Recorded Future®

PLAYBOOK

The Intelligence Playbook: Practical Applications Across the Enterprise

Version 1.0 - December 2021

363 Highland Avenue, Somerville, MA 02144 • 1-617-553-6400 • www.recordedfuture.com

Practical Application Intelligence Playbooks

For intelligence to improve your organization's security posture, it has to be actioned. However, agonizing over the next step can add significant time to resolving an issue or addressing a threat. This collection was developed to provide practical next steps for a variety of common use cases with clear instructions and visual aids.

We recognize our clients have unique teams, technologies, and processes, so these playbooks can serve as a blueprint to reference when building out the custom response plans and workflows that fit your needs.

Each section indicates which license types it is most relevant to, as some of the recommendations require access to particular features of the Recorded Future Portal. However, if a particular workflow is not relevant to a security objective your organization prioritizes, it can still offer key insights into how other Recorded Future users take action.

The most up-to-date versions of these playbooks can always be found in the Support Center.

Request playbooks on additional subjects by writing to playbooks@recordedfuture.com.

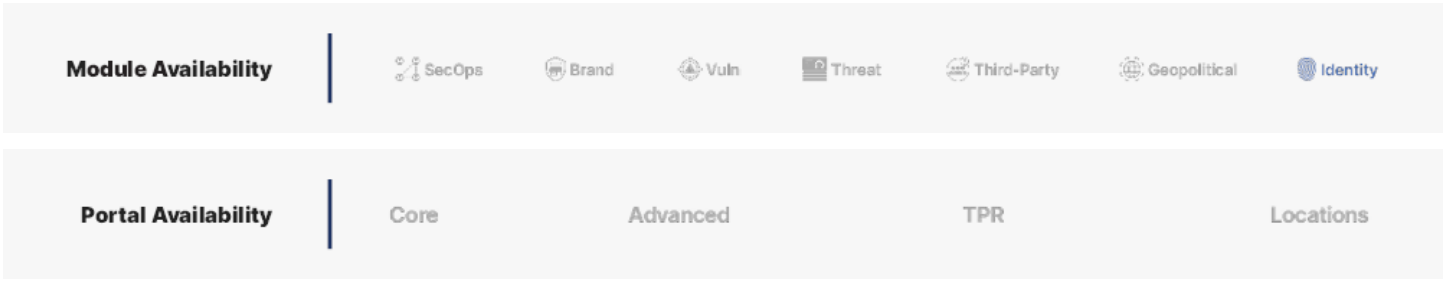
Table of Contents (+ Associated Modules):

Leaked Credentials Playbook for Identity Intelligence Users

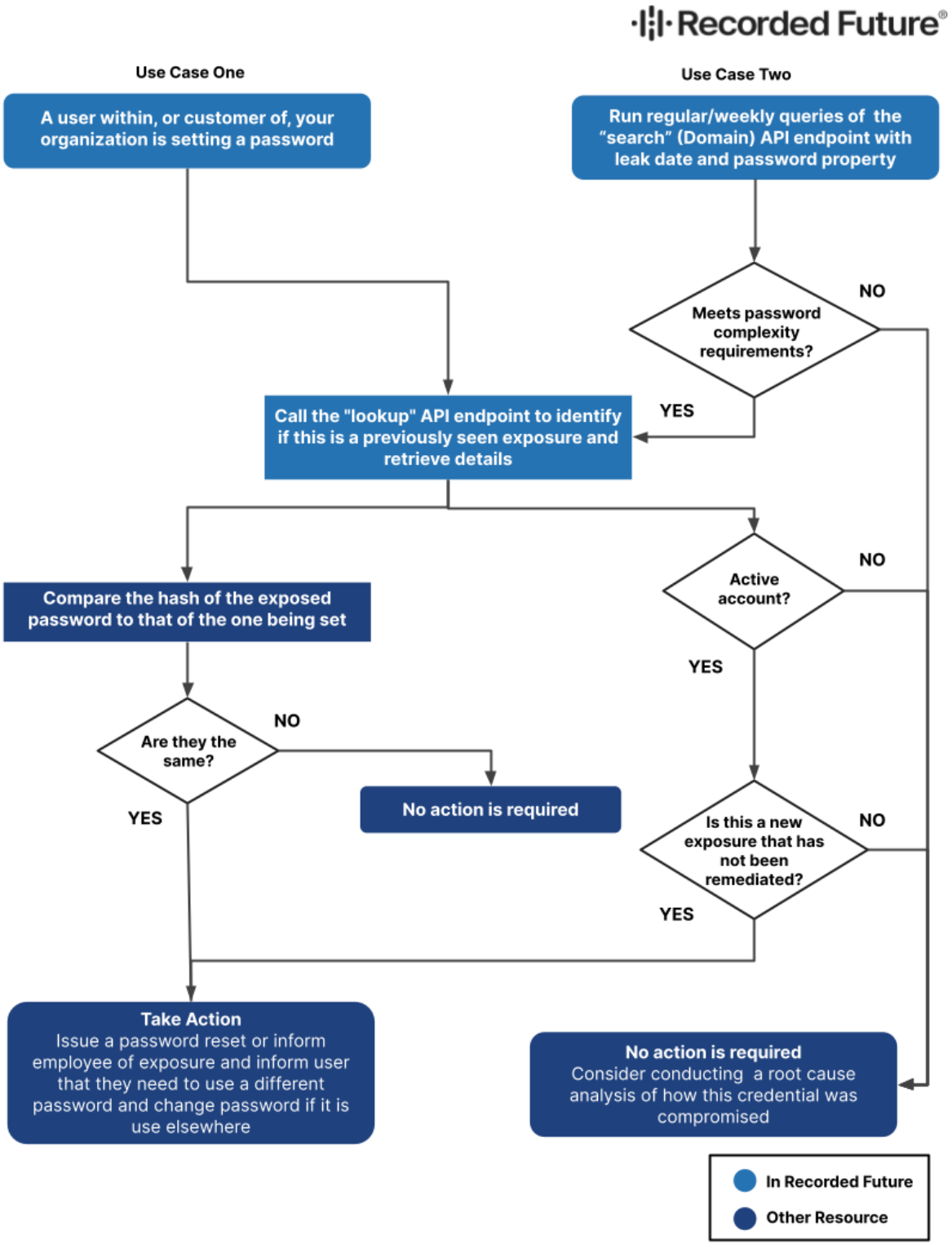
PLAYBOOK

1st edition

Leaked Credentials Playbook for Identity Intelligence Users



Recorded Future's Identity Intelligence Module allows you to quickly triage issues with leaked credentials from start to finish. If you do not have access to the Identity Intelligence Module, check out our original Leaked Credentials Playbook.


Recorded Future
Use Case One
A user within, or customer of, your organization is setting a password
Use Case Two
Run regular/weekly queries of the "search" (Domain) API endpoint with leak date and password property
Meets password complexity requirements?
NO
YES
Call the "lookup" API endpoint to identify if this is a previously seen exposure and retrieve details
Compare the hash of the exposed password to that of the one being set
Active account?
NO
YES
Are they the same?
NO
YES
No action is required
Is this a new exposure that has not been remediated?
NO
YES
Take Action
Issue a password reset or inform employee of exposure and inform user that they need to use a different password and change password if it is use elsewhere
No action is required
Consider conducting a root cause analysis of how this credential was compromised
In Recorded Future
Other Resource

Use Case One: Comparing a password being set against compromised ones

Step 1

You have automated a query to the Recorded Future Identity Intelligence Module API to perform lookups when a user within your organization or customer of your organization (depending on your subscription type) enters a new password.

Step 2

Using the lookup API endpoint, pass the email address (either in clear text or SHA1) over to the API and hashes of leaked passwords associated with that email address are returned to the application.

Step 3

Compare the hash of the password that was just entered into the application to the hash(es) of those passwords that have been leaked to determine if there is a match.

Step 4

If it is determined that there is a match, inform the user that they will need to choose a different password to avoid the possibility of threat actors gaining access to their account using published leaked passwords. and also change their password anywhere else it was being used

Pulling additional information from the API associated with that password hash, you can also inform them regarding the specifics of the breach where the password was leaked.

Use Case Two: Taking action on new password leaks targeting your company

Step 1

Your company wants to know about any new credential leaks that involve your domain and that have occurred in the past 24 hours/7 days (or whichever frequency your organization has decided on). You automate a query of the search API endpoint based on that frequency, for your domain, and in accordance with your company's password requirements to filter out those that could never match one currently in use in your organization.

- Does not meet password complexity requirements → Though you may want to conduct a root cause analysis of how this credential was compromised, it currently does not pose significant risk. No action is required.
- Meets password complexity requirements → Proceed to the next step.

Step 2

Taking the list of email addresses that are returned, use the lookup API endpoint to identify the details of the exposure for those email addresses that were returned in Step 1.

Step 3

Parsing through the details, automate comparing the list of email addresses with an identity management application (e.g., Active Directory) to determine if they are currently active accounts.

- NO, the email address is not active. → Though you may want to conduct a root cause analysis of how this credential was compromised, it currently does not pose significant risk. No action is required.
- YES, the email address is active. → Proceed to the next step.

Step 4

Parsing through the details, determine which are novel credential leaks. Many credentials are recycled; you may only need to perform a reset if it is a novel credential leak that you haven't encountered and forced a reset for previously.

- Recycled → The need to force a password reset will be dependent on If your organization has already performed a reset on the credentials (i.e., if these credentials were exposed previously and the passwords were changed). If you have been diligent in resetting accounts, then no action is required.
- Novel → Proceed to the next step.

Step 5

Take action:

- Issue a password reset
- Inform the employee of exposure; ask the employee to take action if needed, including resetting additional credentials that may share the same password. Remind the user not to use the same password for business and consumer services as this increases the attack surface of credential leakage and re-use.

Step 6

If you have not already done so, log information on the incident.

Have more questions regarding this topic: Submit a request

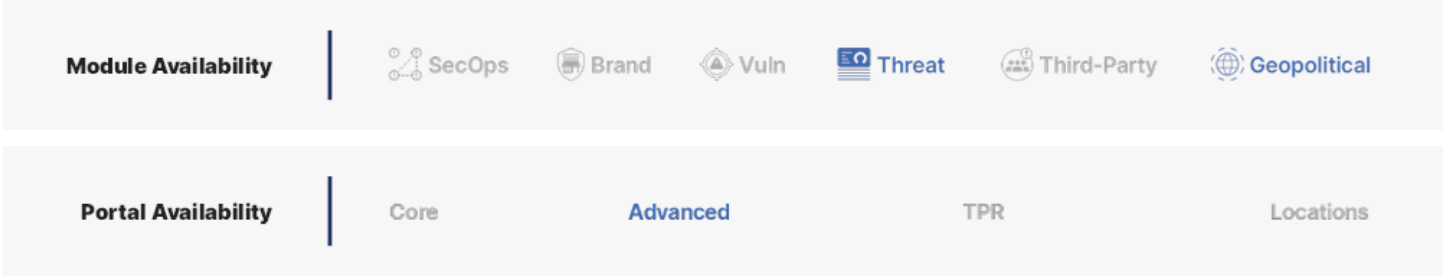
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Alert Tuning

PLAYBOOK

1st edition

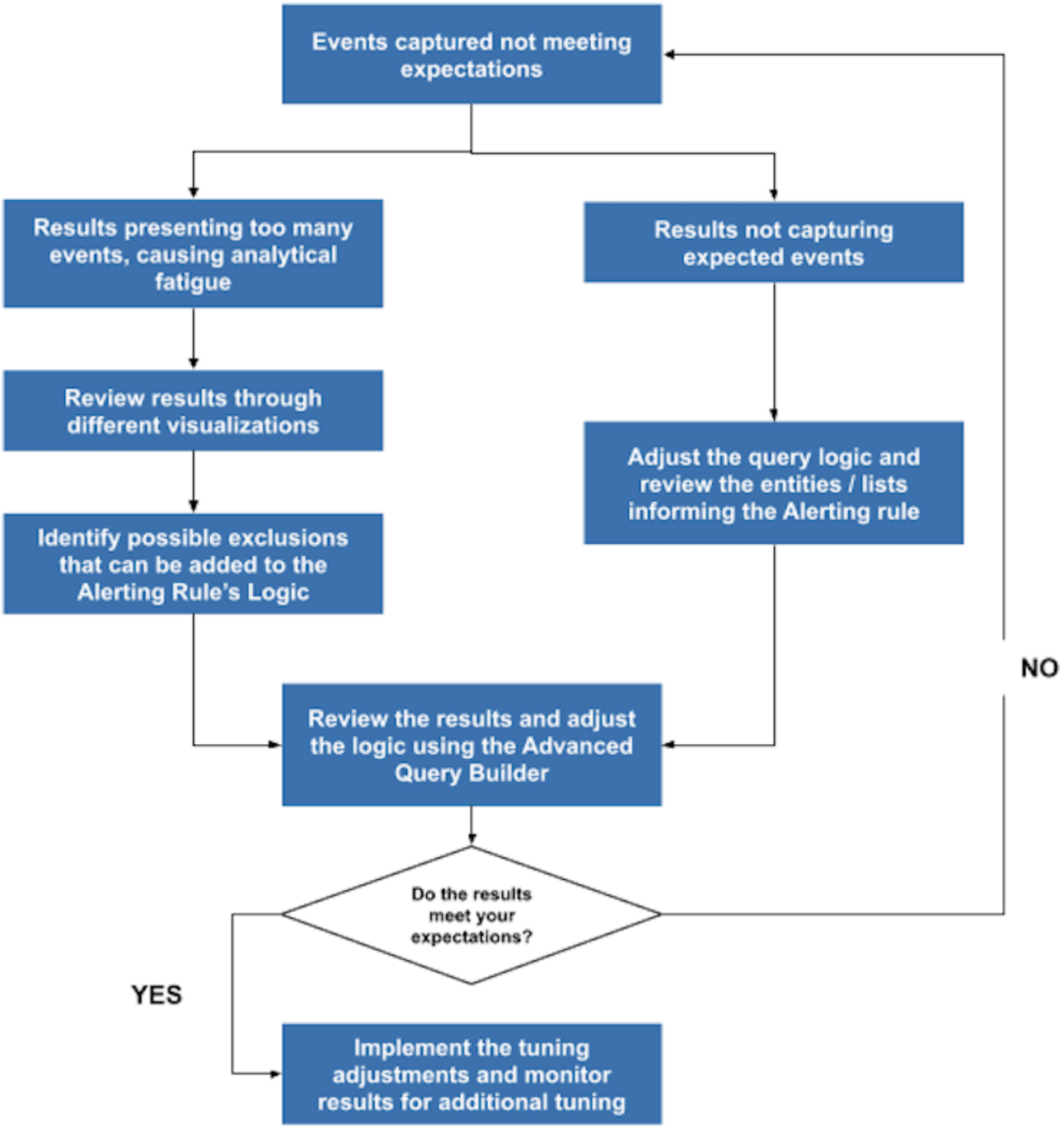
Alert Tuning Playbook



This playbook provides general guidance on how to tune most alerts in Recorded Future and a high-level checklist you can use to regularly update your alerting rules. Incorporating feedback is a critical component of the intelligence cycle, and it is vital to ensure actionable and relevant alerts from the Recorded Future platform. As your organization's requirements change, so too should your alerts.

For recommended actions to take when specific alerts fire, reference the other playbooks available in the Support Center.

> Note: An Alert is simply a query that is configured to trigger on a regular cadence (e.g., Daily at 08:00 AM Asia/Singapore). This is why you can convert any advanced query into an alerting rule.


Events captured not meeting expectations
Results presenting too many events, causing analytical fatigue
Review results through different visualizations
Identify possible exclusions that can be added to the Alerting Rule's Logic
Results not capturing expected events
Adjust the query logic and review the entities / lists informing the Alerting rule
Review the results and adjust the logic using the Advanced Query Builder
Do the results meet your expectations?
NO
YES
Implement the tuning adjustments and monitor results for additional tuning

Step 1

You are reviewing your triggered alerts from the Recorded Future platform, via your email notifications or within the portal itself.

You notice that the alerts are not capturing the events you would like to see, or it has been more than 60 days since you last reviewed your alerting logic for possible updates.

Step 2

Identify which aspects of the results are not meeting your expectations. In most cases, results will fall into one of the two following categories:

- Too broad to be actionable. Events captured in your alerts are too voluminous to facilitate any follow-up activity, meaning they are NOT actionable (e.g., alerts deliver more than 1000 new references, you receive notifications too frequently).
- Not capturing expected events. You are receiving no alerts at all, or your alerts are not capturing information you are looking for (e.g., information that you know exists in the platform, events related to entities you are newly interested in).

Step 3

Review the Logic behind the alerting rule. Take note of the entities, events, time parameters, and sources. Ensure that you are searching for the correct entity or event type (e.g., Domain, Company) and pulling from the correct source or sources.

Step 4

Review the results of the alerting rule using the different visualizations. This will give you a better sense of the results or how you can adjust the logic behind the alert.

If you are receiving no alerts, replicate the logic using the Advanced Query Builder to proceed with your review.

- Review the events captured in the Analytics (Table) view and use the why this alert feature to determine the reasoning behind these results.
- Review the Entity Tree on the left-hand side of the analytics view. By skimming each section you may uncover a specific company, author, etc. that is causing the most noise.

Use this information to exclude one or more entities or refine the logic to reduce false positives.
- Use the Timeline view to view the captured events as a chronological diagram and determine if the lack of results is consistent with previous occurrences (e.g., Event Dormancy Periods).
- Use the Source view to see the origins of these events and determine if you need to remove sources that are 'too noisy' or add other more specific sources. To find out more about a source, create an advanced query that includes a relevant entity and event of your choice. If you feel the source requires curation, let us know by requesting a Data Review from the source entity's Intelligence Card.

Step 5

Depending on the issue, consider the following options:

- If results are too broad to be actionable, use the why this alert feature to determine the reasoning behind your results. Alternatively, analyze your results via the benchmarking option under the main menu to see which alerts are causing the most noise and if your alerts have provided value over the last 30/60/90 days.
- If results are not capturing expected events, configure the alert using the Editing Alerting Rules link from the Mega Menu. Click on the alert to be tuned. Treating the alert like an advanced query, review the Results, Setup, and Logic of the alert using the techniques mentioned in Step 4. This will give you a broader understanding of the conditions and criteria that will trigger the alert.

Step 6

Repeat Steps 3 to 5 using the Advanced Query Builder to adjust the logic behind the alert until you get the results you want. Once you are seeing desired results, either escalate that query into an alerting rule or simply adjust the logic behind the rule you want to tune.

Note: If you have access to a Recorded Future Intelligence Consultant, reach out to them for additional support on tuning your alerts. Consider using the template below when preparing your outreach.

Step 7

As part of the feedback phase of the intelligence lifecycle, *you are responsible for the regular tuning of alerts* on your instance of the Recorded Future platform. If it has been 60+ days since you've reviewed the logic driving your alerts, we recommend using the Benchmarking feature to determine which alerts to focus on first. Then, review the entities, events, sources, and exclusions informing the alerting rule for possible updates. This should be done as a dedicated workshop either internally within your team or with your Intelligence Services Consultant.

Marty's Insight: If your alerts are powered by Custom Lists and Watch Lists, we recommend reviewing and updating these on a recurring basis, which can be streamlined via our List API. If it has been 60+ days since your last review, we recommend that you:

- Remove entities from your Watch Lists that you no longer use
- Update to new version numbers if they've changed
- Add newly identified entities from previous alert results or assessments from within your organization

Checklist

This checklist summarizes the steps presented here into a repeatable alert tuning process.

☐	Review the results from the alert and determine if it is meeting your expectations
☐	Review the alert Setup to determine whether you can use exclusions to remove events that are not relevant
☐	Review the alert Logic to determine which entities, sources, and events can be added or excluded.
☐	Review Custom Lists and Watch Lists to determine if the right entities are being used to inform the alert's logic.
☐	Review adjustment results through different visualizations to determine how the alert Logic can be tuned.
☐	Try the revised alerting rule and observe the results for one week. Repeat the tuning process as needed.

Alert Tuning Support Inquiry Template

To help your Intelligence Services Consultant get a better understanding of the issue you are experiencing, include the following information when preparing your outreach:

- Alerting rule name
- Share link
- Expected outcomes
- Summary of issue experienced
- [Optional] screenshot of the alerting rule results

Have more questions regarding this topic: Submit a request

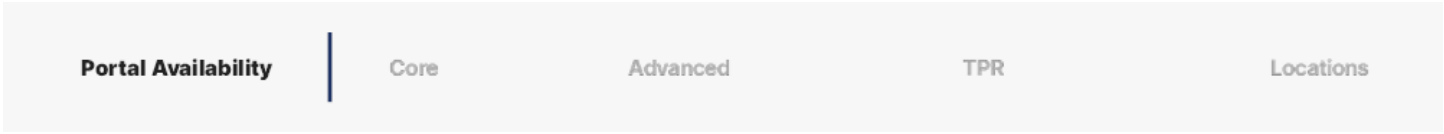
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Executive Impersonation

PLAYBOOK

1st edition

Executive Impersonation Playbook



Recorded Future's Executive Impersonation playbook walks you through how to detect and respond to attempts to impersonate your organization's top executives on LinkedIn and social media.

Refer to the Key Prerequisites below to make sure your organization is prepared to address executive impersonation threats. For more information on this use case, see Executive Impersonation on Professional Networking Website and Social Media.

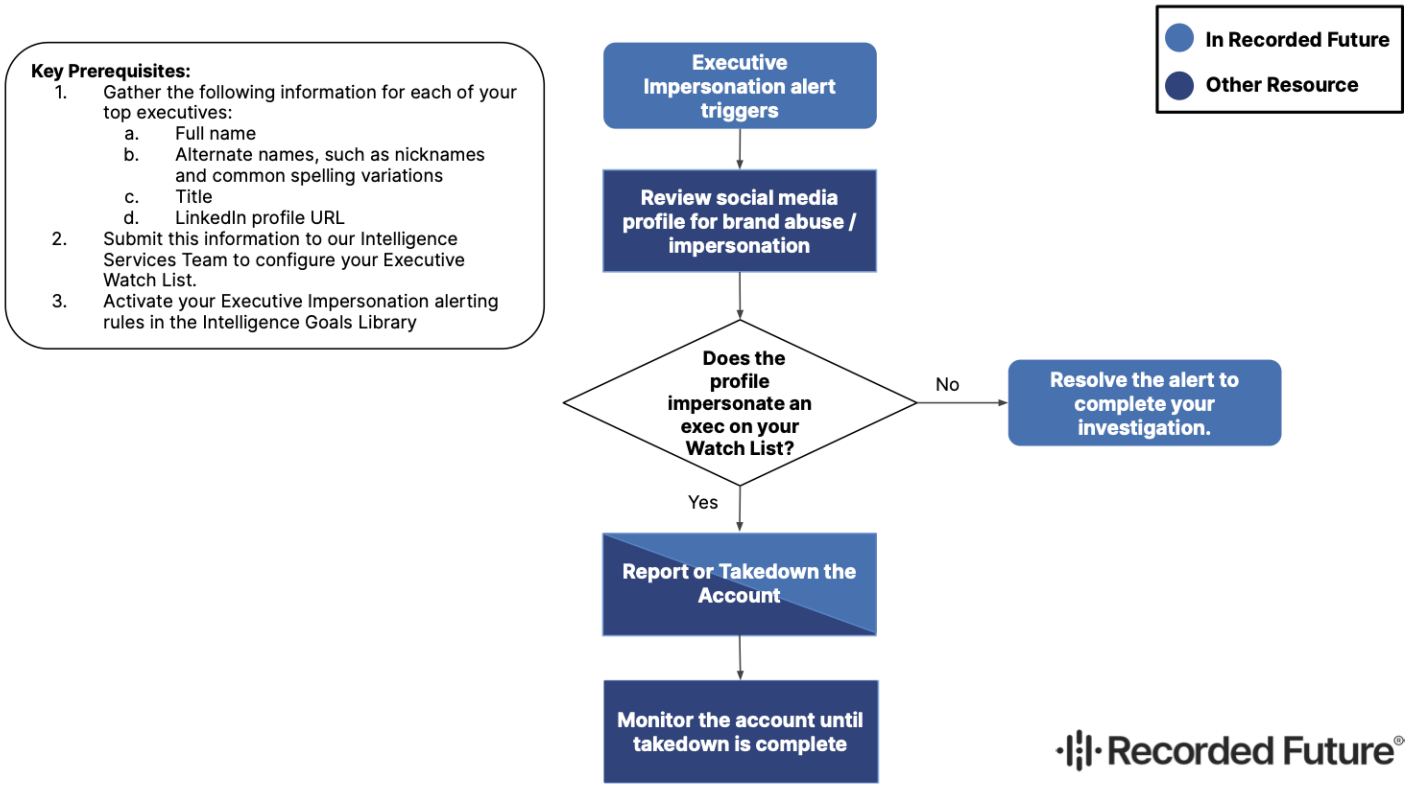
Key Prerequisites

1. Gather the following information for each of your top executives for curation by our data team:

    - Full name
    - Alternate names, such as nicknames and common spelling variations
    - Title
    - LinkedIn profile URL

    Once you have submitted this information to our Intelligence Services Team, we will configure your Executive Watch List.
    Note that this list is limited to 10 executives. If you need to add additional names to your Executive Watch List, reach out to your Intelligence Services Consultant.

2. Activate your certified alerts in the Intelligence Goals Library for Executive Impersonation on Social Media and Executive Impersonation on professional networking websites.



Step 1: You receive an alert from the Executive Impersonation alerts configured according to the recommendations in Key Prerequisites above. Proceed to the next step.

Step 2: Assess whether the identified social media account poses an impersonation/brand abuse threat. The Social Media Brand Abuse page can serve as a guide in this assessment.

Identify the relevant social media account username that triggered the alert. Click the relevant bolded text in the alert to open the Intelligence Card for that username.

- If your organization permits, navigate to the account's page on the relevant social media site (this will be specified in the Intelligence Card). Search on the site, place the username in the relevant URL and navigate there directly (e.g., https://twitter.com/RecordedFuture), or use other resources (search engines, search engine caches or web archives, commercial social media management solutions) to research details such as account profile pictures and other profile metadata.
- If you are not permitted to navigate to certain sites, you can use Recorded Future to research social media impersonation activity. From the Username Intelligence Card, click the link to "Show all events," which will display recent and historical references involving

that username, such as social media posts that were published by or mention the username:

Step 3: Based on your investigation, does the account appear to impersonate an executive within your organization?

→YES, impersonation is evident. → Proceed to Step 4.
→NO, there is no current evidence of impersonation or brand abuse, or indications of potential future abuse. → Resolve the alert to complete your investigation.

Step 4: Request a Takedown.

Use Recorded Future's Brand Protection Takedown Services to take the account down (also see Social Media Brand Abuse). If you are planning to request a takedown, note that takedown providers strongly recommend submitting a copy of the executive's government-issued ID.

Your organization's Legal or Marketing departments may also be able to contact the social media site directly in order to report the account or have the account removed.

Proceed to the next step.

Step 5: Monitor the account until the takedown is complete.

Once you have submitted your takedown request, we recommend continuing to monitor the entity until the takedown is complete.

Have more questions regarding this topic: Submit a request

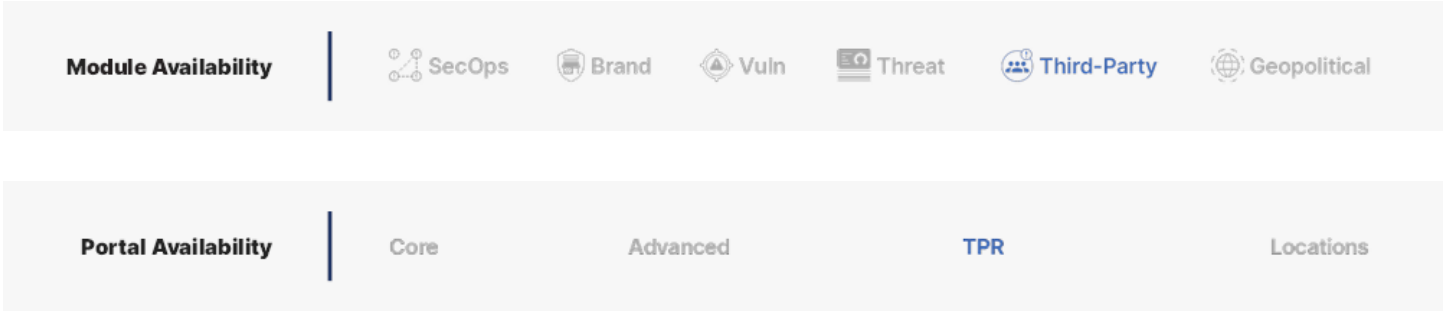
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Vendor Risk Assessment

PLAYBOOK

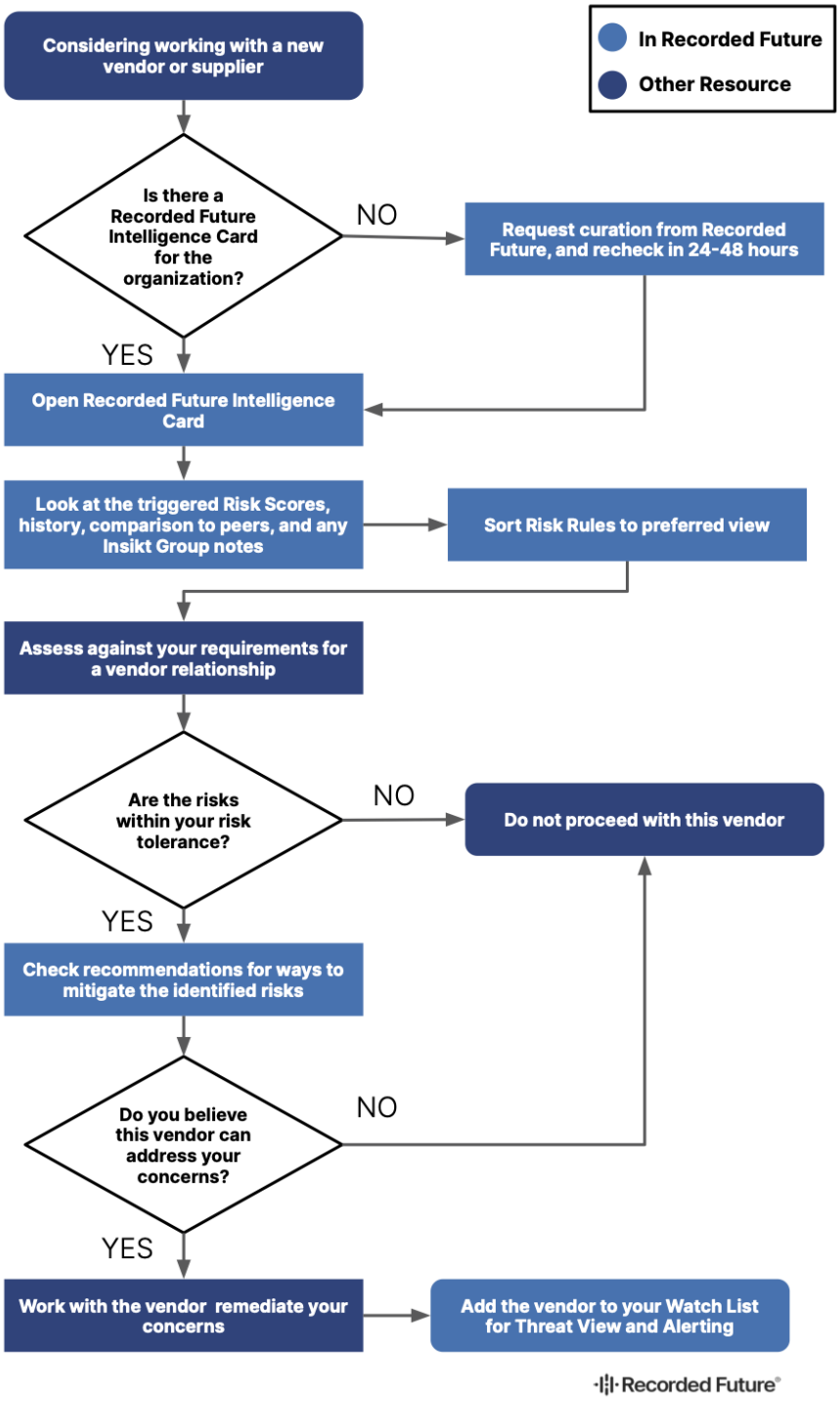
1st edition

Vendor Risk Assessment Playbook



This playbook walks you through using Recorded Future Intelligence Cards to assess the potential risks of a new vendor or re-evaluating a current vendor as part of your compliance processes.

Note: The platform has Intelligence Cards for both Organizations and Companies that trigger the same category of Risk Rules and present the same type of information. We use the term “organization” throughout this playbook, but the same steps would apply when investigating a “company” Intelligence Card.


Considering working with a new vendor or supplier
In Recorded Future
Other Resource
Is there a Recorded Future Intelligence Card for the organization?
NO
Request curation from Recorded Future, and recheck in 24-48 hours
YES
Open Recorded Future Intelligence Card
Look at the triggered Risk Scores, history, comparison to peers, and any Insikt Group notes
Sort Risk Rules to preferred view
Assess against your requirements for a vendor relationship
Are the risks within your risk tolerance?
NO
Do not proceed with this vendor
YES
Check recommendations for ways to mitigate the identified risks
Do you believe this vendor can address your concerns?
NO
YES
Work with the vendor remediate your concerns
Add the vendor to your Watch List for Threat View and Alerting
Recorded Future

Step 1

You are interested in working with a new organization or are conducting an assessment of your current vendor.

First, search the Recorded Future platform for more information.

Is there an Intelligence Card for the organization and does it have a star symbol next to it, if there is?

- If No, Request curation from Recorded Future and search again in 24-48 hours. Learn more about this process here.
- If Yes, open the organization's Intelligence Card.

Step 2

Review the following information on the organization's Intelligence Card:

- Risk score
- Triggered risk rules
- Risk score history and graph
- Comparison to peers
- Analyst notes from Insikt Group

Compare the triggered risk rules against the security standards you hold your vendors to, such as email policies, required disclosure of recent security breaches, or the use of software that is out of date or no longer supported.

Note: To adjust how these risk rules are arranged, click the highlighted word after "Arrange by" and select the view most valuable to you from the dropdown menu.

