CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

April 21, 2021

Iran-Linked Threat Actor The MABNA Institute's Operations in 2020

Recorded Future®

The report aims to provide insight into Iran-linked MABNA Institute campaign activity that was reported on by Insikt Group throughout 2020, as well as by the broader cyber research community. The report is most likely to be of use to scientific organizations, academic institutions, and software groups that service the academic sector. This report will be of interest to blue team defenders working to secure academic and scientific organization's networks, as well as CTI groups that research Iran-nexus cyber activity. The Recorded Future® Platform, Insikt Group threat research, and that from Proofpoint, RiskIQ, and Malwarebytes are referenced. Data sources used to conduct this analysis include the Recorded Future® Platform, Farsight DNSDB, DomainTools and other common open-source tools and techniques.

Executive Summary

The MABNA Institute, a threat actor which has been associated with the Iran's Islamic Revolutionary Guard Corps (IRGC) by the US Department of Justice, continued its global operations against academic and research sector institutions using similar tactics, techniques, and procedures (TTPs) in 2020 as previous years, with large-scale phishing and credential theft characterizing their operations.

Throughout 2020, the MABNA Institute, or operational clusters suspected to be associated with the actor, continued to use infrastructure, including domain registration and hosting services, inside and outside of Iran. Notably, our research did not reveal new evidence of the threat actor's adoption of malware in its campaigns. This continues to suggest that while the threat actor is highly determined to lead its credential theft operations internationally and sell credentials inside Iran to research-oriented organizations, it likely sees no practical use to maintaining persistence in victim networks. This however does not preclude other elements associated with the MABNA Institute from conducting malware-based intrusions against different sectors.

Insikt Group research has further uncovered evidence to suggest that groups which hold no evidence-based association with the MABNA Institute are likely also engaging in almost identical activity. This is suggestive of an underground market that engages interested buyers with illicit access to university and library institutions all around the world.

The threat actor maintained an elevated operational tempo throughout 2020, and this pace of operations is highly likely to persist through 2021 and proceed into the Persian new year of 1400 (March 2021 to March 2022) much as it has in the past, with renewed targeting against academic and scientific organizations remaining top priorities.

Key Judgments

- Recorded Future Network Traffic Analysis from February to March 2021 revealed network communications between MABNA Institute portals and academic institutions in Spain and Switzerland.
- Due to the demand for access to research and information in Iran and international sanctions that have impacted it, the illicit market for stolen credentials will highly likely continue to drive the MABNA Institute's operations in the future.
- International tertiary academic institutions from North America, the United Kingdom, Europe, the Middle East, Africa, Asia, and the Asia-Pacific region, have been identified by Insikt Group as targets for suspected MABNA Institute operations. This characteristic in victimology is likely to continue into the future.

