The Essential Guide to Rapid Response Against Sophisticated Ransomware Attacks

The Rise of Ransomware

With digitization becoming a mainstream phenomenon, cyber hacking is fast evolving to resemble the organized crime syndicates of yesteryear. If there is a type of attack that has been hugely successful and profitable for hackers, it's ransomware. Ransomware attacks can unfold like classic Hollywood crime thrillers. There is a villain or malicious perpetrator, an unsuspecting victim, hostage hijacking, and last but not least, a hefty ransom that needs to be paid before it's too late! Emotions run high on all sides. The victim is left at the mercy of the perpetrator and is looking to the incident responder to come to the rescue.

Ransomware as a Service and the Case of Double Extortion

Ransomware developers are offering ransomware-as-a-service (RaaS) kits, employing the same business model used by SaaS providers. This has resulted in the mass adoption of RaaS by cybercriminals and malicious threat actors with varying degrees of skill and sophistication. A common ransomware attack consists of the ransomware operator encrypting data and forcing the victim to pay a ransom to unlock it. In double extortion, ransomware operators encrypt and steal data to further coerce a victim into paying a ransom. If the victim doesn't pay the ransom, the ransomware operators then release the data on a leak site or dark web domain. The majority of leak sites are hosted on the dark web, where hosting locations are created and managed by ransomware operators. Sophisticated threat actors nowadays use encryption that is as strong as that used by banks to protect payments by their clients, making recovery of files and devices more complicated and, in some cases, impossible. Attackers now see great potential for massive profit and have begun demanding higher ransoms, targeting attacks on industries and organizations whose operations are most vulnerable to systems outages or data loss.

Prevention

Prevention is always better than cure. Every effort must be made to have relevant systems in place to prevent ransomware from making its way into the infrastructure. It is obviously cheaper to focus on prevention than to clean up after the fact. Having said that, given the increasing level of sophistication of threat actors and the relatively slower pace of advancement in preventative measures to prevent ransomware, it's highly unlikely any enterprise can truly be 100% secure against a sophisticated ransomware attack.

Automating the Post Intrusion Ransomware Response

Security teams face unique challenges in today's rapidly changing landscape of sophisticated attacks, expanding threat surfaces, and decentralized workforces. Collaboration across disparate teams and siloed tools adds additional layers of complexity to the day-to-day operations of security teams. The abundance of different systems makes it difficult to track and optimize the full lifecycle management of an incident. To overcome these challenges and enable security programs to scale, it's critical that organizations integrate, automate, and orchestrate as many security tasks as possible across the primary teams, tools, and systems.

For this purpose, Cortex® XSOAR has created an integration with its sister product, Cortex® XDR™. Leveraging the integration between the two platforms, your security team can automate and optimize complex workflows across the full stack of your information systems and tools. Using the Cortex XSOAR and XDR content pack will provide detection and response that natively integrates network, endpoint, and cloud data to stop sophisticated threats. This integration leverages XDR data for use within XSOAR, providing a single-pane-of-glass experience and playbooks that orchestrate broader end-to-end workflows across your whole environment, enabling direct execution of XDR actions within the Cortex XSOAR War Room.

Cortex XDR allows you to integrate endpoint, network, and cloud data to stop sophisticated attacks. The pairing of Cortex XSOAR with XDR's advanced detection and analytics platform leverages the full resources available to your security team. Advanced case management and workflow automation enable Cortex XSOAR users to immediately triage prioritized alerts and gain instant context around incidents. Utilize the full potential of your security resources, including the siloed enrichment data you already have, to expedite the investigation of your Cortex XDR incidents for faster qualified response times.

- Incident Management
  - » Automation of Post Intrusion response needs to be complemented by real-time investigation for complex workflows when human intervention is required. Cortex XSOAR accelerates the response actions by unifying alerts, incidents, and indicators from any source on a single platform for lightning-quick search, query, and investigation.
- Indicator Enrichment
  - » A central indicator repository enables searches and automated indicator correlation across ransomware and related incidents from multiple sources to spot duplicates, trends, and patterns.

- Response Actions
  - » Threat response actions and ransomware handling
    - The ransomware alerts construct the incident. It enriches indicators from your threat feed subscriptions and Palo Alto Networks native threat intel. The incident severity is then updated based on the associated indicator reputation, and an analyst is assigned for manual investigation. The analyst can then choose to initiate automated remediation with Palo Alto Networks NGFWs. After remediation is complete, the incident is closed automatically.
    - A dedicated Post Intrusion Ransomware Investigation and Response playbook kicks off to handle the ransomware. This provides the sequence of steps in the investigation of ransomware itself. The playbook requires the ransom note and an example of an encrypted file to identify the ransomware and find a recovery tool via online databases. The analyst is guided with further investigation steps throughout the playbook.