After reviewing the information, did you identify any risk factors that would make you reconsider doing business with this vendor?

- If Yes, but you would still consider working with them, continue to step 3.
- If Yes, and the risks are too great, do not move forward with this vendor.
- If No, proceed to step 4.

If you need more information to make a decision, work with your Vendor Risk Management team to develop clearer risk assessment criteria.

Step 3

You identified some potential risks but would consider moving forward if the vendor can remediate some of your concerns.

Determine next steps based on the severity and type of risk. For example:

- High-Impact Abuse of Company Infrastructure: Inform the vendor of detection and ask about IT security policy procedures.
- Domain with overly permissive SPF record: Log the domains and reach out to the vendor to discuss their remediation strategy.
- High Volume of Exposed Credentials: Notify the vendor and suggest immediate password changes and multi-factor authentication, especially for accounts or systems that connect to first-party information systems.

See more recommendations by risk factor on the Support Site, which suggests specific actions to mitigate risk for your organization and the organization you are assessing.

Do you feel confident that the vendor will be able to address your concerns?

- If Yes, proceed to Step 4.
- If No, do not move forward with this vendor.

Step 4

Consider the potential impact a security breach or service outage from this vendor could have on your business. Find out if your organization shares sensitive data or client personal identifying information (PII) with this vendor.

Work with the vendor to address your concerns.

With these factors in mind, have you decided to start or continue working with this vendor?

- If No, repeat the process with the next vendor you'd like to review.
- If Yes, add the organization to your Watch List so that you can set up real-time alerts and view that organization in your Threat Views.

We recommend configuring these rules in the Intelligence Goals Library to monitor the suppliers and vendors you choose to work with to alert you to changes in their security posture that may impact your business:

- Third-Party Risk: Increased Company Risk Score
- Third-Party Risk: Trending Companies

Have more questions regarding this topic: Submit a request

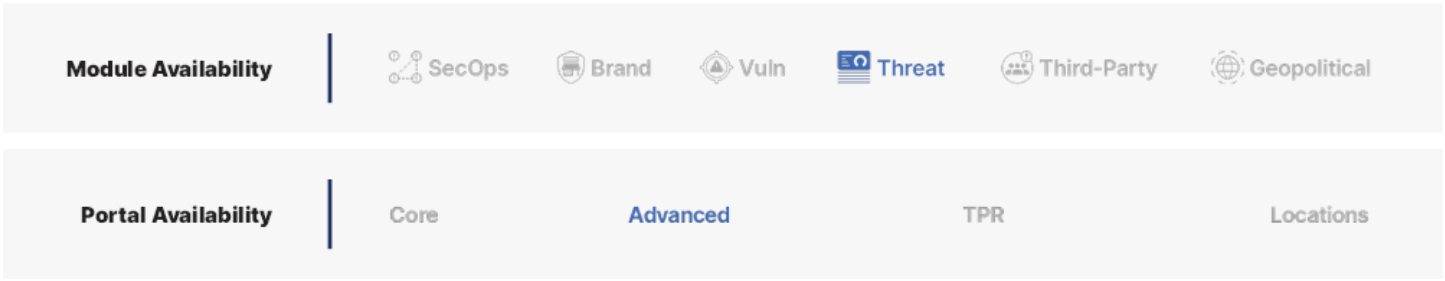
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Operationalizing Ransomware Intelligence

PLAYBOOK

1st edition

Operationalizing Ransomware Intelligence Playbook



Ransomware attacks targeted organizations across all sectors globally in 2020, and the trend has continued in 2021. Ransomware operators constantly evolve their operations and the tactics, techniques, and procedures (TTPs) they use, but Recorded Future is constantly working to keep tabs on these trends. If you are not already subscribed to the Threat Research Blog, we recommend that you subscribe now. Our Insikt Group researchers produce regular reporting on malware, malicious tools, and threat actors, including those related to ransomware, which can help you proactively defend your networks against these types of attacks.

Recorded Future will continue to release hunting packages and recommend mitigation tactics for new ransomware families and variants.

Please note that this guidance is not exhaustive and only represents some of the potential actions to consider. If you suspect a ransomware attack, your teams should immediately consult your own incident response playbooks.

Once you have been targeted by ransomware threat actors, attacks often escalate quickly. We have outlined ways to detect and respond to the threat across different stages of the attack, from initial access to lateral movement to exfiltration to the final opportunity to intervene before your files are encrypted.

Threat actors are continually revising their TTPs to evade defenses, underscoring the need for a layered security control strategy (as well as the need for threat intelligence). This playbook will cover recommendations on how to operationalize Recorded Future resources across the common stages of a ransomware attack:

- Stage 1: Initial Access
- Stage 2: Staging and Distribution

- Stage 3: Exfiltration
- Stage 4: Immediately Before Encryption
- Stage 5: After Encryption

The earlier you can detect the intrusion, the better chance you have of intercepting the threat actors and preventing your files from being ransomed. Your ability to detect and intervene in each stage will depend on detection mechanisms and pre-configured alerting.

Recorded Future®

OPERATIONALIZING RANSOMWARE INTELLIGENCE

Steps with this icon reference intelligence or actions made available through Recorded Future

Across all Stages

Leverage threat hunting packages to detect and hunt suspicious activity in your networks.

1. Set up alerts for new Insikt Group notes on malware/ransomware
2. Download relevant detection signatures
3. Refine for your organization as needed
4. Implement detection signatures in your environment
5. Configure SIEM or IDR alerting rules for the hunting packages you download

1 Initial Access

- Monitor for brand mentions on the dark web
- Track Threat Leads
- Review security controls for phishing
- Monitor for leaks of emails and credentials involving your domains
- Monitor your tech stack for vulnerabilities often used by ransomware actors
- Enable ransomware-related Certified Alerting rules
- Continuously monitor third-party vendors

2 Staging and Distribution

- Monitor for suspicious movement across your environment
- Deploy specific detection signatures and alert on behavior

3 C&C Communication and Exfiltration

- Monitor for large file transfers at all hours
- Block connections associated with C&C infrastructure
- Detect and alert on communications with IPs or domains associated with recent C&Cs
- Monitor for anomalous FTP, SFTP, or SCP traffic and interrupt it if possible

4 Pre-Encryption

- Monitor for unusual parent-child processes
- Detect shadow copy deletion

5 After Encryption

- Minimize destruction. Unplug or shut down the network, if necessary
- Mobilize your plan
- Remove suspicious access to the network and review logs to identify how they got access
- Assess the damage and contact your legal department
- Start the clean-up process and use your backups
- Consider all angles before responding to the ransom request
- Continue monitoring for mentions of internal assets for sale on the dark web

Across All Stages

Leverage threat hunting packages to detect and hunt suspicious activity in your networks.

Insikt Group writes, collects, and publishes a number of detection signatures including YARA, Snort, and Sigma rules that are available in the platform and associated with reports on relevant malware, threat actors, and TTPs. Deploying these detection signatures will require your organization to implement network and/or endpoint logging and to leverage automated event monitoring. For example, your ability to see value from certain Sigma rules will depend on the type of logs ingested into your SIEM. Learn more about Sigma rules if you have questions.

1. Set up alerts for new Insikt Group notes on malware/ransomware
2. Download relevant detection signatures
3. Refine as needed for your organization
4. Implement detection signatures in your environment (SIEM and/or other monitoring systems you already use)
5. Configure SIEM or IDR alerting rules for the hunting packages you download so that you are notified and can react quickly

In each stage, we will reference specific detection signature examples relevant to that stage.

Stage 1. Monitor for initial access

Threat actors can access your system in a number of ways, including exploiting known vulnerabilities, phishing campaigns, brute-forcing passwords, and leveraging toolkits. Use the data in our portal and from our analysts at Insikt Group to determine the most relevant threats to you and your organization.

1. Configure monitoring for mentions on the dark web for awareness of potential compromise or increased interest in your assets.

2. Track Threat Leads, which cover sales of unauthorized access on the dark web/special access forums.

   For more targeted results, create an advanced query for “Threat Lead” AND [your industry/watch list].

3. Review internal security controls for phishing.

   Use Recorded Future Security Control Feeds with email security tools to block or filter potentially malicious inbound communications, and Risk Lists to detect indicators of potential phishing activity that may have already landed on the network.

   Monitor for typosquatting and impersonation domains and take down suspicious or malicious domains that could be used to carry out phishing attacks against your organization.

   Monitor for email, credential, and PII leakage (more details below). Threat actors use leaked data to tailor their messaging as part of spearphishing attacks.

   Reference the Investigating a Potential Phishing Playbook if you do receive suspicious emails.

4. Monitor for leaks of emails and credentials involving your domain. Threat actors regularly use valid accounts or brute-forcing techniques to achieve initial access on victim networks.

5. Monitor your tech stack for vulnerabilities often used by ransomware actors. If you had an unpatched vulnerability known to be of common use to ransomware actors, add it to your patching priority list.

   This example query covers some recently exploited vulnerabilities.

6. Enable the following Certified Alerting rules or create custom variations of these rules:
   - Ransomware: Trending Exploit Kits
   - Ransomware: Trending Ransomware

7. Continuously monitor your third-party vendors, suppliers, and partners for the risks highlighted above. As demonstrated by supply chain attacks throughout 2021, threat actors continuously seek to compromise supply chain entities and then move laterally to other, often higher-value targets.

Stage 2. Look for signs of staging and distribution

1. Monitor your network for signs of staging and distribution activities across your environment.

   The initial access point is just a way in. It is usually insufficient for gathering the desired information or having the environment-wide impact the ransomware actor aims to achieve. Next steps may include dropping additional tools, expanding into other systems, and escalating permissions.
   The "dwell time" associated with these actions allows threat actors to gather more information during their discovery phase, including potentially seeking out financial data so they can determine how much to demand in ransom.
   This time also provides you with an opportunity to discover them in the act.
   To do this, we recommend leveraging hunting packages for the major samples analyzed by Insikt Group in the following reports:
   - Detecting Tool Use with Malign Intent: See the section Staging and Distribution for more guidance.
   - Detecting Cobalt Strike Attacks: See the sections on Detection Techniques related to Persistence and Lateral Movement for more guidance.
2.

   Examples include (but are not limited to):
   - Versions of Qakbot that manipulate registry keys and try to evade detection
   - Sigma rules detecting different stages of Egregor
   - This query finds all hunting packages related to QakBot and Cobalt Strike (a post-exploitation tool designed for pen testers and red team operators but incredibly popular with real threat actors)
   - Use this query to surface additional Hunting Packages from Insikt Group tagged with malware staging and distribution tactics. An effective way to narrow this query's results is to add particular malware or malware categories of interest, such as Ransomware, Offensive Security Tools, or Trojans.
2. If you detect suspicious lateral movement of any kind, follow your incident response plan to isolate and remove the threat.

Stage 3. Look for exfiltration

Threat actors participating in a ransomware attack are often indiscriminate about what data they steal and from where – as it is difficult to determine what is and isn't important or valuable. Because of this, ransomware actors will usually steal large volumes of files at a time.

The following steps will help you identify any large-scale data exfiltration that may have occurred within your environment:

- Monitor for large file transfers at all hours.
  Establish baseline behavior for file transfers within your organization and then monitor for anomalies (e.g., transfers occurring overnight or on weekends or strangely large file transfers).

- Block network communications with current and recently active C&C infrastructure.
  Recorded Future's Insikt Group originates malware signatures and uses a specialized scanner to continuously explore the Internet and identify and validate C&C servers. The Command and Control Security Control Feed provides prevent/block-grade indicators sourced from the C&C list. Synchronize this dataset on a daily basis with an Enterprise Firewall, WAF, Personal Firewall, or Distributed Firewall to block validated C&C infrastructure with low risk for collateral damage.
- Detect and alert on communications with recent C&Cs (and malicious IPs and domains generally).
  Threat actors are limited in where they can host their services and servers; as a result, they reuse infrastructure or acquire new infrastructure from previous providers. Risk Lists provide detect-grade sets of indicators best suited for correlating and alerting on network communications with malicious infrastructure, as determined by Recorded Future risk scoring.
  For mitigating C&C threats, these efforts can be focused on outbound/egress traffic. This query also surfaces malicious infrastructure specifically associated with ransomware, useful for more targeted threat hunting purposes.

- Do you normally use FTP, SFTP, or SCP?
  - If not → Monitor for this type of traffic and investigate if you notice any
  - If yes → Establish a baseline and monitor for anomalous traffic

- If you detect file transfers that suggest exfiltration of your files or a connection to a potentially malicious C&C server, sever their connection and follow your incident response plan to isolate and remove the threat.

Stage 4. Detect right before encryption

The process of encrypting your system's files also can give off tell-tale signs that if you detect while in progress, you may still have time to act.

Note: This process is scripted and could involve hundreds or thousands of machines simultaneously. You need to act very quickly.

1. Monitor for unusual parent-child processes. Often ransomware actors will create a "cmd.exe" child process to accomplish key enablement tasks, such as, deleting shadow copies, killing process / services or tasks. We recommend monitoring for this type of activity with a SIEM or EDR with a Sigma rule.

2. Detect shadow copy deletion. In the ransomware enablement phase, one of the most common actions performed is the deletion of the Windows shadow copies, which contain backups of user data. Use the Insikt Group Sigma rule to help detect this type of activity. A YARA rule is also available to detect MountLocker's shadow copy deletion process, and other detection signatures may become available over time.

You generally have seconds from when Windows shadow copies are deleted to when files start getting encrypted. Whenever possible there should be an automated rule to kill any process deleting Windows Shadow copies.

Stage 5. After encryption

Note: We do not encourage paying a ransom. Doing so may incur fines or other penalties as the politics around these threats continues to evolve. Additionally, you may face other issues with Consumer Protection Policies or GDPR if you do not disclose or regain access to these files.

1. Minimize destruction. Unplug or shut down the network, if necessary.

2. Mobilize your incident response plan.

3. Remove suspicious access to the network and review logs to identify how they got access.

4. Assess the damage.

5. Contact your legal department for their recommended next steps.

6. Start the clean-up process and use your backups.
    - If you are trying to recover files forensically, you might need to bring in a reputable/trusted third party.

7. Consider the following before responding to any extortion demands:
    - How essential are these files?
    - Does your backup work?
    - Understand your exposure and the inherent risk of your different options.
    - Understand what responsibility you have to disclose ransomware attacks.

8. Continue monitoring for mentions of internal assets for sale on the dark web that may have been acquired in the breach.

Additional Reading

Research and Reporting

- Detecting Tool Use With Malign Intent
- Despite Rumors to the Contrary, Cobalt Strike Attacks Can Be Detected
- Introduction to Sigma Rules and Detection of Credential Harvesting
- Protect Against BlackMatter Ransomware Before It's Offered
- An interview with BlackMatter: A new ransomware group that's learning from the mistakes of DarkSide and REvil

Support Resources

- Ransomware Campaign Mitigation Guide
- Sigma Rules in the Recorded Future portal
- Building a Year-in-Review for Ransomware Attacks
- E-learning: Sigma Rules

Webinars

- Rise of the DarkSide and Ransomware-as-a-Service
- Ransomware Trends Update: Here's What We Know From the Recent Attacks
- REvil Unlocks the Key to Kaseya

Outside Resources

CISA: Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches

---

Have more questions regarding this topic: Submit a request

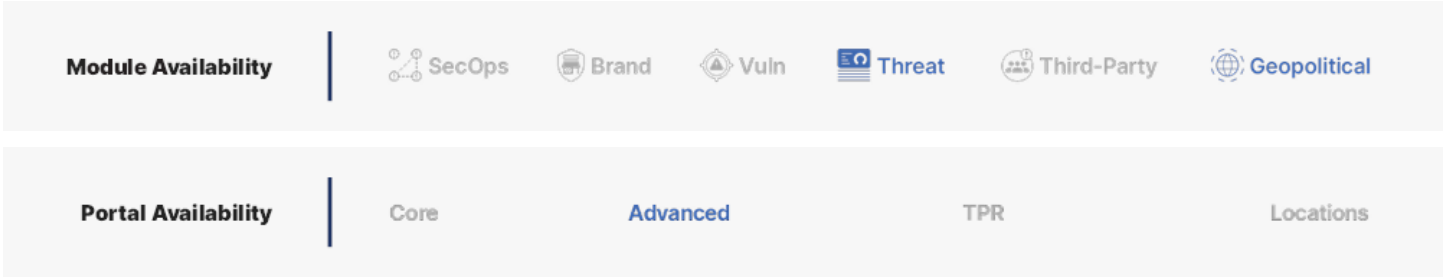
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Investigating Leaked Code

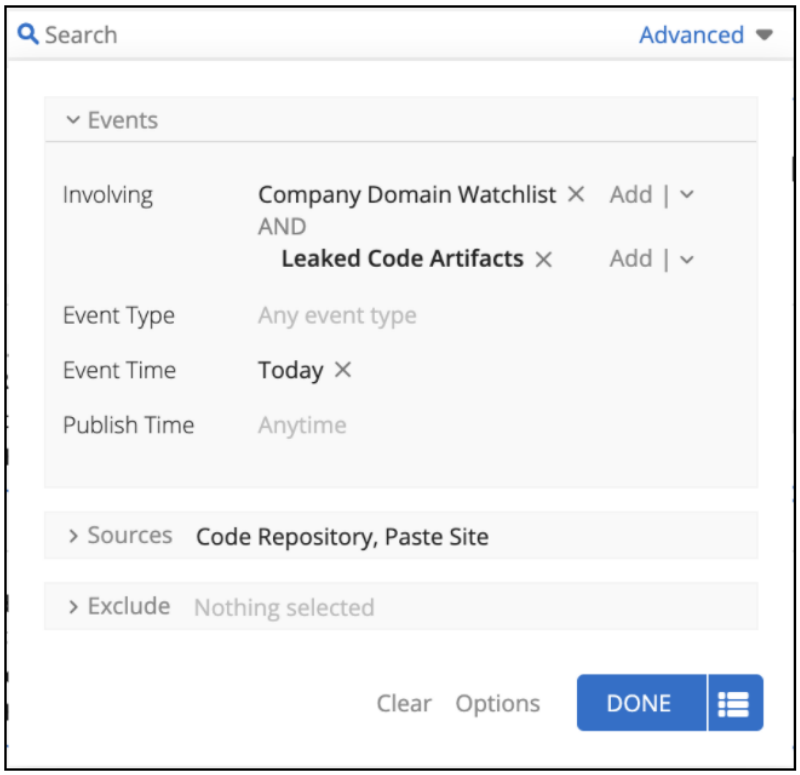
PLAYBOOK

1st edition

Investigating Leaked Code Playbook



This Recorded Future Playbook is designed to walk you through some possible research steps to identify the source for leaked code. If you are using the "Domains on Code Repositories" Intelligence Goal, you may find that it sometimes results in too many alerts to work through in detail. Introducing custom logic like this query into your alerting rules can reduce noise and cover additional proprietary information beyond domains.



Note: "Leaked code artifacts" is a category of text matches that we have curated to surface leaked source code and configuration files; it includes file extensions (.cscfg, .log, .mdf), keywords (config, admin) and other code identifiers (key_token).

For other examples and information on creating queries to monitor for leaked code, see this Insikt Group blog post.

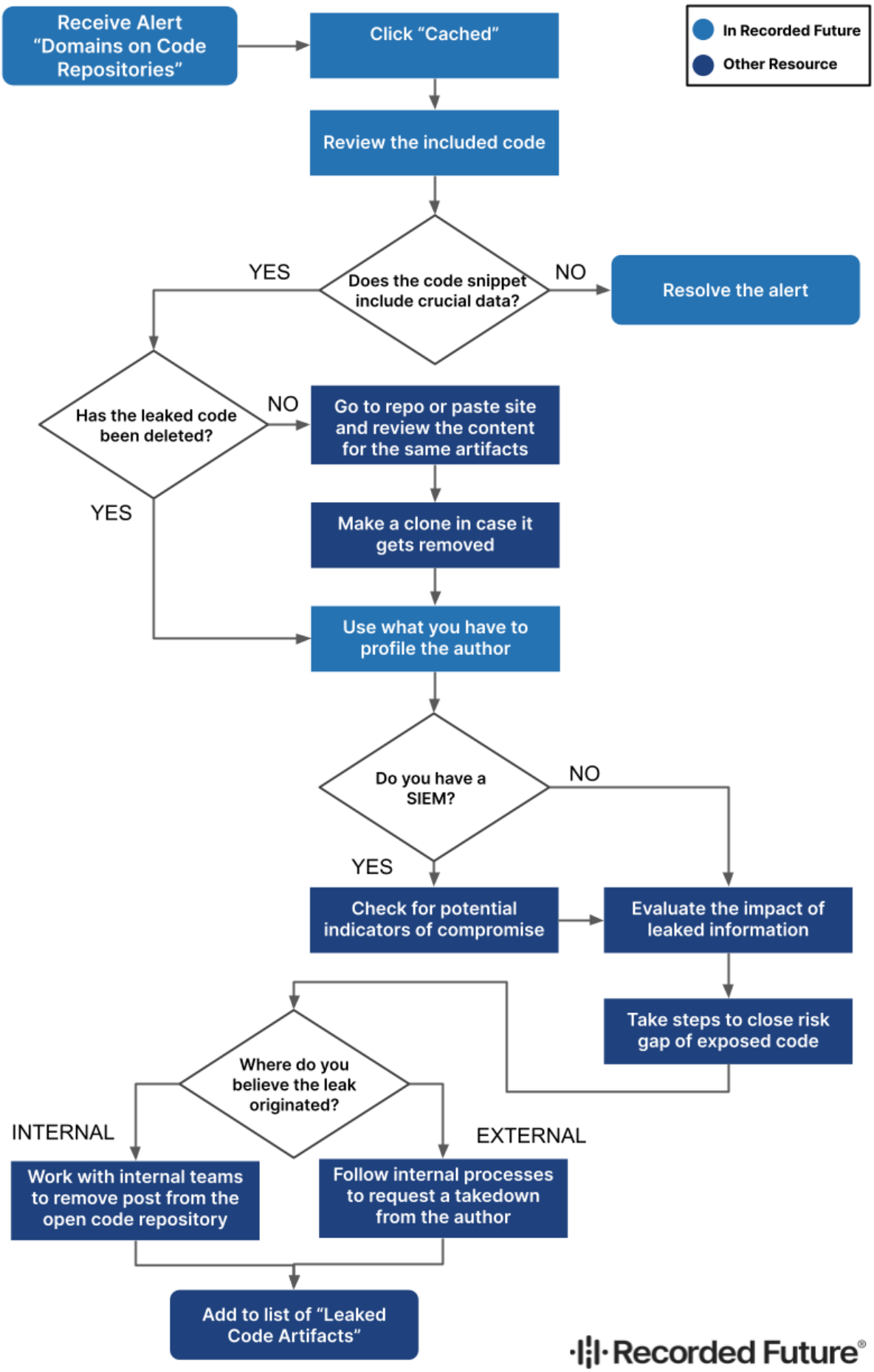
Note: This query is a recommended starting point. Work with your consultant to narrow down the logic if needed.

This logic can be helpful in the following scenarios:

- Employees/developers exchanging data via pastebin as a shortcut
- Admins committing changes into an open repo by mistake
- Developers committing code that includes internal information (e.g., in code comments)
- Contractors, current or prior, who may have posted code as part of their group's workflow, or as an undesired shortcut

The following skills can be helpful when executing the steps in this playbook:

- Familiarity with configuration files
- Parsing and reading json
- A working knowledge of coding languages (python / java / shell / powershell)
- The ability to recognize context based on code syntax (you may be unable to see the full context based on the snippet captured in the platform)


Receive Alert "Domains on Code Repositories"
Click "Cached"
In Recorded Future
Other Resource
Review the included code
Does the code snippet include crucial data?
YES
NO
Resolve the alert
Has the leaked code been deleted?
NO
Go to repo or paste site and review the content for the same artifacts
YES
Make a clone in case it gets removed
Use what you have to profile the author
Do you have a SIEM?
NO
YES
Check for potential indicators of compromise
Evaluate the impact of leaked information
Take steps to close risk gap of exposed code
Where do you believe the leak originated?
INTERNAL
EXTERNAL
Work with internal teams to remove post from the open code repository
Follow internal processes to request a takedown from the author
Add to list of "Leaked Code Artifacts"

Step 1

You receive an alert on “Domains on Code Repositories” Intelligence Goal.

Step 2

Click “Cached.”

Step 3

Review the code. Is any sensitive data included, such as the following?

- Internal URLs/domains
- Usernames
- PII
- Credit card data/BINs
- Keys/tokens
- Passwords
- Cloud Account/Identification IDs
- Port Access Info
- Network Mapping Info
- Critical Infrastructure Info

If NO, resolve the alert.

If YES, continue to the next step.

Step 4

Has the leaked code been deleted?

If so, this is a strong indicator that the data is of concern. These leaks are usually a mistake; if it is noticed and quickly taken down, Threat Actors have often already captured or cloned the data. If this is the case, it’s important to take swift action to remediate the damage that can be done.

Step 5

Go to Repo or Paste (outside RF) and review all of the content for the same artifacts. Make a clone of the repo/paste site in case it is taken down.

Step 6

Profile the author. This will help you determine the circumstances under which the code was leaked. For example, an external author may indicate a system breach.

- What is the nature of other data the author has published?
- Is it supposed to be public?
- Is it test data?
- What can you tell about what the code is doing?
- Is it relevant to your organization or client?
- Is it a 3rd party, employee, or other?

Note: You can see Adversary Behavioral Profiling for an exercise that can help you identify and prioritize actors, malware, and TTPs that threaten your organization.

Step 7

If you have a SIEM, check it for related indications of compromise. Use the following questions to help determine whether this could be the source of the leaked information.

- Look for related leaked applications/host logs.
- Is there any incoming suspicious activity that may have been accessing the code snippet posted?
- Search for unusual activity from any internal developer accounts.

Step 8

Evaluate the impact of the leaked information.

- Is it a cloud resource or local server?
- Can the leaked information be used to extract further data from an open endpoint or compromised resource?

Step 8b

Close the Risk Gap of Exposed Code.

Assume that the threat actor has the data, or has cloned it. Ask yourself the following questions:

- How do you secure your environment with this information out there?
- Do you have the right detection mechanisms and alerts in place to stop an attacker in that threat vector?

Step 9

Remediate this immediate leak.

- Work with your internal teams to remove this post from the open code repository if the author is internal. If not, follow your internal processes to contact the external author and request that they remove this internally sensitive information.
- After this exercise is complete, add any additional entities to the list you use to track leaked code artifacts.

Note: This list should act as a living document. Update your list each time you go through this process or identify any leaked code.

Have more questions regarding this topic: Submit a request

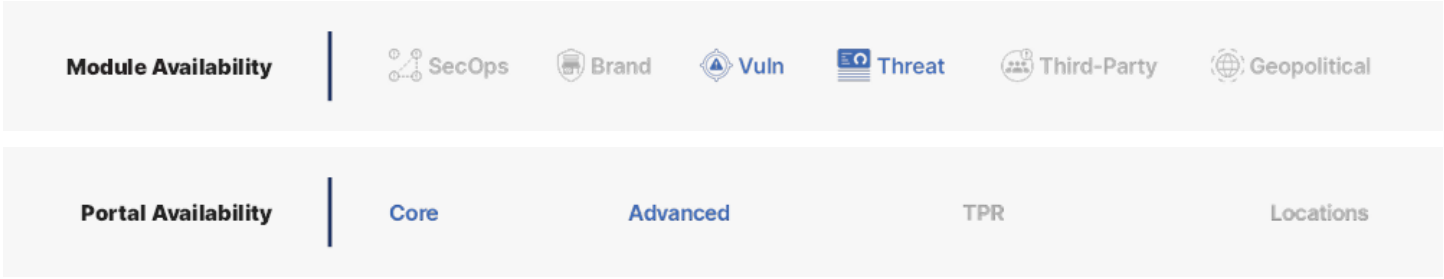
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Patch Tuesday

PLAYBOOK

1st edition

Patch Tuesday Playbook

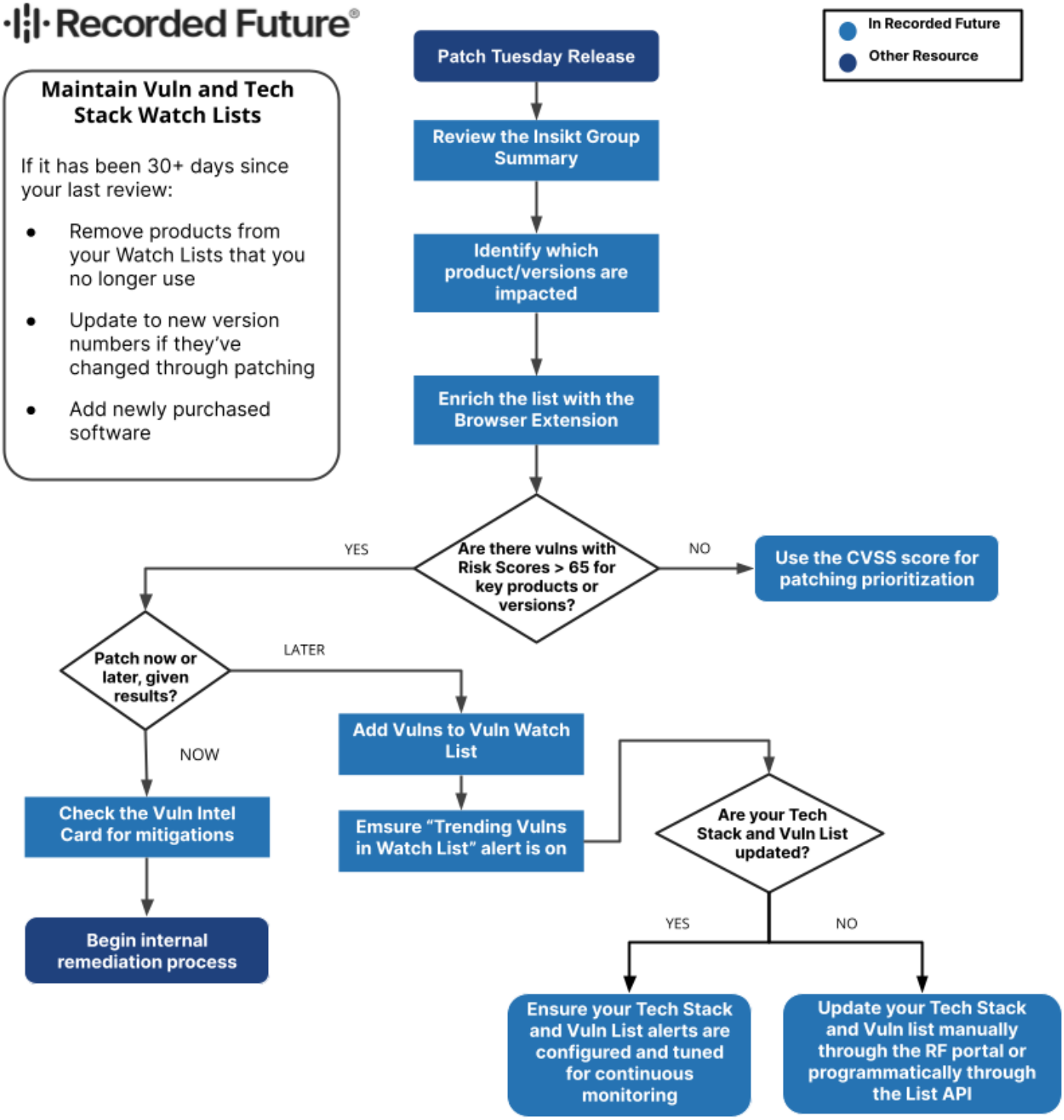


This playbook is designed to help you 1) prioritize and focus your patching efforts on the vulnerabilities that matter most, 2) continuously monitor those vulnerabilities, and 3) update the technology being monitored in a more real-time manner.

Note: This playbook covers vulnerabilities uncovered by a Patch Tuesday release. See our Vulnerability Prioritization Playbook if you're working from a triggered vulnerability alert or network vulnerability scan.

Prerequisites

- Recorded Future Browser Extension (Chrome, Firefox, Edge)
- Access to Insikt "Security Vendor Reporting" Analyst Notes (Core/Advanced platform and Vulnerability module users)
- Access to Vulnerability Watch Lists (Core/Advanced or Vulnerability Module) or Custom Lists (Core/Advanced or Threat Intelligence Module)


Recorded Future
In Recorded Future
Other Resource
Maintain Vuln and Tech Stack Watch Lists
If it has been 30+ days since your last review:
Remove products from your Watch Lists that you no longer use
Update to new version numbers if they've changed through patching
Add newly purchased software
Patch Tuesday Release
Review the Insikt Group Summary
Identify which product/versions are impacted
Enrich the list with the Browser Extension
Are there vulns with Risk Scores > 65 for key products or versions?
YES
NO
Use the CVSS score for patching prioritization
Patch now or later, given results?
LATER
NOW
Add Vulns to Vuln Watch List
Emsure "Trending Vulns in Watch List" alert is on
Check the Vuln Intel Card for mitigations
Begin internal remediation process
Are your Tech Stack and Vuln List updated?
YES
NO
Ensure your Tech Stack and Vuln List alerts are configured and tuned for continuous monitoring
Update your Tech Stack and Vuln list manually through the RF portal or programmatically through the List API

Step 1

It's Tuesday and all your major technology providers have published patches for vulnerabilities discovered that month. Depending on the vendor there are a few steps you can take to begin "Patch Tuesday" prioritization.

Step 2

Recorded Future's Insikt Group writes a note each month addressing the Patch Tuesday release.

Note: You have the option to download the excel sheet detailing the products impacted and exploitability of each vulnerability. Use this spreadsheet to narrow your focus to vulnerabilities impacting versions and products within your network.

Review the summary and run the Browser Extension over the the Insikt Note within the portal. This will help you order the Vulns based on risk, pulling out those identified as relevant and high risk.

Step 3

For more context on the vulnerabilities you plan to remediate, view their Intelligence Cards in the portal. The NVD Summary section may contain impacted products, mitigations, and additional metadata to assist in remediation.

Step 4

Based on the vulnerability, you'll want to weigh the impact to your business and evaluate the overall risk associated with the vulnerability. To better understand overall risk, ask yourself the following questions:

Judging impact

- How many instances of this technology are there throughout my network?
- Is this technology publicly facing?
- Is this technology protecting or embedded within a critical asset (e.g., server or CEO laptop)?

