CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

June 16, 2021

중국 PLA 69010 부대 산하 해커 그룹 RedFoxtrot, 아시아 접경 국가 대상 사이버 침투 자행

이 보고서는 중국계 해커 그룹인 RedFoxtrot과 PLA 69010 부대 관련성을 분석한다. 이들의 활동은 대규모 자동 네트워크 트래픽 분석과 전문가 분석을 통해 확인되었다. 데이터 소스에는 레코디드 퓨처 플랫폼, DomainTools, PolySwarm, Farsight와 일반적인 오픈소스 도구 및 기술이 포함된다. 이 보고서는 중국 군사정보부대 사이버 동향과 관련된 전략 및 작전 정보 담당자와 중앙 아시아 또는 남아시아 지역 네트워크 보안 담당자에게 가장 유용할 것이다. 분석 마감일: 2021년 6월 1일.

개요

레코디드 퓨처 Insikt Group은 배후에 중국 해커그룹 RedFoxtrot과 신장 우루무치에 위치한 중국 군 정보기관인 중국 인민해방군(People's Liberation Army, PLA) 소속 69010 부대 간의 구체적인 관련성을 포착했다. 이는 2015년 인민해방군이 재편되고 정보 공개가 주로 중국 국가안전부(Ministry of State Security, MSS) 관련 그룹에 집중된 시기 이후 PLA 작전이 노출된 이례적인 경우이다.

69010 부대는 PLA의 정보 및 사이버 전쟁 지부인 PLA 전략지원부대(Strategic Support Force, SSF) 네트워크 시스템 부서(Network Systems Department, NSD) 내의 기술 정찰국(Technical Reconnaissance Bureau, TRB) MUCD(Military Unit Cover Designator)일 가능성이 높다. RedFoxtrot의 느슨한 운영 보안 조치로 인해 Insikt Group은 이 해커 그룹의 물리적 주소가 69010 부대 본부와 일치하는 것을 확인했다. 또한 공개된 조달 및 법원 문서에서 69010 부대와 해당 주소 및 SSF 간의 관련성을 추가로 확인하였다. 여러 학술 출판물은69010 부대의 임무가 사이버 작전이라는 가설을 뒷받침한다.

RedFoxtrot은 최소한 2014년부터 활동해 왔으며 중앙아시아, 인도, 파키스탄 전역의 정부, 국방, 통신 부문을 타깃으로 삼아왔는데 이는 69010 부대의 작전 소관과 일치한다. Insikt Group은 특히 지난 6 개월 동안 인도 항공우주 및 방산 업체 3 곳과 아프가니스탄, 인도, 카자흐스탄, 파키스탄의 주요 통신회사, 다수의 정부기관을 대상으로 한 RedFoxtrot 네트워크 침입을 파악했다.

RedFoxtrot은 방대한 작전 인프라를 운영하고 있으며 중국 사이버 스파이 그룹 Icefog, PlugX, Royal Road, Poison Ivy, ShadowPad, PCShare 등이 흔히 사용하는 맞춤형 멀웨어와 공개 멀웨어를 모두 사용했다. RedFoxtrot 활동은 다른 보안회사들이 추적한 Temp.Trident, Nomad Panda 등의 위협 그룹과 겹친다.

주요 내용

- 과거 란저우 군구 제2 기술정찰국으로 알려진 PLA 69010 부대는 2015년 재편 이후 PLA-SSF의 네트워크 시스템 부서에 통합된 것으로 보인다.
- 특정 PLA 유닛과의 관련성과 중국 사이버 스파이 그룹 특유의 맞춤 기능 사용으로 보아 RedFoxtrot은 중국 정부가 배후에 있는 위협 활동 그룹임이 확실시된다.
- RedFoxtrot은 2020년 다른 여러 PLA 및 MSS 산하 위협 그룹들과 함께 ShadowPad 백도어 액세스 권한을 취득했다.
- 2015년 조직 재편 이후에 PLA 산하 사이버 스파이 그룹들의 활동이 감소했다. 이는 기존 그룹의 해체나 병합에 따른 신규 클러스터 형성 때문일 수 있다. Insikt Group은 Tonto Team, Tick, Naikon, RedFoxtrot과 같은 PLA 관련 그룹의 지속적인 활동과 PLA 연관성이 의심되는 새로운 중국 위협 활동 그룹의 출현으로 보아, 국가안전부(MSS)에 대한 관심이 높아졌음에도 불구하고 여전히 PLA 산하 그룹들이 중국 사이버 스파이 영역에서 중요한 위치를 점하고 있다고 본다.

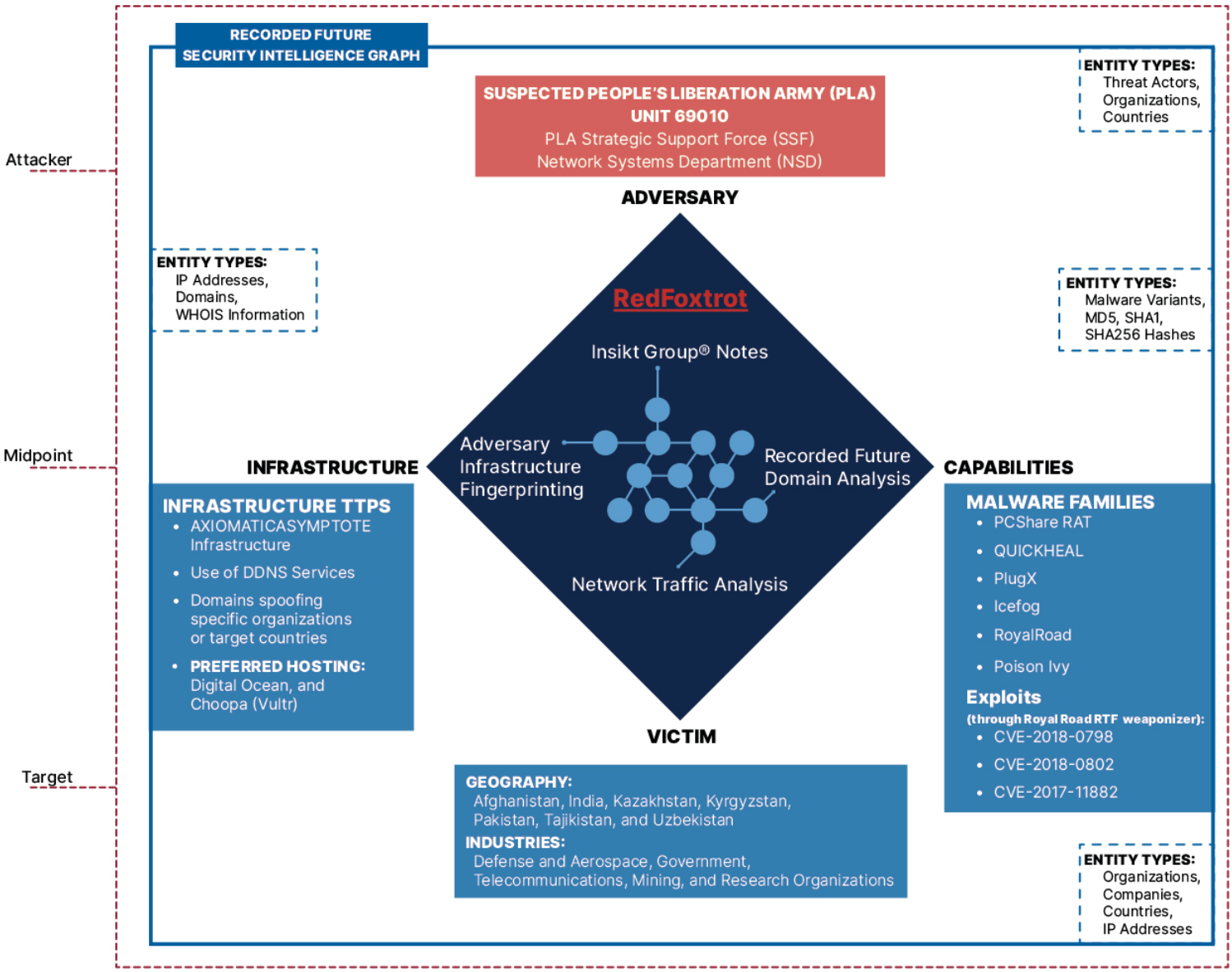


그림 1: 하이레벨 RedFoxtrot TTP 및 Recorded Future 데이터 소싱 그래픽
(출처: Recorded Future)

