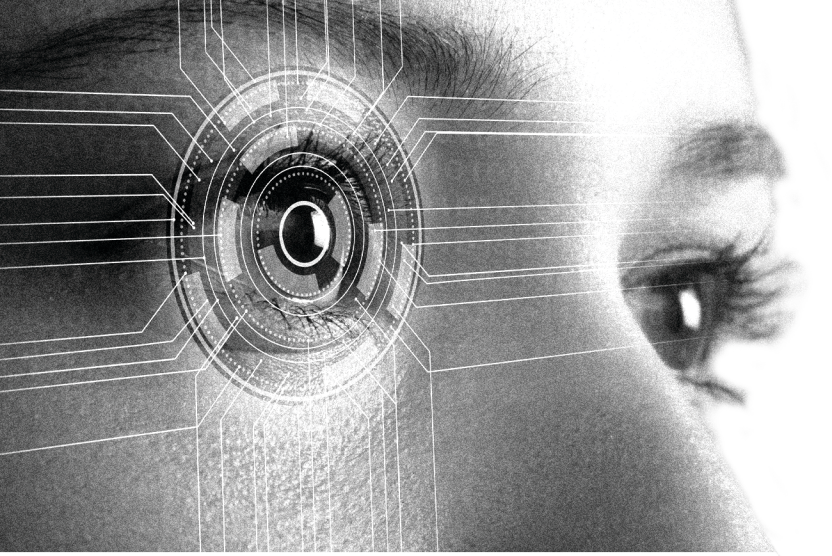
CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

September 21, 2021

중국계 해커 그룹 TAG-28, 인도 언론 The Times Group과 정부기관 UIDAI (Aadhaar)에 Winnti 멀웨어 공격 시도



Recorded Future®

요약

인도는 중국 정부가 배후에 있는 해커 그룹들로부터 끊임 없이 사이버 공격을 받고 있다. 올해 초 Insikt Group은 중국-인도 국경 분쟁으로 양국 관계가 급격히 악화된 가운데 RedEcho가 인도 주요 국가 기반 시설을 겨냥한 사이버 공격을 시도한 상황을 보고한 바 있다. 또한 최근에는 인도의 핵, 우주, 방위 사업 관련 국영 기업을 대상으로 한 새로운 RedFoxtrot 작전이 파악되었다.

인도 기관들을 대상으로 한 중국의 사이버 공격이 이어지는 가운데 우리는 "The Times Group"으로 알려진 인도 미디어 대기업 Bennett Coleman And Co Ltd(BCCL)와 인도 국가 주민증사업을 담당하는 정부 기관인 UIDAI(Unique Identification Authority of India), 인도 마디아프라데시 주 경찰서를 표적으로 하는 의심스러운 침입을 추가로 확인했다. UIDAI는 10억 명 이상의 인도 시민에 대한 개인 생체 정보가 담긴 국가 데이터베이스(일명 "Aadhaar")를 관리하는 정부 기관이다. 우리는 이러한 침입을 자행한 해커 그룹을 TAG-28으로 임시 명명하고 추적했다 [1].

[1] Insikt Group은 RedFoxtrot과 같은 새로운 위협 활동 그룹 또는 캠페인에 이름을 붙인다. 일반적으로 분석가가 다이아몬드 침입 분석 모델(Diamond Model of Intrusion Analysis)에서 최소한 중간 신뢰도의 3개 이상의 포인트에 해당하는 데이터를 확보했을 경우에 명명을 한다. 때때로 TAG-28과 같은 임시 명칭을 사용하여 중요한 활동을 보고하기도 한다. 새롭고 중요한 활동이지만 기존 그룹에 매핑되지 않고, 아직 기성 활동 그룹으로 분류되거나 병합되지 않은 경우이다.

중국 해커들의 언론사 해킹은 어제 오늘 일이 아니다. 2013년에 New York Times, Washington Post, Bloomberg News가 중국에 대한 비판적인 기사를 보도한 후에 중국 해커 그룹의 정보 수집 타겟이 되었다. 그 후 2014년에는 홍콩의 민주화 언론 매체가 우산 운동 시위 기간에 해킹의 타겟이 되었다. 언론 매체를 대상으로 한 중국 해커 그룹의 공격은 오래 전부터 이어져 왔으며, 가장 최근의 사례가 BCCL을 노린 TAG-28의 Winnti 캠페인이다..