Evaluating risk

- Is the risk score above 65?
- Is this vulnerability known to be exploited in the wild?
- Does this vulnerability have any known proof of concept exploits or pen test tools linked to it?

Based on your answers to the above questions, prioritize which vulnerabilities are patched now and which will be patched later. For vulnerabilities that will have a delayed patch or that are not planned for patching, make sure to include higher-risk vulnerabilities in your "Vulnerability Watch List" for continuous monitoring. This can be done manually via the portal or programmatically through our new List API.

Step 5

We recommend updating your Vulnerability and Technology Stack Watch Lists on a recurring basis, which can be streamlined via our List API. If it has been 30+ days since your last review, we recommend that you:

- Remove products from your Watch Lists that you no longer use
- Update to new version numbers if they've changed through patching
- Add newly purchased software

You can then configure vulnerability-related alerts for continuous monitoring of your updated Watch Lists:

- Technology Stack (unknown vulnerabilities) - Configure alerts for monitoring new vulnerability information around your technology stack. In the Intelligence Goals Library there are five separate rules to track and detect on the lifecycle of a vulnerability.
- Specific Vulnerabilities (known vulnerabilities) - Configure alerts to monitor a specific subset of known vulnerabilities impacting your network that have not been patched. Within the Intelligence Goal Library, set up "Trending Vulnerabilities in Watch List" certified alerts to detect on increased cyber chatter related to your Vulnerability Watch List.

Have more questions regarding this topic: Submit a request

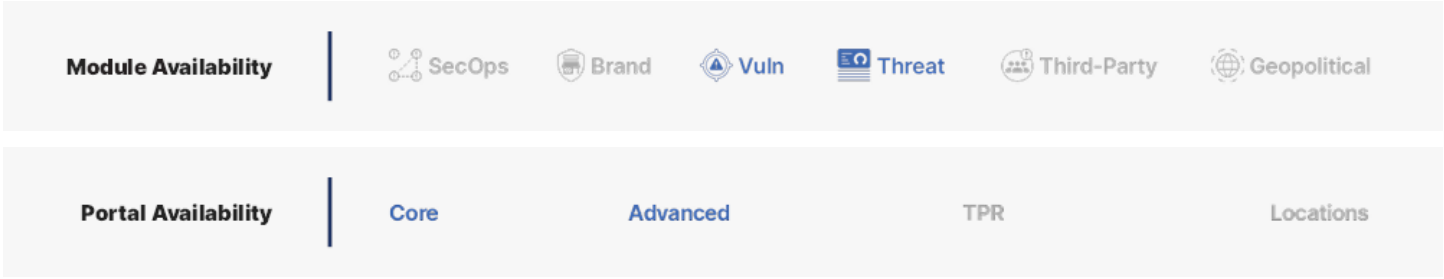
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Vulnerability Prioritization

PLAYBOOK

1st edition

Vulnerability Prioritization Playbook

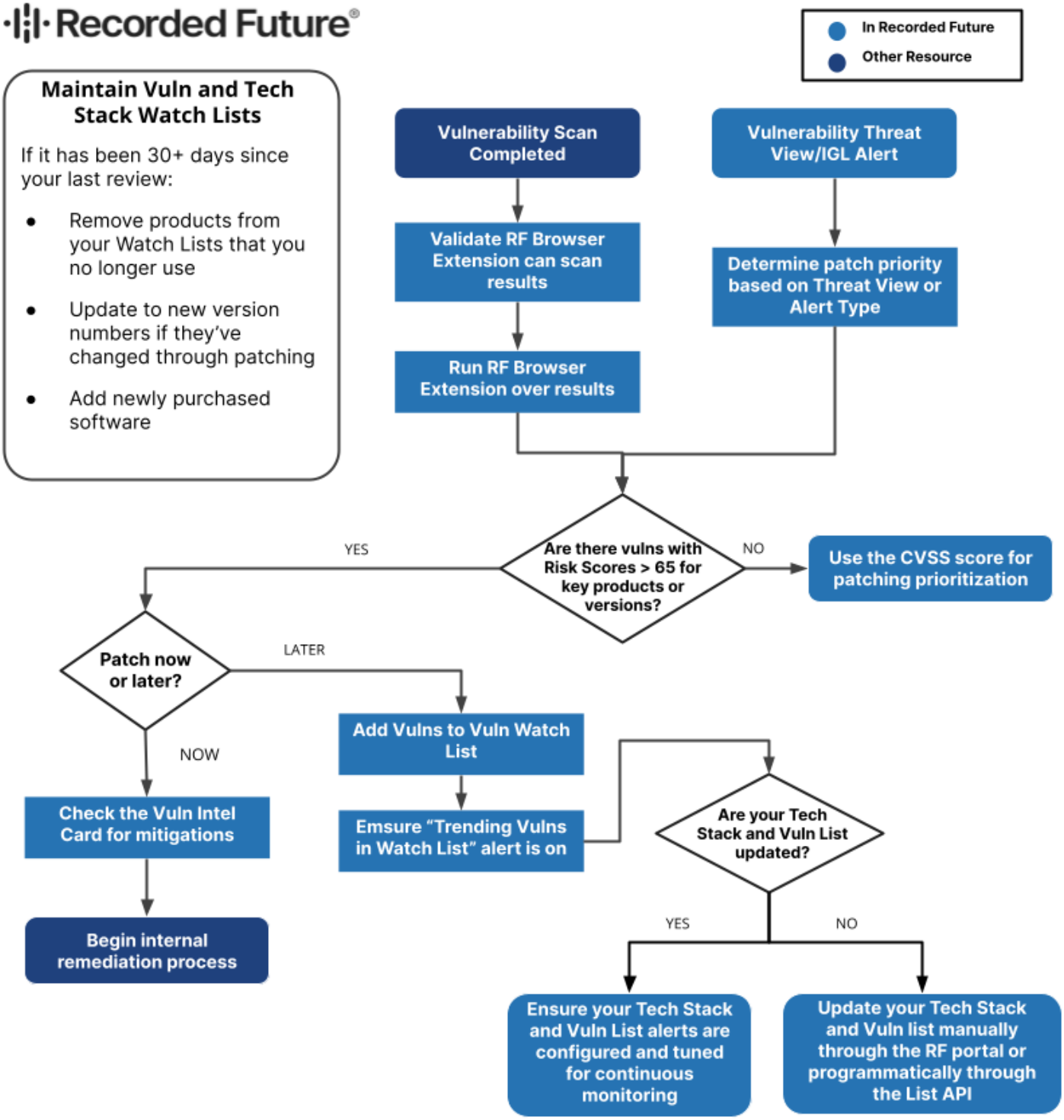


This playbook is designed to help you 1) prioritize and focus your patching efforts on the vulnerabilities that matter most, 2) continuously monitor those vulnerabilities, and 3) update the technology being monitored in a more real-time manner.

Note: This playbook covers vulnerabilities identified during a vulnerability scan of your network or a triggered vulnerability alert. See our Patch Tuesday Playbook if you're looking for information on Patch Tuesday patch prioritization.

Prerequisites

- Recorded Future Browser Extension (Chrome, Firefox, Edge)
- Access to Insikt "Security Vendor Reporting" Analyst Notes (Core/Advanced platform and Vulnerability module users)
- Access to Vulnerability Watch Lists (Core/Advanced platform or Vulnerability Module) or Custom Lists (Core/Advanced platform or Threat Intelligence Module)


Recorded Future
In Recorded Future
Other Resource
Maintain Vuln and Tech Stack Watch Lists
If it has been 30+ days since your last review:
Remove products from your Watch Lists that you no longer use
Update to new version numbers if they've changed through patching
Add newly purchased software
Vulnerability Scan Completed
Validate RF Browser Extension can scan results
Run RF Browser Extension over results
Vulnerability Threat View/IGL Alert
Determine patch priority based on Threat View or Alert Type
Are there vulns with Risk Scores > 65 for key products or versions?
YES
NO
Use the CVSS score for patching prioritization
Patch now or later?
LATER
NOW
Add Vulns to Vuln Watch List
Emsure "Trending Vulns in Watch List" alert is on
Check the Vuln Intel Card for mitigations
Begin internal remediation process
Are your Tech Stack and Vuln List updated?
YES
NO
Ensure your Tech Stack and Vuln List alerts are configured and tuned for continuous monitoring
Update your Tech Stack and Vuln list manually through the RF portal or programmatically through the List API

Outside the RF Portal	Within the RF Portal
Step 1 You've completed a vulnerability scan of your network and see that 100s of vulnerabilities need to be patched.	**Step 1** You receive an alert from Recorded Future based on a Vulnerability Threat View or IGL alerting rule you have set up.

Step 2

Check to see if the Recorded Future Browser Extension is capable of scanning this specific results page (e.g., Qualys, Splunk, ServiceNow).Run the Browser Extension on top of the results you received from your vulnerability scan. Once you've done this, you'll notice that the highest-risk vulnerabilities will appear at the top of the vulnerabilities list within the Browser Extension window. Depending on the number of vulnerabilities and their associated risk scores, we recommend pulling out the vulnerabilities 65 or higher to begin your remediation process. These vulnerabilities are rated both on overall impact and exploitability.

Alternatively, there is a CSV enrichment script available for users with API access. If your output is in CSV format you can use the script to batch enrich the results. For more information, contact your Intelligence Services consultant.

Note: PS credit costs apply.

Step 2

Determine patch priority based on Threat View or Alert Type. For Example:

- Pre CVSS/NVD (TBD based on analysis)
- Linked to Pentest Tools (Medium)
- Exploit Chatter (High)
- Linked to Malware (Critical)
- New Critical (Critical)

Step 3

Visit your technology provider's patch release website and run the Recorded Future Browser Extension over this month's vulnerabilities. Check to see if any of the highest-risk vulnerabilities are associated with the products and versions you're running within your network. If you have a hit, move on to remediation or continuous monitoring.

Step 4

Based on the vulnerability, you'll want to weigh the impact to your business and evaluate the overall risk associated with the vulnerability. To better understand overall risk, ask yourself the following questions:

Judging impact

- How many instances of this technology are there throughout my network?
- Is this technology publicly facing?
- Is this technology protecting or embedded within a critical asset (e.g., server or CEO laptop)?

Evaluating risk

- Is the risk score above 65?
- Is this vulnerability known to be exploited in the wild?
- Does this vulnerability have any known proof of concept exploits or pen test tools linked to it?

Based on your answers to the above questions, prioritize which vulnerabilities are patched now and which will be patched later. For vulnerabilities that will have a delayed patch or that are not planned for patching, make sure to include higher-risk vulnerabilities in your "Vulnerability Watch List" for continuous monitoring. This can be done manually via the portal or programmatically through our new List API.

Step 5

We recommend updating your Vulnerability and Technology Stack Watch Lists on a recurring basis, which can be streamlined via our List API. If it has been 30+ days since your last review, we recommend that you:

- Remove products from your Watch Lists that you no longer use
- Update to new version numbers if they've changed through patching

- Add newly purchased software

You can then configure vulnerability-related alerts for continuous monitoring of your updated Watch Lists:

- Technology Stack (unknown vulnerabilities) - Configure alerts for monitoring new vulnerability information around your technology stack. In the Intelligence Goals Library there are five separate rules to track and detect on the lifecycle of a vulnerability.
- Specific Vulnerabilities (known vulnerabilities) - Configure alerts to monitor a specific subset of known vulnerabilities impacting your network that have not been patched. Within the Intelligence Goal Library, set up “Trending Vulnerabilities in Watch List” certified alerts to detect on increased cyber chatter related to your Vulnerability Watch List.

Have more questions regarding this topic: Submit a request

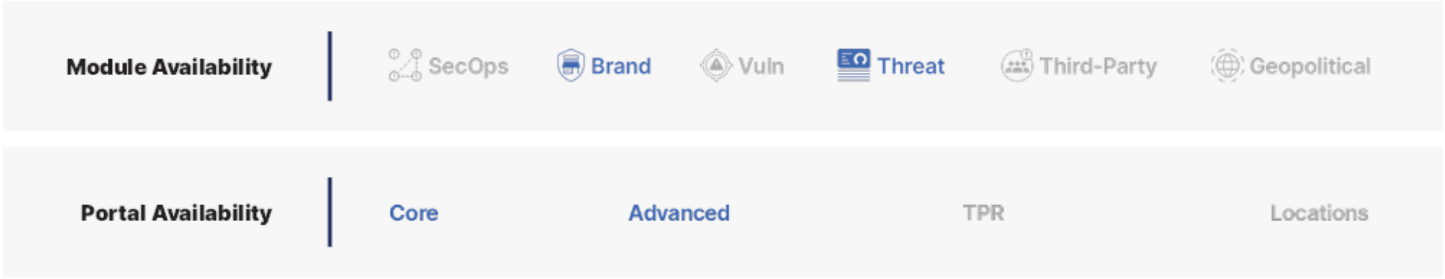
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Russian Market

PLAYBOOK

1st edition

Russian Market Playbook



Recorded Future's Russian Market Alerts Playbook is designed to help you better understand alerts from Russian Market and provide a repeatable set of steps you can follow to triage alerts and take action on Recorded Future intelligence.

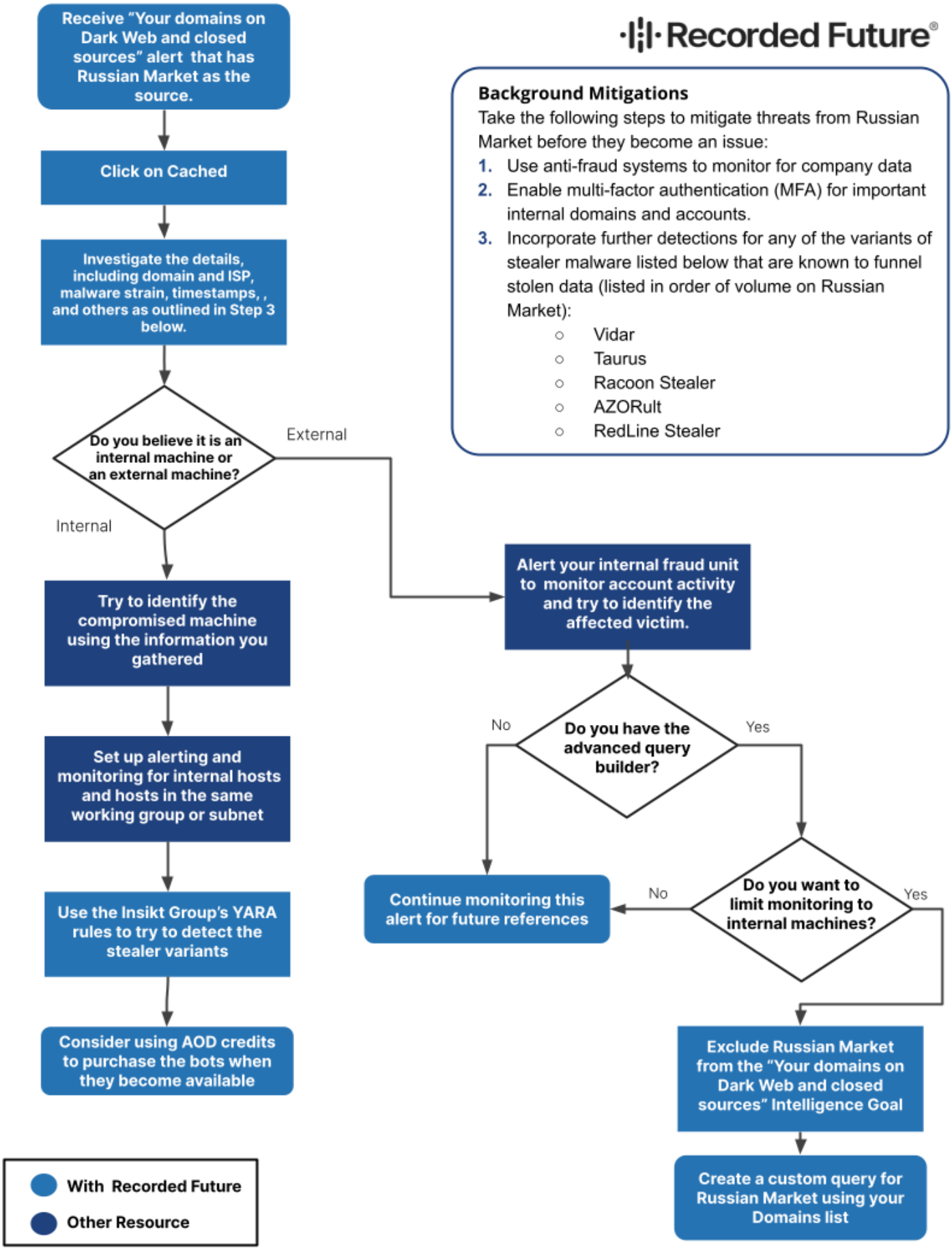
Looking for more information on Russian Market before you take action? Take a look at the Introduction to Russian Market on the Support Site or view Insikt Group's Russian Market Source Profile.

Recorded Future®

Background Mitigations

Take the following steps to mitigate threats from Russian Market before they become an issue:

1. Use anti-fraud systems to monitor for company data
2. Enable multi-factor authentication (MFA) for important internal domains and accounts.
3. Incorporate further detections for any of the variants of stealer malware listed below that are known to funnel stolen data (listed in order of volume on Russian Market):
    - Vidar
    - Taurus
    - Racoon Stealer
    - AZORult
    - RedLine Stealer



(Stealer Malware Listed: Vidar, Taurus, Racoon Stealer, AZORult, RedLine Stealer)

Step 1

You receive an alert from the 'Your domains on Dark Web and closed sources' Intelligence Goal. One of the references in the alert has the source 'Russian Market' and shows one of the domains in your Domains Watch List.

Note: If your enterprise activated this Intelligence Goals Library alert prior to July 21, 2021, it will be titled: 'Domains on Non-Mainstream Sources.'

Step 2

Click the 'Cached' button for information on which domain was alerted on and the other domains referenced alongside it in the advertisement.

Additionally, click 'view all matching references in Table view' and use the cog wheel to highlight matching criteria, which allows you to more easily identify *why* a particular alert was triggered.

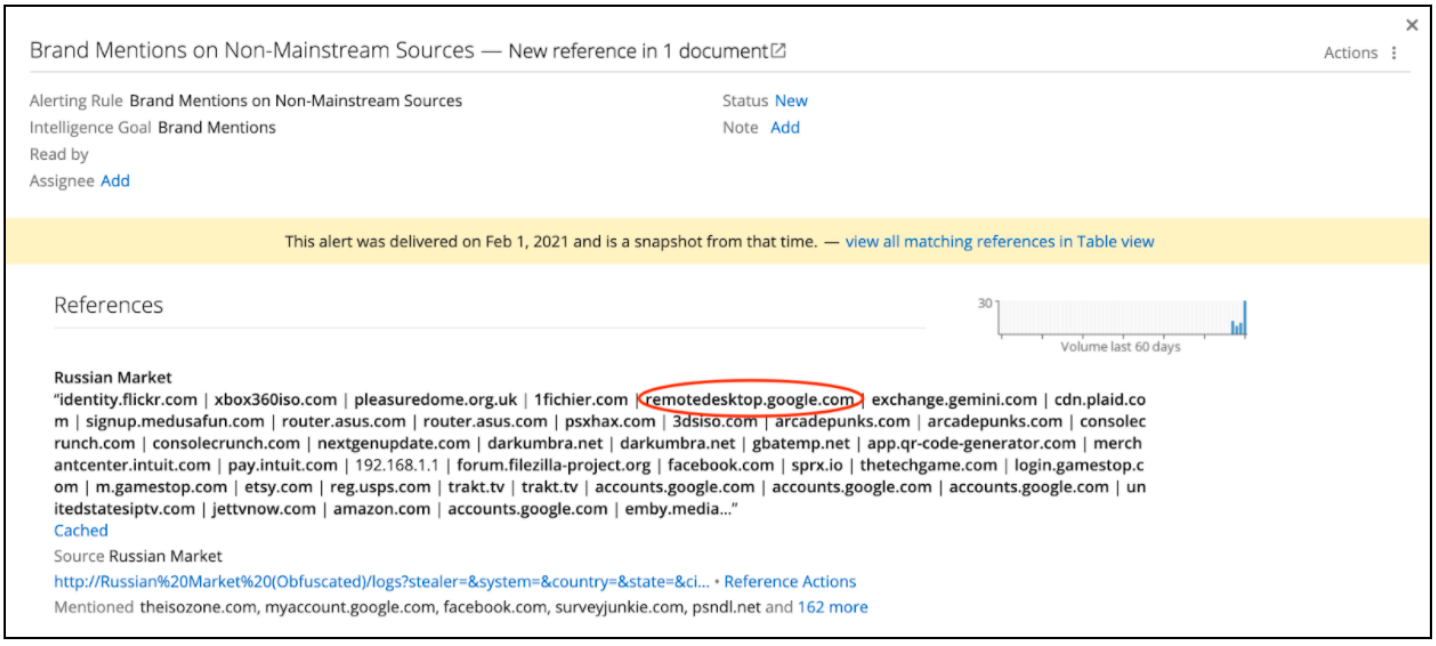


Image: Example of Recorded Future Alert from the 'Your domains on Dark Web and closed sources' Intelligence Goal

Step 3

Determine whether the information is from an internal company machine or an external customer machine.

If we alert you to a domain of interest that has appeared on Russian Market, it is almost certainly a reference to the Stealer Logs section of the marketplace (as of February 2021). Despite the marketplace also having a section devoted to the sale of RDP access for systems infected with an unknown strain of malware, this section of the marketplace does not reference victim domain information.

Gather the following details from the cached information to determine whether they align to details from an internal company machine and user, or an external customer's machine:

3.1. Your company domain is mentioned in the listing (along with possible Internet service provider (ISP)).

The presence of a victim domain indicates that the victim has login information saved to his/her browser, meaning that a purchaser is downloading a combination of login or cookie information rather than purchasing control over the entire machine.

- Is it an internal-only or an external customer domain?
- What ISP is the session information associated with?
- Is the ISP applicable to company business operations?
- What country is identified in the listing?
- Where is the ISP located geographically?

Tip: use Ctrl+F to find where your company domain is mentioned.

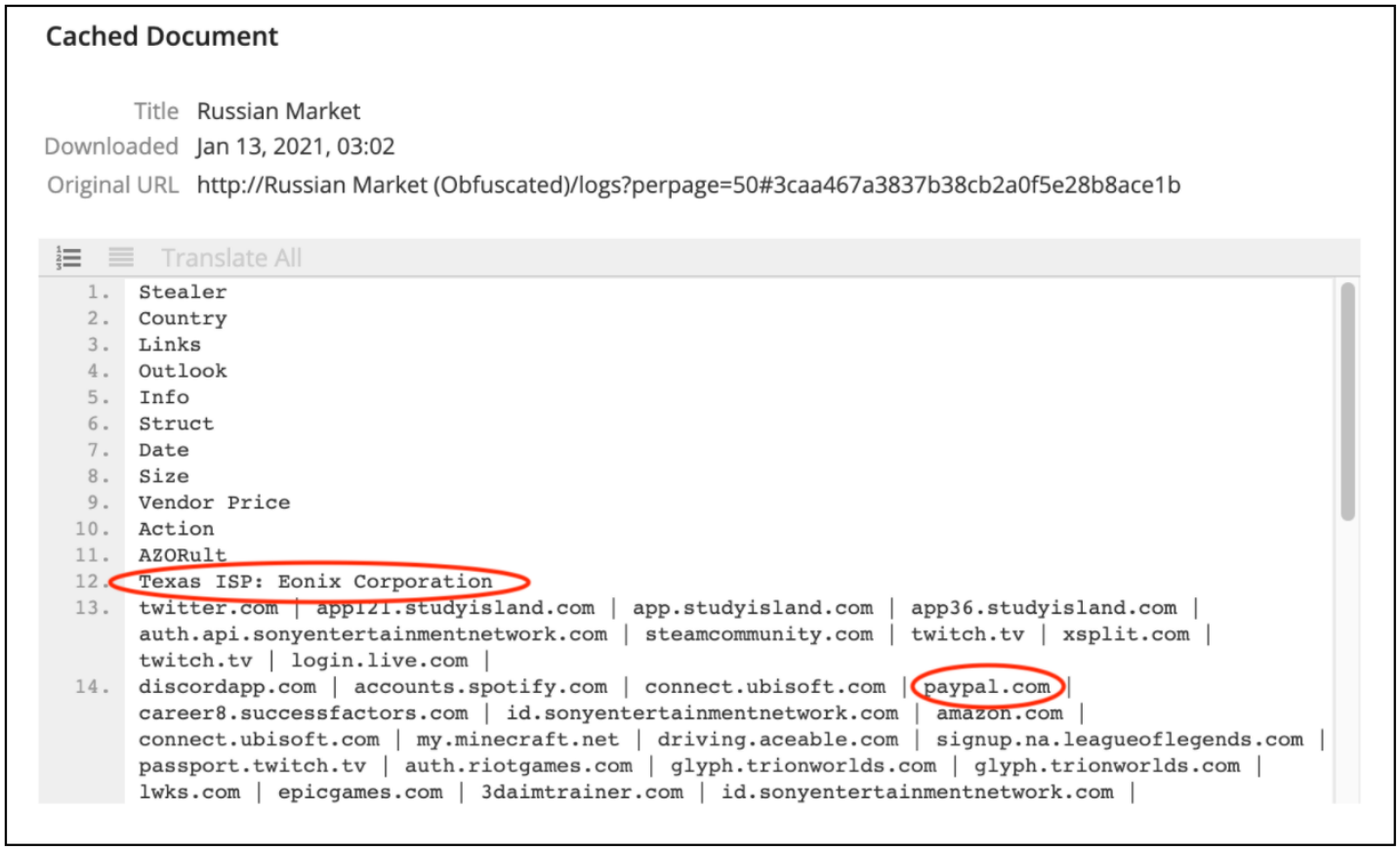


Image: Recorded Future cached information for a Russian Market reference associated with a Stealer Log advertisement, showing that the compromised information is associated with the alerted domain of interest. Additional information on the ISP may be worthwhile to review as well to determine if the ad is linked to an enterprise system.

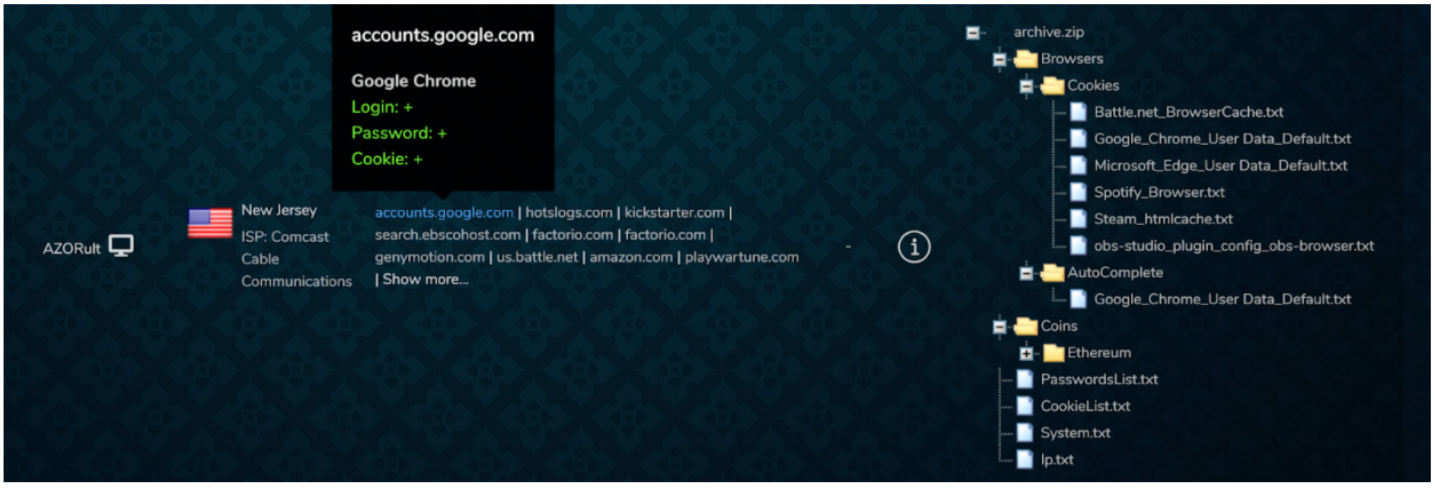


Image: What the cached Stealer Logs information in Recorded Future looks like on Russian Market. Note that this is a screenshot of a different listing being sold than the one in the

Recorded Future screenshot. Information tied to the Google account in this example includes login, password, and cookie information.

3.2. Your company IP address is mentioned in a listing

- Does your company own IP addresses within that address space?
- Are both company domains and company-owned IP addresses included in the same listing?
- What timestamps are shown in the listing? This can be a good data point when trying to identify an internal compromised machine at a later stage.

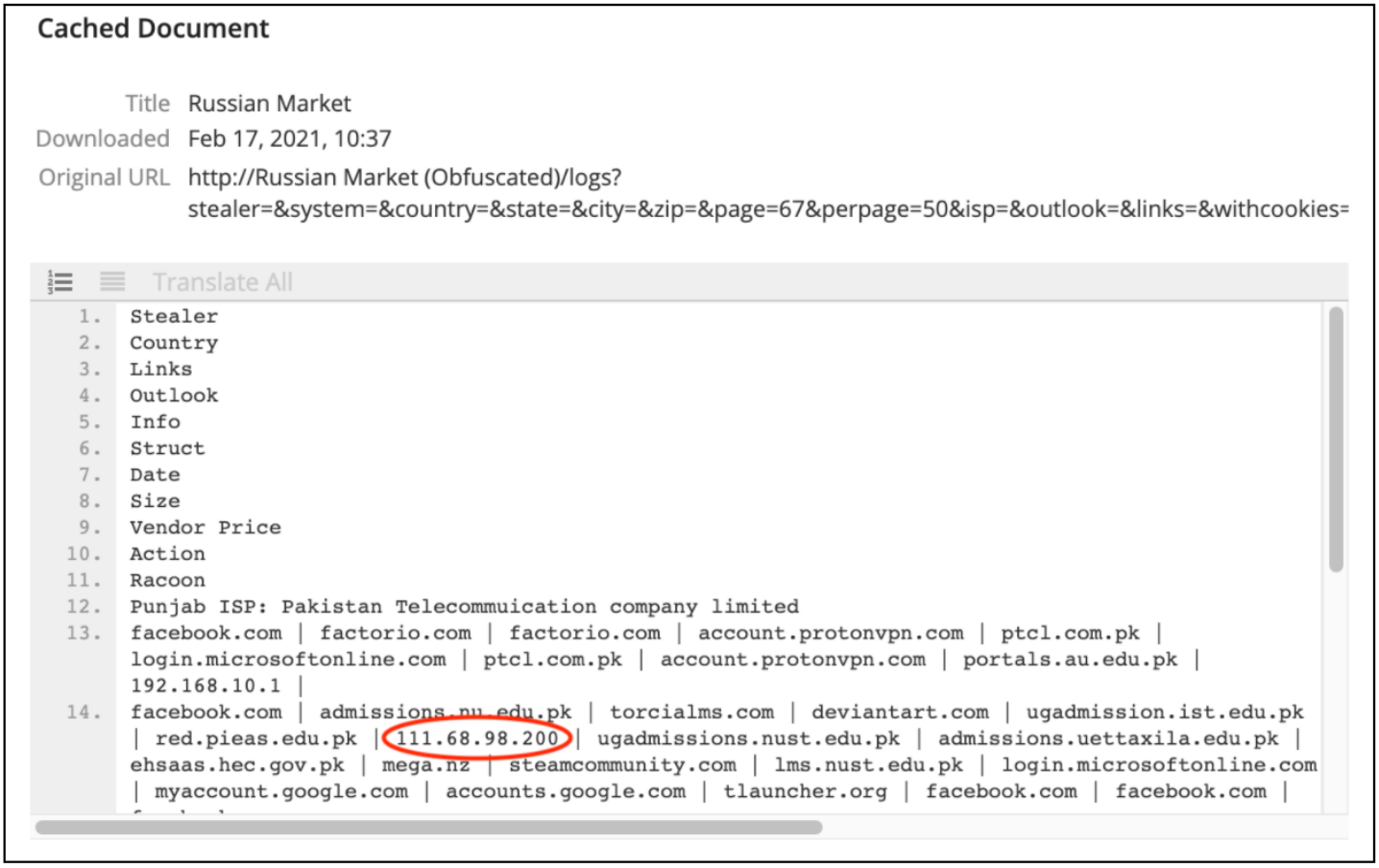


Image: Example of company IP address alert originating from a Russian Market Stealer Logs advertisement.

3.3. Strain of Stealer Malware Linked to Advertisement

- What variant of stealer malware was used to target company data?
- Are detections in place internally to monitor for that variant?