위협 분석

RedFoxtrot는 주로 아프가니스탄, 인도, 카자흐스탄, 키르기스스탄, 파키스탄, 타지키스탄, 우즈베키스탄의 항공 우주 및 국방, 정부, 통신, 광업, 연구 기관을 표적으로 삼았다. 이러한 타깃은 RedFoxtrot이 군사 기술과 방위 관련 정보 수집에 관심이 있음을 시사한다. RedFoxtrot은 PlugX, Poison Ivy, Royal Road, PCShare, IceFog 등 중국 사이버 스파이 그룹들이 흔히 공유하는 다수의 오픈소스/클로즈드소스 도구를 사용했다. Insikt Group은 또한 Recorded Future에서 AXIOMATICASYMPTOTE로 추적한 ShadowPad C2(command and control) 인프라로 의심되는 여러 링크를 파악했다. 이는 커스텀 백도어에 액세스할 수 있는 중국 그룹임을 나타내는 또 다른 증거를 제공한다. 지난 6개월 동안 주목할만한 RedFoxtrot 피해자에는 다수의 인도 항공 우주 및 방산 업체와 아프가니스탄, 인도, 카자흐스탄, 파키스탄의 통신회사, 정부 기관들이 포함된다. 이 기간 동안 인도와 중국 간의 국경 긴장이 고조된 시기에 특히 인도 타깃에 공격이 집중되었다.

RedFoxtrot과 PLA 69010 부대 연관성

Insikt Group은 RedFoxtrot 위협 행위자로 의심되는 배후 조종 인물을 통해 RedFoxtrot 인프라와 PLA 69010 부대 간의 연관성을 확인했다. 이 인물의 허술한 보안 조치 덕분에 우리는 PLA 69010 부대 본부 주소인 No. 553, Wenquan East Road, Shuimogou District, Ürümqi, Xinjiang(新疆乌鲁木齐市水磨沟区温泉东路553号)과의 연결고리를 발견했다. Insikt Group은 이 개인의 신원을 비공개로 한다. 그러나 광범위한 온라인 활동을 통해 이 인물이 우루무치에 있으며, 해킹에 관심이 있고, 과거 우한에 위치한 PLA의 구 Communications Command Academy[1](通信指挥学院)와 관련되어 있음을 보여주는 확실한 증거를 확보했다.

1 Communications Command College로도 알려진 Communications Command Academy는 과거 정보 및 사이버 전쟁과 군사 통신시스템 부문의 3PLA 요원을 훈련하는 역할로 알려졌다. 현재는 중국 정보통신대학(College of Information and Communication)에 편입된 것으로 보인다.

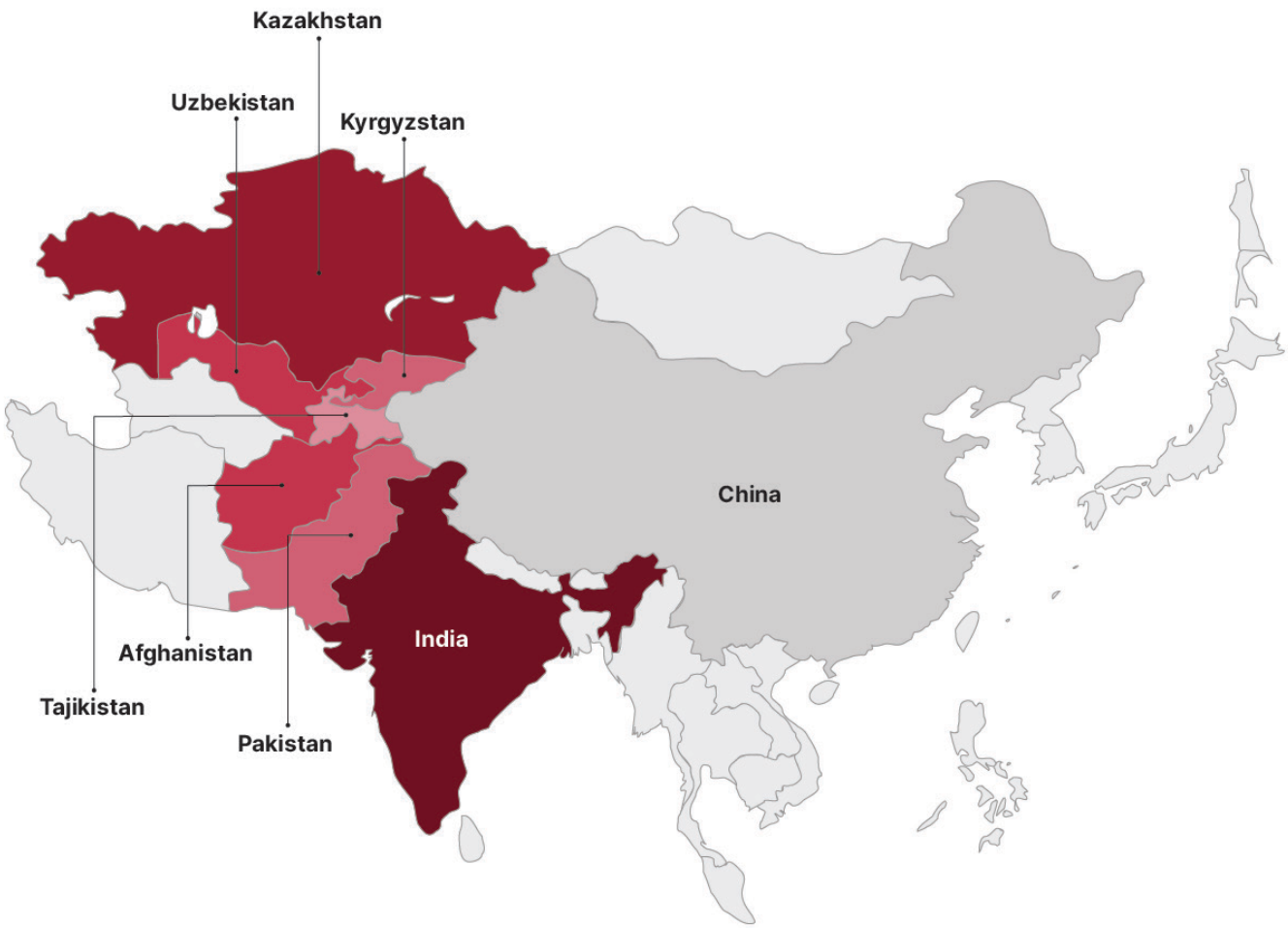


그림 2: 중앙아시아와 남아시아를 타깃으로 한 RedFoxtrot 활동 히트맵

69010 부대의 정체

69010 부대 신장 우루무치에 본부를 둔 PLA-SSF 내부 부서의 MUCD일 가능성이 높다. Project 2049 Institute에서 2011년에 발표한 조사에 따르면 과거 란저우 군구의 Second TRB로 알려진 SIGINT(signals intelligence)가 오랫동안 69010 부대의 소관이었다. 69010 부대는 또한 중국 서부 국경을 따라 군사 활동을 감시하는 일을 주로 담당하는 여러 하위 사무소를 보유하고 있는 것으로 보인다. 학문적 성과 분석에서 69010 부대가 2015년까지 사이버 임무를 수행했다는 증거를 확인할 수 있다(예시 간행물 2,3). 2015년 조직 개편이 시작되기 전에 중국 사이버 스파이 활동의 대부분은 TRB와 3PLA(중국 인민해방군 제3총참모부) 주도로 이루어졌다. 3PLA는 중국 통신 네트워크 모니터링, 중국 국내 컴퓨터 네트워크 보안, 사이버 첩보 활동을 위한 컴퓨터 네트워크 익스플로잇 실행 등의 SIGINT 전반을 담당했다. 2015년부터 TRB와 3PLA의 기능과 임무가 재편되어 신규 설립된 SSF NSD로 대체되었다. 다음 섹션에서 설명하는 증거는 69010 부대가 중국 군사 개혁의 일환으로 SSF NSD 산하로 이전되었음을 시사한다.

