



Leveraging Threat Intelligence in the Financial Sector

Banche & Sicurezza 2021

Gabriele Zanoni

Country Manager Mandiant, Italy

Mandiant Consulting

Prevent, detect, & respond to advanced cyber-security events and protect your organization's critical assets.



Trusted by organizations worldwide – **Over 40%** of Fortune 100 companies¹



14+ years responding to and remediating headline breaches



Mandiant DNA
Pioneers in sophisticated incident response



Portfolio of services to **assess, enhance and transform** security posture and upskill internal security staff



Cutting-edge threat intelligence informed by frontline adversary exposure



Cyber security services enabled by purpose-built technology



Global workforce of over 300 consultants in 20+ countries

Global Attacker Dwell Time



24
DAYS

Median
5
Days



66
DAYS

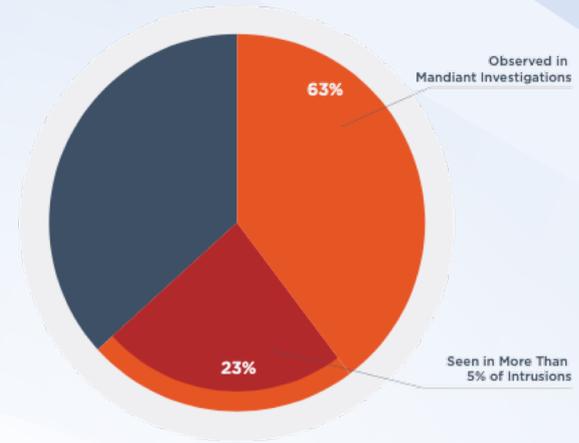
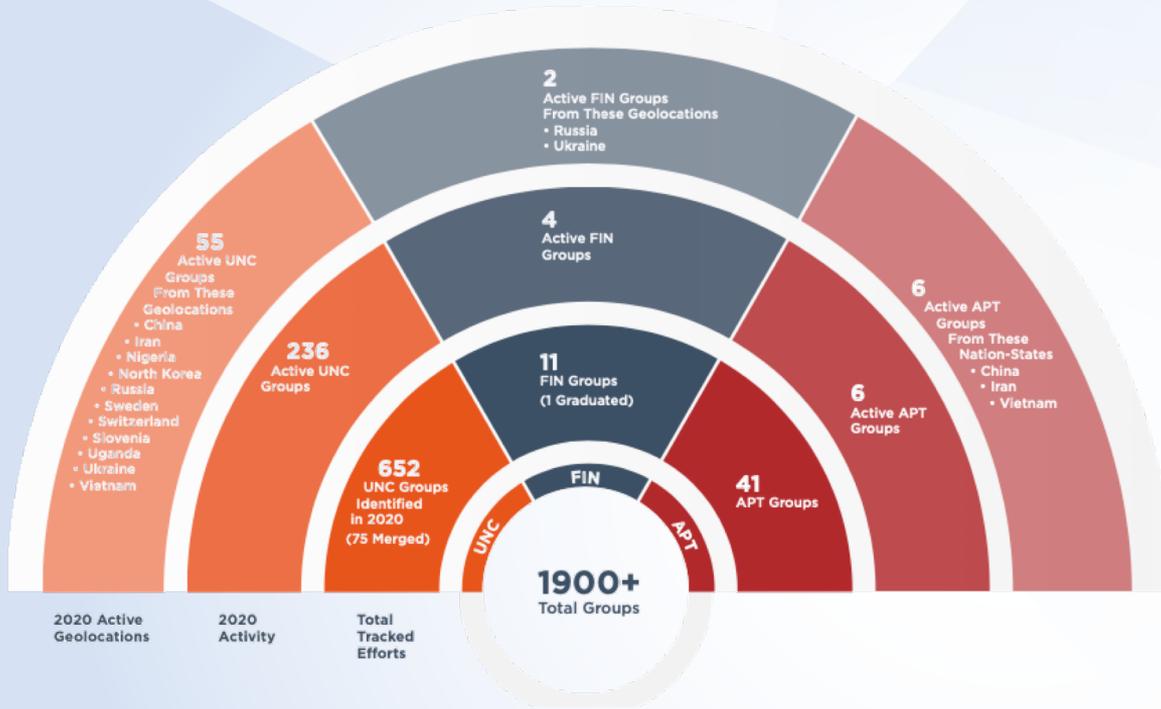
2020 Global Median Dwell Time