주요 내용

- TAG-28은 Aadhaar 데이터베이스를 노리고 UIDAI를 표적으로 삼았을 가능성이 높다. 대량의 개인 식별 정보(PII) 데이터 세트는 국가차원의 지원을 받는(state-sponsored) 해커들에게 특히 가치가 있다. 정부 관리와 같은 고급 타겟을 식별하거나 사회 공학 공격을 시도하는 데 이러한 데이터를 활용할 수 있기 때문이다.
- The Times Group의 매체 영향력과 "인도-중국 전쟁"에 대한 지속적인 보도를 감안할 때, TAG-28의 BCCL 해킹은 중국이나 중국 고위층에 불리한 기사를 사전에 모니터하고 언론인과 기사 소스를 감시하려는 의도로 보인다.
- TAG-28이 중국 정보기관 작전 지원을 위해 언론 매체를 해킹하여 직접적으로 기사를 수정하거나 삭제할 가능성은 적다.
- 2021년 8월 초 현재 레코디드 퓨처 데이터에 따르면 인도 기관 및 기업을 대상으로 한 중국 정부 차원의 사이버 공격은 2019년에서 2020년 사이에 120% 증가하였으며, 2021년에는 전년도에 비해 261% 증가한 것으로 나타났다. 이러한 추세는 최근 몇 년 동안 인도에 대한 중국의 전략적 관심이 증가하고 있음을 보여준다.