이전 란저우 군구는 2015년 재편 이후 PLA의 새로운 서부지역 사령부에 통합되었다. 서부지역 사령부는 PLA의 5개 사령부 중 하나이며 인도, 파키스탄, 중앙 아시아를 모니터링하는 임무를 맡고 있음이 거의 확실하다. 이는 관찰된 RedFoxtrot 활동과 일치한다. 마찬가지로 국방, 군사, 통신, 정부 기관들에 대한 정보 수집은 PLA 부대의 작전 영역과 일치하며 다른 PLA 연계 그룹들의 타깃 프로필에도 부합된다(1,2,3).

그림 3: 69010 부대 입구로 의심되는 No. 553 Wenquan East Road, Ürümqi (출처: Baidu Maps)

No. 553, Wenquan East Road

보고에 따르면 69010 부대는 우루무치시 수이모거우 구에 본부를 두고 있다. 우리는 다수의 신장 지방 법원 문서에 수이모거우 내에 있는 No.553 Wenquan East Road라는 주소가 PLA 69010 부대 소재지로 기재되어 있음을 확인했다. 또한 이 주소는 지난 몇 년간 SSF가 공고한 5 건의 장비 입찰 내역에도 나와 있다. 이 역시 69010 부대가 PLA 개편 이후 SSF로 이전되었을 수 있음을 시사한다.

中国人民解放军69010部队与乌鲁木齐绿洲金叶生态有机种植农民专业合作社返还原物纠纷一审民事裁定书

文书来源：中国裁判文书网 | 发表日期：2018-10-01

关联企业：乌鲁木齐绿洲金叶生态有机种植农民专业合作社

文书正文

新疆维吾尔自治区乌鲁木齐市米东区人民法院

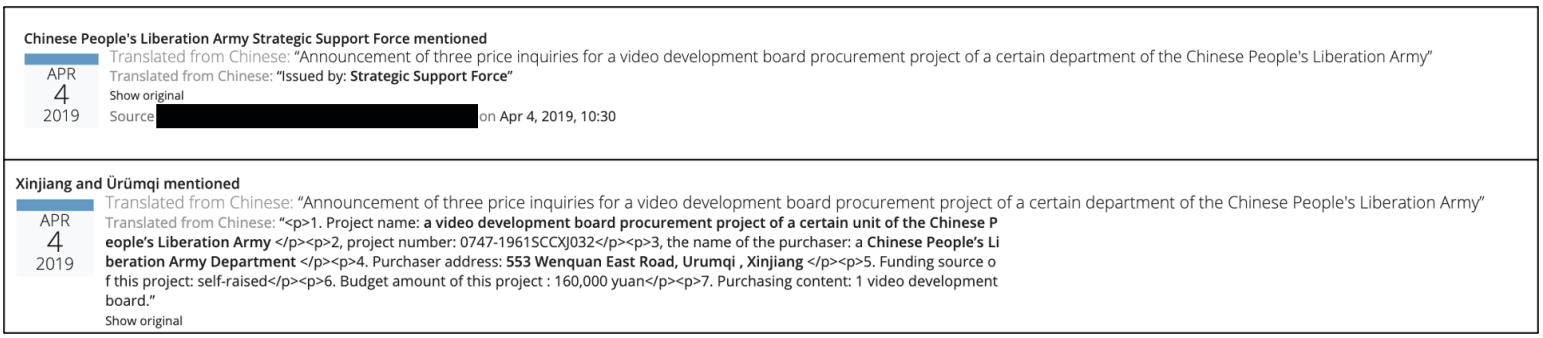
民事裁定书

（2018）新0109民初3858号

当事人信息

原告：中国人民解放军69010部队，住所地：乌鲁木齐市水磨沟区温泉东路553号。

그림 4: 69010 부대 주소가 No. 553 Wenquan East Road로 기재된 법원 문서[4]



Chinese People's Liberation Army Strategic Support Force mentioned

APR 4 2019

Translated from Chinese: "Announcement of three price inquiries for a video development board procurement project of a certain department of the Chinese People's Liberation Army"

Translated from Chinese: "Issued by: **Strategic Support Force**"

Show original

Source [redacted] on Apr 4, 2019, 10:30

Xinjiang and Ürümqi mentioned

APR 4 2019

Translated from Chinese: "Announcement of three price inquiries for a video development board procurement project of a certain department of the Chinese People's Liberation Army"

Translated from Chinese: " 1. Project name: **a video development board procurement project of a certain unit of the Chinese People's Liberation Army** 2, project number: 0747-1961SCCXJ032 3, the name of the purchaser: a **Chinese People's Liberation Army Department** 4. Purchaser address: **553 Wenquan East Road, Urumqi , Xinjiang** 5. Funding source of this project: self-raised 6. Budget amount of this project : 160,000 yuan 7. Purchasing content: 1 video development board."

Show original

그림 5: 553 Wenquan East Road 주소로 SSF가 발행한 군사 조달 문서에 대한 Recorded Future Event (출처: Recorded Future)

[2] Yang Ping 杨萍 and Liang Guangming 梁广明, "物联网安全问题及对策分析" [Security Problems and Solutions for the Internet of Things], 无线互联科技 Wireless Internet Technology 6, (2013): 13.

[3] Yang Ping 杨萍 and Tian Jianchun 田建春, "Wireshark网络安全风险评估关键技术研究" [Research on Key Technologies of Wireshark Network Security Risk Assessment], 网络安全技术与应用 Network Security Technology and Application 9 (2015): 54.

[4] https://m.qcc[.]com/wenshuDetail/b218bb9ef2c2e2b282f8c88e098001b7.html

Baidu Maps에 따르면 이 주소는 여러 건물과 주거 지역으로 구성된 대형 복합 시설에 해당한다. 위성 이미지와 스트리트뷰 이미지에서 알 수 있듯이 부대 본관의 지붕과 건물 뒤의 언덕에서 여러 개의 위성 안테나를 볼 수 있으며 열병장, 런닝 트랙, 운동장, 대형 출입구 등과 같이 PLA 기지에서 흔히 볼 수 있는 다른 특징도 확인된다.

그림 6: Wenquan East Road 5에 위치한 69010 부대 단지로 의심되는 시설의 항공 사진[5]

[5] 두 개의 다른 건물이 69010 부대와 동일한 주소를 공유한다. 길 건너편에 있는 아파트 단지(기지와의 관련 여부는 확인 불가)와 기지 바로 옆에 있는 전자 상점이다. RedFoxtrot 운영자와 관련 사이버 스파이 활동이 이 두 시설 중 하나와 연결되어 있을 가능성은 매우 낮으며, 해당 주소는 우리 조사의 맥락에서 거의 확실하게 69010 부대를 가리킨다.