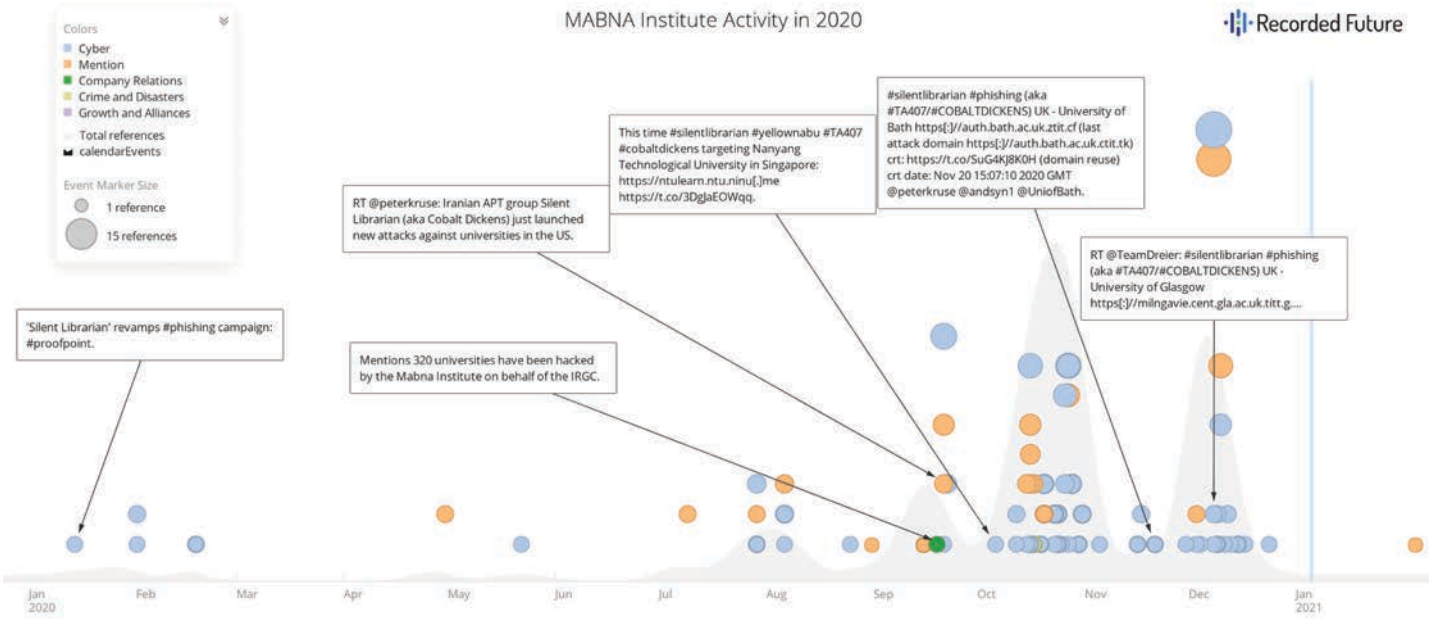

Figure 1: Open source reporting of suspected MABNA Institute activity throughout 2020, with a noticeable lull during the Persian new year period (March 2020 to April 2020) (Source: Recorded Future)

Background

Three years have passed since the US Department of Justice (USDoJ) unsealed an indictment on March 23, 2018, highlighting the operations of the MABNA Institute (aka Silent Librarian, Cobalt Dickens and TA407) which officially date back to at least September 2013. The MABNA Institute is also known by its Farsi language equivalent as the "The Young Thinkers Falinoos Company" or "شرکت ایده پردازان جوان فالینوس" (or the Falinoos Company). In its indictment, the US DoJ identified "megapaper" (megapaper[.]ir) and "gigapaper" (gigapaper[.]ir) as 2 portals used to access information pilfered from academic institutions, libraries, scientific journals, among other targets. The MABNA Institute is also reported to have targeted private sector companies as part of its operations.

The MABNA Institute's major members were identified, as were their TTPs, and their association with the Islamic Revolutionary Guard Corps (IRGC). Since the indictment, multiple cyber research groups and independent researchers have continued to identify suspected MABNA Institute activity, detailing the cyclical nature of their infrastructure use, their phishing tradecraft, and victimology (1, 2, 3, 4, 5).

Threat Analysis of Campaign Activity in 2020

Between March 2020 and March 2021, Insikt Group's tracking of suspected MABNA Institute activity did not reveal a significant pivot in TTPs commonly attributed to the threat actor; however, it maintained an aggressive operational tempo, and most of the phishing operations detected by Insikt Group revealed continued targeting against academic institutions, libraries, and scientific organizations around the world, including institutions in Australia, Estonia, Lebanon, Mexico, the Netherlands, Qatar, Singapore, Sweden, the United Kingdom, and the United States.

We believe our visibility does not comprehensively cover all of MABNA Institute operational activity. Furthermore, Insikt Group's research revealed unreported domains used throughout 2018 and 2019, and DNS infrastructure likely associated with the MABNA Institute, which suggest a portion of their activity likely remains undetected in the public domain.

Network Traffic Indicators

Using Recorded Future Network Traffic Analysis, Insikt Group identified network communications between MABNA Institute-linked IP 5.56.135[.]140, which both megapaper[.]ir and ezaccess[.]ir (an affiliate portal) uniquely resolve to, and networks associated with tertiary academic institutions. For example, from February 2021 to March 2021, 5.56.135[.]140 was observed communicating over SSL via TCP port 443 with apparent networks associated with Spanish and Swiss academic institutions. No malware activity was detected as part of the research associated with these presumed victim networks.