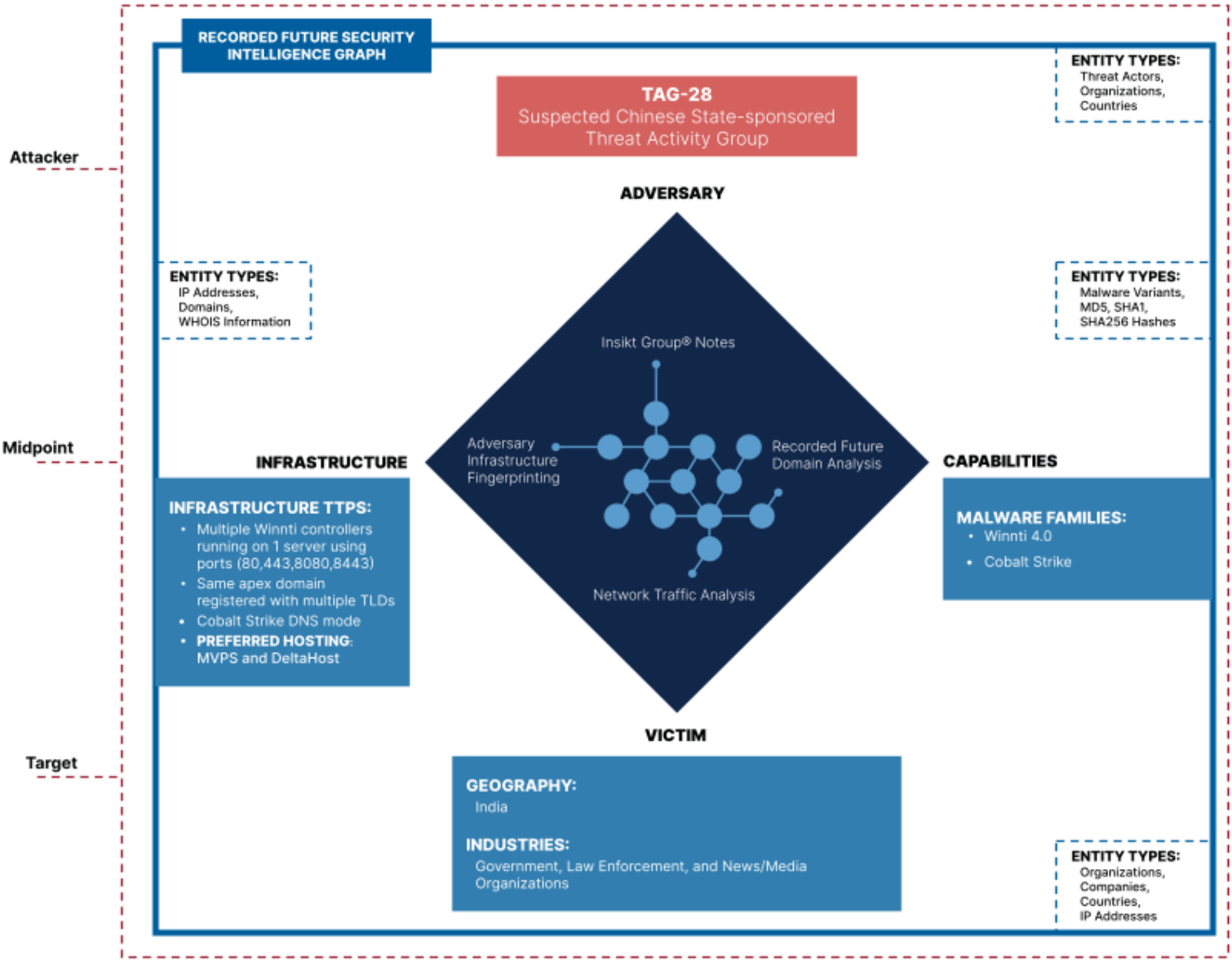


그림 1: *TAG-28 TTP 다이아몬드 모델 (출처: Recorded Future)*

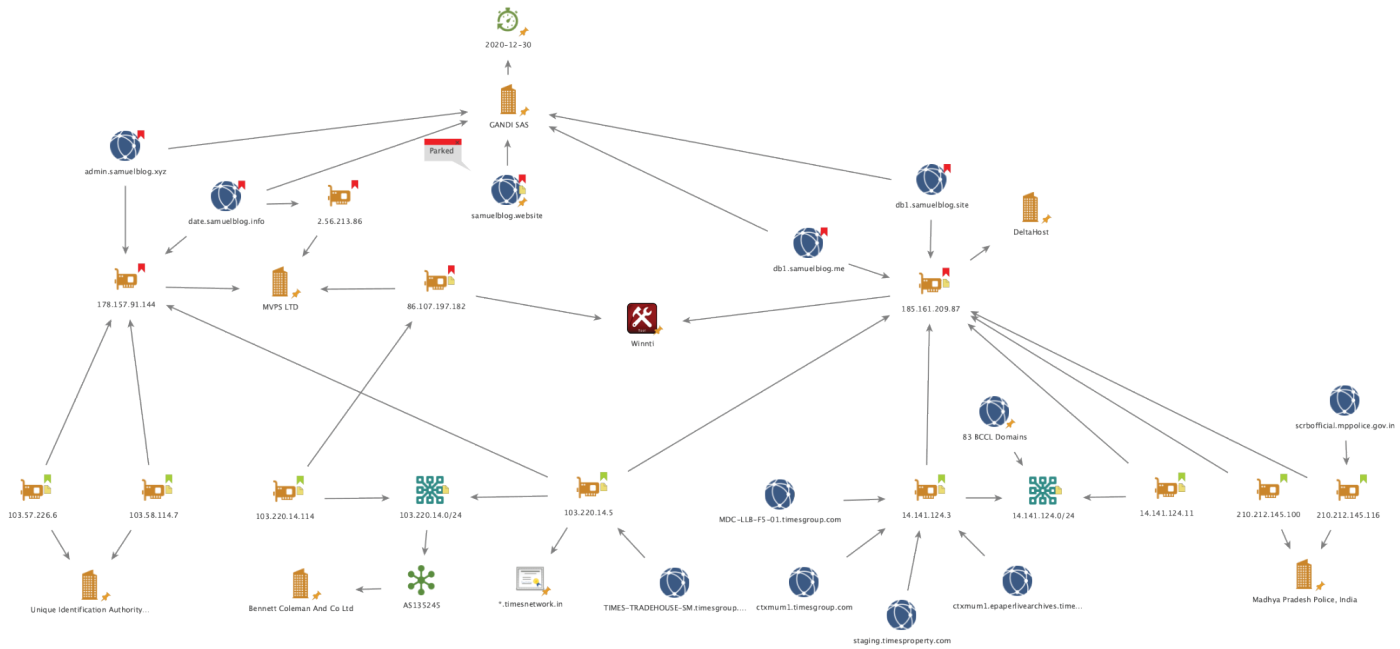


그림 2: *BCC과의 통신에 사용된 TAG-28 인프라 (출처: Recorded Future)*

위협 분석

RedEcho, RedFoxtrot, TAG-26[2], and TAG-27[3]에 대한 Insikt Group 보고서에서 알 수 있듯이 2020년 초부터 중국 정부 배후 해커 그룹들의 인도 조직 해킹 활동이 급증하는 것이 확인되었다.

Insikt Group은 악성 C2(command and control) 탐지 기법과 Recorded Future NTA(Network Traffic Analysis) 데이터를 조합하여 2개의 Winnti 멀웨어 C2 서버와 BCCL 인프라 간의 의심스러운 네트워크 트래픽 패턴을 파악했다.

