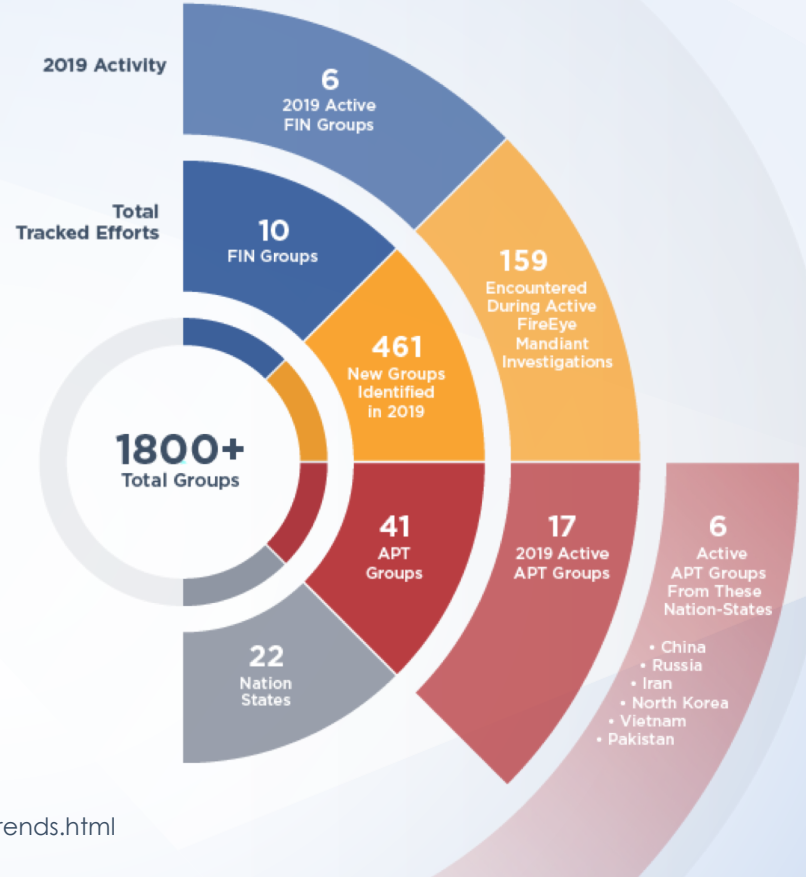
FIREEYE™ | MANDIANT®

Cyber Threat Intelligence for the Financial Sector

Gabriele Zanoni - Mandiant

Financial market is still the most attacked one

- More attackers in more diverse environments:
  - Attackers continue to grow more adept at **working across a range of operating systems** and device types
  - Attacks to both **on-premises** and **cloud** architectures.
- **461 new adversary groups** In 2019
- 41% Unknown Malware families
  - **Linux and Mac malware**
- **Ransomware** becoming second source of income for Credit Card Criminals



https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

Know what the adversary is doing right now

Breach Intelligence

Machine Intelligence

- 15,000 network sensors
- 18M endpoints
- Tens of millions of malware detonations per hour
- 65M emails processed a day

Operational Intelligence

- 5 Security Operations Centers
- 99M+ events ingested
- 21M+ alerts validated by Intel

Adversary Intelligence

- 23 countries
- 30+ languages
- 180+ analysts and researchers
- 30K intel reports per year

Expertise

- 13+ years of investigative expertise
- 26 countries with consultants
- 400+ red team exercises per year