2020 EMEA Median Dwell Time

Over A Decade

Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
All	416	243	229	205	146	99	101	78	56	24

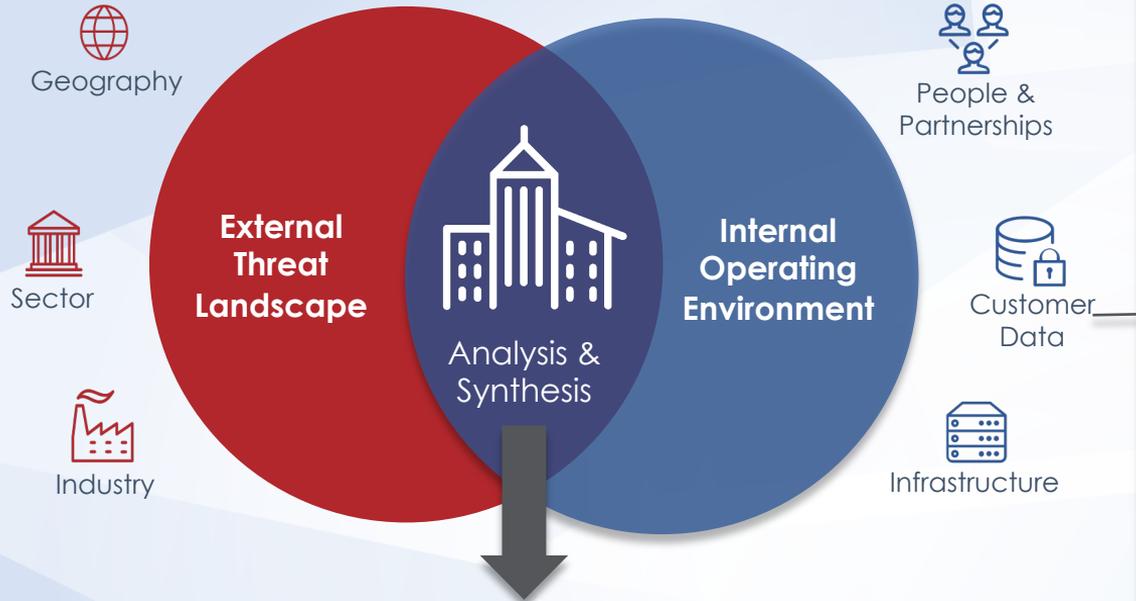
Threat Groups



MITRE ATT&CK TECHNIQUES USED MOST FREQUENTLY

- 63% of MITRE ATT&CK techniques observed
- Only 37% of the techniques observed were seen in more than 5% of intrusions.
- 81% of newly tracked malware families were non-public

Developing a Cyber Threat Profile



External threat landscape knowledge, coupled with a **clear understanding** of your **current security posture** and your ability to **anticipate, mitigate and respond** are key to success.

A Tailored Threat Profile should:

Outline the **relevant threats** you need to **prepare for**

Incorporate **evidence-based analysis techniques** to drive **threat prioritization**

Capture **key business services, critical infrastructure, operating environment** knowledge

Provide **inputs to leadership, cyber defense & risk functions**

Be a **core intelligence product** that is **updated at regular intervals** (i.e. every 6mths or annually)

Threat Identification

From the Strategic Perspective...



