INTEL471

CU-GIRH

CYBER UNDERGROUND GENERAL INTELLIGENCE REQUIREMENTS HANDBOOK

CU-GIRH

CYBER UNDERGROUND GENERAL INTELLIGENCE REQUIREMENTS HANDBOOK

VERSION 4

TABLE OF CONTENTS

TABLE OF CONTENTS CONT.

WHAT IS THE CU-GIRH?

The **Cyber Underground General Intelligence Requirements Handbook (CU-GIRH)** is a baseline tool to assist in organizing, prioritizing, producing and measuring production of cyber underground intelligence.

Central to this handbook are **General Intelligence Requirements (GIRs)** — a compilation of frequently asked questions applicable to the cyber underground (i.e., illicit forums, instant messaging channels, marketplaces, products, services and adversaries). Each GIR includes a definition and the essential elements of information (EEIs) needed to answer the basic questions who, what, when, where, why and how.

WHO IS IT FOR?

Primary users of the CU-GIRH are cyber threat intelligence (CTI) planners, analysts, researchers and collection managers.

HOW IS IT USED?

The CU-GIRH can be used in a variety of ways. An analyst or researcher can use this as a hip-pocket reference to spot ad-hoc collection opportunities in the underground. An intelligence planner or manager can use this to support the development of intelligence requirements and to measure the intel team's value to its stakeholders and organization.

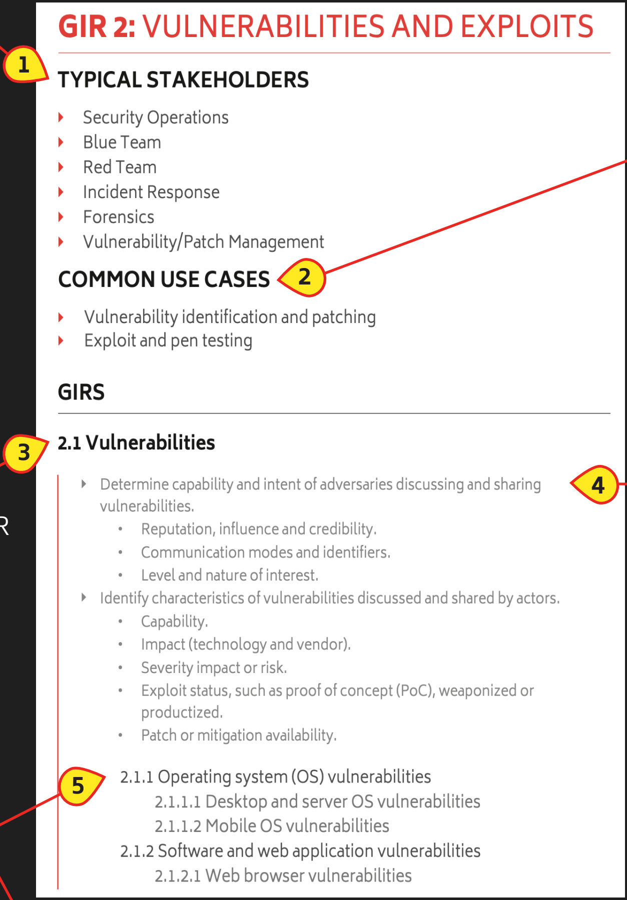
HOW DOES INTEL 471 USE THE CU-GIRH?

Intel 471 shapes its intelligence collection focus and production based largely on GIRs that have been prioritized by our customers. Using the CU-GIRH, each customer selects and ranks a subset of GIRs that Intel 471 uses to task collection and synchronize reporting.

For more information about the GIR framework, visit our blog at **blog.intel471.com**.

ANATOMY OF THE CU-GIR

Intelligence consumers typically interested in this GIR category



GIR 2: VULNERABILITIES AND EXPLOITS

TYPICAL STAKEHOLDERS

- Security Operations
- Blue Team
- Red Team
- Incident Response
- Forensics
- Vulnerability/Patch Management

COMMON USE CASES

- Vulnerability identification and patching
- Exploit and pen testing

GIRS

2.1 Vulnerabilities

- Determine capability and intent of adversaries discussing and sharing vulnerabilities.
  - Reputation, influence and credibility.
  - Communication modes and identifiers.
  - Level and nature of interest.
- Identify characteristics of vulnerabilities discussed and shared by actors.
  - Capability.
  - Impact (technology and vendor).
  - Severity impact or risk.
  - Exploit status, such as proof of concept (PoC), weaponized or productized.
  - Patch or mitigation availability.

2.1.1 Operating system (OS) vulnerabilities

2.1.1.1 Desktop and server OS vulnerabilities

2.1.1.2 Mobile OS vulnerabilities

2.1.2 Software and web application vulnerabilities

2.1.2.1 Web browser vulnerabilities

Typical use cases supported by this GIR

Parent GIR category

Essential Elements of Information (EEIs) for each GIR parent category and subcategories; each EEI can be used as specific intelligence requirement that informs stakeholder

GIR subcategory; inherits parent attributes and EEIs

INTELLIGENCE PLANNING ESSENTIALS CHECKLIST

> The following steps can be implemented using the comprehensive Intel 471 **Intelligence Planning Workbook**, which includes templates and samples to get you started. Contact us at **intelligence@intel471.com** to get the most recent copy of the workbook.

STEP 1

GATHER AND PRIORITIZE INTELLIGENCE REQUIREMENTS FROM KEY STAKEHOLDERS

Create a master stakeholder list with contact details. Survey all stakeholders to understand their use cases and Priority Intelligence Requirements (PIRs). Using the GIR list, select, rank, consolidate and prioritize all stakeholder PIRs into a master PIR register.

STEP 2

CREATE INTELLIGENCE COLLECTION PLAN

Create a plan that employs available collection assets and data sources to address your stakeholders' PIRs.

STEP 3

PUBLISH INTELLIGENCE

Deliver tactical, operational and strategic intelligence products that consistently satisfy your stakeholders' PIRs. Label or tag reports and deliverables with applicable GIRs.

STEP 4

MEASURE SUCCESS

Record intelligence production and stakeholder feedback to track progress against PIRs and return of investment over time. Use the GIRs as a baseline tool for quantifying and qualifying production.

INTELLIGENCE PLANNING: STEP 1

GATHER AND PRIORITIZE INTELLIGENCE REQUIREMENTS FROM KEY STAKEHOLDERS

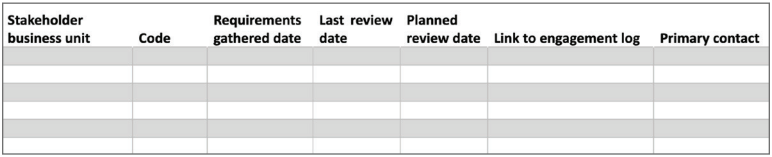
> PURPOSE
>
> This is where it all begins. As intel professionals, we know our job is to be the eyes and ears for our stakeholders to provide them the situational awareness they need to protect our organizations. To do this effectively, you must prioritize and synchronize your collection and production to the needs - or "intelligence requirements" - of your key stakeholders.

DESIRED GOAL

- A master **Stakeholder List** and **Priority Intelligence Requirements (PIR) Register** - a consolidated and prioritized list of intelligence requirements from all key stakeholders.

STEPS

- Create master list of key stakeholders (*Figure 1*) - the business units charged with securing your organization against cyber threats. Typical stakeholders include:
    - Senior or Executive Management
    - Network or Security Operations
    - Fraud
    - Vulnerability or Patch Management
    - Incident Response
    - Forensics
    - Legal and Privacy
    - Risk Management

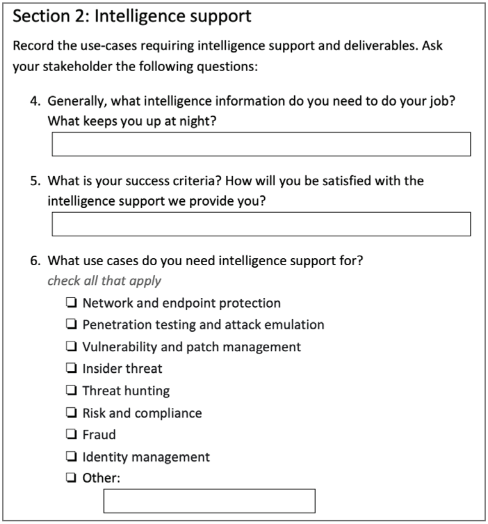


Stakeholder business unit	Code	Requirements gathered date	Last review date	Planned review date	Link to engagement log	Primary contact

Figure 1: Stakeholder Master List Template

INTELLIGENCE PLANNING: STEP 1 CONT.