Throughout the investigated time frames Insikt Group also observed 5.56.135[.]140 predominantly communicating over TCP port 443 with Tor exit nodes, with sessions revealing large data transfers and evidence of users communicating with MABNA Institute portals from various locations inside Iran. VPN connections were also detected from various services such as HOXX VPN, Windscribe VPN, Google's VPN One, and TunnelBear VPN.

Operational Domain Analysis

Insikt Group research of phishing domains detected throughout 2020 revealed that they retain similar naming conventions and characteristics to domains that have been identified since the USDoJ indictment was unsealed in March 23, 2018. Central to the MABNA Institute's phishing tradecraft is the use of an apex domain, which either resembles domains of legitimate computer software such as EZProxy, or that of apex domains likely registered for short-time cyclical use (likely until detected). The latter have previously been marked by 4- or 5-letter domains, for example "unee[.]me", or "vitt[.]cf". Throughout 2020, other domains that do not mimic third-party software but have been used to target tertiary institutions include but are not limited to examples such as "servisedesk[.]me" or "liblog[.]info". In at least one instance, cyber researchers have also detected a previously identified apex domain "nlib[.]ml" which reentered operational circulation after it had been disclosed.

In relation to the subdomain structure, most of the subdomains detected by Insikt Group resemble, if not entirely mimic, the login URLs used by tertiary institutions. The identified subdomains usually include names of third-party student information systems, single sign-on (SSO) software, and academic portals that link their networks to teaching and library systems, as well as international research databases; for example, Ezproxy, ExLibris, Blackboard, ILIAS, OKTA, and Moodle, just to name a few. Once a domain is exposed publicly the threat actors have targeted the same institutions using newly registered apex domains, or by slightly altering subdomains, which enable attackers to launch new waves of phishing attacks.

whel-primo.hosted.exlibrisgroup.nuec[.]cf

login1.ezproxy.vasa.abo.fi.ezlibrarylogin[.]com

ilias.uni-marburg.edunm[.]me

Hostcampusmoodle.rgu.cfek[.]me

uon.okta.com.vitt[.]ga

login1.ep.bib.mdh.se.ezplog[.]in

Figure 2: Examples of subdomain structures revealing the use of differing apex domains (Source: Recorded Future)

Domain Registration and OPSEC

The suspected MABNA Institute operators have revealed differing levels of operational security. In some instances registered domains do not adopt privacy protections, and therefore presumed actor names and email addresses used to register their assets were revealed. These lapses revealed affiliations to companies based in Iran (see Operational Infrastructure Analysis section immediately below). In other cases, in particular with the 4- and 5-letter apex domains that leverage foreign registration and hosting/CDN providers like Freenom and Cloudflare, the opposite transpired, with the majority of identified apex domains using privacy protections. It is currently unclear whether this is representative of differing entities preparing infrastructure for phishing attacks or an indicator of different parties that have adopted the same mission.

Operational Infrastructure Analysis

Throughout 2020, MABNA Institute's targeting patterns and infrastructure use revealed the broad nature of its operations. Certificate registration data was used to reveal information about domain use (including recycling old domains) to enable activity against tertiary institutions in North America, Europe, Africa, the Middle East, East Asia, and the Asia-Pacific region. Infrastructure use was predominantly divided between domestic and international domain registration and proxy hosting services, with Freenom and Cloudflare services being among the most commonly used outside of Iran. Inside Iran, the related operational infrastructure identified by Insikt Group revealed an association between multiple domains and the ISP Sefroyek Pardaz Engineering Company (AS48715).

Domain	IP	ISP
sftt[.]tk	174.136.29[.]110	TierPoint AS36024
jitl[.]tk	174.136.29[.]110	TierPoint AS36024
servisedesk[.]me	172.67.177[.]106	Cloudflare AS13335
itlib[.]me	104.27.161[.]205	Cloudflare AS13335
ulib[.]xyz	209.190.46[.]250	ENet AS10297
ezproxy[.]in	195.201.204[.]148 / 88.135.39[.]38	Hetzner AS24940 / Sefroyek Pardaz AS48715
libpro[.]xyz	185.51.201[.]112	Sefroyek Pardaz AS48715

Table 2: A sample of suspected MABNA Institute domains detected throughout 2020 linked to foreign and Iranian ISPs (Source: Recorded Future)

Other data such as Start of Authority (SOA) or NameServer (NS) records depicted fewer demarcations between suspected MABNA Institute operational infrastructure. For example, the domain ezproxy[.]in, which resolved to IPs 195.201.204[.]148 and 178.63.53[.]55 administered by Hetzner Online GmbH (AS24940), was identified pointing to NS records of Iran-based companies such as Talash Net (talashnet[.]com), and Pouyesh Server (pouyeshserver[.]com), among others. DNS analysis has revealed the continued resolution to infrastructure, and PTR records linked to TalashNet; it is likely this entity's services have been used in suspected MABNA Institute-like operations since at least August 2019.