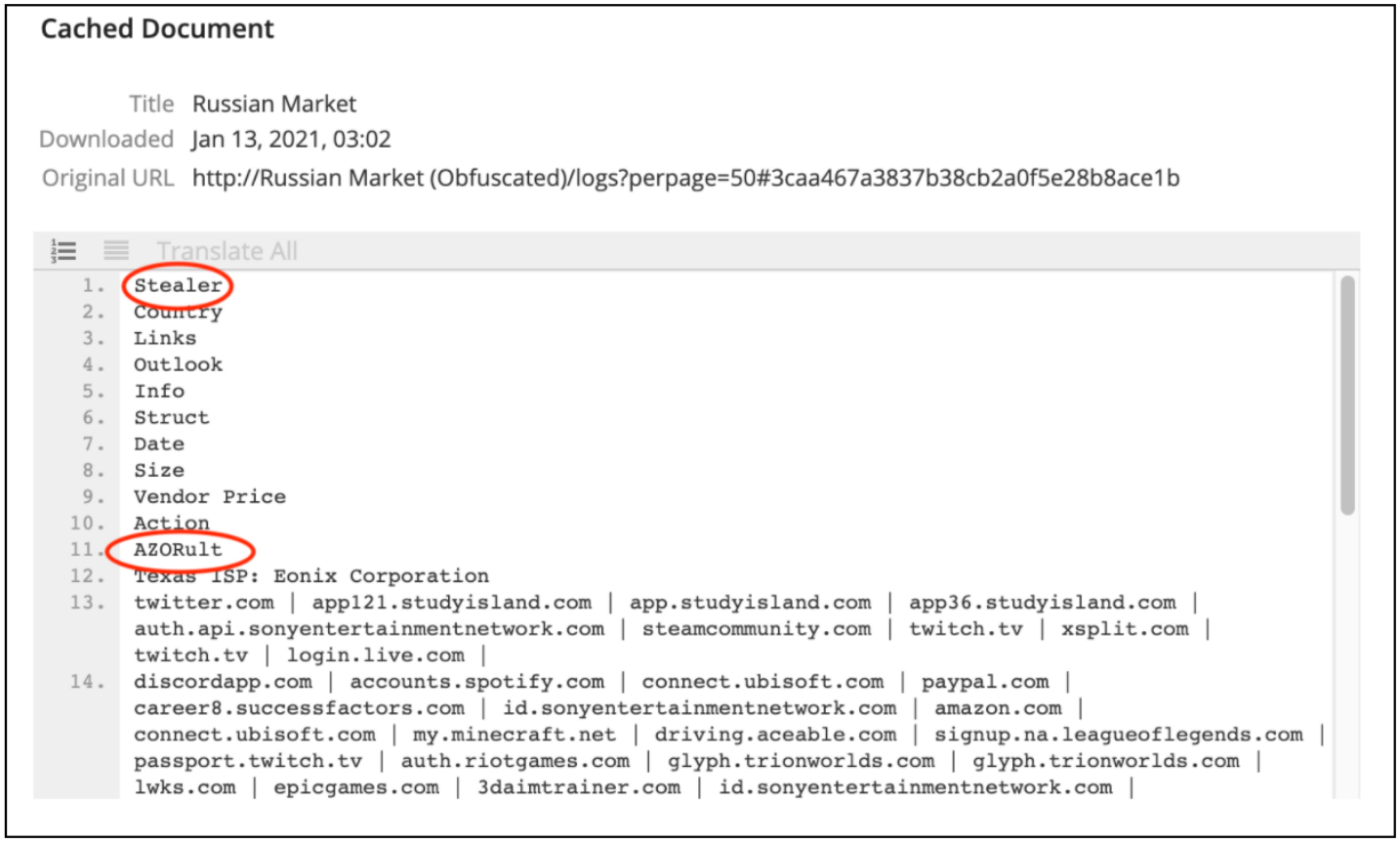


Image: Recorded Future cached information for a Russian Market reference associated with a Stealer Log advertisement, showing that the stealer variant of malware used to exfiltrate the information was AZORult.

3.4. Your company data (listed under “archive[.]zip”)

- What information is being given for that customer domain?
- What information is listed as having been exfiltrated?
- What web browser was the information stolen from?
- Are there references to Operating Systems that align with those used by your company?

Tip: use Ctrl+F to find where your company domain is mentioned.

Cached Document

Title Russian Market
Downloaded Jan 13, 2021, 03:02
Original URL http://Russian Market (Obfuscated)/logs?perpage=50#3caa467a3837b38cb2a0f5e28b8ace1b

Translate All

```
15. Show more...
16. -
17. archive.zip
18. var dirList819637 = [
19. {name: "archive.zip", iconSkin: "pIcon01", children: [ {name: "Browsers", children: [ {name:
    "Cookies",
20. children: [ {name: "AVAST Software Browser_User Data_Default.txt"}, {name:
    "Microsoft_Edge_User Data_Default.txt"}, {name: "Steam_htmlcache.txt"} ]}, {name:
    "AutoComplete",
21. children: [ {name: "Microsoft_Edge_User Data_Default.txt"} ]} ]},
22. {name: "PasswordsList.txt"}, {name: "CookieList.txt"}, {name: "System.txt"}, {name: "Ip.txt"}
    ]}
23. ];
24. $(document).ready(function () {
25. $.fn.zTree.init($("#treeLog819637"), false, dirList819637);
26. });
27. 2020.12.31 0.13Mb
28. nn####an[platinum]
29. $ 11.00
30. Buy Russian Market.
```

Image: What the cached browsing information in Recorded Future looks like in Russian Market. Note that this information is associated with the same advertisement visualized in Step 3.2. This shows that the compromised information for the infected system includes user data and the web browser Microsoft Edge.

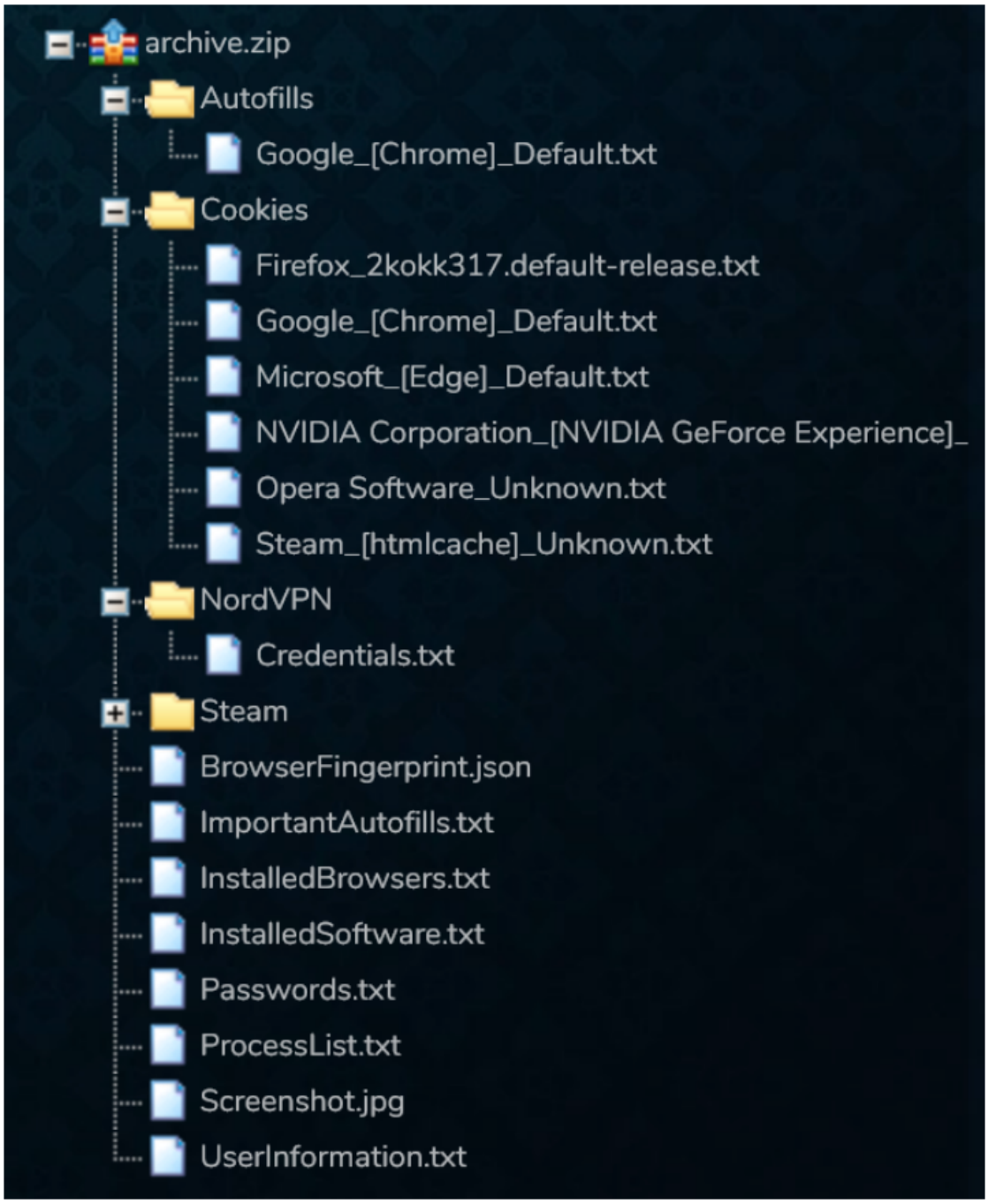


Image: Example breakdown of an archive[.]zip file within a Russian Market ad. This is a different file from the event used in previous examples.

Information purchased from this section is delivered via a ZIP file named archive[.]zip that comes with information associated with a victim's financial, social media, email, and other online accounts. The sample breakdown of information contained within the ZIP file within the

Recorded Future cache is what threat actors are able to preview before deciding whether they want to purchase the information.

3.5. Other resources included with the listing

- What timestamps are associated with the account for your domain?
- Are other common websites and domains included in the listing's resources that your company's users would be expected to access during work hours (e.g., your webex solution and your email provider)?

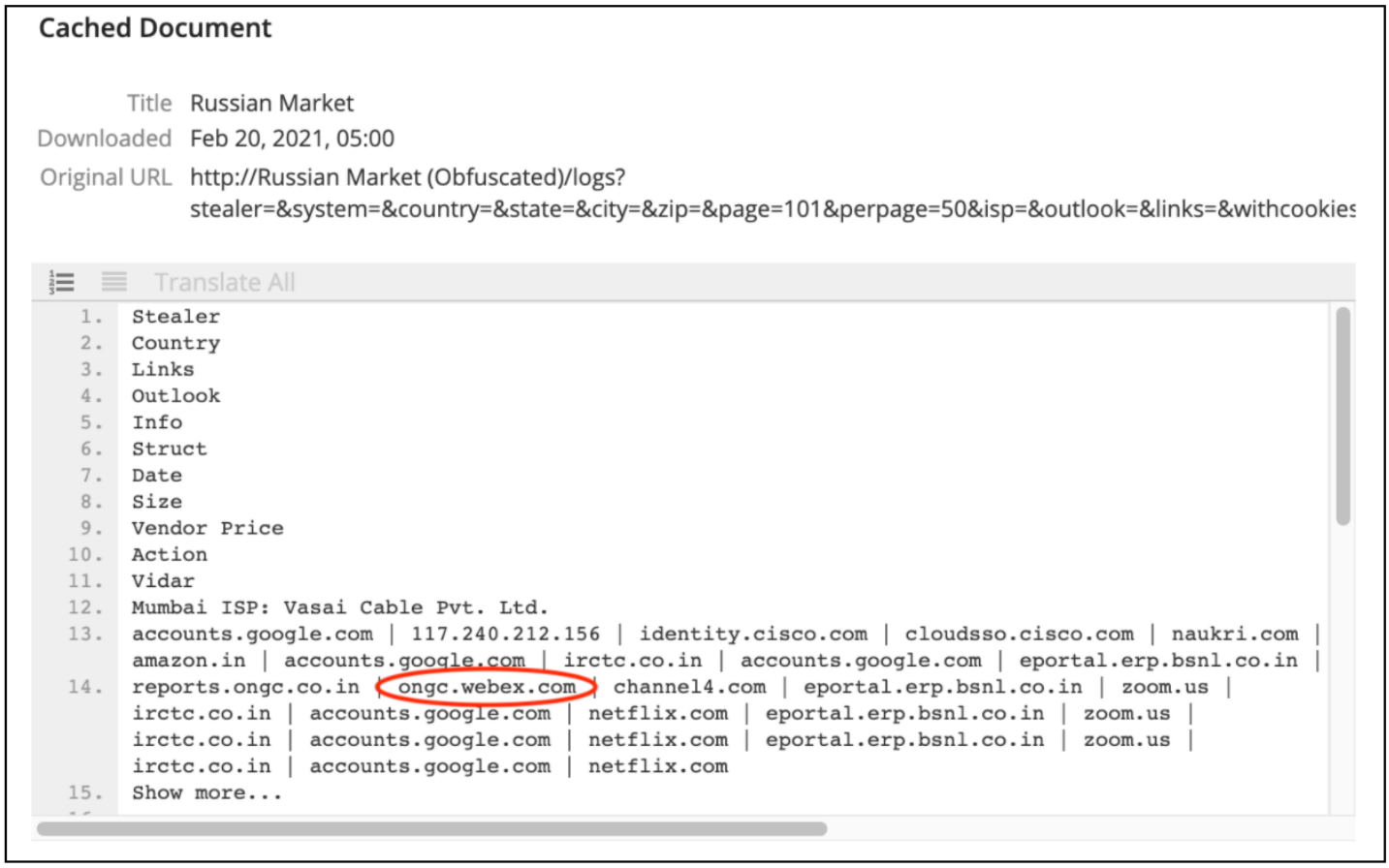


Image: Websites and domains included in the listing's resources that your company's users would be expected to access during work hours can provide valuable context (e.g., a webex solution as seen in the visual above)

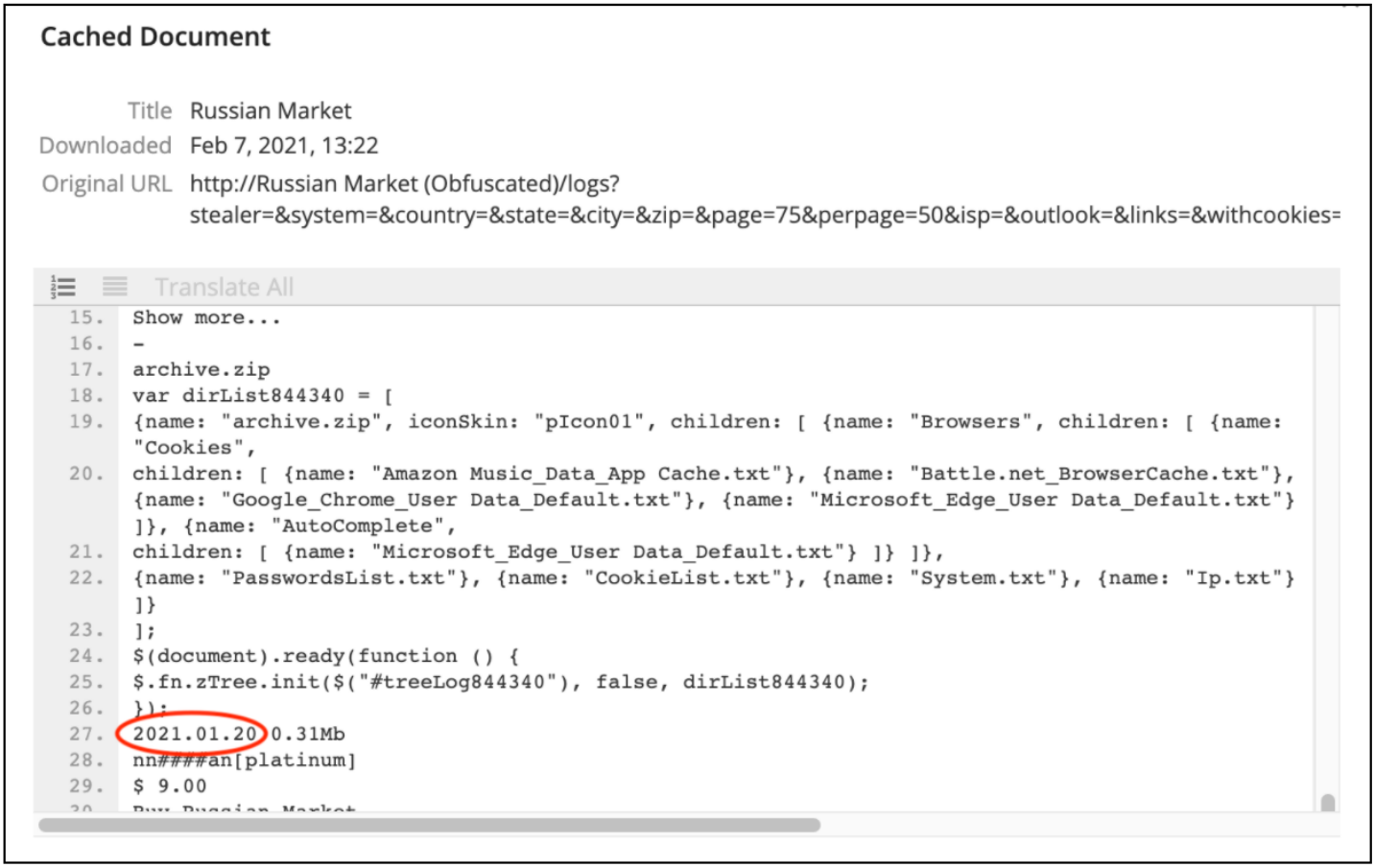


Image: The date when the details were uploaded to Russian Market is highlighted and can be a useful reference if a malware infection is tied to the same stealer mentioned in the alerted advertisement.

Step 4

Based on the above information, assess whether the information being sold on Russian Market that mentions your company domain is from an internal compromised host machine or an external customer machine.

Is the company domain listed with the bot an internal domain? *Yes / No*

Does your company own IPs within the address space?	*Yes / No*
Do any of your company devices use any of the applications listed (especially if it's an enterprise OS that is listed)?	*Yes / No*
Are the browsers associated with the bot permitted on company devices?	*Yes / No*
Does the variant of stealer malware align with any recent detections observed impacting company systems?	*Yes / No*
Does the bot list any resources that would commonly be accessed by your company's employees?	*Yes / No*

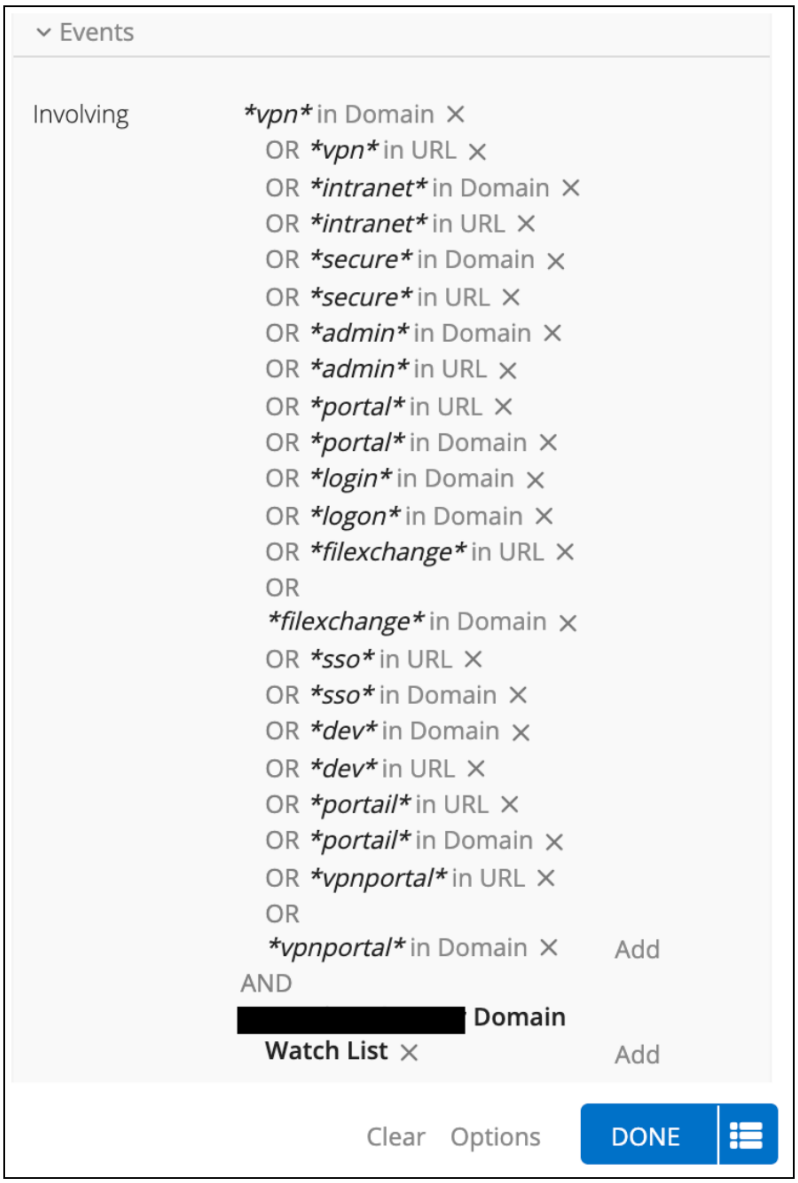
Step 5

If suspected internal…

- Try to identify the compromised machine based on the information you collected.
- Set up alerts and monitoring for internal hosts and for any hosts surrounding users in the same working group or subnet.
- Use Insikt Group's YARA rules to help detect the variants of malware used to infect systems for sale on Russian Market's Stealer Logs section. YARA rules are present within the Recorded Future Platform for the following malware families:
    - Recorded Future YARA Rule for Racoon Stealer
    - Recorded Future YARA Rule for AZORult
- Consider using Recorded Future's Analyst on Demand service to purchase the bots from Russian Market as soon as they become available. Once a bot is sold on Russian Market, the information is removed from the site and any updates the victim makes to the account are also likely captured by Russian Market admins.

If suspected external...

- Pass the above information to your internal fraud unit so that they can monitor account activity and try to identify the affected victim.
- If you aren't concerned about external/customer compromises or are getting too many Russian Market alerts, and if you have an Advanced User or Threat Intelligence Module License, consider excluding Russian Market from the 'Your domains on Dark Web and closed sources' Intelligence Goal. Instead, create a new alerting rule explicitly for Russian Market, cross-referencing your Domains Watch List with terms like 'vpn', 'internal', 'sso', 'portal', etc. For example, the image below is based on this query.



Have more questions regarding this topic: Submit a request

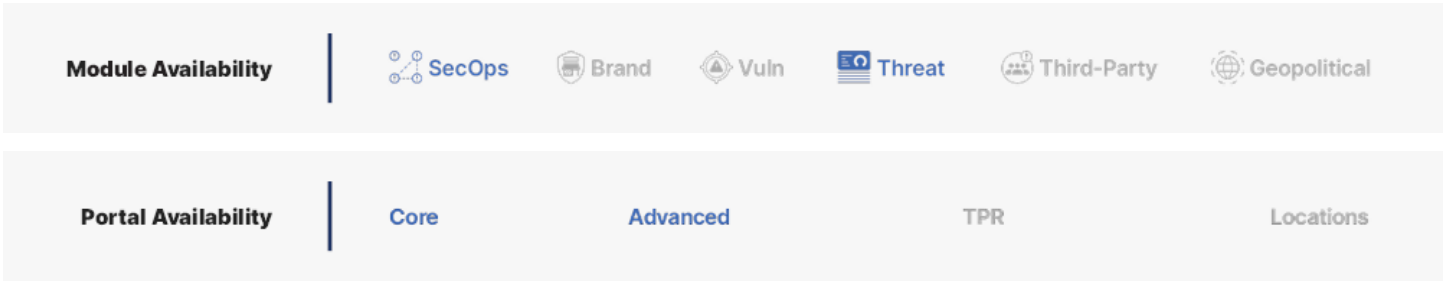
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Investigate a Suspicious Email Attachment

PLAYBOOK

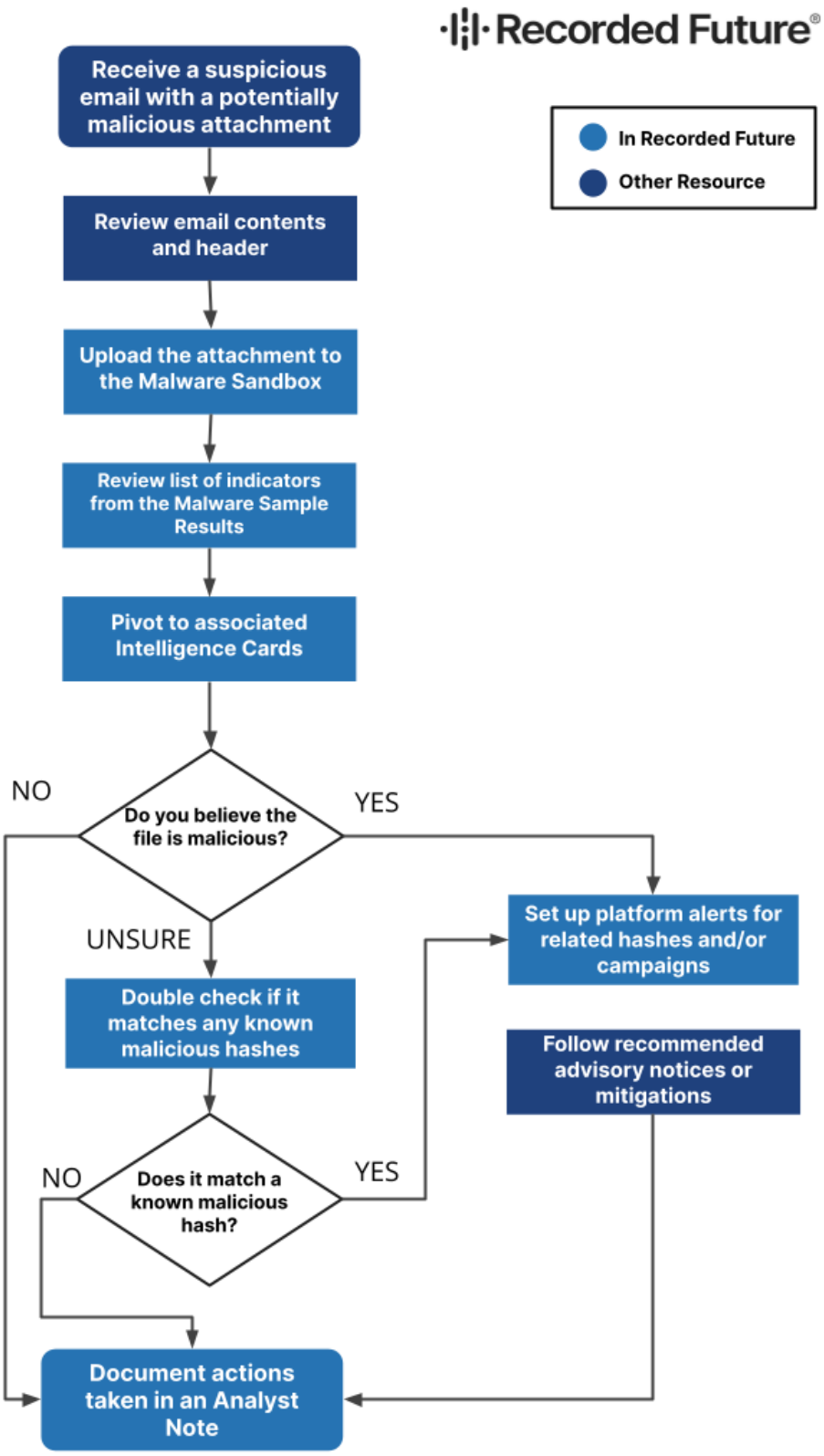
1st edition

Investigate a Suspicious Email Attachment Playbook



A Core, Advanced, or Threat Intelligence seat is required to complete all steps in this playbook. The Malware Sandbox is available for SecOps Intelligence users, but we recommend that you work with your Intelligence Services team to develop a playbook using your preferred integration.

This Recorded Future playbook will walk you through triaging a suspicious email attachment from start to finish using the Malware Sandbox and other Recorded Future product features. Refer to the rubric in Assessing a Potential Phishing Email to help determine whether an email is suspicious.


Recorded Future
In Recorded Future
Other Resource
Receive a suspicious email with a potentially malicious attachment
Review email contents and header
Upload the attachment to the Malware Sandbox
Review list of indicators from the Malware Sample Results
Pivot to associated Intelligence Cards
Do you believe the file is malicious?
NO
YES
UNSURE
Double check if it matches any known malicious hashes
Does it match a known malicious hash?
NO
YES
Set up platform alerts for related hashes and/or campaigns
Follow recommended advisory notices or mitigations
Document actions taken in an Analyst Note

Start

You receive a suspicious email with a potentially malicious attachment.

Firstly, DO NOT OPEN THE ATTACHMENT. Generally, do not open attachments from unknown senders or unexpected attachments from known senders.

Step 1

If you have not already, implement security controls, such as endpoint security, to automatically block malicious file hashes on endpoints using Recorded Future data.

Step 2

Review the email contents and header; use the Assessing a Potential Phishing Email Playbook to learn more about the sender and begin your investigation of the attachment.

Step 3

Upload the suspicious attachment into the Malware Analysis sandbox. After the results process, access the report to see what we found.

- Look at the list of indicators collected in the Malware analysis report
- Pivot to Intelligence Cards for the associated IOCs for context to understand more about the threat
- Follow the recommended advisory notices or mitigations, if any

Step 4

Do you believe that the attached file is malicious?

- If YES - Set up platform alerts related to malicious file hashes for specific, related phishing campaigns or a related recent attack. Follow the recommended advisory notices or mitigations, if any.

- If UNSURE - Check against known malicious hashes in the Recorded Future platform via a search. Confirm that it does not match known malicious hashes.
    - If the hash matches a known value in Recorded Future, review the Intelligence Card to learn more about the threat. Follow the recommended advisory notices or mitigations, if any.
    - Set up platform alerts related to any suspicious domains, URLs, etc. you identified.

- If NO - If it is a known sender, get in touch with the sender through a different communication method and check whether they meant to send you this file. Continue onward.

Step 5

Detail the actions you have taken and information you have found in an Analyst Note to share within your enterprise and capture what you learned.

Additional Mitigations

- If possible, block the ability for executable files to be sent over email unless there is a specific use case.
- Use Recorded Future's API to automate phishing detection by pulling feeds for domains, IPs, hashes, and URLs into your SIEM to correlate between RF feeds and email artifacts from your email gateway or email server. You can then have it trigger an alert to your analyst.
- Search for potential malicious email attachments that have gotten through using the techniques outlined in Hunting for malicious email attachments.

Have more questions regarding this topic: Submit a request

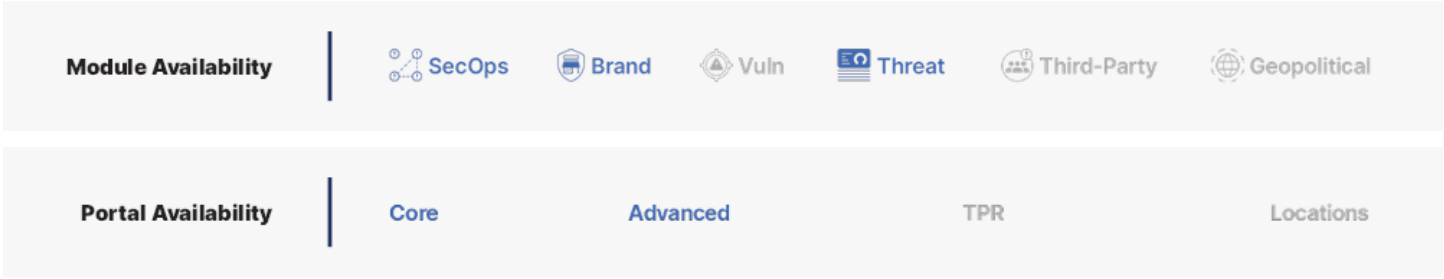
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Assessing a Potential Phishing Email

PLAYBOOK

1st edition

Assessing a Potential Phishing Email Playbook

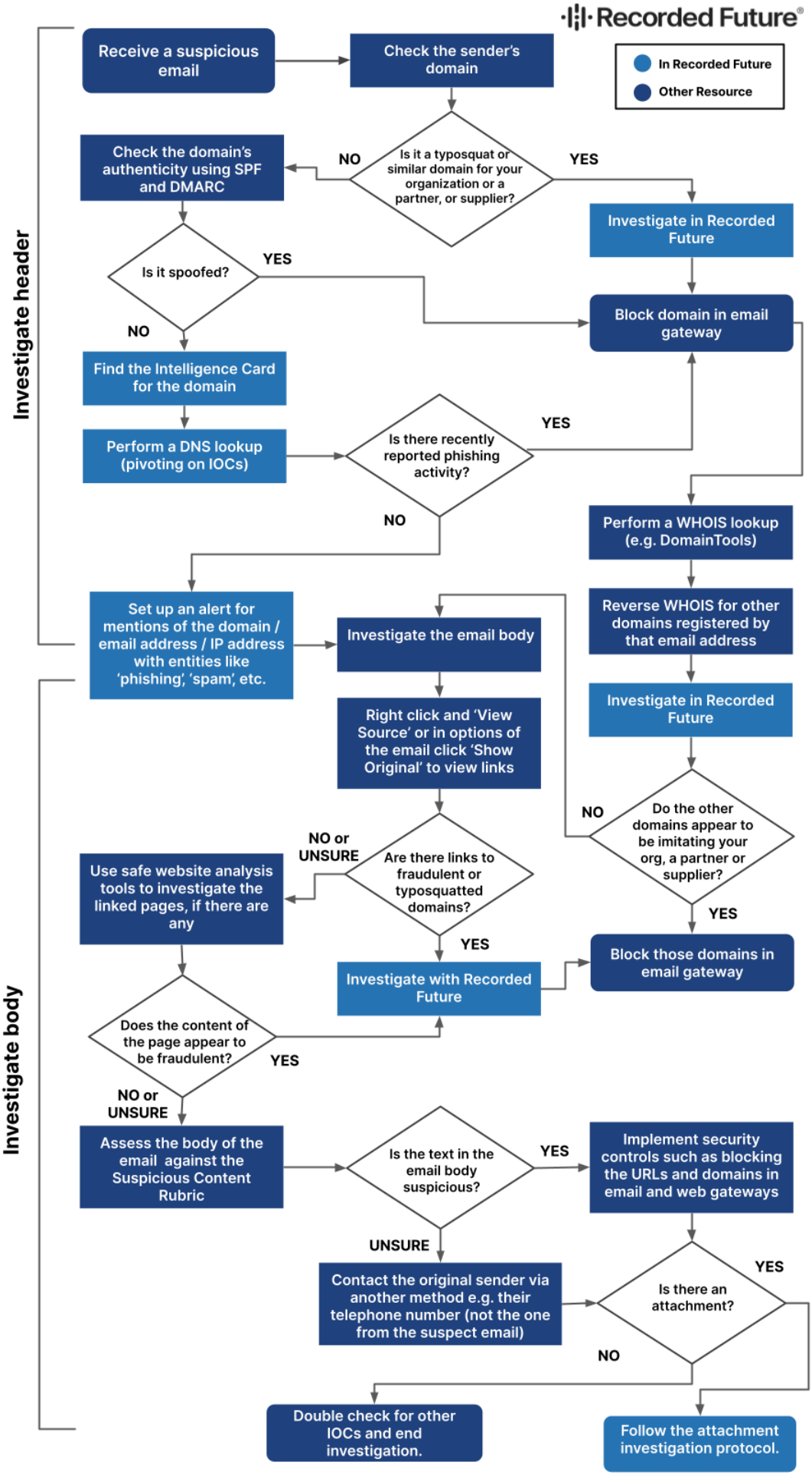


This Recorded Future playbook will help walk you through triaging a suspicious email from start to finish. In addition to the steps below, make the following mitigations a regular part of your security practices:

Background Mitigations

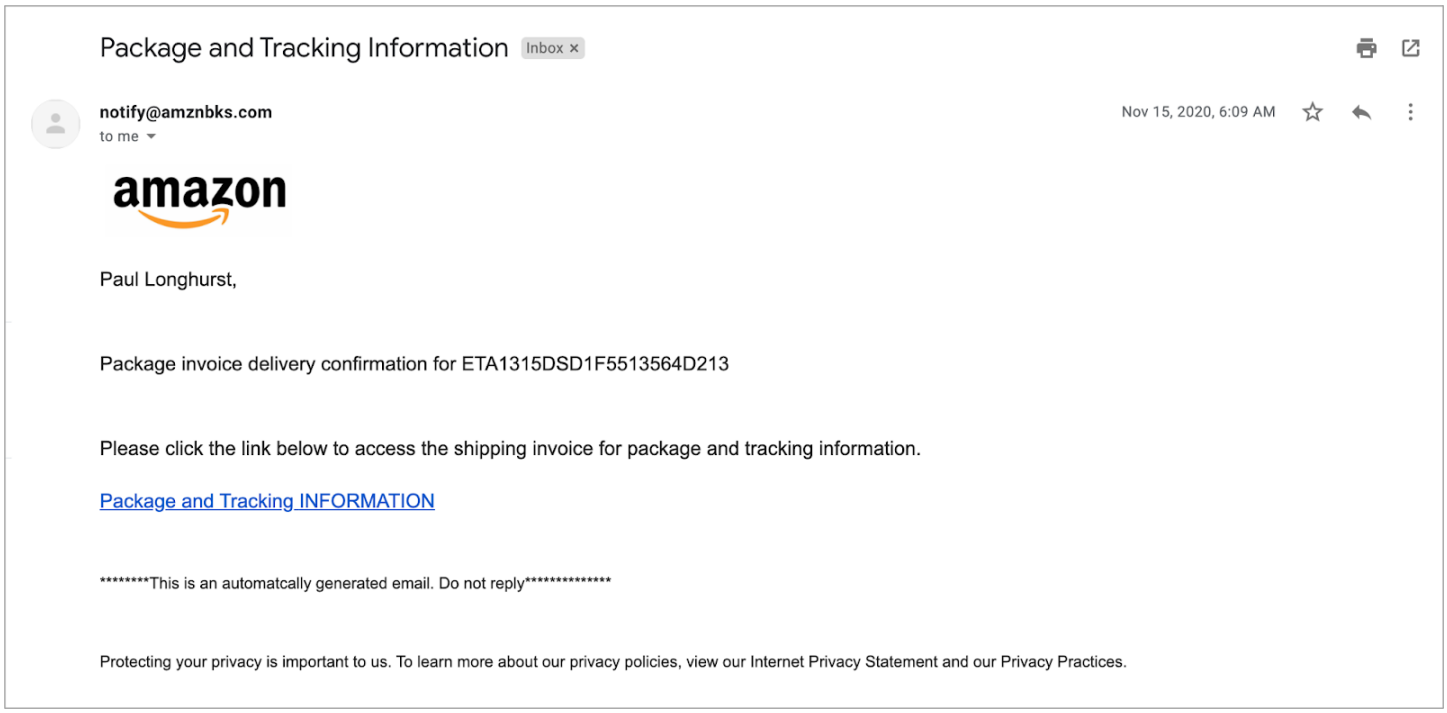
- Use Recorded Future's Security Control Feeds to block malicious domains, IPs, and URLs in your mail server
- Run a user awareness training and simulations to help employees identify phishing emails in advance
- Subscribe to regular updates in trends from National agencies - CISA in the USA, NCSC in the UK, and others
- You can also use Recorded Future's API to automate phishing detection: pull feeds for domains, IPs, hashes, and URLs to your SIEM to correlate between RF feeds and email artifacts from your email gateway or your email server. With this automation, you may not need this playbook very often!