BCCL(Bennett Coleman And Co Ltd) 해킹

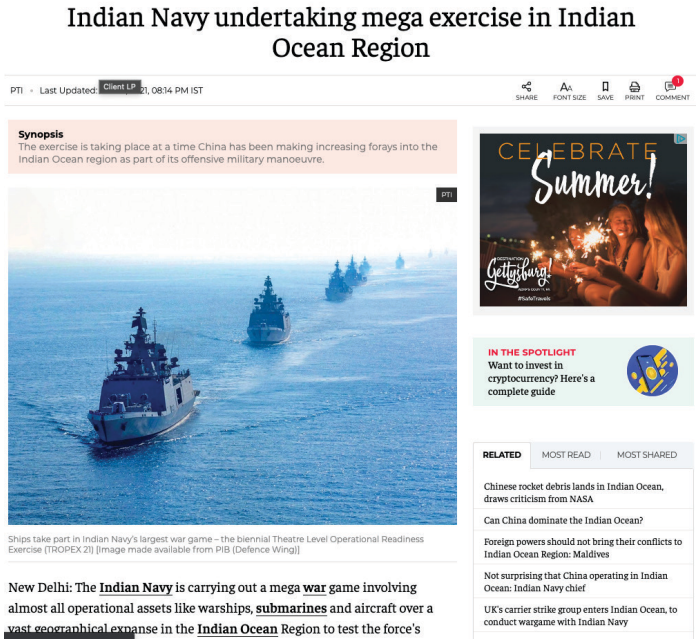
Insikt Group은 2021년 2월부터 8월 사이에 2개의 Winnti C2 서버(185.161.209[.]87 및 IP 86.107.197[.]182) 및 Cobalt Strike C2(178.157.91[.]144)의 지속적인 네트워크 통신에서 BCCL에 할당된 4개의 IP를 식별했다. 구체적으로 어떤 데이터에 액세스했는지 확인할 수는 없지만 BCCL 네트워크에서 악성 인프라로 약 500MB의 데이터가 유출되는 것을 관찰했다.

타겟 인프라는 BCCL이 다음과 같은 이유로 운영하는 것으로 보인다.

- 타겟 IP 중 2개인 103.220.14[.]5 및 103.220.14[.]114는 BCCL에 등록된 자율 시스템(Autonomous System) AS135245으로 어드버타이즈된다.
- 다수의 BCCL 도메인 네임이 타겟 IP 중 2개(103.220.14[.]5및 14.141.124[.]3)와 연결된다.
- 타겟 IP 103.220.14[.]5는 BCCL 도메인 *.timesnetwork[.]in에 대한 SSL 인증서를 제공한다.
- TCP 포트 264에서 IP 103.220.14[.]5를 사용하는 CheckPoint 방화벽은 디바이스 호스트네임 TIMES-TRADEHOUSE-SM.timesgroup[.]com을 리턴한다.
- UDP 포트 53에서 IP 14.141.124[.]3을 사용하는 DNS resolver는 호스트네임 MDC-LLB-F5-01.timesgroup[.]com을 리턴한다.

일반에 "The Times Group"으로 알려진 BCCL은 뭄바이에 본사를 둔 민간 기업으로 발행부수 기준 세계 최대 영어 신문 중 하나인 Times of India를 발행한다. BCCL은 출판, 텔레비전, 인터넷, 라디오를 포함한 다양한 매체를 운영한다. Times of India와 그 자매지들은 인도-중국 긴장에 대한 분석 기사를 빈번하게 게재하고 있으며, 2021년 3월 초에는 RedEcho의 인도 전력 기관 해킹에 대한 Insikt Group 보고서를 기사화했다.

[2] Recorded Future 고객 전용 자료
[3] Recorded Future 고객 전용 자료


Indian Navy undertaking mega exercise in Indian Ocean Region

PTI • Last Updated: [redacted], 08:14 PM IST

SHARE FONT SIZE SAVE PRINT COMMENT

Synopsis
The exercise is taking place at a time China has been making increasing forays into the Indian Ocean region as part of its offensive military manoeuvre.

Ships take part in Indian Navy's largest war game – the biennial Theatre Level Operational Readiness Exercise (TROPEX 21) [Image made available from PIB (Defence Wing)]

New Delhi: The **Indian Navy** is carrying out a mega **war** game involving almost all operational assets like warships, **submarines** and aircraft over a vast geographical expanse in the **Indian Ocean** Region to test the force's

RELATED | MOST READ | MOST SHARED

- Chinese rocket debris lands in Indian Ocean, draws criticism from NASA
- Can China dominate the Indian Ocean?
- Foreign powers should not bring their conflicts to Indian Ocean Region: Maldives
- Not surprising that China operating in Indian Ocean: Indian Navy chief
- UK's carrier strike group enters Indian Ocean, to conduct wargame with Indian Navy