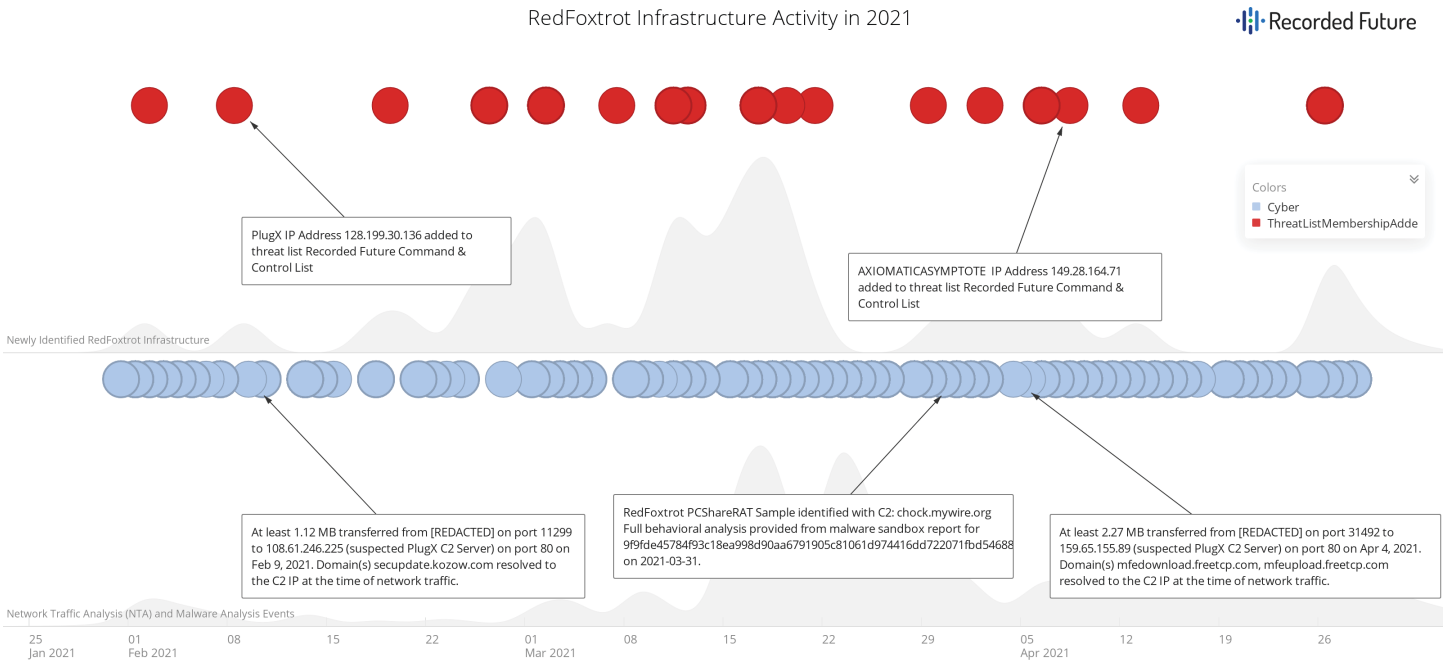


그림 7: 2021년 RedFoxtrot 인프라 탐지, 멀웨어 탐지, NTA 이벤트 타임라인 (출처: Recorded Future)

RedFoxtrot 인프라 매핑

Recorded Future NTA(Network Traffic Analysis), 공격자 인프라 탐지, 기타 일반 분석 기술을 사용하여 지난 6개월 동안 침입에 사용된 RedFoxtrot 인프라와 관련 멀웨어 샘플 클러스터를 추적했다. 이 활동과 최소한 2014년으로 거슬러 올라가는 공개적으로 보고된 캠페인들 사이에 강력한 연관성이 있다. 우리는 확인된 인프라 클러스터에 연결된 도메인들에서 명확하고 일관된 호스팅 일치, 공통 타깃, 동일 멀웨어 사용을 확인했다. 특히 RedFoxtrot의 인프라 TTP(actics, techniques, and procedures)에서 다음과 같은 현상을 파악했다.

- 공통 인프라 클러스터의 일부를 형성하는 다수의 DDNS(Dynamic DNS) 도메인 사용
- DDNS 도메인에는 종종 타깃의 지리적 정보 또는 특정 조직 스푸핑과 관련된 힌트가 포함됨 (예: “inbsnl.ddns[.]info”, “adtl.mywire[.]org”, “indianmail.zyns[.]com”)
- 최근 DigitalOcean 및 Choopa (Vultr) 호스팅 프로바이더 선호
- AXIOMATICASYMPTOTE 인프라 사용, ShadowPad 백도어 액세스 가능성 시사

이전에 중국계 해커 그룹 RedEcho에 대한 보고서에서 언급했듯이 Insikt Group은 ShadowPad 감염에 사용되는 네트워크 인프라를 AXIOMATICASYMPTOTE로 지칭하고 추적한다.

AXIOMATICASYMPTOTE 및 PlugX 클러스터

Recorded Future 공격자 인프라 탐지 기법을 사용하여 RedFoxtrot 도메인의 상당 부분이 AXIOMATICASYMPTOTE 및 PlugX C2 인프라에 연결되어 있음을 확인했다. 이들 중 상당수는 PCShare와 같은 다양한 멀웨어 제품군의 C2로도 사용되었다. RedFoxtrot은 주로 단일 서버를 사용하여 대량의 DDNS 도메인을 호스팅했다.

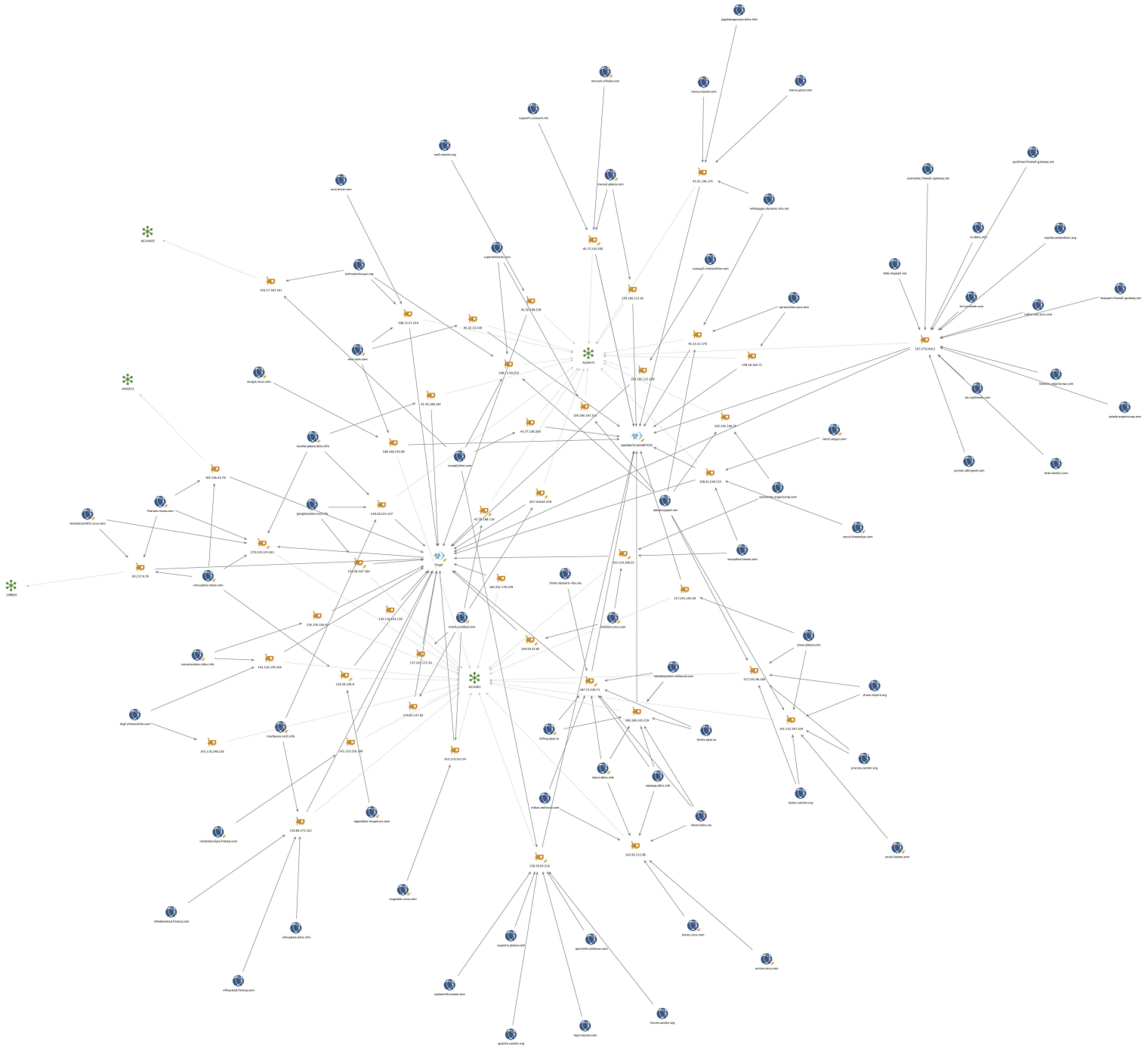


그림 8: RedFoxtrot PlugX 및 AXIOMATICASYMPTOTE 인프라에 대한 Maltego 차트

터키어 사용자를 타깃으로 한 과거 캠페인과의 연관성

2019년 중반에 등록된 RedFoxtrot 활동 관련 도메인 4개(kelimelerdunyasi[.]org, stratejibilimi[.]com, adobesupport[.]net, superkelimeler[.]com)는 모두 터키어로 작성된 합법적인 영어 학습 웹사이트인 ingilizcem[.]org를 미러링하는 데 사용되었다. 호스팅이 일치하고 공통적으로 ingilizcem[.]org를 스푸핑하는 것 외에도 4개 도메인 중 3개가 동일한 개인정보보호 등록 이메일 주소인 stratejibilimi.com@protectdomain[.]org로 연결되었다. 이 웹사이트들은 더 이상 서비스되지 않지만 오픈소스 보고에 따르면 2019년 중반(이 4개 도메인 등록 직후)에 Adobe Flash 설치 프로그램으로 가장한 Poison Ivy SKYLINE 변종을 지원하는 데 adobesupport[.]net이 사용되었다. 이 도메인들은 RedFoxtrot에서 터키어 사용자를 해킹하는 데 사용되었을 가능성이 농후하다. 그 이후로 이 4개의 도메인과 호스팅이 일치하는 다수의 추가 RedFoxtrot 도메인이 있었다. 특히 adobesupport[.]net의 Poison Ivy 변종은 추가로 의심되는 RedFoxtrot 활동과 빈틈없이 일치한다.