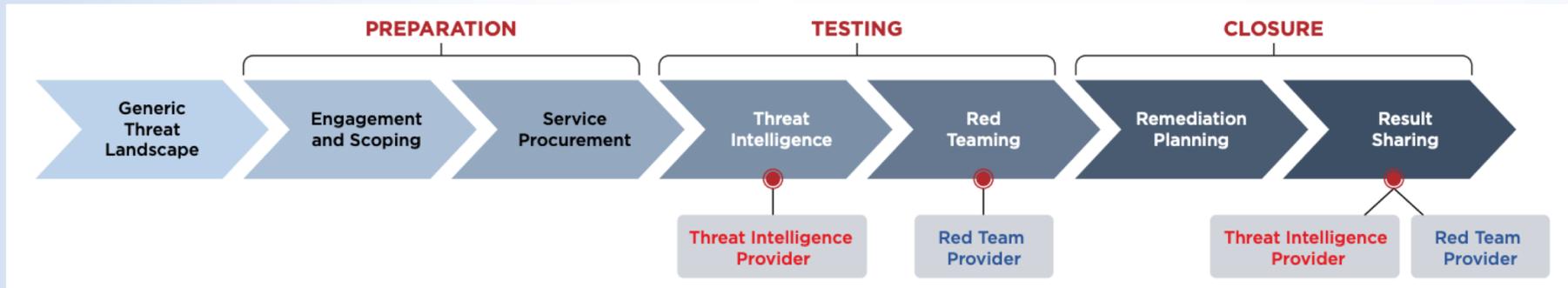
...To Attack Specifics

Year	Event
2016	JANUARY - APT28 is engaged in compromises at multiple international banks concurrently
2016	JANUARY - North Korea conducts fourth nuclear test and the first using a hydrogen bomb
2016	FEBRUARY - North Korea conducts fourth nuclear test and the first using a hydrogen bomb
2016	MARCH - UNSC Resolution 2270 prohibits UN member states from helping North Korean financial institutions supporting proliferation activities and prevents states from opening new banks in North Korea
2016	MAY - SWIFT announces Customer Security Programme with new emphasis on security
2016	SEPTEMBER - North Korea conducts fifth nuclear test involving a nuclear warhead test explosion
2016	OCTOBER - Reported beginning of warlike hole attacks orchestrated on government and media sites
2016	NOVEMBER - Following North Korea's fifth nuclear test, UNSC Resolution 2271 prohibits export of a number of minerals and coal annual sales of coal
2017	FEBRUARY - Shortly after North Korea's ballistic missile test, China suspends all imports of coal from North Korea through end of 2017 as part of its effort to impact United Nations Security Council sanctions
2017	MARCH - SWIFT bans all North Korean banks under UN guidelines from access
2017	JUNE - State-owned oil company China Petroleum Corporation suspends fuel sales to North Korea
2017	August - UNSC Resolution 2371 places strict trade restrictions on North Korea banning coal exports and limits North Korean fisheries exports
2017	SEPTEMBER - North Korea conducts sixth nuclear test setting off a hydrogen bomb
2017	SEPTEMBER - Several Chinese banks restrict financial activities of North Korean individuals and entities
2017	SEPTEMBER - UNSC Resolution 2375 imposes asset freezes on North Korean entities, bans on natural gas and coal petroleum products
2017	OCTOBER - Head of the Asian Infrastructure Bank
2017	NOVEMBER - North Korea states launch of an intercontinental ballistic missile
2017	DECEMBER - UNSC Resolution 2376 bans exports of food and agricultural products, further limits fuel imports, and directs countries to report North Korean vessels within five years
2018	JANUARY - Attempted heist at Bancorbot
2018	FEBRUARY - North reports economic data shows North Korea's trade deficit with China giving rising suspicion about continued sources of foreign currency for North Korea despite sanctions
2018	JANUARY - Russian intelligence reports cyber attacks in Pyongyang between North Korean and South Korean hackers
2018	MAY - Heist at Banco de Cuba
2018	JUNE - Trump-Ahn Summit