Domain	IP	PTR
ezpro[.]xyz	88.135.39[.]38	linux403.talashnet[.]com
libpro[.]xyz	185.51.201[.]112	linux115.talashnet[.]com
ezproxy[.]xyz	185.51.203[.]22	linux113.talashnet[.]com
liblog[.]info	185.51.201[.]112	linux115.talashnet[.]com
ezlogin[.]info	185.51.203[.]22	linux113.talashnet[.]com
ezproxy[.]in	88.135.39[.]137	linux117.talashnet[.]com
ezlibrarylogin[.]com	185.51.203[.]22	linux113.talashnet[.]com

Table 3: A sample of reverse DNS queries listed Talash Net resources (Source: Recorded Future Platform)

Another Hetzner-linked IP, 95.216.33[.]194, which resolved to liblog[.]in, also revealed links to NS data associated with the Pouyesh Server and Berbid Server (berbidserver[.]com) companies. The latter IP was also detected by Insikt Group in December 2020 and was linked to another suspected MABNA-linked operational cluster resolving to ulibr[.]xyz; again research revealed a link to an Iran-based company Server Iran (serveriran[.]net).

The Ecosystem: A Market for Stolen Credentials and Access

The MABNA Institute's operations are driven by the demand for information in the Iranian ecosystem. International sanctions have limited access to research and resources inside Iran. While the MABNA Institute's activities are categorized as an illicit operation by the USDoJ and other international bodies, one of the principal actors of the MABNA Institute, Abuzar Gohari Moqadam (who maintains a public Instagram profile), legitimized the organization's operations in an interview with official Iranian media outlets on March 24, 2018. Moqadam stated that the indictment was further proof of the US government's objective to implement a "scientific apartheid" (آپارتاید علمي) against the Islamic Republic, and insinuated that such activities would not cease.[1]

Additionally, various Iranian universities, for example Ferdowsi University, Kharazmi University, Tabriz University, and Birjand University, have advertised the services of MABNA Institute companies and websites (specifically Megapaper), to provide access to research that would otherwise be inaccessible to Iranian students.

Figure 3: Tabriz University advertises the Megapaper database linked to the MABNA Institute and a registration form to garner approval to use Megapaper via the university's library (Source: Tabriz University[2])

The identified affiliate services in Iran are further suggestive of an existing supplier market which is likely larger than what is cited in public reports. For example, the website "DownloadPaper" (downloadpaper[.]ir), which resolves to 185.141.132[.]14, an IP administered by the same Sefroyek Company, reveals an almost decade-long lifespan according to the Internet Archive "Wayback Machine". The site is likely affiliated with Gigapaper.

1 https[:]//www.irna[.]ir/news/82870383
2 https[:]//lib.tabrizu.ac[.]ir/fa/news/11540