The Response Toolkit Walk-Through

To help incident responders combat this threat, Cortex XSOAR has just the toolkit to help the incident responder be more effective in dealing with these nefarious actors.

Cortex XSOAR's **Ransomware content pack** can immediately help incident response, threat intelligence, and SecOps teams standardize and speed up the Post Intrusion response processes. This content pack automates most of the ransomware response steps, allowing the incident response and SecOps teams to add their guidance and input. This pack can help incident responders better understand their position and exposure against threat actors by collecting the required information from your environment, executing the investigation steps, containing the incident, and visualizing the data with its custom Post Intrusion Ransomware layout.

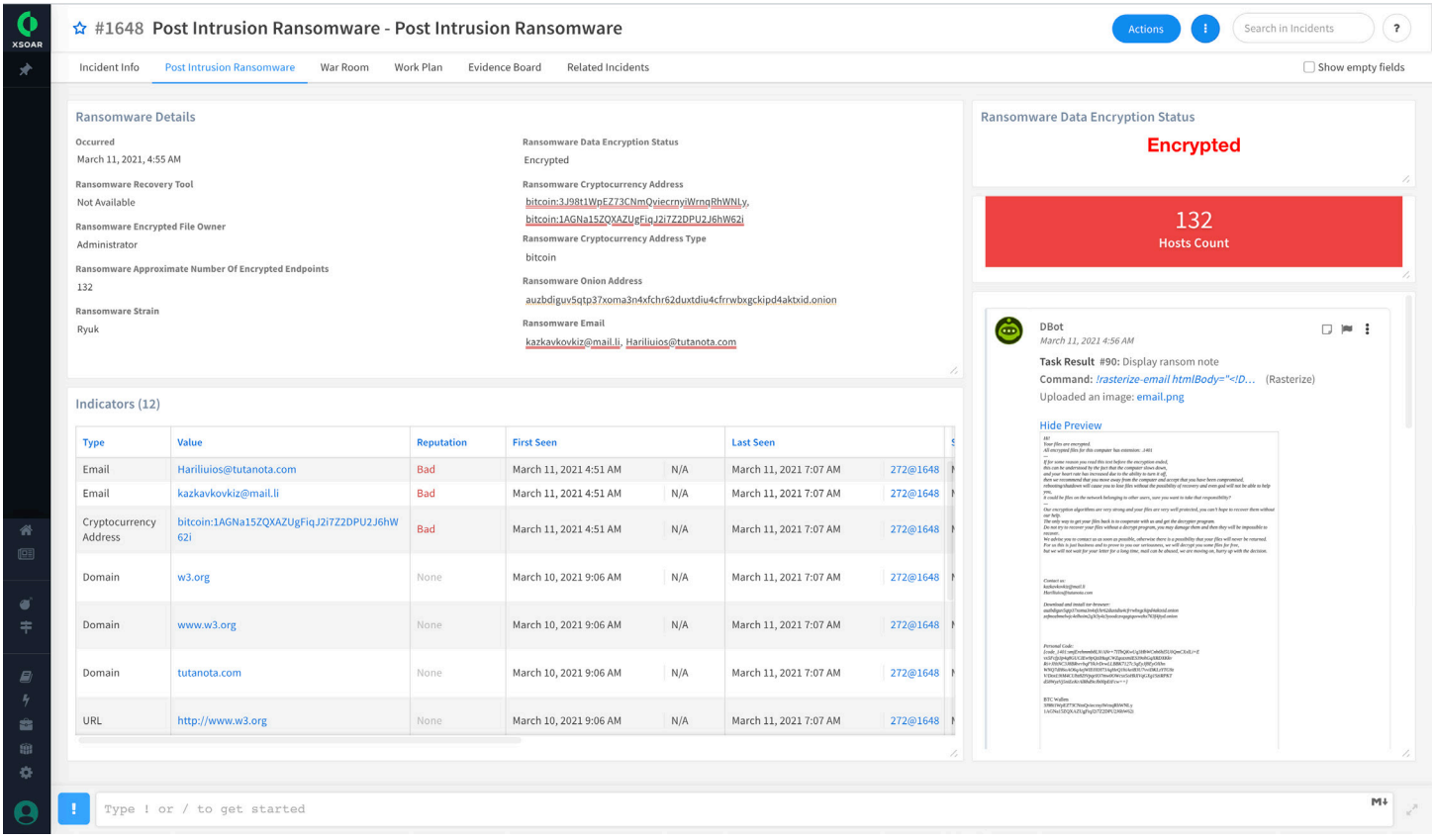