...			
2 - Execution	Rundl32	HOTWAX has been launched using rundl32	Example: rundl32.exe c:\windows\system32\msv2_0.dll SpsaRunInitialize
3 - Persistence	Registry Run Keys / Start Folder	NESTEGG's parent binary creates the registry keys to allow the service to run in safe mode, creating a default value the data of which is set to "Service"	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal*ServiceName* HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network*ServiceName*
5 - Defense Evasion	Disabling Security Tools	NESTEGG runs the a command to open the Windows firewall port	netsh firewall add portopening TCP <port> "Microsoft Update"
...			

Cyber Resilience for Financial Institutions with TIBER-EU

- The Threat Intelligence Based Ethical Red Teaming (TIBER) EU is a framework published by the European Central Bank for delivering “a controlled, bespoke, intelligence-led red team test of entities’ critical live production systems.”
- **Threat Intelligence** provider collects, analyses, and disseminate intelligence from other sources about relevant threat actors and probable threat scenarios for the institution.
- **Red Team** provider will execute an intelligence-led test of specified critical live production systems, people and processes that underpin the institution’s critical functions.





Prioritize Cyber Risks with Threat Intelligence

Banche & Sicurezza 2021

Gabriele Zanoni

Country Manager Mandiant, Italy

Executives are more focused on cyber resilience

- Are critical digital assets protected?
- Are we susceptible to the attack that just happened to company X?
- Can we minimize the impact of a Ransomware attack?
- Could actor group (XYZ) compromise us?
- Can we be compromised by a malicious insider or accidental loss?

Can you prioritize your cyber resilience?

Mandiant Cyber Risk Management Implementation Journey

Define and manage your cyber risk management program



- Cyber Risk Management Operations Service
- Cyber Security Program Assessment

Design a program around the assets that matter most



- Crown Jewels Security Assessment
- Cyber Security Due Diligence Service

Model, align and monitor risks that are most relevant to you



- Threat Modeling Security Service
- Threats and Vulnerability Assessment

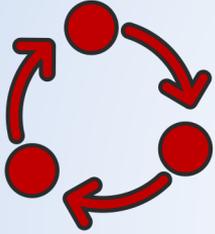
An effective, long-term cyber risk management program that is measurable and testable—at scale

Mandiant Services 2021



Ransomware Resilience Review (R3)

Ransomware is a BUSINESS issue and companies need to verify their resilience from a Strategic and Technical point of view.



Cloud Assessment

In-depth security assessments of client environments across popular cloud platforms.

Elevate security issues and justify further security investments

Crown Jewels Assessment

Identify most critical information assets, define and assess threat profile, and develop strategies for effective protection

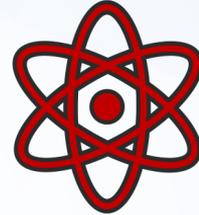


Threat Modeling

Interactive workshops to uncover unidentified risks and consider both current and future state risks [software, acquisition, complex business processes]

Cyber Due Diligence

Mitigate security challenges inherited via a merger/acquisition; or position your client's company as a seller for purchase with proper security controls



Active Directory Security Assessment

During an ADSA, Mandiant helps your organization improve the key processes, configuration standards, security and monitoring controls required to effectively secure an Active Directory environment and its supporting infrastructure.

Address the Cyber Risks that matter to you

Uplift Risk Strategies: Improve your risk management functional capabilities with corrective program actions and risk-based decision-making.

Increase Business Value: Properly balance your business innovations, security safeguards, and related investment priorities.

Protect Critical Assets: Identify and align specific cyber threats to your organization with critical business assets.

Improve Decision-Making: Lead decisions with risk analysis that leverages detailed threat intelligence and attacker insights.

Enhance Risk Prioritization: Develop integration capabilities with enterprise functions to ensure the right security risk context is applied when prioritizing business efforts.