***그림 3**: 인도양 지역에서 훈련 중인 인도 해군: 이 기사는 중국이 군사 훈련의 일환으로 인도양 진출을 확대하고 있을 당시에 실시할 예정으로 계획된 인도 해군 훈련에 대해 설명한다. 2021년 2월 10일 게재. (출처: India Times)*


View: China, Turkey and Pakistan's unholy nuclear nexus and its global ramifications

By Dr. Nalin Kumar Mohapatra, ET CONTRIBUTORS • Last Updated: Feb 11, 2021, 01:23 PM IST

SHARE FONT SIZE SAVE PRINT COMMENT

Synopsis
As has been observed by US Office of the Secretary of Defense in its annual report to the Congress on Military and Security Developments Involving the People's Republic of China 2020', "PLA to develop the capability to project power outside China's borders and immediate periphery to secure the PRC's growing overseas interests and advance its foreign policy goals."

China's President Xi Jinping shakes hands with Pakistan's Prime Minister Imran Khan before a meeting at the Great Hall of the People on April 28, 2019 in Beijing, China

Do also read the rejoinder by Sakir Ozkan Torunlar, Ambassador of Turkey to India, at the end of the piece.

NEW DELHI: The existing unholy nexus among **China**, Turkey and **Pakistan** in the clandestine nuclear program is posing a serious threat to both regional and global security. What is required is that international institutions like the UN and IAEA take strong punitive measures against Beijing, Ankara and Islamabad for their illegal and clandestine activities in the nuclear weaponisation process.

Along with the Covid-19 crisis which is posing a threat to global security, another issue which is causing equal alarm and concerns in the global community is the nexus between Turkey and Pakistan, two rogue states in the field of nuclear weaponisation process. Along with these two, China and **North Korea** are also involved in the illicit transfer of nuclear technologies

RELATED | MOST READ | MOST SHARED

- China must honour legally binding UNCLOS verdict on South China Sea
- Why is China facing record floods?
- Australia takes China to WTO
- China says US revoking of China apps ban a 'positive step'
- China announces Didi cybersecurity investigation
- China challenge for India, the world

***그림 4:** 전망: 중국, 터키, 파키스탄의 사악한 핵 연결고리와 글로벌 파급효과: 이 기사는 중국과 터키, 파키스탄의 핵 관계를 세계 안보에 대한 심각한 위협으로 지적하고 중국에 대한 강력한 징벌적 조치를 촉구한다. 이 기사는 또한 2020년 2월 인도 해군이 원자력 산업에 사용되는 것으로 여겨지는 하드웨어를 싣고 중국에서 파키스탄으로 향하는 선박을 요격했다고 인용한다. 2021년 2월 11일 게재. (출처: India Times)*

중국계 해커 그룹(APT41, APT12)의 언론 매체 해킹이 여러 차례(1,2), 있었는데 가장 크게 이슈가 되었던 사건은 2013년 APT12의 New York Times 해킹이었다. 보고된 바에 따르면 APT41은 개인 사용자를 추적하고 언론 매체를 감시할 수 있는 인프라를 갖추고 있을 가능성이 있다. New York Times는 2013년 APT12 공격 발생 시점이 중국 지도부에 대한 기사 보도와 맞물린다는 점에서 연관성을 주장한다.

데이터 유출의 대부분이 The Economic Times의 미 해군 인도양 순찰에 대한 보도 시점에 발생했다. The Economic Times(Times Group의 자회사)는 Insikt Group이 BCCL에 대한 해킹 활동을 탐지하기 며칠 전에 "인도 중국 전쟁" 하위 섹션에 2개의 기사를 게재했다. 그림 3과 4에 표시된 두 기사와 최근에 발표된 기사는 중국 정부에 적대적인 것으로 간주될 수 있다. 초기 해킹과 데이터 유출이 해군 관련 기사가 보도된 시점과 일치한다는 점에서 공격 의도에 대한 정황 증거를 엿볼 수 있다. 하지만 TAG-28이 미디어 그룹을 해킹하여 인도양 해군 작전에 대한 정보를 수집하고 중국에 불리한 보도를 모니터하려는 목적이 있었다고 보는 것도 그럴듯하다.

UIDAI 해킹

BCCL 해킹에 사용된 인프라를 조사하는 도중에 인도 Aadhaar ID 카드 시스템을 감독하는 UIDAI가 지속적으로 해킹되고 있음이 파악됐다. 2021년 6월 10일에서 7월 20일 사이에 UIDAI로 등록된 2개의 IP가 BCCL, 178.157.91[.]144 해킹에 사용된 것으로 의심되는 Cobalt Strike C2 서버와 통신하는 것이 관찰되었다. UIDAI 네트워크에서 나가는 데이터 전송 규모는 보통 수준이었다. 10MB 미만의 데이터가 유출되었고 약 30MB가 유입되었는데, 이는 공격자 인프라에서 추가 악성 도구가 배포되었음을 나타낼 수 있다.