Poison Ivy SKYLINE Variant	C2 Domain
acb11d9d0652c95b16db17fda918ff5b6ee666815 6a30fe6276b0fa66f74c9720	skylineqaz.crabdance[.]com
c1e3a5e171d0de6054f4a1aeb9a46ff176ef5ba6 464304b2f2660a23396e91f4	coreldraw.kozow[.]com
379af30d508cdbae7eb201041d8eb815b239e18 1dd8106145d4263753df3acd9	hostmail1[.]com
367718fd58c658dce22c995f3e10bc3a5425814 ddf221686e166e3129a53e897	capture.kozow[.]com

이 Poison Ivy 변종과 관련하여 앞서 나온 특성 외에도 kelimelerdunyasi[.]org 도메인과 hostmail1[.]com (45.251.241[.]13), hostmail1[.]com, skylineqaz.crabdance[.]com (206.189.153[.]132) 간에 호스팅 일치 이력이 확인된다.

공개적으로 보고된 해킹과 일치하는 요소

RedFoxtrot 활동은 다른 보안 벤더들이 Temp.Trident/Nomad Panda로 추적한 해커 그룹과 일치한다. RedFoxtrot의 활동과 FireEye가 추적한 WATERFIGHT 및 SKYLINE의 2018 ~ 2019 년 중앙 아시아 국가 대상 캠페인 간에 수많은 인프라, 타겟팅, 멀웨어 공통점이 발견되었다(1,2). 또한 Icefog 및 Poison Ivy 페이로드 딜리버리를 위해 Royal Road (8.t) RTF(rich text format) 무기화를 사용한 RedFoxtrot의 요소가 이전에 문서화되었다. 공개적으로 보고된 활동과의 몇 가지 주목할만한 공통점은 개략적으로 다음과 같다.

1. skylineqaz.crabdance[.]com 도메인은 터키와 카자흐스탄을 대상으로 한 활동과 관련된 공개 보고서에서 언급되었으며 2019년 9월 DigitalOcean IP 주소 206.189.153[.]132에서 호스팅되었다. 이 도메인은 다수의 RedFoxtrot DDNS 도메인과 일시적으로 공통된 호스팅이 확인된다.
    - redhatboy.dynamic-dns[.]net
    - scorpio.dns04[.]com
    - koreckaccord01.zzux[.]com
    - exat.dnset[.]com
    - macfeesyn.ns01[.]info
    - gulistan.wikaba[.]com
    - macfeeupdate.ddns[.]info
    - lexuz.dns05[.]com
    - lexuz.x24hr[.]com
2. Poison Ivy C2 capture.kozow[.]com은 2020년 중반부터 후반까지 DigitalOcean IP 주소 45.76.197[.]157에서 RedFoxtrot PCShare C2 도메인 locker.camdvr[.]org와 동일하게 호스팅되었다. 이전 보고에 나왔듯이 capture.kozow[.]com C2에 연결된 Poison Ivy 샘플은 앞서 언급한 터키와 카자흐스탄을 대상으로 하는 캠페인에 사용된 동일한 SKYLINE 변종이다.
3. 2020년 중반에 pisces.zzux[.]com 도메인이 RedFoxtrot 인도 테마 DDNS 도메인 클러스터와 함께 DigitalOcean IP 주소 142.93.212[.]86에서 동시에 호스팅되었다.
    - inbsnl.ddns[.]info
    - inbsnl.ddns[.]ms
    - indian.mefound[.]com

4. pisces.zzux[.]com 도메인과 RedFoxtrot 인프라 간의 추가적인 연결고리도 이전에 문서화되었다. 또한 위의 RedFoxtrot DDNS 도메인 중 하나인 inbsnl.ddns[.]info는 과거 RedFoxtrot 활동에 사용된 커스텀 멀웨어 QUICKHEAL 샘플인 (f45c6f8695fbc6e537cea15142f062a0d21c4a556c5fc1f7a2f3ee661b036ffc)에 연결되어 있다.

아래의 Maltego 차트는 이전에 공개적으로 보고된 RedFoxtrot 활동과의 추가적인 공통점을 요약하여 보여준다.

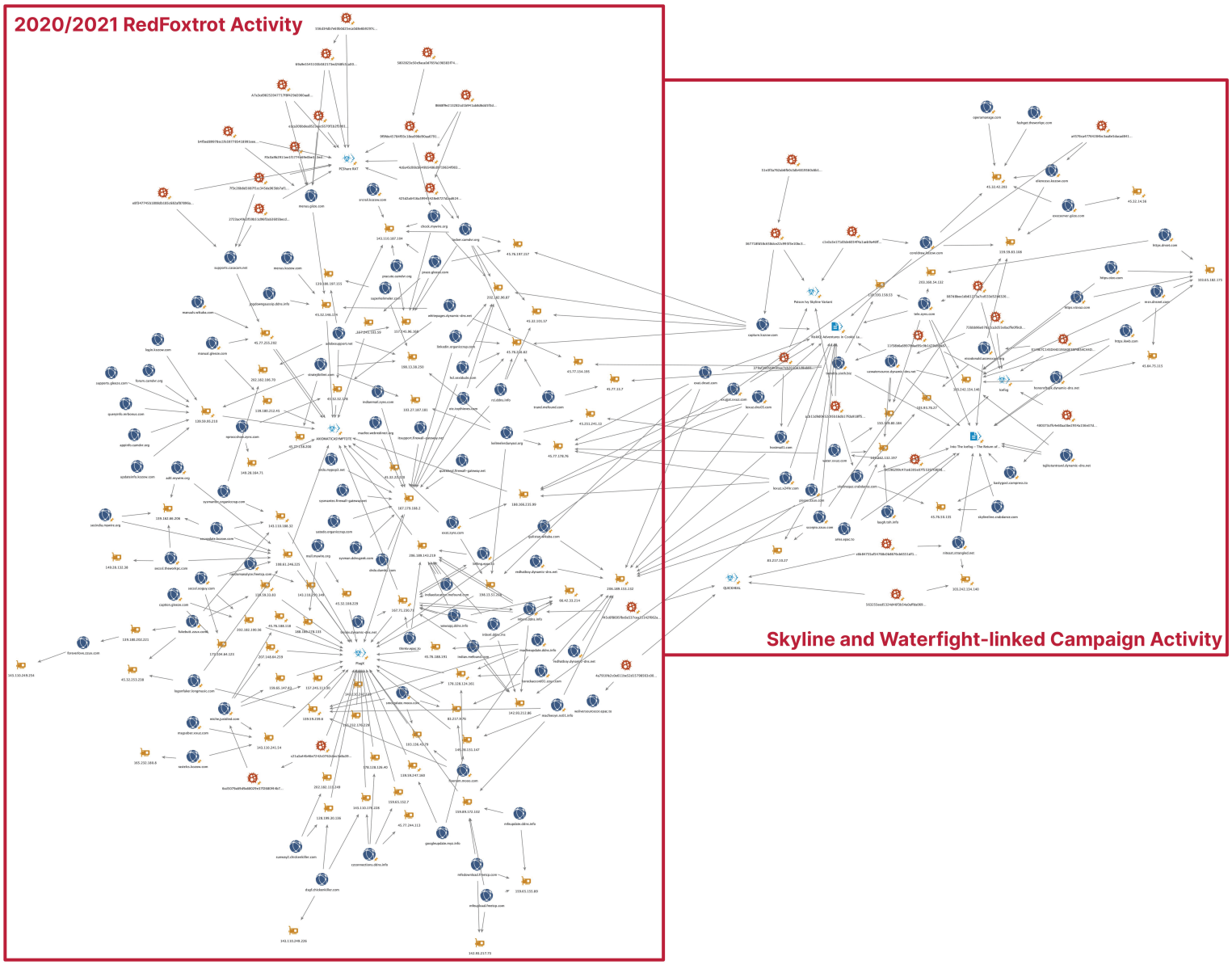


그림 9: 2020/2021 RedFoxtrot 활동과 공개적으로 보고된 SKYLINE 및 WATERFIGHT 캠페인 간의 공통점

대응 방안

RedFoxtrot 활동과 관련된 움직임을 탐지하고 대응하기 위해 다음 조치를 수행할 것을 권고한다.