Unique | Timely

DATA COLLECTION

Unique Data Collection

- Breach
- Operational
- Adversary

ENRICHMENT

Automated Enrichment

- Whois
- PDNS
- Virus Total
- …

SCORING ENGINE

Adding expertise through ML

- Analyst insights built into ML risk model

OUTPUT

-Score

95% Unique Hashes

5% known by VT

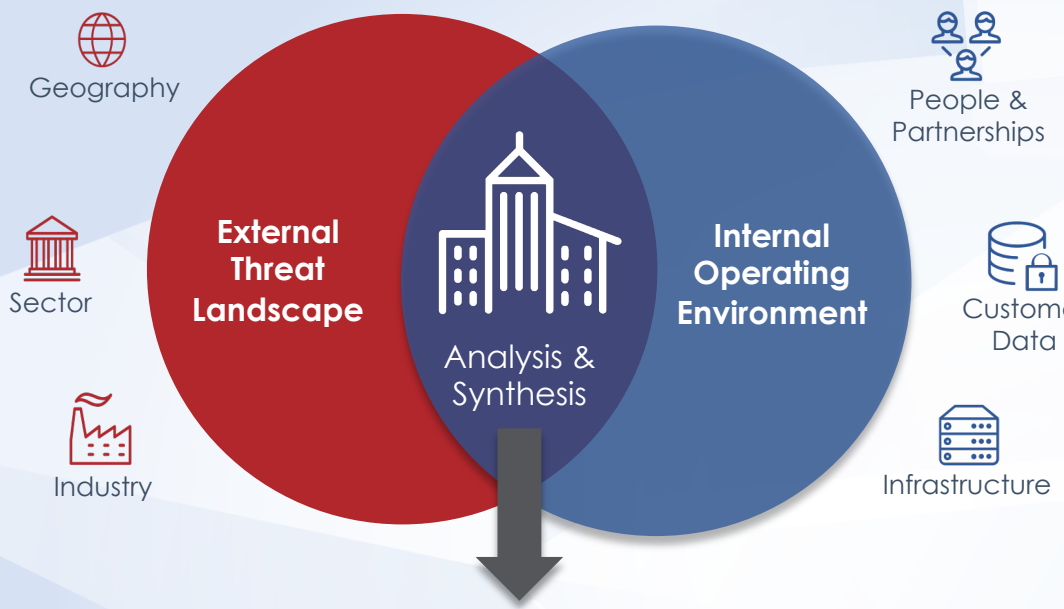
16% - Up to 40 Days Earlier

Mandiant Knows

The World Knows

When would you like to know?

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

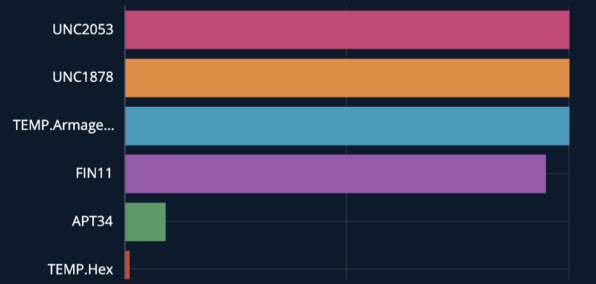
Provide **inputs to leadership, cyber defense & risk functions**

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

Global Dashboard

Actor Activity

Last quarter
3 SEP 2020 - 3 DEC 2020



Most Active Malware

Last month
3 NOV 2020 - 3 DEC 2020

- AgentTesla
- LokiBot
- FORMBOOK
- NanoCore
- Emotet
- Remcos
- Dridex
- AZORult
- Ursnif
- njRAT

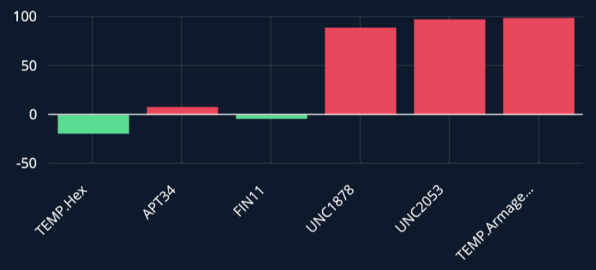
Most Active Vulnerabilities

Last month
3 NOV 2020 - 3 DEC 2020

- CVE-2017-11882
- CVE-2017-0199
- CVE-2018-11776
- CVE-2019-0708
- CVE-2012-0158
- CVE-2017-8759
- CVE-2012-1723
- CVE-2015-1641
- CVE-2014-1761
- CVE-2017-8570

Activity Trend

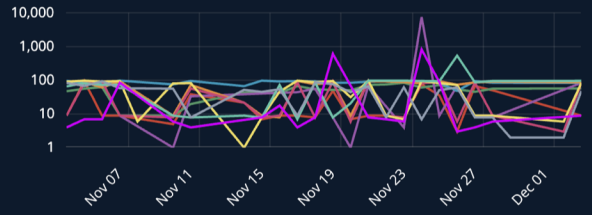
Last quarter
3 SEP 2020 - 3 DEC 2020



Malware Sightings

Last month
3 NOV 2020 - 3 DEC 2020

Andromeda BEACON BEEHIVE CHESSYLITE EQUINOX
FORMBOOK LokiBot SOGU WannaCry njRAT



Latest Reports

Filter

CVE-2020-29370 - Linux Kernel 5.5.10 Race Condition Vulnerability
Vulnerability Report — 14 MINUTES AGO