UIDAI는 Aadhaar 국가 주민증 데이터베이스를 담당하는 인도 정부 기관이다. 여기에는 10억 명 이상의 인도 시민에 대한 개인 식별 및 생체 정보가 들어있다. 일부에서는 Aadhaar 데이터베이스 자체에 논란의 여지가 있다고 지적한다. 시스템에 저장된 방대한 개인 데이터가 타국 정부 해커와 범죄 동기가 있는 공격자 모두에게 매력적인 타겟이 되기 때문이다. 실제로 Aadhaar 시스템은 데이터 유출과 해킹 피해를 입은 전력이 있다(1, 2, 3). 악성 소프트웨어로 시스템을 익스플로잇하여 가짜 신분증을 만든 사례, 보안되지 않은 API로 인해 데이터베이스가 완전히 노출된 사례 등이 그것이다

TAG-28이 Aadhaar 데이터베이스를 노리고 UIDAI를 해킹했을 가능성이 있다. 방대한 PII 데이터 세트는 고급 정보을 가진 타겟(예: 정부 관리) 식별, 정찰, 사회 공학 공격, 기타 데이터 소스 강화 등 다양한 용도로 국가 차원 해커 및 범죄 집단 모두에게 가치가 있다.

마디아프라데시 주 경찰 해킹

우리는 레코디드 퓨처 NTA 데이터를 통해 2021년 6월 1일 포트 80으로 Winnti C2 IP 185.161.209[.]87과 통신하는 MPP(Madhya Pradesh Police) IP를 파악했다. 해당 MPP IP는 SCRB(State Crime Records Bureau) 웹사이트(scrbofficial.mppolice.gov[.]in)와 연결되는데, 이 웹사이트는 SCRB에서 운영하는 다양한 웹 및 모바일 애플리케이션에 대한 링크를 제공한다. Insikt Group은 이어서 2021년 7월 27일부터 최소 8월 9일까지 다른 SCRB IP인 210.212.145[.]100과 185.161.209[.]87 간의 추가적인 네트워크 활동을 관찰했다. 우리는 제한된 가시성을 토대로 해당 기간 동안 MPP와 Winnti 서버 간에 5 MB 이하의 데이터 전송을 확인했다.

마디야프라데시 주 총리 Shivraj Singh Chouhan은 2020년 6월 라다크 지역에서 중국군과의 격렬한 국경 충돌 이후 중국을 비난하면서 주민들에게 중국 제품 불매를 촉구했다. 언론과 대중은 곧바로 인도 집권 여당인 BJP(Bharatiya Janata Party)를 중국 공산당(CCP)에 비유하여 "두 당 사이에 엄청난 유사점이 있다"고 말했던 Chouhan의 2016년 트윗을 지적했는데, 이는 중국에 대한 그의 명확한 입장 변화를 보여준다.

멀웨어 및 인프라

Insikt Group은 2개의 Winnti C2(185.161.209[.]87 및 86.107.197[.]182)와 TAG-28이 운영하는 Cobalt Strike C2(178.157.91[.]144)를 확인했다.

Winnti 멀웨어는 과거 APT41/Barium과 APT17을 비롯한 여러 중국계 해커 그룹이 사용했으며, 일반적으로 중국 국가안전부(Ministry of State Security, MSS) 산하 민간 해커 조직들과 관련이 있다.

2020년 9월, 미국 법무부는 Winnti 멀웨어로 전 세계 100개 이상의 조직을 해킹한 혐의로 APT41과 관련된 5명의 중국인을 기소했다. Winnti 멀웨어를 사용하는 모든 공격을 단일 "Winnti" 그룹 소행으로 클러스터링하는 것은 불충분하다. 여러 그룹들이 기능을 공유하고 Winnti 사용자의 타겟과 작동 방식이 다양하기 때문이다.

C2 IP	최초 확인 날짜	포트	호스팅 프로바이더
Winnti 185.161.209[.]87	March 11, 2021	80, 443, 8080, 8443	Zemlyaniy Dmitro Leonidovich (DeltaHost)
Winnti 86.107.197[.]182	April 8, 2021	443, 8443	MVPS LTD
Suspected Cobalt Strike 178.157.91[.]144	June 10, 2021	443, 53	MVPS LTD

표 1: *이 캠페인에서 TAG-28이 사용하는 악성 인프라*

우리는 C2 IP를 중심으로 여러 연결 도메인을 확인했다. 모든 도메인은 등록기관 Gandi SAS를 사용하여 2020년 12월 30일에 등록되었으며 동일한 Apex 도메인 "samuelblog"를 공유했으며 등록 국가에 "KE"(케냐를 나타냄)를 사용했다.