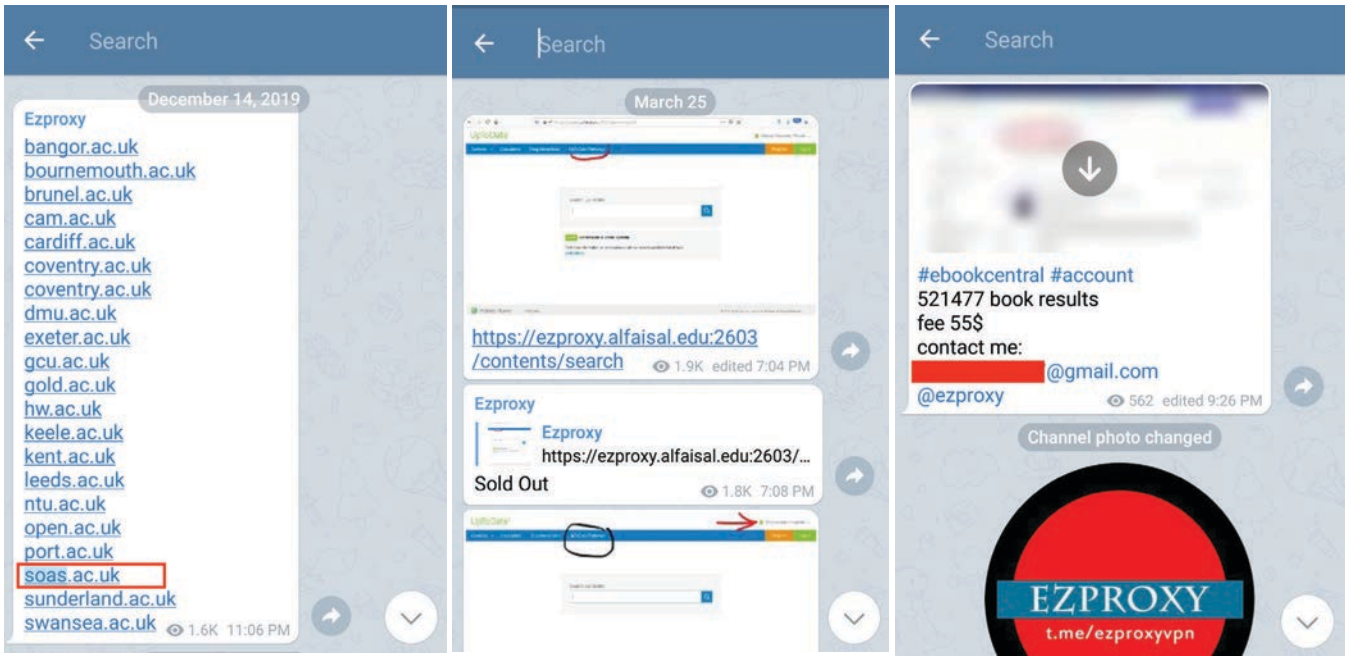

Figure 4: Evidence of Ezproxy's sale of accounts via the Telegram platform including various tertiary institutions in the UK (Source: Telegram)

An early iteration of the DownloadPaper website revealed the actor's motivations for its existence. In its "About Us" page it specified that one of the biggest problems for Iranian researchers and universities was garnering access to global research and information databases. Gaining access to international research is very costly, with a typical access price of $25 to $45 USD for each article. Payment for such resources is further described as problematic, as common payment mechanisms associated with VISA and Mastercard are not available in Iran due to international sanctions.

In some cases, research on entities that contribute to the sale of stolen credentials also depict a direct correlation to the MABNA Institute or websites affiliated with the threat actor. In December 2020, Insikt Group reported on a website which we believe is related to Gigapaper, "Unipassword" (unipassword[.]ir) due to multiple shared hosting infrastructure overlaps. The entity claims to sell account passwords belonging to globally dispersed tertiary academic institutions through a three-tiered service: "premium", "VIP three month access", and a general membership access. The Unipassword domain resolves to a Cloudflare administered IP 104.24.116[.]12. The site has been operational since at least May 5, 2013, when it first resolved to 144.76.39[.]41, a Hetzner IP. In various instances the Unipassword domain shared temporal infrastructure overlaps with Gigapaper domain from April 2014 until May 2020.

These overlaps are outlined in the following table:

Time Frame	IP
April 2014 to September 2015	176.10.37[.]81
September 2015 to March 2016	176.9.140[.]69
March 2016 to July 2017	136.243.28[.]87
July 2017 to August 2017	148.251.237[.]22
July 2017 to September 2017	46.4.143[.]18
December 2018 to May 2020	95.216.72[.]92

Table 4: Infrastructure overlaps between Unipassword and Gigapaper (Source: Recorded Future Platform)

Considering the evidence identified and listed above, we believe that Iranian universities are offering access to sites like Megapaper for students, while groups like Unipassword are suspected of doing so to independent parties and contractors. This would suggest a marketplace for stolen credentials is larger than that associated with the academic and government sectors in Iran.

Credential Theft Operations Beyond MABNA

It is unlikely that the MABNA Institute is the only threat actor engaged in credential theft operations from academic institutions as well as scientific research and journal groups.

