

Claims

1. A computer-implemented method comprising:

receiving automated or manual notification of an attack targeted at a computing device;

responsive to the receiving, configuring a monitored computing process or device to pose as the computing device targeted by the attack;

transitioning the attack to a monitored computing process or device that is configured to pose to an adversary as a from the computing device impacted targeted by the attack to the monitored computing process or device; and

enabling the adversary to obtain deceptive information from the monitored computing process or device; and

correlating information obtained from monitoring attacks on multiple monitored computing processes or devices.

2. The method of claim 1, wherein the attack is one of a spearfish email, a clickable link, a website, a drive by exploit, a QR code, a Near Field Communications (NFC) triggered link, a document, an executable, a removable drive, or an archive.

3. The method of claim 1, wherein receiving the automated or manual notification comprises retrieving the attack from an information sharing system or portal to which the attack has been submitted, and transitioning the attack comprises installing the attack on a monitored computing process or device.

4. The method of claim 3, wherein the information sharing system or portal receives or retrieves the attack from a different entity other than the entity performing the receiving, transitioning, and enabling.

5. The method of claim 1, wherein the notification is received from a person forwarding the attack or from a security agent or service monitoring the impacted computing device.

6. The method of claim 1, further comprising blocking processing of the attack on the impacted computing device.

7. The method of claim 1, further comprising processing the attack on the monitored computing process or device.

8. The method of claim 1, wherein the monitored computing process or device is a physical machine or virtual machine.

5 9. The method of claim 8, wherein the physical machine or virtual machine is configured with an image of the impacted computing device.

10 10. The method of claim 8, wherein the machine is configured with an image that includes at least one or more of a user name, a machine name, an operating system version, desktop screens, folder names, preloaded files or computer firmware versions associated with the impacted computing device.

11. The method of claim 1, wherein the monitored computing process or device is an isolated sandbox on the impacted computing device.

15 12. The method of claim 1, wherein the monitored computing process or device is located on a network of an entity associated with the impacted computing device or is implemented remotely by a security service.

20 13. The method of claim 12, wherein the monitored computing process or device is implemented remotely by the security service while being assigned a network address or domain associated with the entity.

25 14. The method of claim 1, wherein the monitored computing process or device mimics user activity.

30 15. The method of claim 1, further comprising monitoring commands and events issued by the adversary or monitoring network activity, file activity, process activity, execution activity, registry activity, operating system activity, firmware updates, loaded drivers, or kernel extensions of the monitored computing process or device.

16. The method of claim 15, wherein the commands and events issued include keystrokes, mouse activity, or command line interface activity.

35 17. The method of claim 15, further comprising updating a configuration for a security agent of the impacted computing device or providing human-consumable intelligence based at least in part on intelligence derived from the monitoring.

18. The method of claim 1, further comprising enabling an entity associated with the impacted computing device to provide deceptive information for inclusion on the monitored computing process or device.

5 19. The method of claim 1, further comprising monitoring the attack on the monitored computing process or device and providing deceptive information to the adversary repeatedly over a time period.

10 ~~20. The method of claim 1, further comprising correlating information obtained from monitoring attacks on multiple monitored computing processes or devices.~~

~~2024. The method of claim 120, wherein the monitored computing processes or devices are operated by different entities.~~

15 ~~2122. The method of claim 1, further comprising intercepting and decoding communications associated with the attack.~~

~~2223. The method of claim 1, further comprising receiving intelligence from the adversary about at least one of the adversary's tools, tactics, techniques, or procedures.~~

20 ~~24. One or more tangible computer-readable media storing computer-executable instructions configured to program one or more computing devices to perform operations comprising:~~

~~— configuring a document to report identifying information of a device opening the document to the one or more computing devices;~~

25 ~~— receiving a report associated with the document, the report including the identifying information;~~

~~— determining, based on the identifying information that an unauthorized entity is in possession of the document; and~~

30 ~~— alerting an entity associated with the document of the possession by the unauthorized entity.~~

~~25. The one or more tangible computer-readable media of claim 24, wherein the configuring includes embedding executable instructions or a link in the document.~~

35

26. ~~The one or more tangible computer-readable media of claim 25, wherein the link embedded in the document is configured to cause a request to a monitored network address.~~

27. ~~The one or more tangible computer-readable media of claim 25, wherein the executable instructions embedded in the document are configured to open a connection to the one or more computing devices.~~

28. ~~The one or more tangible computer-readable media of claim 25, wherein the executable instructions embedded in the document perform the reporting based at least in part on whether the identifying information differs from identifying information embedded in the document.~~

29. ~~The one or more tangible computer-readable media of claim 24, wherein the identifying information comprises at least one of a network address, a geographic location, a universally unique identifier (UUID), domain information, or derived/upstream network data.~~

30. ~~A computer-implemented method comprising:~~

~~—receiving a domain name resolution request from a requesting process;~~

~~—determining that a domain name included in the domain name resolution request is indicative of malicious activity; and~~

~~—responding to the domain name resolution request with a network address of a monitored computing process or device to cause the requesting process to communicate with the monitored computing process or device in place of an adversary server.~~

31. ~~The method of claim 30, wherein the receiving comprises redirecting the domain name resolution request from a domain name server associated with a device or entity implementing the requesting process.~~

32. ~~The method of claim 30, wherein the determining comprises determining whether the domain name is included in a list of known malicious or suspicious domains.~~

33. ~~The method of claim 30, wherein the determining comprises determining that the domain name is unfamiliar, is associated with a specific geographic location, or is associated with a specific entity.~~

34. ~~The method of claim 30, wherein the monitored computing process or device poses as an adversary command-and-control system or an adversary exfiltration system to the requesting process, the requesting process being part of an attack, or intercepts communications of the requesting process to the adversary command-and-control system.~~

35. ~~The method of claim 30, wherein the monitored computing process or device decodes the communications from the requesting process.~~

36. ~~The method of claim 30, wherein the monitored computing process or device determines that the requesting process is utilizing a specific protocol to encode the communications and selects an appropriate communications protocol for decoding or attempts to learn the specific protocol.~~

37. ~~The method of claim 30, further comprising alerting at least one of a security agent or users of an entity affected by an attack associated with the requesting process.~~

38. ~~The method of claim 30, further comprising transitioning an attack associated with the requesting process to a monitored computing process or device, the monitored computing process or device posing as a computing device impacted by the attack.~~

39. ~~A system comprising:~~

~~— one or more processors;~~

~~— a repository of dormant domain names associated with malicious activity;~~

~~— a monitoring module operated by the one or more processors and configured to monitor for changes to name resolutions or registrations of domain names included in the repository; and~~

~~— a response module operated by the one or more processors and configured to perform at least one of updating a security device or agent configuration or alerting a security service user based on the detected changes.~~

40. ~~The system of claim 39, wherein the monitoring for changes includes continuously or periodically resolving the dormant domain names to determine if their name resolutions have changed.~~

41. ~~The system of claim 39, further comprising a detection module to identify domain names that resolve to local network addresses, domain names that resolve to non-routable network addresses, or domain names that fail to resolve, to ascertain whether the domain names are associated with malicious activity, and to add the domain names to the repository based at least in part on the ascertaining.~~

42. ~~The system of claim 39, further comprising a deception module to associate a monitored computing process or device with one of the dormant domain names and, in response to the dormant domain name becoming active, to respond to domain name resolution requests specifying the now-active domain name with a network address of the monitored computing process or device.~~