- samuelblog[.]me
- samuelblog[.]site
- samuelblog[.]info
- samuelblog[.]website
- samuelblog[.]xyz

추가 4개의 하위 도메인이 표 1에 나열된 동일한 C2 인프라로 확인되었다. 하위 도메인 이름을 놓고 보면 공격자가 데이터베이스 액세스, 어드민 패널 또는 기타 유사한 서비스에 사용되는 호스트 네임을 가장했을 가능성이 있다.

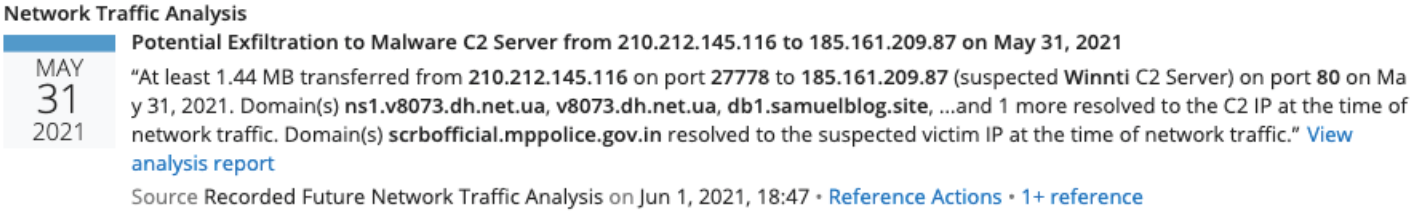


그림 5: *MPP IP와 Winnti C2 185.161.209[.]87이 관련된 레코디드 퓨처 NTA 이벤트. (출처: Recorded Future)*

Sub Domain	IP Resolved
db1.samuelblog[.]me	185.161.209[.]87
db1.samuelblog[.]site	185.161.209[.]87
date.samuelblog[.]info	2.56.213[.]86
	178.157.91[.]144
admin.samuelblog[.]xyz	178.157.91[.]144

표 2: *TAG-28 C2 하위 도메인*

DNS를 통한 Cobalt Strike C2 파악

2021년 1월 4일에서 2월 25일 사이에 도메인 ns1.samuelblog[.]info가 Cobalt Strike C2로 구성되었을 가능성이 있다. 해당 기간 동안 이 도메인에 대한 NS 레코드는 date.samuelblog[.]info를 가리키며, 이것은 이후 2개의 IP, 2.56.213[.]86 및 178.157.91[.]144로 확인되었는데 둘 다 MVPS Ltd.에서 호스팅되었다.

패시브 DNS 데이터를 사용하여 하위 도메인 api.[16진수 표기법과 유사한 데이터].ns1.samuelblog[.]info의 변종에 대한 몇 가지 의심스러운 DNS A 레코드 쿼리를 발견했다. 16진수 데이터가 24자보다 긴 경우 데이터는 마침표로 구분된 56자 실행으로 분할되었다. 추가 조사에서 유사한 패턴을 나타내는 다른 여러 도메인이 확인되었다(api.[hex data].ns1.). 이러한 도메인에서 확인된 대부분의 IP는 Recorded Future Platform에서 Cobalt Strike C2 서버 감지를 트리거했다. 더 나아가 Cobalt Strike의 개발자인 Raphael Mudge가 만든 튜토리얼 비디오는 위에서 관찰된 패턴과 일치하는 DNS 비콘 트래픽을 보여준다. 이러한 요인을 감안할 때 우리는 samuelblog[.]info에 대한 의심스러운 DNS 트래픽이 Cobalt Strike C2로 사용된 결과일 가능성이 있다고 판단했다.

공격자

Insikt Group은 TAG-28이 인도 타겟에 대한 정보 수집 임무를 맡은 중국 정부 산하 해커 그룹이라고 확신한다. 중국계로 판단하는 근거는 Winnti 멀웨어 사용이다. 중국 정부가 후원하는 여러 해커 그룹들이 이 멀웨어를 공유한다. 그리고 이 캠페인이 최소 3개의 개별 인도 조직을 대상으로 하는 것도 중국 해커의 소행으로 보는 이유이다. 우리는 TAG-28의 활동을 지속적으로 추적하면서 그들의 능력과 타겟에 대한 현재 정보를 기반으로 기존 해커 그룹과의 공통점을 파악하거나 TAG-28을 RedEcho나 RedFoxtrot과 같은 어엿한 "Red" 그룹으로 분류할 수 있는 추가 데이터 포인트를 수집할 것이다. 악성 인프라 운영자의 정체, 추가 업스트림 공격자 인프라와 같은 추가 데이터 포인트가 배후 추적의 열쇠가 될 것이다.