For example, Insikt Group identified an entity calling itself "Searchbox" or "Ezproxy", depending on whether a user engages via their website hxxp[:]//searchbox[.]science, or their Telegram Channel EZProxy (t.me/ezproxyvpn). The entity dedicates the latter to the advertisement and sale of apparently compromised accounts affiliated with universities, libraries, and online databases. The Channel marketed access to victim institutions, which are very similar to those linked with the MABNA Institute. While the Channel communicates in English, errors in written form suggest the Channel administrators are likely not English-language natives.

According to information derived from the Channel, the threat actors accept payment in Bitcoin and Amazon gift cards; this information is also cited on their website. The website's WHOIS data is privacy protected, and Recorded Future data sets suggest it was registered in April 2020. Since its inception, it has resolved to Cloudflare-administered IPs 104.24.107[.]38 and 104.21.50[.]251. The website publicly advertises their access and a contact email jbarryj@protonmail[.]com (a second email, eboox.club@gmail[.]com, is advertised on the Channel) is listed for inquiries; the group further lists its Bitcoin address for payments. As of this writing, Insikt Group has not detected threat activity associated with the EzproxyVPN group. We assess that EzproxyVPN is highly likely financially motivated.

In December 2020, RiskIQ's Threat team reported on threat activity it dubbed "Shadow Academy". Beyond highlighting the detected phishing activity which mimicked the TTPs of the MABNA Institute, similar to the Ezproxy VPN development highlighted above, it also introduced an alternative hypothesis to suggest that such activity should not be isolated to the MABNA Institute. RiskIQ's analysis focused on some indicators of compromise that have been researched by Insikt Group in this report, as well as domains exposed in 2019, and others which have previously not been linked in public sources to the MABNA Institute. Their research has broadened the possible links between previously identified operational clusters. Most of the domains investigated used similar apex-to-subdomain naming conventions, but the operational infrastructure revealed few direct links to Iranian service providers.

Mitigations

- When investigating a newly discovered apex domain linked to the MABNA Institute, the Recorded Future Platform is able to detect the creation of subdomains, registered certificates, and associated DNS infrastructure via search functionality. This enables blue teams to rapidly implement defensive mitigations or block incoming email traffic from specific infrastructure nodes.
- Implement strict email filtering practices to discern from external and internal traffic, so as to avoid the spoofing of communications from IT administrations, library services, or other communications platforms.
- Alert student, research, and academic bodies of the threats posed by threat actors such as the MABNA Institute, and implement anti-social engineering and phishing training.
- Consume threat Intelligence feeds that highlight new apex domains and infrastructure, as well as intelligence about shifting TTPs.
- Proactively identify and disrupt any communications or beaconing from internal networks to suspicious infrastructure nodes.
- Maintain oversight of reporting threads in social media platforms, which alert blue teams and the broader cyber research community, when new suspected MABNA Institute domains are discovered.

Outlook

As the Persian year 1400 commences in Iran, it is highly likely that the MABNA Institute will recommence its operations much like when it was first disclosed and tracked as a threat actor in March 2018. There is little evidence, barring minor naming convention alterations, to suggest this actor will significantly change its TTPs throughout 2021.

There is insufficient information to specify whether Iranian companies that offer domain registration and hosting services to suspected MABNA Institute operators are colluding or are even aware that their server infrastructure is being used to execute phishing operations against tertiary institutions around the world. However, evidence noted previously from entities like Downloadpaper or Unipassword suggests cyber threat actors are reacting to a need for information. It is almost certain that such activity is not viewed as illegal inside Iran, and therefore not investigated and prosecuted by Iran's authorities and cyber police (FATA). Additionally, as access to academic and scientific research is framed as a revolutionary struggle, as Abuzar Gohari Moqadam termed defying the "scientific apartheid", the MABNA Institue will not lack the ideological support from Iranian power and security centers.

Notably, the cyber research community continues to label detected instances and operational clusters that are targeting international tertiary institutions as the MABNA Institute. However, surfacing evidence is starting to suggest that other entities are likely engaging in the sale of credentials linked to academic and information resources. This operational activity merits greater investigation to assess whether the threat to the academic and scientific sector is starting to expand beyond the borders of an APT group like the MABNA Institute.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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