Threats to Industrial Pipelines
Trends and Forecasting — 42 MINUTES AGO

CVE-2020-29371 - Linux Kernel 5.8.3 Improper Input Validation Vulnerability
Vulnerability Report — 44 MINUTES AGO

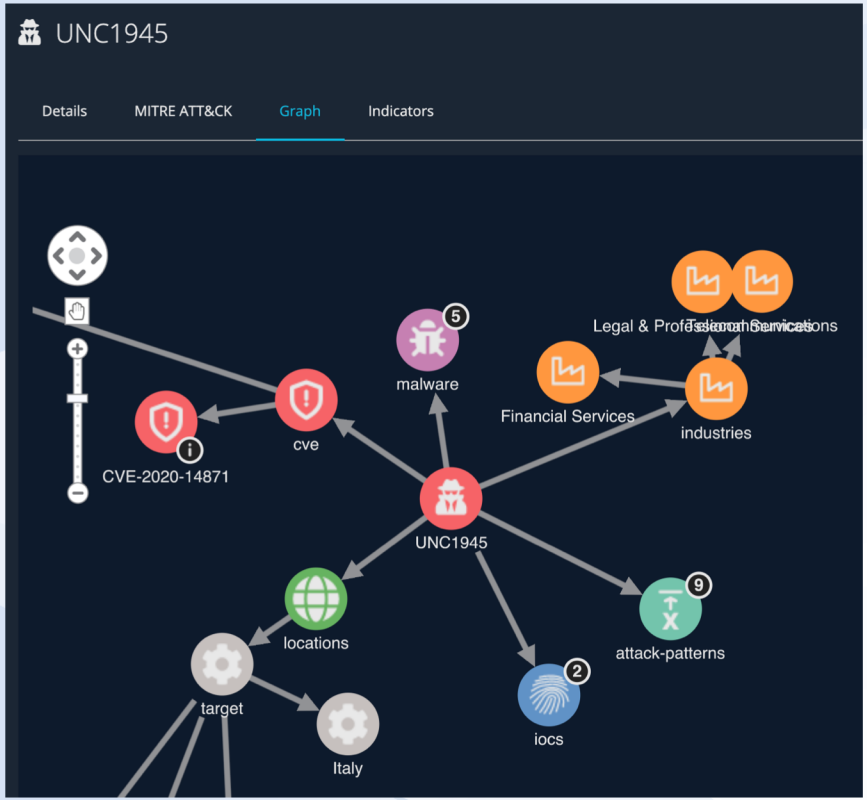
Oracle PeopleSoft Enterprise PeopleTools 8.58 Environment Mgmt Console...
Vulnerability Report — ABOUT 1 HOU

English-Speaking Actor 'mont4n4' Advertises SQLi at U.S. Banks on RAID
Threat Activity Alert — 1 DAY AGO

Russian-Speaking Actor 'InTheBox' Advertises Alien, Cerberus, and Anubis Android Malware Injects for Hungarian Banks on exploit.in
Threat Activity Alert — 1 DAY AGO