향후 전망

이 연구는 중국이 인도의 민간 및 공공 부문 조직들에 대해 지속적으로 전략적, 전술적 관심을 기울이고 있음을 주목한다. 2020년 국경 분쟁과 인도 정부가 인도 시장에서 중국 모바일 애플리케이션을 금지한 이후의 경제 제재로 인해 양국 간의 긴장이 고조되었다. 따라서 인도 정부 부처 및 조직에 침투하고 정보를 얻는 것이 중국 정부 산하 해커들에게 계속해서 가장 중요한 관심사가 될 것이다. 사이버 작전이 정치 및 대외 관계 발전과 더불어 군사 기술 또는 국가 안보 문제에 대한 정보를 수집하는 데 핵심적인 역할을 하기 때문이다.

관찰된 해킹 배후의 의도를 확인할 수는 없지만, 인도 최대 언론사와 Aadhaar 시스템이 정찰, 스파이, 정보 작전에서 중요한 타겟임은 분명하다.

여러 중국계 해커 그룹들이 Shadowpad와 기타 최신 멀웨어 제품군을 사용하는 쪽으로 전환했으나, 이 캠페인은 Winnti와 같은 기존 도구 및 Cobalt Strike와 같은 OST(offensive security tools)가 여전히 중국 산하 해커 그룹의 표적 침투 수행에서 매우 효과적으로 활용되고 있음을 입증한다.

대응

TAG-28 관련 활동 탐지 및 대응을 위해 다음 조치를 수행할 것을 권고한다.

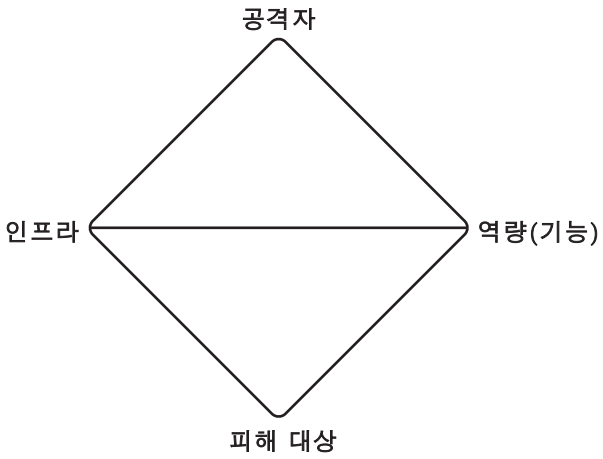
- IDS, IPS 또는 기타 네트워크 방어 메커니즘이 TAG-28과 연결된 외부 IP 주소 및 도메인에 대해 경고하도록 구성하고, 검토 시 차단을 고려해야 한다. 이 보고서의 고객 전용 버전 부록에서 해당 목록을 확인할 수 있다.
- 고객은 Recorded Future Hunting Packages를 사용하여 TAG-28에서 사용하는 멀웨어 패밀리를 헌팅하고 탐지할 수 있다.
- 레코디드 퓨처는 Command and Control Security Control Feed에서 악성 서버 구성을 선제적으로 탐지하고 로깅한다. C2 목록에는 TAG-28 및 Winnti, PlugX, AXIOMATICASYMPTOTE와 같은 중국계 해커 그룹이 사용하는 멀웨어와 도구가 포함된다. 레코디드 퓨처 고객은 이러한 C2 서버에 대해 경고 및 차단을 구성하여 침입 행위를 탐지하고 방어할 수 있다.
- 레코디드 퓨처 위협(Threat Intelligence) 인텔리전스, 써드파티(Third-Party) 인텔리전스, 보안운영(SecOps) 인텔리전스 모듈 사용자는 NTA 및 Malware Analysis 분석의 실시간 결과를 모니터하여 자사 또는 주요 벤더 및 파트너와 관련된 의심스러운 침입 활동을 파악할 수 있다.
- 알려진 취약점을 방어하는 최신 패치를 사용하여 운영 체제와 소프트웨어를 최신 상태로 유지해야 한다.

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 범죄
    - 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. 핸들, 페르소나, 사람, 또는 유책 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 수학 용어를 사용한다.

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.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.