- Complete a key stakeholder interview (*Figure 2*) with each business unit to:
  - Evangelize the mission and purpose of intelligence in your organization.
  - Understand stakeholder use cases for intelligence and the decisions they need to make to do their jobs effectively.
  - Select and rank up to 10 General Intelligence Requirements (GIRs). This becomes each stakeholder's list of PIRs.
  - Agree to the content, frequency and delivery of intelligence you will produce for each stakeholder.
  - Agree to the format, scope and delivery mechanism for ad-hoc Requests for Information (RFIs).



Section 2: Intelligence support

Record the use-cases requiring intelligence support and deliverables. Ask your stakeholder the following questions:

4. Generally, what intelligence information do you need to do your job? What keeps you up at night?

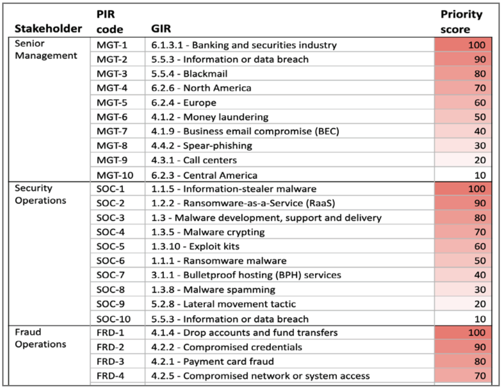
5. What is your success criteria? How will you be satisfied with the intelligence support we provide you?

6. What use cases do you need intelligence support for?
   check all that apply
   - ❑ Network and endpoint protection
   - ❑ Penetration testing and attack emulation
   - ❑ Vulnerability and patch management
   - ❑ Insider threat
   - ❑ Threat hunting
   - ❑ Risk and compliance
   - ❑ Fraud
   - ❑ Identity management
   - ❑ Other:

Figure 2: A section of the 10-question Stakeholder Interview Form Template

INTELLIGENCE PLANNING: STEP 1 CONT.

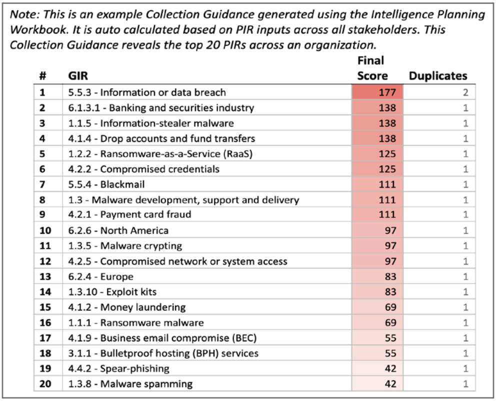
- Consolidate and prioritize all stakeholder PIRs into a master **PIR Register** (*Figure 3*).
  - Record individual PIRs into a single document.



Stakeholder	PIR code	GIR	Priority score
Senior Management	MGT-1	6.1.3.1 - Banking and securities industry	100
	MGT-2	5.5.3 - Information or data breach	90
	MGT-3	5.5.4 - Blackmail	80
	MGT-4	6.2.6 - North America	70
	MGT-5	6.2.4 - Europe	60
	MGT-6	4.1.2 - Money laundering	50
	MGT-7	4.1.9 - Business email compromise (BEC)	40
	MGT-8	4.4.2 - Spear-phishing	30
	MGT-9	4.3.1 - Call centers	20
	MGT-10	6.2.3 - Central America	10
Security Operations	SOC-1	1.1.5 - Information-stealer malware	100
	SOC-2	1.2.2 - Ransomware-as-a-Service (RaaS)	90
	SOC-3	1.3 - Malware development, support and delivery	80
	SOC-4	1.3.5 - Malware crypting	70
	SOC-5	1.3.10 - Exploit kits	60
	SOC-6	1.1.1 - Ransomware malware	50
	SOC-7	3.1.1 - Bulletproof hosting (BPH) services	40
	SOC-8	1.3.8 - Malware spamming	30
	SOC-9	5.2.8 - Lateral movement tactic	20
	SOC-10	5.5.3 - Information or data breach	10
Fraud Operations	FRD-1	4.1.4 - Drop accounts and fund transfers	100
	FRD-2	4.2.2 - Compromised credentials	90
	FRD-3	4.2.1 - Payment card fraud	80
	FRD-4	4.2.5 - Compromised network or system access	70

Figure 3: Sample Priority Intelligence Requirements (PIR) Register

- Consolidate, weigh, deduplicate and score all PIRs across all stakeholders into one master list. This becomes your team's **Collection Guidance** *(Figure 4)*.



Note: This is an example Collection Guidance generated using the Intelligence Planning Workbook. It is auto calculated based on PIR inputs across all stakeholders. This Collection Guidance reveals the top 20 PIRs across an organization.

#	GIR	Final Score	Duplicates
1	5.5.3 - Information or data breach	177	2
2	6.1.3.1 - Banking and securities industry	138	1
3	1.1.5 - Information-stealer malware	138	1
4	4.1.4 - Drop accounts and fund transfers	138	1
5	1.2.2 - Ransomware-as-a-Service (RaaS)	125	1
6	4.2.2 - Compromised credentials	125	1
7	5.5.4 - Blackmail	111	1
8	1.3 - Malware development, support and delivery	111	1
9	4.2.1 - Payment card fraud	111	1
10	6.2.6 - North America	97	1
11	1.3.5 - Malware crypting	97	1
12	4.2.5 - Compromised network or system access	97	1
13	6.2.4 - Europe	83	1
14	1.3.10 - Exploit kits	83	1
15	4.1.2 - Money laundering	69	1
16	1.1.1 - Ransomware malware	69	1
17	4.1.9 - Business email compromise (BEC)	55	1
18	3.1.1 - Bulletproof hosting (BPH) services	55	1
19	4.4.2 - Spear-phishing	42	1
20	1.3.8 - Malware spamming	42	1

Figure 4: Sample Collection Guidance

INTELLIGENCE PLANNING: STEP 2

CREATE INTELLIGENCE COLLECTION PLAN

PURPOSE

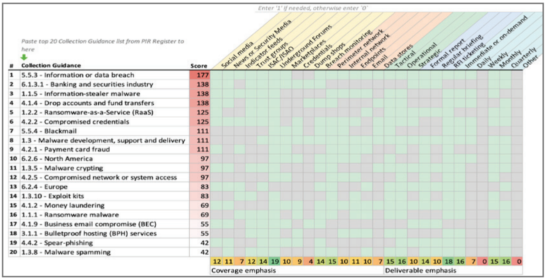
Now that your PIR register is complete and your **Collection Guidance** is in hand, you will develop a **Collection Plan** to ensure you have the necessary coverage and resources to fulfill the PIRs, taking into account the available resources and capabilities of your Cyber Threat Intelligence (CTI) team.

DESIRED GOAL

- A **Collection Plan** that employs available assets and data sources to consistently address your organization's PIRs.

STEPS

- Populate your **Collection Guidance** into your **Collection Plan** (*Figure 5*).
- Use the **Collection Plan** matrix to:
  - (Optional) List specific intelligence requirements corresponding to your **Collection Guidance**. These will become the questions you must answer in your intelligence products.
  - Evaluate available and anticipated resources against your **Collection Guidance**.