Russian-S
Threat Activit

Cyber Threat Intelligence Business outcomes



Focus on the highest-risk issues: **Prioritization**

Validate adversary-specific **controls**: Understand Relevance & Readiness

Proactively **hunt** for key adversaries: Decrease Damage

Intelligence overlaid on every workflow: **Accelerate Response**

Identify important **context** automatically: Efficiency

Better leverage existing security controls: **Optimization** / Rationalization

Mandiant Risk Rating vs. CVSS Scoring

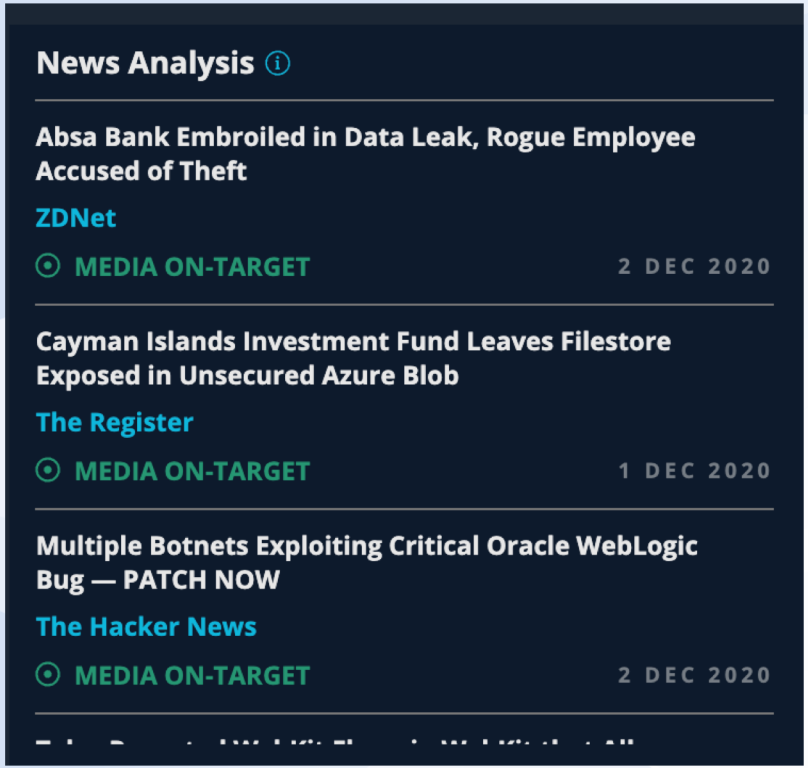
- If everything is "critical," then nothing is critical

	NVD V3 Ratings				Mandiant Ratings			
	2016	2017	2018	2019	2016	2017	2018	2019
LOW	160	93	71	113	4293	6326	5366	4145
MEDIUM	2330	3261	2990	2388	1963	1762	1606	2004
HIGH	2775	3774	3244	2945	60	68	113	106
CRITICAL	1032	1029	780	810	0	1	0	1

Threat Intelligence for assets outside your walls

- Organization Identity
- Brand & Products
- Network Info
- Social Media
- Supply Chain Protection
- BIN Numbers

Cyber New Analysis



MEDIA ON-TARGET

This ranking denotes a media trend in which the information reported is generally verifiable and can be correlated with our additional intelligence sources.

PLAUSIBLE

This ranking refers to a story possessing key information that, although plausible based off our past observations of similar events, we have not been able to validate in the short time available.

JUDGMENT WITHHELD

This ranking refers to a story which is complex enough that we cannot validate it in a short time.

MEDIA OFF-TARGET

This ranking refers to a story in which key elements are unsubstantiated or inaccurate. A story can have a key element which is inaccurate, and the rest accurate, and still receive the ranking Off Target.

https://www.fireeye.com/mandiant/advantage.html

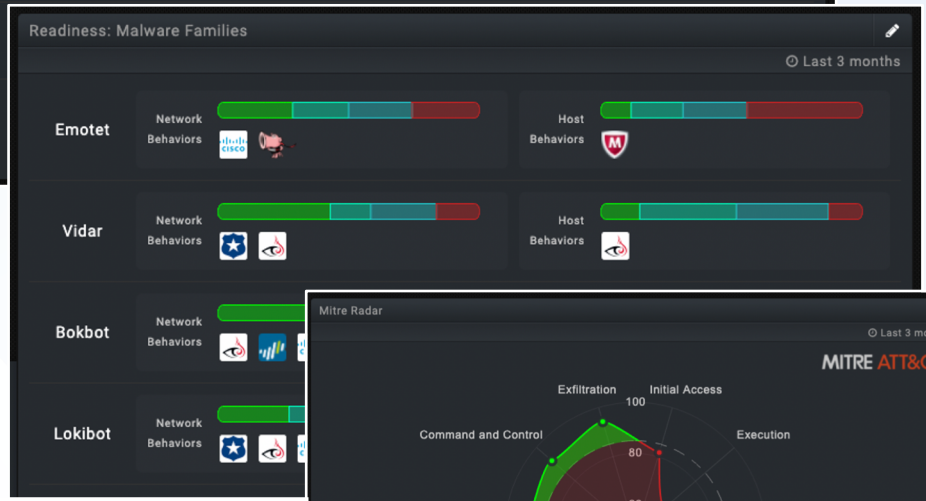
A Global Reset: Cyber Security Predictions 2021