PROTIP: If you have the Recorded Future Browser Extension enabled over your web-based email, it can automatically identify the IOCs within and provide instant Risk Scores. From there, you can quickly pivot to the Recorded Future portal to continue your investigation. If enabled, the extension can also automatically block malicious links.

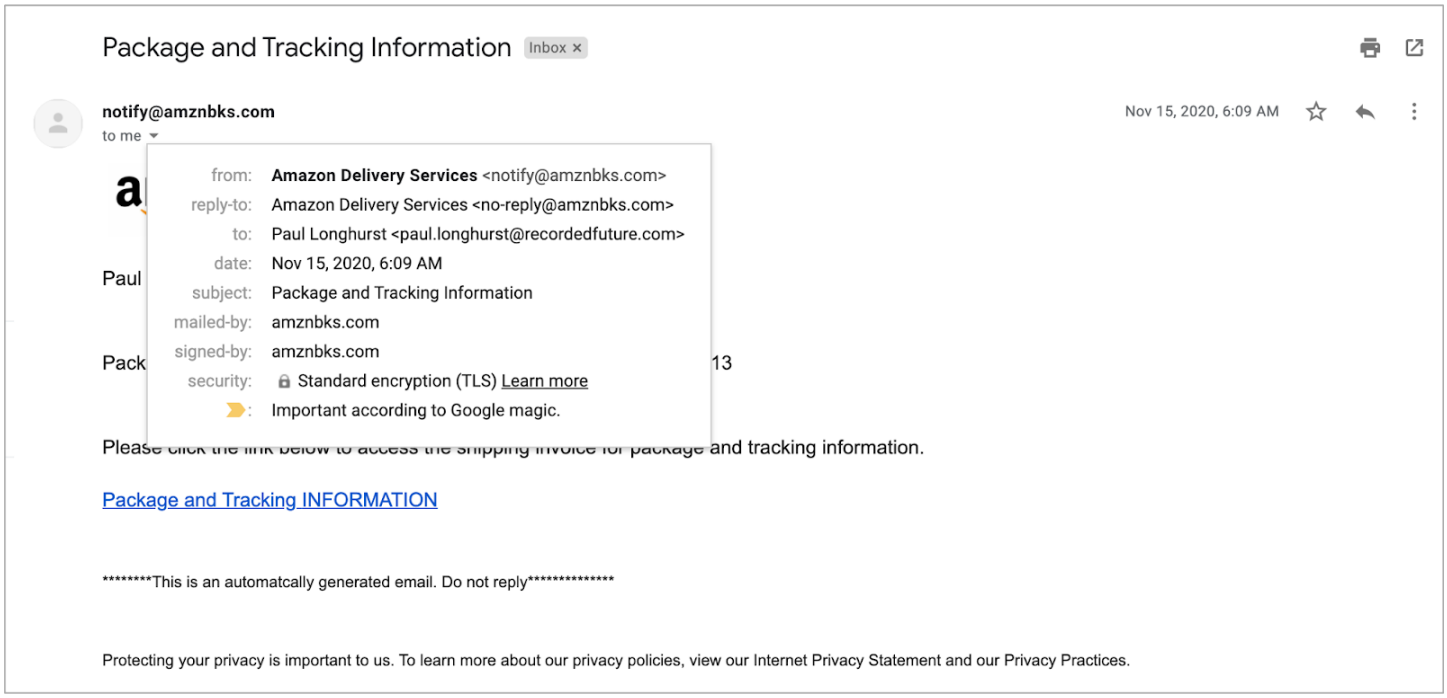

Recorded Future
In Recorded Future
Other Resource
Investigate header
Receive a suspicious email
Check the sender's domain
Is it a typosquat or similar domain for your organization or a partner, or supplier?
NO
YES
Check the domain's authenticity using SPF and DMARC
Investigate in Recorded Future
Is it spoofed?
YES
NO
Block domain in email gateway
Find the Intelligence Card for the domain
Perform a DNS lookup (pivoting on IOCs)
Is there recently reported phishing activity?
YES
NO
Perform a WHOIS lookup (e.g. DomainTools)
Reverse WHOIS for other domains registered by that email address
Investigate in Recorded Future
Do the other domains appear to be imitating your org, a partner or supplier?
NO
YES
Block those domains in email gateway
Set up an alert for mentions of the domain / email address / IP address with entities like 'phishing', 'spam', etc.
Investigate the email body
Right click and 'View Source' or in options of the email click 'Show Original' to view links
Investigate body
Are there links to fraudulent or typosquatted domains?
NO or UNSURE
YES
Use safe website analysis tools to investigate the linked pages, if there are any
Investigate with Recorded Future
Does the content of the page appear to be fraudulent?
YES
NO or UNSURE
Assess the body of the email against the Suspicious Content Rubric
Is the text in the email body suspicious?
YES
UNSURE
Implement security controls such as blocking the URLs and domains in email and web gateways
Contact the original sender via another method e.g. their telephone number (not the one from the suspect email)
Is there an attachment?
YES
NO
Double check for other IOCs and end investigation.
Follow the attachment investigation protocol.

Start

You receive a suspicious email either in your inbox or forwarded to you for investigation. Example:



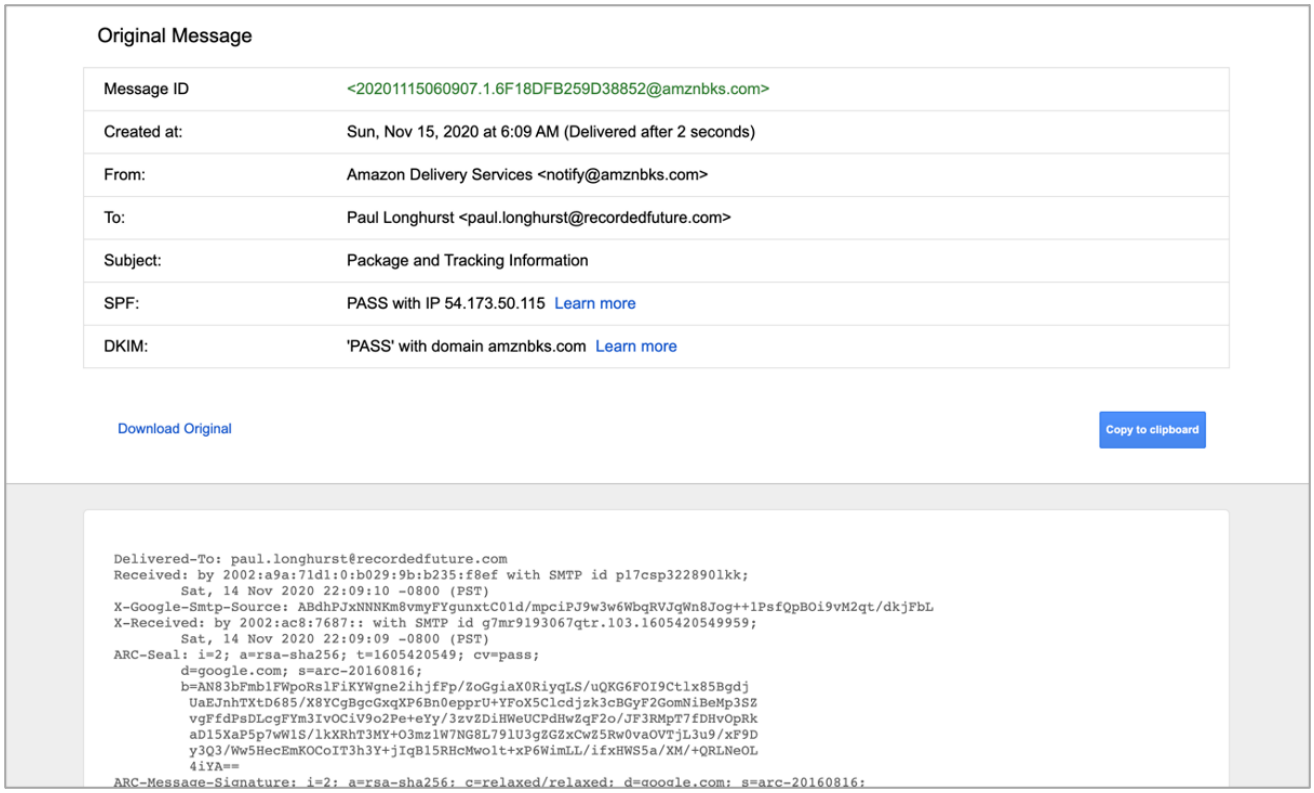
Phase A: Investigate the Header



Step 1

Check the sender's domain.

- Does the domain appear to be impersonating your company, your suppliers, or your partners?
    - If YES → Block the domain in your email gateway. Investigate using steps outlined in the Fraudulent Domains and Typosquats playbook and continue onward.
    - If NO → Continue onward.
- Check the sender's domain authenticity using SPF and DMARC.



- Does it appear to be inauthentic or impersonating another organization?

    - If YES → Block the domain in your email gateway. Continue your investigation.

    - If NO, continue your investigation.

Step 2

Gather additional context around the sender's domain using the Domain Intelligence Card in the Recorded Future.

- Check the Risk Score, triggered Risk Rules, and recent references.

- Perform a DNS Lookup to identify the corresponding IP address. From there, you can investigate the IP address's Risk Score, triggered Risk Rules, and recent references, checking for indicators of phishing activity.

- Perform a WHOIS lookup of the domain (e.g. DomainTools) to identify registrant information.

  To find a unique email address with your WHOIS lookup, perform a reverse WHOIS lookup to find other domains registered by that email address, and expand your investigation to investigate whether any related domains are spoofing a legitimate domain.

    - YES, information suggests that this email is part of a phishing campaign → Take steps to block the related malicious domains and IPs.

    - If NO, there are not any malicious associations → Set up an alert in Recorded Future for any mentions of the relevant domain / email address / IP address with entities like 'phishing', 'spam', etc.

You can perform similar steps investigating the sender's IP address using IP Intelligence Cards in the platform, looking at the triggered Risk Rules, and checking the context section for associations with malware and/or other IPs and domains.

Phase B: Investigate the Body

Step 3

Look for links in the email. Right-click on the body of the email and click 'View Source' or click in the options of the email and choose 'Show Original' to view links in the email without needing to hover over them.

Do not click on any suspicious URL on a production machine.

- Do any of the URLs appear to be obvious typosquats or fraudulent domains?
    - If YES → Investigate in Recorded Future, find related URLs, domains, and IPs as you may have done above for the sender.
    - If NO → Continue on.

Step 4

Compare the email text against our Suspicious Content Rubric.

Social Engineering - Is it asking for money, data, or otherwise making a request?	Yes / No
Writing Quality - Are there typos or grammatical mistakes?	Yes / No
Brand Alignment - If there are images, are they correctly correlated to the brand they are purporting to be?	Yes / No
Authority - Is it claiming to be someone in a position of authority asking you to do something?	Yes / No

Urgency - Is the text trying to rush or pressure you?	Yes / No
Emotion - Is the text trying to persuade you to follow-up, be fearful of consequences, or hopeful of benefit?	Yes / No
Scarcity - Is the message offering something in short supply or something valuable at “better than good” prices?	Yes / No
Current Events - Are you expecting to see a message on this theme? Could malicious actors be using big news stories or routine events at the time of year (e.g. tax reporting)?	Yes / No

Based on the above rubric, do you believe the email is suspicious?

- If YES, you believe the email could be malicious → Implement security controls against the sender’s email and domain, such as blocking them in your email and web gateways.
    - Additionally, detail the actions you have taken and information you have found in an Analyst Note to share within your enterprise and capture the progress you have made
- If MAYBE and you are still uncertain whether it is malicious → Get in touch with the original sender or organization that is attempting to contact you using their phone number, email address, or other communication method from a verified source.

Phase C: Check for attachments

Do not click to open any attachments! If you receive a suspicious email with an attachment, we recommend using the Malware Sandbox to assess it. An additional playbook on potentially malicious attachments is coming soon!

Note: You must have a Core or Advanced license or access to the Threat or SecOps Intelligence module to access the Malware Sandbox.

Have more questions regarding this topic: Submit a request

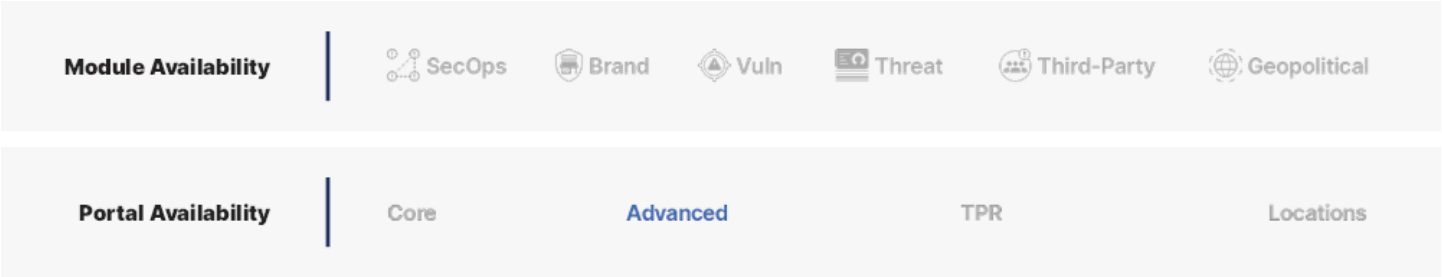
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Continuous Monitoring of Indicators

PLAYBOOK

1st edition

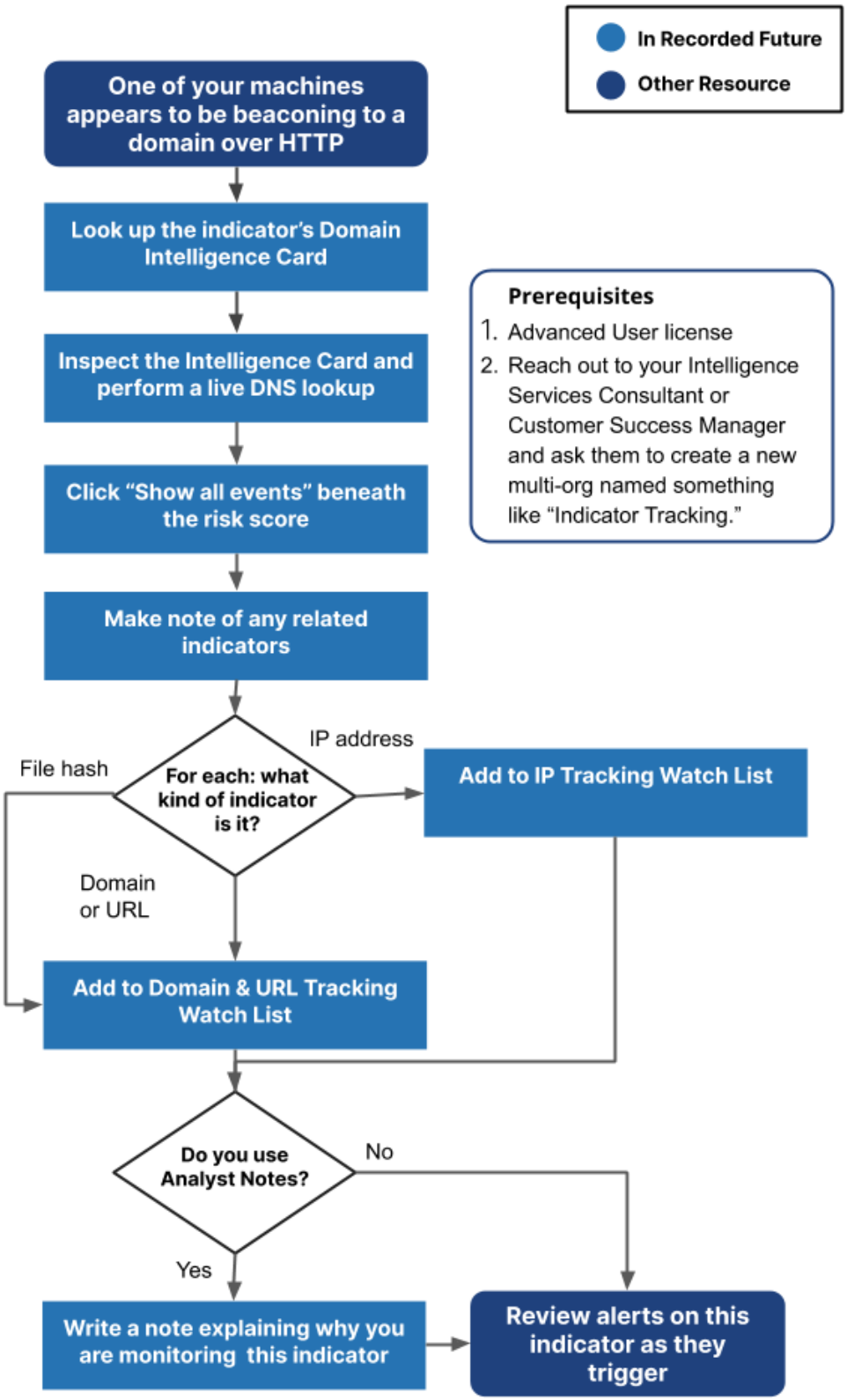
Continuous Monitoring of Indicators Playbook



This Recorded Future playbook walks you through setting up and executing continuous monitoring of indicators for risk score and references using the multi-org capability.

Continuous Monitoring of Indicators Playbook

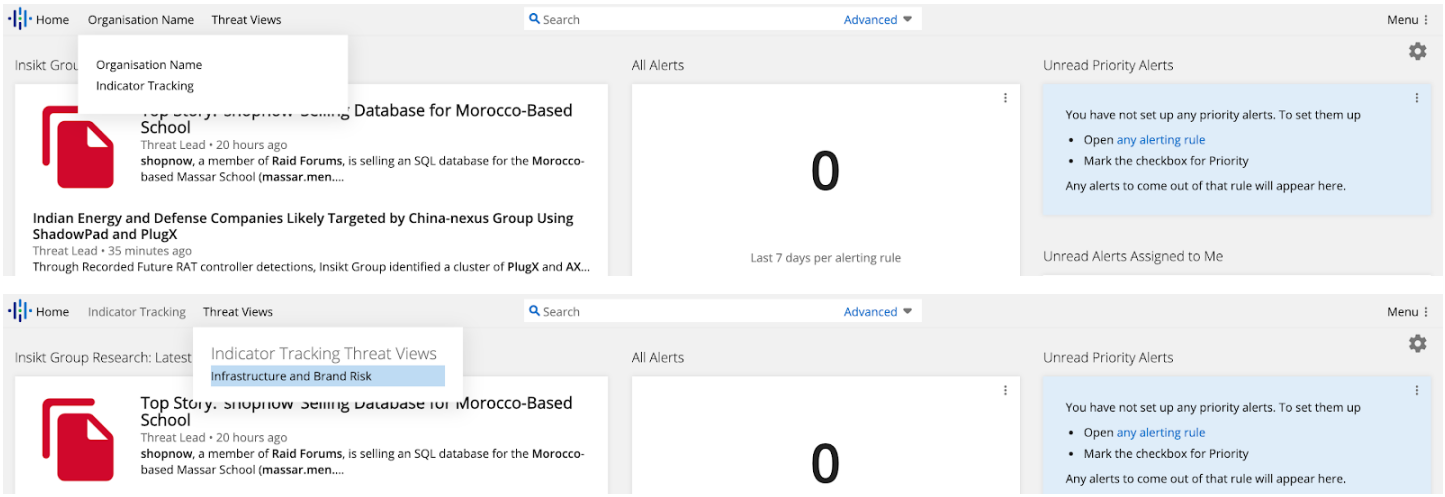
Recorded Future®



Key Prerequisites

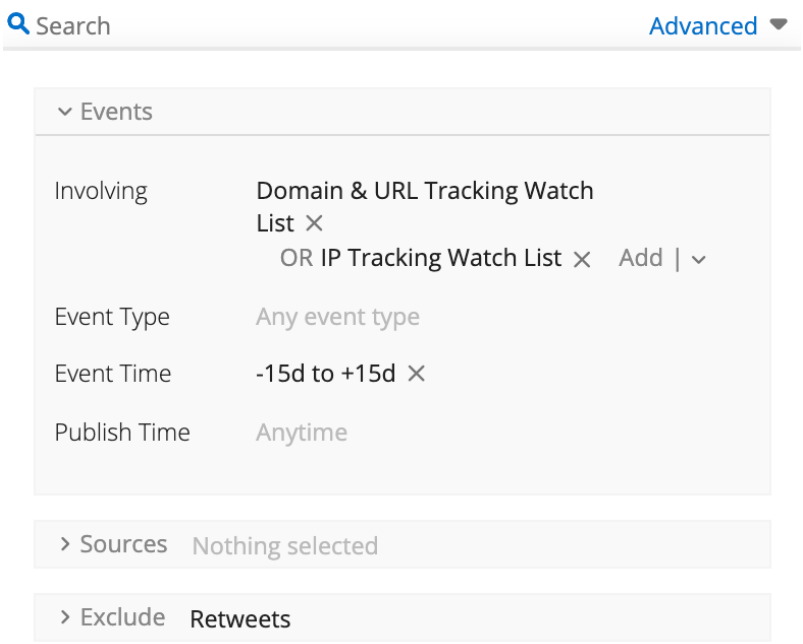
To use the features outlined in this playbook for the continuous monitoring of indicators, you will first need to reach out to your Intelligence Services Consultant or Customer Success Manager and ask them to create a new multi-org named something like “Indicator Tracking.”

Once that work is complete, you will notice a slight change to your Recorded Future enterprise. Next to the ‘Home’ button in the top right of your page, you will see your organization’s name. Click to see the available multi-org for ‘Indicator Tracking.’

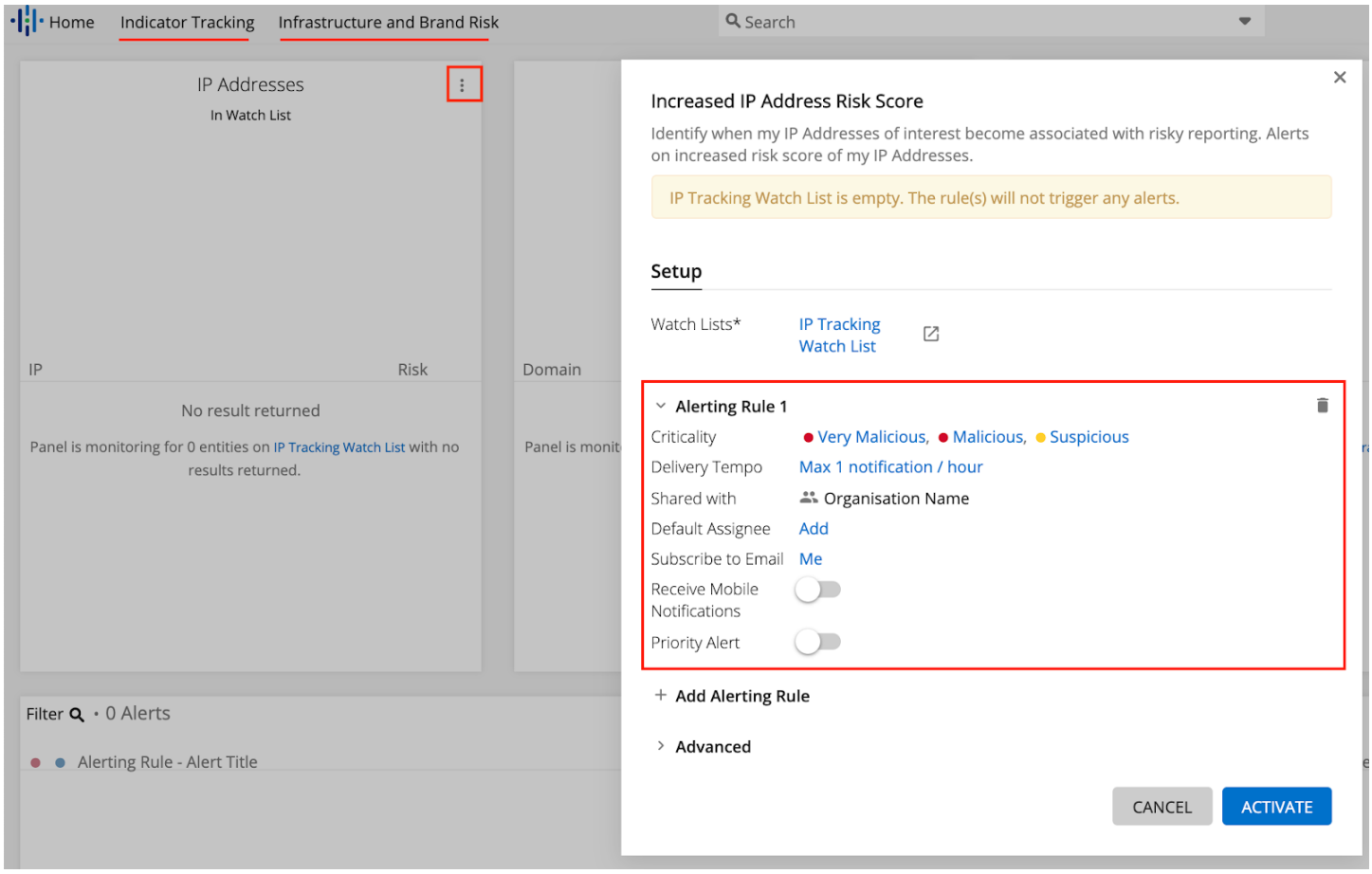


Some things to note about your new multi-org:

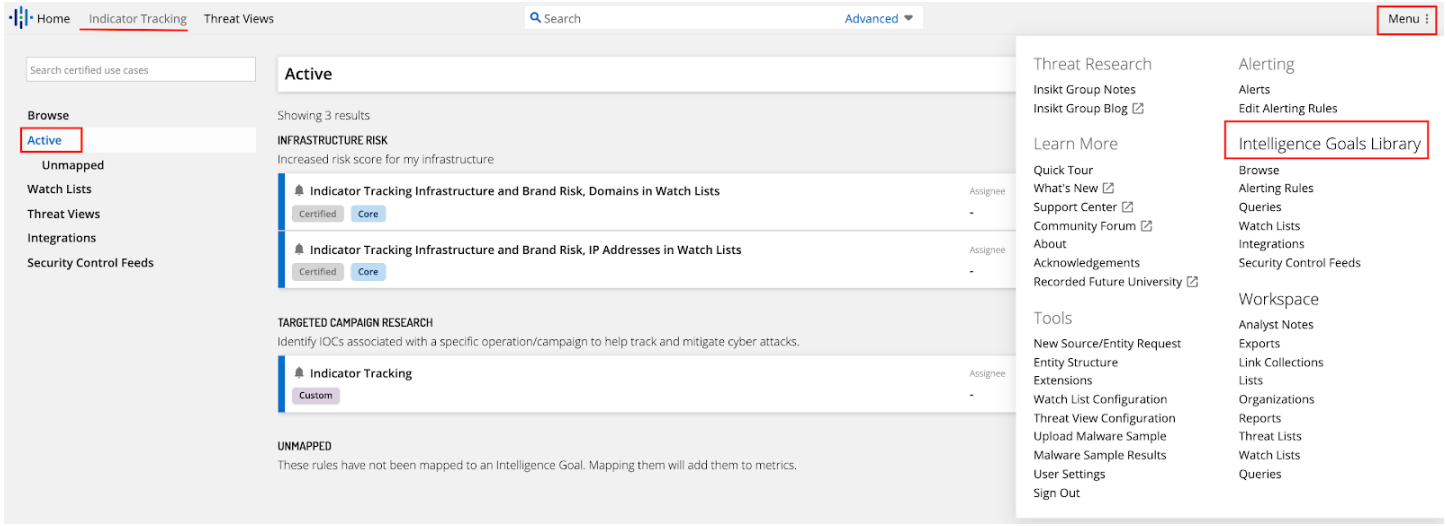
- Only the ‘Infrastructure & Brand Risk Threat View’ is enabled for that multi-org.
- You will have access to two new Watch Lists: (1) Domain & URL Tracking Watch List, and (2) IP Tracking Watch List.
- You will have a new alerting rule called ‘Indicator Tracking’ that searches for any references across all sources to your Domain & URL Tracking Watch List, and IP Tracking Watch List. (Example here.)



Finally, the new alerting rules will notify you any time an IP address, domain, or URL in the two Watch Lists reaches a risk score above 25.



Note: You can view the newly active alerting rules by selecting the 'Indicator Tracking' multi-org and navigating to Menu → Intelligence Goals Library → Active.



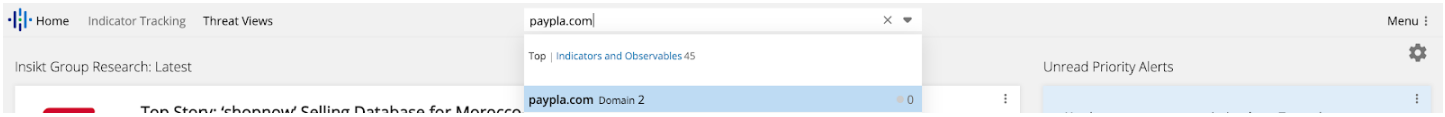
Start

In your logs, you notice that one of your corporate machines may be beaconing to a domain over HTTP. Proceed to Step 1.

Step 1

Lookup the indicator's Domain Intelligence Card.

Go to app.recordedfuture.com and type the indicator in the query search bar. Select the correct option to bring up the Intelligence Card.