Paste top 20 Collection Guidance list from PIR Register to here

Enter '1' if needed, otherwise enter `0`

#	Collection Guidance	Score	Social media	News or Security Media	Indicator feeds	Trust groups	ISAC/ISAO	Underground Forums	Marketplaces	Credentials	Dump shops	Breach monitoring	Perimeter network	Internal network	Endpoints	Email	Data stores	Tactical	Operational	Strategic	Formal report	Regular briefing	RFI ticketing	Immediate or on-demand	Daily	Weekly	Monthly	Quarterly	Other
1	5.5.3 - Information or data breach	177	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	🟩	🟩	⬜
2	6.1.3.1 - Banking and securities industry	138	🟩	🟩	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	⬜	🟩	🟩	⬜
3	1.1.5 - Information-stealer malware	138	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	⬜	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	⬜	🟩	⬜	⬜
4	4.1.4 - Drop accounts and fund transfers	138	🟩	🟩	⬜	🟩	🟩	🟩	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	🟩	⬜
5	1.2.2 - Ransomware-as-a-Service (RaaS)	125	🟩	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	⬜	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	🟩	🟩	⬜
6	4.2.2 - Compromised credentials	125	🟩	🟩	🟩	🟩	🟩	🟩	⬜	🟩	⬜	🟩	🟩	🟩	🟩	⬜	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	🟩	⬜	🟩	🟩	⬜
7	5.5.4 - Blackmail	111	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	⬜	🟩	🟩	🟩	⬜	⬜	🟩	🟩	⬜	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	⬜
8	1.3 - Malware development, support and delivery	111	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	🟩	🟩	⬜
9	4.2.1 - Payment card fraud	111	🟩	⬜	🟩	⬜	⬜	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	🟩	⬜	⬜	🟩	⬜	🟩	⬜	🟩	⬜	⬜	⬜	🟩	🟩	⬜
10	6.2.6 - North America	97	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	⬜	🟩	🟩	🟩	🟩	⬜	⬜	🟩	⬜	🟩	🟩	🟩	🟩	🟩	🟩	⬜	🟩	🟩	⬜
11	1.3.5 - Malware crypting	97	🟩	🟩	⬜	🟩	🟩	🟩	⬜	⬜	⬜	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	⬜
12	4.2.5 - Compromised network or system access	97	⬜	⬜	⬜	⬜	⬜	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	🟩	⬜	🟩	⬜	🟩	🟩	⬜	⬜	🟩	⬜	⬜
13	6.2.4 - Europe	83	🟩	🟩	🟩	⬜	🟩	⬜	⬜	⬜	⬜	🟩	🟩	⬜	⬜	🟩	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	🟩	⬜
14	1.3.10 - Exploit kits	83	⬜	⬜	🟩	🟩	⬜	🟩	⬜	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	🟩	🟩	⬜	🟩	⬜	🟩	🟩	⬜	⬜	🟩	⬜	⬜
15	4.1.2 - Money laundering	69	🟩	🟩	⬜	⬜	⬜	🟩	🟩	🟩	⬜	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	⬜
16	1.1.1 - Ransomware malware	69	⬜	⬜	🟩	🟩	🟩	🟩	⬜	🟩	⬜	🟩	🟩	⬜	🟩	🟩	⬜	🟩	🟩	⬜	⬜	⬜	🟩	🟩	⬜	⬜	⬜	🟩	⬜
17	4.1.9 - Business email compromise (BEC)	55	🟩	🟩	⬜	🟩	🟩	🟩	🟩	⬜	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	⬜	⬜	⬜	⬜	🟩	🟩	⬜
18	3.1.1 - Bulletproof hosting (BPH) services	55	⬜	⬜	⬜	🟩	🟩	🟩	⬜	🟩	⬜	⬜	⬜	🟩	🟩	🟩	⬜	🟩	🟩	⬜	⬜	⬜	🟩	🟩	⬜	⬜	⬜	🟩	⬜
19	4.4.2 - Spear-phishing	42	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	⬜	🟩	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	⬜
20	1.3.8 - Malware spamming	42	⬜	🟩	⬜	🟩	🟩	🟩	⬜	⬜	⬜	🟩	🟩	⬜	⬜	🟩	⬜	🟩	🟩	⬜	🟩	🟩	🟩	🟩	⬜	⬜	🟩	🟩	⬜
			12	11	7	12	14	19	10	9	4	14	15	10	11	10	7	15	16	10	14	10	18	16	7	0	15	16	0
			Coverage emphasis															Deliverable emphasis											

Figure 5: Sample Collection Plan

INTELLIGENCE PLANNING: STEP 3

PUBLISH INTELLIGENCE

PURPOSE

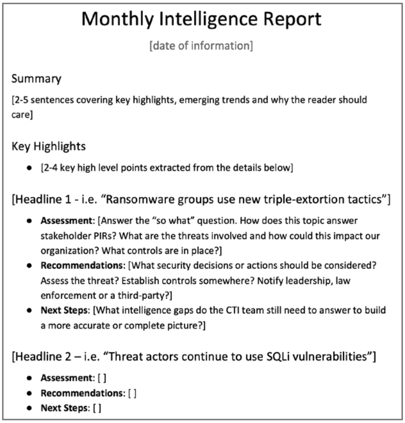
You are now ready to start collecting, compiling and analyzing data from your available sources and delivering intelligence that satisfies your stakeholders' PIRs.

DESIRED GOAL

- Deliver strategic, operational and tactical intelligence products that routinely satisfy your organization's PIRs.

STEPS

- Use stakeholder interviews and the **Collection Plan** to determine appropriate report types, cadence and delivery based on the needs of each stakeholder.
- Start by compiling a regular **Monthly Intelligence Report** (*Figure 6*) for senior management.



Monthly Intelligence Report

[date of information]

Summary

[2-5 sentences covering key highlights, emerging trends and why the reader should care]

Key Highlights

- [2-4 key high level points extracted from the details below]

[Headline 1 - i.e. "Ransomware groups use new triple-extortion tactics"]

- **Assessment:** [Answer the "so what" question. How does this topic answer stakeholder PIRs? What are the threats involved and how could this impact our organization? What controls are in place?]
- **Recommendations:** [What security decisions or actions should be considered? Assess the threat? Establish controls somewhere? Notify leadership, law enforcement or a third-party?]
- **Next Steps:** [What intelligence gaps do the CTI team still need to answer to build a more accurate or complete picture?]

[Headline 2 – i.e. "Threat actors continue to use SQLi vulnerabilities"]

- **Assessment:** [ ]
- **Recommendations:** [ ]
- **Next Steps:** [ ]

Figure 6: First page of Monthly Intelligence Report Template

INTELLIGENCE PLANNING: STEP 3 CONT.

- Consider the key elements of intelligence reporting:
    - Address the "so what" question at the very beginning to communicate how and why the report will support the reader.
    - Consider your audience - tactical, operational or strategic.
    - Separate facts from analytical judgments.
    - Use estimative probability language and avoid "weasel words."
    - Cite data and information sources using footnotes.
    - Tier or rank threats based on potential or probability for impact.
    - Tag individual reports with appropriate GIR(s) that are answered throughout.
- Use the **Collection Guidance** to:
    - Steer and focus your collection and production efforts based on stakeholder and organizational intelligence needs.
    - Look for gaps and opportunities in your reporting.

INTELLIGENCE PLANNING: STEP 4

MEASURE SUCCESS

> PURPOSE
>
> Consistently track production against requirements to demonstrate the value of intelligence to your stakeholders and organization. Regularly seek, gather and analyze feedback from each stakeholder to evaluate how well your intelligence is supporting their needs.

DESIRED GOAL

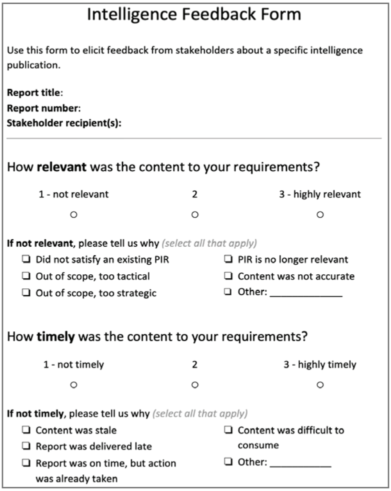
- Capture and share production metrics with each stakeholder using PIR Satisfaction Reporting. Gather and assess feedback from stakeholders.

STEPS

- Create a tracking inventory of all published intelligence.
  - Map each published intelligence to the corresponding GIR(s) covered.
- Establish a feedback mechanism that is *frictionless*, *meaningful* and *measurable*.
  - **Frictionless**: The key is to meet your stakeholder where they are to ensure optimal participation and contribution. Keep in mind certain feedback mechanisms might work better for some stakeholders than others. Options include:
    - Feedback form (*Figure 7*)
    - General surveys
    - In-person Q&A sessions
    - Coffee or happy hour meetups
  - **Meaningful**: Base your feedback loop on production quality, not quantity.
    - Quality = timeliness + relevance.