Figure 1: Ransomware content pack – dashboard layout

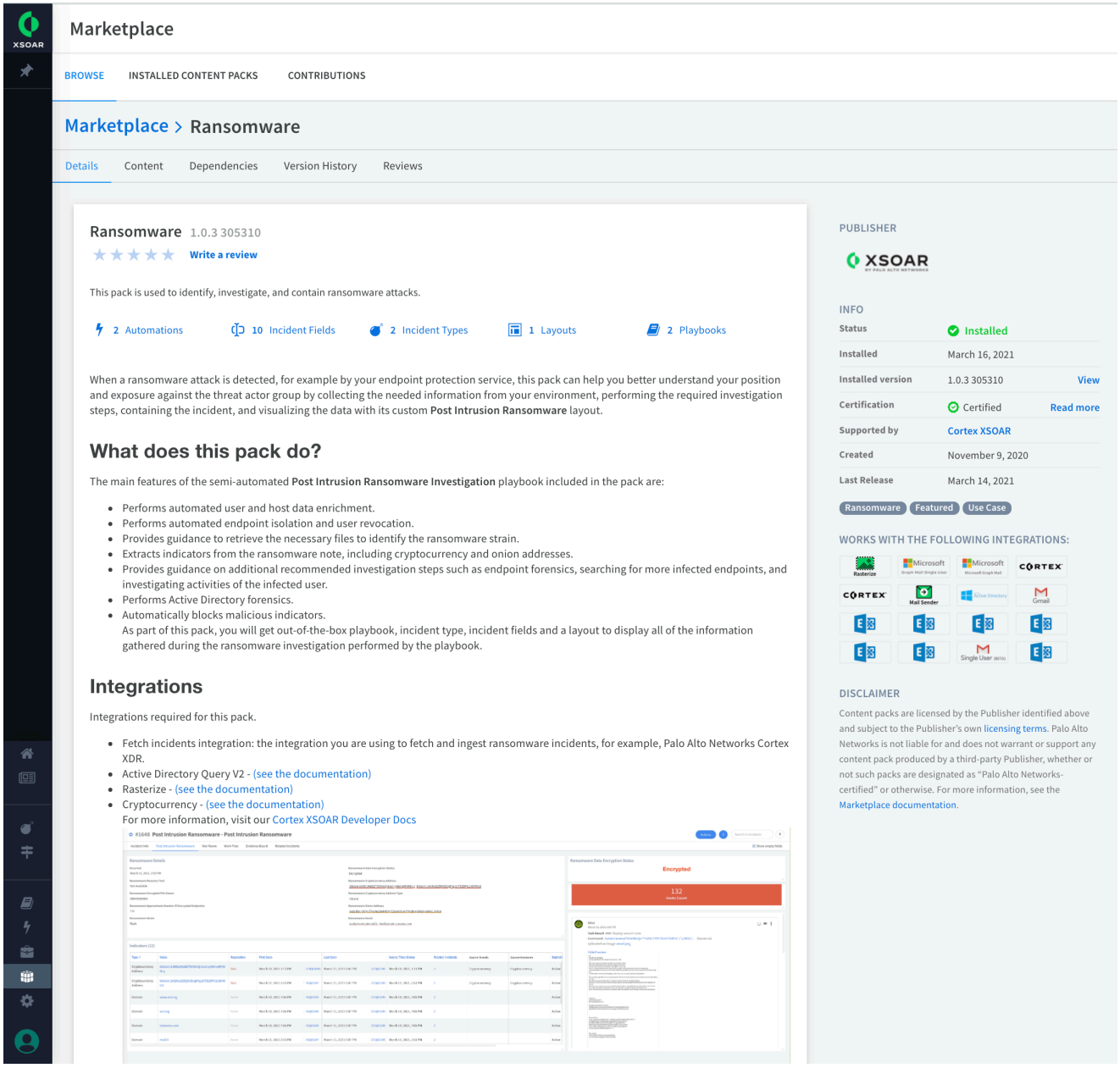

Figure 2: Ransomware content pack in the Cortex XSOAR Marketplace

How Does the Ransomware Content Pack Work?

When a ransomware attack is detected by one of several alert sources such as Cortex XDR, this pack automatically triggers the Post Intrusion Ransomware Investigation and Response playbook to identify, investigate, and contain the ransomware attack. The ransomware pack requires the ransom note and an example of an encrypted file to identify the ransomware variant and find the most appropriate recovery tool via the online database. All relevant stakeholders are automatically notified of the attack. The playbook includes a manual task for determining the incident timeline that is an essential part of the recovery process. Since the data encryption is the final step in the attack, prior attacker actions are investigated.