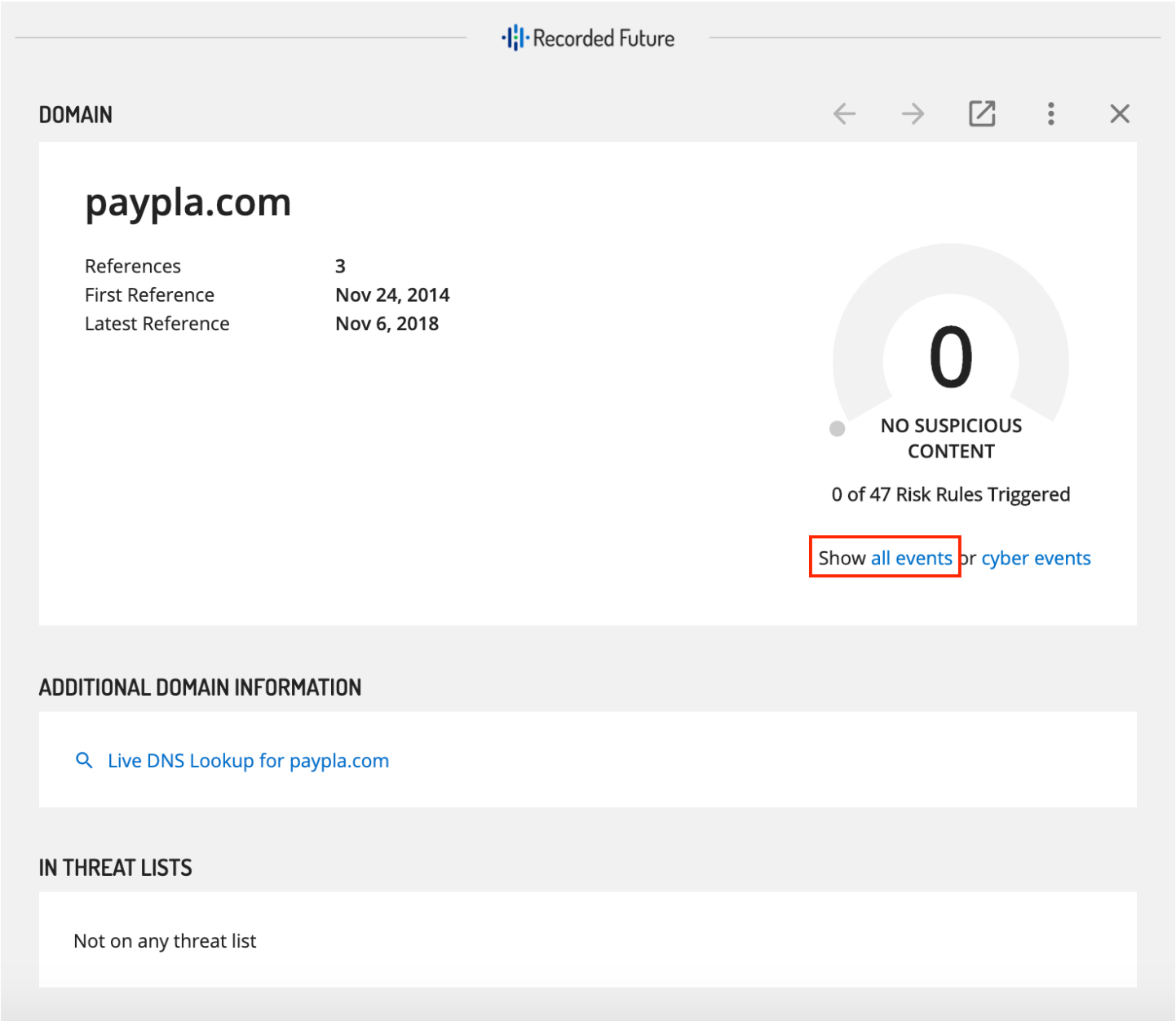


Step 2

Inspect the Intelligence Card.

Pay particular attention to the risk score and triggered risk rules, Insikt Group research, and the Context section. Since this is a Domain Intelligence Card, you can also perform a Live DNS Lookup.

Finally, click 'Show all events…' just below the risk score to search for references to that indicator.



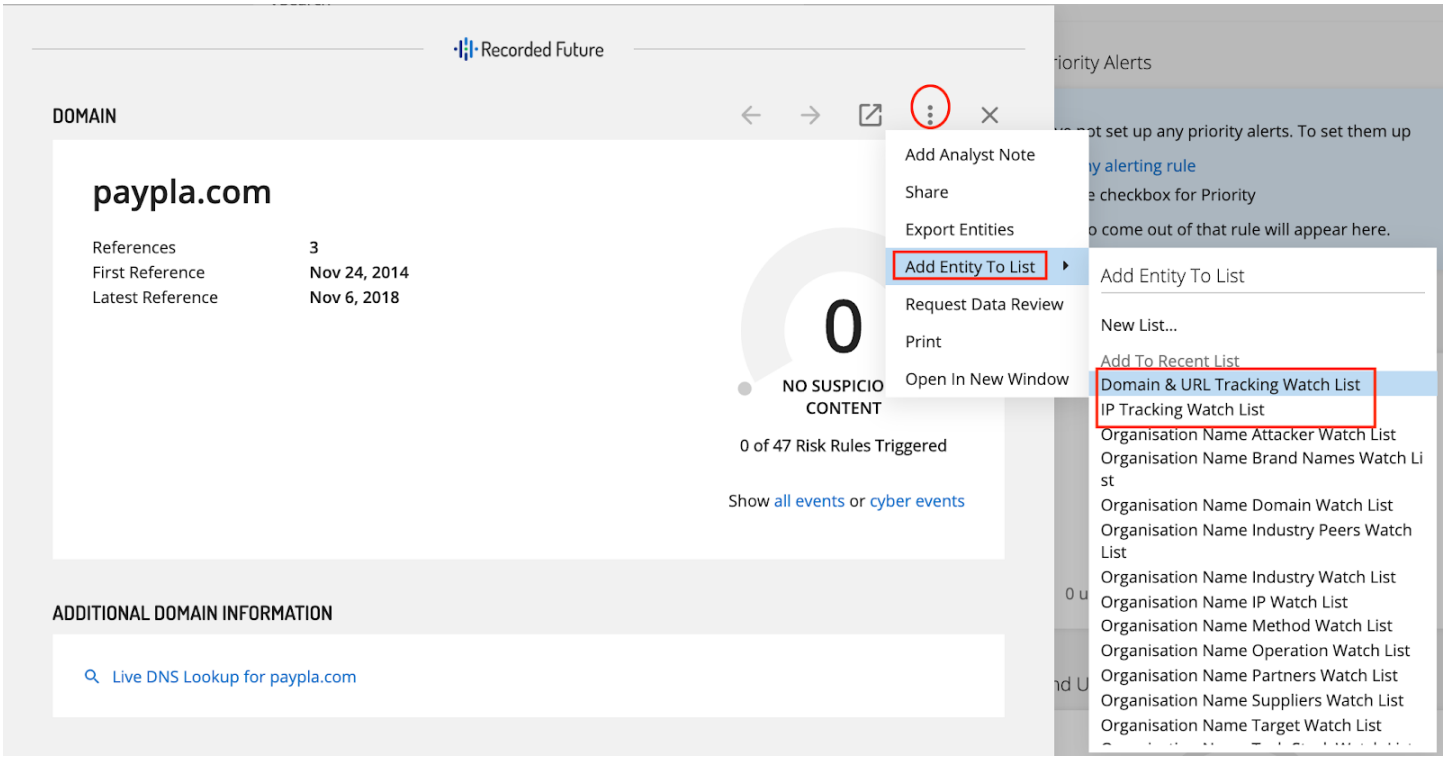
Sometimes, there may not be much information; in these cases, you may want to continuously monitor for the risk scores of those indicators to see if they're referenced.

Step 3

Add to 'Indicator Tracking' Watch Lists for monitoring.

Click the three dots at the top right of the Intelligence Card → Add Entity to List → select either the 'Domain & URL Tracking Watch List' or the 'IP Tracking Watch List', depending on the indicator type.

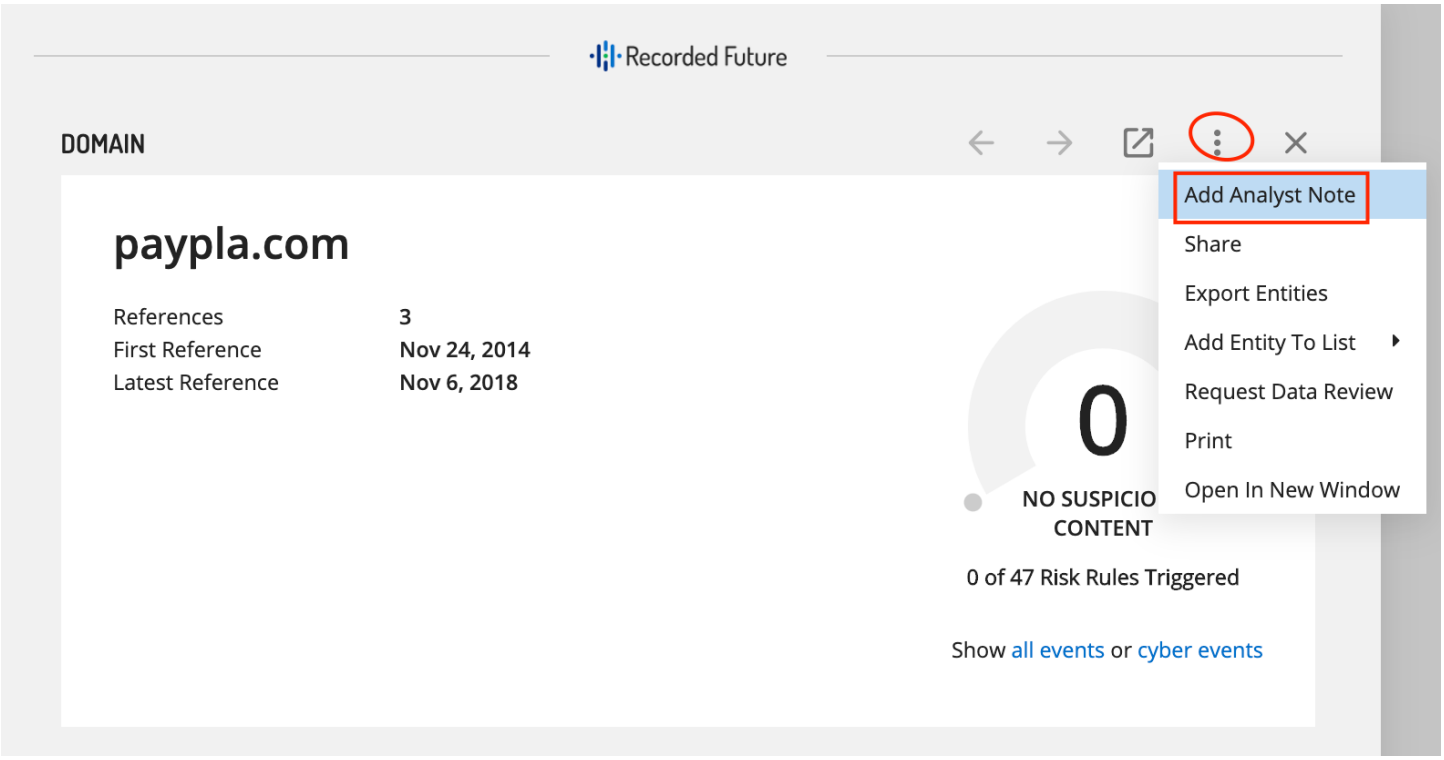
If the indicator is a file hash: Add it to the Domain & URL Tracking Watch List to monitor for references to that hash. Note that you will not be alerted to an increase in risk score of that file hash.



Step 4 (Optional)

Add an Analyst Note.

Click the three dots at the top right of the Intelligence Card again, but this time click 'Add Analyst Note'. Write yourself a short Analyst Note on 1) why you're researching that indicator and 2) why you want to continuously monitor for the indicator. Now when you receive an alert on the indicator, you can pull up the Intelligence Card and review the Analyst Note to jog your memory.



Step 5

Review your alerts and sanitize your Watch Lists.

You'll now start receiving alerts from the three alerting rules created by your consultant whenever there is new information. Once you no longer need to continuously monitor an indicator, remove it from the 'Domain & URL Tracking Watch List' or the 'IP Tracking Watch List'.

Have more questions regarding this topic: Submit a request

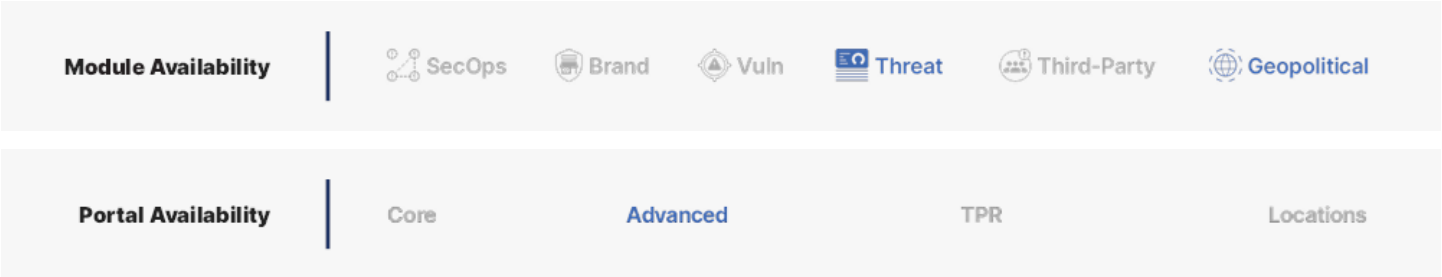
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Social Media Impersonation

PLAYBOOK

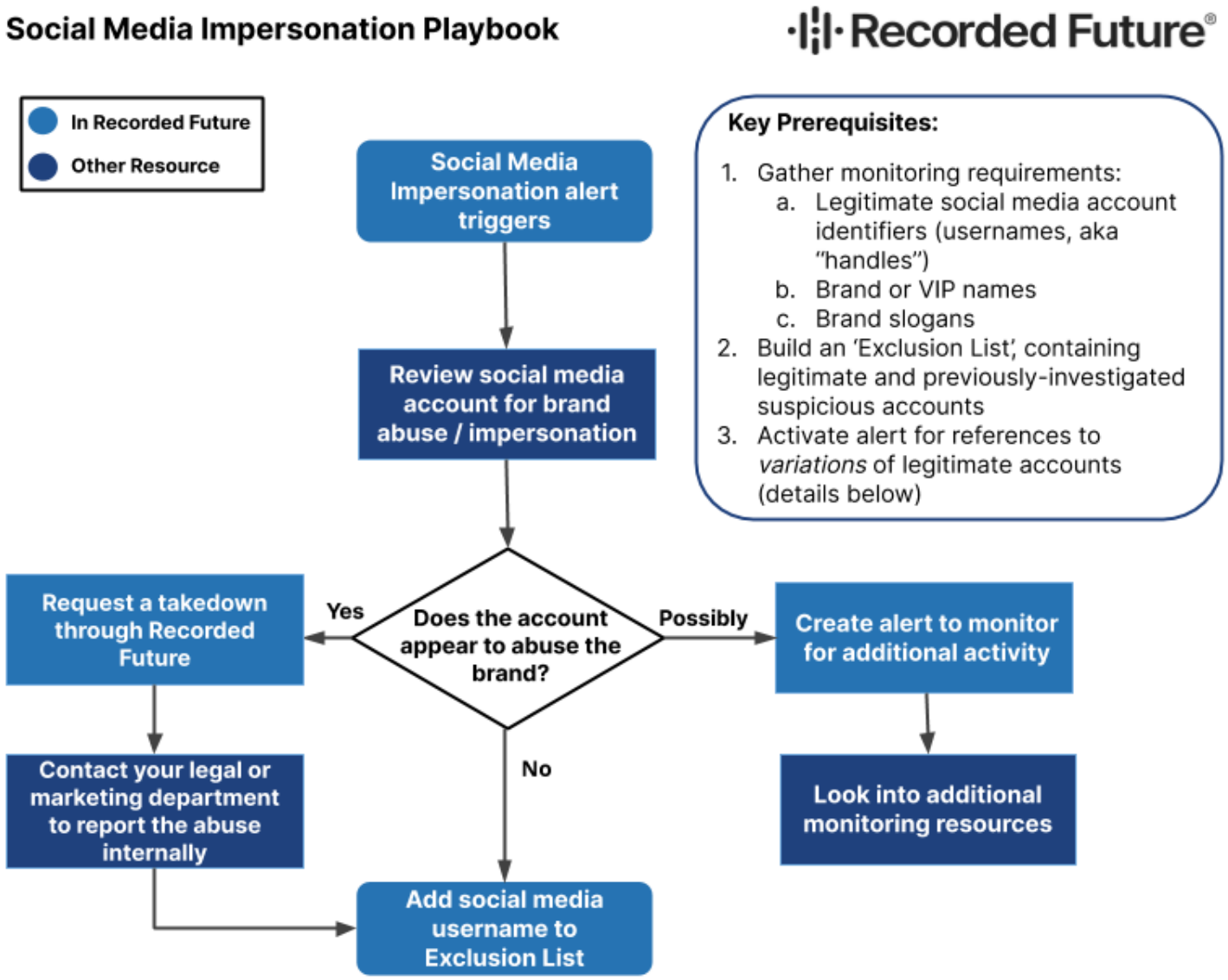
1st edition

Social Media Impersonation Playbook



Recorded Future's Social Media Impersonation playbook walks you through identifying and taking action on social media accounts that may be abusing your brand.

Looking for more information on Recorded Future's social media source coverage? Take a look at Source Types for more details on the sources used in the queries & alerting rules in this playbook. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library and refer to the Key Prerequisites below to make sure your organization is prepared to address social media impersonation threats.

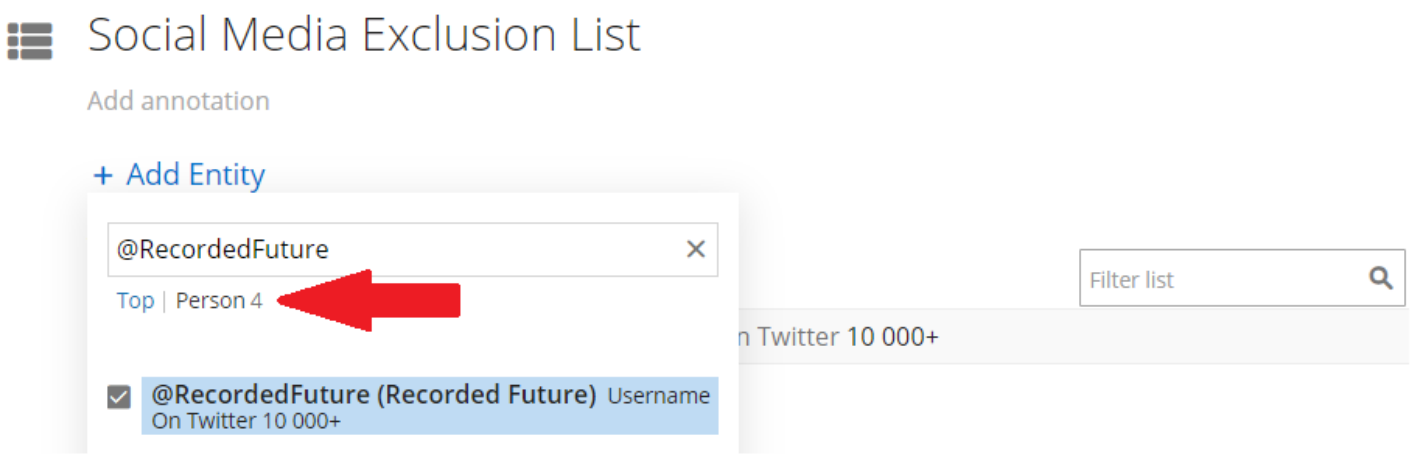


Key Prerequisites

1. Gather monitoring requirements. This includes a list of legitimate social media account names and "handles" (e.g., @RecordedFuture), brand names, VIP names, or slogans to monitor for impersonation attempts. A search engine may help identify your organization's legitimate social media accounts, or your organization may maintain a list of legitimate accounts.

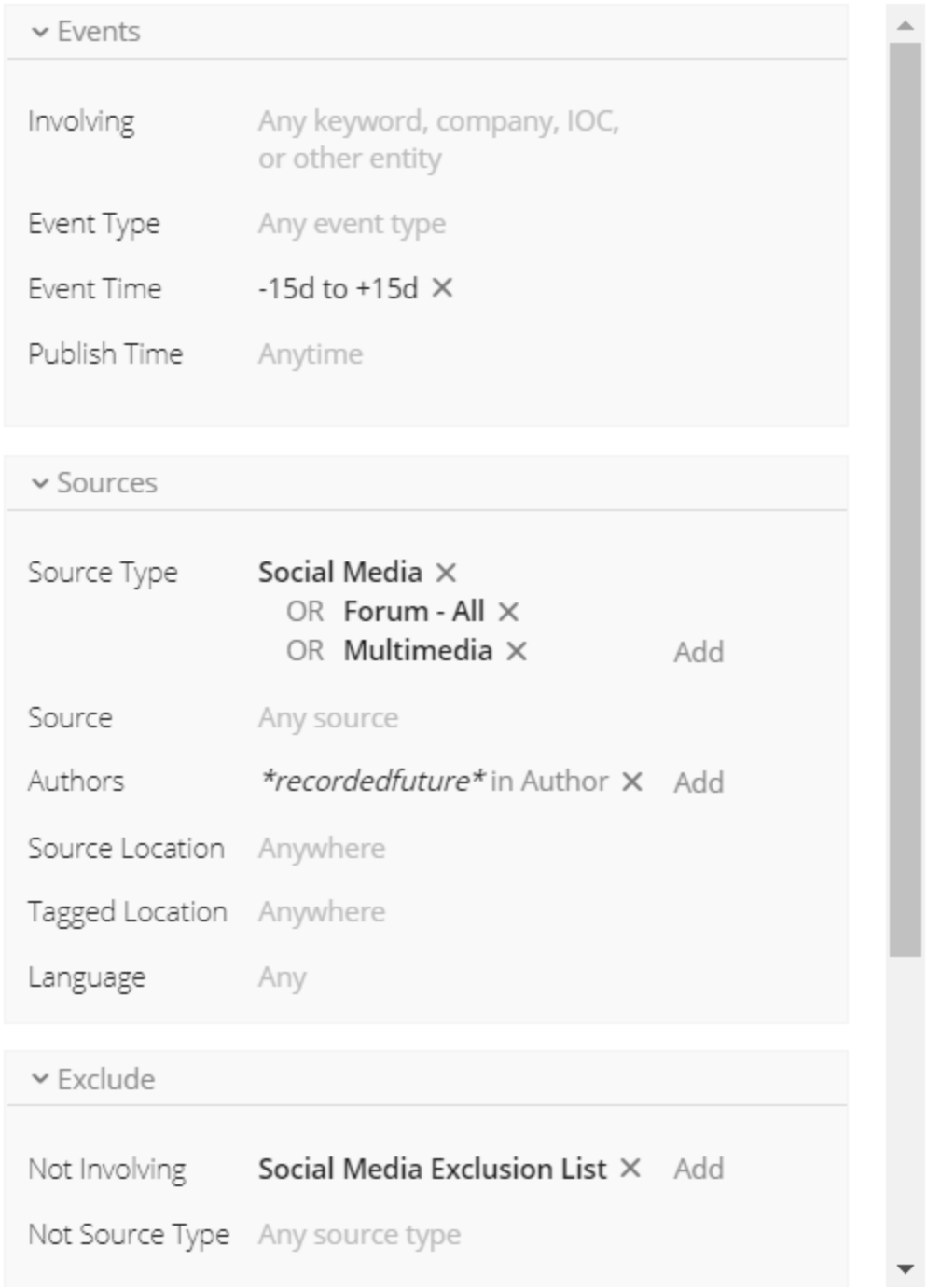
2. Create a new custom List to exclude the following accounts from your alerting results:
   - Legitimate accounts
   - Impersonation accounts you have investigated (See Step 5 below)

When adding account names, use the @ symbol before the name to add a Twitter account. For others, be sure to select the "Username" entity type, which can be filtered with the "Person" option in the entity picker (arrow below). You may also choose the "Company" or "Organization" entity type, which often contains legitimate usernames within its Recorded Future Entity Structure.

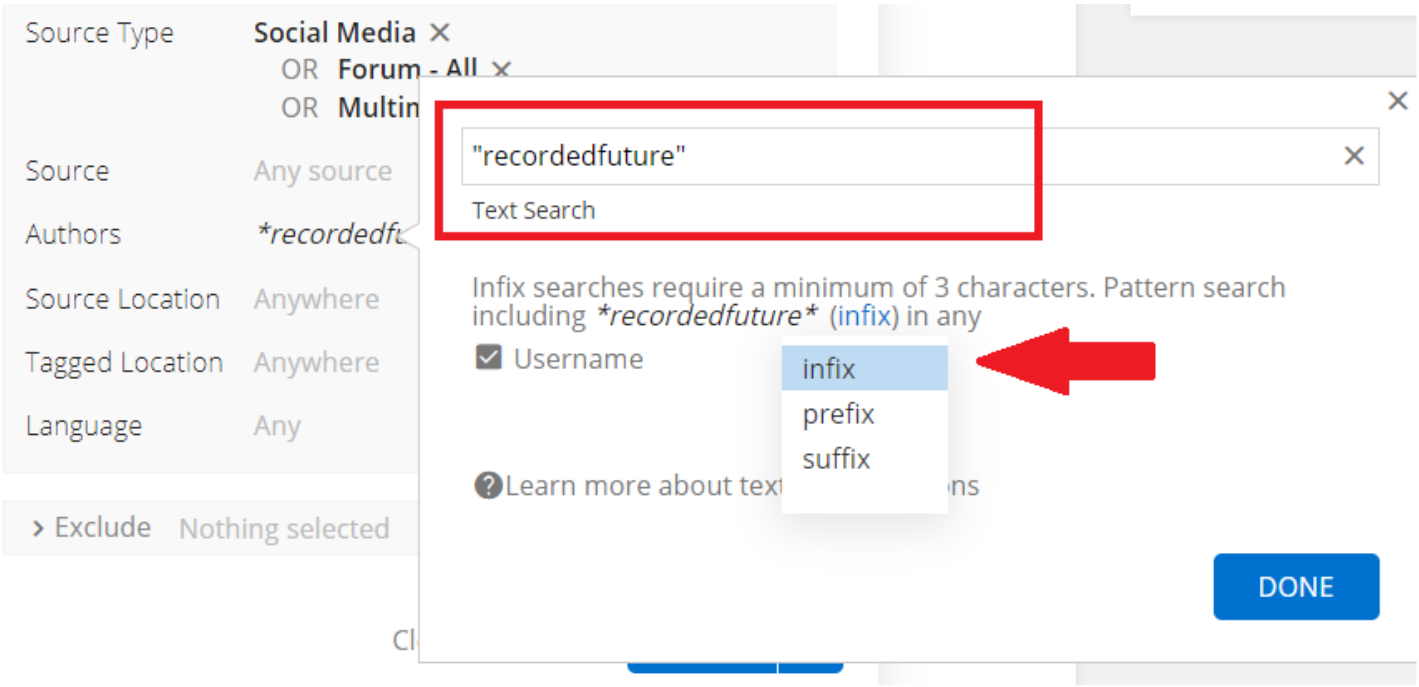


3. Configure a query and/or activate an alerting rule to identify social media accounts that use variations of your legitimate accounts in their names. See here for the basics of activating custom alerting rules.

- An example of the recommended query logic can be seen below:

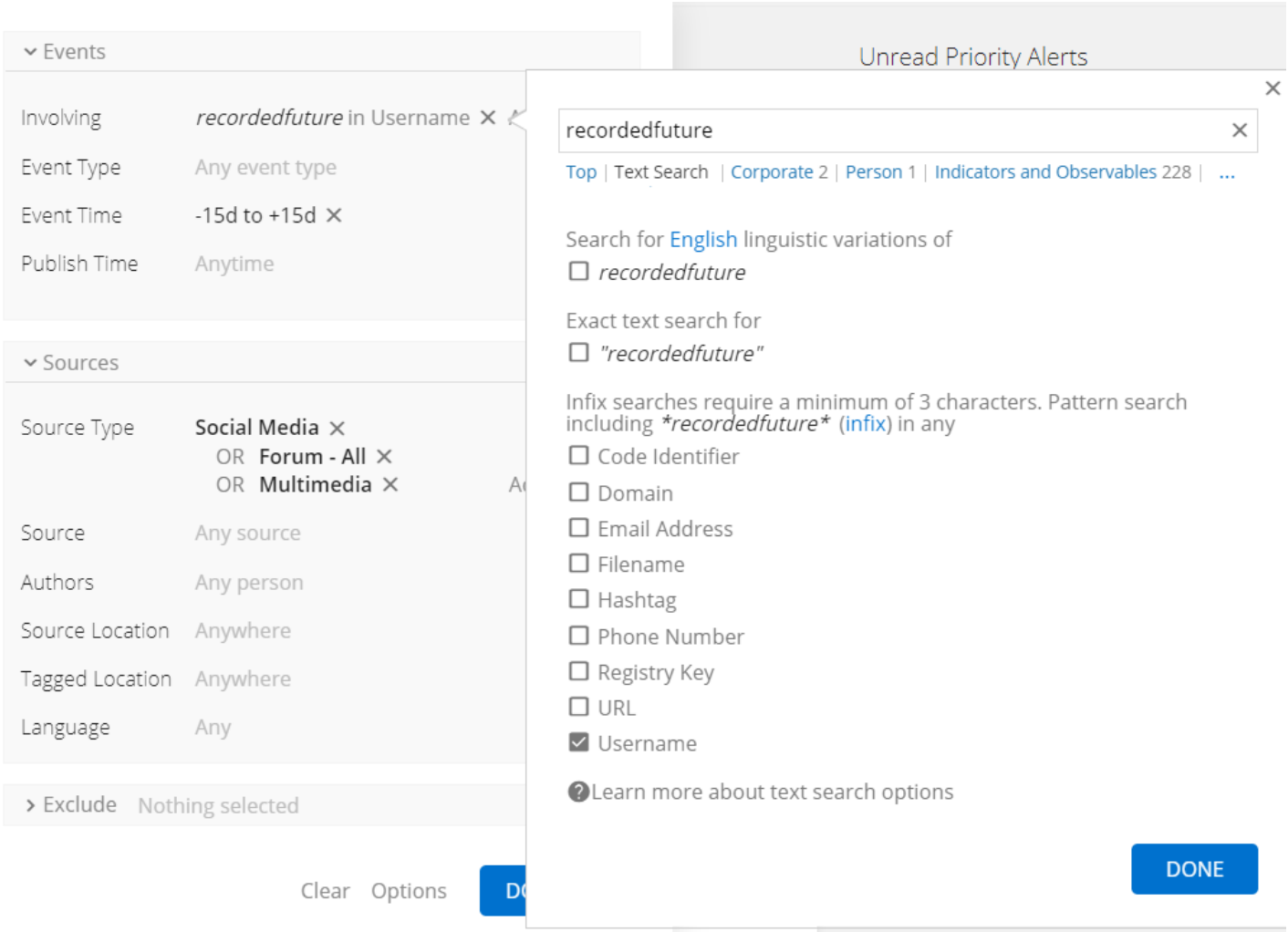


Use quotations around any keyword typed into the Authors field to search for that keyword as a text string within a username. The placement of the text string can be changed to infix (anywhere in the username), prefix, or suffix. Text searches are not case sensitive.



We recommend starting with text strings that exactly match how they appear in your legitimate social media accounts (mentions of the legitimate accounts will be excluded from your results). You may also want to include variations on those text strings, which are often used in impersonation accounts. Some of the most common variations include adding or removing spaces between keywords, inserting underscores in place of spaces, and adding or removing key letters:

A variation of the query above places the Username text strings in the Involving field at the top of the Advanced Query Builder. This returns results any time the relevant username is mentioned in the reference - not just when they are the social media post author. By nature this variation of the query typically returns more results. There is also a higher potential for false positive results, many times resulting from a social media user inadvertently misspelling an intended account's "handle."



Step 1

You receive an alert from the alert configured according to the recommendations in Key Prerequisites above. Proceed to the next step.

Step 2

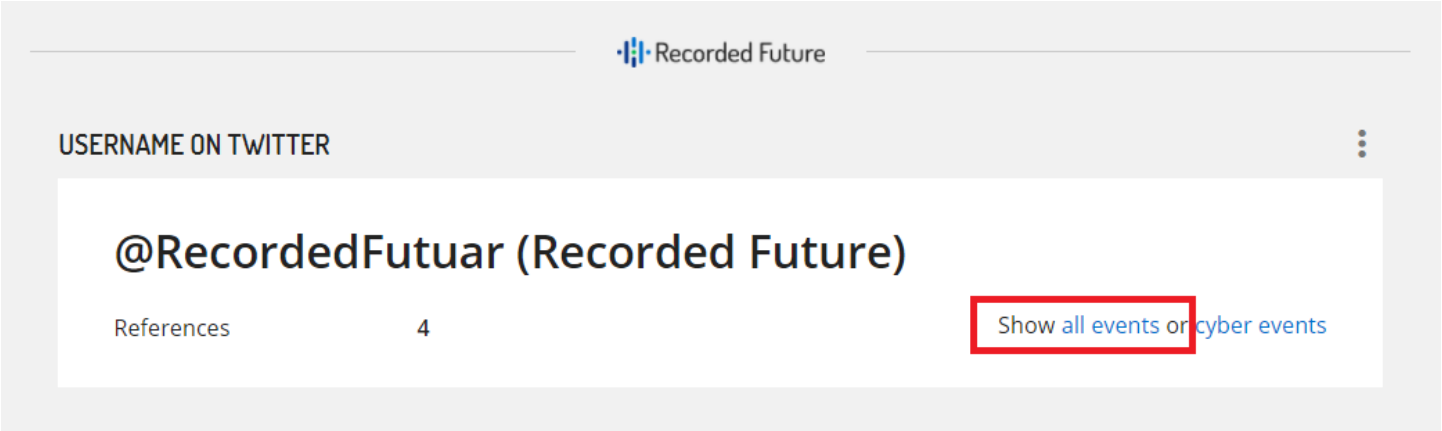
Assess whether the identified social media account poses an impersonation/brand abuse threat.

The Social Media Brand Abuse page can serve as a guide in this assessment.

Identify the relevant social media account username that triggered the alert. Click the relevant bolded text in the alert to open the Intelligence Card for that username.

- If your organization permits, navigate to the account's page on the relevant social media site (this will be specified in the Intelligence Card). Search on the site, place the username in the relevant URL and navigate there directly (e.g., https://twitter.com/RecordedFuture), or use other resources (search engines, search engine caches or web archives, commercial social media management solutions) to research details such as account profile pictures and other profile metadata.

- If you are not permitted to navigate to certain sites, you can use Recorded Future to research social media impersonation activity. From the Username Intelligence Card, click the link to "Show all events," which will display recent and historical references involving that username, such as social media posts that were published by or mention the username:



Step 3

Based on your investigation, does the account appear to abuse your brand?