INTELLIGENCE PLANNING: STEP 4 CONT.

- **Measurable**: Apply a numerical scale to stakeholder feedback input so you can aggregate and analyze responses across all stakeholders over time. This will help drive the ROI narrative and provide objective evidence of your value.



Intelligence Feedback Form

Use this form to elicit feedback from stakeholders about a specific intelligence publication.

Report title:
Report number:
Stakeholder recipient(s):

How **relevant** was the content to your requirements?

1 - not relevant	2	3 - highly relevant
○	○	○

If not relevant, please tell us why *(select all that apply)*

❑ Did not satisfy an existing PIR
❑ Out of scope, too tactical
❑ Out of scope, too strategic
❑ PIR is no longer relevant
❑ Content was not accurate
❑ Other: ___________

How **timely** was the content to your requirements?

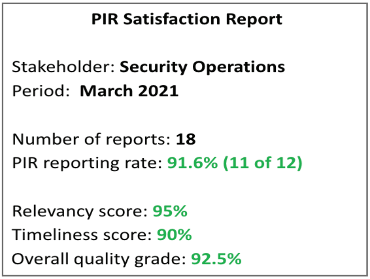
1 - not timely	2	3 - highly timely
○	○	○

If not timely, please tell us why *(select all that apply)*

❑ Content was stale
❑ Report was delivered late
❑ Report was on time, but action was already taken
❑ Content was difficult to consume
❑ Other: __________

Figure 7: Intelligence Feedback Form Template

- Schedule formal stakeholder review sessions no less than every quarter to review and revise PIR selections as needed (*Figure 8*).



PIR Satisfaction Report

Stakeholder: **Security Operations**
Period: **March 2021**

Number of reports: **18**
PIR reporting rate: **91.6% (11 of 12)**

Relevancy score: **95%**
Timeliness score: **90%**
Overall quality grade: **92.5%**

Figure 8: Monthly PIR satisfaction reporting for each stakeholder

CYBER UNDERGROUND GENERAL INTELLIGENCE REQUIREMENTS (GIRs)

GIR 1: MALWARE

TYPICAL STAKEHOLDERS

- Security Operations
- Blue Team
- Red Team
- Incident Response
- Forensics
- Threat Hunting

COMMON USE CASES

- Network and endpoint protection
  - Identify, block and mitigate malware targeting brand, industry, supply chain or geography
  - Attack reproduction and pen testing
- Attack investigation and remediation

GIRS

1.1 Malware variants

- Determine capability and intent of adversaries developing, sharing, discussing and operating malware.
  - Reputation, influence and credibility.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify the characteristics of existing, new and emerging malware variants and campaigns.
  - Functionality.
  - Capability.
  - Signatures.
  - Distribution methods.
  - Targeting (industry and geographic).
  - Impact (potential and real).
- Determine when new variants will come to market.
- Determine the various countermeasures to which malware operators are adapting.

1.1.1 Ransomware malware

- Identify available decryption capabilities.

1.1.2 Mobile malware

- Determine operating systems targeted by mobile malware.

1.1.3 Remote access trojan (RAT) malware

- Identify the impacted or targeted operating system or network device.

1.1.4 Banking trojan malware

- Identify the impacted or targeted financial institutions and applications.

1.1.5 Information-stealer malware

- Identify the type and location of data targeted for theft.
- Determine the methods and functionality used to collect and log stolen information.

1.1.6 Loader malware

- Identify the malicious payload(s) dropped.

1.1.7 Botnet malware

- Identify known associations with other malware families.
- Identify unique controller functionality.
- Determine potential migration or countermeasure suggestions.

1.1.8 Worm malware

- Identify vulnerabilities leveraged.

1.1.9 Point-of-sale (PoS) malware

- Identify how malware is deployed onto PoS device.
- Determine the type(s) and volume of payment card data targeted or stolen.

1.1.10 ATM malware

- Determine ATM vendors targeted by ATM malware.

1.1.11 Internet of Things (IoT) malware

- Determine IoT vendors or technologies targeted by IoT malware.

1.1.12 Denial of service (DoS) malware

- Identify Open System Interconnection (OSI) model targeted.
- Identify the protocol leveraged and/or targeted.
- Identify dependencies (e.g., open source technologies) required for functionality.

1.1.13 Proxy malware

- Identify devices targeted for proxy malware (e.g., MikroTik routers).
- Determine any secondary malware used in conjunction with proxy malware.
- Identify proxy protocol (e.g., SOCKS5).

1.1.14 Destructive malware

- Identify method(s) used for data destruction.
- Determine types of data targeted for destruction.

1.1.15 Cryptomining malware

- Identify mined cryptocurrency types.
- Identify platform(s) targeted.
- Identify method(s) for installation.

1.2 Malware-as-a-service (MaaS)

- Determine capability and intent of adversaries developing, administrating, purchasing and discussing MaaS platforms.
  - Reputation, influence and credibility.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify the characteristics of existing, new and emerging MaaS platforms and associated malware variants and campaigns.
  - Functionality.
  - Capability.
  - Signatures.
  - Distribution methods.
  - Targeting (industry and geographic).
  - Impact (potential and real).
- Determine when new MaaS offerings will come to market or came online.
- Determine the various countermeasures to which MaaS administrators and operators are adapting.

1.2.1 Multifunctional malware-as-a-service (MaaS)

1.2.2 Ransomware-as-a-service (RaaS)

- Identify affiliate operators and groups.
- Identify tactics used by RaaS operators to pressure victims into paying.

- Determine precursor tool sets and activities that are precursors to ransomware attacks.
- Locate RaaS blackmail blog(s).

1.3 Malware development, support and delivery

- Determine capability and intent of adversaries involved the development, support and distribution of malware.
  - Reputation, influence and credibility.
  - Capability and intent.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify characteristics of existing, new and emerging products, services and goods used to support the development and distribution of malware.

1.3.1 Malware installs

1.3.2 Malvertising

1.3.3 Malware source code

1.3.4 Web-injects

- Identify suppliers and consumers of web-injects.
- Determine malware families or variants that use web-injects.

1.3.4.1 Automatic transfer systems (ATSs)

1.3.5 Malware crypting

1.3.6 Counter antivirus (CAV)

1.3.7 Rogue certificates

1.3.7.1 Rogue code-signing certificates

1.3.7.2 Rogue web certificates

1.3.8 Malware spamming

1.3.9 Traffic redistribution system

1.3.10 Exploit kits

1.3.11 Illicit use of legitimate tools and software

1.3.11.1 Post-exploitation frameworks

1.3.11.2 Network scanners

1.3.11.3 Authentication and credential tools

1.3.11.4 Active Directory tools

1.3.11.5 Remote access tools

GIR 2: VULNERABILITIES AND EXPLOITS

TYPICAL STAKEHOLDERS

- Security Operations
- Blue Team
- Red Team
- Incident Response
- Forensics
- Vulnerability/Patch Management

COMMON USE CASES

- Vulnerability identification and patching
- Exploit and pen testing

GIRS

2.1 Vulnerabilities

- Determine capability and intent of adversaries discussing and sharing vulnerabilities.
    - Reputation, influence and credibility.
    - Communication modes and identifiers.
    - Level and nature of interest.
- Identify characteristics of vulnerabilities discussed and shared by actors.
    - Capability.
    - Impact (technology and vendor).
    - Severity impact or risk.
    - Exploit status, such as proof of concept (PoC), weaponized or productized.
    - Patch or mitigation availability.

