹
- 레코디드 퓨처가 새롭게 파악하여 명명한 사이버 범죄자 개인 및 집단
- 최신 멀웨어, 널리 보급되고 상품화된 멀웨어 (commodity malware)

Insikt Group은 Security Intelligence Graph의 침입 분석 다이아몬드 모델(Diamond Model of Intrusion Analysis)에서 최소 중간 신뢰도로 3개 이상의 포인트에 해당하는 데이터를 확보했을 때 새로운 해커 그룹 또는 캠페인에 이름을 붙인다. 배후에서 조종하는 인물이나 조직을 특정할 수 있는 경우에만 이를 위협 행위자와 연결할 수 있다. 이 정도의 공격자 데이터가 없는 경우에는 해당 활동을 캠페인으로 다루어 보고서를 작성한다. 기존 그룹의 활동임이 확실한 경험적 증거가 있을 경우, 특정 그룹에 대해 가장 널리 알려진 이름을 사용한다.

Insikt Group은 새로운 국가 주도 해커 그룹 또는 캠페인에 간단한 색상 및 알파벳 명명 규칙을 사용한다. 색상은 아래 표시된 해당 국가의 국기 색상에 해당한다. 국가 주도 해커 그룹이 신규로 파악되면 색상/국가 표시가 추가될 것이다.

신규 파악된 사이버 범죄 집단에 대해서는 그리스 문자에 해당하는 명명 규칙을 사용한다. 특정 국가와 관련된 범죄 단체가 식별된 경우 국가 색상을 적용하고, 해당 그룹이 특정 정부 조직과 관련될 경우 해당 엔티티와 연결한다.

Insikt Group은 새롭게 파악된 멀웨어에 이름을 붙일 때 수학적 용어를 사용한다.



CHINA



IRAN



NORTH KOREA



RUSSIA

레코디드 퓨처에 대하여

레코디드 퓨처(Recorded Future)는 세계 최대 엔터프라이즈 보안 인텔리전스 제공업체이다. 레코디드 퓨처는 지속적이고 광범위한 자동 데이터 수집 및 분석에 전문가 분석을 결합하여 적시에 정확하고 실행 가능한 인텔리전스를 제공한다. 레코디드 퓨처는 끊임없이 증가하는 혼란과 불확실성의 세계에서 조직이 위협을 신속하게 파악하고 탐지하는 데 필요한 가시성을 제공한다. 조직은 이러한 가시성을 확보함으로써 선제적 대응을 통해 공격을 저지하고 사용자, 시스템, 자산을 보호하여 비즈니스를 안정적으로 수행할 수 있다. 레코디드 퓨처는 전세계 1,000개 이상의 기업과 정부 기관에서 신뢰받고 있다.

자세한 사항은 www.recordedfuture.com과 Twitter @RecordedFuture에서 확인할 수 있다.