- 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS) 또는 다른 네트워크 방어 메커니즘을 구성하여 경고를 설정하고 검토하여 부록 A에 나열된 외부 IP 주소와 도메인에 대한 연결 시도를 차단할 것.
- 다수의 정부 지원 위협 활동 그룹과 금전적 이익을 노리는 위협 활동 그룹이 계속해서 네트워크 침입 활동에서 DDNS 도메인을 사용하고 있다. DDNS 서브도메인과 관련된 모든 TCP/UDP 네트워크 트래픽을 차단하고 로깅해야 한다. (DNS RPZ 또는 이와 유사한 설정을 사용할 것)
- Recorded Future Threat Intelligence, Third-Party Intelligence, SecOps Intelligence 모듈 사용자는 NTA 및 Malware Analysis 분석의 실시간 아웃풋을 모니터하여 자사 또는 주요 벤더 및 파트너를 타깃으로 한 수상한 침입 활동을 파악할 수 있다.
- Microsoft Office 및 Windows 소프트웨어를 항상 최신 업데이트 상태로 유지하여 Royal Road RTF weaponizer를 사용하여 생성된 것과 같은 알려진 코드 실행 취약점을 익스플로잇하려는 악성 문서로부터 보호할 것.

향후 전망

우리는 이번 조사에서 PLA-SSF의 69010 부대 산하 그룹인 RedFoxtrot의 사이버 스파이 활동을 밝혀냈다. 특히 주목할만한 점은 2020년부터 2021년까지 중국과 인도 간의 긴장이 고조되는 시기에 RedFoxtrot이 인도 방산 업체, 통신 사업자, 정부 기관을 집중적으로 해킹했다는 것이다. 또한 우리는 최근 인도 내 주요 인프라를 노린 RedEcho라는 해커 그룹의 캠페인을 공개한 바 있다. RedEcho 캠페인이 인도 전력 시스템 내부 사전 침투에 대한 우려를 불러일으킨 반면, RedFoxtrot의 활동은 군사 정보 수집 측면에서 기존 PLA 관련 활동과 더 근접한다. 이러한 다양한 작전은 사이버 공간 내에서 중국 정부의 다각적인 접근 방식을 예증한다. 중국 정부는 군사 기술 및 국가 안보 문제는 물론 정치 발전 및 대외 관계에 대한 정보를 수집하는 도구로 사이버 작전을 사용한다. 이는 위구르인, 티베트인, 가톨릭교도와 같은 소수 민족 및 종교적 소수자 모니터링부터 일대일로(Belt and Road Initiative), Made in China 2025와 같은 전략적 정책 목표 달성에 이르기까지 다양한 목적으로 활용되고 있다.

최근 몇 년 동안 PLA 산하 사이버 스파이 그룹들의 활동이 명백히 감소했다. 이는 2015년 재편 이후 이전의 활동 그룹들이 해체되거나 병합되어 새로운 클러스터를 형성했기 때문으로 보인다. 이 기간 동안 중국의 사이버 스파이 활동은 주로 중국 정보기관인 국가안전부(Ministry of State Security, MSS) 주도로 이루어졌다. 미국 정부의 기소와 익명의 중국 APT 독싱(doxxing) 운영자인 Intrusion Truth에 따르면 MSS는 사이버 스파이 활동을 위해 종종 민간 하청 모델을 사용하는 것으로 확인되었다. 그러나 MSS에 이목이 집중되고 있음에도 불구하고 Tonto Team, Tick, Naikon, RedFoxtrot과 같은 PLA 관련 그룹들이 지속적으로 활동하고 있는 것으로 보아 PLA 산하 그룹이 중국 사이버 스파이 영역에서 여전히 건재한 것으로 보인다.

부록 A 침해 지표(Indicators of Compromise)

Insikt Group Github 저장소 https://github.com/Insikt-Group/Research에서 아래 나열된 지표들을 확인할 수 있다. (RedFoxtrot – June 2021)

Network Indicators:

Domains:

adobesupport[.]net
adtl.mywire[.]org
appinfo.camdvr[.]org
aries.epac[.]to
billing.epac[.]to
capture.kozow[.]com
chock.mywire[.]org
coreldraw.kozow[.]com
czconnections.ddns[.]info
drdo.dumb1[.]com
drdo.mypop3[.]net
dsgf.chickenkiller[.]com
elienceso.kozow[.]com
exat.dnset[.]com
exat.zyns[.]com
execserver.giize[.]com
exujjat.xxuz[.]com
fashget.theworkpc[.]com
fivenum.mooo[.]com
foreverlove.zzux[.]com
forum.camdvr[.]org
fukebutt.zzux[.]com
googleupdate.myz[.]info
gulistan.wikaba[.]com
hcl.sexidude[.]com
honoroftajik.dynamic-dns[.]net
hostmail1[.]com
https.dnset[.]com
https.ikwb[.]com
https.otzo[.]com
https.vizvaz[.]com
inbsnl.ddns[.]info
inbsnl.ddns[.]ms
indiaeducation.mefound[.]com
indian.mefound[.]com
indianmail.zyns[.]com
itsupport.firewall-gateway[.]net
jpgdowngaussip.ddns[.]info
kastygost.compress[.]to
kelimelerdunyasi[.]org
koreckaccord01.zzux[.]com
laugh.toh[.]info
lexuz.dns05[.]com
lexuz.x24hr[.]com
linkedin[.]organiccrap[.]com
locker.camdvr[.]org
login.kozow[.]com
logonfaker.longmusic[.]com
macfee.webredirect[.]org
macfeesyn.ns01[.]info
macfeeupdate.ddns[.]info
mall.mywire[.]org
manual.gleeze[.]com
manuals.wikaba[.]com
menus.giize[.]com
menus.kozow[.]com
mfedownload.freetcp[.]com
mfeupdate.ddns[.]info
mfeupload.freetcp[.]com
miche.justdied[.]com
msgsober.xxuz[.]com
msn.dnsnet[.]com
nicodonald.accesscam[.]org
niteast.strangled[.]net
notice.theworkpc[.]com
nproccshow.zyns[.]com
otc[.]toythieves[.]com
pisces.zzux[.]com
prace.gleeze[.]com
pracute.camdvr[.]org
queryinfo.mrbonus[.]com
quickheal.firewall-gateway[.]net
randomanalyze.freetcp[.]com
rastelcs.kozow[.]com
rci.ddns[.]info
redhatboy.dynamic-dns[.]net
scorpio.zzux[.]com
secindia.mywire[.]org
secssl.ooguy[.]com
secssl.theworkpc[.]com
secupdate.kozow[.]com
skylineline.crabdance[.]com
skylineqaz.crabdance[.]com
smcupdate.mooo[.]com
srcrail.kozow[.]com
stratejibilimi[.]com
sunway2.chickenkiller[.]com
superkelimeler[.]com
supports.casacam[.]net
supports.gleeze[.]com
sysman.ddnsgeek[.]com
sysmantec.firewall-gateway[.]net
sysmantec[.]organiccrap[.]com
tajikstantravel.dynamic-dns[.]net
tele.zyns[.]com
thinkv.dynamic-dns[.]net
thinkv.epac[.]to
trand.mefound[.]com
trendiis.sixth[.]biz
updateinfo.kozow[.]com
uzwatersource.dynamic-dns[.]net
water.xxuz[.]com
wawaqq.ddns[.]info
whitepages.dynamic-dns[.]net
wsliversourcecor.epac[.]to
yatedo.organiccrap[.]com