2.1.1 Operating system (OS) vulnerabilities

2.1.1.1 Desktop and server OS vulnerabilities

2.1.1.2 Mobile OS vulnerabilities

2.1.2 Software and web application vulnerabilities

2.1.2.1 Web browser vulnerabilities

- 2.1.2.2 Office and productivity software vulnerabilities
- 2.1.2.3 Open source software library vulnerabilities

2.1.3 Protocol vulnerabilities

2.1.4 Server platform vulnerabilities

- 2.1.4.1 Database server vulnerabilities
- 2.1.4.2 Web server vulnerabilities
- 2.1.4.3 Email server vulnerabilities
- 2.1.4.4 Content management server vulnerabilities
- 2.1.4.5 Application server vulnerabilities
- 2.1.4.6 Identity management or authentication server vulnerabilities

2.1.5 Network appliance or endpoint vulnerabilities

2.1.6 Cloud computing or storage vulnerabilities

2.1.7 Hardware vulnerabilities

2.1.8 Industrial control systems (ICS) or supervisory control and data acquisition (SCADA) vulnerabilities

2.1.9 IoT-related vulnerabilities

2.1.10 Health care systems-related vulnerabilities

2.1.11 Cryptocurrency and exchanges vulnerabilities

2.2 Exploit development

- Determine capability and intent of adversaries developing, sharing and discussing exploits.
  - Reputation, influence and credibility.
  - Communication modes and identifiers.
- Identify and characterize active exploits impacting my organization, industry, geographic region or supply chain.

2.2.1 Proof-of-concept (PoC) exploit code

- Identify the existence, location and characteristics of PoC exploit code.
- Determine the validity of PoC exploit code.

GIR 3: MALICIOUS INFRASTRUCTURE

TYPICAL STAKEHOLDERS

- Security Operations
- Blue Team
- Red Team
- Incident Response
- Forensics

COMMON USE CASES

- Identification and monitoring of malicious infrastructure for front-line protection

GIRS

3.1 Infrastructure-as-a-service (IaaS)

- Determine capability and intent of adversaries building, maintaining, operating and utilizing IaaS.
  - Reputation, influence and credibility.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify and characterize existing, new and emerging IaaS.
  - Capability.
  - Targeting.
  - Reputation.

3.1.1 Bulletproof hosting (BPH) services
3.1.2 Proxy services
3.1.3 Domain registration services
3.1.4 Botnet services

3.2 Legitimate infrastructure repurposed for malicious activity

- Determine capability and intent of adversaries leveraging or leasing infrastructure belonging to a legitimate person or enterprise for malicious purposes.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize compromised or abused legitimate infrastructure used for malicious purposes.
    - Capability.
    - Targeting.
    - Reputation.
    - Geolocation.
    - Technical indicators.
    - Legitimate owner or operator.

3.3 Dedicated criminal infrastructure

- Determine capability and intent of adversaries leveraging infrastructure designed for malicious activity.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize dedicated criminal infrastructure.
    - Capability.
    - Targeting.
    - Reputation.
    - Geolocation.
    - Technical indicators.

GIR 4: FRAUD, IDENTITY THEFT AND UNAUTHORIZED ACCESS

TYPICAL STAKEHOLDERS

- Fraud
- Forensics
- Incident Response
- Legal and Privacy
- Risk Management

COMMON USE CASES

- Stolen credentials
- Stolen credit cards
- Compromised information
  - Database dumps
  - Fullz, PII, PHI, IP
- Fraud chain
- Account checking and brute forcing
- Phishing

GIRS

4.1 Fraud supply chain monetization

- Determine capability and intent of adversaries building, maintaining or operating products, tools, shops and services that enable fraudulent activities.
  - Reputation, influence and credibility.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify capability and intent of adversaries discussing, transacting, consuming and monetizing fraudulent goods.
- Identify and characterize tactics, techniques, procedures and methods utilized in conducting fraudulent activity impacting my organization, industry or supply chain.

4.1.1 Cashout

4.1.2 Money laundering

4.1.2.1 Cryptocurrency exchange fraud

4.1.3 Mules and networks

4.1.4 Drop accounts and fund transfers

4.1.5 Prepaid or gift card fraud

4.1.6 Travel fraud

4.1.7 Hospitality fraud

4.1.8 Tax fraud and scams

4.1.9 Business email compromise (BEC)

4.1.10 Document fraud

4.1.11 Insurance fraud

- Identify threat actors or groups involved in insurance client interception through the use of insiders or unauthorized network access.
    - Identify source of customer listings and contact data.
    - Where and how are malicious call centers operated?
- Identify threat actors or groups involved in fraudulent insurance claims.
    - What method(s) is used to fabricate a fraudulent claim?
    - How do the actors source legitimate customer accounts?

4.1.12 Registration fraud

4.1.13 Reshipping fraud

4.1.14 Payroll fraud scam

4.2 Compromised data or access

- Determine capability and intent of adversaries selling and buying stolen data or network accesses.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize compromised data or accesses impacting my organization, industry or supply chain.

4.2.1 Payment card fraud

4.2.1.1 Online payment card skimming

4.2.2 Compromised credentials

4.2.2.1 Credential combination list(s)

4.2.3 Compromised personally identifiable information (PII)

4.2.3.1 Compromised protected health information (PHI)

4.2.4 Compromised intellectual property (IP)

4.2.5 Compromised network or system access

- Determine the nature of the network or system access.

4.2.6 Compromised business intelligence

4.3 Account takeover (ATO)

- Determine capability and intent of adversaries conducting ATO attacks.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize products, tools, services and methods to conduct ATO attacks against my organization, industry or supply chain.

4.3.1 Call centers

- Identify social engineering techniques used by call centers.

4.3.2 Account checking and credential stuffing

4.3.2.1 Account-checking configuration file(s)

4.3.3 Account brute forcing

4.3.3.1 Password spraying

4.3.4 Subscriber identity module (SIM) swapping

4.4 Social engineering

- Determine capability and intent of adversaries conducting various social engineering attacks.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize products, tools, services and methods to conduct social engineering attacks against my organization, industry or supply chain.

4.4.1 Phishing
4.4.2 Spear-phishing
4.4.3 Vishing
4.4.4 Social media scams
4.4.5 Smishing

GIR 5: ADVERSARY TACTICS AND ACTIVITIES

TYPICAL STAKEHOLDERS

- Security Operations
- Blue Team
- Red Team
- Incident Response
- Insider Threats

COMMON USE CASES

- Technique reproduction, pen testing
- Network or system access
    - Initial access
    - Privilege escalation

GIRS

GIR categories 5.1 and 5.2 are adapted from MITRE's Enterprise ATT&CK framework found here: https://attack.mitre.org/tactics/enterprise/

5.1 Pre-attack tactics

- Determine capability and intent of adversaries planning attacks.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize products, tools, services, infrastructure, tactics and techniques used by adversaries during attack planning and preparation. Reveal and understand pre-attack indicators.
    - Adversary discussions and coordination.
    - Target selection and staging.

5.1.1 Reconnaissance and information gathering tactic

- Identify adversary tactics and techniques used to identify and target people and organizations.

5.1.2 Build capabilities tactic

- Identify adversary tactics and techniques used to obtain or develop capabilities, tooling or services for attack.

5.2 Post-attack tactics

- Determine capability and intent of adversaries throughout the various stages of the attack lifecycle against systems or networks.
  - Reputation, influence and credibility.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify and characterize products, tools, services, infrastructure, tactics and techniques used by adversaries to carry out network or system attacks.

5.2.1 Initial access tactic

- Identify adversary tactics and techniques used to gain initial access to a system or network. Examples include:
  - Spear-phishing.
  - Vulnerability exploitation.
  - Third-party compromise.
  - Credential access.

5.2.2 Execution tactic

- Identify adversary tactics and techniques used to run malicious code on a local or remote system.

5.2.3 Persistence tactic

- Identify adversary tactics and techniques used to maintain access inside a system or network.

5.2.4 Privilege escalation tactic

- Identify adversary tactics and techniques used to gain higher-level privileges or access inside a system or network.

5.2.5 Defense evasion tactic

- Identify adversary tactics and techniques used to evade detection throughout the compromise of a system or network.

5.2.6 Credential access tactic

- Identify adversary tactics and techniques used to steal credentials such as account names and passwords. Examples include:
    - Keylogging.
    - Credential dumping.
    - Brute forcing.
    - Credential access.
    - Network sniffing.
    - Multi-factor authentication interception.

5.2.7 Discovery tactic

- Identify adversary tactics and techniques used to gain knowledge about a system or network. Examples include:
    - Account discovery.
    - Domain, network and file discovery.

