Best practices for managing connected security data, no matter where it resides

Chris Meenan
Director, Security Intelligence Offering Management and Strategy
Please note

IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM’s sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
Security is fragmented, disconnected, & exacerbated by multicloud
What if security were unified, connected?

Gain security insights
Connect data

Take action faster
Connect workflows

Run anywhere
Connect openly
What you can achieve with connected security

Connect data
Operationalize threat intelligence for a consistent view of threats

Connect workflows
Orchestrate case management for consistent visibility and coordination across incidents

Connect openly
Reduce vendor lock-in by future-proofing with open and interoperable security
1. Federated query using a STIX pattern
2. Query is translated to the native query language of each of the data sources
3. The converted query is then sent (transmitted) to all data sources
4. Each data source runs its own native query
5. The native query results are then returned from the data source
6. Returned results translated into STIX Objects (basically a JSON structure)
7. The STIX Objects are then stored in the cloud where they are used by other services

Connecting data for unified insights

IBM QRadar

Federated query using a STIX pattern
Query is translated to the native query language of each of the data sources
The converted query is then sent (transmitted) to all data sources
Each data source runs its own native query

Operationalize threat intelligence with connected data

– Connect organization details to quickly focus on threats organized by relevance

– Connect threat sources to view threats in a consistent format

– Connect your data sources to scan for threat indicators in your environment
Example: Quickly understand if you’re affected by a new threat

Coronavirus Used In Android App Exploits

In its latest report, Symantec has found 11 Android applications purportedly used to track COVID-19 but are actually infected with malware.

Overview

Complete analysis

On March 20, in the midst of the COVID-19 pandemic, Symantec discovered 11 Android applications masquerading as legitimate applications for tracking COVID-19 patients. The apps were downloaded in large numbers after installation. The applications were created after March 20 during the most active spreading of the virus in Europe. The applications were targeting Daily but were also seen in the U.S. and France. The legitimate applications, named COVID Tracker apps, "present the risk of transmission of the malware containing the number, duration, and type of contacts (phone book)". While keeping track of the legitimate applications, the malicious worms also hold a malware that could download any payload from the attacker’s server. With this ability to download any payload, the malware could be used to infect the victim device with any type of additional malware, such as a ransomware, malware, and other types of malware. The researchers were able to detect the server address as well as a second server address.

Recommendation

- Use only known, backed software to gather the latest on these types of pandemics.
- Use an anti-virus program on your mobile device with up-to-date definitions.
- Keep applications and operating systems running at the current released patch level.
- Delete any shared software to help alleviate any further complications that could arise.

Sources

Orchestrate case management with connected workflows

- Organize analyst workflows within cases for simple coordination
- Connect data seamlessly across one platform for greater visibility
- Improve investigations with stronger connections across data and case activity
Example: Find connections between activity in different data sources
Reduce vendor lock-in by connecting openly

- Adopt built-in security capabilities to maximize best-of-breed from new vendors
- Increase overall security by adding without duplicating capabilities or data
- Easily adapt to new technologies with open standards to maximize value and minimize duplication
IBM Cloud Pak for Security

Security capabilities

Core platform services

Hybrid multicloud architecture

Open integration with existing security tools and data sources

Unified Security Workflows

Threat Intelligence Insights:
Prioritized, actionable threat intelligence

Data Explorer:
Federated search for investigation

Resilient:
Incident response and team collaboration

Universal data insights
Security orchestration & automation
Development framework

Open Hybrid Multicloud Platform

IBM Cloud
AWS
Microsoft Azure
Google Cloud

QRadar
Guardium
tenable
splunk
IBM Cloud

elasticsearch
Carbon Black
BigFix
Microsoft
aws
Thank you

Chris Meenan
Director, Security Intelligence
Offering Management and Strategy

—
c.meenan@ibm.com
ibm.com/security
Notices and disclaimers

© 2020 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity. IBM products and services are warranted per the terms and conditions of the agreements under which they are provided. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM’s future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM’s products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at: [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).