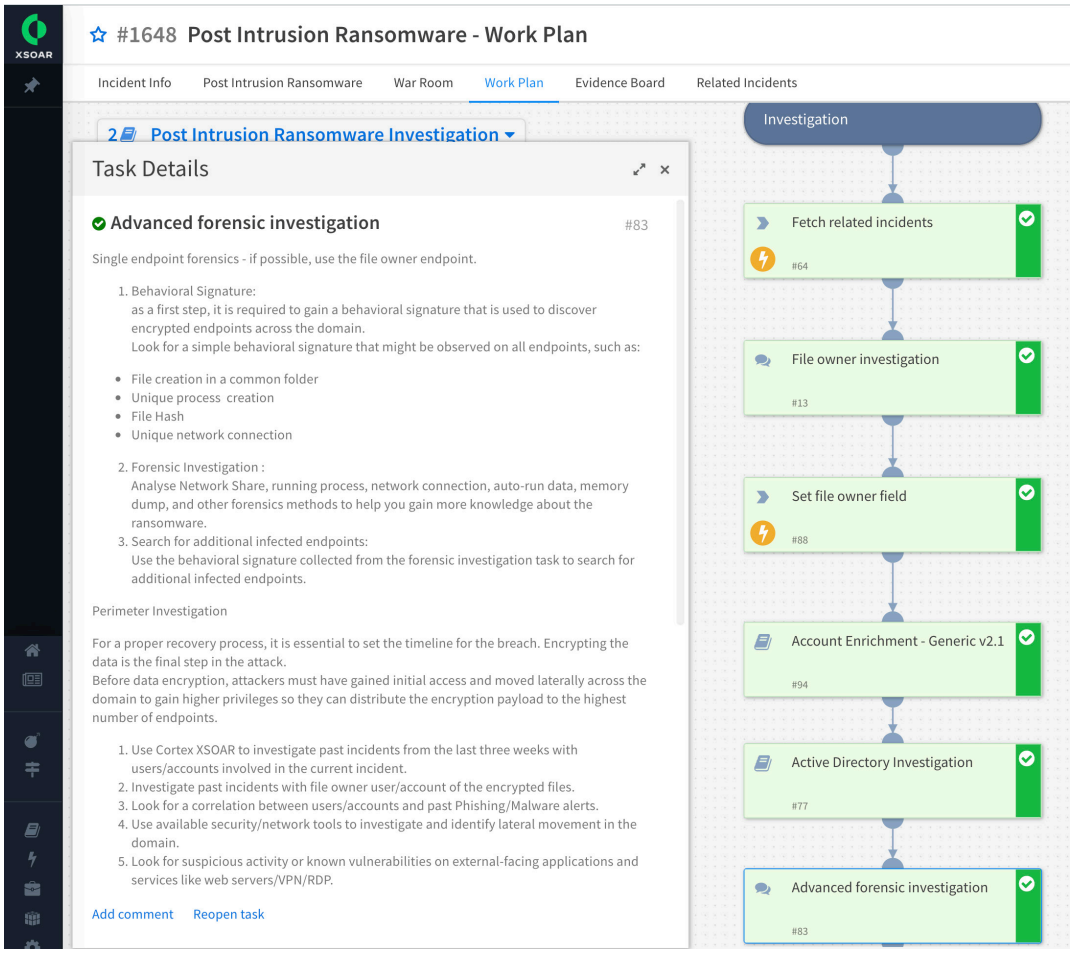

Figure 3: Expanded view of the advanced forensics investigation tasks in the playbook

The playbook includes options to further investigate the user's activity whose files were encrypted and identify additional endpoints that experienced the attack. If auto-remediation is approved, the malicious indicators from the ransom note are automatically blocked. Alternatively, the containment can be done manually as well.

To learn more about the associated integrations, playbooks, scripts, commands, and automations, please refer to the playbook documentation section.

Summary

With the help of the Ransomware content pack and Cortex XSOAR core capabilities and integrations, incident response, SecOps, and threat intel teams can save many hours of manual labor trying to piece disparate sources of information together from multiple tools. Cortex XSOAR can automate the whole process of user investigation, endpoint isolation, notifications, enrichment, and threat hunting by orchestrating across SIEM, firewalls, endpoint security, and threat intelligence sources so that response teams can quickly shut down the ransomware, minimize the risk of losing data, limit the financial impact of ransom demands and their impact on the enterprise.

Don't have Cortex XSOAR yet? Try the free Community Edition today.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com