5.2.8 Lateral movement tactic

- Identify adversary tactics and techniques used to enter and remotely control systems on a network. Examples include:
    - Remote desktop protocol (RDP).
    - Remote services such as Telnet, SSH and VNC.
    - Third-party software.

5.2.9 Collection tactic

- Identify adversary tactics and techniques used to gather information to further the end goal. Examples include:
    - Data from shared network drives.
    - Email collection.
    - Screen, sound or video capture.

5.2.10 Command and control tactic

- Identify adversary tactics and techniques used to communicate with systems under the actor's control within a victim network.
- Examples include:
    - Remote access tools such as Team Viewer, Go2Assist and VNC.
    - Malware command and control communications.

5.2.11 Exfiltration tactic

- Identify adversary tactics and techniques used to steal data from a system or network.

5.2.12 Impact tactic

- Identify adversary tactics and techniques used to disrupt availability or compromise the integrity of a system or network.

5.2.12.1 Defacement technique

5.2.12.2 Denial of service (DoS) technique

5.3 Physical attack techniques against systems

- Determine capability and intent of adversaries carrying out physical attacks impacting the confidentiality, integrity and availability of networks or systems.
  - Reputation, influence and credibility.
  - Output capacity and resiliency.
  - Communication modes and identifiers.
- Identify and characterize products, tools, services, infrastructure, tactics and techniques used by adversaries to carry out physical attacks.

5.3.1 Physical ATM attack techniques

5.3.2 Physical point-of-sale (PoS) system attack techniques

5.3.3 Physical sabotage techniques

5.4 Insider threat tactics

- Determine capability and intent of adversaries seeking or claiming insider access impacting my organization, industry, third parties or geographic region.

5.5 Information compromise or disclosure tactics

- Determine capability and intent of adversaries compromising or disclosing information from a network or system.

5.5.1 Espionage

5.5.2 Outsider trading

5.5.3 Information or data breach

5.5.4 Blackmail

GIR 6: THREATS IMPACTING INDUSTRY OR REGION

TYPICAL STAKEHOLDERS

- Senior Management
- Legal and Privacy
- Risk Management

COMMON USE CASES

- Third-party risk assessment and management
- Situational awareness of threats and events

GIRS

6.1 All sectors and industries

- Determine capability and intent of adversaries impacting specific industries.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize the use of products, services and illicit digital goods impacting specific industries.
- Determine and characterize key tactics, techniques and procedures used to target and impact organizations or individuals within certain industries.

6.1.1 Consumer and industrial products sector

6.1.1.1 Consumer business industry

6.1.1.2 Aviation and transportation industry

6.1.1.3 Consumer products industry

6.1.1.4 Sports and leisure industry

6.1.1.5 Hospitality industry

6.1.1.6 Restaurants and food service industry

6.1.1.7 Retail, wholesale and distribution industry

6.1.2 Energy, resources and agriculture sector

6.1.2.1 Oil, gas and consumable fuels industry

- 6.1.2.2 Power and utilities industry
- 6.1.2.3 Shipping and ports industry
- 6.1.2.4 Water industry
- 6.1.2.5 Agriculture, farming and food production industry

6.1.3 Financial services sector

- 6.1.3.1 Banking and securities industry
- 6.1.3.2 Insurance industry
- 6.1.3.3 Investment management industry
- 6.1.3.4 Payment processing industry

6.1.4 Life sciences and health care sector

- 6.1.4.1 Health care providers and services industry
- 6.1.4.2 Health care equipment and technology industry
- 6.1.4.3 Pharmaceuticals, biotechnology and life sciences industry

6.1.5 Manufacturing sector

- 6.1.5.1 Aerospace and defense industry
- 6.1.5.2 Automotive industry
- 6.1.5.3 Industrial products and services industry
- 6.1.5.4 Chemicals and specialty materials industry

6.1.6 Public sector

- 6.1.6.1 International government
- 6.1.6.2 National government
- 6.1.6.3 Regional government
- 6.1.6.4 Education
- 6.1.6.5 Public safety
- 6.1.6.6 Military and defense

6.1.7 Real estate sector

- 6.1.7.1 Engineering and construction industry
- 6.1.7.2 Real estate fund and investor industry
- 6.1.7.3 Real estate investment trust (REIT) and property company industry
- 6.1.7.4 Real estate management, brokerage and service provider industry
- 6.1.7.5 Tenants and occupiers industry

6.1.8 Technology, media and telecommunications sector

- 6.1.8.1 Technology industry
- 6.1.8.2 Media and entertainment industry

6.2 All geographic regions

- Determine capability and intent of adversaries impacting specific geographic regions.
    - Reputation, influence and credibility.
    - Output capacity and resiliency.
    - Communication modes and identifiers.
- Identify and characterize the use of products, services and illicit digital goods impacting specific geographic regions.
- Determine and characterize key tactics, techniques and procedures used to target and impact organizations or individuals within specific geographic regions and impact organizations or individuals within certain industries.

6.2.1 Africa
6.2.2 Asia
6.2.3 Central America
6.2.4 Europe
6.2.5 Middle East
6.2.6 North America
6.2.7 Oceania
6.2.8 South America
6.2.9 The Caribbean

ADDENDUMS

ADDENDUM A: CYBERCRIME GLOSSARY

ACCOUNT BRUTE FORCING: a credential attack method used to crack the username and password of accounts through trial and error. 27

ACCOUNT CHECKING AND CREDENTIAL STUFFING: a credential-based attack used to test the validity of compromised credentials against login forms. 27

ACCOUNT-CHECKING CONFIGURATION FILE(S): text configuration files developed for use in account-checking tools to target specific organizations using combination lists. 27

ACCOUNT TAKEOVER (ATO): a form of identity theft in which the criminal obtains access to a victim's bank or credit card accounts — through a data breach, malware or phishing — and uses them to make unauthorized transactions. 27

ACTIVE DIRECTORY TOOLS: tools to gather information about or exploit an Active Directory server. Examples include AdFind and BloodHound. 20

ADVOCACY NGOs: organized to promote particular causes. 35

ATM MALWARE: designed to steal financial information and/or cash from automated teller machines (ATMs) by exploiting vulnerabilities in the machine's hardware or software. 18

AUTHENTICATION AND CREDENTIAL TOOLS: tools that can steal passwords from a host. Examples include LaZagne and Mimikatz. 20

AUTOMATIC TRANSFER SYSTEMS (ATSs): an advanced type of web-inject that automatically initiates fund transfers from an infected victim account and conceals funds stolen. 20

BANKING TROJAN MALWARE: malicious software designed to steal account-related information related to card payments, online banking and e-payment gateways. 18

BOTNET MALWARE: a type of trojan used to form a botnet (a collection of internet-connected devices, known as bots, that are commanded and controlled by malicious actors to carry out nefarious activities). 18

BOTNET SERVICES: services offering botnets for lease, typically to conduct spamming, phishing, distributed denial of service (DDoS) attacks and/or credential theft. 23

BUILD CAPABILITIES TACTIC: developing and/or acquiring the software, data and techniques used at different phases of an operation. This is the process of identifying development requirements and implementing solutions such as malware, delivery mechanisms, obfuscation and cryptographic protections, and call back and operation and maintenance (O&M) functions. (source: Mitre ATT&CK) 30

BULLETPROOF HOSTING (BPH) SERVICES: hosting services that are considerably lenient about the kinds of activity and material they allow their customers to upload and distribute and are generally immune to law enforcement or takedown efforts. 23

BUSINESS EMAIL COMPROMISE (BEC): a type of scam that relies heavily on social engineering tactics to trick unsuspecting employees and executives into executing fraudulent wire transfer payments. 26

CALL CENTERS: a service that allows scammers to hire multilingual men and women to defeat phone-based anti-fraud measures using social engineering techniques. 27

CASHOUT: the process, typically at the final stage of a fraudulent scheme, of transferring illicit proceeds to a threat actor or designated representative. Common methods include ATM withdrawals, purchasing digital currencies, transferring funds to online payment platforms or buying goods or gift cards. 26

CHARITABLE ORGANIZATIONS: commonly known as true "nonprofits" by those who work in the industry, a charitable organization receives IRS tax exemption status and is funded primarily through charitable donations and government grants. Examples include churches, hospitals dedicated to medical research and government units involved in charitable causes. 35