IP Addresses (May 2021):

206.189.153[.]132
45.77.178[.]76
45.32.22[.]220
66.42.33[.]214
45.76.216[.]62
142.93.217[.]73
143.110.241[.]54
141.164.43[.]124
149.28.131[.]147
143.110.187[.]104
165.232.180[.]8
143.110.249[.]226
178.128.124[.]161
159.89.172[.]102
188.166.235[.]99
172.104.64[.]123
198.13.51[.]228
188.166.178[.]133
206.189.143[.]219
198.13.42[.]157
45.32.146[.]174
202.182.111[.]249

Malware Samples:

PCShare

```
2723ac49d3f59b51d96f3ab3605becdef1987242ef3d9d5b8490b0c9abe45049
425d2a6416a59943428e8727d2ad6247eb8342c35c4bd1d5b80df25d6fbcae94
4c6a45d08cb649b5486d9719634f903b3561e7820eda31bd50d811a01bd3481b
b668f9e213282cd1b941ab8d6dd5f3dd3266011ae16c0795ca86d12a57c095cc
69a9e5545103b582173ed268fc5ca0014c4d2e17337a953752b0157a76cc0bcb
7f3c26b8d3087f1cc345da965bb7af1a58488c6e260f12e72d8274d949a857bd
556d34db7e60b0d25eca0d8e6b9297cd9f2174c0d2ca013c0036a067457a2d01
e8f347745b1808db185c682af87896a941b4042f5de919e2010749152bda48ad
a7a3cd98252047717f8f429d2060aa84c6ee4ed8ae60ee15ad0b2b5807158c70
e1ca30bbdea8523aec6570f1b2f59012d0899875325a9ac88f09e09c14734ecc
f0c0a9b2911ee1f1774e69e0be313eda2054d744fa547f1c64ba0f078db3fcd9
9f9fde45784f93c18ea998d90aa6791905c81061d974416dd722071fbd54688e
69a9e5545103b582173ed268fc5ca0014c4d2e17337a953752b0157a76cc0bcb
8afcc6a25320a28833334a413a0f395a73bacf033fe0e84fea7ed4fec7945ca4
eeef1439b17280dfd7ce821752551aee57f3d1b7f385fe9cf331f69abd35cd96
8afcc6a25320a28833334a413a0f395a73bacf033fe0e84fea7ed4fec7945ca4
```

QUICKHEAL

```
4a7910fe2c0e611be52d15798563c007aa632d47eae1f020be95fde27d963da9
f45c6f8695fbc6e537cea15142f062a0d21c4a556c5fc1f7a2f3ee661b036ffc
851010b875a2ae5c68e85c7d549082539e427b0e9f0c5efef92e1396c6d8a0ae
```

PlugX

```
c21a3a44b46e7242c0762c8ec5e8a394ddc74b747244c5b83678620ae141e59c
6cd5079a69d9a68029e37f2680f44b7ba71c2b1eecf4894c2a8b293d5f768f10
45c944889a482ae2e0e0a8e260c3be737cb612c8804164badef61e8a8713b92f
```

Icefog

```
0c596299c47ce6305e07f55397fd69d49c8cab4f4b34a617bb6670dcaac9d9f2
11f38b6a69978dad95c9b1479db9a8729ca57329855998bd41befc364657d654
D096EECD60710CCF7F1658A52D54CAEF9CB26B3857B3A3DBEFA688C769E07339
087d8bee1db61273a7cd533d52b63265d3a8a8b897526d7849c48bcdba4b22ec
73bbb96e078a2ca3d55e0acffe0f9c80edf6ff0459a25c34edb4c14bb88783c1
e149E7C145D440193A0E3BF4B54C44DE00BBC3872EF18D6DA3C12F1E7ADD3053
```

PoisonIvy

```
acb11d9d0652c95b16db17fda918ff5b6ee668156a30fe6276b0fa66f74c9720
c1e3a5e171d0de6054f4a1aeb9a46ff176ef5ba6464304b2f2660a23396e91f4
379af30d508cdbae7eb201041d8eb815b239e181dd8106145d4263753df3acd9
367718fd58c658dce22c995f3e10bc3a5425814ddf221686e166e3129a53e897
```

Royal Road

```
51e3f3a762ab6fb0c3db4819560c6b1607cdcd257ce375e68fdf1a17ff5c2cb5
597c0c6f397eefb06155abdf5aa9a7476c977c44ef8bd9575b01359e96273486
4e1a2f731688f9aab80b1f55d9101bb1cddec08214d4379621c434899a01efbf
a95bbc1f067783c1107566ed7897549f6504d5367b8282efe6f06dc31414c314
9d239ddd4c925d14e00b5a95827e9191bfda7d59858f141f6f5dcc52329838f0
f5365387320ae6e6907fd2700f340ba8712cb08f7e52b2ec4dccfe99b3d648ef
ecdf806bb7ac876bac8250a1f0ff40395faf7a6738df6e0f62553c4164fdf16d
5238f8d8c3d16b52d39aa722daff663a5e6307c4b46e360969d84bf409a2690f
```

부록 B 멀웨어 상세 분석

중국 사이버 스파이 그룹들이 사용하는 공통 기능

RedFoxtrot 인프라는 그룹에서 사용하는 다양한 PlugX, Poison Ivy, Royal Road, PCShare, IceFog 샘플과 연결되어 있다. 또한 AXIOMATICASYMPTOTE 인프라 사용은 ShadowPad 멀웨어의 사용과 관련이 있다. 이 도구들 중 2개인 IceFog와 ShadowPad는 중국 사이버 스파이 그룹들이 특징적으로 사용하는 기능이다. 이에 비해 Royal Road, PCShare, PlugX, Poison Ivy는 비교적 보편적이지만, 이들을 사용하는 것 역시 다수의 중국계 위협 활동 그룹과 밀접하게 연관되어 있다. 최근 RedFoxtrot은 PCShare, PlugX, ShadowPad 사용을 점점 더 선호하는 추세이며 IceFog, Poison Ivy, Royal Road의 사용은 감소하고 있다.

PCShare RAT

중국 오픈소스 RAT(remote access trojan) PCShare는 중국 지하 사이버 범죄조직에 뿌리를 두고 있는 것으로 생각되며, 현재 GitHub를 통해 툴 버전을 무료로 사용할 수 있다. 최근 몇 년 동안 PCShare 변종이 동남아시아 정부를 대상으로 한 중국 사이버 스파이 활동과 중국 그룹 Cycldek(AKA Goblin Panda)의 캠페인에 사용되었다. 우리는 다수의 PCShare 샘플이 RedFoxtrot 인프라 클러스터 내에서 인프라와 통신하는 것을 파악했다. 이는 PCShare RAT 페이로드를 합법적인 rdpclip.exe 프로세스에 주입하는 드로퍼(dropper) 및 로더(loader) 요소로 구성되었다. 우리는 PCShareRAT 로더를 드롭하는 데 사용되는 아래의 세 가지 샘플을 확인했다.

File Name	SHA256 Hash
Sophos System Protection Service.exe	556d34db7e60b0d25eca0d8e6b9297cd9f2174c0d2ca013c0036a067457a2d01
osloader.exe	B668f9e213282cd1b941ab8d6dd5f3dd3266011ae16c0795ca86d12a57c095cc
security_audit_template_final.doc	5802823e50e9aca0d765fa198383f74ca18859b1181cfc3f72f62667bca67dc2

Sophos System Protection Service.exe 샘플은 东莞信大融合创新研究院 (SHA1 thumbprint: 8E3991D623A7FFD86516224A0B6932785EF63F9E)에 발급된 디지털 코드 서명 인증서를 사용하여 서명되었으며, 이는 Dongguan Xinda Integrated Innovation Research Institute로 변환된다.