- YES, brand abuse is evident. → Use Recorded Future's Brand Protection Takedown Services to take the account down (see Social Media Brand Abuse). Your organization's Legal or Marketing departments may also be able to contact the social media site directly in order to report the account or have the account removed. Proceed to Step 5.

- NO, there is no current evidence of brand abuse, or indications of potential future abuse. → Proceed to Step 5.

- MAYBE, brand abuse is possible but further investigation is warranted. → Proceed to Step 4.

Step 4

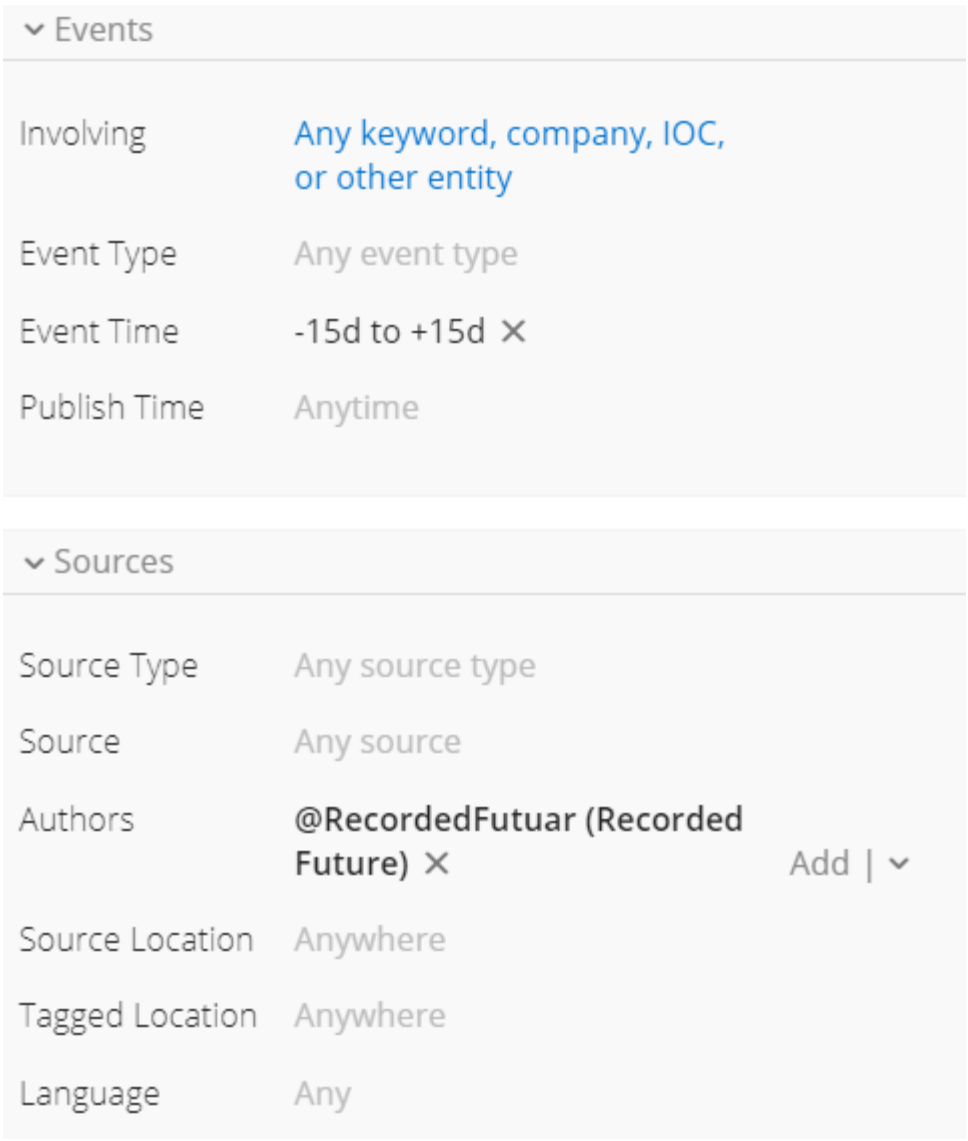
Use Recorded Future to configure an alert for new mentions of the account.

If the identified account appears suspicious but warrants further monitoring prior to escalation.

Use the a) "Involving" field to alert on all references or b) "Authors" field to alert on posts published by this username:

a)

b)

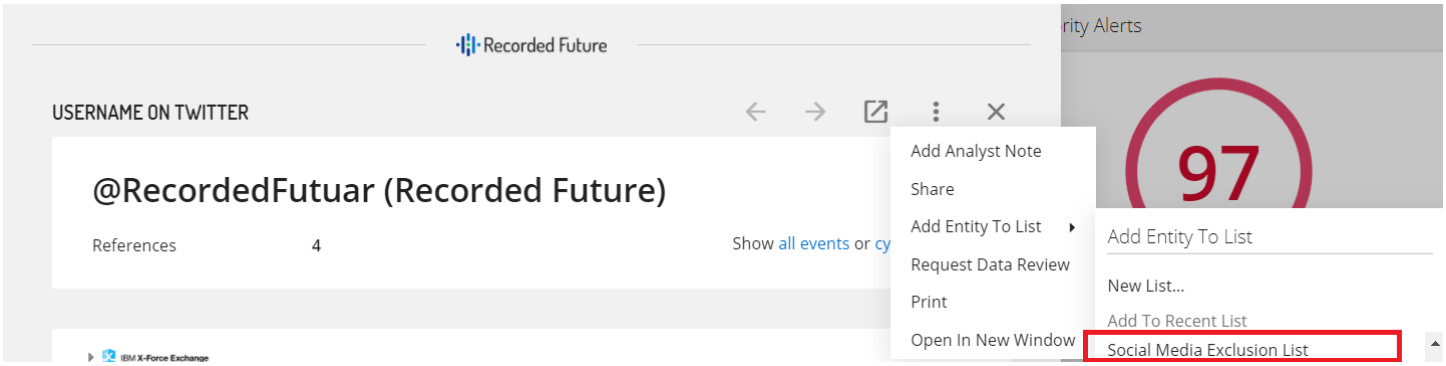


Other resources, such as commercial social media management solutions, may provide additional options for monitoring account activity. Proceed to Step 5.

Step 5

Add the entity to an Exclusion List.

Once you have investigated a given account, we recommend adding its Recorded Future entity to an “Exclusion List” so it does not continue to appear in future alert results. This can be done easily from the account’s Username Intelligence Card by clicking the three vertical dots in the upper-right and choosing “Add Entity To List.” The Exclusion List will appear in your alerting rule logic as described above.



Have more questions regarding this topic: Submit a request

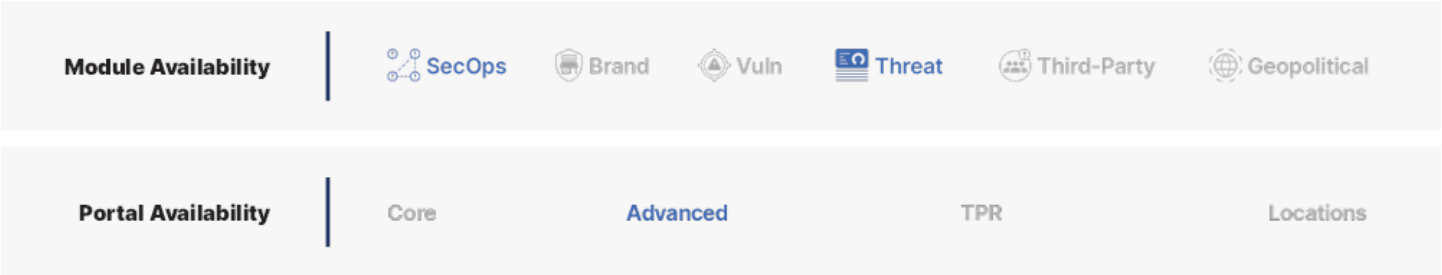
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Genesis Store

PLAYBOOK

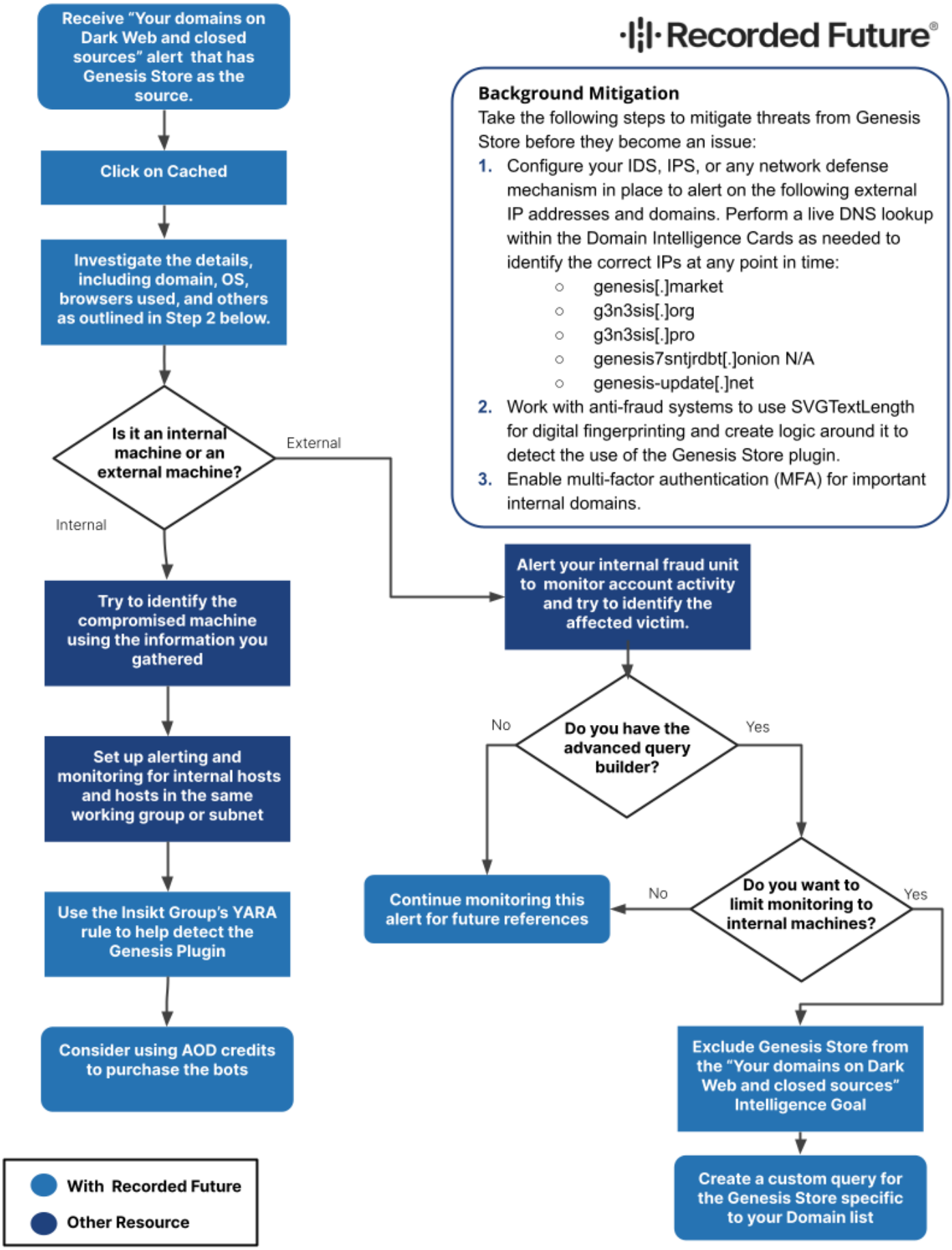
1st edition

Genesis Store Playbook



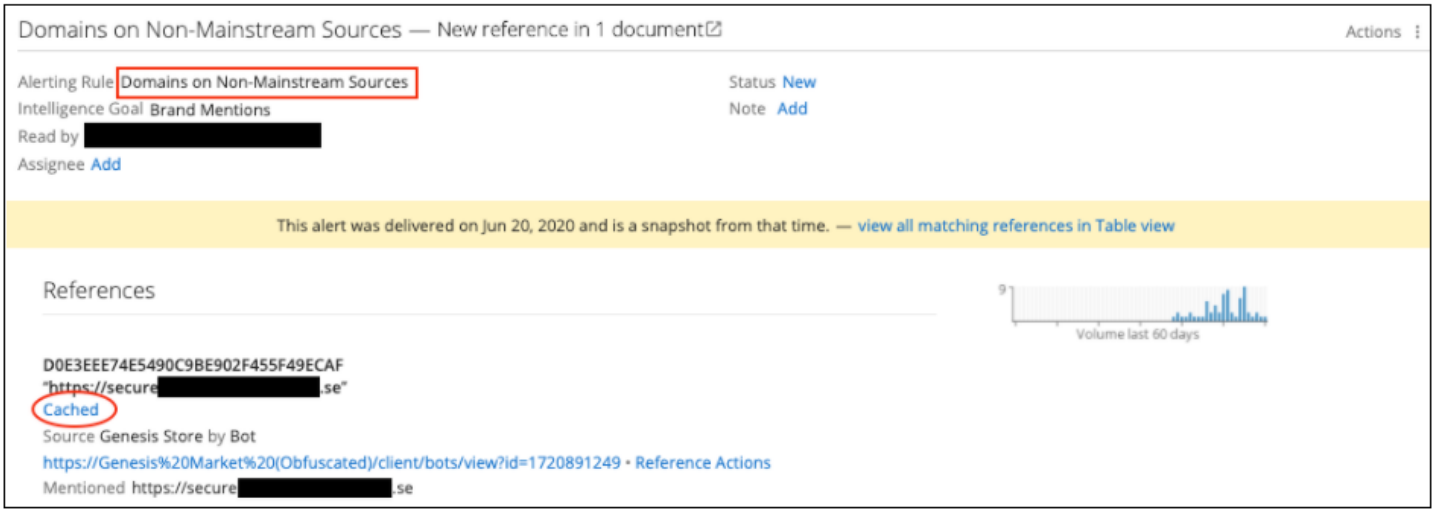
Recorded Future's Genesis Store playbook walks you through triaging Genesis Store alerts from start to finish. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library.

Looking for more information on Genesis Store before you take action? Take a look at the Introduction to Genesis Store for an explanation of the marketplace and links to more research.


Recorded Future
Background Mitigation
Take the following steps to mitigate threats from Genesis Store before they become an issue:
1. Configure your IDS, IPS, or any network defense mechanism in place to alert on the following external IP addresses and domains. Perform a live DNS lookup within the Domain Intelligence Cards as needed to identify the correct IPs at any point in time:
genesis[.]market
g3n3sis[.]org
g3n3sis[.]pro
genesis7sntjrdbt[.]onion N/A
genesis-update[.]net
2. Work with anti-fraud systems to use SVGTextLength for digital fingerprinting and create logic around it to detect the use of the Genesis Store plugin.
3. Enable multi-factor authentication (MFA) for important internal domains.
Receive "Your domains on Dark Web and closed sources" alert that has Genesis Store as the source.
Click on Cached
Investigate the details, including domain, OS, browsers used, and others as outlined in Step 2 below.
Is it an internal machine or an external machine?
External
Internal
Try to identify the compromised machine using the information you gathered
Set up alerting and monitoring for internal hosts and hosts in the same working group or subnet
Use the Insikt Group's YARA rule to help detect the Genesis Plugin
Consider using AOD credits to purchase the bots
Alert your internal fraud unit to monitor account activity and try to identify the affected victim.
Do you have the advanced query builder?
No
Yes
Continue monitoring this alert for future references
Do you want to limit monitoring to internal machines?
No
Yes
Exclude Genesis Store from the "Your domains on Dark Web and closed sources" Intelligence Goal
Create a custom query for the Genesis Store specific to your Domain list
With Recorded Future
Other Resource

Step 1

You receive an alert from the 'Your domains on Dark Web and closed sources' Intelligence Goal. One of the references in the alert has the source 'Genesis Store' and shows one of the domains in your Domain Watch List. Click 'Cached' to get more information.



Note: If your enterprise activated this Intelligence Goals Library alert prior to July 21, 2021, it will be titled: 'Domains on Non-Mainstream Sources.'

Step 2

Gather the following details from the cached information and determine whether they align to details from an internal company machine and user or an external customer machine:

2.1 Your company domain mentioned in the bot and associated web browser

- Is it an internal-only or an external customer domain?
- What information is being given for that customer domain?
- Which web browser was the information stolen from?
- Which timestamps are associated with the account for your domain?
- *Tip: use Ctrl+F to find where your company domain is mentioned*

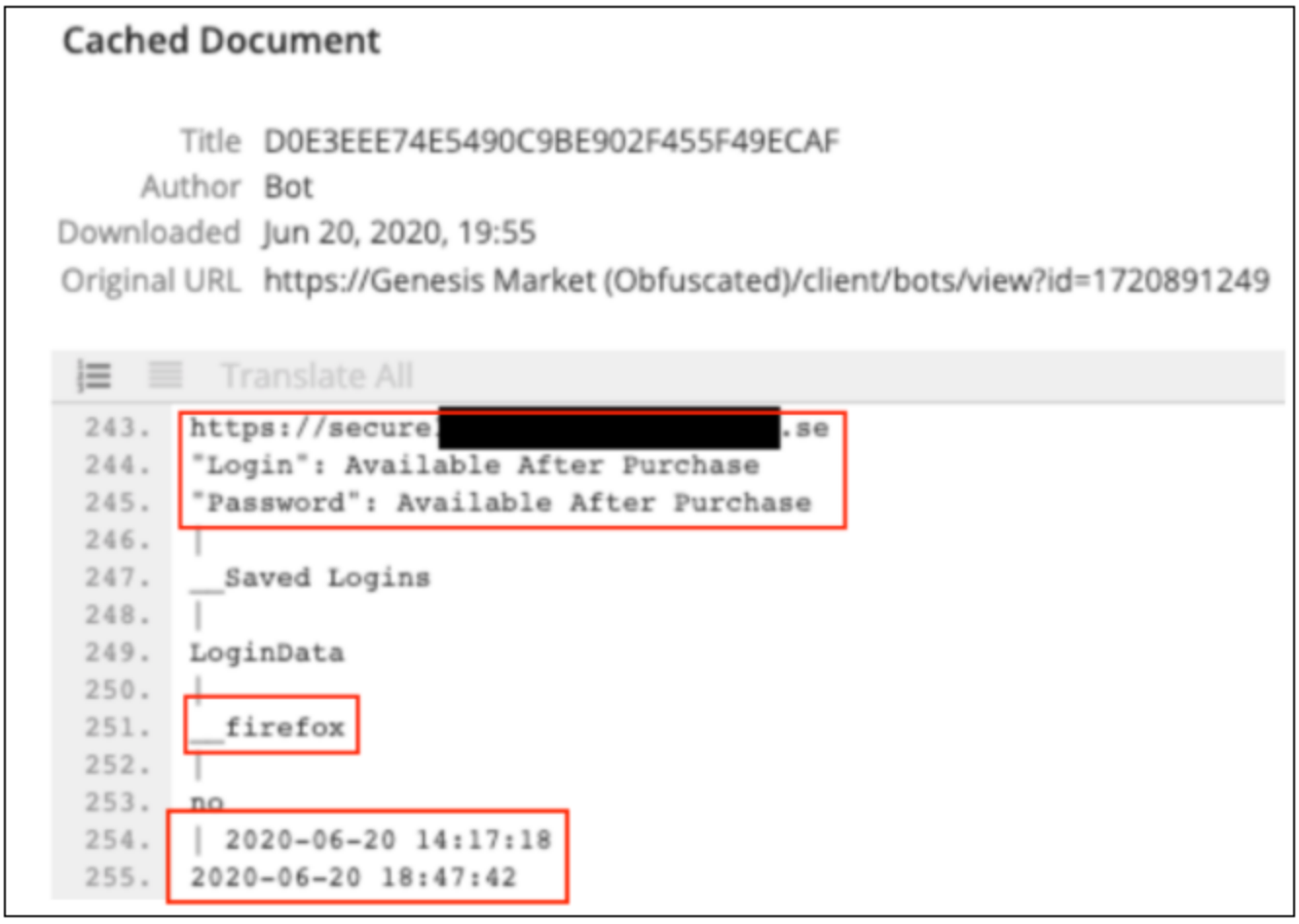


Image: Cached information for a Genesis Store reference, showing that the compromised information for the domain is the login and password, and that the web browser was Firefox. Also highlighted are the timestamps (in UTC) for this particular account - when the details were first stolen and then when it was most recently updated.

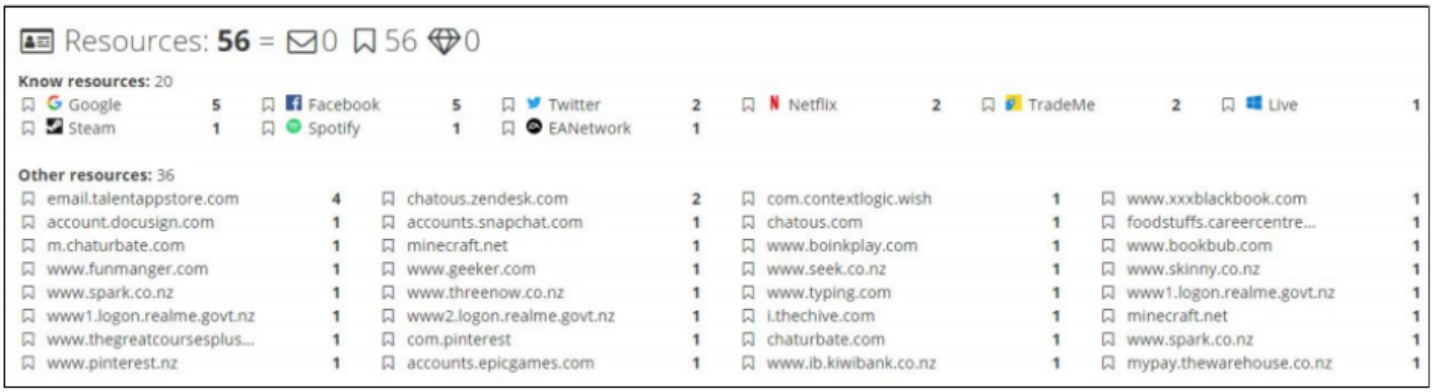


Image: What the cached information in Recorded Future looks like in Genesis Store. Note that this is a screenshot of a different bot being sold than the one in the Recorded Future screenshot.

2.2 The first 2 octets of the bot's IP address, country, and timestamps for the bot

- Does your company own IP addresses within that address space?
- What country is the bot from?
- What timestamps are shown for the bot? This can be a good data point in trying to identify an internal compromised machine at a later stage.

Image: Cached information for a Genesis Store reference, highlighting that the first two octets of the compromised host's IP address are 85.229 and that the associated country code is SE (Sweden). The timestamps (in UTC) are also shown for the bot. The first timestamp is when the information was initially stolen (upon installation of the malware) and the second represents when it was most recently updated.

Image: What the cached information for the bot may look like in Genesis Store, in this case showing the first two octets of the compromised host's IP address are 158.140... and the associated country is the US. Note that this is a screenshot of a different bot being sold than the one in the Recorded Future screenshot.

2.3 The operating system (OS) of the bot

- Do any devices at your company use that OS?
- Does the OS indicate that the compromised machine is an enterprise device (e.g., is the OS Windows Pro, Windows 10 Enterprise, Windows 10 for Business)?

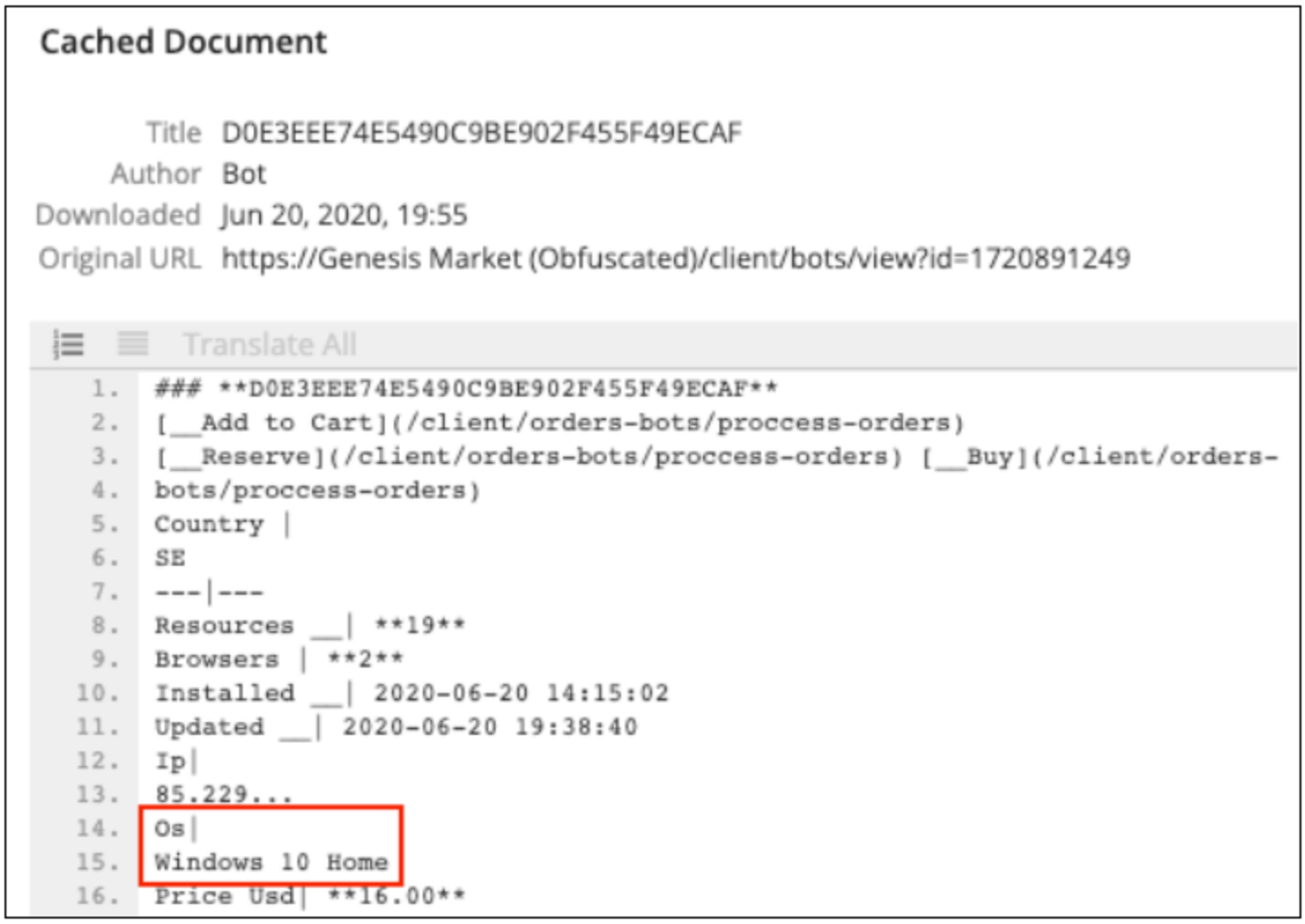
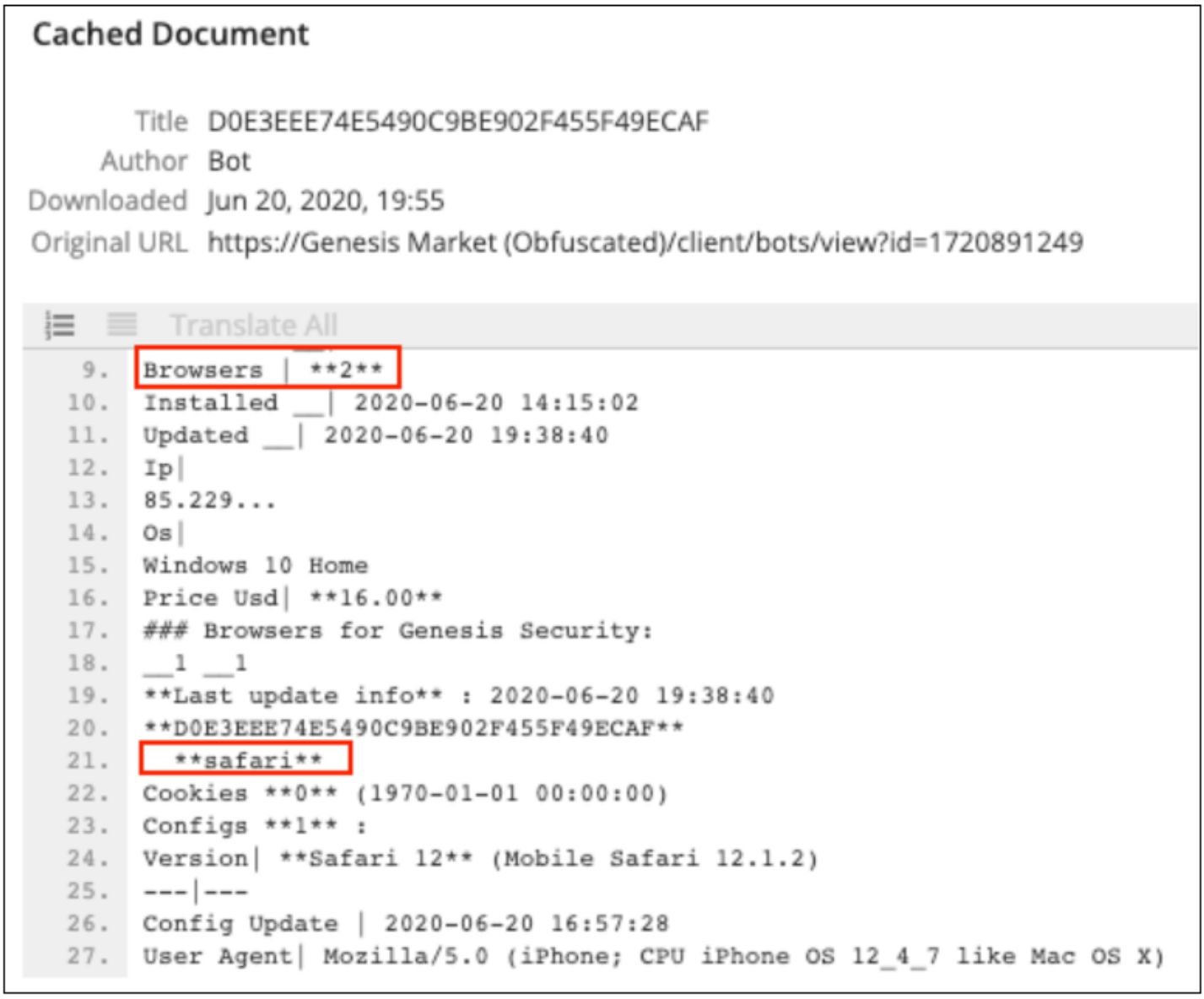


Image: Recorded Future cached information for a Genesis Store reference, highlighting that the most recently identified OS of the compromised host was Windows 10 Home, as opposed to an enterprise OS such as Windows 10 Enterprise. Note that the user agent information discussed below will show other historical operating systems associated with this bot.

Image: What the cached information for the bot may look like in Genesis Store - in this case, showing the operating system of the compromised host was Windows 8. Note that this is a screenshot of a different bot being sold than the one in the Recorded Future screenshot.

2.4 The browsers listed in the bot where the information has been stolen from

- Does your company permit those browsers to be used on company devices?
  Note that this step isn't just focused on the browser mentioned alongside your company domain in step 2.1, but on all browsers included in the bot. If there are resources from a browser that is banned from your company's work devices, it can help with your assessment in determining whether the bot is from an internal compromised host machine or external customer machine.



Cached Document

Title D0E3EEE74E5490C9BE902F455F49ECAF
Author Bot
Downloaded Jun 20, 2020, 19:55
Original URL https://Genesis Market (Obfuscated)/client/bots/view?id=1720891249

Translate All

```
9.  Browsers | **2**
10. Installed __| 2020-06-20 14:15:02
11. Updated __| 2020-06-20 19:38:40
12. Ip|
13. 85.229...
14. Os|
15. Windows 10 Home
16. Price Usd| **16.00**
17. ### Browsers for Genesis Security:
18. __1 __1
19. **Last update info** : 2020-06-20 19:38:40
20. **D0E3EEE74E5490C9BE902F455F49ECAF**
21.   **safari**
22. Cookies **0** (1970-01-01 00:00:00)
23. Configs **1** :
24. Version| **Safari 12** (Mobile Safari 12.1.2)
25. ---|---
26. Config Update | 2020-06-20 16:57:28
27. User Agent| Mozilla/5.0 (iPhone; CPU iPhone OS 12_4_7 like Mac OS X)
```

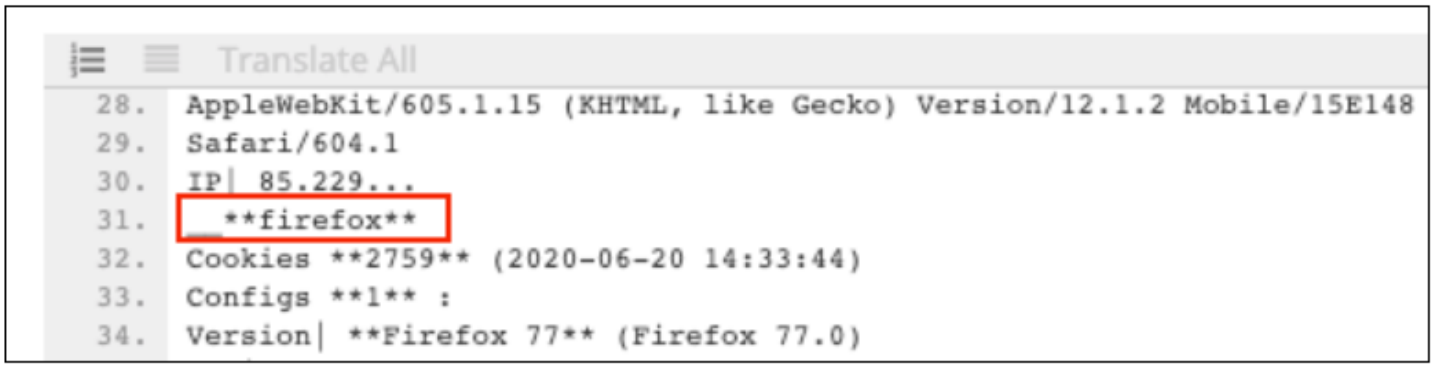


Image: Recorded Future cached information for a Genesis Store reference, highlighting that the bot has resources for two browsers, and that those browsers are Safari and Firefox.