CIVIC LEAGUES AND SOCIAL WELFARE ORGANIZATIONS: organizations that promote philanthropy and positive change through their work and mission. They are allowed to freely participate in lobbying efforts that might help pass or repeal legislation. They are also allowed to publicly endorse and promote legislation to gain support. Examples include the American Association of Retired Persons (AARP), the American Civil Liberties Union (ACLU), health maintenance organizations (HMOs) and Rotary clubs. 35

COLLECTION TACTIC: consists of techniques adversaries may use to gather information that is relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal or exfiltrate the data. Common target sources include various drive types, browsers, audio, video and email. Common collection methods include capturing screenshots and keyboard input. (source: Mitre ATT&CK) 31

COMMAND AND CONTROL TACTIC: consists of techniques adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection. There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses. (source: Mitre ATT&CK) 31

COMPROMISED BUSINESS INTELLIGENCE: the unlawful exposure, sale or unauthorized use of sensitive information used for business operations such as internal-only documents, financial statements, emails and employee information. 27

COMPROMISED CREDENTIALS: the unlawful exposure, sale or unauthorized use of legitimate user account authentication information - typically username and password - that has been stolen for malicious purposes. 27

COMPROMISED INTELLECTUAL PROPERTY (IP): the unlawful exposure, sale or unauthorized use of copyrights, patents, trademarks, trade secrets or any product of the human intellect that the law protects from unauthorized use by others. 27

COMPROMISED NETWORK OR SYSTEM ACCESS: the exposure or sale of unlawful or unauthorized access to a network or system. 27

COMPROMISED PERSONALLY IDENTIFIABLE INFORMATION (PII): the unlawful exposure, sale or unauthorized use of any data that potentially could be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number and email address. 27

COMPROMISED PROTECTED HEALTH INFORMATION (PHI): (also known as personal health information) the unlawful exposure, sale or unauthorized use of any health data that potentially could be used to identify a particular person. Examples include a full name, medical record number, health insurance information and certificate or license number. 27

COUNTER ANTIVIRUS (CAV): enables the semiautomated and clandestine development of malware, maximizing the malware's impact when deployed in the wild. 20

CREDENTIAL ACCESS TACTIC: consists of techniques to steal credentials such as account names and passwords. Techniques used to obtain credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect and provide the opportunity to create more accounts to help achieve their goals. (source: Mitre ATT&CK) 31

CREDENTIAL COMBINATION LIST(S): (also known as "combo list") refers to a usually long text file containing compromised credential pairs that are used in account-checking tools to check validity of credentials against login forms. 27

CRYPTOCURRENCY EXCHANGE FRAUD: the misuse of legitimate or nefarious exchanges and services for money laundering purposes, bypassing fraud controls to cash out criminally obtained funds. 26

CRYPTOMINING MALWARE: cryptocurrency mining (cryptomining) or cryptojacking is malicious software designed to use a device's CPU resources to mine cryptocurrency without authorization. 19

DEDICATED CRIMINAL INFRASTRUCTURE: infrastructure intended for malicious activity and not attributed to IaaS offerings or compromised or abused legitimate systems. 24

DEFACEMENT TECHNIQUE: adversaries may modify visual content available internally or externally to an enterprise network. Reasons for defacement include delivering messaging, intimidation or claiming real or false credit for an intrusion. (source: Mitre ATT&CK) 32

DEFENSIVE EVASION TACTIC: consists of techniques adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling or disabling security software or obfuscating and encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. (source: Mitre ATT&CK) 30

DENIAL OF SERVICE (DOS) MALWARE: a type of trojan used to conduct denial of service attacks. 18

DENIAL OF SERVICE (DOS) TECHNIQUE: adversaries may perform network denial of service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS attacks can be performed by exhausting the network bandwidth services use. Example resources include specific websites, email services, domain name system (DNS) and web-based applications. (source: Mitre ATT&CK) 32

DESTRUCTIVE MALWARE: a type of trojan used to destroy or delete files on a computer system or network. 19

DISCOVERY TACTIC: consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective. (source: Mitre ATT&CK) 31

DOCUMENT FRAUD: schemes to manufacture, counterfeit, alter, sell and/or use identity documents and other fraudulent documents. Also known as identity fraud. 26

DOMAIN REGISTRATION SERVICES: services offering private and anonymous domain registration on behalf of nefarious clients. 23

DROP ACCOUNTS AND FUND TRANSFERS: refers to threat actor-controlled or compromised victim accounts, typically online banking or e-commerce, used for receiving illicit funds for cashout or laundering purposes. 26

EXECUTION TACTIC: consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, such as exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does remote system discovery. (source: Mitre ATT&CK) 30

EXFILTRATION TACTIC: consists of techniques adversaries may use to steal data from a network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques to exfiltrate data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission. (source: Mitre ATT&CK) 31

EXPLOIT: a program or piece of code designed to take advantage of a security flaw or vulnerability in a system or application. 22

EXPLOIT KITS: automated threats that utilize compromised websites to divert web traffic, scan for vulnerable browser-based applications and run malware. 20

HOSPITALITY FRAUD: the abuse of legitimate hotel and accommodation services via compromised loyalty accounts or fraudulent documents. 26

ILLICIT USE OF LEGITIMATE TOOLS AND SOFTWARE: the abuse of open and closed source tools and software normally used for legitimate administrative or security functions such as penetration testing, domain administration, network and vulnerability scanning, etc. 20

IMPACT TACTIC: consists of techniques adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. Adversaries might use these techniques to follow through on their end goal or to provide cover for a confidentiality breach. (source: Mitre ATT&CK) 32

INFORMATION-STEALER MALWARE: (or info stealer) malicious software designed to gather information from a system such as login credentials, keystrokes and screenshots of sensitive information. 18

INFRASTRUCTURE-AS-A-SERVICE (IAAS): a service model that delivers computer infrastructure - solely dedicated for criminal use or otherwise legitimate but compromised - on an outsourced basis to support criminal operations. 23

INITIAL ACCESS TACTIC: consists of techniques that use various entry vectors to gain an initial foothold within a network. Techniques used to gain a foothold include targeted spear-phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, such as valid accounts and use of external remote services, or may be of limited use due to changing passwords. (source: Mitre ATT&CK) 30

INSURANCE FRAUD: schemes that involve interception of customers or fraudulent claims in the form of fraudulent applications or insurance ATO. 26

INTERNET OF THINGS (IOT) MALWARE: a type of trojan used to compromise networked devices for nefarious purposes such as forming botnets to launch network attacks. 18

LATERAL MOVEMENT TACTIC: consists of techniques adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gain access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish lateral movement or use legitimate credentials with native network and operating system tools, which may be stealthier. (source: Mitre ATT&CK) 31

LEGITIMATE INFRASTRUCTURE REPURPOSED FOR MALICIOUS ACTIVITY: infrastructure belonging to legitimate individual or business entities that is repurposed for malicious activity. 24

LOADER MALWARE: malicious software designed to download and/or drop malicious payload code onto an infected computer system. 18

MALVERTISING: the use of online advertising to spread malware typically involving injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. 20

MALWARE: malicious software that is purpose-built to disrupt, damage or gain unauthorized access to a computer system including the mechanisms for its development, production and delivery. 17

MALWARE-AS-A-SERVICE (MAAS): the lease of software or hardware for developing, testing and/or distributing malware. 19

MALWARE CRYPTING: fully undetectable (FUD) malicious code that has been encrypted, making it more difficult for antivirus signature detection. 20

MALWARE DEVELOPMENT, SUPPORT AND DELIVERY: various tools, delivery methods and providers used to enable, distribute and execute malware attacks. 20

MALWARE INSTALLS: services provided to client actors for distributing, installing and executing malware onto a number of target hosts either directly or through a third-party affiliate. 20

MALWARE SOURCE CODE: the list of human-readable instructions that a programmer writes to develop a malware program. 20

MALWARE SPAMMING: unsolicited email, short message service (SMS) and other types of messages used to deliver malware or malspam. 20

MALWARE VARIANTS: the various types of malicious software used to disrupt, damage or gain unauthorized access to a computer system. 17