이 조직은 Dongguan Municipal People's Government와 PLA-SSF Information Engineering University가 공동으로 설립한 중국 군민 개방형 혁신 플랫폼이다. 우리는 이 인증서로 서명된 추가적인 파일을 확인할 수 없었는데, 이는 이것이 널리 사용되지 않음을 나타낸다. 현재 위협 활동 그룹이 코드 서명 인증서에 대한 액세스 권한을 획득한 방법은 명확하지 않지만 PLA 연계 기관과의 추가적인 관련성을 제공한다. 모든 경우에 드로퍼는 PCShare 로더를 다음 위치에 드롭하고 rundll32.exe를 사용하여 실행한다.

```
C:\{user}\AppData\Local\Microsoft\Windows\Credentials\
Winload\halmacpi.slt
```

각 로더 샘플에서 PCShare 페이로드는 로더에 의해 합법적인 프로세스 RDPclip.exe에 삽입된다. 각 PCShare 페이로드는 공통된 뮤텍스 (78de65b0701f3c9238a37)도 공유한다.

확인된 RedFoxtrot PCShare C2 도메인(supports.casacam[.]net) 중 하나가 유사한 PCShare 드로퍼 및 로더 구성요소를 사용하여 동남아시아 정부 기관을 공격한 중국 해커 그룹에 대해 설명한 2020 Bitdefender 보고서에서 언급되었다. 그러나 연구원들은 이 도메인과 RDPclip.exe에 주입되는 다른 샘플이 해당 보고서에서 분석된 FunnyDream 캠페인과는 무관한 것으로 보인다고 지적한다. 이는 이것이 중국 위협 활동 그룹들이 공유하는 도구의 또 다른 사례일 가능성이 있다는 우리의 발견과 일맥상통한다.

PlugX

Sys.exe (SHA256:c21a3a44b46e7242c0762c8ec5e8a394ddc74b747244c5b83678620ae141e59c)라는 RedFoxtrot PlugX 샘플이 2020년 9월 인도에서 멀웨어 저장소에 업로드되었다. Sys.exe는 RasTls.exe(합법적인 Symantec 실행 파일), RasTls.dll(DLL 하이재킹에 사용되는 악성 DLL), RasTls.dll.db(PlugX 페이로드)의 3개 파일이 포함된 자체 추출(self-extracting) RAR로서 많은 중국 활동 그룹들이 사용하는 DLL 하이재킹의 'triad' 기법을 반영한다.

RasTls.exe는 실행 시 악성 코드 RasTls.dll (6cd5079a69d9a68029e37f2680f44b7ba71c2b1eecf4894c2a8b293d5f768f10)을 사이드로드한 다음, RasTls.dll.db (fe18adaec076ffce63da6a2a024ce99b8a55bc40a1f06ed556e0997ba6b6d716)에서 PlugX 페이로드를 복호화하여 로드한다. 로드된 다음에는 페이로드가 TCP port 80을 통해 C2 도메인 miche.justdied[.]com에 연결한다. 이와 동일한 합법적인 Symantec 실행 파일이 여러 위협 활동 그룹에서 PlugX 로딩에 악용되었으며, 이전에 RedFoxtrot에서 IceFog와 QuickHeal을 로딩하는 데에도 사용되었다. RedFoxtrot이 사용하는 PlugX 샘플은 모두 유사한 디코딩 방법을 사용하는 MSCORE라는 내보내기 기능을 사용한다.

QUICKHEAL

또한 우리는 FireEye에서 QUICKHEAL로 추적한 악성 코드 변종과 동일한 것으로 확인된 공격자 인프라 클러스터와 관련된 다수의 샘플을 파악했다. 모든 샘플은 비정상적인 내보내기 "GetOfficeDatatal"을 실행하며, WATERFIGHT, SKYLINE 캠페인과 관련하여 FireEye가 보고한 2개의 QUICKHEAL 샘플과 여러 공통점을 갖고 있다.

주목할만한 공통 코드 중 하나는 SQLite 및 NSS 함수에 대한 메모리 주소를 로드하는 함수이다. 이 함수는 피해자의 Mozilla 프로필에서 사용자 이름과 암호 조합을 파싱(parse), 디코딩, 복호화하는데 사용된다. QUICKHEAL은 또한 백도어가 프록시에서 실행 중인지 확인하기 위해 코드를 계속 사용하고 있으며 하드코딩된 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.210을 공유한다.

Royal Road, IceFog, Poison Ivy

RedFoxtrot이 2018년과 2019년에 IceFog와 Poison Ivy 백도어를 로드하기 위해 Royal Road RTF weaponizer를 사용하는 요소는 이전에 문서화되었다. 그러나 우리는 RedFoxtrot이 이 두 가지 이외의 Royal Road를 사용하여 다른 멀웨어 패밀리를 로드하는 것을 관찰하지 못했다. 일부 중국계 그룹에서 Royal Road weaponizer를 지속적으로 광범위하게 사용하는 반면에 RedFoxtrot와 다른 몇몇 중국계 그룹들의 사용은 2020년 초부터 감소했다. RedFoxtrot이 이러한 기능을 사용하는 것에 대해서는 공개 보고에 자세히 나와있으며 중앙 아시아, 파키스탄, 인도를 타깃으로 이러한 도구를 사용한 과거 사례는 다음과 같다.

- 2019년 RedFoxtrot Royal Road 샘플 (51e3f3a762ab6fb0c3db4819560c6b1607cdcd257ce375e68fdf1a17ff5c2cb5)은 확인된 인프라 클러스터에 연결되어 있으며 C2 도메인은 2020년 말까지 활성 상태로 남아 있다. RTF 문서 제목은 "DYSL-QT_Slide_DMC_090719.doc"이며, 이는 인도 하이데라바드에 위치한 "DRDO DYSL-QT(Defence Research and Development Organisation Young Scientist Laboratory for Quantum Technologies)"에 해당한다. 또한 DMC는 DRDO Management Council과 관련된 것으로 보이며, 이 그룹이 인도 국방 연구기관을 타깃으로 한 활동에 이 미끼를 사용했음을 시사한다. RTF 문서는 C2 capture.kozow[.]com과 통신하도록 구성된 Poison Ivy SKYLINE 변종 페이로드 (367718fd58c658dce22c995f3e10bc3a5425814ddf221686e166e3129a53e897)를 드롭한다.
- 또 다른 RedFoxtrot 도메인 water.xxuz[.]com은 과거 Icefog 샘플 (ICEFOG-P version) (SHA256 : 0c596299c47ce6305e07f55397fd69d49c8cab4f4b34a617bb6670dcaac9d9f2)에 연결되어 있다. 이 샘플은 WATERFIGHT 캠페인에 사용되었을 가능성이 높다.
- 특히 2018년과 2019년에 RedFoxtrot이 사용한 2개의 Royal Road 미끼에 파키스탄과 인도의 2개 통신회사가 언급되었다. 이후 우리는 이 두 조직을 타깃으로 한 2021년 침입을 확인했다. Royal Road를 사용한 이전의 침입 시도가 성공했는지 여부는 확인할 수 없지만 통신회사들이 RedFoxtrot의 장기적인 목표임을 알 수 있다.

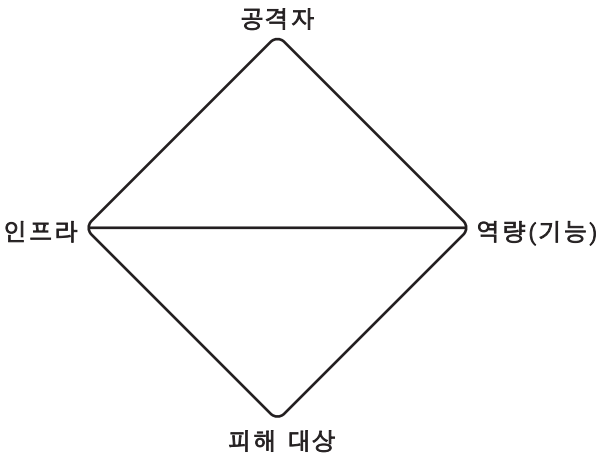
Recorded Future®

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

recordsfuture.com에서 자세한 사항을 알아보고 Twitter(@RecordedFuture)에서 팔로우하세요.