2.5. The user agent of the bot

- Do any of the user agents listed match devices and user agent footprints of any devices owned by your company?
- Note that user agents can be updated and this will be reflected in Genesis Store and the cached information in Recorded Future.

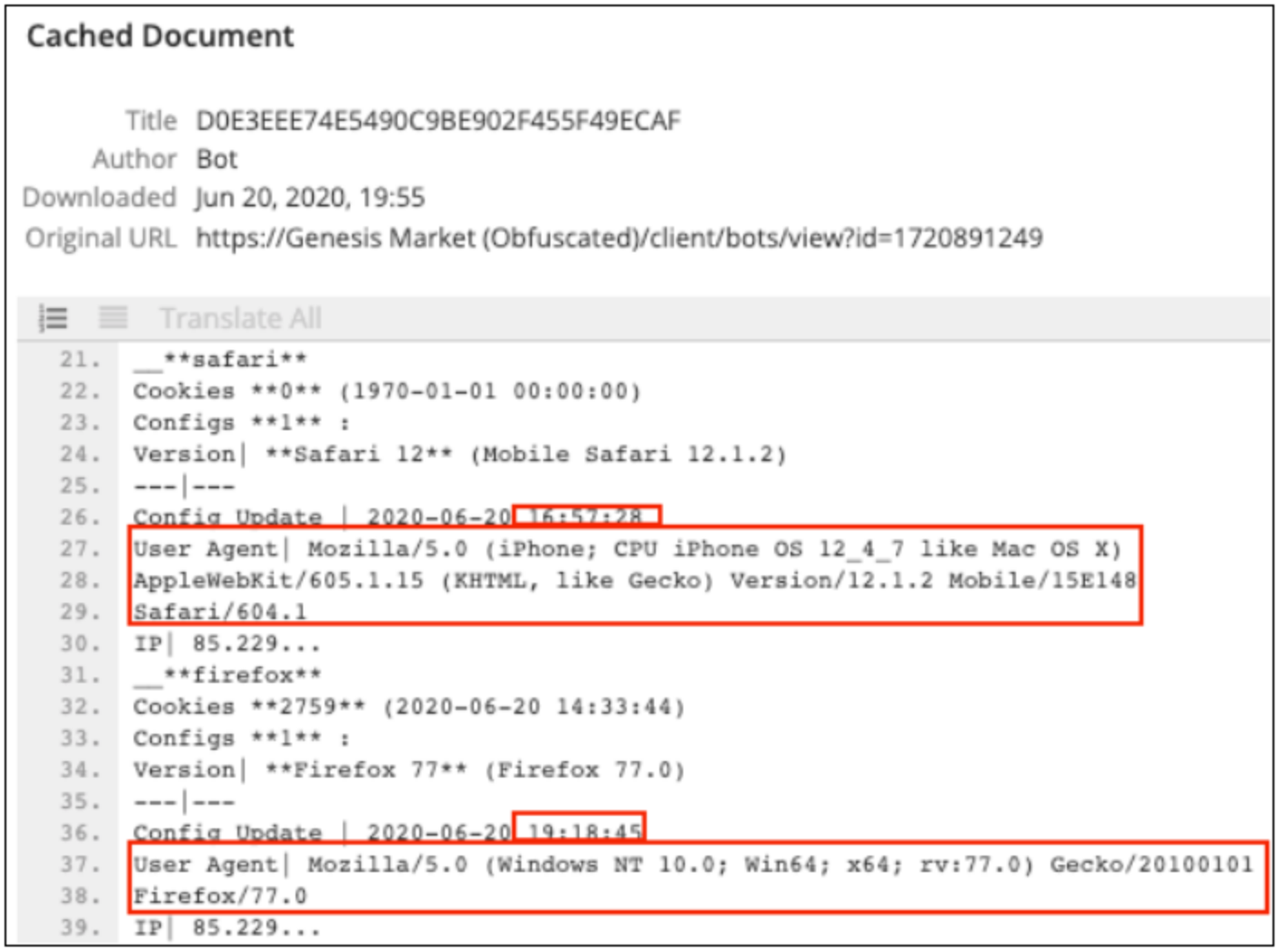


Image: Recorded Future cached information for a Genesis Store reference, highlighting the user agent information. The user agent can be updated repeatedly, and you should make note of all the user agents listed.

Image: Chrome browser fingerprint information of a victim as it appears in Genesis Store. There are 123 session cookies associated with this victim. The user agent in this example is Mozilla/5.0 (Windows NT 10.0; Win64: x64) AppleWebKit/537.36. Note that this is a screenshot of a different bot being sold than the one in the Recorded Future screenshot.

2.6. Other resources that are included with the bot

- Are there other common websites and domains listed in the bot's resources that your company's users would be expected to access during the work that they perform (e.g., your webex solution and your email provider)?

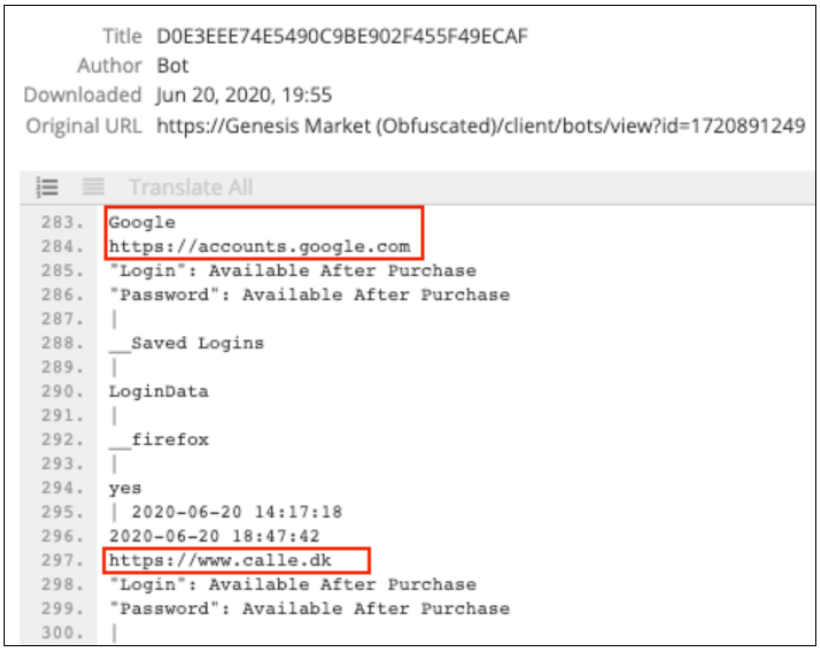


Image: Cached information for a Genesis Store reference, highlighting other resources included with the bot, in this case accounts[.]google[.]com and callee[.]dk. If a username or password is listed as "empty," there is likely no information associated with that field even after a Genesis Store purchase is made.

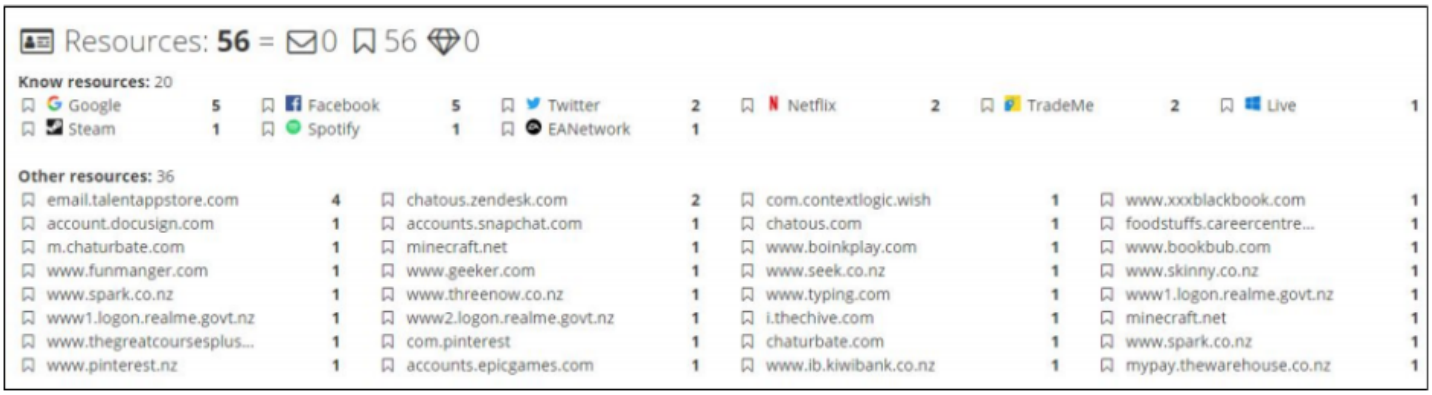


Image: What the cached information for the bot may look like in Genesis Store. Accounts associated with an individual bot are divided into "Known resources," typically meaning well-known websites, and "Unknown resources," meaning lesser-known websites. Note that this is a screenshot of a different bot being sold than the one in the Recorded Future screenshot.

Step 3

Based on the information you gathered, assess whether the bot of system information being sold is from an internal compromised host machine or an external customer machine. The following questions should help you with this assessment.

Is your company domain listed with the bot an internal domain?	*Yes / No*
Does your company own IPs within the address space?	*Yes / No*
Do any of your company devices use the OS listed (especially if it's an enterprise OS that is listed)?	*Yes / No*
Are the browsers associated with the bot permitted on company devices?	*Yes / No*
Do the user agents match the devices owned by your company?	*Yes / No*
Does the bot list any resources that would commonly be accessed by your company's employees?	*Yes / No*

If suspected internal, proceed to Step 4; if suspected external, proceed to Step 5.

Step 4

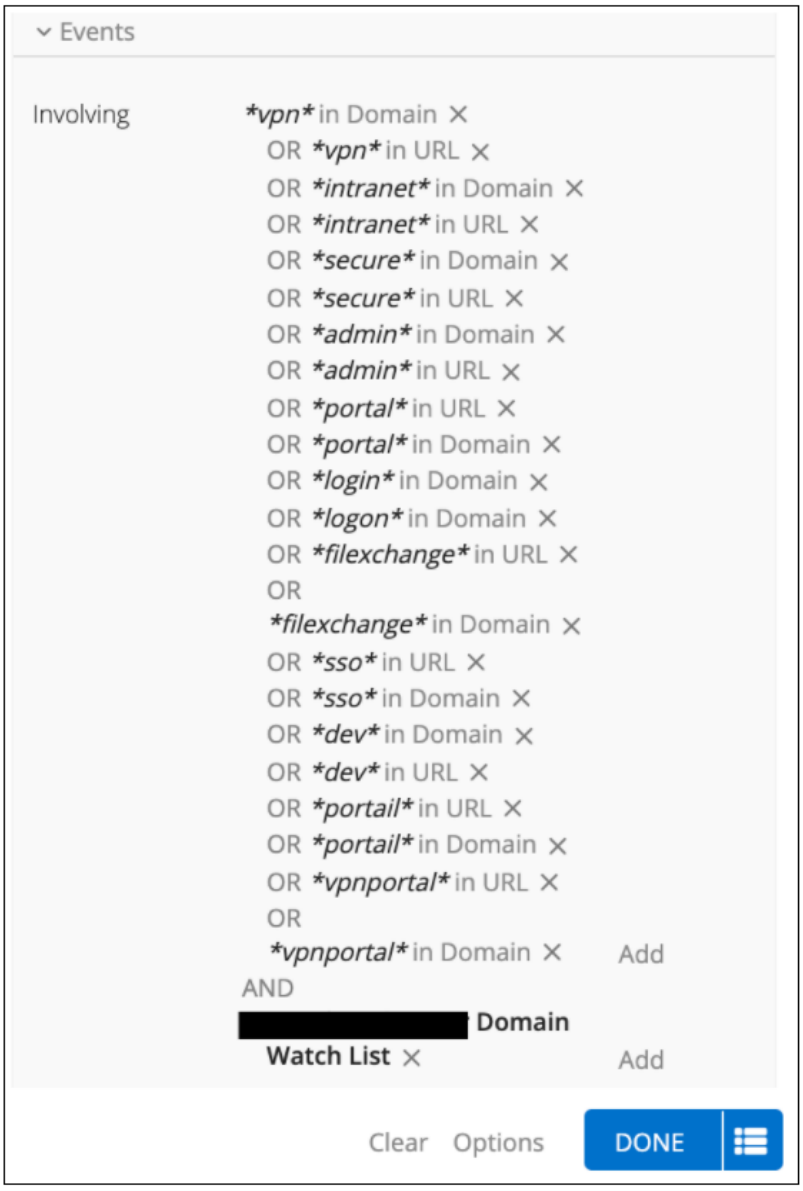
If you suspect the information is from an internal host machine...

- Try to identify the compromised machine based on the information collected above.
- Set up alerting and monitoring for internal hosts as well as any hosts surrounding those users in the same working group or subnet.
- Use the Insikt Group's YARA rule to help detect the Genesis Plugin running in memory (Appendix C, here).
- Consider using the Analyst on Demand service to purchase the bots from Genesis Store as soon as they become available. Once a bot is sold on Genesis Store, the information is removed from the site and any updates the victim makes to the account are also captured by Genesis Store admins.

Step 5

If you suspect the information is from an external customer machine...

- Pass the above information to your internal fraud unit to monitor account activity and try to identify the affected victim.
- If you aren't concerned about external customer compromises or are getting too many Genesis Store alerts, and if you have an Advanced User license, consider excluding Genesis Store from the 'Your domains on Dark Web and closed sources' Intelligence Goal and instead, create a new alerting rule explicitly for Genesis Store, cross referencing your Domain Watch List with terms like 'vpn', 'internal', 'sso', 'portal', etc. See this query for the example shown below.



Have more questions regarding this topic: Submit a request

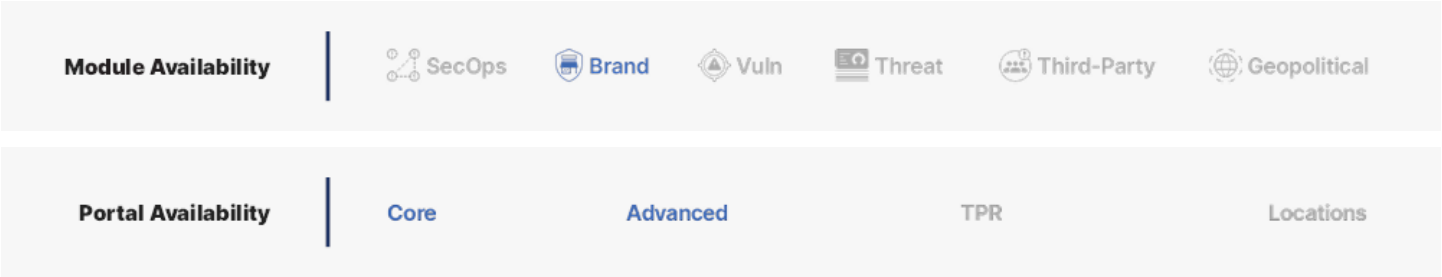
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Leaked Credentials

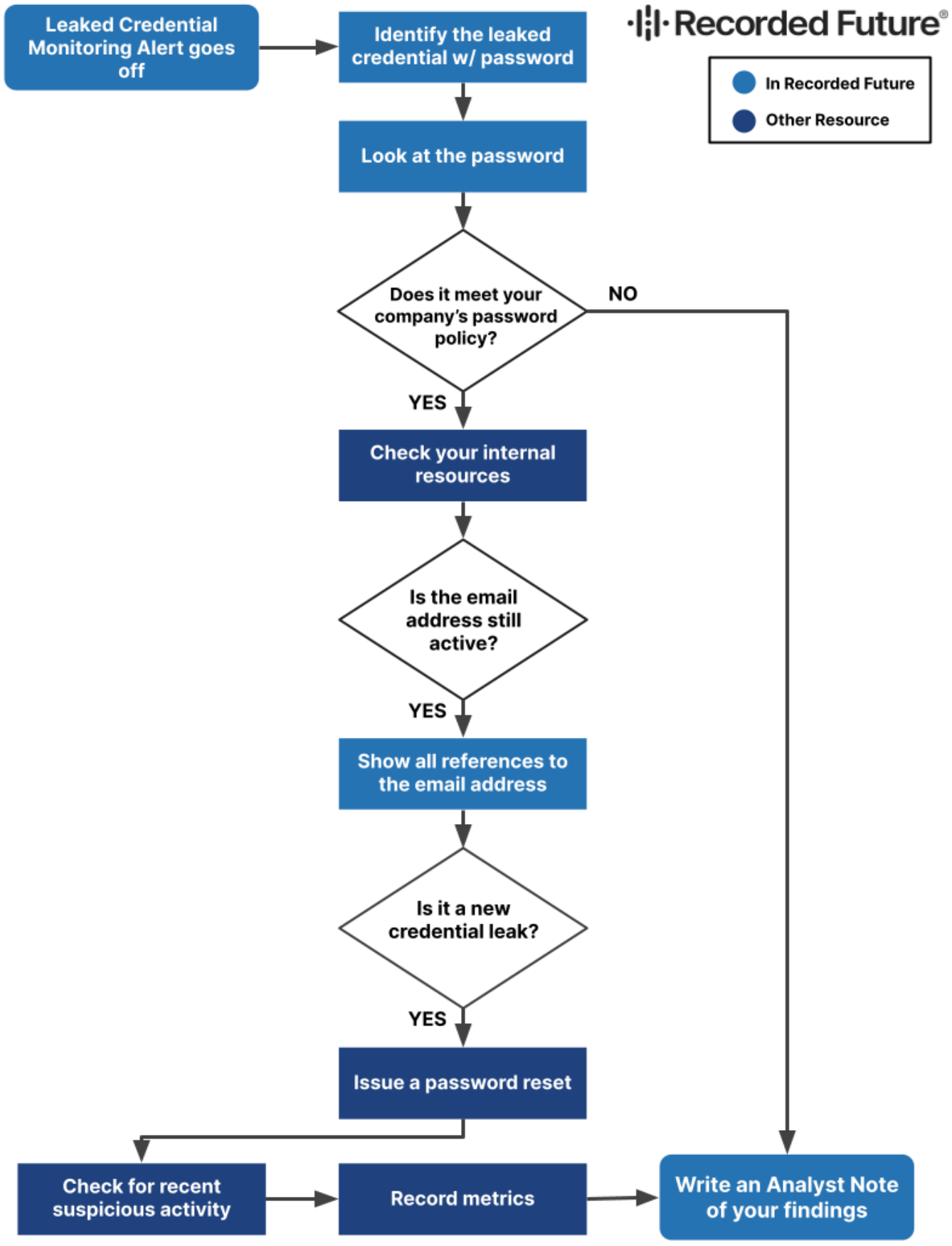
PLAYBOOK

1st edition

Leaked Credentials Playbook



Recorded Future's Leaked Credentials playbook walks you through triaging a Leaked Credentials Monitoring alert from start to finish. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library.


Leaked Credential Monitoring Alert goes off
Identify the leaked credential w/ password
Look at the password
Does it meet your company's password policy?
NO
YES
Check your internal resources
Is the email address still active?
YES
Show all references to the email address
Is it a new credential leak?
YES
Issue a password reset
Check for recent suspicious activity
Record metrics
Write an Analyst Note of your findings
Recorded Future
In Recorded Future
Other Resource

ge

Step 1

You identify leaked credentials that include a password via alerts generated by the 'Leaked Credential Monitoring' Alerting Rule. Proceed to the next step.

Step 2

Does the password adhere to your company password policy, or can you not confirm because it's a hashed password?

- NO, the password does not meet company policy → Dismiss alert status.
- YES, the password meets company policy or you cannot confirm → Proceed to the next step.

Step 3

Check internal resources to see if the email address is still active.

- NO, the email address is not active. → Exclude the email and password string from the alerting rule e.g. 'johnsmith1@gmail.com:password123'.
- YES, the email address is active. → Proceed to the next step.

Step 4

Click on the Email Address to bring up the Intelligence Card and click 'Show all events.' Have the same Email Address and Password been identified in the past (e.g., in an older breach)?

- NO, they have not been identified in past events. → Issue a password reset, check for recent suspicious activity, and record metrics. Finally, create an Analyst Note in the Email Address Intelligence Card showing the password and confirming that a password reset was issued.
- YES, the email and password were identified in past events. → Exclude the email and password string from the alerting rule (e.g., 'johnsmith1@gmail.com:password123').

Have more questions regarding this topic: Submit a request

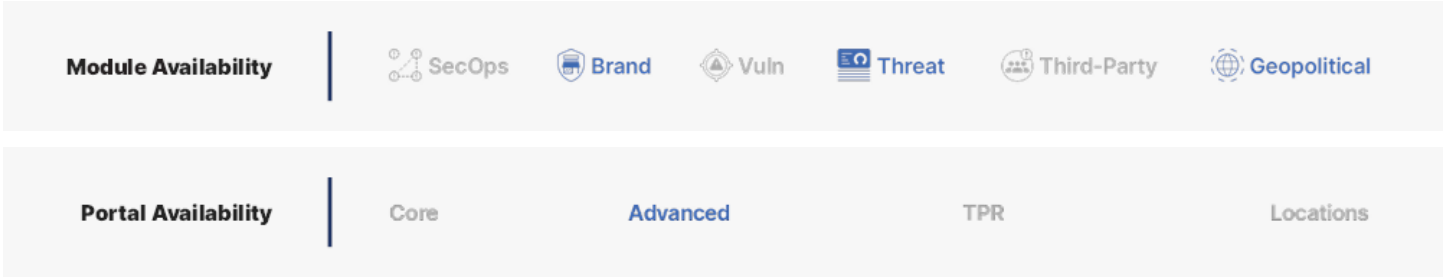
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Fraudulent Domains & Typosquats

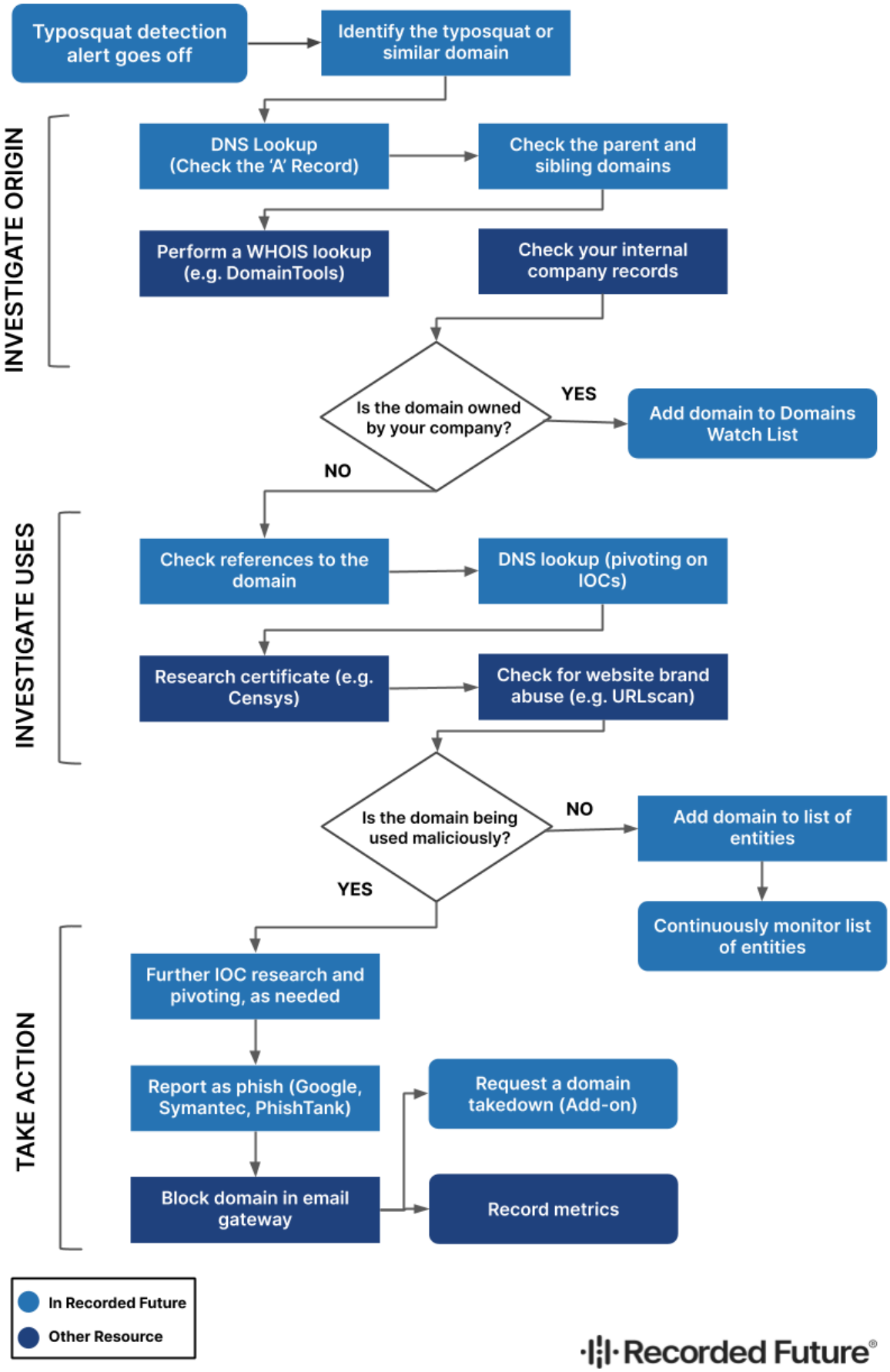
PLAYBOOK

1st edition

Fraudulent Domains and Typosquats Playbook



Recorded Future's Fraudulent Domains and Typosquats playbook walks you through triaging a typosquatting or similar domains alert from start to finish. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library.


Typosquat detection alert goes off
Identify the typosquat or similar domain
INVESTIGATE ORIGIN
DNS Lookup (Check the 'A' Record)
Check the parent and sibling domains
Perform a WHOIS lookup (e.g. DomainTools)
Check your internal company records
Is the domain owned by your company?
YES
Add domain to Domains Watch List
NO
INVESTIGATE USES
Check references to the domain
DNS lookup (pivoting on IOCs)
Research certificate (e.g. Censys)
Check for website brand abuse (e.g. URLscan)
Is the domain being used maliciously?
NO
Add domain to list of entities
Continuously monitor list of entities
YES
TAKE ACTION
Further IOC research and pivoting, as needed
Report as phish (Google, Symantec, PhishTank)
Request a domain takedown (Add-on)
Block domain in email gateway
Record metrics
In Recorded Future
Other Resource

Step 1

You identify what appears to be a typosquat or fraudulent domain via alerts generated by your Typosquatting Detection IGL Alerts. Proceed to the next step.

Step 2

Check to see if the domain is owned by your company:

- Perform a DNS Lookup in the Intelligence Card: Check the "A" record
- Check the parent and sibling domains
- Perform a WHOIS lookup (e.g., DomainTools)
- Check your internal company record

YES, the domain is owned by your company → Add the domain to your Domains Watch List

NO, the domain is now owned by your company → Proceed to the next step

Step 3

Find out if the domain is being used maliciously:

- Review references to the domain
- Perform a DNS Lookup in the Intelligence Card: Pivot to related IOCs
- Research the certificate (e.g., Censys)
- Check for website brand abuse (e.g., using URLScan)

NO, the domain is not being used maliciously → Add the domain to a List of Entities in the portal and set up continuous monitoring on that list

YES, the domain is being used maliciously → Proceed to the next step

Step 4

Take action:

- Request a domain takedown (Recorded Future add-on)
- Report as phish or malicious via Google, Symantec, Phishtank
- Conduct more IOC research, pivoting to other entities
- Block the domain in your email gateway
- Record metrics of value

Note: Purchasing a typosquat or potentially fraudulent domain (i.e., defensive registration) may be an option for your organization. For more information, we recommend you contact legal counsel and your Intelligence Services Consultant.

Have more questions regarding this topic: Submit a request

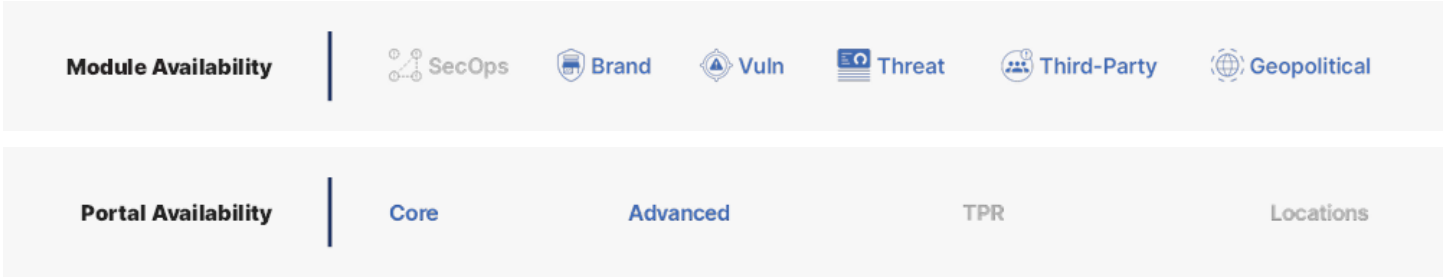
Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.

Leaked Payment Cards

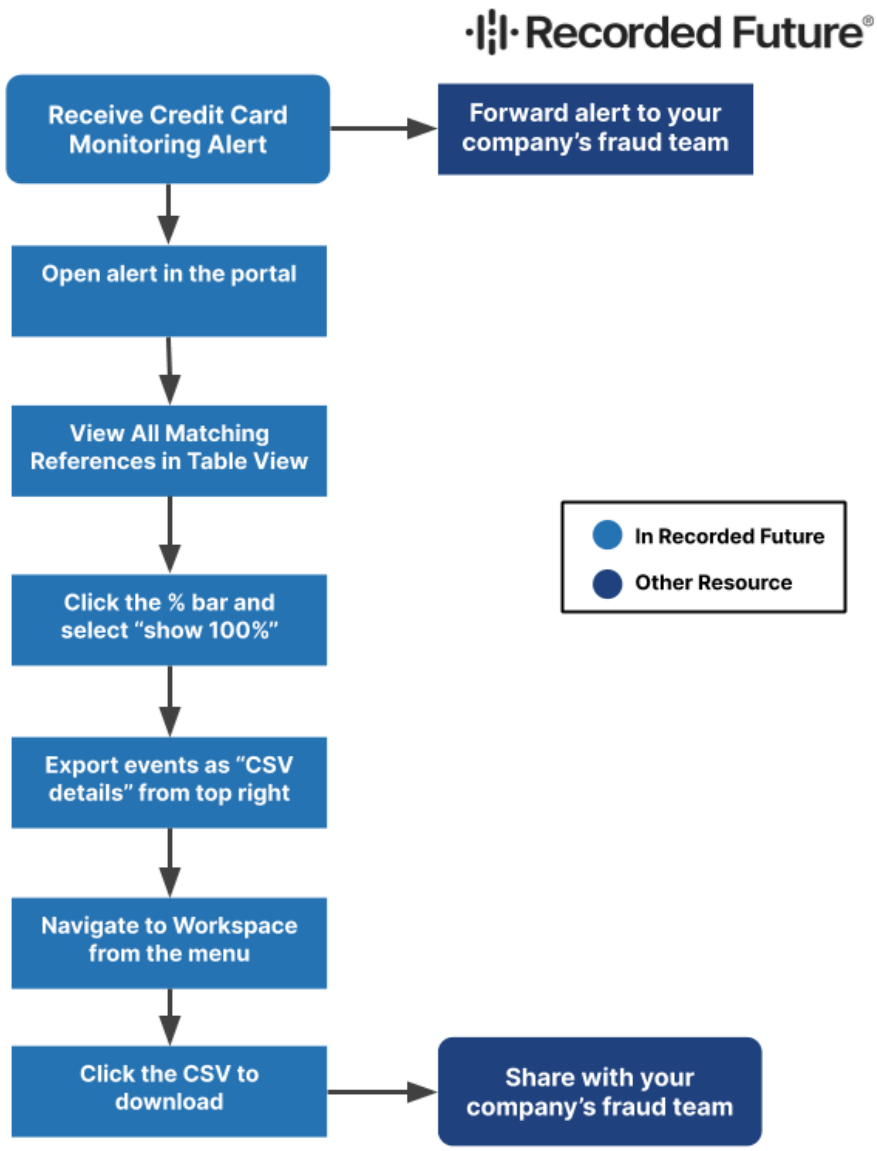
PLAYBOOK

1st edition

Leaked Payment Cards Playbook



Recorded Future's Leaked Payment Cards playbook walks you through triaging a Credit Card Monitoring alert from start to finish. If you have not yet set up your alerts, see activating certified alerts in the Intelligence Goals Library.



Step 1

You receive an alert that one or more credit cards belonging to your company have been stolen and posted online. Forward the alert to your company's fraud team before continuing in the Recorded Future portal.

Step 2

Open the alert in the Recorded Future portal.

Step 3

Click “View all matching references in Table View.”

Learn more about the Table View here.

Step 4

Click the % bar in the bottom right corner of the Table View and select “show 100%.”

Step 5

Click “Export” in the top right and “Export Events As CSV Details.”

Step 6

Navigate to “Workspace > Exports” from the Menu in the top right corner.

Step 7

Click to download the CSV from the Workspace.

Step 8

As a final step, share the CSV with your company’s fraud team.

Additional Information for Following Up on Leaked Payment Cards

If you do not have a Fraud team or if they request more information, the following ideas may be helpful beyond what is outlined above:

- Have the card disabled and a new one issued.
- Correlate all card information with the same date of publication on the dark web or with a publication date in the same month; investigate common e-commerce and online payments between those cards to identify a common point of purchase.
- Determine how the card information was collected to identify the root cause of the compromise. For example, if it was sniffed, this could be done via a vulnerable website that an attacker was able to compromise; if it was skimmed, you know that the card was physically compromised.

Have more questions regarding this topic: Submit a request

Need more help? Try asking your question in our RFUN Community, the client-exclusive workspace for sharing tradecraft, tools, and intelligence with other security professionals. You can email community@recordedfuture.com to request an invitation.