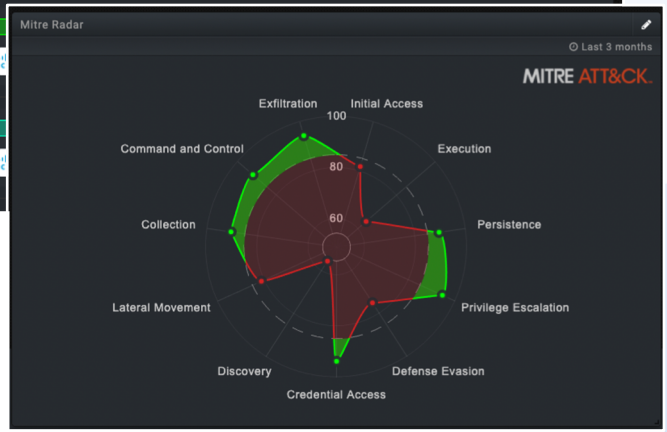
- **Remote Work and Other Impacts of the Global Pandemic**: Remote access will continue to be explored, especially around helpdesk and related employee interfaces .
- **Persistence and Growth of Ransomware**: One troubling trend is that attackers are not only making adjustments to their ransomware TTPs, but also increasingly moving to ransomware-as-a-service, which includes offering malware and the skills to deploy it on a one-time or ongoing basis .
- **Cloud Security Taking the Limelight:**
  - Stolen credentials, typically via phishing
  - Exploitation of cloud misconfigurations
  - Vulnerable cloud application hacking
- **Security Validation to Keep Defenses and Budgets in Check**: Security effectiveness as a business metric will grow in 2021, the use of the Threat Intelligence will help in focusing on the most critical priorities.

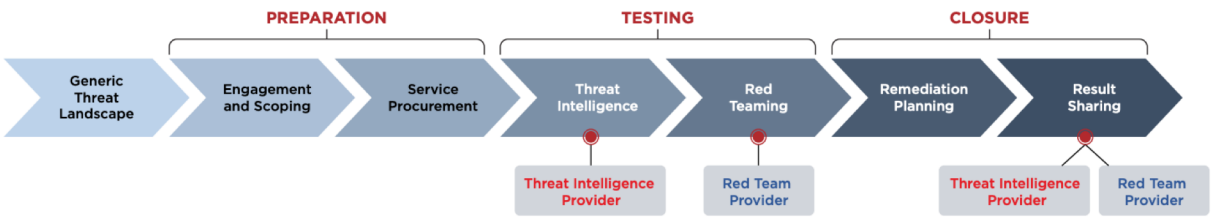
https://www.fireeye.com/current-threats/annual-threat-report/cyber-security-predictions.html

Actionable Threat Intelligence for TIBER EU assessments

- 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.







Intelligence Capability Development

Intelligence Capability Assessment
Evaluate CTI capabilities across multiple InfoSec domains and CTI disciplines, identify maturity levels and growth opportunities.

Cyber Threat Diagnostics
Identify potential or active threat actors targeting the organization through analysis of security log data.

Threat Intel Foundations
Establish the basic building blocks for developing capabilities. Identify relevant threats, the stakeholders who require visibility, and CTI requirements.

Hunt Mission Workshop
Guide analysts and operators in adopting an intelligence-driven approach to proactively identify threats, using a structured methodology.

Analytic Tradecraft Workshop
Enhance the analytical skillset necessary to support the client CTI capabilities.

Intelligence Capability Uplift
Develop scalable, repeatable processes for the collection, analysis and dissemination of intelligence throughout the organization.

Know The Threats That Matter To You Right Now

Understand recent actor, malware or vulnerability trends.

Proactively hunt threat actors targeting your organization or sector.

Accelerate your threat response by prioritizing the threats that matter most.

Access threat intelligence via the platform, the browser plugin, or APIs.

Thanks

gabriele.zanoni@mandiant.com