MOBILE MALWARE: malicious software designed to compromise devices such as phones, smartwatches and tablets to steal sensitive financial and personal information and to gain remote access. 18

MONEY LAUNDERING: a fraudulent scheme involving layering, transferring or changing the form of money through complex transactions to obscure the origin and/or destination of illicit funds. 26

MULES AND NETWORKS: mules are people who wittingly or unwittingly were recruited to launder stolen money or goods for criminals or criminal organizations. 26

MULTIFUNCTIONAL MALWARE-AS-A-SERVICE (MAAS): services leased to offer multifunctional malware with various functionalities. 19

NETWORK SCANNERS: tools that enumerate hosts on a network and probe them for vulnerabilities or information. Examples include Nessus, Nmap and custom tools. 20

NONGOVERNMENTAL ORGANIZATIONS (NGOs): a nonprofit, citizen-based group that functions independently of a government. Sometimes called civil societies, NGOs are organized on community, national and international levels to serve specific social or political purposes and are cooperative, rather than commercial, in nature. Examples include The American Red Cross, the World Wildlife Fund and Oxfam. 35

ONLINE PAYMENT CARD SKIMMING: a form of payment card fraud whereby a payment page on a website is compromised using a malicious script. 26

OPERATIONAL NGOS: focus on development projects. 35

PASSWORD SPRAYING: a type of brute-force attack in which a malicious actor uses a single password against targeted user accounts before moving on to attempt a second password, and so on. 27

PAYMENT CARD FRAUD: (also known as "carding") credit or debit card information obtained, sold or used by unauthorized individuals. Card verification value (CVV) is underground jargon for a stolen credit card consisting of data that can only be used with online retailers (also known as "card not present" fraud). "Fullz" refers to financial information associated with stolen credit cards that includes more than standard account information including Social Security number, date of birth and more. "Dump" is underground jargon for stolen credit card data that can be encoded onto a physical plastic card and used for instore purchases (also known as "card present" fraud). 26

PAYROLL FRAUD SCAM: the scammer impersonates a legitimate employee and sends an email to payroll or human resources (HR) personnel who is tricked into updating the employee's payroll records with the scammer's bank account and routing number, leading to further fraudulent payroll deposits and payments. The scheme involves social engineering, phishing and business email compromise (BEC)/email account compromise (EAC)/business email spoofing (BES). 26

PERSISTENCE TACTIC: consists of techniques adversaries use to keep access to systems across restarts, changed credentials and other interruptions that could cut off their access. Techniques used for persistence include any access, action or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.
(source: Mitre ATT&CK) 30

PHISHING: the fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers. 28

POINT-OF-SALE (POS) MALWARE: malicious software designed to steal information related to financial transactions such as payment card data from compromised PoS devices. 18

POST-EXPLOITATION FRAMEWORKS: frameworks used to manage hosts after initial access, fingerprint vulnerable hosts and exploit them. Examples include Cobalt Strike, Core Impact, Immunity Canvas, Metasploit and PowerShell Empire. 20

PREPAID OR GIFT CARD FRAUD: the abuse, compromise or tampering of legitimate prepaid or gift cards for fraudulent purposes. 26

PRIVATE CHARITABLE FOUNDATIONS: a privately owned nonprofit established to address global concerns such as education, medical research, environmental issues and more. Private charitable foundations are normally established by a single wealthy benefactor or business and are used to grant money to smaller, more niche nonprofits. Examples include the Bill and Melinda Gates Foundation and the Coca-Cola Foundation Inc. 35

PRIVILEGE ESCALATION TACTIC: consists of techniques adversaries use to gain higher-level permissions on a system or network. Adversaries often can enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations and vulnerabilities. Examples of elevated access include: SYSTEM or root level, local administrator, user account with administrator-like access and user accounts with access to specific systems or which perform specific functions. These techniques often overlap with persistence techniques, as OS features that let an adversary persist can execute in an elevated context. (source: Mitre ATT&CK) 30

PROOF OF CONCEPT EXPLOIT CODE: (aka PoC code) code developed to demonstrate the vulnerability of a system. 22

PROXY MALWARE: a type of trojan used to turn an infected computer system into a proxy server from which an attacker can stage nefarious activities anonymously. 19

PROXY SERVICES: services offering leased infrastructure, typically residential consumer IP addresses, as proxy servers to anonymize illicit communications and obfuscate the true origin of nefarious clients. 23

RANSOMWARE: malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. 18

RANSOMWARE-AS-A-SERVICE (RAAS): services typically sold or leased as an affiliate program to other actors for launching ransomware attacks and sharing profits. 19

RECONNAISSANCE AND INFORMATION GATHERING TACTIC: consists of identifying critical technical, personnel and organizational elements of intelligence an adversary would need about a target to best attack. (source: Mitre ATT&CK) 29

REGISTRATION FRAUD: schemes involving the creation or registration of new fictitious accounts using stolen personally identifiable information (PII). 26

REMOTE ACCESS TOOLS: Tools to manipulate a system remotely over the network. Examples include LogMeIn, PuTTY and TeamViewer. 20

REMOTE ACCESS TROJAN (RAT) MALWARE: malicious software designed to allow attackers to monitor and control a computer system or network remotely. 18

RESHIPPING FRAUD: schemes involving the fraudulent purchase, typically using stolen payment cards, and delivery of items from an online merchant to a reshipper to resell on the black market. 26

ROGUE CERTIFICATES: stolen digital certificates actors use to sign malicious software or impersonate legitimate websites. 20

ROGUE CODE-SIGNING CERTIFICATES: stolen digital certificates actors use to sign malicious software to evade detection. 20

ROGUE WEB CERTIFICATES: stolen digital certificates used by actors to create illegitimate websites for nefarious purposes, typically by impersonating legitimate banking, e-commerce and social networking websites. 20

SMISHING: (also known as SMS phishing) the fraudulent practice of tricking a user into revealing sensitive personal data or sending money via a text or SMS message. 28

SOCIAL ADVOCACY GROUPS: primarily focus on lobbying and promoting social and political change and are proactively involved in legislation for advancing change. Social advocacy groups rely heavily on membership dues to help supplement the money they receive from public donations. Examples include the Electronic Frontier Foundation, the National Association for the Advancement of Colored People (NAACP), the National Rifle Association (NRA) and the World Economic Forum. 35

SOCIAL MEDIA SCAMS: the fraudulent practice of tricking social media users into revealing sensitive personal data or sending money. Types include romance scams, sextortion, imposter scams and more. 28

SPEAR-PHISHING: the fraudulent practice of sending emails ostensibly from a known or trusted sender to induce targeted individuals to reveal confidential information. 28

SUBSCRIBER IDENTITY MODULE (SIM) SWAPPING: (also known as port-out scam, SIM splitting and simjacking) a type of account takeover fraud that targets a weakness in short message service (SMS)-based two-factor authentication (2FA) and two-step verification by tricking a target's mobile carrier into transferring someone's wireless service to a device controlled by an illicit actor. 27

TAX FRAUD AND SCAMS: schemes typically employed during tax season involving deceiving or tricking victims into unwittingly disclosing credentials, money and personally identifiable information (PII). 26

TRAFFIC REDISTRIBUTION SYSTEM: services that buy and sell web traffic to direct users from one website to another, typically to distribute malware. 20

TRAVEL FRAUD: the abuse of legitimate travel services such as airlines and car-sharing rides (shuttles or ride-sharing such as Uber or Lyft) via compromised travel rewards points, membership accounts or fraudulent travel documents. 26

VISHING: the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies to induce individuals to reveal personal information, such as bank details and credit card numbers. 28

VULNERABILITY: a weakness in a system, tool, application or protocol that can be exploited by a threat actor. 21

WEB-INJECTS: modules or packages used in financial malware that typically inject hypertext markup language (HTML) or JavaScript code into content before it's rendered on a web browser, altering what the unsuspecting user sees on the browser, as opposed to what's actually sent by the server. 20

WORM MALWARE: a self-replicating, stand-alone software program designed to spread throughout a network without human assistance. 18

INTEL471

VISIT US AT:

www.Intel471.com

EMAIL US AT:

Intelligence@Intel471.com

CALL US AT:

+1 800.833.1471