Incident Name:

Investigation Date:

Escalation Date:

MTTR:

Copyright

Contents

Incident Handling Workflow

When an anomaly is detected by implemented use cases, the L1 Analyst performs the initial investigation to verdict the anomaly as a True Positive or a False Positive. If the anomaly is found to be true positive, the analyst initiates the incident triage to gather all relevant information related to that detected anomaly and creates an investigation. L2 Analyst firstly, analyze the complete investigation to confirm the True Positive nature of the anomaly and populate the evidence along with the other relevant information required to add in the investigation. After the population and gathering, L2 analyst update the investigation to confirmed incidents and reports that to the relevant team with relevant and effective remediation and continuous to take follow-ups until the remediation has been performed.

Alert Information

Alert Summary L1			
First Handler	Justin		
Alert Type	New/Follow-up		
Alert Name	Phish Delivered to Mary Jane		
Time Generated	Hh:mm:ss DD:MM:YY		
Alert Severity	Critical/High/Medium/Low/Informational		
Product	Office 365/ Defender/ Firewall/ Proxy/UEBA		
Compromised Entity Type	Hostname	**Entity**	JA-Laptop 10.24.19.203
Detection Time	Hh:mm:ss DD:MM:YY	**Investigation Time**	Hh:mm:ss DD:MM:YY
Follow up Time	Hh:mm:ss DD:MM:YY	**Response Time**	Hh:mm:ss DD:MM:YY

Analysis:

Dear Team, We have recieved an alert on ss:mm:hh DD:MM:YY from the Office 365 stating that Phish delievered to Mary Jane, the email sender was johndoe@example.com and subject was (Warning: Your account is blocked), the email also contain an attachment of the below mentioned URL (www[.]example2[.]com) asking the user to initiate the request for account unblocking.

Upon further analysis, we have found that the email sender domain is marked malicious on MXTool Box and following URL contains bad reputation on different OSINT platforms (e.g Virus Total, Cisco Talos and etc), For your reference; Evidences are attached.

Moreover, the email was delieverd successfully to the user indicating that the control was unable to quarantine or blocked the email from sender.

The email sender was also found in the following IOCs presents on Github or OSINT platform.

Analysis on URL:

Upon running the URL on Anyrun platform, we have found that the URL is a fake website asking user to put their credentials for initiating a request to

	unblock their outlook account and also the URL requesting following IP (1.2.3.4) which is marked as a CnC Server located in Russia.

Remediation Steps:

- Kindly block the following domain, URL and IP address on respective controls
  - www[.]example1[.]com
  - example[.]com
  - 1.2.3.4
- Kindly initiate the deep scan on the involved host
- Train user to not to open emails from unknown sender.
- Delete the email from the sender after sending the email to InfoSec Team for further analysis.

Evidence

Evidence 1: Alert received

Evidence 2: Alert involved entities

Evidence 3: IOCs reputations